

(I.103) PRZYKŁAD. Pierścień liczb całkowitych (I.96) oraz pierścienie  $\text{re } \mathcal{A}$  z przykładu (I.101) są izomorficzne, co sprawdzamy z łatwością, przyjmując odwzorowanie  $f(a) = (a, a)$  dla  $a \in \mathbb{Z}$ . ■

W każdym pierścieniu z jedyneką (I.51), a więc w szczególności w każdym pierścieniu z transpozycją (I.61) wprowadza się pojęcie  $\mathcal{A}$ -liczb naturalnych, przyjmując jako pierwszą  $\mathcal{A}$ -liczbę naturalną  $\mathcal{A}$ -jedynekę 1 i dla każdej  $\mathcal{A}$ -liczby naturalnej  $n$  określając jej następnik jako  $n+1$ . Dołączając do zbioru wszystkich  $\mathcal{A}$ -liczb naturalnych  $\mathcal{A}$ -zero oraz wszystkie elementy postaci  $-n$ , gdzie  $n$  jest  $\mathcal{A}$ -liczbą naturalną, otrzymujemy zbiór  $\mathcal{A}$ -liczb całkowitych.

Zbiór  $\mathcal{A}$ -liczb naturalnych oznaczamy symbolem  $\mathfrak{N}_{\mathcal{A}}$ , a zbiór  $\mathcal{A}$ -liczb całkowitych symbolem  $\mathfrak{Z}_{\mathcal{A}}$ . Jeżeli  $\mathcal{A}$ -zero nie jest  $\mathcal{A}$ -liczbą naturalną, lub — co na jedno wychodzi — wszystkie wyrazy ciągu kolejnych  $\mathcal{A}$ -liczb naturalnych są różne, można udowodnić, że podpierścień  $\mathcal{L}_{\mathcal{A}} := (\mathfrak{Z}_{\mathcal{A}}, +, \cdot, -, s, t, 0, 1)$  pierścienia (I.61) jest izomorficzny z pierścieniem liczb całkowitych (I.96). Przypadek, gdy  $\mathcal{A}$ -zero jest  $\mathcal{A}$ -liczbą naturalną, lub — co na jedno wychodzi — istnieje taka  $\mathcal{A}$ -liczba naturalna  $n$ , że  $n=0$ , jest w niniejszej książce dopuszczany, ale szczegółowo analizować go nie będziemy, odsyłając zainteresowanego czytelnika do podręczników algebry zawierających teorię kongruencji. Najważniejsze elementy tej teorii znajdzie czytelnik w rozdziale XIV wspomnianej monografii H. Rasiowej.

Jeżeli  $n$  jest dowolną  $\mathcal{A}$ -liczbą całkowitą w pierścieniu (I.51) lub (I.61), to na mocy (I.50), (I.44) i (I.45) dla dowolnego  $a \in \mathcal{A}$  mamy

$$(I.104) \quad na = an,$$

a ponadto w pierścieniu (I.61) mamy na mocy (I.92)

$$(I.105) \quad n = \bar{n} = n^T = n^*,$$

co wykazujemy analogicznie do dowodu twierdzenia (I.99). Ze wzoru (I.105) wynika, że podpierścień  $\text{re } \mathcal{A}$  dowolnego przemiennego pierścienia z transpozycją  $\mathcal{A}$  zawiera wszystkie  $\mathcal{A}$ -liczby całkowite.

#### § I.4. Dzielniki zera. Odwrotności

(I.106) DEFINICJA. W dowolnym pierścieniu  $\mathcal{A}$  element  $a$  nazywamy lewym (prawym) dzielnikiem zera wtedy i tylko wtedy, gdy istnieje takie  $b \in \mathcal{A}$ ,  $b \neq 0$ , że  $ab=0$  ( $ba=0$ ). ■

(I.107) DEFINICJA. Dzielnikiem zera dowolnego pierścienia  $\mathcal{A}$  nazywamy każdy lewy i każdy prawy dzielnik zera tego pierścienia. ■

(I.108) DEFINICJA. Dzielnik zera dowolnego pierścienia  $\mathcal{A}$  nazywamy właściwym wtedy i tylko wtedy, gdy nie jest  $\mathcal{A}$ -zerem. ■

(I.109) DEFINICJA. Pierścieniem całkowitym albo dziedziną całkowitości nazywamy każdy przemienny pierścień z jedyneką, który nie zawiera właściwych dzielników zera. ■

(I.110) PRZYKŁAD. Pierścień (I.96) jest całkowity. Pierścień z przykładu (I.69) nie jest całkowity, bo jego elementy postaci  $(a, 0)$  i  $(0, b)$ ,  $a \neq 0$ ,  $b \neq 0$ , są właściwymi dzielnikami zera. ■

(I.111) TWIERDZENIE. *W dowolnym pierścieniu  $\mathcal{A}$  iloczyn elementów nie będących dzielnikami zera nie jest dzielnikiem zera. W pierścieniu przemiennym  $\mathcal{A}$  iloczyn nie jest dzielnikiem zera wtedy i tylko wtedy, gdy jego czynniki nie są dzielnikami zera.*

Dowód. Niech  $a, b \in \mathcal{A}$  nie będą dzielnikami zera, a  $c \in \mathcal{A}$  niech będzie takim elementem, że  $(ab)c=0$ , czyli  $a(bc)=0$ . Wtedy  $bc=0$ , a następnie  $c=0$ . Wynika stąd, że  $ab$  nie jest lewym dzielnikiem zera. Analogicznie dowodzimy, że  $ab$  nie jest prawym dzielnikiem zera. Odwrotnie, gdyby  $ab$  nie był dzielnikiem zera, a  $a$  był prawym dzielnikiem zera, wtedy istniałby element  $c \neq 0$ , taki, że  $ca=0$  i wobec tego  $cab=c(ab)=0$ , skąd sprzeczność. Zatem  $a$  nie jest prawym dzielnikiem zera, a w pierścieniu przemiennym  $\mathcal{A}$  nie jest również lewym dzielnikiem zera. Analogicznie dowodzimy, że  $b$  nie jest dzielnikiem zera. Dla większej liczby czynników dowód przeprowadzamy z łatwością przez indukcję. ■

(I.112) TWIERDZENIE. *Jeżeli w dowolnym pierścieniu  $\mathcal{A}$  jego element  $a$  nie jest lewym dzielnikiem zera, to dla dowolnych  $b, c \in \mathcal{A}$*

$$(I.113) \quad ab=ac \Rightarrow b=c,$$

*jeśli natomiast  $a$  nie jest prawym dzielnikiem zera, to*

$$(I.114) \quad ba=ca \Rightarrow b=c.$$

Dowód. Równość  $ab=ac$  jest równoważna  $a(b-c)=0$ . Gdy  $a$  nie jest lewym dzielnikiem zera, mamy stąd  $b-c=0$ , czyli  $b=c$ . Implikację (I.114) dowodzimy analogicznie. ■

(I.115) DEFINICJA. W dowolnym pierścieniu z jedyneką  $\mathcal{A}$  jego element  $b$  nazywamy *lewą (prawą) odwrotnością* elementu  $a \in \mathcal{A}$  wtedy i tylko wtedy, gdy  $ba=1$  ( $ab=1$ ). ■

