

Wtedy — co dowodzimy indukcyjnie — dla każdego $a \in \mathcal{F}$, $a \neq 0$ i dowolnych $m, n \in \mathbb{Z}$

$$(I.248) \quad a^m a^n = a^{m+n},$$

$$(I.249) \quad (a^m)^n = a^{mn},$$

$$(I.250) \quad \frac{a^m}{a^n} = a^{m-n}.$$

(I.251) DEFINICJA. *Podciałem* ciała (ciała z transpozycją) \mathcal{F} nazywamy każdy podpierścień (podpierścień z transpozycją) ciała \mathcal{F} , który jest ciałem. ■

(I.252) PRZYKŁAD. Ciało liczb wymiernych \mathbb{Q} jest podciałem ciała liczb rzeczywistych \mathbb{R} . ■

(I.253) DEFINICJA. Ciała (ciała z transpozycją) \mathcal{F}_1 i \mathcal{F}_2 nazywamy *izomorficznymi* wtedy i tylko wtedy, gdy są pierścieniami (pierścieniami z transpozycją) izomorficznymi. ■

(I.254) DEFINICJA. W dowolnym ciele \mathcal{F} \mathcal{F} -liczbą wymierną nazywamy każdy element postaci p/q , gdzie p jest \mathcal{F} -liczbą całkowitą, a q — \mathcal{F} -liczbą naturalną. ■

(I.255) TWIERDZENIE. W dowolnym ciele z transpozycją \mathcal{F} każda \mathcal{F} -liczba wymierna jest *quasi-rzeczywista*.

Dowód wynika ze wzorów (I.105), (I.239), (I.240) i (I.241). ■

(I.256) TWIERDZENIE. W dowolnym ciele \mathcal{F} zbiór wszystkich \mathcal{F} -liczb wymiernych tworzy podciało.

Dowód wynika ze wzorów (I.232), (I.236), (I.234), a dla ciał z transpozycją ponadto ze wzorów (I.239) i (I.240). ■

Można wykazać, że dla ciała \mathcal{F} , w którym \mathcal{F} -zero nie jest \mathcal{F} -liczbą naturalną, czyli nie istnieje \mathcal{F} -liczba naturalna $n=0$, podciało \mathcal{F} -liczb wymiernych jest izomorficzne z ciałem liczb wymiernych \mathbb{Q} .

(I.257) TWIERDZENIE. Jeżeli \mathcal{F} jest ciałem z transpozycją, to $\text{re } \mathcal{F}$ jest też ciałem i jest podciałem ciała \mathcal{F} .

Dowód. Na mocy twierdzenia (I.99) $\text{re } \mathcal{F}$ jest podpierścieniem ciała \mathcal{F} . Ponieważ na mocy (I.239), (I.240), (I.241), (I.92) $a \neq 0 \wedge a \in \text{re } \mathcal{F} \Rightarrow \frac{1}{a} \in \text{re } \mathcal{F}$, więc $\text{re } \mathcal{F}$ jest ciałem i jest podciałem ciała \mathcal{F} . ■

§ I.8. Liczby zespolone

(I.258) DEFINICJA. *Ciałem liczb zespolonych* nazywamy ciało z transpozycją

$$(I.259) \quad \mathbb{C} := (\mathbb{C}, +, \cdot, -, s, t, o, e),$$

gdzie $\mathbb{C} := \mathbb{R}^2$ jest zbiorem wszystkich uporządkowanych par (czyli ciągów dwuwyrzowych) liczb rzeczywistych z warunkiem określonym dla dowolnych $a, b, c, d \in \mathbb{R}$ i (a, b) ,

$(c, d) \in \mathbb{C}$ wzorem

$$(I.260) \quad (a, b) = (c, d) \Leftrightarrow a = c \wedge b = d,$$

$+$, \cdot , $-$, s , t , o , e są operacjami określonymi dla dowolnych $a, b, c, d \in \mathbb{R}$ i $(a, b), (c, d) \in \mathbb{C}$ wzorami:

$$(I.261) \quad (a, b) + (c, d) := (a + c, b + d),$$

$$(I.262) \quad (a, b)(c, d) := (ac - bd, ad + bc),$$

$$(I.263) \quad -(a, b) := (-a, -b),$$

$$(I.264) \quad \overline{(a, b)} := (a, -b),$$

$$(I.265) \quad (a, b)^T := (a, b),$$

$$(I.266) \quad o := (0, 0),$$

$$(I.267) \quad e := (1, 0). \quad \blacksquare$$

Sprawdzamy, że dla (I.259) są spełnione wszystkie warunki stawiane ciałom z transpozycją. W szczególności dla każdego elementu $(a, b) \in \mathbb{C}$, $(a, b) \neq o$ istnieje odwrotność

$$(I.268) \quad \frac{e}{(a, b)} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right).$$

(I.269) TWIERDZENIE. W ciele liczb zespolonych \mathbb{C} zbiór wszystkich elementów postaci $(a, 0) \in \mathbb{C}$ tworzy podciało izomorficzne z ciałem liczb rzeczywistych \mathbb{R} .

