FOLIA 141

Annales Universitatis Paedagogicae Cracoviensis

Studia ad Didacticam Mathematicae Pertinentia V (2013)

Antoni Chronowski

Uporządkowane struktury liczbowe*

Abstract. In this article we consider the ordered algebraic structures of the systems of natural numbers, integers, rational and real numbers. We present the ordered algebra of natural numbers, the ordered ring of integers, and the ordered fields of rational and real numbers. The main problem considered for ordered number structures is the categoricity of these systems determined by a suitable isomorphism. First of all, this article is addressed at Mathematics students of pedagogical studies and at teachers of Mathematics.

1. Wstęp

Począwszy od najstarszych cywilizacji ludzi fascynowały liczby i różne ich zadziwiające własności. Pitagorejczycy (VI-V w. p.n.e.) przypisywali liczbom cechy mistyczne i uważali je za podstawową zasadę bytu i harmonii świata. W słynnej teorii Platona (427-347 p.n.e.) o niezmiennych ideach i zmiennych rzeczach matematyka (tzw. czysta) jest nauką o ideach, a więc również liczby mają charakter idei istniejących poza czasem i przestrzenią. Ogromny wpływ na rozwój matematyki, w tym geometrii i arytmetyki liczb, miało dzieło Euklidesa (ok. 365-ok. 300 p.n.e.) *Elementy*, napisane w formie systemu aksjomatyczno-dedukcyjnego. Teoria proporcji Eudoxosa, którą Euklides stosuje w *Elementach* (księga V), jest uważana za pierwowzór teorii liczb rzeczywistych. W księgach VII-IX jest rozwijana arytmetyka liczb naturalnych.

Ze względu na treść tego artykułu warto wspomnieć o pewnych systemach arytmetyki liczb, które odegrały bardzo ważną rolę w pracach badawczych matematyków nad tzw. podstawami matematyki na przełomie XIX i XX wieku. W tym okresie rozwinęły się trzy główne kierunki w filozofii matematyki: logicyzm, intuicjonizm i formalizm. Badaniami filozoficznych podstaw matematyki zajmowali się wtedy wybitni matematycy: Richard Dedekind (1831-1916), Georg Cantor (1845-1918), Gottlob Frege (1848-1925), Giuseppe Peano (1858-1932), David Hilbert (1862-1943), Bertrand Russell (1872-1970), Luitzen Brouwer (1881-1966). Zasadniczym kierunkiem prac matematyków nad podstawami matematyki w tym okresie

*Ordered number structures

2010 Mathematics Subject Classification: Primary: 97H50, Secondary: 97F30, 97F40, 97F50

Key words and phrases: ordered number systems, categoricity

była logiczna systematyzacja matematyki, polegająca na zastąpieniu intuicyjnych pojęć i rozumowań przez formalne dowody twierdzeń, oparte na logicznie precyzyjnych definicjach i układach aksjomatów. Warto tu jednak wspomnieć, że inticjoniści mieli krytyczny stosunek do takich formalnych teorii matematycznych. Zaczął kształtować się pogląd, że należy najpierw utworzyć precyzyjną, ścisłą aksjomatyczną teorię liczb naturalnych, która będzie podstawą do rozwijania teorii liczb całkowitych, wymiernych i rzeczywistych. Powstały wtedy systemy aksjomatyczne liczb naturalnych utworzone przez G. Fregego, R. Dedekinda i G. Peana. W tym artykule teoria G. Peana będzie wykorzystana do analizy zagadnień dotyczących liczb naturalnych.

Bardzo ważna jest teoria liczb rzeczywistych opracowana przez R. Dedekinda oparta na tzw. *przekrojach* zbioru liczb wymiernych. R. Dedekind nawiązywał w niej do idei teorii proporcji Eudoxosa, ale zdecydowanie podkreślał, że w teorii Eudoxosa (i *Elementach* Euklidesa) brak bardzo ważnej własności, tzw. *zasady ciągłości* zbioru liczb rzeczywistych. We współczesnym sformułowaniu zasada ciągłości postulowana przez Dedekinda brzmi:

Dla każdego przekroju zbioru liczb rzeczywistych albo w klasie pierwszej (*dolnej*) *istnieje liczba największa, albo w klasie drugiej* (*górnej*) *istnieje liczba najmniejsza.*

Drugą popularną teorię liczb rzeczywistych opracował G. Cantor, opierając zasady tej teorii na *ciągach podstawowych* (spełniających warunek Cauchy'ego) liczb wymiernych i używając do tej konstrukcji relacji równoważności w zbiorze wymiernych ciągów podstawowych. Konstrukcja Cantora liczb rzeczywistych jest w sposób istotny wykorzystana w tym artykule.

W roku 1900 David Hilbert (1900, tłum. Pogonowski, 2012) opublikował aksjomatyczną teorię liczb rzeczywistych, nazywając *metodami genetycznymi* konstrukcje Dedekinda i Cantora zbioru liczb rzeczywistych. Powyższe uwagi dotyczące filozofii matematyki może Czytelnik rozszerzyć np. na podstawie przystępnie napisanej książki R. Murawskiego (2005).

W tym artykule rozważane są struktury algebraiczno-porządkowe systemów liczb naturalnych, całkowitych, wymiernych i rzeczywistych. Zatem będą zaprezentowane: uporządkowana algebra liczb naturalnych, uporządkowany pierścień liczb całkowitych, ciała uporządkowane liczb wymiernych i rzeczywistych. Głównym zagadnieniem we wszystkich rozważanych strukturach liczbowych będzie *kategoryczność* tych systemów, a priorytetowym pojęciem będzie *izomorfizm* stosownych systemów liczbowych.

Artykuł jest zaadresowany przede wszystkim do studentów nauczycielskich studiów matematycznych, ale może być przydatny również dla nauczycieli matematyki. Prezentowane zagadnienia mogą zostać wykorzystane na zajęciach seminaryjnych ze studentami, a także mogą być inspiracją do tematyki prac dyplomowych pisanych przez studentów nauczycielskich studiów matematycznych.

Z mojego długoletniego doświadczenia w pracy dydaktycznej ze studentami matematyki studiów nauczycielskich wynika, że studenci rozpoczynający studia mają na podstawie nauczania szkolnego pewną intuicyjną wiedzę o liczbach naturalnych, całkowitych, wymiernych i rzeczywistych. W czasie studiów studenci pogłębiają i rozszerzają intuicyjną znajomość systemów liczbowych, a także potrafią określić, jakimi strukturami algebraicznymi są poszczególne podstawowe zbiory liczbowe z wyróżnionymi w nich działaniami. Jednak ta abstrakcyjna wiedza o strukturach liczbowych ciągle jest oparta na intuicyjnym szkolnym nauczaniu. Przyjmujemy, że studenci znają własności działań na liczbach, a na zajęciach prowadzonych ze studentami porządkujemy tę wiedzę systematyzując ją w odpowiednie struktury algebraiczne. W dodatku na ogół w programach studiów nie występują struktury algebraiczno-porządkowe lub są traktowane informacyjnie. Używając pojęć z prac Semadeniego (2002, 2005) można stwierdzić, że studenci mają dość dobrze ukształtowane tzw. *idee głębokie* poszczególnych arytmetyk liczbowych, ale wyraźnie gorzej przedstawia się opanowanie przez nich tzw. *modeli formalnych* arytmetyk liczbowych w teoriach aksjomatycznych. Studenci na różnych przedmiotach (kursach) spotykają się z informacjami: o aksjomatyce Peana liczb naturalnych, o konstrukcjach liczb całkowitych i wymiernych za pomocą relacji równoważności, o konstrukcjach Dedekinda i Cantora liczb rzeczywistych, a także o schemacie aksjomatyki liczb rzeczywistych. Wiedza studentów z tego zakresu jest powierzchowna i ma charakter informacyjny. Brak systematycznych i pogłębionych studiów w zakresie teoretycznych arytmetyk liczbowych powoduje pewien chaos w wiedzy studentów o systemach liczbowych, gdyż intuicyjna szkolna nauka o liczbach została „zakłócona" abstrakcyjnymi teoriami o liczbach, a z kolei teorie abstrakcyjne o liczbach nie zostały tak rozwinięte i poznane przez studentów, aby utworzyć spójny system nauki o liczbach, zaczynając od nauczania szkolnego, a kończąc na abstrakcyjnym kształceniu na studiach matematycznych.