(I.116) TWIERDZENIE. *Jeżeli w dowolnym pierścieniu z jedyneką  $\mathcal{A}$  element  $a$  ma lewą (prawą) odwrotność, to nie jest lewym (prawym) dzielnikiem zera.*

Dowód. Niech  $ba=1$ . Gdyby element  $a$  był lewym dzielnikiem zera, wtedy istniałby element  $c \in \mathcal{A}$ ,  $c \neq 0$ , taki że  $ac=0$ . Stąd byłoby  $bac=c=0$ , co dałoby sprzeczność. Analogicznie dowodzimy, że jeżeli  $ab=1$ , to  $a$  nie jest prawym dzielnikiem zera. ■

(I.117) TWIERDZENIE. *Jeżeli w dowolnym pierścieniu z jedyneką  $\mathcal{A}$  element  $a$  ma zarówno lewą jak i prawą odwrotność, to ma tylko jedną lewą i tylko jedną prawą odwrotność i są one równe.*

Dowód. Gdy  $ab_1=1$  i  $ab_2=1$ , wtedy  $a(b_1-b_2)=0$  i na mocy twierdzeń (I.112) i (I.116)  $b_1=b_2$ . Gdy  $ca=1$  i  $ab=1$ , wtedy  $(ca)b=b$ , czyli  $c(ab)=b$ , skąd  $c=b$ . ■

(I.118) DEFINICJA. W dowolnym pierścieniu z jedyneką  $\mathcal{A}$  jego element  $b$  nazywamy *odwrotnością elementu  $a \in \mathcal{A}$*  i piszemy  $b=a^{-1}$  lub  $b=1/a$  wtedy i tylko wtedy, gdy  $b$  jest zarówno lewą jak i prawą odwrotnością  $a$ . ■

(I.119) DEFINICJA. W dowolnym pierścieniu z jedyneką  $\mathcal{A}$  element  $a$  nazywamy *odwracalnym* wtedy i tylko wtedy, gdy ma odwrotność. ■

(I.120) TWIERDZENIE. *Każdy element odwracalny dowolnego pierścienia z jedynek  $\mathcal{A}$  nie jest dzielnikiem zera tego pierścienia.*

Dowód wynika z twierdzenia (I.116) i definicji (I.119). ■

(I.121) TWIERDZENIE. *W dowolnym pierścieniu z jedynek  $\mathcal{A}$  iloczyn elementów odwracalnych  $a_1, \dots, a_n$  jest odwracalny i*

$$(I.122) \quad (a_1 \dots a_n)^{-1} = a_n^{-1} \dots a_1^{-1}.$$

Dowód. Dla  $n=2$  teza jest oczywista, ponieważ  $(a_2^{-1} a_1^{-1})(a_1 a_2) = (a_1 a_2)(a_2^{-1} a_1^{-1}) = 1$ . Dowód dla dowolnego  $n \in \mathfrak{N}$  przeprowadzamy z łatwością przez indukcję zupełną. ■

(I.123) TWIERDZENIE. *W dowolnym przemiennym pierścieniu z jedynek  $\mathcal{A}$  iloczyn  $a_1 \dots a_n$  jest odwracalny wtedy i tylko wtedy, gdy wszystkie elementy  $a_1, \dots, a_n$  są odwracalne.*

Dowód. Jeżeli  $a_1, \dots, a_n$  są odwracalne, to iloczyn  $a_1 \dots a_n$  jest odwracalny na mocy poprzedniego twierdzenia. Jeżeli  $x \in \mathcal{A}$  jest takim elementem, że  $a_1 \dots a_n x = x a_1 \dots a_n = 1$ , to dla dowolnego  $a_k$  ( $k=1, \dots, n$ ) mamy  $a_k(a_1 \dots a_{k-1} a_{k+1} \dots a_n x) = (a_1 \dots a_{k-1} a_{k+1} \dots a_n x) a_k = 1$ , skąd wynika odwracalność elementu  $a_k$ . ■

(I.124) TWIERDZENIE. *W dowolnym pierścieniu z jedynek  $\mathcal{A}$ , jeżeli element  $a$  jest odwracalny, to elementy  $\bar{a}$ ,  $a^T$ ,  $a^*$ ,  $a^n$  ( $n \in \mathfrak{N}$  albo  $n=-1$ ) są również odwracalne i*

$$(I.125) \quad (\bar{a})^{-1} = \overline{(a^{-1})},$$

$$(I.126) \quad (a^T)^{-1} = (a^{-1})^T,$$

$$(I.127) \quad (a^*)^{-1} = (a^{-1})^*,$$

$$(I.128) \quad (a^n)^{-1} = (a^{-1})^n, \quad (a^{-1})^{-1} = a.$$

Dowód. Wzory (I.125), (I.126), (I.127) otrzymujemy na mocy równości

$$\overline{(aa^{-1})} = \overline{(a^{-1}a)} = \bar{1} = 1, \quad (aa^{-1})^T = (a^{-1}a)^T = 1^T = 1, \quad (aa^{-1})^* = (a^{-1}a)^* = 1^* = 1$$

oraz na mocy wzorów (I.64), (I.67) i (I.75). Wzór (I.128) wynika z (I.122) i (I.114). ■

(I.129) PRZYKŁAD. W każdym pierścieniu z jedynek elementy 1 i  $-1$  są odwracalne i każdy z nich jest swoją odwrotnością. ■

## § I.5. Pierścień uporządkowany

(I.130) DEFINICJA. Pierścień  $\mathcal{A}$  nazywamy *uporządkowanym* wtedy i tylko wtedy, gdy:

1° jest pierścieniem całkowitym z transpozycją,

2° wszystkie jego elementy są quasi-rzeczywiste,

3° jest w nim określona relacja porządkująca  $\leq$ , spełniająca dla dowolnych  $a, b, c \in \mathcal{A}$  następujące warunki:

$$(I.131) \quad a \leq b \vee b \leq a \quad (\text{w szczególności } a \leq a),$$

$$(I.132) \quad a \leq b \wedge b \leq a \Rightarrow a = b,$$

$$(I.133) \quad a \leq b \wedge b \leq c \Rightarrow a \leq c,$$

$$(I.134) \quad a \leq b \Rightarrow a + c \leq b + c,$$

$$(I.135) \quad a \leq b \wedge 0 \leq c \Rightarrow ac \leq bc,$$

$$(I.136) \quad 0 \leq a \wedge a \neq 0 \Rightarrow \text{istnieje taka } \mathcal{A}\text{-liczba naturalna } n, \text{ że } b \leq na. \quad \blacksquare$$

Zamiast  $a \leq b$  piszemy również  $b \geq a$ , a zamiast  $a \leq b \wedge a \neq b$  piszemy  $a < b$  albo  $b > a$ .