Dowód. Ze wzorów (I.261), ..., (I.268) wynika, że zbiór wszystkich elementów postaci $(a, 0) \in \mathbb{C}$ tworzy podciało ciała \mathbb{C} . Wprowadzając odwzorowanie różnowartościowe h określone dla dowolnego $a \in \mathbb{R}$ wzorem $h(a) := (a, 0) \in \mathbb{C}$, sprawdzamy z łatwością, że to podciało jest izomorficzne z \mathbb{R} . \blacksquare

Na podstawie twierdzenia (I.269) utożsamia się wymienione tam ciała izomorficzne przyjmując, że dla każdego $a \in \mathbb{R}$

$$(I.270) \quad (a, 0) = a.$$

(I.271) DEFINICJA. Jedynką urojoną nazywamy element ciała liczb zespolonych (I.259)

$$(I.272) \quad i := (0, 1). \quad \blacksquare$$

Symbol (I.272) obowiązuje w całej niniejszej książce.

(I.273) DEFINICJA. Liczbą zespoloną nazywamy każdy element ciała (I.259). \blacksquare

(I.274) TWIERDZENIE. Dla każdej liczby zespolonej $(a, b) \in \mathbb{C}$ jest

$$(I.275) \quad (a, b) = a + bi.$$

Dowód. Mamy $(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1)$, skąd na mocy (I.270) i (I.272) wzór (I.275). \blacksquare

Ze wzorów (I.272), (I.270) i (I.262) wynika, że

$$(I.276) \quad i^2 = -1.$$

Ze wzorów (I.266), (I.267) i (I.270) wynika, że

$$(I.277) \quad o=0, \quad e=1.$$

Ze wzorów (I.264) i (I.265) wynika, że

$$(I.278) \quad (a, b)^* = (a, -b),$$

a ze wzorów (I.229), (I.262) i (I.268) oraz (I.275)

$$(I.279) \quad \frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2} i \quad \text{dla } c+di \neq 0.$$

(I.280) DEFINICJA. Częścią rzeczywistą liczby zespolonej (I.275) nazywamy liczbę rzeczywistą a , a częścią urojoną — liczbę rzeczywistą b . ■

Część rzeczywistą liczby zespolonej c oznaczamy symbolem $\operatorname{re} c$, a część urojoną symbolem $\operatorname{im} c$. Symbol re jest skrótem wyrazu angielskiego *real*=rzeczywisty, a symbol im skrótem wyrazu angielskiego *imaginary*=urojony. Mamy zatem dla liczby zespolonej (I.275) $\operatorname{re}(a, b) = a$ i $\operatorname{im}(a, b) = b$.

(I.281) TWIERDZENIE. Ciało liczb zespolonych \mathcal{C} ze zwykłą nierównością dla liczb rzeczywistych (I.270) jest pierścieniem częściowo uporządkowanym i jest pierścieniem z pierwiastkowaniem.

Dowód. Na mocy twierdzenia (I.222) ciało \mathcal{C} jest pierścieniem całkowitym. Podpierścień $\operatorname{re} \mathcal{C}$ na mocy (I.264) i (I.265) składa się z liczb postaci (I.270) i ze zwykłą nierównością liczb rzeczywistych jest uporządkowany. Jeżeli $(a, b)^* = (a, b)$, to na mocy wzorów (I.278) i (I.260) $b = -b$, skąd $b = 0$ i wobec tego $(a, b) \in \operatorname{re} \mathcal{C}$. Wreszcie dla każdej liczby zespolonej (I.275) mamy $(a, b)^*(a, b) = (a+bi)^*(a+bi) = (a-bi)(a+bi) = a^2 + b^2 \geq 0$. Ciało \mathcal{C} jest zatem pierścieniem częściowo uporządkowanym. Na mocy definicji (I.169) jest też pierścieniem z pierwiastkowaniem. ■

(I.282) TWIERDZENIE. Ciało liczb zespolonych \mathcal{C} ze zwykłą nierównością dla liczb rzeczywistych (I.270) jest pierścieniem z wartością bezwzględną określoną dla dowolnej liczby zespolonej (I.275) wzorem:

$$(I.283) \quad |a+bi| := \sqrt{a^2+b^2}.$$

Dowód. Wynika z definicji (I.168), ponieważ $(a+bi)^*(a+bi) = a^2 + b^2$. ■

(I.284) TWIERDZENIE. Dla każdej liczby zespolonej $a+bi \neq 0$ istnieją dokładnie dwa pierwiastki kwadratowe, określone wzorem

$$(I.285) \quad \sqrt{a+bi} = \pm \left(\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + i\varepsilon_b \sqrt{\frac{\sqrt{a^2+b^2}-a}{2}} \right),$$

gdzie

$$\varepsilon_b := \begin{cases} -1 & \text{dla } b < 0, \\ 1 & \text{dla } b \geq 0. \end{cases}$$

Wzór (I.285) obejmuje również jedyny pierwiastek kwadratowy liczby $a+bi=0$ równy 0.

Dowód. Ponieważ

$$\sqrt{a^2+b^2}+a \geq 0 \quad \text{oraz} \quad \sqrt{a^2+b^2}-a \geq 0,$$

więc istnieją pierwiastki kwadratowe

$$\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}, \sqrt{\frac{\sqrt{a^2+b^2}-a}{2}} \in \operatorname{re} \mathcal{C}.$$

Sprawdzamy, że dla $\sqrt{a+bi}$ określonego wzorem (I.285) jest

$$(\sqrt{a+bi})^2 = a+bi,$$

czyli wzór (I.285) — istotnie — określa dwa pierwiastki kwadratowe dla dowolnej liczby zespolonej $a+bi \neq 0$, a jeden dla $a+bi=0$. Na mocy twierdzenia (I.164) innych pierwiastków kwadratowych liczba zespolona $a+bi$ nie ma. ■

(I.286) PRZYKŁAD. Na mocy wzoru (I.285)

$$\sqrt{i} = \pm \left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i \right), \quad \sqrt{-i} = \pm \left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} i \right). \quad \blacksquare$$