Studenci kończący studia matematyczne często nie umieją przekonująco odpowiedzieć na podstawowe pytanie typu:

Co łączy wszystkie konstruowane lub postulowane aksjomatycznie systemy liczb naturalnych, całkowitych, wymiernych i rzeczywistych, że pomimo tak wielu metod ich konstruowania (postulowania) w matematyce abstrakcyjnej, możemy w szkole mówić o jednej arytmetyce dla poszczególnych zbiorów liczbowych?

Przyszły nauczyciel matematyki powinien mieć w miarę dobrze ukształtowany pogląd na zagadnienia przedstawione w powyższym pytaniu. Nauka o liczbach stanowi bardzo duży obszar nauczania szkolnego matematyki. Obowiązujące dotychczas *standardy kształcenia* na kierunku matematyka określone przez MNiSW nie przewidywały obszerniejszego kształcenia w zakresie teoretycznej arytmetyki liczb i teorii liczb. Wprowadzane obecnie systemy kształcenia studentów oparte na tzw. efektach kształcenia umożliwiają swobodniejsze kształtowanie programów studiów. Czy tematyka abstrakcyjnej arytmetyki liczb znajdzie uznanie matematyków przygotowujących programy na uczelniach (wydziałach) kształcących nauczycieli matematyki? Wyraźnie pragnę podkreślić, że powyższe refleksje o kształceniu matematycznym studentów są oparte jedynie na moich doświadczeniach i analizie różnych programów studiów kształcących przyszłych nauczycieli matematyki, natomiast nie prowadziłem w tym zakresie systematycznych badań pedagogicznych.

W tym artykule została podjęta pewna próba przedstawienia propozycji dydaktycznej umożliwiającej uzupełnienie istotnej luki w wiedzy studentów matematycznych studiów nauczycielskich, dotyczącej kategoryczności podstawowych systemów liczbowych i umożliwiającej merytoryczną odpowiedź na wyżej postawione pytanie dotyczące systemów liczbowych.

2. Uporządkowana algebra liczb naturalnych

Głównymi pojęciami w tej części artykułu są: aksjomatyka Peana liczb naturalnych, model aksjomatyki Peana, uporządkowana algebra liczb naturalnych. Podstawowe twierdzenie dotyczy izomorfizmu uporządkowanych algebr liczb naturalnych.

W roku 1889 włoski matematyk Giusseppe Peano podał aksjomatykę arytmetyki liczb naturalnych (zob. Chronowski, 1999a, 29-30).

Pojęciami pierwotnymi są: *liczba* 0 (*zero*), *zbiór wszystkich liczb naturalnych* $\mathcal{N}_A$, *funkcja następnika* $*\colon \mathcal{N}_A \ni n \longrightarrow n^* \in \mathcal{N}_A$.

Aksjomaty:

$(A1)$ $0 \in \mathcal{N}_A$.

$(A2)$ $\forall\, n \in \mathcal{N}_A[n^* \in \mathcal{N}_A]$.

$(A3)$ $\forall\, n \in \mathcal{N}_A[n^* \neq 0]$.

$(A4)$ $\forall\, m, n \in \mathcal{N}_A[m^* = n^* \Longrightarrow m = n]$.

$(A5)$ $\forall\, M \subseteq \mathcal{N}_A[(0 \in M \wedge \forall\, n \in \mathcal{N}_A(n \in M \Longrightarrow n^* \in M)) \Longrightarrow M = \mathcal{N}_A]$.

Aksjomat $(A5)$ nazywa się *aksjomatem indukcji* (*zasadą indukcji*).

Uwaga: W książce (Chronowski, 1999a) zamiast symbolu $\mathcal{N}_A$ występuje symbol N zbioru liczb naturalnych.

Definicja 2.1

Modelem aksjomatyki Peana nazywamy system (ciąg) (A, S, a) spełniający następujące warunki:

$(M1)$ $a \in A$.

$(M2)$ $S\colon A \longrightarrow A$ jest funkcją.

$(M3)$ $a \notin S(A)$, gdzie $S(A)$ oznacza zbiór wartości funkcji S.

$(M4)$ Funkcja S jest injekcją.

$(M5)$ Jeżeli M jest dowolnym podzbiorem zbioru A takim, że:
 (a) $a \in M$,
 (b) $\forall\, p \in A[p \in M \Longrightarrow S(p) \in M]$,

to $M = A$.

Warunek $(M5)$ nazywa się *aksjomatem indukcji* (*zasadą indukcji*) w modelu aksjomatyki Peana.

W książce W. Guzickiego i P. Zakrzewskiego (2005, s. 197) model aksjomatyki Peana nazywa się algebrą Peana.

Łatwo zauważyć, że prawdziwy jest następujący

Wniosek 2.2

System $(\mathcal{N}_A, *, 0)$ *jest modelem aksjomatyki Peana.*

Na podstawie twierdzenia 11.3 (Guzicki, Zakrzewski, 2005, s. 200) łatwo zauważyć, że prawdziwe jest następujące *twierdzenie o definiowaniu przez indukcję*:

TWIERDZENIE 2.3
Niech (A, S, a) będzie modelem aksjomatyki Peana. Niech B będzie niepustym zbiorem, $T\colon B \longrightarrow B$ – dowolną funkcją, $b \in B$ – dowolnie ustalonym elementem. Wtedy istnieje dokładnie jedna funkcja $F\colon A \longrightarrow B$ taka, że:
$(I1)$ $F(a) = b$,
$(I2)$ $\forall\, x \in A[F(S(x)) = T(F(x))]$.

TWIERDZENIE 2.4
Niech (A, S, a) będzie modelem aksjomatyki Peana. Istnieje dokładnie jedna funkcja $F\colon A \times A \longrightarrow A$ taka, że:
(a) $F(p, a) = p$ dla każdego $p \in A$,
(b) $F(p, S(q)) = S(F(p, q))$ dla dowolnych $p, q \in A$.

Dowód. Niech $p \in A$ będzie dowolnie ustalonym elementem. Zastosujemy twierdzenie 2.3 przyjmując: $B = A$, $T = S$, $b = p$. Z twierdzenia 2.3 wynika, że istnieje dokładnie jedna funkcja $F_p\colon A \longrightarrow A$ taka, że:
(a_1) $F_p(a) = p$,
(b_1) $F_p(S(q)) = S(F_p(q))$ dla każdego $q \in A$.
Określamy funkcję $F\colon A \times A \longrightarrow A$ przyjmując:

$$F(p, q) = F_p(q)$$

dla dowolnych $p, q \in A$. Warunek (a_1) implikuje równości: $F(p, a) = F_p(a) = p$ dla dowolnego $p \in A$. Z warunku (b_1) wynika, że $F(p, S(q)) = F_p(S(q)) = S(F_p(q)) = S(F(p, q))$ dla dowolnych $p, q \in A$. Zatem funkcja F spełnia warunki (a) i (b).

Udowodnimy jednoznaczność funkcji F. Niech $G\colon A \times A \longrightarrow A$ spełnia warunki (a) i (b), czyli:
(a_2) $G(p, a) = p$ dla każdego $p \in A$,
(b_2) $G(p, S(q)) = S(G(p, q))$ dla dowolnych $p, q \in A$.
Rozważmy zbiór $M \subseteq A$ określony następująco:

$$M = \{q \in A\colon\ \forall\, p \in A[F(p, q) = G(p, q)]\}.$$

Zauważmy, że $a \in M$, gdyż $F(p, a) = p = G(p, a)$ dla każdego $p \in A$. Niech $q \in M$, czyli $F(p, q) = G(p, q)$ dla dowolnego $p \in A$. Udowodnimy, że $S(q) \in M$. Istotnie, dla dowolnego $p \in A$ mamy: $F(p, S(q)) = S(F(p, q)) = S(G(p, q)) = G(p, S(q))$, a więc $S(q) \in M$. Z aksjomatu indukcji w modelu aksjomatyki Peana (A, S, a) wynika, że $M = A$, czyli $F(p, q) = G(p, q)$ dla dowolnych $p, q \in A$, a więc $F = G$. Dowód twierdzenia został zakończony.