(I.137) TWIERDZENIE. W każdym pierścieniu uporządkowanym  $\mathcal{A}$  dla dowolnych  $a, b, c, d, a_1, \dots, a_n \in \mathcal{A}$  jest:

$$(I.138) \quad a < b \vee a = b \vee a > b \text{ i każda z tych możliwości wyklucza dwie pozostałe,}$$

$$(I.139) \quad (a \leq b \wedge b < c) \vee (a < b \wedge b \leq c) \vee (a < b \wedge b < c) \Rightarrow a < c,$$

$$(I.140) \quad a < b \Rightarrow a + c < b + c,$$

$$(I.141) \quad a \leq b \wedge c \leq d \Rightarrow a + c \leq b + d,$$

$$(I.142) \quad (a \leq b \wedge c < d) \vee (a < b \wedge c \leq d) \vee (a < b \wedge c < d) \Rightarrow a + c < b + d,$$

$$(I.143) \quad a_j \geq 0 \text{ dla } j=1, \dots, n \Rightarrow \sum_{j=1}^n a_j \geq 0,$$

$$(I.144) \quad a_j \geq 0 \text{ dla } j=1, \dots, n \wedge \bigvee_{k \in \{1, \dots, n\}} a_k \neq 0 \Rightarrow \sum_{j=1}^n a_j > 0,$$

$$(I.145) \quad a_j \geq 0 \text{ dla } j=1, \dots, n \wedge \sum_{j=1}^n a_j = 0 \Rightarrow a_1 = \dots = a_n = 0,$$

$$(I.146) \quad a \leq b \Rightarrow -a \geq -b,$$

$$(I.147) \quad a < b \Rightarrow -a > -b,$$

$$(I.148) \quad a < b \wedge c > 0 \Rightarrow ac < bc,$$

$$(I.149) \quad a \leq b \wedge c \leq 0 \Rightarrow ac \geq bc,$$

$$(I.150) \quad a < b \wedge c < 0 \Rightarrow ac > bc,$$

$$(I.151) \quad a^2 = a^* a \geq 0 \wedge (a \neq 0 \Rightarrow a^2 = a^* a > 0),$$

$$(I.152) \quad n > 0 \text{ dla każdej } \mathcal{A}\text{-liczby naturalnej } n,$$

$$(I.153) \quad a > 0 \Rightarrow \text{istnieje taka } \mathcal{A}\text{-liczba całkowita } n, \text{ że } na \leq b < (n+1)a.$$

Dowód. Wzór (I.138) wynika z (I.131), (I.132) i określenia symbolu  $<$ . Ponieważ na mocy (I.133)  $a \leq b \wedge b < c \Rightarrow a \leq b \wedge b \leq c \Rightarrow a \leq c$ , a dla  $a = c$  byłoby  $a \leq b \wedge b < c \Rightarrow a \leq b \wedge b \leq a$ , czyli na mocy (I.132)  $a = b = c$ , co byłoby sprzeczne z założeniem  $b < c$ , więc  $a \leq b \wedge b < c \Rightarrow a < c$ . Dwa pozostałe przypadki wzoru (I.139) dowodzimy analogicznie.

Ponieważ  $a=b \Leftrightarrow a+c=b+c$ , więc wzór (I.140) wynika z (I.134). Mamy dalej na mocy (I.134) i (I.133)

$$a \leq b \wedge c \leq d \Rightarrow a+c \leq b+c \wedge b+c \leq b+d \Rightarrow a+c \leq b+d,$$

czyli wzór (I.141). Następnie na mocy (I.140) i (I.139)

$$a \leq b \wedge c < d \Rightarrow a+c \leq b+c \wedge b+c < b+d \Rightarrow a+c < b+d.$$

Analogicznie dowodzimy dwa pozostałe przypadki wzoru (I.142). Na mocy (I.141) mamy  $a_1 \geq 0 \wedge a_2 \geq 0 \Rightarrow a_1 + a_2 \geq 0$ , skąd przez indukcję zupełną dowodzimy (I.143). Analogicznie na mocy (I.142) mamy  $a_1 \geq 0 \wedge a_2 \geq 0 \wedge (a_1 \neq 0 \vee a_2 \neq 0) \Leftrightarrow (a_1 \geq 0 \wedge a_2 > 0) \vee (a_1 > 0 \wedge a_2 \geq 0) \vee (a_1 > 0 \wedge a_2 > 0) \Rightarrow a_1 + a_2 > 0$ , skąd przez indukcję zupełną dowodzimy (I.144). Wzór (I.145) wynika z dwu poprzednich.

Na mocy (I.134) mamy  $a \leq b \Rightarrow a - (a+b) \leq b - (a+b) \Rightarrow -b \leq -a$ , czyli wzór (I.146) i analogicznie na mocy (I.140) wzór (I.147). Mamy dalej na mocy (I.135)

$$a < b \wedge c > 0 \Rightarrow a \leq b \wedge 0 \leq c \Rightarrow ac \leq bc.$$

Ponieważ  $a < b \Rightarrow a \neq b$ , natomiast  $c > 0 \wedge ac = bc$  pociąga za sobą na mocy twierdzenia (I.112)  $a = b$ , co daje sprzeczność, zatem  $ac \neq bc$  i otrzymujemy wzór (I.148). Jeżeli  $c \leq 0$ , to na mocy (I.146)  $-c \geq 0$  i wzór (I.149) otrzymujemy z (I.135) i (I.146). Analogicznie dowodzimy wzór (I.150).

Na mocy (I.138) mamy  $a < 0 \vee a = 0 \vee a > 0$ . Jeżeli  $a < 0$ , to na mocy (I.150)  $a^2 > 0$ . Jeżeli  $a = 0$ , to  $a^2 = 0$ . Jeżeli  $a > 0$ , to na mocy (I.148)  $a^2 > 0$ . Biorąc pod uwagę, że  $a^* = a$ , otrzymujemy stąd wzór (I.151).

Na mocy twierdzenia (I.55)  $1 \neq 0$ , a na mocy (I.151)  $1 = 1^2 > 0$ , skąd przez indukcję zupełną na mocy wzoru (I.142) otrzymujemy (I.152).

Na mocy (I.136) istnieją takie  $\mathcal{A}$ -liczby naturalne  $p$  i  $q$ , że  $b \leq qa$  i  $-b \leq pa$ , czyli  $-pa \leq b \leq qa$ . Pomiedzy  $\mathcal{A}$ -liczbami całkowitymi  $-p, -p+1, \dots, q-1, q$  istnieje największa  $n$  taka, że  $na \leq b$ , skąd  $(n+1)a > b$  i wzór (I.153). ■

(I.154) DEFINICJA. W pierścieniu uporządkowanym każdy element  $a \geq 0$  nazywamy *nieujemnym*, każdy element  $a \leq 0$  — *niedodatnim*, każdy element  $a > 0$  — *dodatnim*, a każdy element  $a < 0$  — *ujemnym*. ■

(I.155) PRZYKŁAD. Pierścień liczb całkowitych ze zwykłą nierównością jest uporządkowany. ■

(I.156) DEFINICJA. Pierścień  $\mathcal{A}$  nazywamy *częściowo uporządkowanym* wtedy i tylko wtedy, gdy:

- 1° jest pierścieniem całkowitym z transpozycją,
- 2° podpierścień  $\text{re } \mathcal{A}$  jest uporządkowany,
- 3°  $a \in \mathcal{A} \wedge a = a^* \Rightarrow a \in \text{re } \mathcal{A}$ ,
- 4°  $a \in \mathcal{A} \Rightarrow a^* a \geq 0$ . ■

(I.157) PRZYKŁAD. Niech  $\mathcal{A} := (\mathbb{N}, +, \cdot, -, s, t, 0, 1)$  będzie pierścieniem, w którym

