

# Wielomiany

## § II.1. Określenie wielomianu. Pierścienie wielomianowe

(II.1) DEFINICJA. *Wielomianem nad pierścieniem  $\mathcal{A}$  albo po prostu wielomianem nazywamy każdy ciąg nieskończony*

$$(i) \quad a := (a_0, a_1, \dots), \quad a_0, a_1, \dots \in \mathcal{A},$$

spełniający warunek

$$(II.2) \quad \bigvee_{n \in \mathbb{N}} \bigwedge_{k \geq n} a_k = 0. \quad \blacksquare$$

(II.3) DEFINICJA. *Współczynnikami wielomianu (i) nazywamy elementy  $a_0, a_1, \dots$*   $\blacksquare$

(II.4) DEFINICJA. *Wyrazem wolnym wielomianu (i) nazywamy jego współczynnik  $a_0$ .*  $\blacksquare$

(II.5) DEFINICJA. *Wielomian (i) nazywamy zerowym wtedy i tylko wtedy, gdy jego wszystkie współczynniki są  $\mathcal{A}$ -zerami.*  $\blacksquare$

(II.6) DEFINICJA. *W pierścieniu  $\mathcal{A}$  z jedyneką wielomian (i) nazywamy jedynkowym wtedy i tylko wtedy, gdy  $a_0 = 1$ , a wszystkie pozostałe współczynniki są  $\mathcal{A}$ -zerami.*  $\blacksquare$

W niniejszym rozdziale wielomian zerowy oznaczamy symbolem  $o$ , a wielomian jedynkowy symbolem  $e$ . Mamy zatem

$$o := (0, 0, \dots), \quad e := (1, 0, 0, \dots).$$

(II.7) DEFINICJA. *Stopniem wielomianu niezerowego (i) nazywamy taką liczbę całkowitą nieujemną  $n$ , że*

$$a_n \neq 0 \wedge \bigwedge_{k > n} a_k = 0.$$

Stopniem wielomianu zerowego nazywamy liczbę nieskończoną  $-\infty$ .  $\blacksquare$

Stopień wielomianu (i) oznaczamy symbolem  $\text{st } a$ .

(II.8) DEFINICJA. *Wielomian (i) nazywamy statym wtedy i tylko wtedy, gdy  $\text{st } a = 0$  albo  $\text{st } a = -\infty$ .*  $\blacksquare$

(II.9) DEFINICJA. Najwyższym współczynnikiem wielomianu niezerowego (i) nazywamy współczynnik  $a_n$ , gdzie  $n := \text{st } a$ . Wielomian zerowy nie ma najwyższego współczynnika. ■

(II.10) DEFINICJA. Wielomian nazywamy *lewostronnie* (*prawostronnie*) *nieosobliwym* wtedy i tylko wtedy, gdy nie jest zerowy, a jego najwyższy współczynnik ma lewą (prawą) odwrotność. Wielomian nazywamy *nieosobliwym* wtedy i tylko wtedy, gdy jest zarówno lewostronnie jak i prawostronnie nieosobliwy, tzn. gdy jest niezerowy i jego najwyższy współczynnik jest odwracalny. ■

(II.11) DEFINICJA. Wielomian nad pierścieniem z jedynek  $\mathcal{A}$  nazywamy *monicznym* wtedy i tylko wtedy, gdy nie jest zerowy, a jego najwyższy współczynnik jest  $\mathcal{A}$ -jedyką. ■

Z powyższych definicji wynika, że każdy wielomian moniczny jest nieosobliwy.

(II.12) DEFINICJA. Pierścieniem wielomianowym generowanym przez pierścień  $\mathcal{A}$  albo po prostu *pierścieniem wielomianowym* nazywamy pierścień

$$(ii) \quad \mathcal{P}[\mathcal{A}] := (\mathfrak{P}[\mathcal{A}], +, \cdot, -, o),$$

w przypadku pierścienia  $\mathcal{A}$  z jedyką — pierścień z jedyką

$$(iii) \quad \mathcal{P}[\mathcal{A}] := (\mathfrak{P}[\mathcal{A}], +, \cdot, -, o, e),$$

a w przypadku pierścienia  $\mathcal{A}$  z transpozycją — pierścień z transpozycją

$$(iv) \quad \mathcal{P}[\mathcal{A}] := (\mathfrak{P}[\mathcal{A}], +, \cdot, -, s, t, o, e),$$

gdzie  $\mathfrak{P}[\mathcal{A}]$  jest zbiorem wszystkich wielomianów nad pierścieniem  $\mathcal{A}$ , a  $+$ ,  $\cdot$ ,  $-$ ,  $s$ ,  $t$  są operacjami określonymi dla dowolnych wielomianów

$$(v) \quad a := (a_0, a_1, \dots), \quad b := (b_0, b_1, \dots), \quad a_0, b_0, a_1, b_1, \dots \in \mathcal{A},$$

wzorami:

$$(II.13) \quad a + b := (a_0 + b_0, a_1 + b_1, \dots),$$

$$(II.14) \quad ab := (c_0, c_1, \dots),$$

gdzie  $c_k := \sum_{j=0}^k a_j b_{k-j}$  dla  $k=0, 1, \dots$ ,

$$(II.15) \quad -a := (-a_0, -a_1, \dots),$$

$$(II.16) \quad \bar{a} := (\bar{a}_0, \bar{a}_1, \dots),$$

$$(II.17) \quad a^T := (a_0^T, a_1^T, \dots). \quad \blacksquare$$

Sprawdzamy z łatwością, że dla pierścienia (ii) są spełnione wszystkie warunki (I.39), ..., (I.45), dla pierścienia (iii) ponadto

$$(II.18)_e \quad ea = ae = a,$$

a dla pierścienia (iv) jeszcze warunki (I.62), ..., (I.68).

Pierścień wielomianowy (iii) i (iv) traktujemy jako pierścień nad pierścieniem z jedyką  $\mathcal{A}$ , przyjmując, że dla dowolnego wielomianu (i) i dowolnego elementu  $\alpha \in \mathcal{A}$

jest

$$(II.19) \quad \alpha a := (\alpha a_0, \alpha a_1, \dots),$$

$$(II.20) \quad a\alpha := (a_0\alpha, a_1\alpha, \dots).$$

Sprawdzamy z łatwością, że są wtedy spełnione wszystkie warunki (I.193), ..., (I.208), gdzie  $o$  jest wielomianem zerowym, a  $e$  wielomianem jedynkowym pierścienia  $\mathcal{P}[\mathcal{A}]$ .

(II.21) TWIERDZENIE. Dla dowolnych wielomianów (v) jest

$$(II.22) \quad \text{st}(a+b) \leq \max(\text{st } a, \text{st } b),$$

$$(II.23) \quad \text{st}(ab) \leq \text{st } a + \text{st } b,$$

$$(II.24) \quad \text{st } a = \text{st } \bar{a} = \text{st } a^T = \text{st } a^*.$$

We wzorze (II.22) mamy ostrą nierówność  $<$  jedynie wtedy, gdy  $\text{st } a = \text{st } b \neq -\infty$  i suma najwyższych współczynników wielomianów  $a$  i  $b$  jest równa 0. W pozostałych przypadkach w (II.22) mamy równość. We wzorze (II.23) mamy ostrą nierówność  $<$  jedynie wtedy, gdy wielomiany  $a$ ,  $b$  są niezerowe, a iloczyn ich najwyższych współczynników jest równy 0. W pozostałych przypadkach w (II.23) mamy równość.

Dowód. Niech  $\text{st } a = m$ ,  $\text{st } b = n$ ,  $m, n \neq -\infty$ . Zatem

$$a := (a_0, a_1, \dots, a_m, 0, 0, \dots), \quad b := (b_0, b_1, \dots, b_n, 0, 0, \dots), \quad a_m, b_n \neq 0.$$

Mamy  $(a+b)_k = a_k + b_k = 0$  dla  $k > \max(m, n)$ . Jeżeli  $m < n$ , to  $(a+b)_n = b_n \neq 0$ , a jeżeli  $m > n$ , to  $(a+b)_m = a_m \neq 0$ , wobec czego dla  $m \neq n$  jest  $\text{st}(a+b) = \max(\text{st } a, \text{st } b)$ . Jeżeli  $m = n$ , to  $(a+b)_m = a_m + b_m$  i jeżeli  $a_m + b_m \neq 0$ , to  $\text{st}(a+b) = \max(\text{st } a, \text{st } b)$ , a jeżeli  $a_m + b_m = 0$ , to  $\text{st}(a+b) < \max(\text{st } a, \text{st } b)$ . Mamy dalej  $(ab)_k = 0$  dla  $k > m+n$  i  $(ab)_{m+n} = a_m b_n$ . Jeżeli  $a_m b_n \neq 0$ , to  $\text{st}(ab) = \text{st } a + \text{st } b$ , a jeżeli  $a_m b_n = 0$ , to  $\text{st}(ab) < \text{st } a + \text{st } b$ .

Jeżeli  $m = -\infty$ , to  $a = o$  i  $\text{st}(a+b) = \text{st } b = \max(\text{st } a, \text{st } b)$  oraz  $\text{st}(ab) = \text{st } o = -\infty = -\infty + \text{st } b = \text{st } a + \text{st } b$ . Jeżeli  $n = -\infty$ , to  $b = o$  i, analogicznie,  $\text{st}(a+b) = \max(\text{st } a, \text{st } b)$  i  $\text{st}(ab) = \text{st } a + \text{st } b$ .

Jeżeli  $m = -\infty$ , to  $a = \bar{a} = a^T = a^* = o$  i  $\text{st } a = \text{st } \bar{a} = \text{st } a^T = \text{st } a^*$ . Jeżeli  $m \neq -\infty$  i  $a := (a_0, a_1, \dots, a_m, 0, 0, \dots)$ ,  $a_m \neq 0$ , to na mocy (I.91)  $\bar{a}_m \neq 0$ ,  $a_m^T \neq 0$ ,  $a_m^* \neq 0$  i wobec tego również  $\text{st } a = \text{st } \bar{a} = \text{st } a^T = \text{st } a^*$ . ■

(II.25) TWIERDZENIE. Jeżeli dla wielomianów (v)  $a$  jest lewostronnie nieosobliwy albo  $b$  prawostronnie nieosobliwy, albo pierścień  $\mathcal{A}$  nie zawiera właściwych dzielników zera, to

$$(II.26) \quad \text{st}(ab) = \text{st } a + \text{st } b.$$

Dowód. Gdyby wzór (II.26) nie zachodził, wtedy na mocy twierdzenia (II.21) wielomiany  $a$  i  $b$  byłyby niezerowe, a iloczyn ich najwyższych współczynników  $a_m \neq 0$  i  $b_n \neq 0$  byłby  $a_m b_n = 0$ . Jeżeli  $a$  jest lewostronnie nieosobliwy, to oznacza to, że  $a_m$  ma lewą odwrotność  $\alpha$  i otrzymalibyśmy  $\alpha a_m b_n = 0$ , czyli  $b_n = 0$ , co byłoby sprzeczne. Jeżeli  $b$  jest prawostronnie nieosobliwy, to otrzymalibyśmy analogiczną sprzeczność. Gdy pierścień  $\mathcal{A}$  nie ma właściwych dzielników zera, wtedy dla  $a_m \neq 0$  i  $b_n \neq 0$  musi być  $a_m b_n \neq 0$ . Stąd wynika teza. ■

Niech teraz  $\mathcal{A}$  będzie pierścieniem z jedyneką i niech

$$(II.27) \quad \lambda := (0, 1, 0, 0, 0, \dots).$$

Z łatwością dowodzimy przez indukcję, że dla dowolnego  $k \in \mathbb{N}_0$

$$\lambda^k = (\underbrace{0, \dots, 0}_{k \text{ razy}}, 1, 0, 0, \dots)$$

i dla dowolnego  $\alpha \in \mathcal{A}$  jest  $\alpha \lambda^k = \lambda^k \alpha$ . Wobec tego każdy wielomian  $a := (a_0, a_1, \dots)$  można napisać w postaci:

$$(II.28) \quad a = \sum_{j=0}^{\infty} a_j \lambda^j = \sum_{j=0}^{\infty} \lambda^j a_j,$$

gdzie  $\lambda^0 = e$ . Przyjmując, że

$$\sum_{j=0}^n a_j \lambda^j = \sum_{j=0}^n \lambda^j a_j = 0 \quad \text{dla} \quad n < 0,$$

możemy wzór (II.28) napisać w postaci:

$$(II.29) \quad a = \sum_{j=0}^n a_j \lambda^j = \sum_{j=0}^n \lambda^j a_j, \quad \text{gdzie} \quad n := \text{st } a.$$