DEFINICJA 2.5
Niech (A, S, a) będzie modelem aksjomatyki Peana. W zbiorze A określamy *dodawanie* $+\colon A \times A \longrightarrow A$ następująco:
(a) $p + a = p$ dla każdego $p \in A$,
(b) $p + S(q) = S(p + q)$ dla dowolnych $p, q \in A$.

Z twierdzenia 2.4 wynika, że dodawanie $+$ w zbiorze A jest jednoznacznie określonym działaniem w tym zbiorze.

Twierdzenie 2.6
Niech (A, S, a) będzie modelem aksjomatyki Peana. Istnieje dokładnie jedna funkcja $F \colon A \times A \longrightarrow A$ taka, że:
(a) $F(p, a) = a$ dla każdego $p \in A$,
(b) $F(p, S(q)) = F(p, q) + p$ dla dowolnych $p, q \in A$.

Dowód tego twierdzenia jest analogiczny do dowodu twierdzenia 2.4.
Wskazówka: Niech $p \in A$ będzie dowolnie ustalonym elementem. Zastosować twierdzenie 2.3 przyjmując: $B = A$, $T(q) = q + p$ dla dowolnego $q \in A$, $b = a$.

Definicja 2.7
Niech (A, S, a) będzie modelem aksjomatyki Peana. W zbiorze A określamy *mnożenie* $\cdot \colon A \times A \longrightarrow A$ następująco:
(a) $p \cdot a = a$ dla każdego $p \in A$,
(b) $p \cdot S(q) = p \cdot q + p$ dla dowolnych $p, q \in A$.

Z twierdzenia 2.6 wynika, że mnożenie $\cdot$ w zbiorze A jest jednoznacznie określonym działaniem w tym zbiorze.

Definicja 2.8
Niech (A, S, a) będzie modelem aksjomatyki Peana. W zbiorze A określamy relację $\leqslant$ następująco:
$$p \leqslant q \Longleftrightarrow \exists\, s \in A[q = p + s] \tag{1}$$
dla dowolnych $p, q \in A$.

Dla modelu aksjomatyki Peana (A, S, a) możemy otrzymać analogiczne rezultaty do tych, które są zamieszczone w książce (Chronowski, 1999a, podrozdziały 3.1-3.3) dla modelu $(\mathcal{N}_A, *, 0)$. W szczególności otrzymujemy poniższy analogon twierdzenia 3.5 (Chronowski, 1999a, s. 39).

Twierdzenie 2.9
Niech (A, S, a) będzie modelem aksjomatyki Peana. System $(A, \leqslant)$, gdzie relacja $\leqslant$ jest określona wzorem (1), jest zbiorem liniowo uporządkowanym.

Na podstawie definicji 2.1, 2.5, 2.7, 2.8 i twierdzenia 2.9, możemy przyjąć następującą definicję.

Definicja 2.10
System (ciąg) $(A, S, a, +, \cdot, \leqslant)$ nazywamy *uporządkowaną algebrą liczb naturalnych*, jeżeli spełnione są następujące warunki:
$(W1)$ System (A, S, a) jest modelem aksjomatyki Peana.
$(W2)$ System $(A, +)$ jest grupoidem, w którym działanie dodawania $+$ jest określone następująco:
(a) $p + a = p$ dla każdego $p \in A$,
(b) $p + S(q) = S(p + q)$ dla dowolnych $p, q \in A$.
$(W3)$ System $(A, \cdot)$ jest grupoidem, w którym działanie mnożenia $\cdot$ jest określone następująco:
(a) $p \cdot a = a$ dla każdego $p \in A$,

(b) $p \cdot S(q) = p \cdot q + p$ dla dowolnych $p, q \in A$.
$(W4)$ System $(A, \leqslant)$ jest zbiorem liniowo uporządkowanym, w którym relacja liniowo porządkująca $\leqslant$ jest określona następująco:

$$p \leqslant q \Longleftrightarrow \exists\, s \in A[q = p + s]$$

dla dowolnych $p, q \in A$.

Na podstawie wniosku 2.2, definicji 2.3 (Chronowski, 1999a, s. 33) definicji 2.9 (Chronowski, 1999a, s. 35) definicji 3.1 (Chronowski, 1999a, s. 38) i twierdzenia 3.5 (Chronowski, 1999a, s. 39) otrzymujemy następujące twierdzenie.

Twierdzenie 2.11
System $(\mathcal{N}_A, *, 0, +, \cdot, \leqslant)$ *jest uporządkowaną algebrą liczb naturalnych.*

Uwaga: W ramach aksjomatyki teorii mnogości możemy skonstruować uporządkowaną algebrę liczb naturalnych $(\mathcal{N}_K, *, 0, +, \cdot, \leqslant)$ (Chronowski, 1999a, podrozdział 3.5).

Definicja 2.12
Niech $(A, S, a, +, \cdot, \leqslant)$ i $(B, T, b, +, \cdot, \leqslant)$ będą uporządkowanymi algebrami liczb naturalnych. Bijekcję $F\colon A \longrightarrow B$ nazywamy *izomorfizmem*, jeżeli spełnione są następujące warunki:
(a) $F(a) = b$,
(b) $F(S(p)) = T(F(p))$ dla każdego $p \in A$,
(c) $F(p + q) = F(p) + F(q)$ dla dowolnych $p, q \in A$,
(d) $F(p \cdot q) = F(p) \cdot F(q)$ dla dowolnych $p, q \in A$,
(e) $p \leqslant q \Longleftrightarrow F(p) \leqslant F(q)$ dla dowolnych $p, q \in A$.

Definicja 2.13
Uporządkowane algebry liczb naturalnych $(A, S, a, +, \cdot, \leqslant)$ i $(B, T, b, +, \cdot, \leqslant)$ nazywamy *izomorficznymi*, jeżeli istnieje izomorfizm $F\colon A \longrightarrow B$.

Twierdzenie 2.14
Dowolne dwie uporządkowane algebry liczb naturalnych $(A, S, a, +, \cdot, \leqslant)$ *oraz* $(B, T, b, +, \cdot, \leqslant)$ *są izomorficzne.*

Dowód. Zgodnie z twierdzeniem 2.3 istnieje dokładnie jedna funkcja $F\colon A \longrightarrow B$ taka, że:

$$\begin{aligned} &(a_1)\ F(a) = b,\\ &(b_1)\ F(S(p)) = T(F(p)) \text{ dla kadego } p \in A. \end{aligned} \tag{2}$$

Udowodnimy, że F jest izomorfizmem uporządkowanych algebr liczb naturalnych $(A, S, a, +, \cdot, \leqslant)$ i $(B, T, b, +, \cdot, \leqslant)$. Najpierw wykażemy, że funkcja $F\colon A \longrightarrow B$ jest bijekcją. Na podstawie twierdzenia 2.3 istnieje dokładnie jedna funkcja $G\colon B \longrightarrow A$ taka, że:
(a_2) $G(b) = a$,
(b_2) $G(T(p)) = S(G(p))$ dla każdego $p \in B$.
Niech

$$M = \{p \in A\colon (G \circ F)(p) = p\}.$$

Oczywiście $a \in M$, gdyż $(G \circ F)(a) = G(F(a)) = G(b) = a$. Zakładamy, że $p \in M$, czyli $(G \circ F)(p) = p$. Udowodnimy, że $S(p) \in M$. Istotnie,

$$\begin{aligned}(G \circ F)(S(p)) &= G(F(S(p))) \\ &= G(T(F(p))) \\ &= S(G(F(p))) \\ &= S((G \circ F)(p)) \\ &= S(p).\end{aligned}$$

Stąd $S(p) \in M$. Zatem $M = A$, czyli

$$(G \circ F)(p) = p$$

dla każdego $p \in A$. Analogicznie można wykazać, że

$$(F \circ G)(p) = p$$

dla każdego $p \in B$. Zatem funkcje F i G są wzajemnie odwrotnymi bijekcjami.