$\mathfrak{A}$  jest zbiorem wszystkich uporządkowanych par liczb całkowitych, a operacje  $+$ ,  $\cdot$ ,  $-$ ,  $s$ ,  $t$ ,  $0$ ,  $1$  dla dowolnych  $(a, b)$ ,  $(c, d) \in \mathfrak{A}$  są określone wzorami:

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

$$-(a, b) := (-a, -b), \quad \overline{(a, b)} := (a, b), \quad (a, b)^T := (a, -b),$$

$$0 := (0, 0), \quad 1 := (1, 0).$$

Sprawdzamy z łatwością, że  $\mathcal{A}$  jest pierścieniem całkowitym z transpozycją. Jeżeli w podpierścieniu  $\text{re } \mathcal{A}$ , który – jak łatwo sprawdzić – jest utworzony przez wszystkie pary postaci  $(a, 0)$ , wprowadzić relację  $\leq$  wzorem  $(a, 0) \leq (b, 0) \Leftrightarrow a \leq b$ , to  $\mathcal{A}$  staje się pierścieniem częściowo uporządkowanym. ■

(I.158) TWIERDZENIE. *Każdy pierścień uporządkowany jest pierścieniem częściowo uporządkowanym.*

Dowód. Wynika z faktu, że dla pierścienia uporządkowanego  $\mathcal{A}$  jest  $\text{re } \mathcal{A} = \mathcal{A}$ . ■

(I.159) TWIERDZENIE. *W dowolnym pierścieniu częściowo uporządkowanym  $\mathcal{A}$  dla dowolnych  $a_1, \dots, a_n, b_1, \dots, b_n \in \mathcal{A}$  jest*

$$(I.160) \quad \left( \sum_{j=1}^n a_j^* b_j \right)^* \left( \sum_{j=1}^n a_j^* b_j \right) \leq \left( \sum_{j=1}^n a_j^* a_j \right) \left( \sum_{j=1}^n b_j^* b_j \right),$$

gdzie równość zachodzi wtedy i tylko wtedy, gdy istnieją takie elementy  $c, d \in \mathcal{A}$ , z których co najmniej jeden nie jest  $\mathcal{A}$ -zerem, że

$$(I.161) \quad ca_j + db_j = 0 \quad \text{dla } j = 1, \dots, n.$$

Gdy  $\mathcal{A}$  jest pierścieniem uporządkowanym, wzór (I.160) można napisać w postaci

$$(I.162) \quad \left( \sum_{j=1}^n a_j b_j \right)^2 \leq \left( \sum_{j=1}^n a_j^2 \right) \left( \sum_{j=1}^n b_j^2 \right).$$

Dowód. Jeżeli  $\sum_{j=1}^n a_j^* a_j = 0$ , to na mocy 4° i (I.145)  $a_j^* a_j = 0$  dla  $j = 1, \dots, n$  i na mocy 1°, (I.73), (I.91)  $a_1 = \dots = a_n = 0$  i warunek (I.160) jest spełniony, jak również (I.161) dla  $c = 1$  i  $d = 0$ . Pozostaje zatem przeprowadzenie dowodu w przypadku, gdy  $\sum_{j=1}^n a_j^* a_j > 0$ . Mamy na mocy 4° i (I.143)

$$(i) \quad \sum_{j=1}^n \left( \left( \sum_{k=1}^n a_k^* b_k \right) a_j - \left( \sum_{k=1}^n a_k^* a_k \right) b_j \right)^* \left( \left( \sum_{k=1}^n a_k^* b_k \right) a_j - \left( \sum_{k=1}^n a_k^* a_k \right) b_j \right) \geq 0,$$

czyli

$$\begin{aligned} & \left( \sum_{k=1}^n a_k^* b_k \right)^* \left( \sum_{k=1}^n a_k^* b_k \right) \left( \sum_{j=1}^n a_j^* a_j \right) - \left( \sum_{k=1}^n a_k^* b_k \right)^* \left( \sum_{k=1}^n a_k^* a_k \right) \left( \sum_{j=1}^n a_j^* b_j \right) - \\ & - \left( \sum_{k=1}^n a_k^* a_k \right) \left( \sum_{k=1}^n a_k^* b_k \right) \left( \sum_{j=1}^n a_j^* b_j \right)^* + \left( \sum_{k=1}^n a_k^* a_k \right)^2 \left( \sum_{j=1}^n b_j^* b_j \right) \geq 0. \end{aligned}$$

Ponieważ można tu wskaźnik  $k$  zastąpić wskaźnikiem  $j$ , otrzymujemy po uporządkowaniu

$$(ii) \quad \left( \sum_{j=1}^n a_j^* a_j \right) \left( \sum_{j=1}^n a_j^* a_j \right) \left( \sum_{j=1}^n b_j^* b_j \right) - \left( \sum_{j=1}^n a_j^* b_j \right)^* \left( \sum_{j=1}^n a_j^* b_j \right) \geq 0,$$

wobec czego na mocy (I.131), (I.135) i (I.149) musi zachodzić nierówność (I.160).

Jeżeli w (I.160) zachodzi równość, to zachodzi również w (ii) i w (i), a wobec tego na mocy (I.145) i 1° otrzymujemy dla  $c := \sum_{k=1}^n a_k^* b_k$  i  $d := - \sum_{k=1}^n a_k^* a_k$  spełnienie warunku (I.161).

Jeżeli – odwrotnie – zachodzi równość (I.161) i  $c \neq 0$ , to

$$\begin{aligned} c^* c \left( \sum_{j=1}^n a_j^* b_j \right)^* \left( \sum_{j=1}^n a_j^* b_j \right) &= \left( \sum_{j=1}^n (ca_j)^* b_j \right)^* \left( \sum_{j=1}^n (ca_j)^* b_j \right) = d^* d \left( \sum_{j=1}^n b_j^* b_j \right)^2 = \\ &= \left( \sum_{j=1}^n (ca_j)^* (ca_j) \right) \left( \sum_{j=1}^n b_j^* b_j \right) = c^* c \left( \sum_{j=1}^n a_j^* a_j \right) \left( \sum_{j=1}^n b_j^* b_j \right), \end{aligned}$$

skąd wynika równość we wzorze (I.160). Gdy  $d \neq 0$ , dowód jest analogiczny.

Gdy  $\mathfrak{A}$  jest pierścieniem uporządkowanym, wtedy dla każdego  $a \in \mathfrak{A}$  jest  $a = a^*$ , wobec czego wzór (I.160) przyjmuje postać (I.162). ■

(I.163) DEFINICJA. *Pierwiastkiem kwadratowym* elementu  $a$  dowolnego pierścienia  $\mathcal{A}$  nazywamy każdy taki element (o ile istnieje)  $b \in \mathcal{A}$ , że  $b^2 = a$ . ■

Pierwiastek kwadratowy nie zawsze istnieje. Na przykład, liczba całkowita 2 w pierścieniu liczb całkowitych  $\mathbb{Z}$  nie ma pierwiastka kwadratowego.

