

Algebra

Rozdział I

Pierścienie

§ I.1. Półgrupy i grupy

(I.1) DEFINICJA. *Półgrupą* nazywamy algebrę

$$(i) \quad \mathcal{S} := (\mathfrak{S}, \circ),$$

gdzie \mathfrak{S} jest zbiorem niepustym, a \circ operacją (działaniem) dwuargumentową, spełniającą dla dowolnych $a, b, c \in \mathfrak{S}$ warunek

$$(I.2) \quad (a \circ b) \circ c = a \circ (b \circ c). \quad \blacksquare$$

(I.3) DEFINICJA. *Elementem jedyńkowym półgrupy* (i) nazywamy taki (o ile istnieje) element $e \in \mathfrak{S}$, że dla dowolnego $a \in \mathfrak{S}$ jest

$$(I.4) \quad e \circ a = a \circ e = a. \quad \blacksquare$$

(I.5) DEFINICJA. *Elementem zerowym półgrupy* (i), w której \mathfrak{S} jest zbiorem zawierającym co najmniej 2 elementy, nazywamy taki (o ile istnieje) element $o \in \mathfrak{S}$, że dla dowolnego $a \in \mathfrak{S}$ jest

$$(I.6) \quad o \circ a = a \circ o = o. \quad \blacksquare$$

Półgrupę z elementem jedyńkowym, półgrupę z elementem zerowym oraz półgrupę z elementem jedyńkowym i z elementem zerowym można traktować jako algebry odpowiednio

$$(\mathfrak{S}, \circ, e), \quad (\mathfrak{S}, \circ, o); \quad (\mathfrak{S}, \circ, o, e),$$

gdzie e i o są operacjami zeroargumentowymi, czyli elementami wyróżnionymi ze zbioru \mathfrak{S} .

(I.7) PRZYKŁAD. Zbiór liczb całkowitych \mathbb{Z} ze zwykłym mnożeniem \cdot tworzy półgrupę z elementem jedyńkowym i z elementem zerowym $(\mathbb{Z}, \cdot, 0, 1)$. \blacksquare

(I.8) PRZYKŁAD. Zbiór liczb naturalnych \mathbb{N} ze zwykłym mnożeniem \cdot tworzy półgrupę z elementem jedyńkowym $(\mathbb{N}, \cdot, 1)$, która nie zawiera elementu zerowego. Zbiór liczb

całkowitych parzystych 3_p ze zwykłym mnożeniem \cdot tworzy półgrupę z elementem zerowym $(3_p, \cdot, 0)$, która nie zawiera elementu jedynekowego. ■

(I.9) PRZYKŁAD. Zbiór liczb naturalnych \mathbb{N} ze zwykłym dodawaniem $+$ tworzy półgrupę $(\mathbb{N}, +)$, która nie zawiera ani elementu jedynekowego, ani zerowego. ■

(I.10) TWIERDZENIE. *Półgrupa ma co najwyżej jeden element jedynekowy.*

Dowód. Załóżmy, że półgrupa (i) ma element jedynekowy e spełniający warunek (I.4) oraz element jedynekowy e_1 spełniający dla każdego $a \in \mathfrak{S}$ warunek

$$(ii) \quad e_1 \circ a = a \circ e_1 = a.$$

Na mocy (I.4) jest $e_1 = e_1 \circ e$, na mocy (ii) $e_1 \circ e = e$, wobec czego $e_1 = e$. ■

(I.11) TWIERDZENIE. *Półgrupa ma co najwyżej jeden element zerowy.*

Dowód. Załóżmy, że półgrupa (i) ma element zerowy o spełniający warunek (I.6) oraz element zerowy o_1 spełniający dla każdego $a \in \mathfrak{S}$ warunek $o_1 \circ a = a \circ o_1 = o_1$. Z tego ostatniego wynika w szczególności, że $o_1 = o_1 \circ o$, a na mocy (I.6) jest $o_1 \circ o = o$, wobec czego $o_1 = o$. ■

(I.12) TWIERDZENIE. *Jeżeli półgrupa ma element jedynekowy e i element zerowy o , to $e \neq o$.*

Dowód. Gdyby $e = o$, wtedy na mocy (I.4) dla każdego $a \in \mathfrak{S}$ byłoby $a = e \circ a = o \circ a$, skąd na mocy (I.6) $a = o$, co byłoby sprzeczne z założeniem uczynionym w definicji (I.5), że zbiór \mathfrak{S} zawiera co najmniej 2 elementy. ■