(II.30) PRZYKŁAD. Wielomiany w zakresie, w jakim poznajemy je w szkole średniej, są to wielomiany postaci (II.29), generowane przez ciało liczb rzeczywistych  $\mathcal{R}$ . Jednak – mimo podobieństwa formy – występuje zasadnicza różnica. W szkole średniej określa się wielomiany (II.29) jako funkcje zmiennej  $\lambda$ , podczas gdy tutaj  $\lambda$  jest konkretnym ciągiem (II.27). Algebraiczna definicja (II.1) wielomianów jest – zdaniem autora – wygodniejsza od funkcyjnej, a podobieństwo formy powinno czytelnikowi ułatwić przyswojenie sobie faktów wynikających z przedstawionej teorii. Ponadto – jak zobaczymy niżej – algebraiczna definicja wielomianów nie wyklucza możliwości funkcyjnego ich traktowania przez wprowadzenie pojęcia funkcji wielomianowej. ■

## § II.2. Wartość wielomianu w punkcie. Pierwiastki wielomianu

(II.31) DEFINICJA. Lewą (prawą) wartością wielomianu (II.29) nad pierścieniem z jedyneką  $\mathcal{A}$  w punkcie  $x \in \mathcal{X}$ , gdzie  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedyneką  $\mathcal{A}$ , nazywamy element  ${}_{(x)}a \in \mathcal{X}$ . ( $a_{(x)} \in \mathcal{X}$ ) określony wzorem:

$$(II.32) \quad {}_{(x)}a := \sum_{j=0}^n x^j a_j \quad (a_{(x)} := \sum_{j=0}^n a_j x^j). \quad \blacksquare$$

(II.33) DEFINICJA. Jeżeli  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedyneką  $\mathcal{A}$  i jeżeli lewa wartość wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  w punkcie  $x \in \mathcal{X}$  jest równa prawej, tzn.  ${}_{(x)}a = a_{(x)}$ , to nazywamy ją wartością wielomianu  $a$  w punkcie  $x$  i oznaczamy symbolem  $a(x)$ . ■

(II.34) PRZYKŁAD. Jak wynika z porównania wzorów (II.29) i (II.32), wartość wielomianu  $a \in \mathcal{P}[\mathcal{A}]$ , gdzie  $\mathcal{A}$  jest pierścieniem z jedyneką, w punkcie  $\lambda \in \mathcal{P}[\mathcal{A}]$ , gdzie  $\lambda$  jest wielomianem (II.27), jest równa samemu wielomianowi  $a$ , czyli

$$(II.35) \quad a(\lambda) = a. \quad \blacksquare$$

(II.36) DEFINICJA. Jeżeli  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedyneką  $\mathcal{A}$ , to *prawym (lewym) iloczynem dowolnego elementu  $x \in \mathcal{X}$  przez dowolny wielomian  $a := (a_0, a_1, \dots) \in \mathcal{P}[\mathcal{A}]$  nazywamy wielomian*

$$(II.37) \quad xa := (xa_0, xa_1, \dots) \in \mathcal{P}[\mathcal{X}] \quad (ax := (a_0x, a_1x, \dots) \in \mathcal{P}[\mathcal{X}]). \quad \blacksquare$$

(II.38) TWIERDZENIE. Dla lewej (prawej) wartości sumy wielomianów

$$(i) \quad a := (a_0, a_1, \dots), \quad b := (b_0, b_1, \dots), \quad a_0, b_0, a_1, b_1, \dots \in \mathcal{A}$$

w punkcie  $x \in \mathcal{X}$ , gdzie  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedyneką  $\mathcal{A}$ , zachodzi wzór

$$(II.39) \quad {}_{(x)}(a+b) = {}_{(x)}a + {}_{(x)}b \quad ((a+b)_{(x)} = a_{(x)} + b_{(x)}).$$

Dla lewej (prawej) wartości iloczynu wielomianów (i) w punkcie  $x \in \mathcal{X}$  mamy

$$(II.40) \quad {}_{(x)}(ab) = {}_{(x)}({}_{(x)}a \cdot b) \quad ((ab)_{(x)} = (a \cdot b)_{(x)}).$$

Dowód. Wzór (II.39) wynika bezpośrednio z określenia lewej (prawej) wartości wielomianu w punkcie  $x$  oraz wzoru (II.13). Dla iloczynu wielomianów (i) mamy na mocy (II.41)

$$(ii) \quad {}_{(x)}(ab) = \sum_{k=0}^{\infty} x^k \sum_{j=0}^k a_j b_{k-j} = \sum_{k=0}^{\infty} \sum_{j=0}^k x^k a_j b_{k-j} = \sum_{j=0}^{\infty} \sum_{k=j}^{\infty} x^{k-j} x^j a_j b_{k-j} = \\ = \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} x^k x^j a_j b_k = \sum_{k=0}^{\infty} x^k \left( \sum_{j=0}^{\infty} x^j a_j \right) b_k = {}_{(x)}({}_{(x)}a \cdot b).$$

Dowód dla prawej wartości jest analogiczny.  $\blacksquare$

(II.41) TWIERDZENIE. Jeżeli  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedyneką  $\mathcal{A}$  i jest przemienny, to wzór (II.40) jest równoważny wzorowi

$$(II.42) \quad {}_{(x)}(ab) = {}_{(x)}a \cdot {}_{(x)}b \quad ((ab)_{(x)} = a_{(x)} \cdot b_{(x)}).$$

Dowód. Na mocy (ii) mamy

$${}_{(x)}(ab) = \sum_{k=0}^{\infty} x^k \left( \sum_{j=0}^{\infty} x^j a_j \right) b_k = \sum_{k=0}^{\infty} \left( \sum_{j=0}^{\infty} x^j a_j \right) x^k b_k = \\ = \left( \sum_{j=0}^{\infty} x^j a_j \right) \left( \sum_{k=0}^{\infty} x^k b_k \right) = {}_{(x)}a \cdot {}_{(x)}b.$$

Dowód dla prawej wartości jest analogiczny.  $\blacksquare$

(II.43) TWIERDZENIE. Jeżeli  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedyneką  $\mathcal{A}$  i dla do-

wolnych  $y \in \mathcal{X}$ ,  $c \in \mathcal{A}$  jest

$$(iii) \quad cy = yc,$$

to lewa (prawa) wartość dowolnego wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  w dowolnym punkcie  $x \in \mathcal{X}$  jest wartością tego wielomianu w punkcie  $x$ .

Dowód wynika ze wzorów (II.32) i (iii). ■

(II.44) TWIERDZENIE. Jeżeli  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedynką  $\mathcal{A}$  i dla dowolnych  $y \in \mathcal{X}$ ,  $c \in \mathcal{A}$  jest spełniony warunek (iii), to dla dowolnych wielomianów  $a, b \in \mathcal{P}[\mathcal{A}]$  i dowolnego elementu  $x \in \mathcal{X}$  jest

$$(II.45) \quad (a+b)(x) = a(x) + b(x).$$

$$(II.46) \quad (ab)(x) = a(x) \cdot b(x).$$

Dowód. Wzór (II.45) wynika ze wzoru (II.39) na mocy twierdzenia (II.43). Następnie na mocy (ii) i (iii) mamy

$$\begin{aligned} {}_{(x)}(ab) &= \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} x^k x^j a_j b_k = \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} x^j x^k a_j b_k = \\ &= \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} x^j a_j x^k b_k = \left( \sum_{j=0}^{\infty} x^j a_j \right) \left( \sum_{k=0}^{\infty} x^k b_k \right) = {}_{(x)}a \cdot {}_{(x)}b, \end{aligned}$$

skąd na mocy twierdzenia (II.43) otrzymujemy wzór (II.46). ■

(II.47) DEFINICJA. Lewym (prawym) miejscem zerowym wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  w pierścieniu  $\mathcal{X}$ , gdzie  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedynką  $\mathcal{A}$ , nazywamy każdy taki element  $x \in \mathcal{X}$ , że  ${}_{(x)}a = 0$  ( $a_{(x)} = 0$ ), gdzie 0 jest  $\mathcal{X}$ -zerem. ■

(II.48) DEFINICJA. Miejscem zerowym wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  w pierścieniu  $\mathcal{X}$ , gdzie  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedynką  $\mathcal{A}$ , nazywamy każdy taki element  $x \in \mathcal{X}$ , który jest zarówno lewym jak i prawym miejscem zerowym wielomianu  $a$ , tzn. każdy taki element  $x \in \mathcal{X}$ , dla którego  $a(x) = 0$ , gdzie 0 jest  $\mathcal{X}$ -zerem. ■

(II.49) DEFINICJA. Lewym (prawym) pierwiastkiem wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  nazywamy każde jego lewe (prawe) miejsce zerowe w pierścieniu z jedynką  $\mathcal{A}$ . ■

(II.50) DEFINICJA. Pierwiastkiem wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  nazywamy każde jego miejsce zerowe w pierścieniu z jedynką  $\mathcal{A}$ , tzn. każdy taki element  $x \in \mathcal{A}$ , że  $a(x) = 0$ , gdzie 0 jest  $\mathcal{A}$ -zerem. ■

(II.51) TWIERDZENIE. Jeżeli  $x \in \mathcal{X}$ , gdzie  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedynką  $\mathcal{A}$ , jest lewym (prawym) miejscem zerowym wielomianu  $a \in \mathcal{P}[\mathcal{A}]$ , to  $x$  jest również lewym (prawym) miejscem zerowym wielomianu  $ab$  (wielomianu  $ba$ ), gdzie  $b \in \mathcal{P}[\mathcal{A}]$ .

Dowód wynika z definicji (II.47) i wzoru (II.40). ■

## § II.3. Podzielność wielomianów

(II.52) TWIERDZENIE. *Każdy pierścień wielomianowy  $\mathcal{P}[\mathcal{A}]$  nad pierścieniem całkowitym  $\mathcal{A}$  jest pierścieniem z quasi-podzielnością z funkcją porządkującą  $\varphi : \mathcal{P}[\mathcal{A}] \rightarrow \mathfrak{N}_0$  określoną dla dowolnego wielomianu  $x \in \mathcal{P}[\mathcal{A}]$  wzorem*

$$(II.53) \quad \varphi(x) := \begin{cases} \text{st } x + 1, & \text{gd}y \quad \text{st } x \geq 0, \\ 0, & \text{gd}y \quad \text{st } x = -\infty. \end{cases}$$

Dowód. Funkcja (II.53) spełnia warunki (I.305), (I.306) i jest funkcją porządkującą. Niech  $a, b \in \mathcal{P}[\mathcal{A}]$  i niech  $b \neq 0$ . Zatem  $\text{st } b \neq -\infty$ . Jeżeli  $\text{st } a < \text{st } b$ , to kładąc  $q := 0$ ,  $r := a$  i  $\alpha = 1$  otrzymujemy

$$(II.54) \quad \begin{aligned} \alpha a &= qb + r, & \alpha &\neq 0, \\ \varphi(r) &< \varphi(b). \end{aligned}$$