(I.287) DEFINICJA. Postacią trygonometryczną liczby zespolonej $c:=a+bi \neq 0$ nazywamy postać

$$(I.288) \quad c = r(\cos \varphi + i \sin \varphi),$$

gdzie

$$(I.289) \quad r := |c| = \sqrt{a^2+b^2}, \quad \cos \varphi := \frac{a}{r}, \quad \sin \varphi := \frac{b}{r}. \quad \blacksquare$$

(I.290) DEFINICJA. Argumentem liczby zespolonej $c:=a+bi \neq 0$ nazywamy każdą liczbę rzeczywistą $\arg c := \varphi$, gdzie φ spełnia warunki (I.289). Argumentem głównym liczby zespolonej $c:=a+bi \neq 0$ nazywamy ten jej argument $\operatorname{Arg} c$, który spełnia warunek

$$(I.291) \quad 0 \leq \operatorname{Arg} c < 2\pi. \quad \blacksquare$$

Dla liczby $c=0$ argument, a więc i postać trygonometryczna nie są określone. Każda liczba zespolona $c \neq 0$ ma nieskończenie wiele argumentów, ale dokładnie jeden argument główny. Dla dowolnego argumentu $\arg c$ istnieje taka liczba całkowita k , że

$$(I.292) \quad \arg c = \operatorname{Arg} c + k \cdot 2\pi.$$

(I.293) PRZYKŁAD. Dla $c := \sqrt{3} + i$ mamy na mocy (I.289) $r = |c| = 2$, $\cos \varphi = \frac{1}{2}\sqrt{3}$, $\sin \varphi = \frac{1}{2}$, wobec czego $\operatorname{Arg} c = \frac{1}{6}\pi$ i dla dowolnego całkowitego k

$$c = 2(\cos(\frac{1}{6}\pi + 2k\pi) + i \sin(\frac{1}{6}\pi + 2k\pi)). \quad \blacksquare$$

Sprawdzamy, że dla dowolnych niezerowych liczb zespolonych

$$c_j = r_j (\cos \varphi_j + i \sin \varphi_j), \quad j = 1, 2,$$

mamy

$$(I.294) \quad c_1 c_2 = r_1 r_2 (\cos (\varphi_1 + \varphi_2) + i \sin (\varphi_1 + \varphi_2)),$$

$$(I.295) \quad \frac{c_1}{c_2} = \frac{r_1}{r_2} (\cos (\varphi_1 - \varphi_2) + i \sin (\varphi_1 - \varphi_2)).$$

Wychodząc ze wzorów (I.294) i (I.295) z łatwością dowodzi się przez indukcję zupełną, że dla dowolnej niezerowej liczby zespolonej $c = r(\cos \varphi + i \sin \varphi)$ i dowolnej liczby całkowitej k

$$(I.296) \quad c^k = r^k (\cos k\varphi + i \sin k\varphi).$$

Jest to tzw. wzór Moivre'a.

(I.297) DEFINICJA. Pierwiastkiem n -tego stopnia ($n \in \mathbb{N}$) liczby zespolonej c nazywamy każdą taką liczbę zespoloną $\sqrt[n]{c}$, która spełnia warunek

$$(I.298) \quad (\sqrt[n]{c})^n = c. \quad \blacksquare$$

(I.299) TWIERDZENIE. Każda liczba zespolona $c = r(\cos \varphi + i \sin \varphi) \neq 0$ ma dokładnie n różnych pierwiastków n -tego stopnia ($n \in \mathbb{N}$), a mianowicie

$$(I.300) \quad \sqrt[n]{c} = \sqrt[n]{r} \left(\cos \frac{\varphi + k \cdot 2\pi}{n} + i \sin \frac{\varphi + k \cdot 2\pi}{n} \right) \quad \text{dla} \quad k = 0, 1, \dots, n-1.$$

Liczba zespolona 0 ma tylko jeden pierwiastek n -tego stopnia $\sqrt[n]{0} = 0$.

Dowód wynika z definicji (I.297) i ze wzoru Moivre'a (I.296). \blacksquare

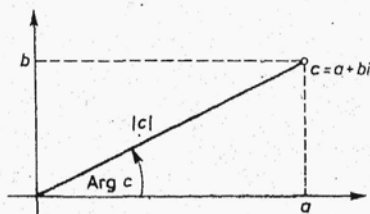
(I.301) PRZYKŁAD. Na mocy (I.300) i przykładu (I.293) liczba zespolona $\sqrt{3} + i$ ma 5 pierwiastków piątego stopnia:

$$\sqrt[5]{2} (\cos 6^\circ + i \sin 6^\circ), \quad \sqrt[5]{2} (\cos 78^\circ + i \sin 78^\circ), \quad \sqrt[5]{2} (\cos 150^\circ + i \sin 150^\circ),$$

$$\sqrt[5]{2} (\cos 222^\circ + i \sin 222^\circ), \quad \sqrt[5]{2} (\cos 294^\circ + i \sin 294^\circ). \quad \blacksquare$$

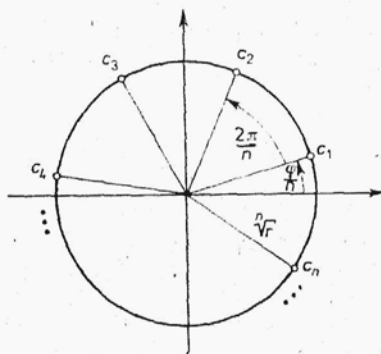
(I.302) DEFINICJA. Obrazem geometrycznym liczby zespolonej $c = a + bi$ na płaszczyźnie współrzędnych nazywamy punkt (a, b) na tej płaszczyźnie. \blacksquare

Jak wynika z tej definicji, wartość bezwzględna i argument liczby zespolonej są współrzednymi biegunowymi jej obrazu geometrycznego (rys. 1).