(I.164) TWIERDZENIE. *Jeżeli  $\mathcal{A}$  jest pierścieniem całkowitym, w którym  $2 \neq 0$ , to  $\mathcal{A}$ -zero ma dokładnie jeden pierwiastek kwadratowy, a mianowicie  $\mathcal{A}$ -zero, natomiast każdy element  $a \in \mathcal{A}$ ,  $a \neq 0$ , mający pierwiastek kwadratowy  $b \in \mathcal{A}$ , ma ich dokładnie dwa, a mianowicie  $b$  i  $-b$ .*

Dowód. Pierścień  $\mathcal{A}$  z założenia nie ma właściwych dzielników zera. Wobec tego równość  $b^2 = 0$  jest równoważna równości  $b = 0$ . Ponadto pierścień  $\mathcal{A}$  jest z założenia przemienny, wobec czego z równości  $x^2 = b^2 = a \neq 0$  wynika, że  $x^2 - b^2 = (x - b)(x + b) = 0$ , a stąd  $x = b$  albo  $x = -b$ . Gdyby  $b = -b$ , wtedy  $2b = 0$  i  $b = 0$ , skąd  $a = b^2 = 0$ , wbrew założeniu. ■

Twierdzenie (I.164) dotyczy w szczególności pierścieni częściowo uporządkowanych, które z definicji są pierścieniami całkowitymi i dla których na mocy (I.152) jest  $2 > 0$ , a zatem  $2 \neq 0$ .

Symbolem  $\sqrt{a}$  oznaczamy dowolny pierwiastek kwadratowy elementu  $a$  pierścienia  $\mathcal{A}$ , o ile takowy pierwiastek kwadratowy istnieje. Gdy  $\mathcal{A}$  jest pierścieniem częściowo uporządkowanym i  $\sqrt{a} \in \text{re } \mathcal{A}$ , symbolem  $\sqrt{a}$  oznaczamy **wyłącznie** nieujemny pierwiastek kwadratowy elementu  $a$ . Drugim jest wtedy  $-\sqrt{a}$ , niedodatni.

(I.165) DEFINICJA. W dowolnym pierścieniu częściowo uporządkowanym  $\mathcal{A}$  *kwadratową wartością bezwzględną* dowolnego elementu  $a \in \mathcal{A}$  nazywamy element

$$(I.166) \quad |a|^2 := a^* a. \quad \blacksquare$$

(I.167) DEFINICJA. W dowolnym pierścieniu częściowo uporządkowanym  $\mathcal{A}$  wartością bezwzględną dowolnego elementu  $a \in \mathcal{A}$  nazywamy taki element (o ile istnieje)  $|a| \in \text{re } \mathcal{A}$ ,  $|a| \geq 0$ , że

$$(I.168) \quad |a| := \sqrt{a^* a} \quad \mathbf{I}$$

(I.169) DEFINICJA. Pierścień  $\mathcal{A}$  nazywamy pierścieniem z wartością bezwzględną wtedy i tylko wtedy, gdy jest częściowo uporządkowany i dla każdego elementu  $a \in \mathcal{A}$  istnieje wartość bezwzględna (I.168), a pierścieniem z pierwiastkowaniem nazywamy wtedy i tylko wtedy, gdy jest częściowo uporządkowany i dla każdego elementu  $a \in \text{re } \mathcal{A}$ ,  $a \geq 0$ , istnieje  $\sqrt{a} \in \text{re } \mathcal{A}$ .

Jak wynika z powyższej definicji, pierścień z pierwiastkowaniem jest zawsze pierścieniem z wartością bezwzględną.

Jak wynika z tejże definicji, klasa pierścieni częściowo uporządkowanych jest szersza od klasy pierścieni z wartością bezwzględną i tym samym szersza od klasy pierścieni z pierwiastkowaniem. Wprowadzenie pojęcia kwadratowej wartości bezwzględnej (I.166), mającej wiele własności analogicznych do własności wartości bezwzględnej (I.168), pozwala przenieść wiele własności pierścieni z wartością bezwzględną na pierścienie częściowo uporządkowane.

(I.170) TWIERDZENIE. W dowolnym pierścieniu częściowo uporządkowanym  $\mathcal{A}$  dla dowolnych  $a, b \in \mathcal{A}$  i kwadratowej wartości bezwzględnej (I.166) mamy:

$$(I.171) \quad |a|^2 \geq 0,$$

$$(I.172) \quad |a|^2 = 0 \Leftrightarrow a = 0,$$

$$(I.173) \quad a \in \text{re } \mathcal{A} \Rightarrow |a|^2 = a^2,$$

$$(I.174) \quad |a|^2 = |-a|^2 = |\bar{a}|^2 = |a^T|^2 = |a^*|^2,$$

$$(I.175) \quad |ab|^2 = |a|^2 |b|^2,$$

$$(I.176) \quad |a^n|^2 = (|a|^2)^n \quad \text{dla } n \in \mathbb{N}_0,$$

$$(I.177) \quad ||a+b|^2 - |a|^2 - |b|^2| \leq 4|ab|^2.$$

Dowód. Wzór (I.171) wynika z definicji (I.156). Pierścień  $\mathcal{A}$  z założenia nie ma właściwych dzielników zera, wobec czego na mocy (I.166)  $|a|^2 = 0 \Leftrightarrow a = 0 \vee a^* = 0$ . Ale na mocy (I.73) i (I.91)  $a^* = 0 \Leftrightarrow a = (a^*)^* = 0^* = 0$ , wobec czego jest (I.172). Dla  $a \in \text{re } \mathcal{A}$  mamy  $a^* = a$  i na mocy (I.166) wzór (I.173).

Na mocy (I.75), (I.73) i warunku 3° z definicji (I.156) mamy  $a^* a = (a^* a)^* \in \text{re } \mathcal{A}$ , wobec czego na mocy (I.81), (I.64), (I.77), (I.67), (I.78), (I.73):

$$a^* a = (-a^*)(-a) = (-a)^*(-a),$$

$$a^* a = \overline{a^* a} = \overline{a^*} \overline{a} = (\bar{a})^* \bar{a},$$

$$a^* a = a a^* = (a a^*)^T = (a^*)^T a^T = (a^T)^* a^T,$$



$$a^*a = aa^* = (a^*)^*a^*,$$

skąd otrzymujemy wzór (I.174).

Mamy dalej  $|ab|^2 = (ab)^*ab = b^*a^*ab = (a^*a)(b^*b)$  i stąd wzór (I.175). Wzór (I.176), trywialnie prawdziwy dla  $n=0$  i  $n=1$ , dla  $n>1$  otrzymujemy przez indukcję zupełną na mocy (I.175).

Na mocy (I.166) mamy  $|a+b|^2 - |a|^2 - |b|^2 = (a+b)^*(a+b) - a^*a - b^*b = (a^*+b^*) \times (a+b) - a^*a - b^*b = a^*b + b^*a$ , wobec czego wzór (I.177) wynika z (I.160). ■

(I.178) TWIERDZENIE. W dowolnym pierścieniu  $\mathcal{A}$  z wartością bezwzględną (I.168) dla dowolnych  $a, b \in \mathcal{A}$  mamy:

$$(I.179) \quad |a| \geq 0,$$

$$(I.180) \quad |a| = 0 \Leftrightarrow a = 0,$$

$$(I.181) \quad a \in \text{re } \mathcal{A} \wedge a \geq 0 \Rightarrow |a| = a,$$

$$(I.182) \quad a \in \text{re } \mathcal{A} \wedge a \leq 0 \Rightarrow |a| = -a,$$

$$(I.183) \quad ||a|| = |a|,$$

$$(I.184) \quad |a| = |-a| = |\bar{a}| = |a^T| = |a^*|,$$

$$(I.185) \quad |ab| = |a||b|,$$

$$(I.186) \quad |a^n| = |a|^n \quad \text{dla } n \in \mathfrak{N}_0,$$

$$(I.187) \quad ||a| - |b|| \leq |a+b| \leq |a| + |b|.$$

Dowód. Wzór (I.179) wynika z definicji (I.168). Z tejże definicji i twierdzenia (I.164) wynika, że  $a=0 \Rightarrow |a|=0$ . Odwrotnie, jeżeli  $|a|=0$ , to  $|a|^2=0$  i na mocy (I.172)  $a=0$ . Mamy zatem (I.180).