(I.13) DEFINICJA. Grupę nazywamy algebrą

$$(iii) \quad \mathcal{G} := (\mathfrak{G}, \circ, ^{-1}, e),$$

gdzie \mathfrak{G} jest zbiorem niepustym, \circ — operacją (działaniem) dwuargumentową, $^{-1}$ — operacją jednoargumentową, e — operacją zeroargumentową, czyli elementem wyróżnionym ze zbioru \mathfrak{G} i dla dowolnych $a, b, c \in \mathfrak{G}$ są spełnione następujące warunki:

$$(I.14) \quad (a \circ b) \circ c = a \circ (b \circ c),$$

$$(I.15) \quad e \circ a = a,$$

$$(I.16) \quad a^{-1} \circ a = e. \quad \blacksquare$$

(I.17) PRZYKŁAD. Zbiór niezerowych liczb rzeczywistych $\mathbb{R} - \{0\}$ ze zwykłym mnożeniem i odwrotnością $a^{-1} := 1/a$ tworzy grupę $(\mathbb{R} - \{0\}, \cdot, ^{-1}, 1)$. ■

(I.18) PRZYKŁAD. Zbiór liczb całkowitych \mathbb{Z} ze zwykłym dodawaniem i $a^{-1} := -a$ tworzy grupę $(\mathbb{Z}, +, -, 0)$. ■

(I.19) TWIERDZENIE. *Dla grupy (iii) i dowolnych $a, b, c \in \mathfrak{G}$*

$$a \circ b = a \circ c \Rightarrow b = c.$$

Dowód. Jeżeli $a \circ b = a \circ c$, to $a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c)$, czyli na mocy (I.14) $(a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c$, skąd na mocy (I.16) $e \circ b = e \circ c$ i na mocy (I.15) $b = c$. ■

(I.20) TWIERDZENIE. Dla grupy (iii) i dowolnego $a \in \mathfrak{G}$ jest

$$a \circ e = a.$$

Dowód. Na mocy (I.14), (I.15) i (I.16) mamy

$$a^{-1} \circ (a \circ e) = (a^{-1} \circ a) \circ e = e \circ e = e = a^{-1} \circ a,$$

skąd na mocy twierdzenia poprzedniego wynika teza. ■

(I.21) TWIERDZENIE. Dla grupy (iii) algebra (\mathfrak{G}, \circ, e) jest półgrupą z elementem jedykno-
wyni.

Dowód wynika z definicji i twierdzenia poprzedniego. ■

(I.22) TWIERDZENIE. Grupa nie zawiera elementu zerowego.

Dowód. Gdyby dla grupy (iii) istniał element zerowy $o \in \mathfrak{G}$ spełniający warunek (I.6), wtedy na mocy (I.16) istniałby element $o^{-1} \in \mathfrak{G}$ taki, że $o^{-1} \circ o = e$, a na mocy (I.6) byłoby $o^{-1} \circ o = o$, wobec czego mielibyśmy $e = o$ wbrew twierdzeniu (I.12). ■

(I.23) TWIERDZENIE. Dla grupy (iii) i dowolnego $a \in \mathfrak{G}$ jest

$$a \circ a^{-1} = e.$$

Dowód. Na mocy (I.14), (I.15), (I.16) oraz twierdzenia (I.20) mamy

$$a^{-1} \circ (a \circ a^{-1}) = (a^{-1} \circ a) \circ a^{-1} = e \circ a^{-1} = a^{-1} = a^{-1} \circ e,$$

skąd na mocy twierdzenia (I.19) wynika teza. ■

(I.24) TWIERDZENIE. Dla grupy (iii) i dowolnego $a \in \mathfrak{G}$ istnieje dokładnie jeden element $x \in \mathfrak{G}$ spełniający warunek

$$x \circ a = e.$$

Dowód. Istnienie elementu x spełniającego powyższy warunek wynika z (I.16). Gdyby dla jakiegoś $x \in \mathfrak{G}$ ten warunek był spełniony, wtedy na mocy twierdzeń (I.20) i (I.23) byłoby $x = x \circ e = x \circ (a \circ a^{-1}) = (x \circ a) \circ a^{-1} = e \circ a^{-1} = a^{-1}$. ■

(I.25) DEFINICJA. W grupie (iii) element a^{-1} spełniający warunek (I.16) nazywamy od-
wrotnością elementu a . ■