Rys. 1

Jak wynika ze wzoru (I.300), obrazy geometryczne n pierwiastków n -tego stopnia c_1, \dots, c_n liczby zespolonej $c = r(\cos \varphi + i \sin \varphi) \neq 0$ leżą na okręgu koła o środku w początku układu współrzędnych i promieniu $\sqrt[n]{r}$ i dzielą ten okrąg na n równych części (rys. 2).



Rys. 2

§ I.9. Liczby nieskończone

(I.303) **DEFINICJA.** *Liczbami nieskończonymi* nazywamy dwa elementy ∞ i $-\infty$ dołączane do zbioru liczb rzeczywistych \mathbb{R} z następującym określeniem działań na nich, gdzie r jest dowolną liczbą rzeczywistą, a n dowolną liczbą naturalną:

$$\infty + \infty = \infty, \quad \infty - (-\infty) = \infty, \quad -\infty - \infty = -\infty, \quad -(-\infty) = \infty,$$

$$r + \infty = \infty, \quad r - \infty = -\infty,$$

$$\infty \cdot \infty = (-\infty)(-\infty) = \infty, \quad (-\infty) \cdot \infty = -\infty,$$

$$r \cdot \infty = \begin{cases} \infty & \text{dla } r > 0, \\ -\infty & \text{dla } r < 0, \end{cases} \quad r \cdot (-\infty) = \begin{cases} -\infty & \text{dla } r > 0, \\ \infty & \text{dla } r < 0, \end{cases}$$

$$\frac{r}{\infty} = \frac{r}{-\infty} = 0,$$

$$\infty^n = \infty, \quad (-\infty)^n = \begin{cases} \infty & \text{dla } n \text{ parzystych,} \\ -\infty & \text{dla } n \text{ nieparzystych.} \end{cases} \quad \blacksquare$$

Dodawanie i mnożenie w powyższych wzorach traktujemy jako przemienne.

Symbole $\infty - \infty$, $-\infty + \infty$, $0 \cdot \infty$, $0 \cdot (-\infty)$, $\frac{\infty}{\infty}$, $\frac{\infty}{-\infty}$, $\frac{-\infty}{\infty}$, $\frac{-\infty}{-\infty}$, uważamy za nieokreślone. Przyjmuje się, że dla każdej liczby rzeczywistej r jest $-\infty < r < \infty$ oraz że $|- \infty| = |\infty| = \infty$. Ponadto $\overline{\infty} = \infty^T = \infty$ oraz $\overline{-\infty} = (-\infty)^T = -\infty$.

§ I.10. Pierścienie z podzielnością

(I.304) DEFINICJA. *Pierścieniem z lewą (prawą) podzielnością* nazywamy każdy pierścień $\mathcal{A} := (\mathcal{A}, +, \cdot, -, 0)$, który spełnia następujące dwa warunki:

1° istnieje funkcja zwana *porządkującą* $\varphi: \mathcal{A} \rightarrow \mathfrak{B}$, gdzie \mathfrak{B} jest zbiorem uporządkowanym z relacją porządkującą \leq zawierającym element wyróżniony o , spełniająca dla każdego $a \in \mathcal{A}$ warunki:

$$(I.305) \quad \varphi(a) \geq o,$$

$$(I.306) \quad \varphi(a) = o \Leftrightarrow a = 0;$$

2° dla każdych $a, b \in \mathcal{A}$, $b \neq 0$, istnieją takie $q, r \in \mathcal{A}$, że

$$(I.307) \quad a = bq + r \quad (a = qb + r),$$

$$(I.308) \quad \varphi(r) < \varphi(b). \quad \blacksquare$$

(I.309) DEFINICJA. *Pierścieniem z podzielnością* nazywamy każdy pierścień z zarówno lewą jak i prawą podzielnością z tą samą funkcją porządkującą. \blacksquare

(I.310) PRZYKŁAD. Pierścień liczb całkowitych \mathcal{Z} z funkcją porządkującą $\varphi(z) \equiv |z|$ ($z \in \mathcal{Z}$) jest pierścieniem z podzielnością. \blacksquare

(I.311) TWIERDZENIE. *Jeżeli w pierścieniu częściowo uporządkowanym \mathcal{A} istnieje taki element λ , że*

$$(I.312) \quad \lambda \neq 0 \wedge \lambda^* = -\lambda \wedge \lambda^* \lambda < 3,$$

to \mathcal{A} jest pierścieniem z podzielnością z funkcją porządkującą określoną dla $x \in \mathcal{A}$ wzorem

$$(I.313) \quad \varphi(x) \equiv x^* x.$$

Dowód. Niech $a, b \in \mathcal{A}$, $b \neq 0$. Na mocy (I.153) istnieją takie \mathcal{A} -liczby całkowite m i n , że

$$2mb^*b \leq b^*b + (a^*b + ab^*) < 2(m+1)b^*b,$$

$$2n\lambda^*\lambda b^*b \leq \lambda^*\lambda b^*b + \lambda(a^*b - ab^*) < 2(n+1)\lambda^*\lambda b^*b,$$

czyli

$$(i) \quad -b^*b \leq -2mb^*b + (a^*b + ab^*) < b^*b,$$

$$-\lambda^*\lambda b^*b \leq -2n\lambda^*\lambda b^*b + \lambda(a^*b - ab^*) < \lambda^*\lambda b^*b.$$