Ze wzoru (I.173) wynika, że  $(|a|-a)(|a|+a)=0$ , skąd  $|a|=a$  albo  $|a|=-a$  i na mocy (I.179) otrzymujemy (I.181) i (I.182). Wzór (I.183) wynika z (I.179) i (I.181). Wzór (I.184) wynika z (I.174).

Ze wzoru (I.175) wynika, że  $(|ab|-|a||b|)(|ab|+|a||b|)=|ab|^2-|a|^2|b|^2=0$ , skąd  $|ab|=|a||b|$  albo  $|ab|=-|a||b|$ . Jeżeli  $|ab|=-|a||b|$ , to na mocy (I.179) i (I.135) jest  $-|a||b| \geq 0$  i  $|a||b| \geq 0$ , czyli  $|a||b| \leq 0$  i  $|a||b| \geq 0$ , skąd na mocy (I.132)  $|a||b|=0$ . Wobec tego  $|a|=0 \vee |b|=0$  i  $|ab|=-|a||b| \Rightarrow |ab|=|a||b|$ . Wynika z powyższego prawdziwość wzoru (I.185).

Wzór (I.186), trywialnie prawdziwy dla  $n=0$  i  $n=1$ , otrzymujemy dla  $n>1$  przez indukcję zupełną na mocy wzoru (I.185).

Ze wzoru (I.177) wynika, że

$$(2|ab| - ||a+b|^2 - |a|^2 - |b|^2|)(2|ab| + ||a+b|^2 - |a|^2 - |b|^2|) \geq 0.$$

Ponieważ na mocy (I.179)  $2|ab| + ||a+b|^2 - |a|^2 - |b|^2| \geq 0$ , więc

$$2|ab| - ||a+b|^2 - |a|^2 - |b|^2| \geq 0, \quad \text{czyli} \quad ||a+b|^2 - |a|^2 - |b|^2| \leq 2|ab|.$$

Zarówno, gdy  $|a+b|^2 - |a|^2 - |b|^2 \geq 0$ , jak i gdy  $|a+b|^2 - |a|^2 - |b|^2 \leq 0$ , na mocy (I.181) i (I.182) otrzymujemy stąd

$$(|a| - |b|)^2 \leq |a+b|^2 \leq (|a| + |b|)^2,$$

czyli

$$(|a| - |b| + ||a| - |b||)(|a+b| - ||a| - |b||) \geq 0,$$

$$(|a| - |b| + |a+b|)(|a| + |b| - |a+b|) \geq 0.$$

Z uwagi na to, że  $|a+b| + ||a| - |b|| \geq 0$  i  $|a| + |b| + |a+b| \geq 0$ , otrzymujemy stąd wzór (I.187). ■

(I.188) TWIERDZENIE. *Każdy pierścień uporządkowany  $\mathcal{A}$  jest pierścieniem z wartością bezwzględną określoną dla dowolnego  $a \in \mathcal{A}$  wzorem:*

$$(I.189) \quad |a| := \begin{cases} a & \text{dla } a \geq 0, \\ -a & \text{dla } a \leq 0. \end{cases}$$

Dowód. Z definicji re  $\mathcal{A} = \mathcal{A}$  i (I.189) wynika ze wzorów (I.173) i (I.168). ■

(I.190) PRZYKŁAD. Pierścień liczb całkowitych  $\mathcal{Z}$  ze zwykłą nierównością i wartością bezwzględną (I.189) jest pierścieniem z wartością bezwzględną, ale nie jest pierścieniem z pierwiastkowaniem. ■

(I.191) PRZYKŁAD. Pierścień z przykładu (I.157) jest częściowo uporządkowany. Na mocy definicji (I.166) kwadratowa wartość bezwzględna jest w nim określona wzorem

$$|(a, b)|^2 = (a^2 + b^2, 0) \quad \text{dla } a, b \in \mathcal{Z}.$$

Nie jest to pierścień z wartością bezwzględną, ponieważ, na przykład,

$$|(1, 1)|^2 = (2, 0)$$

i nie ma takiej liczby całkowitej  $n$ , aby  $(n, 0)^2 = (2, 0)$ . ■

## § I.6. Pierścienie nad pierścieniami

(I.192) DEFINICJA. *Pierścieniem nad pierścieniem z jedyneką  $\mathcal{A}$  nazywamy każdy pierścień z jedyneką  $\mathcal{X}$ , dla którego zostało określone lewostronne i prawostronne mnożenie przez elementy z  $\mathcal{A}$ , przyporządkowujące każdemu elementowi  $x \in \mathcal{X}$  i każdemu elementowi  $a \in \mathcal{A}$  elementy  $ax, xa \in \mathcal{X}$  ze spełnieniem dla dowolnych  $x, y \in \mathcal{X}$ ,  $a, b \in \mathcal{A}$  następujących warunków, w których  $o$  jest  $\mathcal{X}$ -zerem,  $e$  —  $\mathcal{X}$ -jedyneką,  $0$  —  $\mathcal{A}$ -zerem, a  $1$  —  $\mathcal{A}$ -jedyneką:*

$$(I.193) \quad a(bx) = (ab)x,$$

$$(I.194) \quad a(xy) = (ax)y,$$

$$(I.195) \quad (xa)b = x(ab),$$

$$(I.196) \quad (xy)a = x(ya),$$

$$(I.197) \quad (ax)b = a(xb),$$

$$(I.198) \quad (xa)y = x(ay),$$

$$(I.199) \quad a(x+y) = ax + ay,$$

$$(I.200) \quad (a+b)x = ax + bx,$$

$$(I.201) \quad (x+y)a = xa + ya,$$

$$(I.202) \quad x(a+b) = xa + xb,$$

$$(I.203) \quad 1x = x1 = x,$$

$$(I.204) \quad ae = o \vee ea = o \Rightarrow a = o.$$

Gdy  $\mathcal{A}$  i  $\mathcal{X}$  są pierścieniami z transpozycją, żądamy dodatkowo, aby

$$(I.205) \quad \overline{ax} = \overline{a}\overline{x},$$

$$(I.206) \quad \overline{xa} = \overline{x}\overline{a},$$

$$(I.207) \quad (ax)^T = x^T a^T,$$

$$(I.208) \quad (xa)^T = a^T x^T. \quad \blacksquare$$

(I.209) TWIERDZENIE. W pierścieniu (I.192) dla wszystkich  $a \in \mathcal{A}$  i  $x \in \mathcal{X}$  jest:

$$(I.210) \quad ao = oa = o,$$

$$(I.211) \quad 0x = x0 = o,$$

$$(I.212) \quad ae = ea,$$

$$(I.213) \quad (ax)^* = x^* a^* \quad \left. \begin{array}{l} (I.214) \quad (xa)^* = a^* x^* \end{array} \right\} \text{ dla pierścieni } \mathcal{A} \text{ i } \mathcal{X} \text{ z transpozycją,}$$

$$(I.215) \quad nx = xn \quad \text{dla każdej } \mathcal{A}\text{-liczby całkowitej } n,$$

$$(I.216) \quad a\eta = \eta a \quad \text{dla każdej } \mathcal{X}\text{-liczby całkowitej } \eta.$$