Z warunków (a_1) i (b_1) wynika, że funkcja F spełnia warunki (a) i (b) definicji 2.12. Udowodnimy warunek (c) definicji 2.12. Rozważmy zbiór

$$M_1 = \{q \in A\colon\ \forall\, p \in A[F(p+q) = F(p) + F(q)]\}.$$

Zauważmy, że $a \in M_1$, gdyż $F(p + a) = F(p) = F(p) + b = F(p) + F(a)$ dla każdego $p \in A$. Zakładamy, że $q \in M_1$, czyli $F(p+q) = F(p) + F(q)$ dla każdego $p \in A$. Uzasadnimy, że $S(q) \in M_1$. Istotnie,

$$\begin{aligned}F(p + S(q)) &= F(S(p+q)) \\ &= T(F(p+q)) \\ &= T(F(p) + F(q)) \\ &= F(p) + T(F(q)) \\ &= F(p) + F(S(q))\end{aligned}$$

dla każdego $p \in A$. Stąd $S(q) \in M_1$, a więc $M_1 = A$. Zatem spełniony jest warunek (c) definicji 2.12.

Dowód warunku (d) definicji 2.12 jest analogiczny do dowodu warunku (c).

Udowodnimy warunek (e) definicji 2.12. Niech $p, q \in A$. Wtedy

$$\begin{aligned}p \leqslant q &\iff \exists\, s \in A[q = p + s] \\ &\iff \exists\, s \in A[F(q) = F(p+s)] \\ &\iff \exists\, s \in A[F(q) = F(p) + F(s)] \\ &\iff F(p) \leqslant F(q).\end{aligned}$$

Zatem spełniony jest warunek (e) definicji 2.12. Dowód twierdzenia został zakończony.

Na mocy twierdzeń 2.11 i 2.14 otrzymujemy następujący

Wniosek 2.15
Każda uporządkowana algebra liczb naturalnych $(A, S, a, +, \cdot, \leqslant)$ *jest izomorficzna z uporządkowaną algebrą liczb naturalnych* $(\mathcal{N}_A, *, 0, +, \cdot, \leqslant)$.

Wniosek 2.15 możemy również sformułować następująco:

Wniosek 2.16
Istnieje tylko jedna, z dokładnością do izomorfizmu, uporządkowana algebra liczb naturalnych.

Korzystając z wniosku 2.16 możemy przyjąć zapis $(\mathcal{N}, *, 0, +, \cdot, \leqslant)$ dla uporządkowanej algebry liczb naturalnych, związany z tradycyjnymi oznaczeniami w arytmetyce liczb naturalnych. Przyjmujemy, że $\mathcal{N}_1 = \mathcal{N} \setminus \{0\}$.

3. Uporządkowany pierścień liczb całkowitych

Głównymi pojęciami w tej części artykułu są: uporządkowany pierścień całkowity, uporządkowany pierścień całkowity spełniający aksjomat indukcji, uporządkowany pierścień liczb całkowitych. Podstawowymi twierdzeniami są: twierdzenie o izomorfizmie uporządkowanych pierścieni całkowitych spełniających aksjomat indukcji, twierdzenie o izomorficznym zanurzeniu uporządkowanego pierścienia liczb całkowitych w dowolnym uporządkowanym pierścieniu całkowitym.

Definicja 3.1
System (ciąg) $(P, +, \cdot, \leqslant)$ nazywamy *uporządkowanym pierścieniem całkowitym*, jeżeli spełnione są następujące warunki:
(a_1) $(P, +, \cdot)$ jest pierścieniem całkowitym,
(a_2) $(P, \leqslant)$ jest zbiorem liniowo uporządkowanym,
(a_3) $\forall\, a, b, c \in P[a \leqslant b \Longrightarrow a + c \leqslant b + c]$,
(a_4) $\forall\, a, b, c \in P[(a \leqslant b \wedge 0 \leqslant c) \Longrightarrow a \cdot c \leqslant b \cdot c]$.

Niech $(P, +, \cdot, \leqslant)$ będzie uporządkowanym pierścieniem całkowitym. Przyjmujemy:

$$P_0^+ = \{a \in P \colon 0 \leqslant a\}. \tag{3}$$

W kolejnych kilku twierdzeniach i lematach sformułujemy pewne elementarne własności uporządkowanych pierścieni całkowitych, z których będziemy korzystać w dalszej części artykułu. Dowody tych własności są łatwe i mogą służyć jako dobre ćwiczenia dla Czytelnika (można wykorzystać również np. książkę A. Kurosza (1965), gdzie w rozdziale VI zostały przedstawione podstawowe własności pierścieni uporządkowanych).

Twierdzenie 3.2
Niech $(P, +, \cdot, \leqslant)$ *będzie uporządkowanym pierścieniem całkowitym. Wtedy spełnione są następujące warunki:*
(a_1) $0 \in P_0^+$,
(a_2) $\forall\, a, b \in P[(a, b \in P_0^+) \Longrightarrow a + b \in P_0^+]$,

(a_3) $\forall\, a, b \in P[(a, b \in P_0^+) \Longrightarrow a \cdot b \in P_0^+]$,
(a_4) $\forall\, a \in P[(a \in P_0^+ \wedge -a \in P_0^+) \Longrightarrow a = 0]$,
(a_5) $\forall\, a \in P[a \in P_0^+ \vee -a \in P_0^+]$,
(a_6) $\forall\, a, b \in P[a \leqslant b \Longleftrightarrow b - a \in P_0^+]$.

Niech $(P, +, \cdot, \leqslant)$ będzie uporządkowanym pierścieniem całkowitym. Przyjmujemy:

$$a < b \Longleftrightarrow (a \leqslant b \wedge a \neq b)$$

dla $a, b \in P$. Wobec tego

$$a \leqslant b \Longleftrightarrow (a < b \vee a = b)$$

dla $a, b \in P$.

Ponadto przyjmujemy:

$$a \geqslant b \Longleftrightarrow b \leqslant a,$$

$$a > b \Longleftrightarrow b < a$$

dla $a, b \in P$.

Określamy następujący zbiór:

$$P^+ = \{a \in P\colon 0 < a\}.$$

Lemat 3.3
Niech $(P, +, \cdot, \leqslant)$ będzie uporządkowanym pierścieniem całkowitym. Wtedy:
(a) $\forall\, a, b, c \in P[a < b \Longrightarrow a + c < b + c]$,
(b) $\forall\, a, b, c \in P[(a < b \wedge 0 < c) \Longrightarrow a \cdot c < b \cdot c]$.

Twierdzenie 3.4
Niech $(P, +, \cdot, \leqslant)$ będzie uporządkowanym pierścieniem całkowitym. Wtedy spełnione są następujące warunki:

(a_1) $\forall\, a, b, c \in P[(a < b \wedge b < c) \Longrightarrow a < c]$,
(a_2) $\forall\, a, b \in P[a \leqslant b \Longleftrightarrow -b \leqslant -a]$,
(a_3) $\forall\, a, b \in P[a < b \Longleftrightarrow -b < -a]$,
(a_4) $\forall\, a, b, c, d \in P[(a < b \wedge c < d) \Longrightarrow a + c < b + d]$,
(a_5) $\forall\, a, b \in P[(a < 0 \wedge 0 < b) \Longrightarrow a \cdot b < 0]$,
(a_6) $\forall\, a, b, c, d \in P[(a < b \wedge c \leqslant d) \Longrightarrow a + c < b + d]$,
(a_7) $0 < 1$.