(I.26) TWIERDZENIE. Dla grupy (iii) i dowolnych $a, b \in \mathfrak{G}$ istnieją takie elementy $x, y \in \mathfrak{G}$,
że

$$(iv) \quad x \circ a = b, \quad a \circ y = b$$

Dowód. Niech

$$(v) \quad x := b \circ a^{-1}, \quad y := a^{-1} \circ b.$$

Wtedy $x \circ a = (b \circ a^{-1}) \circ a = b \circ (a^{-1} \circ a) = b \circ e = b$ oraz $a \circ y = a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$, czyli są spełnione warunki (iv). ■

(I.27) TWIERDZENIE. Dla grupy (iii) i danych $a, b \in \mathfrak{G}$ elementy (v) są jedynymi elementami spełniającymi odpowiednio warunki (iv).

Dowód. Jeżeli elementy $x, y \in \mathfrak{G}$ spełniają odpowiednio warunki (iv), to

$$(x \circ a) \circ a^{-1} = b \circ a^{-1}, \quad a^{-1} \circ (a \circ y) = a^{-1} \circ b,$$

czyli

$$x \circ (a \circ a^{-1}) = x \circ e = x = b \circ a^{-1}, \quad (a^{-1} \circ a) \circ y = e \circ y = y = a^{-1} \circ b. \quad \blacksquare$$

(I.28) DEFINICJA. Półgrupę (i), dla której dla dowolnych $a, b \in \mathfrak{S}$ jest

$$(I.29) \quad a \circ b = b \circ a$$

nazywamy *półgrupą przemenną* albo *półgrupą abelową*. \blacksquare

(I.30) PRZYKŁAD. Półgrupy z przykładów (I.7), (I.8), (I.9) są wszystkie półgrupami przemennymi. \blacksquare

(I.31) DEFINICJA. Grupę (iii), dla której dla dowolnych $a, b \in \mathfrak{G}$ jest spełniony warunek (I.29), nazywamy *grupą przemenną* albo *grupą abelową*. \blacksquare

(I.32) PRZYKŁAD. Grupy z przykładów (I.17) i (I.18) są obie grupami przemennymi. \blacksquare

Przykłady półgrup i grup nie przemennych poznamy w dalszych rozdziałach.

(I.33) DEFINICJA. Podgrupą grupy (iii) nazywamy każdą podalgebrę grupy (iii), tzn. każdą taką grupę $\mathfrak{G}_1 := (\mathfrak{G}_1, \circ, ^{-1}, e)$, że $\mathfrak{G}_1 \subset \mathfrak{G}$ i zbiór \mathfrak{G}_1 jest zamknięty ze względu na operację \circ , $^{-1}$, e , czyli

$$\mathfrak{G}_1 \circ \mathfrak{G}_1 \subset \mathfrak{G}_1, \quad \mathfrak{G}_1^{-1} \subset \mathfrak{G}_1, \quad e \in \mathfrak{G}_1.$$

Podpółgrupą półgrupy (i) (półgrupy (\mathfrak{S}, \circ, e) , półgrupy (\mathfrak{S}, \circ, o) , półgrupy $(\mathfrak{S}, \circ, o, e)$) nazywamy każdą podalgebrę półgrupy (i) (półgrupy (\mathfrak{S}, \circ, e) , półgrupy (\mathfrak{S}, \circ, o) , półgrupy $(\mathfrak{S}, \circ, o, e)$), tzn. każdą taką półgrupę $\mathcal{P}_1 := (\mathfrak{S}_1, \circ)$ (półgrupę $(\mathfrak{S}_1, \circ, e)$, półgrupę $(\mathfrak{S}_1, \circ, o)$, półgrupę $(\mathfrak{S}_1, \circ, o, e)$), że $\mathfrak{S}_1 \subset \mathfrak{S}$ i zbiór \mathfrak{S}_1 jest zamknięty ze względu na operację \circ (operacje \circ, e , operacje \circ, o , operacje \circ, e, o), czyli odpowiednio

$$\mathfrak{S}_1 \circ \mathfrak{S}_1 \subset \mathfrak{S}_1, \quad e \in \mathfrak{S}_1, \quad o \in \mathfrak{S}_1. \quad \blacksquare$$