Możemy zatem założyć, że  $\text{st } a \geq \text{st } b \geq 0$ . Niech  $m := \text{st } a$ ,  $n := \text{st } b$  i

$$a := \sum_{j=0}^m a_j \lambda^j, \quad b := \sum_{j=0}^n b_j \lambda^j, \quad a_m, b_n \neq 0,$$

gdzie  $a_0, \dots, a_m, b_0, \dots, b_n \in \mathcal{A}$ , a  $\lambda$  jest wielomianem (II.27). Niech  $u := a_m \lambda^{m-n}$ . Mamy wtedy

$$(i) \quad \begin{aligned} c := b_n a - ub &= \sum_{j=0}^m a_j b_n \lambda^j - \sum_{j=0}^n a_m \lambda^{m-n} b_j \lambda^j = \\ &= \sum_{j=0}^m a_j b_n \lambda^j - \sum_{j=0}^n a_m b_j \lambda^{j+m-n} = \\ &= \sum_{j=0}^{m-1} a_j b_n \lambda^j - \sum_{j=0}^{n-1} a_m b_j \lambda^{j+m-n}, \end{aligned}$$

wobec czego  $\text{st } c < \text{st } a = m$ . Wykazaliśmy zatem, że jeżeli  $b \neq 0$  i  $\text{st } a \geq \text{st } b$ , to istnieją takie wielomiany  $u, c \in \mathcal{P}[\mathcal{A}]$  i taki element  $b_n \in \mathcal{A}$ , że

$$(ii) \quad b_n a = ub + c, \quad \text{st } c < \text{st } a, \quad b_n \neq 0.$$

Jeżeli  $\text{st } c < \text{st } b$ , to kładąc  $q := u$ ,  $r := c$ ,  $\alpha := b_n$ , otrzymujemy (II.54). Jeżeli  $\text{st } c \geq \text{st } b$ , to na mocy już przeprowadzonego rozumowania istnieją takie wielomiany  $v, d \in \mathcal{P}[\mathcal{A}]$  i taki element  $\beta \in \mathcal{A}$ ,  $\beta \neq 0$ , że  $\beta c = vb + d$  i  $\text{st } d < \text{st } c$ , czyli

$$\beta b_n a = (\beta u + v)b + d, \quad \text{st } d < \text{st } c < \text{st } a, \quad \beta b_n \neq 0.$$

Przez indukcję skończoną dochodzimy do wzorów (II.54). ■

(II.55) DEFINICJA. Pierścień wielomianowy  $\mathcal{P}[\mathcal{A}]$  nazywamy *regularnym* wtedy i tylko wtedy, gdy  $\mathcal{A}$  jest pierścieniem całkowitym, a  $\mathcal{P}[\mathcal{A}]$  na mocy twierdzenia (II.52) jest traktowany jako pierścień z quasi-podzielnością z funkcją porządkującą określoną wzorem (II.53). ■

(II.56) TWIERDZENIE. *Każdy pierścień wielomianowy  $\mathcal{P}[\mathcal{F}]$  nad ciałem  $\mathcal{F}$  jest pierścieniem z podzielnością z funkcją porządkującą (II.52) i jest regularny.*

Dowód. Analogiczny do dowodu twierdzenia (II.52). ■

(II.57) PRZYKŁAD. Pierścień wielomianowy  $\mathcal{P}[\mathcal{C}]$  generowany przez ciało liczb zespolonych  $\mathcal{C}$  jest pierścieniem z podzielnością z funkcją porządkującą (II.53) i jest regularny. Dla wielomianów

$$a := (1-i)e - i\lambda + \lambda^2 - (1+i)\lambda^3 + 2i\lambda^4,$$

$$b := (-3+2i)e + (3-5i)\lambda + (4+3i)\lambda^2,$$

gdzie  $e$  jest wielomianem jedynkowym,  $\lambda$  – wielomianem (II.27) i  $\lambda^0 = e$ , mamy

$$b_2^{-1} = \frac{1}{4+3i} = \frac{4}{25} - \frac{3}{25}i,$$

$$2ib_2^{-1} = \frac{6}{25} + \frac{8}{25}i, \quad u := \left(\frac{6}{25} + \frac{8}{25}i\right)\lambda^2,$$

$$c := a - ub = (1-i)e - i\lambda + \left(\frac{59}{25} + \frac{12}{25}i\right)\lambda^2 + \left(-\frac{83}{25} - \frac{19}{25}i\right)\lambda^3,$$

$$v := \left(-\frac{83}{25} - \frac{19}{25}i\right)\left(\frac{4}{25} - \frac{3}{25}i\right)\lambda = \left(-\frac{389}{625} + \frac{173}{625}i\right)\lambda,$$

$$d := c - vb = (1-i)e + \left(-\frac{821}{625} + \frac{672}{625}i\right)\lambda + \left(\frac{1777}{625} - \frac{2164}{625}i\right)\lambda^2,$$

$$w := \left(\frac{1777}{625} - \frac{2164}{625}i\right)\left(\frac{4}{25} - \frac{3}{25}i\right)e = \left(\frac{616}{15625} - \frac{13987}{15625}i\right)e,$$

$$r := d - wb = \left(-\frac{10501}{15625} - \frac{58818}{15625}i\right)e + \left(\frac{47562}{15625} + \frac{61841}{15625}i\right)\lambda.$$

Stąd  $a = ub + c = (u+v)b + d = (u+v+w)b + r$  i kładąc

$$q := u + v + w = \left(\frac{616}{15625} - \frac{13987}{15625}i\right)e + \left(-\frac{389}{625} + \frac{173}{625}i\right)\lambda + \left(\frac{6}{25} + \frac{8}{25}i\right)\lambda^2,$$

otrzymujemy  $a = qb + r$ ,  $\varphi(r) < \varphi(b)$ , gdzie  $\varphi$  jest funkcją (II.53). ■

Przyjmujemy, że w każdym pierścieniu wielomianowym jest określona funkcja porządkująca (II.53).

(II.58) TWIERDZENIE. *W dowolnym pierścieniu wielomianowym  $\mathcal{P}[\mathcal{A}]$  każdy wielomian jest lewostronnie (prawostronnie) podzielny z resztą w sensie wzorów (I.307) i (I.308) przez każdy wielomian prawostronnie (lewostronnie) nieosobliwy.*

Dowód jest analogiczny do dowodu twierdzenia (II.52), jeżeli zamiast (i) przyjąć

$$c := a - bu \quad (c := a - ub),$$

gdzie  $u := b_n^{-1}a_m\lambda^{m-n}$  ( $u := a_m b_n^{-1}\lambda^{m-n}$ ),  $b_n b_n^{-1} = 1$  ( $b_n^{-1}b_n = 1$ ). ■

(II.59) TWIERDZENIE. *W dowolnym pierścieniu wielomianowym  $\mathcal{P}[\mathcal{A}]$  każdy wielomian jest lewostronnie (prawostronnie) podzielny z resztą przez każdy wielomian moniczny.*

Dowód wynika z twierdzenia poprzedniego. ■

(II.60) TWIERDZENIE. *Iloraz i reszta z lewostronnego (prawostronnego) podzielenia dowolnego wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  przez dowolny wielomian nieosobliwy  $b \in \mathcal{P}[\mathcal{A}]$  są określone jednoznacznie.*



Dowód. Na mocy twierdzenia (II.58) wielomian  $a$  jest podzielny z resztą przez wielomian  $b$ . Jeżeli

$$a = bq_1 + r_1, \quad a = bq_2 + r_2,$$

$$\text{st } r_1 < \text{st } b, \quad \text{st } r_2 < \text{st } b,$$

to

$$b(q_1 - q_2) = r_2 - r_1.$$

Na mocy (II.22) i (II.23) mamy  $\text{st}(r_2 - r_1) \leq \max(\text{st } r_1, \text{st } r_2) < \text{st } b$  oraz  $\text{st}(r_2 - r_1) = \text{st}(b(q_1 - q_2)) = \text{st } b + \text{st}(q_2 - q_1)$ , ponieważ z nieosobliwości wielomianu  $b$  wynika, że iloczyn najwyższych współczynników wielomianów  $b$  i  $q_2 - q_1$  nie może być zerem, gdy te wielomiany nie są zerowe. Gdyby  $\text{st}(q_2 - q_1) \neq -\infty$ , mielibyśmy  $\text{st } b \leq \text{st}(r_2 - r_1) < \text{st } b$ , co dałoby sprzeczność. Zatem  $\text{st}(q_2 - q_1) = -\infty$ , co oznacza, że  $q_1 = q_2$ . Stąd równość  $r_1 = r_2$ . Dowód dla prawostronnego dzielenia jest analogiczny. ■

(II.61) TWIERDZENIE. Jeżeli w dowolnym pierścieniu wielomianowym  $\mathcal{P}[\mathcal{A}]$

$$(iii) \quad a = bq + r, \quad \text{st } r < \text{st } b,$$

gdzie  $b$  jest wielomianem prawostronnie nieosobliwym i

$$a := \sum_{j=0}^m a_j \lambda^j, \quad b := \sum_{j=0}^n b_j \lambda^j, \quad q := \sum_{j=0}^k q_j \lambda^j, \quad a_m, b_n, q_k \neq 0,$$

gdzie  $a_0, \dots, a_m, b_0, \dots, b_n, q_0, \dots, q_k \in \mathcal{A}$ , a  $\lambda$  jest wielomianem (II.27), to iloraz  $q$  i reszta  $r$  są określone wzorami:

$$(II.62) \quad q_k = b_n^{-1} a_m, \\ q_{k-l} = b_n^{-1} (a_{m-l} - \sum_{j=1}^{\min(n, l)} b_{n-j} q_{k-l+j}) \quad \text{dla } l=1, \dots, k,$$

$$(II.63) \quad r = a - bq.$$

Jeżeli natomiast  $b$  jest wielomianem lewostronnie nieosobliwym i

$$(iv) \quad a = qb + r, \quad \text{st } r < \text{st } b,$$

to iloraz  $q$  i reszta  $r$  są określone wzorami:

$$(II.64) \quad q_k = a_m b_n^{-1}, \\ q_{k-l} = (a_{m-l} - \sum_{j=1}^{\min(n, l)} q_{k-l+j} b_{n-j}) b_n^{-1} \quad \text{dla } l=1, \dots, k,$$

$$(II.65) \quad r = a - qb.$$

Dowód. Polega na sprawdzeniu, że gdy są spełnione wzory (II.62) i (II.63), wtedy są spełnione warunki (iii), a gdy są spełnione wzory (II.64) i (II.65), wtedy warunki (iv). ■

(II.66) TWIERDZENIE. Jeżeli wielomian  $a \in \mathcal{P}[\mathcal{A}]$  jest lewostronnie nieosobliwy, to dla dowolnego wielomianu  $b \in \mathcal{P}[\mathcal{A}]$

$$(II.67) \quad ab = 0 \Rightarrow b = 0.$$

Jeżeli wielomian  $b \in \mathcal{P}[\mathcal{A}]$  jest prawostronnie nieosobliwy, to dla dowolnego wielomianu  $a \in \mathcal{P}[\mathcal{A}]$

$$(II.68) \quad ab = o \Rightarrow a = o.$$

Dowód. Jeżeli wielomian  $a$  jest lewostronnie nieosobliwy, to  $\text{st } a \neq -\infty$ , a na mocy twierdzenia (II.25)  $\text{st}(ab) = -\infty = \text{st } a + \text{st } b$ , skąd jest  $\text{st } b = -\infty$ , czyli  $b = o$ . Dowód drugiej części tezy jest analogiczny. ■

(II.69) TWIERDZENIE. Jeżeli  ${}_{(x)}a$  ( $a_{(x)}$ ) jest lewą (prawą) wartością wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  w punkcie  $x \in \mathcal{X}$ , gdzie  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedyneką  $\mathcal{A}$ , i jeżeli  $0$  jest  $\mathcal{X}$ -zerem,  $1$  —  $\mathcal{X}$ -jedyneką,  $I := (1, 0, 0, \dots)$ ,  $\Lambda := (0, 1, 0, 0, \dots)$ ,  $\alpha := 1a \in \mathcal{P}[\mathcal{X}]$  ( $\alpha := a1 \in \mathcal{P}[\mathcal{X}]$ ),  $\beta := (x, -1, 0, 0, \dots) = xI - \Lambda \in \mathcal{P}[\mathcal{X}]$ , to reszta lewostronnego (prawostronnego) podzielenia wielomianu  $\alpha$  przez wielomian  $\beta$  jest równa  ${}_{(x)}aI$  ( $a_{(x)}I$ ).