Twierdzenie 3.5
Prawo trychotomii.
Niech $(P, +, \cdot, \leqslant)$ będzie uporządkowanym pierścieniem całkowitym. Dla dowolnych elementów $a, b \in P$ spełniony jest dokładnie jeden ze składników następującej alternatywy:

$$a < b \ \vee\ b < a \vee\ a = b.$$

Definicja 3.6
Bijekcję $F\colon P \longrightarrow U$ nazywamy *izomorfizmem* uporządkowanych pierścieni całkowitych $(P, +, \cdot, \leqslant)$ i $(U, +, \cdot, \leqslant)$, jeżeli spełnione są następujące warunki:
(a) $\forall\, a, b \in P[F(a+b) = F(a) + F(b)]$,
(b) $\forall\, a, b \in P[F(a \cdot b) = F(a) \cdot F(b)]$,
(c) $\forall\, a, b \in P[a \leqslant b \Longleftrightarrow F(a) \leqslant F(b)]$.

Łatwo udowodnić następujący

Lemat 3.7
Bijekcja $F\colon P \longrightarrow U$ jest izomorfizmem uporządkowanych pierścieni całkowitych $(P, +, \cdot, \leqslant)$ i $(U, +, \cdot, \leqslant)$ wtedy i tylko wtedy, gdy spełnione są następujące warunki:
(a) $\forall\, a, b \in P[F(a+b) = F(a) + F(b)]$,
(b) $\forall\, a, b \in P[F(a \cdot b) = F(a) \cdot F(b)]$,
(c) $\forall\, a, b \in P[a < b \Longleftrightarrow F(a) < F(b)]$.

Definicja 3.8
Niech $(P, +, \cdot, \leqslant)$ będzie uporządkowanym pierścieniem całkowitym. Zakładamy, że spełniony jest następujący warunek:
Jeżeli $M \subseteq P_0^+$ jest zbiorem takim, że:
(a) $0 \in M$,
(b) $\forall\, a \in M[a+1 \in M]$,
to $M = P_0^+$.
Wtedy mówimy, że uporządkowany pierścień całkowity $(P, +, \cdot, \leqslant)$ *spełnia aksjomat indukcji.*

Na bazie arytmetyki liczb naturalnych możemy skonstruować za pomocą odpowiedniej relacji równoważności zbiór $\mathcal{Z}_N$ liczb całkowitych. W zbiorze $\mathcal{Z}_N$ określamy dodawanie $+$, mnożenie $\cdot$ oraz relację $\leqslant$ liniowego porządku.

Na podstawie konstrukcji liczb całkowitych i twierdzeń zamieszczonych w książce (Chronowski, 1999a, podrozdziały 4.1-4.3), możemy sformułować następujące

Twierdzenie 3.9
Uporządkowany pierścień całkowity $(\mathcal{Z}_N, +, \cdot, \leqslant)$ spełnia aksjomat indukcji.

Uwaga: W książce (Chronowski, 1999a) zamiast symbolu $\mathcal{Z}_N$ występuje symbol Z zbioru liczb całkowitych.

Niech $(P, +, \cdot, \leqslant)$ będzie uporządkowanym pierścieniem całkowitym spełniającym aksjomat indukcji. Określamy funkcję $S\colon P_0^+ \longrightarrow P_0^+$ następująco:

$$S(a) = a + 1 \tag{4}$$

dla $a \in P_0^+$.

Łatwo wykazać, że system $(P_0^+, S, 0)$ jest modelem aksjomatyki Peana.

Na podstawie twierdzenia 3.2(a_2),(a_3) wiemy, że działania dodawania $+$ i mnożenia $\cdot$ w pierścieniu całkowitym P, ograniczone do zbioru P_0^+, są działaniami w tym zbiorze. Korzystając z faktu, że system $(P_0^+, S, 0)$ jest modelem aksjomatyki Peana możemy określić indukcyjnie działania dodawania $\oplus$ i mnożenia $\odot$ za pomocą odpowiednio definicji 2.5 i 2.7 następująco:

(a) $a \oplus 0 = a$ dla każdego $a \in P_0^+$,

(b) $a \oplus S(b) = S(a \oplus b)$ dla dowolnych $a, b \in P_0^+$

oraz

(a) $a \odot 0 = 0$ dla każdego $a \in P_0^+$,

(b) $a \odot S(b) = (a \odot b) \oplus a$ dla dowolnych $a, b \in P_0^+$.

Wykażemy, że:

(a) $\forall\, a, b \in P_0^+ [a \oplus b = a + b]$,

(b) $\forall\, a, b \in P_0^+ [a \odot b = a \cdot b]$.

Najpierw udowodnimy warunek (a). Rozważmy zbiór

$$A = \{b \in P_0^+ :\ \forall\, a \in P_0^+ [a \oplus b = a + b]\}.$$

Ponieważ $a \oplus 0 = a = a + 0$ dla dowolnego $a \in P_0^+$, więc $0 \in A$. Niech $b \in A$, uzasadnimy, że $S(b) \in A$. Istotnie, $a \oplus S(b) = S(a \oplus b) = S(a + b) = (a + b) + 1 = a + (b + 1) = a + S(b)$ dla dowolnego $a \in P_0^+$. Z aksjomatu indukcji wynika, że $A = P_0^+$. Zatem spełniony jest warunek (a).

Analogicznie można udowodnić warunek (b).

Na mocy definicji 2.8 i twierdzenia 2.9 w modelu aksjomatyki Peana $(P_0^+, S, 0)$ określamy relację liniowo porządkującą $\leqslant^*$ następująco:

$$a \leqslant^* b \Longleftrightarrow \exists\, p \in P_0^+ [b = a + p]$$

dla $a, b \in P_0^+$. Zauważmy, że na podstawie twierdzenia 3.2(a_6) dla dowolnych $a, b \in P_0^+$ mamy: $a \leqslant b \Longleftrightarrow b - a \in P_0^+ \Longleftrightarrow \exists\, p \in P_0^+ [b = a + p] \Longleftrightarrow a \leqslant^* b$.

Udowodniliśmy (zob. definicja 2.10) następujące twierdzenie.

Twierdzenie 3.10

Niech $(P, +, \cdot, \leqslant)$ będzie uporządkowanym pierścieniem całkowitym spełniającym aksjomat indukcji. System $(P_0^+, S, 0, +, \cdot, \leqslant)$, gdzie P_0^+ i S są określone odpowiednio warunkami (3) i (4), jest uporządkowaną algebrą liczb naturalnych.

W dowodzie następnego twierdzenia o izomorfizmie uporządkowanych pierścieni całkowitych spełniających aksjomat indukcji wykorzystamy poniższe lematy.

Lemat 3.11

Niech $(P, +, \cdot, \leqslant)$ będzie uporządkowanym pierścieniem całkowitym. Wtedy

$$\forall\, a \in P [a \in P \setminus P_0^+ \Longleftrightarrow a < 0].$$

Dowód. Niech $a \in P$. Korzystając z prawa trychotomii (zob. twierdzenie 3.5) otrzymujemy:

$$\begin{aligned} a \in P \setminus P_0^+ &\Longleftrightarrow [a \in P \wedge a \notin P_0^+] \\ &\Longleftrightarrow [a \in P \wedge \sim (0 \leqslant a)] \\ &\Longleftrightarrow [a \in P \wedge \sim (0 < a \vee a = 0)] \\ &\Longleftrightarrow [a \in P \wedge a < 0]. \end{aligned}$$

Łatwo udowodnić trzy następujące lematy.