(I.34) PRZYKŁAD. Zbiór niezerowych liczb wymiernych $\mathfrak{Q}_0 := \mathfrak{Q} - \{0\}$ tworzy podgrupę $(\mathfrak{Q}_0, \cdot, ^{-1}, 1)$ grupy z przykładu (I.17), ponieważ

$$\mathfrak{Q}_0 \subset \mathfrak{R} - \{0\}, \quad \mathfrak{Q}_0 \cdot \mathfrak{Q}_0 = \mathfrak{Q}_0, \quad \mathfrak{Q}_0^{-1} = \mathfrak{Q}_0, \quad 1 \in \mathfrak{Q}_0. \quad \blacksquare$$

(I.35) DEFINICJA. Grupy

$$\mathcal{G}_1 := (\mathfrak{G}_1, \circ, ^{-1}, e_1), \quad \mathcal{G}_2 := (\mathfrak{G}_2, (\circ), ^{(-1)}, e_2)$$

nazywamy *izomorficznymi* wtedy i tylko wtedy, gdy są algebrami izomorficznymi, tzn. istnieje takie różnowartościowe przekształcenie f zbioru \mathfrak{G}_1 na \mathfrak{G}_2 , które zachowuje operacje \circ , $^{-1}$, e_1 , czyli dla dowolnych $a, b \in \mathfrak{G}_1$ jest

$$f(a \circ b) = f(a) (\circ) f(b), \quad f(a^{-1}) = (f(a))^{(-1)}, \quad f(e_1) = e_2.$$

Analogicznie definiujemy izomorfizm półgrup, półgrup z elementem jedynkowym, półgrup z elementem zerowym, półgrup z elementem jedynkowym i z elementem zerowym. ■

(I.36) PRZYKŁAD. Rozpatrzmy grupę z przykładu (I.18) oraz grupę $(\mathbb{Z}_p, +, -, 0)$, gdzie \mathbb{Z}_p jest zbiorem wszystkich liczb całkowitych parzystych. Druga z tych grup jest podgrupą pierwszej. Ponadto grupy te są izomorficzne, ponieważ istnieje różnowartościowe przekształcenie f zbioru \mathbb{Z} na \mathbb{Z}_p określone wzorem $f(x) = 2x$, zachowujące operacje $+$, $-$, 0 , czyli dla dowolnych $a, b \in \mathbb{Z}$ jest

$$f(a+b) = f(a) + f(b), \quad f(-a) = -f(a), \quad f(0) = 0. \quad \blacksquare$$

§ I.2. Pierścienie

(I.37) DEFINICJA. *Pierścieniem* nazywamy algebrę

$$(I.38) \quad \mathcal{A} := (\mathfrak{A}, +, \cdot, -, 0),$$

gdzie \mathfrak{A} jest zbiorem zawierającym co najmniej dwa elementy, $+$ i \cdot są operacjami (działaniami) dwuargumentowymi, które umownie nazywamy dodawaniem i mnożeniem i oznaczamy podobnie jak dodawanie i mnożenie liczb rzeczywistych, $-$ jest operacją jednoargumentową, 0 — operacją zeroargumentową, czyli elementem wyróżnionym ze zbioru \mathfrak{A} i dla dowolnych $a, b, c \in \mathfrak{A}$ są spełnione następujące warunki:

$$(I.39) \quad a + b = b + a,$$

$$(I.40) \quad (a + b) + c = a + (b + c),$$

$$(I.41) \quad 0 + a = a,$$

$$(I.42) \quad -a + a = 0,$$

$$(I.43) \quad (ab)c = a(bc),$$

$$(I.44) \quad a(b + c) = ab + ac,$$

$$(I.45) \quad (a + b)c = ac + bc. \quad \blacksquare$$

(I.46) TWIERDZENIE. W pierścieniu (I.38) dla dowolnego $a \in \mathfrak{A}$ jest

$$(I.47) \quad 0 \cdot a = a \cdot 0 = 0.$$

Dowód. Na mocy (I.44) i (I.45) dla dowolnych $a, c \in \mathfrak{A}$

$$ca + 0 \cdot a = (c + 0)a, \quad ac + a \cdot 0 = a(c + 0),$$

skąd na mocy (I.39) i (I.41)

$$ca + 0 \cdot a = ca, \quad ac + a \cdot 0 = ac,$$

czyli

$$-ca + ca + 0 \cdot a = -ca + ca, \quad -ac + ac + a \cdot 0 = -ac + ac$$

i na mocy (I.42)

$$0 + 0 \cdot a = 0, \quad 0 + a \cdot 0 = 0,$$

skąd na mocy (I.41) otrzymujemy (I.47). ■

(I.48) DEFINICJA. \mathcal{A} -zerem albo po prostu zerem w pierścieniu (I.38) nazywamy element wyróżniony 0, spełniający warunki (I.41), (I.42) i (I.47). ■