Przyjmując $q := m + \lambda n$, mamy $q^* + q = 2m$ i $\lambda(q^* - q) = 2n\lambda^*\lambda$ i wzory (i) można napisać w postaci:

$$(ii) \quad -b^*b \leq -(q^* + q)b^*b + (a^*b + ab^*) < b^*b,$$

$$-\lambda^*\lambda b^*b \leq -\lambda(q^* - q)b^*b + \lambda(a^*b - ab^*) < \lambda^*\lambda b^*b.$$

Przyjmując następnie $r := a - qb$, mamy

$$br^* + b^*r = -(q^* + q)b^*b + (a^*b + ab^*), \quad \lambda(br^* - b^*r) = -\lambda(q^* - q)b^*b + \lambda(a^*b - ab^*),$$

wobec czego na mocy (ii)

$$-b^*b \leq br^* + b^*r < b^*b, \quad -\lambda^*\lambda b^*b \leq \lambda(br^* - b^*r) < \lambda^*\lambda b^*b,$$

a stąd

$$0 \leq (br^* + b^*r)^2 \leq (b^*b)^2, \quad 0 \leq -\lambda^*\lambda (br^* - b^*r)^2 \leq (\lambda^*\lambda)^2 (b^*b)^2,$$

czyli

$$0 \leq (br^* + b^*r)^2 \leq (b^*b)^2,$$

$$0 \leq -(br^* - b^*r)^2 \leq (\lambda^*\lambda)(b^*b)^2.$$

Sumując te nierówności stronami, otrzymujemy

$$4b^*br^*r \leq (1 + \lambda^*\lambda)(b^*b)^2,$$

czyli

$$(I.314) \quad 4r^*r \leq (1 + \lambda^*\lambda)(b^*b)$$

i dla $\lambda^*\lambda < 3$ otrzymujemy $r^*r < b^*b$, czyli $\varphi(r) < \varphi(b)$. ■

Następujący przykład pokazuje, że nie wszystkie pierścienie częściowo uporządkowane z funkcją porządkującą (I.313) są pierścieniami z podzielnością.

(I.315) PRZYKŁAD. Niech \mathcal{A} będzie pierścieniem utworzonym przez wszystkie liczby zespolone postaci $a + 2bi$, gdzie a, b są dowolnymi liczbami całkowitymi. Sprawdzamy z łatwością, że \mathcal{A} jest pierścieniem częściowo uporządkowanym. Przyjmujemy (I.313) jako funkcję porządkującą. Niech $x + 2yi, r + 2si$ będą takimi elementami z pierścienia \mathcal{A} , że

$$-5 + 4i = (x + 2yi)(5 + 4i) + (r + 2si).$$

Otrzymujemy stąd

$$\varphi(r + 2si) = (r + 2si)^*(r + 2si) = r^2 + 4s^2 = 41x^2 + 18x + 164y^2 - 160y + 41.$$

W zakresie liczb rzeczywistych $41x^2 + 18x < 0 \Leftrightarrow -\frac{18}{41} < x < 0$ oraz $164y^2 - 160y < 0 \Leftrightarrow 0 < y < \frac{160}{164}$, wobec czego dla całkowitych x i y jest

$$\varphi(r + 2si) \geq 41 = (5 + 4i)^*(5 + 4i) = \varphi(5 + 4i).$$

Oznacza to, że \mathcal{A} nie jest pierścieniem z podzielnością z funkcją porządkującą (I.313). ■

(I.316) PRZYKŁAD. Pierścień utworzony przez wszystkie liczby zespolone postaci $a + bi$, gdzie a, b są dowolnymi liczbami całkowitymi, jest na mocy twierdzenia (I.311) pierścieniem z podzielnością z funkcją porządkującą (I.313). Przyjmując bowiem $\lambda := i$ mamy spełnione warunki (I.312), a nierówność (I.314) przyjmuje postać $2r^*r \leq b^*b$. ■

(I.317) TWIERDZENIE. Każdy pierścień uporządkowany \mathcal{A} jest pierścieniem z podzielnością, a jako funkcję porządkującą można przyjąć $\varphi(x) := x^2$ ($x \in \mathcal{A}$).

Dowód. Niech $a, b \in \mathcal{A}$, $b \neq 0$. Na mocy (I.153) istnieje taka \mathcal{A} -liczba całkowita n , że $nb \leq a < (n+1)b$ dla $b > 0$ i $nb \leq a < (n-1)b$ dla $b < 0$. Kładąc $q := n$ i $r = a - qb$, otrzymujemy $0 \leq r < b$ dla $b > 0$, a $0 \leq r < -b$ dla $b < 0$, a stąd otrzymujemy $\varphi(r) < \varphi(b)$ i wzory (I.307), (I.308). ■

(I.318) DEFINICJA. Pierścieniem z lewą (prawą) quasi-podzielnością nazywamy każdy pierścień $\mathcal{X} := (\mathcal{X}, +, \cdot, -, 0, 1)$ nad pierścieniem z jedynką \mathcal{A} spełniający następujące dwa warunki:

1° istnieje funkcja porządkująca φ spełniająca warunki (I.305) i (I.306);

2° dla każdych $x, y \in \mathcal{X}$, $y \neq 0$, istnieją takie $q, r \in \mathcal{X}$ i element $a \in \mathcal{A}$, nie będący dzielnikiem zera, że

$$(I.319) \quad ax = yq + r \quad (xa = qy + r),$$

$$(I.320) \quad \varphi(r) < \varphi(b). \quad \blacksquare$$

(I.321) DEFINICJA. Pierścieniem z quasi-podzielnością nazywamy każdy pierścień \mathcal{X} nad pierścieniem z jedynką \mathcal{A} z zarówno lewą jak i prawą quasi-podzielnością z tą samą funkcją porządkującą. ■

Przykłady pierścieni z quasi-podzielnością poznamy w następnych rozdziałach.