Lemat 3.12
Niech $(P, +, \cdot, \leqslant)$ *będzie uporządkowanym pierścieniem całkowitym. Wtedy*

$$\forall\, a \in P[(a \in P_0^+ \wedge a \neq 0) \Longleftrightarrow -a \in P \setminus P_0^+].$$

Lemat 3.13
Niech $(P, +, \cdot, \leqslant)$ *będzie uporządkowanym pierścieniem całkowitym. Wtedy*

$$\forall\, a \in P[a \in P \setminus P_0^+ \Longleftrightarrow (-a \in P_0^+ \wedge a \neq 0)].$$

Lemat 3.14
Niech $(P, +, \cdot, \leqslant)$ *będzie uporządkowanym pierścieniem całkowitym. Wtedy*

$$\forall\, a, b \in P[(a \in P \setminus P_0^+ \wedge b \in P_0^+) \Longrightarrow a < b].$$

Niech $(P, +, \cdot, \leqslant)$ i $(U, +, \cdot, \leqslant)$ będą uporządkowanymi pierścieniami całkowitymi spełniającymi aksjomat indukcji. Na mocy twierdzenia 3.10 rozważmy uporządkowane algebry liczb naturalnych $(P_0^+, S, 0, +, \cdot, \leqslant)$ i $(U_0^+, T, 0, +, \cdot, \leqslant)$. Na podstawie wzorów (2) i dowodu twierdzenia 2.14 funkcja $F_0 \colon P_0^+ \longrightarrow U_0^+$ taka, że:
(a_1) $F_0(0) = 0$,
(b_1) $F_0(S(p)) = T(F_0(p))$ dla każdego $p \in A$,
jest izomorfizmem uporządkowanych algebr liczb naturalnych $(P_0^+, S, 0, +, \cdot, \leqslant)$ i $(U_0^+, T, 0, +, \cdot, \leqslant)$.

Określamy funkcję $F \colon P \longrightarrow U$ następująco:

$$F(a) = \begin{cases} F_0(a) \text{ dla } a \in P_0^+, \\ -F_0(-a) \text{ dla } a \in P \setminus P_0^+. \end{cases}$$

Z lematu 3.13 wynika, że funkcja F jest dobrze określona.

Najpierw udowodnimy, że

$$F(-a) = -F(a)$$

dla $a \in P$. Niech $a \in P$. Rozważymy dwa przypadki:
(a) $a \in P_0^+$,
(b) $a \in P \setminus P_0^+$.
Jeżeli $a \in P_0^+$ i $a = 0$, to $F(-a) = F(0) = F_0(0) = 0 = -F(0) = -F(a)$. Jeżeli $a \in P_0^+$ i $a \neq 0$, to $-a \in P \setminus P_0^+$ na podstawie lematu 3.12. Stąd $F(-a) = -F_0(-(-a)) = -F_0(a) = -F(a)$. Jeżeli $a \in P \setminus P_0^+$, to $-a \in P_0^+$ na podstawie lematu 3.13. Stąd $F(-a) = F_0(-a)$ oraz $F(a) = -F_0(-a)$, czyli $-F(a) = F_0(-a)$, a więc $F(-a) = -F(a)$.

Udowodnimy, że $F \colon P \longrightarrow U$ jest izomorfizmem pierścieni uporządkowanych $(P, +, \cdot, \leqslant)$ i $(U, +, \cdot, \leqslant)$. Najpierw wykażemy, że F jest bijekcją. Niech $a_1, a_2 \in P$ oraz $F(a_1) = F(a_2)$. Jeżeli $a_1, a_2 \in P_0^+$, to $F_0(a_1) = F_0(a_2)$, czyli $a_1 = a_2$. Jeżeli $a_1, a_2 \in P \setminus P_0^+$, to:

$$\begin{aligned} F(a_1) = F(a_2) &\Longrightarrow -F_0(-a_1) = -F_0(-a_2) \\ &\Longrightarrow F_0(-a_1) = F_0(-a_2) \\ &\Longrightarrow -a_1 = -a_2 \\ &\Longrightarrow a_1 = a_2. \end{aligned}$$

Niech $a_1 \in P \setminus P_0^+$ i $a_2 \in P_0^+$. Oczywiście $a_1 \neq a_2$. Ponieważ $F(a_1) = -F_0(-a_1) \in U \setminus U_0^+$, gdyż $F_0(-a_1) \in U_0^+$ i $F_0(-a_1) \neq 0$, bo $a_1 \neq 0$ (zob. lemat 3.12) oraz $F(a_2) = F_0(a_2) \in U_0^+$, więc $F(a_1) \neq F(a_2)$. Zatem F jest injekcją. Następnie wykażemy, że F jest surjekcją. Niech $b \in U$. Jeżeli $b \in U_0^+$, to istnieje $a \in P_0^+$ takie, że $F_0(a) = b$. Stąd $F(a) = F_0(a) = b$. Niech $b \in U \setminus U_0^+$. Stąd $-b \in U_0^+$ oraz $-b \neq 0$ (zob. lemat 3.13). Istnieje $a \in P_0^+$ i $a \neq 0$ takie, że $F_0(a) = -b$. Ponieważ $-a \in P \setminus P_0^+$ (zob. lemat 3.12), więc $F(-a) = -F_0(-(-a)) = -F_0(a) = -(-b) = b$. Zatem F jest surjekcją, a w konsekwencji F jest bijekcją.

Udowodnimy, że

$$\forall\, a, b \in P[F(a + b) = F(a) + F(b)].$$

Jeżeli $a, b \in P_0^+$, to $a+b \in P_0^+$ (zob. twierdzenie 3.2(a_2)) oraz $F(a+b)=F_0(a+b)= F_0(a) + F_0(b) = F(a) + F(b)$. Jeżeli $a, b \in P \setminus P_0^+$, to $a + b \in P \setminus P_0^+$ (z lematu 3.11 i twierdzenia 3.4(a_4)) oraz $F(a + b) = -F_0(-(a + b)) = -F_0((-a) + (-b)) = -(F_0(-a) + F_0(-b)) = (-F_0(-a)) + (-F_0(-b)) = F(a) + F(b)$.
Niech $a \in P_0^+$ i $b \in P \setminus P_0^+$. Rozważmy dwa przypadki:
(a) $a + b \in P_0^+$,
(b) $a + b \in P \setminus P_0^+$.
Niech $a + b \in P_0^+$, a więc $a + b = p$ dla pewnego $p \in P_0^+$. Stąd $p + (-b) = a$, więc $F(a)=F(p+(-b))=F_0(p+(-b))=F_0(p)+F_0(-b) = F(p)+F(-b) = F(p)-F(b)$, czyli $F(p) = F(a)+F(b)$, tzn. $F(a+b) = F(a)+F(b)$. Niech $a+b \in P \setminus P_0^+$, a więc $a + b = p$ dla pewnego $p \in P \setminus P_0^+$. Stąd $(-a) + (-b) = -p$, czyli $-b = (-p) + a$.

Mamy:

$$F(-b) = F_0((-p) + a) = F_0(-p) + F_0(a) = F(-p) + F(a) = -F(p) + F(a).$$

Wobec tego

$$F(-b) = -F(p) + F(a),$$

czyli

$$F(p) = F(a) + F(b),$$

a więc

$$F(a + b) = F(a) + F(b).$$

Podobnie możemy uzasadnić, że

$$\forall\, a, b \in P[F(a \cdot b) = F(a) \cdot F(b)].$$

Wykażemy, że

$$\forall\, a, b \in P[a \leqslant b \Longleftrightarrow F(a) \leqslant F(b)].$$

Rozważmy następujące przypadki:
(a) Jeżeli $a, b \in P_0^+$, to $a \leqslant b \Longleftrightarrow F_0(a) \leqslant F_0(b) \Longleftrightarrow F(a) \leqslant F(b)$.
(b) Jeżeli $a, b \in P \setminus P_0^+$, to $a \leqslant b \Longleftrightarrow -b \leqslant -a \Longleftrightarrow F_0(-b) \leqslant F_0(-a) \Longleftrightarrow -F_0(-a) \leqslant -F_0(-b) \Longleftrightarrow F(a) \leqslant F(b)$.

Przed rozważeniem trzeciego przypadku uzasadnimy pewne dodatkowe własności funkcji F.