(I.49) DEFINICJA. \mathcal{A} -jedyneką albo po prostu jedynką w pierścieniu (I.38) nazywamy taki (o ile istnieje) element $1 \in \mathfrak{A}$, że dla dowolnego $a \in \mathfrak{A}$ jest

$$(I.50) \quad 1a = a1 = a. \quad \blacksquare$$

Pierścień z jedynką można zatem traktować jako algebrę

$$(I.51) \quad \mathcal{A} := (\mathfrak{A}, +, \cdot, -, 0, 1),$$

gdzie przyjęto oznaczenia jak w definicjach (I.37) i (I.49) i są spełnione warunki (I.39), ..., (I.45), (I.47) i (I.50).

(I.52) PRZYKŁAD. Zbiór liczb całkowitych \mathbb{Z} ze zwykłym dodawaniem i mnożeniem, zwykłym zerem i jedynką tworzy pierścień z jedynką $(\mathbb{Z}, +, \cdot, -, 0, 1)$. ■

(I.53) TWIERDZENIE. Dla pierścieni (I.38) i (I.51) algebra $(\mathfrak{A}, +, -, 0)$ jest grupą przemenną, a algebra $(\mathfrak{A}, \cdot, 0)$ — półgrupą z elementem zerowym, ponadto dla pierścienia (I.51) algebra $(\mathfrak{A}, \cdot, 0, 1)$ jest półgrupą z elementem jedynkowym i z elementem zerowym.

Dowód wynika z definicji i twierdzenia (I.46). ■

(I.54) TWIERDZENIE. W każdym pierścieniu (I.38) lub (I.51) \mathcal{A} -zero 0, a w każdym pierścieniu (I.51) \mathcal{A} -jedyńska 1 są określone jednoznacznie.

Dowód wynika z twierdzeń (I.53), (I.10) i (I.11). ■

(I.55) TWIERDZENIE. W każdym pierścieniu (I.51) jest $1 \neq 0$.

Dowód wynika z twierdzeń (I.53) i (I.12). ■

(I.56) TWIERDZENIE. W każdym pierścieniu (I.38) lub (I.51) dla każdej pary elementów $a, b \in \mathfrak{A}$ istnieje dokładnie jeden taki element $x \in \mathfrak{A}$, że $a + x = b$.

Dowód wynika z twierdzeń (I.53), (I.26) i (I.27). ■

(I.57) DEFINICJA. W pierścieniu (I.38) lub (I.51) działanie przyporządkowujące dowolnej parze uporządkowanej elementów $a, b \in \mathfrak{A}$ taki element $x \in \mathfrak{A}$, że $a + x = b$, nazywamy odejmowaniem. ■

Zamiast $a + (-b)$ piszemy $a - b$. Z łatwością dowodzi się, że

$$-(a + b) = -a - b, \quad -(a - b) = -a + b, \quad -abc = (-a)bc = a(-b)c = ab(-c)$$

i innych wzorów analogicznych do znanych dla liczb rzeczywistych.

W każdym pierścieniu (I.38) lub (I.51) wprowadza się również *potęgowanie* określone dla dowolnego elementu $a \in \mathfrak{A}$ i dowolnego wykładnika $m \in \mathbb{N}$ wzorem rekurencyjnym

$$a^m := \begin{cases} a & \text{dla } m=1, \\ aa^{m-1} & \text{dla } m \geq 2. \end{cases}$$

W każdym pierścieniu (I.51) wprowadza się ponadto dla $a \neq 0$

$$a^0 := 1,$$

gdzie 1 jest \mathcal{A} -jedyneką.