(I.322) DEFINICJA. W dowolnym pierścieniu \mathcal{A} z lewą (prawą) podzielnością i funkcją porządkującą φ o wartościach rzeczywistych całkowitych algorytmem Euklidesa nazywamy algorytm określony dla dowolnego niezerowego ciągu (a_1, \dots, a_n) elementów z \mathcal{A} ($n \geq 2$), a polegający na konstrukcji ciągów $(a_1^{(k)}, \dots, a_n^{(k)})$ elementów z \mathcal{A} , gdzie $k = 0, 1, 2, \dots$, i

$$(I.323) \quad (a_1^{(0)}, \dots, a_n^{(0)}) := (a_1, \dots, a_n)$$

przez ustalenie wzoru rekurencyjnego

$$(I.324) \quad (a_1^{(k+1)}, \dots, a_n^{(k+1)}) := (r_1^{(k)}, \dots, r_n^{(k)})$$

i podanie następującego sposobu obliczania elementów $r_1^{(k)}, \dots, r_n^{(k)}$:

1) Jeżeli $n-1$ elementów spośród $a_1^{(k)}, \dots, a_n^{(k)}$ jest \mathcal{A} -zerami, to algorytm kończy się i nie obliczamy następnego ciągu (I.324).

2) Jeżeli co najmniej dwa elementy spośród $a_1^{(k)}, \dots, a_n^{(k)}$ nie są \mathcal{A} -zerami, to wybieramy taki $b^{(k)} := a_{u_k}^{(k)}$ spośród nich, który dla wszystkich $a_j^{(k)} \neq 0$ spełnia warunek

$$(I.325) \quad 0 < \varphi(b^{(k)}) \leq \varphi(a_j^{(k)}).$$

3) Dla każdego elementu $a_j^{(k)}$, $j \neq u_k$, znajdujemy takie elementy $q_j^{(k)}$ i $r_j^{(k)}$, że

$$(I.326) \quad a_j^{(k)} = b^{(k)} q_j^{(k)} + r_j^{(k)} \quad (a_j^{(k)} = q_j^{(k)} b^{(k)} + r_j^{(k)}),$$

$$(I.327) \quad \varphi(r_j^{(k)}) < \varphi(b^{(k)}).$$

4) Dla $j = u_k$ przyjmujemy

$$(I.328) \quad q_j^{(k)} = 0, \quad r_j^{(k)} = a_j^{(k)} = b^{(k)}. \quad \blacksquare$$

(I.329) DEFINICJA. W dowolnym pierścieniu \mathcal{X} nad pierścieniem z jedynką \mathcal{A} z lewą (prawą) quasi-podzielnością i funkcją porządkującą φ o wartościach całkowitych *slabym algorytmem Euklidesa* nazywamy algorytm określony analogicznie jak w (I.322) z tą jedyną różnicą, że zamiast (I.326) znajdujemy takie elementy $q_j^{(k)}, r_j^{(k)} \in \mathcal{X}$ i taki element $\alpha_j^{(k)} \in \mathcal{A}$ nie będący dzielnikiem zera, że

$$(I.330) \quad \alpha_j^{(k)} a_j^{(k)} = b^{(k)} q_j^{(k)} + r_j^{(k)} \quad (a_j^{(k)} \alpha_j^{(k)} = q_j^{(k)} b^{(k)} + r_j^{(k)}). \quad \blacksquare$$

(I.331) TWIERDZENIE. *Każdy algorytm Euklidesa i każdy słaby algorytm Euklidesa jest skończony, tzn. dla dowolnego niezerowego ciągu (a_1, \dots, a_n) z pierścienia \mathcal{A} (z pierścienia \mathcal{X}) istnieje takie $p \in \mathbb{N}_0$ i taki element $b^{(p-1)}$, że — zgodnie ze wzorem (I.324)*

$$(I.332) \quad (a_1^{(p)}, \dots, a_n^{(p)}) = (0, \dots, 0, b^{(p-1)}, 0, \dots, 0).$$

Dowód. Jeżeli dla $p=0$ zachodzi wzór (I.332), to algorytm kończy się zanim się zaczął. W pozostałych przypadkach mamy na mocy (I.325) i (I.327)

$$(I.333) \quad \varphi(b^{(0)}) > \varphi(b^{(1)}) > \dots > 0.$$

Ponieważ funkcja φ z założenia przyjmuje tylko wartości całkowite nieujemne, w ciągu (I.333) musi więc pojawić się wyraz ostatni $\varphi(b^{(p-1)})$, gdzie $b^{(p-1)}$ musi być jedynym niezerowym wyrazem ciągu (I.332). \blacksquare