Udowodnimy, że dla dowolnego $a \in P$ mamy:

$$a \in P \setminus P_0^+ \Longleftrightarrow F(a) \in U \setminus U_0^+.$$

Niech $a \in P \setminus P_0^+$. Gdyby $F(a) \in U_0^+$, to istniałby element $b \in P_0^+$ taki, że $F_0(b) = F(a)$, czyli $F(b) = F(a)$, a więc $b = a$, co jest niemożliwe. Stąd $F(a) \in U \setminus U_0^+$. Odwrotnie, niech $F(a) \in U \setminus U_0^+$. Gdyby $a \in P_0^+$, to $F_0(a) \in U_0^+$, a więc $F(a) \in U_0^+$, co jest niemożliwe.

Zatem otrzymujemy następujący warunek:

$$\forall\, a, b \in P[(a \in P \setminus P_0^+ \wedge b \in P_0^+) \Longleftrightarrow (F(a) \in U \setminus U_0^+ \wedge F(b) \in U_0^+)]. \qquad (5)$$

(c) Jeżeli $a \in P \setminus P_0^+$ i $b \in P_0^+$, to nierówności $a \leqslant b$ i $F(a) \leqslant F(b)$ są prawdziwe (zob. lemat 3.14 i warunek (5)), czyli $a \leqslant b \Longleftrightarrow F(a) \leqslant F(b)$. Jeżeli $b \in P \setminus P_0^+$ i $a \in P_0^+$, to nierówności $a \leqslant b$ i $F(a) \leqslant F(b)$ są fałszywe (zob. lemat 3.14, twierdzenie 3.5 i warunek (5)), czyli $a \leqslant b \Longleftrightarrow F(a) \leqslant F(b)$.

Udowodniliśmy następujące

Twierdzenie 3.15
Jeżeli $(P, +, \cdot, \leqslant)$ i $(U, +, \cdot, \leqslant)$ są uporządkowanymi pierścieniami całkowitymi spełniającymi aksjomat indukcji, to uporządkowane pierścienie $(P, +, \cdot, \leqslant)$ i $(U, +, \cdot, \leqslant)$ są izomorficzne.

Na mocy twierdzeń 3.15 i 3.9 otrzymujemy następujący

Wniosek 3.16
Każdy uporządkowany pierścień całkowity $(P, +, \cdot, \leqslant)$ spełniający aksjomat indukcji jest izomorficzny z uporządkowanym pierścieniem całkowitym $(\mathcal{Z}_N, +, \cdot, \leqslant)$ liczb całkowitych.

Na mocy wniosku 3.16 możemy przyjąć następującą definicję.

Definicja 3.17
Każdy uporządkowany pierścień całkowity spełniający aksjomat indukcji nazywamy *uporządkowanym pierścieniem liczb całkowitych.*

Na podstawie wniosku 3.16 i definicji 3.17 otrzymujemy następujący

Wniosek 3.18
Istnieje tylko jeden, z dokładnością do izomorfizmu, uporządkowany pierścień liczb całkowitych.

Korzystając z wniosku 3.18 możemy przyjąć tradycyjny zapis $(\mathcal{Z}, +, \cdot, \leqslant)$ dla uporządkowanego pierścienia liczb całkowitych.

W dalszym ciągu tego paragrafu zajmiemy się izomorficznym zanurzeniem uporządkowanego pierścienia $(\mathcal{Z}, +, \cdot, \leqslant)$ liczb całkowitych w dowolnym uporządkowanym pierścieniu całkowitym $(P, +, \cdot, \leqslant)$. Zaczniemy od lematów, które będą wykorzystane w dalszych rozważaniach.

Lemat 3.19

Niech $(\mathcal{Z}, +, \cdot, \leqslant)$ będzie uporządkowanym pierścieniem liczb całkowitych. Wtedy dla dowolnych liczb całkowitych $m, n \in \mathcal{Z}$ spełnione są warunki:

(a) $|m+n| = |m| + |n| \Longleftrightarrow [(m \geqslant 0 \wedge n \geqslant 0) \vee (m \leqslant 0 \wedge n \leqslant 0)]$,

(b) $|m+n| < |m| + |n| \Longleftrightarrow [(m > 0 \wedge n < 0) \vee (m < 0 \wedge n > 0)]$.

Dowód. Niech $m, n \in \mathcal{Z}$. Jeżeli $m \geqslant 0$ i $n \geqslant 0$ lub $m \leqslant 0$ i $n \leqslant 0$, to łatwo sprawdzić, że $|m+n| = |m| + |n|$.

Niech $m > 0$ i $n < 0$. Stąd $|m| = m$ i $|n| = -n$. Mamy $|m| + |n| = m + |n|$. Ponadto $m + n = m - |n|$. Jeżeli $m - |n| \geqslant 0$, to $|m+n| = |m - |n|| = m - |n|$. Ponieważ $-|n| < |n|$, więc $|m+n| = m - |n| < m + |n| = |m| + |n|$. Jeżeli $m - |n| < 0$, to $|m+n| = |m - |n|| = -(m - |n|) = |n| - m$. Ponieważ $-m < m$, więc $|m+n| = |n| - m < m + |n| = |m| + |n|$. Dowód w przypadku, gdy $m < 0$ i $n > 0$ jest analogiczny.

Niech $(P, +, \cdot)$ będzie pierścieniem oraz $a \in P$ i $m \in \mathcal{Z}$. Przyjmujemy:

$$m \cdot a = \begin{cases} \underbrace{a + a + \ldots + a}_{m} \text{ dla } m > 0, \\ 0 \text{ dla } m = 0, \\ \underbrace{(-a) + (-a) + \ldots + (-a)}_{|m|} \text{ dla } m < 0. \end{cases}$$

Lemat 3.20

Niech $(P, +, \cdot)$ będzie pierścieniem. Wtedy

$$\forall\, a \in P\; \forall\, m, n \in \mathcal{Z} [(m+n) \cdot a = m \cdot a + n \cdot a].$$

Dowód. Rozważymy przypadek, gdy $m > 0$ i $n < 0$. Ponieważ $n = -|n|$, więc $m + n = m - |n|$.

(a) Zakładamy, że $m + n > 0$, czyli $m > |n|$. Wtedy mamy:

$$\begin{aligned} m \cdot a + n \cdot a &= \underbrace{a + a + \ldots + a}_{m} + \underbrace{(-a) + (-a) + \ldots + (-a)}_{|n|} \\ &= \underbrace{(a + (-a)) + (a + (-a)) + \ldots + (a + (-a))}_{m} + \underbrace{a + a + \ldots + a}_{m-|n|} \\ &= \underbrace{a + a + \ldots + a}_{m-|n|} \\ &= \underbrace{a + a + \ldots + a}_{m+n} \\ &= (m+n) \cdot a. \end{aligned}$$

(b) Zakładamy, że $m+n<0$, czyli $m<|n|$. Wtedy mamy:

$$\begin{aligned} m\cdot a+n\cdot a &= \underbrace{a+a+...+a}_{m}+\underbrace{(-a)+(-a)+...+(-a)}_{|n|} \\ &= \underbrace{(a+(-a))+(a+(-a))+...+(a+(-a))}_{m}+\underbrace{(-a)+(-a)+...+(-a)}_{|n|-m} \\ &= \underbrace{(-a)+(-a)+...+(-a)}_{|n|-m} \\ &= \underbrace{(-a)+(-a)+...+(-a)}_{-(m-|n|)} \\ &= \underbrace{(-a)+(-a)+...+(-a)}_{|m-|n||} \\ &= \underbrace{(-a)+(-a)+...+(-a)}_{|m+n|} \\ &= (m+n)\cdot a. \end{aligned}$$

(c) Zakładamy, że $m+n=0$, czyli $m=|n|$. Wtedy mamy: $(m+n)\cdot a=0\cdot a=0$ oraz

$$\begin{aligned} m\cdot a+n\cdot a &= \underbrace{a+a+...+a}_{m}+\underbrace{(-a)+(-a)+...+(-a)}_{|n|} \\ &= \underbrace{(a+(-a))+(a+(-a))+...+(a+(-a))}_{m} \\ &= 0. \end{aligned}$$

Zatem $(m+n)\cdot a=m\cdot a+n\cdot a$.