(I.58) DEFINICJA. Pierścień (I.38) lub (I.51) nazywamy *przemiennym* wtedy i tylko wtedy, gdy dla dowolnych $a, b \in \mathfrak{A}$ jest

$$(I.59) \quad ab = ba. \quad \blacksquare$$

§ I.3. Pierścienie z transpozycją

(I.60) DEFINICJA. *Pierścieniem z transpozycją* nazywamy algebrę

$$(I.61) \quad \mathcal{A} := (\mathfrak{A}, +, \cdot, -, s, t, 0, 1),$$

gdzie \mathfrak{A} jest zbiorem zawierającym co najmniej 2 elementy, $(\mathfrak{A}, +, \cdot, -, 0, 1)$ jest pierścieniem z jedynką (I.51), s i t są operacjami jednoargumentowymi, zwanymi odpowiednio *sprzężeniem* i *transpozycją*, przyporządkowującymi dowolnemu elementowi $a \in \mathfrak{A}$ odpowiednio elementy \bar{a} , $a^T \in \mathfrak{A}$ i dla dowolnych $a, b \in \mathfrak{A}$ są spełnione następujące warunki:

$$(I.62) \quad \overline{(\bar{a})} = a,$$

$$(I.63) \quad \overline{a+b} = \bar{a} + \bar{b},$$

$$(I.64) \quad \overline{ab} = \bar{a}\bar{b},$$

$$(I.65) \quad (a^T)^T = a,$$

$$(I.66) \quad (a+b)^T = a^T + b^T,$$

$$(I.67) \quad (ab)^T = b^T a^T,$$

$$(I.68) \quad (\bar{a})^T = \overline{(a^T)}. \quad \blacksquare$$

Z powyższej definicji wynika, że dla pierścienia z transpozycją (I.61) i dla dowolnych $a, b, c \in \mathfrak{A}$ są spełnione warunki (I.39), ..., (I.45), (I.47), (I.50) i są ważne definicje (I.48), (I.49), (I.57), (I.58) oraz twierdzenia (I.46), (I.53), (I.54), (I.55) i (I.56).

Zarówno dla pierścieni (I.38) i (I.51) jak i dla pierścieni z transpozycją (I.61) przyjmujemy, że zdanie

$$a \in \mathcal{A}$$

jest równoważne zdaniu $a \in \mathfrak{A}$.

W niniejszej książce będziemy mieć do czynienia prawie wyłącznie z pierścieniami z transpozycją. Wprowadzenie sprzężenia spełniającego warunki (I.62), (I.63) i (I.64) nie jest ograniczeniem klasy rozpatrywanych pierścieni, ponieważ zawsze istnieje sprzężenie trywialne $\bar{a} := a$. Wprowadzenie transpozycji spełniającej warunki (I.65), ..., (I.68) nie jest ograniczeniem dla pierścieni przemennych, ponieważ dla nich zawsze istnieje transpozycja trywialna $a^T := a$. Natomiast wprowadzenie transpozycji ogranicza klasę pierścieni z mnożeniem nieprzemennym. Dlatego pierścienie (I.61) nazwalismy pierścieniami z transpozycją.

Pierścienie (I.51) i (I.61) traktujemy jako przypadki szczególne pierścienia (I.38). Zatem mówiąc o pierścieniu (I.38), mamy na myśli również pierścienie (I.51) i (I.61).

(I.69) PRZYKŁAD. Niech \mathfrak{A} będzie zbiorem wszystkich uporządkowanych par liczb całkowitych. Niech $+$, \cdot , $-$, s , t będą działaniami określonymi dla dowolnych par (a, b) , $(c, d) \in \mathfrak{A}$, gdzie $(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$, wzorami:

$$\begin{aligned}(a, b) + (c, d) &:= (a + c, b + d), & (a, b)(c, d) &:= (ac, bd), \\ -(a, b) &:= (-a, -b), & \overline{(a, b)} &:= (a, b), & (a, b)^T &:= (b, a).\end{aligned}$$

Niech ponadto

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

Sprawdzamy z łatwością, że algebra $\mathcal{A} := (\mathfrak{A}, +, \cdot, -, s, t, 0, 1)$ jest pierścieniem przemennym z transpozycją. ■