Dowód. Rozpatrzmy przypadek lewej wartości wielomianu  $a$  w punkcie  $x$ . Na mocy twierdzenia (II.58) wielomian  $\alpha$  jest podzielny z resztą przez wielomian  $\beta$ . Istnieje zatem lewy iloraz  $\gamma \in \mathcal{P}[\mathcal{X}]$  i lewa reszta  $\rho \in \mathcal{P}[\mathcal{X}]$  takie, że  $\alpha = \beta\gamma + \rho$  i  $\text{st } \rho < \text{st } \beta = 1$ . Oznacza to, że reszta  $\rho$  jest wielomianem stałym i ma postać  $rI$ , gdzie  $r \in \mathcal{X}$ . Ponieważ  ${}_{(x)}\beta = 0$ , więc na mocy (II.40) jest  ${}_{(x)}(\beta\gamma) = 0$  i na mocy (II.39)  ${}_{(x)}\alpha = {}_{(x)}\rho = r$ . Zatem  $\rho = {}_{(x)}a \cdot I$ . Dowód dla prawej wartości wielomianu  $a$  w punkcie  $x$  jest analogiczny. ■

(II.70) TWIERDZENIE. Reszta z lewostronnego (prawostronnego) podzielenia wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  przez wielomian  $b := (x, -1, 0, 0, \dots) = xe - \lambda \in \mathcal{P}[\mathcal{A}]$ , gdzie  $\mathcal{A}$  jest pierścieniem z jedyneką,  $x \in \mathcal{A}$ ,  $e$  jest wielomianem jedynekowym, a  $\lambda$  wielomianem (II.27), jest równa  ${}_{(x)}a \cdot e$  ( $a_{(x)} \cdot e$ ).

Dowód. Twierdzenie (II.70) jest szczególnym przypadkiem twierdzenia (II.69). ■

(II.71) TWIERDZENIE. W oznaczeniach twierdzenia (II.69) element  $x \in \mathcal{X}$  jest lewym (prawym) miejscem zerowym wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  w pierścieniu  $\mathcal{X}$  wtedy i tylko wtedy, gdy wielomian  $\alpha$  jest lewostronnie (prawostronnie) podzielny przez wielomian  $\beta$ . ■

Dowód wynika z twierdzenia (II.69). ■

(II.72) TWIERDZENIE. Element  $x \in \mathcal{A}$ , gdzie  $\mathcal{A}$  jest pierścieniem z jedyneką, jest lewym (prawym) pierwiastkiem wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  wtedy i tylko wtedy, gdy wielomian  $a$  jest lewostronnie (prawostronnie) podzielny przez wielomian  $xe - \lambda$ , gdzie  $e$  jest wielomianem jedynekowym, a  $\lambda$  — wielomianem (II.27).

Dowód. Twierdzenie (II.72) jest szczególnym przypadkiem twierdzenia (II.71). ■

(II.73) PRZYKŁAD. Niech  $a \in \mathcal{P}[\mathcal{C}]$  będzie wielomianem z przykładu (II.57). Sprawdzamy, że liczba zespolona  $-i$  jest pierwiastkiem wielomianu  $a$ , tzn.  $a(-i) = 0$ . Sprawdzamy również, że

$$a = (1-i)e - i\lambda + \lambda^2 - (1+i)\lambda^3 + 2i\lambda^4 = (-ie - \lambda)((1+i)e + i\lambda + (-1+i)\lambda^2 - 2i\lambda^3),$$

co oznacza, że wielomian  $a$  jest podzielny przez wielomian  $-ie - \lambda$ . ■

(II.74) DEFINICJA. Element  $x \in \mathcal{A}$ , gdzie  $\mathcal{A}$  jest pierścieniem z jedynką, nazywamy  $k$ -krotnym lewym (prawym) pierwiastkiem wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  wtedy i tylko wtedy, gdy wielomian  $a$  jest lewostronnie (prawostronnie) podzielny przez wielomian  $(xe - \lambda)^k \in \mathcal{P}[\mathcal{A}]$ , a nie jest lewostronnie (prawostronnie) podzielny przez wielomian  $(xe - \lambda)^{k+1} \in \mathcal{P}[\mathcal{A}]$  ( $k \in \mathbb{N}$ ). ■

(II.75) DEFINICJA. Element  $x \in \mathcal{A}$ , gdzie  $\mathcal{A}$  jest pierścieniem z jedynką, nazywamy  $k$ -krotnym pierwiastkiem wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  wtedy i tylko wtedy, gdy jest zarówno  $k$ -krotnym lewym jak i  $k$ -krotnym prawym pierwiastkiem tego wielomianu. ■

Pierwiastek jednokrotny wielomianu  $a$  nazywamy również *pierwiastkiem pojedynczym* tego wielomianu.

(II.76) PRZYKŁAD. Liczba zespolona  $-i$  jest pierwiastkiem pojedynczym wielomianu  $a$  z przykładów (II.57) i (II.73), ponieważ wykazaliśmy w drugim z nich, że wielomian  $a$  jest podzielny przez wielomian  $-ie - \lambda$ , i mamy

$$a = (-ie - \lambda)^2((-1 - 4i)e + (3 - i)\lambda + 2i\lambda^2) + 5(-ie - \lambda),$$

co oznacza, że wielomian  $a$  nie jest podzielny przez wielomian  $(-ie - \lambda)^2$ . ■

(II.77) TWIERDZENIE. Jeżeli  $\mathcal{A}$  jest pierścieniem całkowitym, to:

- 1°  $\mathcal{P}[\mathcal{A}]$  jest także pierścieniem całkowitym,
- 2° lewa wartość dowolnego wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  w dowolnym punkcie  $x \in \mathcal{A}$  jest równa prawej i jest równa wartości wielomianu  $a$  w punkcie  $x$ ,
- 3° dla dowolnych wielomianów  $a, b \in \mathcal{P}[\mathcal{A}]$  i dowolnego elementu  $x \in \mathcal{A}$  są prawdziwe wzory (II.45) i (II.46),
- 4° każdy lewy (prawy) pierwiastek dowolnego wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  jest pierwiastkiem tego wielomianu,
- 5° iloraz i reszta z lewostronnego (prawostronnego) quasi-podzielenia dowolnego wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  przez dowolny wielomian  $b \in \mathcal{P}[\mathcal{A}]$ ,  $b \neq 0$ , są odpowiednio ilorazem i resztą z quasi-podzielenia wielomianu  $a$  przez wielomian  $b$ ,
- 6° jeżeli wielomian  $a \in \mathcal{P}[\mathcal{A}]$  jest lewostronnie (prawostronnie) podzielny z resztą przez wielomian  $b \in \mathcal{P}[\mathcal{A}]$ , to jest podzielny z resztą przez wielomian  $b$ , a iloraz i reszta z lewostronnego (prawostronnego) podzielenia  $a$  przez  $b$  są odpowiednio ilorazem i resztą z podzielenia  $a$  przez  $b$ .

Dowód. Jeżeli  $\mathcal{A}$  jest pierścieniem przemiennym, to na mocy (II.14)  $\mathcal{P}[\mathcal{A}]$  jest też pierścieniem przemiennym.

Jeżeli  $\mathcal{A}$  nie zawiera właściwych dzielników zera, to dla dowolnych wielomianów niezerowych  $a, b \in \mathcal{P}[\mathcal{A}]$  ich iloczyn  $ab$  jest na mocy twierdzenia (II.25) niezerowy. Oznacza to, że pierścień  $\mathcal{P}[\mathcal{A}]$  nie zawiera właściwych dzielników zera.

Z powyższego wynika część 1° tezy. Z przemienności pierścienia  $\mathcal{A}$  wynika na mocy twierdzenia (II.43) i wzorów (II.19), (II.20) część 2°, a na mocy twierdzenia (II.41) część 3°. Część 4° wynika z 2°. Części 5° i 6° wynikają z przemienności pierścienia  $\mathcal{P}[\mathcal{A}]$ . ■

(II.78) TWIERDZENIE. Każdy pierścień wielomianowy regularny, a w szczególności każdy pierścień wielomianowy nad ciałem jest pierścieniem całkowitym.

Dowód wynika z twierdzenia poprzedniego. ■

(II.79) TWIERDZENIE. Jeżeli  $a, b, c$  są wielomianami z regularnego pierścienia wielomianowego  $\mathcal{P}[\mathcal{A}]$  i  $c \neq 0$ , to

$$ac = bc \Rightarrow a = b.$$

Dowód wynika z twierdzeń (II.78) i (I.112). ■

(II.80) TWIERDZENIE. Jeżeli  $a$  jest wielomianem z regularnego pierścienia wielomianowego  $\mathcal{P}[\mathcal{A}]$ , a  $x_1, \dots, x_n \in \mathcal{A}$  są różnymi pierwiastkami wielomianu  $a$  o krotnościach odpowiednio  $k_1, \dots, k_n$ , to wielomian  $a$  jest podzielny przez wielomian  $(x_1 e - \lambda)^{k_1} \dots (x_n e - \lambda)^{k_n}$ .

Dowód. Stosujemy indukcję. Dla  $n=1$  twierdzenie jest prawdziwe na mocy definicji (II.74) i twierdzenia (II.77). Jeżeli jest prawdziwe dla pierwiastków  $x_1, \dots, x_p$  ( $p < n$ ), to istnieje taki wielomian  $b \in \mathcal{P}[\mathcal{A}]$ , że  $a = (x_1 e - \lambda)^{k_1} \dots (x_p e - \lambda)^{k_p} \cdot b$ . Jeżeli  $x_{p+1}$  jest pierwiastkiem wielomianu  $a$  o krotności  $k_{p+1}$  różnym od  $x_1, \dots, x_p$ , to

$$a(x_{p+1}) = (x_1 - x_{p+1})^{k_1} \dots (x_p - x_{p+1})^{k_p} \cdot b(x_{p+1}) = 0,$$

skąd  $b(x_{p+1}) = 0$ , co oznacza, że  $x_{p+1}$  jest pierwiastkiem wielomianu  $b$ . Niech  $l_{p+1}$  będzie jego krotnością. Istnieją zatem takie wielomiany  $c, d \in \mathcal{P}[\mathcal{A}]$ , że

$$a = (x_{p+1} e - \lambda)^{k_{p+1}} c, \quad b = (x_{p+1} e - \lambda)^{l_{p+1}} d,$$

skąd

$$(x_{p+1} e - \lambda)^{k_{p+1}} c = (x_1 e - \lambda)^{k_1} \dots (x_p e - \lambda)^{k_p} (x_{p+1} e - \lambda)^{l_{p+1}} d.$$

Gdyby  $l_{p+1} > k_{p+1}$ , wtedy na mocy twierdzenia (II.79) mielibyśmy

$$c = (x_1 e - \lambda)^{k_1} \dots (x_p e - \lambda)^{k_p} (x_{p+1} e - \lambda)^{l_{p+1} - k_{p+1}} d,$$

skąd  $c(x_{p+1}) = 0$  i istniałby taki wielomian  $f$ , że  $c = (x_{p+1} e - \lambda) f$  i  $a = (x_{p+1} e - \lambda)^{k_{p+1}+1} f$ , wbrew założeniu, że  $k_{p+1}$  jest krotnością pierwiastka  $x_{p+1}$ . Analogicznie wykazujemy, że nie może być także  $l_{p+1} < k_{p+1}$ , wobec czego  $l_{p+1} = k_{p+1}$  i

$$a = (x_1 e - \lambda)^{k_1} \dots (x_{p+1} e - \lambda)^{k_{p+1}} d.$$

Jeżeli zatem twierdzenie jest prawdziwe dla  $x_1, \dots, x_p$  ( $p < n$ ), to jest również prawdziwe dla  $x_1, \dots, x_{p+1}$ . Na mocy indukcji otrzymujemy stąd tezę. ■

(II.81) DEFINICJA II.23. Łączną krotnością pierwiastków wielomianu  $a$  nazywamy liczbę całkowitą nieujemną  $k = k_1 + \dots + k_s$ , gdzie  $k_j$  ( $j = 1, \dots, s$ ) jest krotnością pierwiastka  $x_j$  wielomianu  $a$ , który poza  $x_1, \dots, x_s$  ( $x_j \neq x_l$  dla  $j \neq l$ ) nie ma już innych pierwiastków. ■

(II.82) TWIERDZENIE. Łączna krotność pierwiastków wielomianu  $a$  stopnia  $m$ ,  $m \neq -\infty$ , z regularnego pierścienia wielomianowego  $\mathcal{P}[\mathcal{A}]$  jest nie większa niż  $m$ .