Dowód. Mamy  $ax + ao = a(x + o) = ax$ , skąd  $ao = o$ . Analogicznie dowodzimy, że  $oa = o$ . Otrzymujemy wzór (I.210). Wzór (I.211) dowodzimy analogicznie. Mamy dalej  $ae = e(ae) = (ea)e = ea$ , czyli wzór (I.212). Wzory (I.213) i (I.214) wynikają z (I.205), ..., (I.208). Wzór (I.215) dowodzimy indukcyjnie na mocy wzorów (I.203) oraz (I.200) i (I.202), a wzór (I.216) dowodzimy analogicznie ze wzoru (I.212).  $\blacksquare$

(I.217) TWIERDZENIE. Jeżeli pierścień  $\mathcal{X}$  nad pierścieniem z jedynką  $\mathcal{A}$  jest przemienny, to pierścień  $\mathcal{A}$  też jest przemienny.

Dowód. Dla dowolnych  $a, b \in \mathcal{A}$  mamy

$$(ab)e = a(be) = a(ebe) = (ae)(be),$$

$$(ba)e = b(ae) = b(eae) = (be)(ae) = (ae)(be),$$

skąd  $(ab - ba)e = o$  i na mocy (I.204)  $ab = ba$ .  $\blacksquare$

(I.218) TWIERDZENIE. Jeżeli w pierścieniu  $\mathcal{X}$  nad pierścieniem z jedyneką  $\mathcal{A}$  dla każdego  $a \in \mathcal{A}$  i  $x \in \mathcal{X}$  jest

$$(I.219) \quad ax = xa,$$

to pierścień  $\mathcal{A}$  jest przemienny.

Dowód. Dla dowolnych  $a, b \in \mathcal{A}$  mamy na mocy (I.219)

$$(ab)e = e(ab),$$

$$(ba)e = b(ae) = (ae)b = (ea)b = e(ab),$$

skąd  $(ab - ba)e = 0$  i na mocy (I.204)  $ab = ba$ . ■

(I.220) TWIERDZENIE. Jeżeli pierścień  $\mathcal{X}$  nad pierścieniem z jedyneką  $\mathcal{A}$  jest całkowity, to  $\mathcal{A}$  jest również pierścieniem całkowitym.

Dowód. Jeżeli pierścień  $\mathcal{X}$  jest całkowity, to jest przemienny i na mocy twierdzenia (I.217) pierścień  $\mathcal{A}$  jest też przemienny.

Jeżeli  $\mathcal{X}$  jest pierścieniem całkowitym, to nie zawiera właściwych dzielników zera. Gdyby pierścień  $\mathcal{A}$  takie dzielniki zawierał, istniałyby elementy  $a, b \in \mathcal{A}$ , takie że  $a \neq 0 \wedge b \neq 0 \wedge ab = 0$ . Ponieważ byłoby wtedy na mocy (I.211)

$$(ab)e = a(be) = a(ebe) = (ae)(be) = 0,$$

wiec istniałby element  $c \in \mathcal{A}$  ( $c = a$  albo  $c = b$ ), taki że  $c \neq 0 \wedge ce = 0$  wbrew (I.204). Wynika stąd, że pierścień  $\mathcal{A}$  nie ma właściwych dzielników zera i wobec powyższego jest całkowity. ■

Pierścienie nad pierścieniami stanowią przypadek szczególny tzw. modułów, którym będzie poświęcony rozdział IV. Wobec tego do pierścieni nad pierścieniami będą się odnosić własności modułów, które udowodnimy w rozdziale IV.

## § I.7. Ciała

(I.221) DEFINICJA. Ciałem nazywamy każdy przemienny pierścień z jedyneką, w którym każdy element niezerowy ma odwrotność. ■

(I.222) TWIERDZENIE. Każde ciało jest pierścieniem całkowitym.

Dowód. Z definicji każde ciało jest pierścieniem przemiennym. Wobec tego teza wynika z twierdzenia (I.120). ■

(I.223) DEFINICJA. Ciałem liczb wymiernych nazywamy pierścień z jedyneką

$$\mathcal{Q} := (\mathbb{Q}, +, \cdot, -, 0, 1),$$

gdzie  $\mathbb{Q}$  jest zbiorem wszystkich liczb wymiernych, a  $+$ ,  $\cdot$ ,  $-$  jest odpowiednio zwykłym ich dodawaniem, zwykłym mnożeniem i zwykłą zmianą znaku. W niektórych przypadkach

będziemy traktować ciało liczb wymiernych jako pierścień z transpozycją

$$\mathcal{Q} := (\mathcal{Q}, +, \cdot, -, s, t, 0, 1)$$

z trywialnym sprzężeniem  $s$  i trywialną transpozycją  $t$ , określonymi dla dowolnego  $a \in \mathcal{Q}$  wzorami:  $\bar{a} := a$  i  $a^T := a$ . ■

(I.224) DEFINICJA. *Ciałem liczb rzeczywistych* nazywamy pierścień z jedyneką

$$\mathcal{R} := (\mathcal{R}, +, \cdot, -, s, t, 0, 1),$$

gdzie  $\mathcal{R}$  jest zbiorem wszystkich liczb rzeczywistych, a  $+$ ,  $\cdot$ ,  $-$  jest odpowiednio zwykłym ich dodawaniem, zwykłym mnożeniem i zwykłą zmianą znaku. W niektórych przypadkach będziemy traktować ciało liczb rzeczywistych jako pierścień z transpozycją

$$\mathcal{R} := (\mathcal{R}, +, \cdot, -, s, t, 0, 1)$$

z trywialnym sprzężeniem  $s$  i trywialną transpozycją  $t$ , określonymi dla dowolnego  $a \in \mathcal{R}$  wzorami:  $\bar{a} := a$  i  $a^T := a$ . ■

Definicje (I.223) i (I.224) są oparte na oczywistym fakcie, że każda niezerowa liczba rzeczywista (a w szczególności każda niezerowa liczba wymierna)  $a$  ma odwrotność  $1/a$ .

(I.225) TWIERDZENIE. *W każdym ciele  $\mathcal{F}$  dla każdej pary elementów  $a, b \in \mathcal{F}$  takiej, że  $a \neq 0$ , istnieje dokładnie jeden taki element  $x \in \mathcal{F}$ , że  $ax = b$ .*

Dowód. Niech  $x := a^{-1}b$ . Wtedy  $ax = aa^{-1}b = b$ . Gdyby były dwa takie elementy  $x$  i  $y$ , że  $ax = b$  i  $ay = b$ , wtedy byłoby  $ax - ay = a(x - y) = 0$ . Ponieważ ciało  $\mathcal{F}$  nie zawiera właściwych dzielników zera, mamy stąd  $x - y = 0$ , czyli  $x = y$ . ■

Taki element  $x$ , że  $ax = b$ , gdzie  $a \neq 0$ , nazywamy *ilorazem* elementu  $b$  przez element  $a$  i oznaczamy symbolem  $b/a$ . Działanie przyporządkowujące elementom  $b$  i  $a \neq 0$  element  $b/a$  nazywamy *dzieleniem*. W szczególności  $1/a$  oznacza odwrotność elementu  $a \neq 0$ .