(I.70) DEFINICJA. W dowolnym pierścieniu z transpozycją (I.61) *transpozycją sprzężoną* nazywamy operację jednoargumentową $*$ określoną dla dowolnego $a \in \mathfrak{A}$ wzorem:

$$(I.71) \quad a^* := (\bar{a})^T. \quad \blacksquare$$

(I.72) TWIERDZENIE. W dowolnym pierścieniu z transpozycją (I.61) dla dowolnych $a, b, a_1, \dots, a_n \in \mathfrak{A}$

$$(I.73) \quad (a^*)^* = a,$$

$$(I.74) \quad (a + b)^* = a^* + b^*,$$

$$(I.75) \quad (ab)^* = b^* a^*,$$

$$(I.76) \quad a^* = \overline{(a^T)},$$

$$(I.77) \quad (\bar{a})^* = \overline{(a^*)} = a^T,$$

$$(I.78) \quad (a^T)^* = (a^*)^T = \bar{a},$$

$$(I.79) \quad \overline{(-a)} = -\bar{a},$$

$$(I.80) \quad (-a)^T = -a^T,$$

$$(I.81) \quad (-a)^* = * - a,$$

$$\begin{aligned}
(I.82) \quad & \overline{a-b} = \bar{a} - \bar{b}, \\
(I.83) \quad & (a-b)^T = a^T - b^T, \\
(I.84) \quad & (a-b)^* = a^* - b^*, \\
(I.85) \quad & \overline{a_1 + \dots + a_n} = \bar{a}_1 + \dots + \bar{a}_n, \\
(I.86) \quad & (a_1 + \dots + a_n)^T = a_1^T + \dots + a_n^T, \\
(I.87) \quad & (a_1 + \dots + a_n)^* = a_1^* + \dots + a_n^*, \\
(I.88) \quad & \overline{a_1 \dots a_n} = \bar{a}_1 \dots \bar{a}_n, \\
(I.89) \quad & (a_1 \dots a_n)^T = a_n^T \dots a_1^T, \\
(I.90) \quad & (a_1 \dots a_n)^* = a_n^* \dots a_1^*, \\
(I.91) \quad & 0 = \bar{0} = 0^T = 0^*, \\
(I.92) \quad & 1 = \bar{1} = 1^T = 1^*.
\end{aligned}$$

Dowód. Wzór (I.73) wynika z (I.71), (I.68), (I.65) i (I.62), ponieważ

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

Wzór (I.74) wynika z (I.71), (I.63), (I.66), a wzór (I.75) z (I.71), (I.64) i (I.67). Analogicznie dowodzimy prawdziwości wzorów (I.76), (I.77) i (I.78).

Na mocy (I.41) i (I.63) mamy $\overline{0+a} = \bar{a}$, czyli $\bar{0} + \bar{a} = \bar{a}$, skąd na mocy twierdzenia (I.54)

$$(i) \quad \bar{0} = 0.$$

Wobec tego z (I.42) wynika, że

$$\overline{(-a)} + \bar{a} = 0,$$

a stąd wzór (I.79). Analogicznie, ze wzoru (I.41) wynika, że

$$(ii) \quad 0^T = 0$$

i na mocy wzorów (I.42) oraz (I.66) wzór (I.80). Wzór (I.81) wynika ze wzorów (I.71), (I.79) i (I.80). Na mocy równości $a-b = a+(-b)$ wzory (I.82), (I.83) i (I.84) wynikają ze wzorów (I.63), (I.66), (I.74) oraz (I.79), (I.80), (I.81).

Wzory (I.85), ..., (I.90) dowodzimy z łatwością przez indukcję.

Wzór (I.91) wynika ze wzorów (i), (ii) oraz (I.71). Na mocy (I.64) dla każdego $b \in \mathfrak{A}$ mamy $\bar{1} \cdot \bar{b} = \overline{1 \cdot b} = \bar{b}$, skąd na mocy twierdzenia (I.54) $\bar{1} = 1$ i analogicznie ze wzoru (I.67) wynika $1^T = 1$. Stąd i ze wzoru (I.71) otrzymujemy (I.92). ■

(I.93) DEFINICJA. Element $a \in \mathfrak{A}$ z pierścienia z transpozycją (I.61) nazywamy *samosprzężonym* wtedy i tylko wtedy, gdy $\bar{a} = a$, *symetrycznym* wtedy i tylko wtedy, gdy $a^T = a$, *hermitowskim* wtedy i tylko wtedy, gdy $a^* = a$, oraz *quasi-rzeczywistym* wtedy i tylko wtedy, gdy

$$(I.94) \quad a = \bar{a} = a^T = a^*. \quad \blacksquare$$

(I.95) DEFINICJA. *Pierścieniem liczb całkowitych* \mathcal{Z} nazywamy pierścień z transpozycją

$$(I.96) \quad \mathcal{Z} := (\mathbb{Z}, +, \cdot, -, s, t, 0, 1),$$

gdzie \mathbb{Z} jest zbiorem wszystkich liczb całkowitych, $+$ jest zwykłym dodawaniem, \cdot — zwykłym mnożeniem, $-$ jest zwykłą zmianą znaku, a s i t odpowiednio sprzężeniem trywialnym i transpozycją trywialną, określonymi dla dowolnej liczby całkowitej $z \in \mathbb{Z}$ wzorami $\bar{z} := z$ i $z^T := z$. ■