Dowód wynika z twierdzenia (II.80), ponieważ na mocy twierdzenia (II.25)

$$\text{st}((x_1 e - \lambda)^{k_1} \dots (x_s e - \lambda)^{k_s}) = k_1 + \dots + k_s \leq m. \quad \blacksquare$$

(II.83) TWIERDZENIE. Łączna krotność pierwiastków dowolnego wielomianu stopnia  $m > 0$  nad ciałem liczb zespolonych  $\mathbb{C}$  jest równa  $m$ .

Dowód pomijamy, ponieważ jest długi i żmudny, a z punktu widzenia niniejszej książki nie ma znaczenia metodologicznego. Zainteresowanych odsyłamy, na przykład, do monografii A. Mostowskiego i M. Starka<sup>(1)</sup>. ■

#### § II.4. Największy wspólny dzielnik wielomianów

(II.84) TWIERDZENIE. *Dowolne, ale nie wszystkie zerowe, wielomiany  $w_1, \dots, w_s$  z pierścienia wielomianowego nad ciałem (z regularnego pierścienia wielomianowego) mają największy wspólny dzielnik (największy wspólny quasi-dzielnik).*

Dowód wynika z twierdzeń (II.52), (II.56) i (I.341). ■

(II.85) TWIERDZENIE. *Jeżeli wielomiany  $d_1$  i  $d_2$  są największymi wspólnymi quasi-dzielnikami wielomianów  $w_1, \dots, w_s$  w regularnym pierścieniu wielomianowym  $\mathcal{P}[\mathcal{A}]$ , to istnieją takie elementy  $a_1, a_2 \in \mathcal{A}$ ,  $a_1, a_2 \neq 0$ , że*

$$(II.86) \quad a_1 d_1 = a_2 d_2.$$

Dowód. Na mocy definicji największego wspólnego quasi-dzielnika istnieją takie elementy  $a_1, a_2 \in \mathcal{A}$ ,  $a_1, a_2 \neq 0$ , że wielomian  $a_1 d_1$  jest podzielny przez wielomian  $d_2$ , a wielomian  $a_2 d_2$  jest podzielny przez wielomian  $d_1$ , czyli istnieją takie wielomiany  $v_1, v_2 \in \mathcal{P}[\mathcal{A}]$ , że

$$(i) \quad a_1 d_1 = v_2 d_2, \quad a_2 d_2 = v_1 d_1,$$

skąd  $a_1 a_2 d_1 = v_1 v_2 d_1$  i na mocy twierdzenia (II.79)  $v_1 v_2 \equiv a_1 a_2$ . Wobec tego  $\text{st}(v_1 v_2) = 0$  i na mocy twierdzenia (II.25)  $\text{st } v_1 = \text{st } v_2 = 0$ . Zatem istnieją takie elementy  $v_1, v_2 \in \mathcal{A}$ ,  $v_1, v_2 \neq 0$ , że jest (i) i kładąc  $a_2 = v_2$ , otrzymujemy (II.86). ■

(II.87) TWIERDZENIE. *Dla dowolnych wielomianów  $w_1, \dots, w_s$  z pierścienia wielomianowego  $\mathcal{P}[\mathcal{F}]$  nad ciałem  $\mathcal{F}$  istnieje dokładnie jeden największy wspólny dzielnik, będący wielomianem monicznym.*

Dowód. Największy wspólny dzielnik  $d$  wielomianów  $w_1, \dots, w_s$  istnieje na mocy twierdzenia (II.84). Jeżeli  $a_m$  jest najwyższym współczynnikiem wielomianu  $d$ , to  $d_1 := \frac{1}{a_m} d$  jest wielomianem monicznym i jest największym wspólnym dzielnikiem wielomianów  $w_1, \dots, w_s$ . Gdyby istniał inny jeszcze największy wspólny dzielnik  $d_2$ , będący wielomianem monicznym, wtedy na mocy (II.86) byłoby  $d_1 = d_2$ . ■

(II.88) TWIERDZENIE. *Jeżeli co najmniej jeden z wielomianów  $v, w \in \mathcal{P}[\mathcal{A}]$ , gdzie  $\mathcal{P}[\mathcal{A}]$  jest pierścieniem wielomianowym nad ciałem  $\mathcal{A}$  (regularnym pierścieniem wielomianowym), nie jest wielomianem zerowym, to istnieją takie wielomiany  $p, q \in \mathcal{P}[\mathcal{A}]$ , że*

$$(II.89) \quad pv + qw = d,$$

<sup>(1)</sup> A. Mostowski, M. Stark, *Elementy algebry wyższej*, wyd. IX, PWN, Warszawa 1977.

gdzie  $d$  jest największym wspólnym dzielnikiem (największym wspólnym quasi-dzielnikiem) wielomianów  $v$  i  $w$ .

Dowód. Rozpatrzmy przypadek, gdy  $\mathcal{P}[\mathcal{A}]$  jest pierścieniem wielomianowym nad ciałem  $\mathcal{A}$ . Na mocy twierdzeń (II.56) i (I.331) dla wielomianów  $v$  i  $w$  istnieje skończony algorytm Euklidesa z funkcją porządkującą (II.53), czyli istnieje taki ciąg par  $(v^{(k)}, w^{(k)})$ ,  $k=0, 1, \dots, p$ , że:

$$\begin{aligned} (v^{(0)}, w^{(0)}) &= (v, w), \\ (v^{(k+1)}, w^{(k+1)}) &= (r_1^{(k)}, r_2^{(k)}), \\ 0 \leq \text{st } b^{(k)} &\leq \min(\text{st } v^{(k)}, \text{st } w^{(k)}), \\ r_1^{(k)} &:= \begin{cases} b^{(k)}, & \text{gdy } b^{(k)} := v^{(k)}, \\ v^{(k)} - b^{(k)} q_1^{(k)}, & \text{gdy } b^{(k)} := w^{(k)}, \end{cases} \\ \text{(ii)} \quad r_2^{(k)} &:= \begin{cases} w^{(k)} - b^{(k)} q_2^{(k)}, & \text{gdy } b^{(k)} := v^{(k)}, \\ b^{(k)}, & \text{gdy } b^{(k)} := w^{(k)}, \end{cases} \\ \text{st } r_1^{(k)} &< \text{st } b^{(k)}, & \text{gdy } b^{(k)} := w^{(k)}, \\ \text{st } r_2^{(k)} &< \text{st } b^{(k)}, & \text{gdy } b^{(k)} := v^{(k)}, \\ (v^{(p+1)}, w^{(p+1)}) &= (d, 0) \quad \text{albo} \quad (v^{(p+1)}, w^{(p+1)}) = (0, d). \end{aligned}$$

Rozpatrzmy przypadek, gdy  $\text{st } v \leq \text{st } w$ . Można wobec tego przyjąć, że  $b^{(0)} := v$ . Wtedy  $(v^{(1)}, w^{(1)}) = (r_1^{(0)}, r_2^{(0)}) = (v, w - v \cdot q_2^{(0)})$  i  $\text{st } r_2^{(0)} < \text{st } b^{(0)} = \text{st } v$ . Wobec tego  $b^{(1)} := r_2^{(0)} = w^{(1)}$  i  $(v^{(2)}, w^{(2)}) = (v - (w - v q_2^{(0)}) q_1^{(1)}, w - v \cdot q_2^{(0)})$ . Z łatwością dowodzimy przez indukcję, że dla każdego  $k \in \{0, 1, \dots, p\}$  istnieją takie wielomiany  $p_1^{(k)}, p_2^{(k)}, q_1^{(k)}, q_2^{(k)} \in \mathcal{P}[\mathcal{A}]$ , że  $(v^{(k)}, w^{(k)}) = (p_1^{(k)} v + q_1^{(k)} w, p_2^{(k)} v + q_2^{(k)} w)$ . Dla  $k=p$  otrzymujemy stąd tezę. Dowód w przypadku, gdy  $\text{st } v \geq \text{st } w$  i  $b^{(0)} := w$  jest analogiczny.

Gdy  $\mathcal{P}[\mathcal{A}]$  jest regularnym pierścieniem wielomianowym, dowód przebiega analogicznie. ■

(II.90) PRZYKŁAD. Obliczmy za pomocą algorytmu Euklidesa największy wspólny dzielnik następujących wielomianów  $v, w \in \mathcal{P}[\mathcal{R}]$ , gdzie  $\mathcal{R}$  jest ciałem liczb rzeczywistych:

$$v := 2e - 2\lambda + \lambda^2 - \lambda^3 - \lambda^4 + \lambda^5, \quad w := -e - \lambda^2 + \lambda^4 + \lambda^6.$$

Zgodnie z (ii) mamy

$$\begin{aligned} (v^{(0)}, w^{(0)}) &:= (v, w), \quad \text{st } v < \text{st } w, \\ b^{(0)} &:= v, \\ w &= (e + \lambda)v + (-3e + 3\lambda^4), \\ r_1^{(0)} &:= v, \quad r_2^{(0)} := -3e + 3\lambda^4, \\ (v^{(1)}, w^{(1)}) &:= (v, -3e + 3\lambda^4), \quad \text{st } (-3e + 3\lambda^4) < \text{st } v, \\ b^{(1)} &:= -3e + 3\lambda^4 = w^{(1)}, \end{aligned}$$



$$v^{(1)} = v = (-3e + 3\lambda^4)(-\frac{1}{3}e + \frac{1}{3}\lambda) + (e - \lambda + \lambda^2 - \lambda^3),$$

$$r_1^{(1)} := e - \lambda + \lambda^2 - \lambda^3, \quad r_2^{(1)} := b^{(1)},$$

$$(v^{(2)}, w^{(2)}) := (e - \lambda + \lambda^2 - \lambda^3, -3e + 3\lambda^4),$$

$$b^{(2)} := v^{(2)} = e - \lambda + \lambda^2 - \lambda^3,$$

$$w^{(2)} := (e - \lambda + \lambda^2 - \lambda^3)(-3e - 3\lambda),$$

$$r_1^{(2)} := e - \lambda + \lambda^2 - \lambda^3, \quad r_2^{(2)} = 0.$$

Stąd  $p=2$  i  $(v^{(p+1)}, w^{(p+1)}) := (e - \lambda + \lambda^2 - \lambda^3, 0)$ . Na mocy twierdzenia (I.341) wielomian  $d := e - \lambda + \lambda^2 - \lambda^3$  jest największym wspólnym dzielnikiem wielomianów  $v$  i  $w$ .

Obliczymy teraz wielomiany  $p$  i  $q$  takie, aby była spełniona równość (II.89). Mamy

$$\begin{aligned} d = r_1^{(2)} = b^{(2)} = v^{(2)} = r_1^{(1)} = v - (-3e + 3\lambda^4)(-\frac{1}{3}e + \frac{1}{3}\lambda) = \\ = v + (\frac{1}{3}e - \frac{1}{3}\lambda)w^{(1)} = v + (\frac{1}{3}e - \frac{1}{3}\lambda)r_2^{(0)} = \\ = v + (\frac{1}{3}e - \frac{1}{3}\lambda)(w - (e + \lambda)v) = (\frac{2}{3}e + \frac{1}{3}\lambda^2)v + (\frac{1}{3}e - \frac{1}{3}\lambda)w. \quad \blacksquare \end{aligned}$$

## § II.5. Rozkład wielomianu na czynniki elementarne

(II.91) DEFINICJA. Wielomian  $w \in \mathcal{P}[\mathcal{A}]$  nazywamy *rozkładalnym* wtedy i tylko wtedy, gdy można go przedstawić w postaci iloczynu co najmniej dwu wielomianów stopni dodatnich, a *quasi-rozkładalnym* wtedy i tylko wtedy, gdy istnieje element  $a \in \mathcal{A}$  nie będący dzielnikiem zera taki, że wielomian  $aw$  jest rozkładalny. ■

Z powyższej definicji wynika, że w regularnych pierścieniach wielomianowych wielomiany stopni mniejszych niż 2 są zawsze nierozkładalne.