(I.334) PRZYKŁAD. Skonstruujemy algorytm Euklidesa w pierścieniu liczb całkowitych \mathcal{Z} z funkcją porządkującą $\varphi(x) := |x|$ dla ciągu (42, 78, 30). Zgodnie z (I.323) mamy

$$(a_1^{(0)}, a_2^{(0)}, a_3^{(0)}) = (42, 78, 30).$$

Ponieważ $\varphi(30) < \varphi(42) < \varphi(78)$, więc przyjmujemy $b^{(0)} := 30$. Wobec tego, że $42 = 1 \cdot 30 + 12$, $\varphi(12) < \varphi(30)$ oraz $78 = 2 \cdot 30 + 18$, $\varphi(18) < \varphi(30)$, mamy

$$(a_1^{(1)}, a_2^{(1)}, a_3^{(1)}) = (r_1^{(0)}, r_2^{(0)}, r_3^{(0)}) = (12, 18, 30).$$

Stąd $b^{(1)} := 12$. Ponieważ $18 = 1 \cdot 12 + 6$, $\varphi(6) < \varphi(12)$ oraz $30 = 2 \cdot 12 + 6$, więc

$$(a_1^{(2)}, a_2^{(2)}, a_3^{(2)}) = (r_1^{(1)}, r_2^{(1)}, r_3^{(1)}) = (12, 6, 6).$$

Stąd $b^{(2)} := 6$. Ponieważ $12 = 2 \cdot 6 + 0$ i $6 = 1 \cdot 6 + 0$, mamy więc

$$(a_1^{(3)}, a_2^{(3)}, a_3^{(3)}) = (r_1^{(2)}, r_2^{(2)}, r_3^{(2)}) = (0, 0, 6).$$

Na tym algorytm kończy się. \blacksquare

(I.335) DEFINICJA. Jeżeli dla dowolnych elementów a, b, c w dowolnym pierścieniu \mathcal{A} jest $a = bc$, to w przypadku $b \neq 0$ element a nazywamy *lewostronnie podzielny przez b* ,

a element b lewym dzielnikiem a , a w przypadku $c \neq 0$ element a nazywamy *prawostronnie podzielny* przez c , a element c *prawym dzielnikiem* a . ■

(I.336) DEFINICJA. W dowolnym pierścieniu \mathcal{A} element a nazywamy *podzielny* przez $b \neq 0$, a b — *dzielnikiem* a wtedy i tylko wtedy, gdy a jest zarówno lewostronnie jak i prawostronnie podzielny przez b . ■

(I.337) DEFINICJA. W dowolnym pierścieniu \mathcal{A} *wspólnym dzielnikiem* (*wspólnym lewym dzielnikiem*, *wspólnym prawym dzielnikiem*) elementów a_1, \dots, a_n nazywamy każdy element d , który jest dzielnikiem (lewym dzielnikiem, prawym dzielnikiem) każdego z elementów a_1, \dots, a_n . ■

(I.338) DEFINICJA. W dowolnym pierścieniu \mathcal{A} *największym wspólnym dzielnikiem* (*największym wspólnym lewym dzielnikiem*, *największym wspólnym prawym dzielnikiem*) elementów a_1, \dots, a_n nazywamy każdy taki element d , że:

1° d jest wspólnym dzielnikiem (wspólnym lewym dzielnikiem, wspólnym prawym dzielnikiem) elementów a_1, \dots, a_n ,

2° d jest podzielny (lewostronnie podzielny, prawostronnie podzielny) przez każdy wspólny dzielnik (wspólny lewy dzielnik, wspólny prawy dzielnik) elementów a_1, \dots, a_n . ■

W teorii pierścieni istnieje rozbudowana teoria dzielników, wspólnych dzielników i w szczególności największych wspólnych dzielników. W niniejszej książce wykorzystuje się z tego niewiele. Warto zauważyć, że w definicji (I.338) nie żąda się, aby pierścień \mathcal{A} był uporządkowany czy nawet częściowo uporządkowany. Warto również zauważyć, że definicja (I.338) ma niewielki sens w przypadku ciała, ponieważ w każdym ciele każdy element różny od zera jest największym wspólnym dzielnikiem każdego skończonego ciągu liczbowego.

(I.339) TWIERDZENIE. Jeżeli w pierścieniu całkowitym \mathcal{A} , w którym jedynymi elementami mającymi lewą (prawą) odwrotność są 1 i -1 , istnieje dla elementów a_1, \dots, a_n największy wspólny lewy (prawy) dzielnik d , to jedynymi największymi wspólnymi lewymi (prawymi) dzielnikami elementów a_1, \dots, a_n są d i $-d$.

Dowód. Jeżeli d_1 i d_2 są dwoma największymi wspólnymi lewymi dzielnikami elementów a_1, \dots, a_n , to z definicji (I.338) wynika istnienie takich elementów a, b , że $d_1 = d_2 a$ i $d_2 = d_1 b$, skąd $d_1 = d_1 \cdot 1 = d_1 b a$. Na mocy twierdzenia (I.112) $ba = 1$, co oznacza, że $a = b = 1$ albo $a = b = -1$, skąd wynika teza. Dla największych wspólnych prawych dzielników dowód przebiega analogicznie. ■

(I.340) DEFINICJA. Jeżeli dla dowolnych elementów x, y, z w dowolnym pierścieniu \mathcal{A} nad pierścieniem \mathcal{Z} z jedynką \mathcal{A} istnieje taki element $a \in \mathcal{A}$ nie będący dzielnikiem zera, że $az = xy$, to w przypadku $x \neq 0$ element z nazywamy *lewostronnie quasi-podzielny* przez x , a element x *lewym quasi-dzielnikiem* z , a w przypadku $y \neq 0$ element z nazywamy *prawostronnie quasi-podzielny* przez y , a element y *prawym quasi-dzielnikiem* z . ■

Spostrzegamy analogię między definicjami (I.335) i (I.340). Analogicznie do (I.336) definiujemy *elementy quasi-podzielne* i *quasi-dzielniki*, a analogicznie do (I.337) i (I.338) —

wspólne quasi-dzielniki, lewe i prawe oraz największe wspólne quasi-dzielniki, lewe i prawe dla pierścieni \mathcal{R} nad pierścieniami z jedyneką \mathcal{A} .