(I.226) TWIERDZENIE. *W każdym ciele  $\mathcal{F}$  dla dowolnych elementów  $a, b, c, d \in \mathcal{F}$  jest:*

$$(I.227) \quad a \cdot \frac{b}{a} = b \quad \text{dla} \quad a \neq 0,$$

$$(I.228) \quad \frac{b}{1} = b,$$

$$(I.229) \quad \frac{b}{a} = b \cdot \frac{1}{a} \quad \text{dla} \quad a \neq 0,$$

$$(I.230) \quad \frac{b}{a} = \frac{bc}{ac} \quad \text{dla} \quad a \neq 0 \wedge c \neq 0,$$

$$(I.231) \quad \frac{b}{a} + \frac{c}{a} = \frac{b+c}{a} \quad \text{dla} \quad a \neq 0,$$

$$(I.232) \quad \frac{b}{a} + \frac{d}{c} = \frac{bc+ad}{ac} \quad \text{dla} \quad a \neq 0 \wedge c \neq 0,$$

$$(I.233) \quad \frac{b}{a} = \frac{d}{c} \Leftrightarrow ad = bc \quad \text{dla} \quad a \neq 0 \wedge c \neq 0,$$

$$(I.234) \quad -\frac{b}{a} = \frac{-b}{a} = \frac{b}{-a} \quad \text{dla} \quad a \neq 0,$$

$$(I.235) \quad \frac{b}{a} - \frac{d}{c} = \frac{bc - ad}{ac} \quad \text{dla} \quad a \neq 0 \wedge c \neq 0,$$

$$(I.236) \quad \frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac} \quad \text{dla} \quad a \neq 0 \wedge c \neq 0,$$

$$(I.237) \quad \frac{0}{a} = 0 \quad \text{dla} \quad a \neq 0,$$

$$(I.238) \quad \frac{\frac{b}{a}}{\frac{d}{c}} = \frac{bc}{ad} \quad \text{dla} \quad a \neq 0 \wedge c \neq 0 \wedge d \neq 0.$$

Gdy  $\mathcal{F}$  jest pierścieniem z transpozycją, mamy

$$(I.239) \quad \overline{\left(\frac{b}{a}\right)} = \frac{\bar{b}}{\bar{a}} \quad \text{dla} \quad a \neq 0,$$

$$(I.240) \quad \left(\frac{b}{a}\right)^T = \frac{b^T}{a^T} \quad \text{dla} \quad a \neq 0,$$

$$(I.241) \quad \left(\frac{b}{a}\right)^* = \frac{b^*}{a^*} \quad \text{dla} \quad a \neq 0.$$

Gdy  $\mathcal{F}$  jest pierścieniem częściowo uporządkowanym i  $a, b \in \text{re } \mathcal{F}$ , wtedy

$$(I.242) \quad a > 0 \Rightarrow \frac{1}{a} > 0,$$

$$(I.243) \quad a < 0 \Rightarrow \frac{1}{a} < 0,$$

$$(I.244) \quad 0 < a < b \Rightarrow \frac{1}{a} > \frac{1}{b} > 0,$$

$$(I.245) \quad \left|\frac{b}{a}\right|^2 = \frac{|b|^2}{|a|^2} \quad \text{dla} \quad a \neq 0.$$

Gdy  $\mathcal{F}$  jest pierścieniem z wartością bezwzględną i  $a, b \in \mathcal{F}$ , wtedy

$$(I.246) \quad \left|\frac{b}{a}\right| = \frac{|b|}{|a|} \quad \text{dla} \quad a \neq 0.$$

Dowód. Wzór (I.227) wynika z określenia symbolu  $\frac{b}{a}$ . Z tegoż określenia wynika, że  $1 \cdot \frac{b}{1} = b$ , skąd wzór (I.228). Mamy dalej  $a \left( b \frac{1}{a} \right) = a \frac{1}{a} b = b$ , skąd na mocy (I.227) i twierdzenia (I.225) wynika wzór (I.229).

Ponieważ na mocy (I.227)

$$ac \cdot \left( \frac{b}{a} \right) = c \left( a \cdot \frac{b}{a} \right) = cb = bc, \quad ac \cdot \frac{bc}{ac} = bc,$$

więc na mocy twierdzenia (I.225) otrzymujemy (I.230). Analogicznie dowodzimy (I.231) i (I.232). Dla  $a \neq 0 \wedge c \neq 0$  mamy na mocy (I.230)

$$\frac{b}{a} = \frac{d}{c} \Leftrightarrow \frac{bc}{ac} = \frac{ad}{ac} \Leftrightarrow bc = ad,$$

czyli wzór (I.233). Wzory (I.234), ..., (I.238) dowodzimy analogicznie, jak (I.230). Dalej

$$\overline{a \left( \frac{b}{a} \right)} = \overline{a \cdot \frac{b}{a}} = \overline{b}, \quad \overline{a} \cdot \frac{\overline{b}}{\overline{a}} = \overline{b},$$

skąd na mocy twierdzenia (I.225) wzór (I.239). Wzory (I.240) i (I.241) dowodzimy analogicznie.

Na mocy (I.239), (I.240), (I.241) i (I.92)  $a \in \text{re } \mathcal{F} \Rightarrow \frac{1}{a} \in \text{re } \mathcal{F}$ . Wobec tego na mocy (I.138) jest  $\frac{1}{a} < 0$  albo  $\frac{1}{a} > 0$  i wzory (I.242), (I.243) wynikają z (I.148) i (I.150). Jeżeli  $0 < a < b$ , to na mocy (I.148)  $ab > 0$ , na mocy (I.242)  $\frac{1}{ab} > 0$  i na mocy (I.148)  $\frac{1}{ab} \cdot 0 < \frac{1}{ab} \cdot a < \frac{1}{ab} \cdot b$ , czyli wzór (I.244).

Na mocy (I.166), (I.241) i (I.236) jest

$$\left| \frac{b}{a} \right|^2 = \left( \frac{b}{a} \right)^* \cdot \frac{b}{a} = \frac{b^*}{a^*} \cdot \frac{b}{a} = \frac{b^* b}{a^* a} = \frac{|b|^2}{|a|^2},$$

czyli wzór (I.245). Wzór (I.246) wynika na mocy twierdzenia (I.225) i wzoru (I.185) z faktu, że

$$\left| a \right| \left| \frac{b}{a} \right| = \left| a \cdot \frac{b}{a} \right| = |b| \quad \text{oraz} \quad \left| a \right| \cdot \frac{|b|}{|a|} = |b|. \quad \blacksquare$$

W każdym ciele  $\mathcal{F}$  wprowadza się *potęgowanie* z dowolnym wykładnikiem całkowitym  $m$ , przyjmując dla dowolnego elementu  $a \neq 0$  i dowolnego  $n \in \mathfrak{N}$

$$(I.247) \quad a^{-n} := \frac{1}{a^n}.$$

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  $(a, b)$ ,