(II.92) TWIERDZENIE. Jeżeli wielomian  $w \in \mathcal{P}[\mathcal{A}]$ , gdzie  $\mathcal{P}[\mathcal{A}]$  jest pierścieniem wielomianowym nad ciałem  $\mathcal{A}$  (regularnym pierścieniem wielomianowym), jest iloczynem wielomianów  $v_1, \dots, v_s \in \mathcal{P}[\mathcal{A}]$  stopni dodatnich, a wielomian nierozkładalny (quasi-nierozkładalny)  $u \in \mathcal{P}[\mathcal{A}]$  jest dzielnikiem (quasi-dzielnikiem) wielomianu  $w$ , to pomiędzy wielomianami  $v_1, \dots, v_s$  istnieje wielomian podzielny (quasi-podzielny) przez  $u$ .

Dowód. Niech  $\mathcal{P}[\mathcal{A}]$  będzie pierścieniem wielomianowym nad ciałem  $\mathcal{A}$ . Jeżeli  $u$  jest dzielnikiem wielomianu  $v_k \dots v_s$  ( $k=1, \dots, s-1$ ), czyli istnieje taki wielomian  $t \in \mathcal{P}[\mathcal{A}]$ , że  $v_k \dots v_s = ut$ , a  $u$  nie jest dzielnikiem  $v_k$ , to na mocy twierdzenia (II.88) istnieją takie wielomiany  $p$  i  $q$ , że  $pu + qv_k = e$ , wobec czego  $qut = (e - pu)v_{k+1} \dots v_s$ , czyli  $u(qt + pv_{k+1} \dots v_s) = v_{k+1} \dots v_s$  i  $u$  jest dzielnikiem wielomianu  $v_{k+1} \dots v_s$ . Zatem, jeśli  $u$  jest dzielnikiem wielomianu  $v_k \dots v_s$ , to albo jest dzielnikiem wielomianu  $v_k$ , albo dzielnikiem wielomianu  $v_{k+1} \dots v_s$ . Stąd przez indukcję otrzymujemy tezę. Jeżeli  $\mathcal{P}[\mathcal{A}]$  jest regularnym pierścieniem wielomianowym, to dowód przebiega analogicznie. ■

(II.93) DEFINICJA. Czynnikiem pierwszym (quasi-czynnikiem pierwszym) wielomianu nazywamy każdy wielomian nierozkładalny (quasi-nierozkładalny) stopnia dodatniego. ■

(II.94) DEFINICJA. Czynnikiem elementarnym wielomianu  $w \in \mathcal{P}[\mathcal{A}]$  albo  $k$ -krotnym czynnikiem elementarnym wielomianu  $w$  ( $k \in \mathbb{N}$ ) nazywamy każdy wielomian postaci  $v^k$ , gdzie  $v \in \mathcal{P}[\mathcal{A}]$  jest czynnikiem pierwszym, taki że  $v^k$  jest, a  $v^{k+1}$  nie jest dzielnikiem wielomianu  $w$ . ■

(II.95) DEFINICJA. Quasi-czynnikiem elementarnym wielomianu  $w \in \mathcal{P}[\mathcal{A}]$  nazywamy każdy wielomian  $v \in \mathcal{P}[\mathcal{A}]$ , dla którego istnieje taki element  $a \in \mathcal{A}$ , nie będący dzielnikiem zera, że  $v$  jest czynnikiem elementarnym wielomianu  $aw$ . ■

(II.96) DEFINICJA. Rozkładem wielomianu  $w$  na czynniki elementarne nazywamy przedstawienie go w postaci iloczynu czynników elementarnych wielomianu  $w$  (w szczególności w postaci jednego czynnika elementarnego). ■

(II.97) DEFINICJA. Quasi-rozkładem wielomianu  $w \in \mathcal{P}[\mathcal{A}]$  na quasi-czynniki elementarne nazywamy przedstawienie jakiegokolwiek wielomianu  $aw$ , gdzie  $a \in \mathcal{A}$  nie jest dzielnikiem zera, w postaci iloczynu quasi-czynników elementarnych wielomianu  $w$  (w szczególności w postaci jednego quasi-czynnika elementarnego). ■

(II.98) DEFINICJA. Rozkładem wielomianu  $w$  z pierścienia wielomianowego nad ciałem na moniczne czynniki elementarne nazywamy przedstawienie go w postaci iloczynu jego najwyższego współczynnika i monicznych czynników elementarnych. ■

(II.99) TWIERDZENIE. W regularnym pierścieniu wielomianowym  $\mathcal{P}[\mathcal{A}]$  równość  $aw = v_1^{k_1} \dots v_s^{k_s}$ , gdzie  $v_1, \dots, v_s \in \mathcal{P}[\mathcal{A}]$ ,  $k_1, \dots, k_s \in \mathbb{N}$ ,  $a \in \mathcal{A}$ ,  $a \neq 0$ , przedstawia quasi-rozkład wielomianu  $w$  na quasi-czynniki elementarne wtedy i tylko wtedy, gdy  $v_1, \dots, v_s$  są takimi czynnikiem pierwszymi, że dla dowolnych  $\alpha, \beta \in \mathcal{A}$ ,  $j, l \in \{1, \dots, s\}$

$$(II.100) \quad av_j = \beta v_l \Rightarrow \alpha = \beta = 0, \quad \text{gdy } j \neq l.$$

Dowód. Przypadek  $s=1$  jest oczywisty. Załóżmy zatem, że  $s \geq 2$ . Jeżeli równość  $aw = v_1^{k_1} \dots v_s^{k_s}$  przedstawia quasi-rozkład wielomianu  $w$  na quasi-czynniki elementarne, to dla każdego  $q \in \{1, \dots, s\}$  wielomian  $w$  nie jest quasi-podzielny przez wielomian  $v_q^{k_q+1}$ . Gdyby istniały takie elementy  $\alpha, \beta \in \mathcal{A}$  i takie wskaźniki  $j, l \in \{1, \dots, s\}$ ,  $j \neq l$ , że  $av_j = \beta v_l$  i  $\alpha \neq 0$  albo  $\beta \neq 0$ , wtedy na mocy definicji czynnika pierwszego oba elementy  $\alpha$  i  $\beta$  nie byłyby zerami i mielibyśmy

$$\alpha aw = v_1^{k_1} \dots \alpha v_j^{k_j} \dots v_l^{k_l} \dots v_s^{k_s} = v_1^{k_1} \dots v_j^{k_j-1} \dots \beta v_l^{k_l+1} \dots v_s^{k_s},$$

co oznaczałoby, że wielomian  $w$  jest quasi-podzielny przez wielomian  $v_l^{k_l+1}$  i dałoby sprzeczność. Musi być zatem spełniony warunek (II.100).

Jeżeli — odwrotnie — jest spełniony warunek (II.100) i  $aw = v_1^{k_1} \dots v_s^{k_s}$ , to gdyby wielomian  $w$  był quasi-podzielny przez  $v_q^{k_q+1}$  ( $q \in \{1, \dots, s\}$ ), istniałby taki element  $\alpha \in \mathcal{A}$ ,  $\alpha \neq 0$  i taki wielomian  $u \in \mathcal{P}[\mathcal{A}]$ , że  $aw = uv_q^{k_q+1}$ , skąd

$$\alpha v_1^{k_1} \dots v_s^{k_s} = auv_q^{k_q+1}$$

i na mocy twierdzenia (II.79)

$$\alpha v_1^{k_1} \dots v_{q-1}^{k_{q-1}} v_{q+1}^{k_{q+1}} \dots v_s^{k_s} = auv_q.$$

Na mocy twierdzenia (II.92) istniałby wielomian  $v_p$ ,  $p \in \{1, \dots, q-1, q+1, \dots, s\}$ , quasi-



-podzielny przez  $v_q$ , czyli — z uwagi na nierozkładalność wielomianu  $v_p$  — istniałyby takie elementy  $\alpha, \beta \in \mathcal{A}$ ,  $\alpha \neq 0$ , że  $\alpha v_p = \beta v_q$  wbrew (II.100). Z powyższego wynika, że każdy wielomian  $v_q^{k_q}$ ,  $q=1, \dots, s$ , jest quasi-czynnikiem elementarnym wielomianu  $w$ , wobec czego równość  $aw = v_1^{k_1} \dots v_s^{k_s}$  przedstawia quasi-rozkład wielomianu  $w$  na quasi-czynniki elementarne. ■

(II.101) TWIERDZENIE. W pierścieniu wielomianowym  $\mathcal{P}[\mathcal{F}]$  nad ciałem  $\mathcal{F}$  równość  $w = av_1^{k_1} \dots v_s^{k_s}$ , gdzie  $v_1, \dots, v_s \in \mathcal{P}[\mathcal{F}]$ ,  $k_1, \dots, k_s \in \mathbb{N}$ ,  $a \in \mathcal{F}$ ,  $a \neq 0$ , przedstawia rozkład wielomianu  $w$  na moniczne czynniki elementarne wtedy i tylko wtedy, gdy  $v_1, \dots, v_s$  są różnymi monicznymi czynnikami pierwszymi.

Dowód jest analogiczny do dowodu twierdzenia poprzedniego. ■

(II.102) TWIERDZENIE. W pierścieniu wielomianowym  $\mathcal{P}[\mathcal{F}]$  nad ciałem  $\mathcal{F}$  dla każdego wielomianu stopnia dodatniego istnieje dokładnie jeden rozkład na moniczne czynniki elementarne, jeśli nie uwzględniać kolejności czynników elementarnych.

Dowód. Jeżeli wielomian  $w$  jest nierozkładalny i stopnia dodatniego, a  $a_m$  jest jego najwyższym współczynnikiem, to  $v := \frac{1}{a_m} w$  jest wielomianem monicznym, a równość  $w = a_m v$  przedstawia rozkład wielomianu  $w$  na moniczne czynniki elementarne. Jeżeli natomiast wielomian  $w$  jest rozkładalny, to można go przedstawić w postaci  $w = u_1 \dots u_r$ , gdzie  $u_1, \dots, u_r$  są wielomianami stopnia dodatniego. Można tu założyć, że  $u_1, \dots, u_r$  są nierozkładalne, bo gdyby tak nie było, prowadzilibyśmy rozkład dalej, a postępowanie takie musi doprowadzić do czynników nierozkładalnych. Sprowadzając wielomiany  $u_1, \dots, u_r$  przez dzielenie przez najwyższe współczynniki do wielomianów monicznych i łącząc jednakowe czynniki w potęgi, otrzymujemy rozkład wielomianu  $w$  na moniczne czynniki elementarne.