(I.341) TWIERDZENIE. W algorytmie Euklidesa (I.322) (w słabym algorytmie Euklidesa (I.329)) element $b^{(p-1)}$ z ostatniego ciągu (I.332) jest największym wspólnym lewym (prawym) dzielnikiem (największym wspólnym lewym (prawym) quasi-dzielnikiem) elementów a_1, \dots, a_n .

Dowód. Element $b^{(p-1)}$ jest wspólnym lewym dzielnikiem wyrazów ciągu (I.332). Jeżeli $b^{(p-1)}$ jest wspólnym lewym dzielnikiem wyrazów ciągu (I.324), to na mocy (I.328) jest lewym dzielnikiem elementu $b^{(k)}$ i na mocy (I.326) jest wspólnym lewym dzielnikiem wyrazów ciągu $(a_1^{(k)}, \dots, a_n^{(k)})$. Stąd na mocy indukcji skończonej $b^{(p-1)}$ jest wspólnym lewym dzielnikiem wyrazów ciągu (I.323). Jeżeli — odwrotnie — d jest wspólnym lewym dzielnikiem wyrazów ciągu $(a_1^{(k)}, \dots, a_n^{(k)})$, to w szczególności jest lewym dzielnikiem elementu $b^{(k)}$ i na mocy (I.326) jest wspólnym lewym dzielnikiem wyrazów ciągu (I.324). Na mocy indukcji d jest wspólnym lewym dzielnikiem wyrazów ciągu (I.332), czyli jest lewym dzielnikiem elementu $b^{(p-1)}$. Stąd na mocy definicji (I.338) wynika teza.

Dowód w przypadku prawostronnej podzielności, jak również w przypadkach lewostronnej lub prawostronnej quasi-podzielności, przebiega analogicznie. ■

(I.342) PRZYKŁAD. Na mocy przykładu (I.334) liczba 6 jest największym wspólnym dzielnikiem liczb 42, 78, 30. Na mocy twierdzenia (I.339) w pierścieniu liczb całkowitych \mathbb{Z} jest to jedyny dodatni największy wspólny dzielnik tych liczb. ■

(I.343) PRZYKŁAD. Niech \mathcal{A} będzie pierścieniem z przykładu (I.316) z funkcją porządkującą (I.313). Na mocy twierdzenia (I.331) dla każdego ciągu skończonego w \mathcal{A} istnieje skończony algorytm Euklidesa. Rozpatrzmy ciąg $(10, 4+2i, 7+i)$. Ponieważ $\varphi(10)=100$, $\varphi(4+2i)=20$, $\varphi(7+i)=50$, więc przyjmujemy $b^{(0)}:=4+2i$. Wobec tego, że $10=(4+2i)(2-i)+0$ i $7+i=1 \cdot (4+2i)+(3-i)$ oraz $\varphi(3-i)=10 < \varphi(4+2i)$, mamy

$$(a_1^{(1)}, a_2^{(1)}, a_3^{(1)}) = (r_1^{(0)}, r_2^{(0)}, r_3^{(0)}) = (0, 4+2i, 3-i)$$

i przyjmujemy $b^{(1)}:=3-i$. Ponieważ $4+2i=(3-i)(1+i)+0$, więc

$$(a_1^{(2)}, a_2^{(2)}, a_3^{(2)}) = (0, 0, 3-i)$$

i algorytm kończy się. Na mocy twierdzenia (I.341) liczba zespolona $3-i$ jest w pierścieniu \mathcal{A} największym wspólnym dzielnikiem liczb $10, 4+2i, 7+i$.

Jak łatwo spostrzec, liczba zespolona $3-i$ nie jest jedynym największym wspólnym dzielnikiem liczb $10, 4+2i, 7+i$. Jeżeli d jest największym wspólnym dzielnikiem tych liczb, to na mocy definicji (I.338) istnieją w \mathcal{A} takie liczby zespolone a i b , że

$$3-i=ad, \quad d=(3-i)b,$$

skąd wynika, że $ab=1$. Na mocy (I.175) jest wobec tego $|a|=1$ i $|b|=1$. Stąd b musi być jedną z 4 liczb zespolonych $1, -1, i, -i$. W konsekwencji jedynymi największymi wspólnymi dzielnikami liczb $10, 4+2i, 7+i$ w pierścieniu \mathcal{A} są liczby $3-i, -3+i, 1+3i, -1-3i$. ■

(I.344). PRZYKŁAD. Jeżeli pierścień \mathcal{A} z przykładu (I.315) traktować jako pierścień nad pierścieniem liczb całkowitych \mathbb{Z} , to każdy element $a+2bi$ tego pierścienia jest quasi-podzielny przez każdy element $c+2di \neq 0$, gdzie a, b, c, d są dowolnymi liczbami całkowitymi, ponieważ

$$(c^2 + 4d^2)(a + 2bi) = (a + 2bi)(c - 2di)(c + 2di).$$

Wobec tego \mathcal{A} jest wtedy pierścieniem z quasi-podzielnością z funkcją porządkującą (I.313). Każdy element różny od zera w \mathcal{A} jest największym wspólnym quasi-dzielnikiem każdego skończonego ciągu elementów tego pierścienia. ■