(I.97) DEFINICJA. *Podpierścieniem* dowolnego pierścienia z transpozycją (I.61) nazywamy każdą podalgebrę tego pierścienia, czyli każdy pierścień z transpozycją $\mathcal{B} := (\mathcal{B}, +, \cdot, -, s, t, 0, 1)$, dla którego $\mathcal{B} \subset \mathcal{A}$ i

$$\begin{aligned} \mathcal{B} + \mathcal{B} &\subset \mathcal{B}, & \mathcal{B} \cdot \mathcal{B} &\subset \mathcal{B}, & -\mathcal{B} &\subset \mathcal{B}, & s(\mathcal{B}) &\subset \mathcal{B}, \\ t(\mathcal{B}) &\subset \mathcal{B}, & 0 &\in \mathcal{B}, & 1 &\in \mathcal{B}. \end{aligned} \quad \blacksquare$$

(I.98) PRZYKŁAD. Biorąc w (I.69) zamiast \mathcal{A} zbiór wszystkich par liczb całkowitych postaci (a, a) , otrzymujemy podpierścień pierścienia \mathcal{A} . ■

Podpierścień pierścieni (I.38) i (I.51) definiujemy analogicznie do (I.97).

(I.99) TWIERDZENIE. *W każdym przemennym pierścieniu z transpozycją (I.61) zbiór wszystkich elementów quasi-rzeczywistych tworzy podpierścień.*

Dowód. Niech \mathfrak{X} będzie w pierścieniu (I.61) zbiorem wszystkich elementów quasi-rzeczywistych. Zbiór ten zawiera na mocy (I.91) i (I.92) co najmniej dwa elementy 0 i 1. Na mocy (I.63), (I.66) i (I.74) zbiór \mathfrak{X} jest zamknięty ze względu na dodawanie $+$, na mocy (I.64), (I.67) wraz z (I.59) oraz (I.75) jest zamknięty ze względu na mnożenie \cdot , na mocy (I.79), (I.80) i (I.81) jest zamknięty ze względu na operację $-$, na mocy (I.94) jest zamknięty ze względu na operacje sprzężenia i transpozycji. Zatem \mathfrak{X} , istotnie, tworzy podpierścień pierścienia z transpozycją (I.61). ■

(I.100) DEFINICJA. *Częścią quasi-rzeczywistą* dowolnego przemennego pierścienia z transpozycją (I.61) nazywamy jego podpierścień utworzony przez wszystkie elementy quasi-rzeczywiste. ■

Część quasi-rzeczywistą dowolnego pierścienia przemennego z transpozycją \mathcal{A} oznaczamy symbolem $\text{re } \mathcal{A}$.

(I.101) PRZYKŁAD. W pierścieniu przemennym z transpozycją z przykładu (I.69) podpierścień $\text{re } \mathcal{A}$ jest utworzony przez wszystkie elementy postaci (a, a) . ■

(I.102) DEFINICJA. Pierścień z transpozycją (I.61) i $\mathcal{B} := (\mathcal{B}, (+), (\cdot), (-), s_1, t_1, o, e)$ nazywamy *izomorficznymi* wtedy i tylko wtedy, gdy są algebrami izomorficznymi, tzn. istnieje różnowartościowe przekształcenie f zbioru \mathcal{A} na zbiór \mathcal{B} , zachowujące operacje $+$, \cdot , $-$, s , t , 0 , 1 , a więc takie, że

$$\begin{aligned} f(a+b) &= f(a)(+)f(b), & f(ab) &= f(a)(\cdot)f(b), & f(-a) &= (-)f(a), \\ f(\bar{a}) &= s_1(f(a)), & f(a^T) &= t_1(f(a)), & f(0) &= o, & f(1) &= e. \end{aligned} \quad \blacksquare$$

Izomorfizm pierścieni (I.38) oraz pierścieni (I.51) określamy analogicznie.

(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 *dziedzina całkowitości* nazywamy każdy przemienny pierścień z jedyneką, który nie zawiera właściwych dzielników zera. ■