Gdyby istniały dwa rozkłady na moniczne czynniki elementarne

$$w = au_1^{k_1} \dots u_r^{k_r} = bv_1^{l_1} \dots v_s^{l_s},$$

gdzie  $a, b \in \mathcal{F}$ ,  $a, b \neq 0$ ,  $u_1, \dots, u_r, v_1, \dots, v_s \in \mathcal{P}[\mathcal{F}]$ ,  $k_1, \dots, k_r, l_1, \dots, l_s \in \mathbb{N}$ , wtedy z uwagi na moniczność czynników elementarnych byłoby  $a=b$ . Na mocy twierdzenia (II.92) dla każdego czynnika pierwszego  $v_q$  ( $q=1, \dots, s$ ) istniałby czynnik pierwszy  $u_p$  ( $p \in \{1, \dots, r\}$ ) przez niego podzielny, co z uwagi na ich nierozkładalność i moniczność dałoby  $v_q = u_p$ . Uwzględniając symetrię, dochodzimy do wniosku, że  $r=s$  i ciągi  $u_1, \dots, u_r$  oraz  $v_1, \dots, v_s$  różnią się co najwyżej kolejnością wyrazów. Gdyby  $u_p = v_q$  i  $k_p < l_q$ , wtedy na mocy twierdzenia (II.79) mielibyśmy

$$u_1^{k_1} \dots u_{p-1}^{k_{p-1}} u_{p+1}^{k_{p+1}} \dots u_r^{k_r} = v_1^{l_1} \dots v_{q-1}^{l_{q-1}} v_{q+1}^{l_{q+1}} \dots v_s^{l_s},$$

wobec czego na mocy twierdzenia (II.92) pomiędzy czynnikami pierwszymi  $u_1, \dots, u_{p-1}, u_{p+1}, \dots, u_r$  istniałby podzielny przez  $v_q = u_p$ , co byłoby sprzeczne. Ze względu na symetrię nie może być również  $k_p > l_q$  i wobec tego  $k_p = l_q$ . Ponieważ czynnik  $v_q$  został wybrany dowolnie, wykazaliśmy, że rozkład na moniczne czynniki elementarne jest jednoznaczny z dokładnością do kolejności czynników elementarnych. ■

(II.103) DEFINICJA. W regularnym pierścieniu wielomianowym  $\mathcal{P}[\mathcal{A}]$  dwa quasi-rozkłady wielomianu  $w \in \mathcal{P}[\mathcal{A}]$  na quasi-czynniki elementarne

$$(i) \quad aw = u_1^{k_1} \dots u_r^{k_r}, \quad bw = v_1^{l_1} \dots v_s^{l_s},$$

gdzie  $a, b \in \mathcal{A}$ ,  $a, b \neq 0$ ,  $u_1, \dots, u_r, v_1, \dots, v_s \in \mathcal{P}[\mathcal{A}]$ ,  $k_1, \dots, k_r, l_1, \dots, l_s \in \mathbb{N}$ , nazywamy *równoważnymi* wtedy i tylko wtedy, gdy  $r=s$  i dla każdego czynnika pierwszego  $u_p$  ( $p=1, \dots, r$ ) istnieje taki czynnik pierwszy  $v_q$  ( $q \in \{1, \dots, s\}$ ) i takie elementy  $\alpha, \beta \in \mathcal{A}$ ,  $\alpha, \beta \neq 0$ , że  $\alpha u_p = \beta v_q$ . ■

(II.104) TWIERDZENIE. W regularnym pierścieniu wielomianowym  $\mathcal{P}[\mathcal{A}]$  dla każdego wielomianu stopnia dodatniego istnieje quasi-rozkład na quasi-czynniki elementarne, a każde dwa quasi-rozkłady dowolnego wielomianu  $w \in \mathcal{P}[\mathcal{A}]$  na quasi-czynniki elementarne są równoważne.

Dowód. Jeżeli wielomian  $w$  stopnia dodatniego jest quasi-nierozkładalny, to równość  $w = w$  przedstawia jego quasi-rozkład na quasi-czynniki elementarne. Jeżeli natomiast jest quasi-rozkładalny, to istnieje taki element  $c \in \mathcal{A}$ ,  $c \neq 0$ , i takie wielomiany  $u_1, \dots, u_r$  stopni dodatnich, że  $cw = u_1 \dots u_r$ . Można tu przyjąć, że wielomiany  $u_1, \dots, u_r$  nie są już quasi-rozkładalne. Łącząc jednakowe czynniki w potęgi, otrzymujemy równość postaci  $cw = w_1^{l_1} \dots w_s^{l_s}$ , gdzie  $w_j \neq w_k$  dla  $j \neq k$ . Jeżeli pomiędzy wielomianami  $w_1, \dots, w_s$  istnieją takie dwa  $w_p$  i  $w_q$ , że  $\alpha w_p = \beta w_q$ ,  $\alpha, \beta \in \mathcal{A}$ ,  $\alpha, \beta \neq 0$ , to mamy

$$\begin{aligned} \alpha^{l_p} \beta^{l_q} cw &= w_1^{l_1} \dots (\alpha w_p)^{l_p} \dots (\beta w_q)^{l_q} \dots w_s^{l_s} = \\ &= w_1^{l_1} \dots w_{p-1}^{l_{p-1}} w_{p+1}^{l_{p+1}} \dots (\beta w_q)^{l_p+l_q} \dots w_s^{l_s}. \end{aligned}$$

Łącząc w powyższy sposób wszystkie możliwe wielomiany spośród  $w_1, \dots, w_s$  dochodzimy do równości postaci  $aw = v_1^{k_1} \dots v_r^{k_r}$ , gdzie jest spełniony warunek (II.100). Na mocy twierdzenia (II.99) równość ta przedstawia quasi-rozkład wielomianu  $w$  na quasi-czynniki elementarne.

Niech teraz (i) będą dwoma quasi-rozkładami wielomianu  $w$  na quasi-czynniki elementarne. Mamy

$$abw = bu_1^{k_1} \dots u_r^{k_r} = av_1^{l_1} \dots v_s^{l_s}.$$

Na mocy twierdzenia (II.92) dla każdego quasi-czynnika  $v_q$  ( $q=1, \dots, s$ ) istnieje quasi-czynnik  $u_p$  ( $p \in \{1, \dots, r\}$ ) quasi-podzielny przez  $v_q$ , czyli – z uwagi na quasi-nierozkładalność wielomianu  $u_p$  – istnieją takie elementy  $\alpha, \beta \in \mathcal{A}$ ,  $\alpha, \beta \neq 0$ , że  $\alpha u_p = \beta v_q$ . Stąd  $r \geq s$ , a ze względu na symetrię  $s \geq r$ , wobec czego  $r=s$ . Na mocy definicji (II.103) quasi-rozkłady (i) są równoważne. ■

(II.105) TWIERDZENIE. W pierścieniu wielomianowym  $\mathcal{P}[\mathcal{F}]$  nad ciałem  $\mathcal{F}$  wielomian niezerowy  $u \in \mathcal{P}[\mathcal{F}]$  jest dzielnikiem wielomianu  $w \in \mathcal{P}[\mathcal{F}]$ , którego rozkład na moniczne czynniki elementarne ma postać  $w = av_1^{k_1} \dots v_s^{k_s}$  ( $a \in \mathcal{F}$ ,  $a \neq 0$ ,  $v_1, \dots, v_s \in \mathcal{P}[\mathcal{F}]$ ,  $k_1, \dots, k_s \in \mathbb{N}$ ) wtedy i tylko wtedy, gdy można go przedstawić w postaci

$$(II.106) \quad u = cv_1^{l_1} \dots v_s^{l_s},$$

gdzie  $c \in \mathcal{F}$ ,  $c \neq 0$ ,  $l_1, \dots, l_s \in \mathbb{N}_0$  i  $0 \leq l_j \leq k_j$  dla  $j=1, \dots, s$ .

Dowód. Gdy  $u$  jest wielomianem stałym, wystarczy przyjąć  $l_1 = \dots = l_s = 0$  i  $u = ce$ . Załóżmy zatem, że  $u$  jest wielomianem stopnia dodatniego. Na mocy twierdzenia (II.102) niech  $u = cu_1^{m_1} \dots u_r^{m_r}$  będzie rozkładem wielomianu  $u$  na moniczne czynniki elementarne. Z założenia istnieje taki wielomian  $t \in \mathcal{P}[\mathcal{P}]$ , że

$$c \cdot u_1^{m_1} \dots u_r^{m_r} \cdot t = a \cdot v_1^{k_1} \dots v_s^{k_s}.$$

Można przyjąć, że wielomian  $t$  jest moniczny i wtedy  $c = a$ . Dla każdego czynnika pierwszego  $u_p$  ( $p = 1, \dots, r$ ) na mocy twierdzenia (II.92) istnieje czynnik pierwszy  $v_q$  przez niego podzielny, skąd  $u_p = v_q$  i  $m_p \leq k_q$ . Dopisując ewentualnie w rozkładzie wielomianu  $u$  na czynniki elementarne brakujące czynniki spośród  $v_1, \dots, v_s$  z wykładnikami zerowymi, otrzymujemy (II.106). Odwrotnie, gdy  $u$  ma postać (II.106), wtedy w sposób oczywisty jest dzielnikiem wielomianu  $w$ . ■

(II.107) TWIERDZENIE. W regularnym pierścieniu wielomianowym  $\mathcal{P}[\mathcal{A}]$  wielomian niezerowy  $u \in \mathcal{P}[\mathcal{A}]$  jest quasi-dzielnikiem wielomianu  $w \in \mathcal{P}[\mathcal{A}]$ , którego quasi-rozkład na quasi-czynniki elementarne ma postać  $aw = v_1^{k_1} \dots v_s^{k_s}$  ( $a \in \mathcal{A}$ ,  $a \neq 0$ ,  $v_1, \dots, v_s \in \mathcal{P}[\mathcal{A}]$ ,  $k_1, \dots, k_s \in \mathbb{N}$ ) wtedy i tylko wtedy, gdy istnieją takie elementy  $b, c \in \mathcal{A}$ ,  $b, c \neq 0$ , że

$$(II.108) \quad bu = cv_1^{l_1} \dots v_s^{l_s},$$

gdzie  $l_1, \dots, l_s \in \mathbb{N}_0$  i  $0 \leq l_j \leq k_j$  dla  $j = 1, \dots, s$ .

Dowód jest analogiczny do dowodu twierdzenia poprzedniego. ■

(II.109) TWIERDZENIE. Każdy wielomian stopnia dodatniego  $w \in \mathcal{P}[\mathcal{C}]$ , gdzie  $\mathcal{C}$  jest ciałem liczb zespolonych, ma rozkład na moniczne czynniki elementarne postaci:

$$(II.110) \quad w = a(x_1 e - \lambda)^{k_1} \dots (x_s e - \lambda)^{k_s},$$

gdzie  $a \in \mathcal{C}$ ,  $a \neq 0$ ,  $k_1, \dots, k_s \in \mathbb{N}$ ,  $a, x_1, \dots, x_s \in \mathcal{C}$  są pierwiastkami wielomianu  $w$  o krotnościach odpowiednio  $k_1, \dots, k_s$  i  $k_1 + \dots + k_s = \text{st } w$ .

Dowód wynika z twierdzeń (II.83), (II.80) i (II.101). ■

(II.111) TWIERDZENIE. W pierścieniu wielomianowym  $\mathcal{P}[\mathcal{C}]$  nad ciałem liczb zespolonych  $\mathcal{C}$  jedynymi monicznymi czynnikami pierwszymi są wielomiany postaci  $ae - \lambda$ , gdzie  $a \in \mathcal{C}$ .

Dowód wynika z twierdzenia poprzedniego. ■

(II.112) TWIERDZENIE. Rozkład na czynniki elementarne dowolnego wielomianu  $w \in \mathcal{P}[\mathcal{R}]$ , gdzie  $\mathcal{R}$  jest ciałem liczb rzeczywistych, stopnia dodatniego ma postać:

$$(II.113) \quad w = a(x_1 e - \lambda)^{k_1} \dots (x_t e - \lambda)^{k_t} (q_1 e + p_1 \lambda + \lambda^2)^{l_1} \dots (q_r e + p_r \lambda + \lambda^2)^{l_r},$$

gdzie  $a \in \mathcal{R}$ ,  $a \neq 0$ ,  $x_1, \dots, x_t \in \mathcal{R}$  są pierwiastkami wielomianu  $w$  o krotnościach odpowiednio  $k_1, \dots, k_t$ ,  $p_j, q_j \in \mathcal{R}$ ,  $p_j^2 - 4q_j < 0$  dla  $j = 1, \dots, r$  i  $k_1 + \dots + k_t + 2(l_1 + \dots + l_r) = \text{st } w$ .

Dowód. Wielomian  $w$  można traktować jako przypadek szczególny wielomianu z pierścienia  $\mathcal{P}[\mathcal{C}]$ , gdzie  $\mathcal{C}$  jest ciałem liczb zespolonych, i wobec tego jego rozkład na czynniki elementarne w pierścieniu  $\mathcal{P}[\mathcal{C}]$  ma postać (II.110), gdzie  $x_1, \dots, x_s \in \mathcal{C}$  są pierwiastkami zespolonymi wielomianu zespolonego  $w$ . Można tak dobrać wskaźniki, aby z tych

pierwiastków  $x_1, \dots, x_t$  ( $t \leq s$ ) były rzeczywiste, a  $x_{t+1}, \dots, x_s$  już nie. Niech  $x_j$  będzie jednym z pierwiastków nierzeczywistych, a więc takim, że  $x_j^* \neq x_j$  ( $t+1 \leq j \leq s$ ). Ponieważ  $w^* = w$ ,  $\lambda^* = \lambda$ ,  $e^* = e$ , więc na mocy (II.110)  $w = a(x_1^* e - \lambda)^{k_1} \dots (x_s^* e - \lambda)^{k_s}$ , skąd wynika, że jeżeli  $(x_j e - \lambda)^{k_j}$  jest czynnikiem elementarnym wielomianu  $w$ , to  $(x_j^* e - \lambda)^{k_j}$  też jest czynnikiem elementarnym tego wielomianu. Ponieważ

$$(x_j^* e - \lambda)^{k_j} (x_j e - \lambda)^{k_j} = (q_j e + p_j \lambda + \lambda^2)^{k_j},$$

gdzie  $q_j = x_j^* x_j \in \mathcal{R}$ ,  $p_j = -x_j - x_j^* \in \mathcal{R}$  oraz

$$p_j^2 - 4q_j = (x_j + x_j^*)^2 - 4x_j^* x_j = (x_j - x_j^*)^2 = -4(\operatorname{im} x_j)^2 < 0,$$

więc z rozkładu (II.110) wielomianu  $w$  na czynniki elementarne zespolone otrzymujemy rozkład (II.113) wielomianu  $w$  na czynniki elementarne rzeczywiste. ■

(II.114) TWIERDZENIE. W pierścieniu wielomianowym  $\mathcal{P}[\mathcal{R}]$  nad ciałem liczb rzeczywistych  $\mathcal{R}$  jedynymi monicznymi czynnikami pierwszymi są wielomiany postaci  $ae - \lambda$  i  $qe + p\lambda + \lambda^2$ , gdzie  $a, p, q \in \mathcal{R}$  i  $p^2 - 4q < 0$ .

Dowód wynika z twierdzenia poprzedniego. ■

## § II.6. Wzór interpolacyjny Lagrange'a

(II.115) TWIERDZENIE. W dowolnym pierścieniu wielomianowym  $\mathcal{P}[\mathcal{F}]$  nad ciałem  $\mathcal{F}$  istnieje dokładnie jeden wielomian w stopnia co najwyżej  $m \geq 0$  taki, który w  $m+1$  różnych punktach  $a_0, \dots, a_m \in \mathcal{F}$  przyjmuje odpowiednio wartości  $y_0, \dots, y_m \in \mathcal{F}$ . Tym wielomianem jest

$$(II.116) \quad w := \sum_{k=0}^m y_k \cdot \frac{(a_0 e - \lambda) \dots (a_{k-1} e - \lambda)(a_{k+1} e - \lambda) \dots (a_m e - \lambda)}{(a_0 - a_k) \dots (a_{k-1} - a_k)(a_{k+1} - a_k) \dots (a_m - a_k)}.$$

Dowód. Wielomian (II.116) przyjmuje w punktach  $a_0, \dots, a_m$  wartości odpowiednio  $y_0, \dots, y_m$  i jest stopnia co najwyżej  $m$ . Gdyby istniały dwa takie wielomiany  $w$  i  $v$ , wtedy wielomian  $w - v$  byłby też stopnia co najwyżej  $m$  i miałby  $m+1$  różnych pierwiastków, a mianowicie  $a_0, \dots, a_m$ . Na mocy twierdzenia (II.82) wielomian  $w - v$  musiałby być zerowy, skąd  $w = v$ . ■

(II.117) PRZYKŁAD. Znajdziemy wielomian  $w \in \mathcal{P}[\mathcal{R}]$ , gdzie  $\mathcal{R}$  jest ciałem liczb rzeczywistych, który w punktach  $-2, -1, 0, 2$  przyjmuje odpowiednio wartości  $3, 1, 1, 7$  i jest stopnia co najwyżej  $3$ . Na mocy (II.116) mamy

$$\begin{aligned} w = & 3 \cdot \frac{(-e - \lambda)(-\lambda)(2e - \lambda)}{(-1+2) \cdot 2 \cdot (2+2)} + 1 \cdot \frac{(-2e - \lambda)(-\lambda)(2e - \lambda)}{(-2+1) \cdot 1 \cdot (2+1)} + \\ & + 1 \cdot \frac{(-2e - \lambda)(-e - \lambda)(2e - \lambda)}{(-2-0)(-1-0)(2-0)} + 7 \cdot \frac{(-2e - \lambda)(-e - \lambda)(-\lambda)}{(-2-2)(-1-2)(-2)} = e + \lambda + \lambda^2. \quad \blacksquare \end{aligned}$$

Wzór (II.116) nosi nazwę wzoru interpolacyjnego Lagrange'a.

## § II.7. Funkcje wielomianowe

(II.118) DEFINICJA. Lewą (prawą) funkcją wielomianową  $f: \mathcal{X} \rightarrow \mathcal{X}$ , gdzie  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedynką  $\mathcal{A}$ , nazywamy funkcję, która każdemu elementowi  $x \in \mathcal{X}$  przyporządkowuje — zgodnie ze wzorem (II.32) — lewą (prawą) wartość  ${}_x a$  ( $a_{(x)}$ ) określonego wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  w punkcie  $x$ . ■

(II.119) DEFINICJA. Funkcją wielomianową  $f: \mathcal{X} \mapsto \mathcal{X}$ , gdzie  $\mathcal{X}$  jest pierścieniem nad pierścieniem z jedynką  $\mathcal{A}$ , nazywamy funkcję, która każdemu elementowi  $x \in \mathcal{X}$  przyporządkowuje wartość  $a(x)$  określonego wielomianu  $a \in \mathcal{P}[\mathcal{A}]$  w punkcie  $x$ , przy założeniu, że dla każdego  $x \in \mathcal{X}$  taka wartość istnieje. ■

Jeden i ten sam wielomian  $a \in \mathcal{P}[\mathcal{A}]$  może służyć do określenia wielu funkcji wielomianowych, ponieważ można rozpatrywać jego wartości w różnych pierścieniach  $\mathcal{X}$  nad pierścieniem z jedynką  $\mathcal{A}$ .

(II.120) PRZYKŁAD. Wielomian  $a \in \mathcal{P}[\mathcal{R}]$ , gdzie  $\mathcal{R}$  jest ciałem liczb rzeczywistych, określony wzorem  $a := (3, -2, 0, 1, 0, \dots)$  może służyć do określenia funkcji wielomianowej  $f: \mathcal{R} \mapsto \mathcal{R}$  wzorem

$$(i) \quad f(x) := a(x) := 3 - 2x + x^3.$$

Ten sam wzór (i) może służyć do określenia funkcji wielomianowej  $f: \mathcal{C} \mapsto \mathcal{C}$ , gdzie  $\mathcal{C}$  jest ciałem liczb zespolonych.

Wielomian  $a$  może również służyć do określenia funkcji wielomianowej  $f: \mathcal{P}[\mathcal{R}] \mapsto \mathcal{P}[\mathcal{R}]$  wzorem

$$f(x) := a(x) := 3e - 2x + x^3$$

i, na przykład, dla  $x := (1, 1, 0, \dots)$ , czyli — zgodnie ze wzorem (II.29) — dla wielomianu  $x := e + \lambda$  dawać

$$f(e + \lambda) = 3e - 2(e + \lambda) + (e + \lambda)^3 = 2e + \lambda + 3\lambda^2 + \lambda^3. \quad \blacksquare$$

Z drugiej strony jedna i ta sama funkcja wielomianowa

$$f(x) \equiv a_0 + a_1 x + \dots + a_n x^n$$

może nie wyznaczyć współczynników  $a_0, \dots, a_n$  jednoznacznie.

(II.121) PRZYKŁAD. Niech  $\mathcal{A} := (\mathcal{U}, +, \cdot, -, 0, 1)$  będzie pierścieniem z jedynką, gdzie  $\mathcal{U} := \{0, 1\}$ , a działania  $+$ ,  $\cdot$ ,  $-$  są określone wzorami:

$$\begin{aligned} 0+0=0, & \quad 0+1=1, & 1+0=1, & \quad 1+1=0, \\ 0 \cdot 0=0, & \quad 0 \cdot 1=0, & 1 \cdot 0=0, & \quad 1 \cdot 1=1, \\ -0=0, & \quad -1=1. \end{aligned}$$

Rozpatrzmy funkcje wielomianowe  $f, g: \mathcal{A} \mapsto \mathcal{A}$  określone dla dowolnych  $x \in \mathcal{A}$  wzorami:

$$(ii) \quad f(x) := 1 + x, \quad g(x) := 1 + x - x^2 + x^3.$$

Mamy

$$f(0)=1, \quad f(1)=0 \quad \text{oraz} \quad g(0)=1, \quad g(1)=0.$$

Zatem  $f$  i  $g$  są jedną i tą samą funkcją, która może być określona różnymi wielomianami, na przykład wielomianami (ii). ■

(II.122) TWIERDZENIE. Dla regularnego pierścienia wielomianowego  $\mathcal{P}[\mathcal{A}]$ , gdzie  $\mathcal{A}$  jest pierścieniem z jedynek o nieskończenie wielu elementach, każdemu wielomianowi  $a \in \mathcal{P}[\mathcal{A}]$  odpowiada w sposób wzajemnie jednoznaczny funkcja wielomianowa  $f: \mathcal{A} \rightarrow \mathcal{A}$  określona wzorem  $f(x) \equiv a(x)$ ,  $x \in \mathcal{A}$  (a zatem każda taka funkcja wielomianowa  $f$  wyznacza współczynniki wielomianu  $a$  jednoznacznie).

Dowód. Ze wzoru  $f(x) \equiv a(x)$  wynika, że każdy wielomian  $a \in \mathcal{P}[\mathcal{A}]$  wyznacza tę funkcję wielomianową  $f$  jednoznacznie. Gdyby  $f(x) \equiv a(x)$  i  $f(x) \equiv b(x)$  oraz  $a \neq b$ , wtedy każdy element  $x \in \mathcal{A}$  byłby pierwiastkiem wielomianu  $c := a - b$ , czyli wielomian niezerowy  $c$  miałby nieskończenie wiele pierwiastków, wbrew twierdzeniu (II.82). Zatem każda funkcja wielomianowa  $f: \mathcal{A} \rightarrow \mathcal{A}$  wyznacza wielomian  $a$  jednoznacznie. ■

(II.123) TWIERDZENIE. Dla regularnego pierścienia wielomianowego  $\mathcal{P}[\mathcal{A}]$ , gdzie  $\mathcal{A}$  jest pierścieniem z jedynek o nieskończenie wielu elementach, zbiór wszystkich funkcji wielomianowych  $f: \mathcal{A} \rightarrow \mathcal{A}$ , określonych wzorami postaci  $f(x) \equiv a(x)$ ,  $x \in \mathcal{A}$ , tworzy pierścień izomorficzny z  $\mathcal{P}[\mathcal{A}]$ .

Dowód, na mocy twierdzenia poprzedniego, wynika ze wzoru  $f(x) \equiv a(x)$ . ■

Definicje (II.118) i (II.119) oraz twierdzenie (II.123) kładą pomost między teorią wielomianów wyłożoną wyżej a teorią opartą na definicji wielomianu jako funkcji. W obu teoriach rozpatrujemy wiele analogicznych faktów, ich zapis też bywa analogiczny, a różnica leży wtedy głównie w interpretacji wzorów.

Główna korzyść płynąca z wprowadzenia algebraicznej definicji wielomianu, jak to było wyłożone wyżej, polega na tym, że jeden i ten sam wielomian może służyć — jak widzieliśmy w przykładzie (II.120) — do określenia różnych funkcji wielomianowych.