Uzasadnienie pozostałych możliwych przypadków pozostawiamy Czytelnikowi.

Lemat 3.21
Niech $(P,+,\cdot)$ będzie pierścieniem. Wtedy

$$\forall\, a\in P\,\forall\, m\in\mathcal{Z}[(-m)\cdot a=-(m\cdot a)=m\cdot(-a)].$$

Łatwy dowód tego lematu pozostawiamy Czytelnikowi.

Lemat 3.22
Niech $(P,+,\cdot)$ będzie pierścieniem. Wtedy

$$\forall\, a\in P\,\forall\, m,n\in\mathcal{Z}[(m-n)\cdot a=m\cdot a-n\cdot a].$$

Łatwy dowód tego lematu pozostawiamy Czytelnikowi.

Proponujemy Czytelnikowi znaleźć przykład (związany z następnymi dwoma lematami i twierdzeniem) pierścienia $(P,+,\cdot)$ z jednością, w którym istnieje element $a\in P\setminus\{1\}$ taki, że $a^2=a$ oraz $m\cdot a\neq 0$ dla każdego $m\in\mathcal{Z}\setminus\{0\}$.

Lemat 3.23
Niech $(P, +, \cdot)$ *będzie pierścieniem. Jeżeli* $a \in P$ *jest elementem takim, że* $a^2 = a$, *to*

$$\forall\, m, n \in \mathcal{Z}[(mn) \cdot a = (m \cdot a)(n \cdot a)].$$

Powyższy lemat łatwo udowodnić rozważając stosowne przypadki dla a, m i n.

Lemat 3.24
Niech $(P, +, \cdot)$ *będzie pierścieniem. Jeżeli* $a \in P$ *jest elementem takim, że* $a^2 = a$, *to podzbiór*

$$P_a = \{m \cdot a \colon m \in \mathcal{Z}\}$$

jest przemiennym podpierścieniem z jednością pierścienia $(P, +, \cdot)$.

Dowód. Z określenia podzbioru P_a wynika, że $a \in P_a$. Niech $m \cdot a, n \cdot a \in P_a$. Z lematu 3.22 wynika, że $m \cdot a - n \cdot a = (m - n) \cdot a \in P_a$. Z lematu 3.23 wynika, że $(m \cdot a)(n \cdot a) = (mn) \cdot a \in P_a$. Wobec tego P_a jest podpierścieniem pierścienia $(P, +, \cdot)$. Ponieważ $(m \cdot a)(n \cdot a) = (mn) \cdot a = (nm) \cdot a = (n \cdot a)(m \cdot a)$ oraz $a(m \cdot a) = (1 \cdot a)(m \cdot a) = (1 \cdot m) \cdot a = m \cdot a$, więc podpierścień P_a jest przemienny i jego jednością jest element a.

Twierdzenie 3.25
Niech $(P, +, \cdot)$ *będzie pierścieniem. Niech* $a \in P$ *będzie elementem takim, że* $a^2 = a$ *oraz*

$$\forall\, m \in \mathcal{N}_1[m \cdot a \neq 0].$$

Wtedy pierścienie $(\mathcal{Z}, +, \cdot)$ *liczb całkowitych oraz* $(P_a, +, \cdot)$ *są izomorficzne.*

Dowód. Zauważmy, że $a \neq 0$. Określamy funkcję $\varphi \colon \mathcal{Z} \longrightarrow P_a$ następująco:

$$\varphi(m) = m \cdot a$$

dla $m \in \mathcal{Z}$. Korzystając z lematów 3.20 i 3.23 dla dowolnych $m, n \in \mathcal{Z}$ mamy: $\varphi(m + n) = (m + n) \cdot a = m \cdot a + n \cdot a = \varphi(m) + \varphi(n)$; $\varphi(mn) = (mn) \cdot a = (m \cdot a)(n \cdot a) = \varphi(m)\varphi(n)$. Wobec tego φ jest homomorfizmem. Niech $m \cdot a \in P_a$, wtedy $\varphi(m) = m \cdot a$, czyli φ jest surjekcją. Uzasadnimy, że φ jest injekcją. Najpierw zauważmy, że

$$\forall\, m \in \mathcal{Z} \setminus \{0\}[m \cdot a \neq 0].$$

Istotnie, jeżeli $m \in \mathcal{N}_1$, to korzystając z lematu 3.21 mamy: $(-m) \cdot a = -(m \cdot a) \neq 0$. Niech $m, n \in \mathcal{Z}$, wtedy stosując lemat 3.22 mamy: $\varphi(m) = \varphi(n) \Longrightarrow m \cdot a = n \cdot a \Longrightarrow m \cdot a - n \cdot a = 0 \Longrightarrow (m - n) \cdot a = 0 \Longrightarrow m - n = 0 \Longrightarrow m = n$. Zatem φ jest izomorfizmem. Dowód twierdzenia został zakończony.

Jeżeli $(P, +, \cdot)$ jest pierścieniem z jednością 1 , to

$$P_1 = \{m \cdot 1 \colon m \in \mathcal{Z}\}. \tag{6}$$

Z twierdzenia 3.25 wynika następujący

Wniosek 3.26
Niech $(P, +, \cdot)$ *będzie pierścieniem z jednością* 1 *takim, że*

$$\forall\, m \in \mathcal{N}_1 [m \cdot 1 \neq 0].$$

Wtedy pierścienie $(\mathcal{Z}, +, \cdot)$ *liczb całkowitych oraz* $(P_1, +, \cdot)$ *są izomorficzne.*

Łatwo udowodnić trzy poniższe lematy.

Lemat 3.27
Niech $(P, +, \cdot, \leqslant)$ *będzie uporządkowanym pierścieniem całkowitym. Dla dowolnych* $a \in P$, $a > 0$, $m \in \mathcal{Z}$ *spełnione są warunki:*
(a) $m \cdot a > 0 \Longleftrightarrow m > 0$,
(b) $m \cdot a < 0 \Longleftrightarrow m < 0$,
(c) $m \cdot a = 0 \Longleftrightarrow m = 0$.

Lemat 3.28
Niech $(P, +, \cdot, \leqslant)$ *będzie uporządkowanym pierścieniem całkowitym. Dla dowolnych* $a \in P$, $a < 0$, $m \in \mathcal{Z}$ *spełnione są warunki:*
(a) $m \cdot a > 0 \Longleftrightarrow m < 0$,
(b) $m \cdot a < 0 \Longleftrightarrow m > 0$,
(c) $m \cdot a = 0 \Longleftrightarrow m = 0$.

Lemat 3.29
Niech $(P, +, \cdot, \leqslant)$ *będzie uporządkowanym pierścieniem całkowitym. Dla dowolnych* $a \in P$, $m, n \in \mathcal{Z}$ *spełnione są warunki:*
(a) *Jeżeli* $a > 0$, *to*

$$m \cdot a \leqslant n \cdot a \Longleftrightarrow m \leqslant n.$$

(b) *Jeżeli* $a < 0$, *to*

$$m \cdot a \leqslant n \cdot a \Longleftrightarrow m \geqslant n.$$

Niech $(P, +, \cdot, \leqslant)$ będzie uporządkowanym pierścieniem całkowitym. Przypomnijmy (zob. (6)), że

$$P_1 = \{m \cdot 1 \colon m \in \mathcal{Z}\}.$$

Lemat 3.30
Niech $(P, +, \cdot, \leqslant)$ *będzie uporządkowanym pierścieniem całkowitym. Wtedy* $(P_1, +, \cdot, \leqslant|_{P_1})$ *jest uporządkowanym podpierścieniem całkowitym uporządkowanego pierścienia całkowitego* $(P, +, \cdot, \leqslant)$.

Dowód. Z lematu 3.24 wynika, że $(P_1, +, \cdot)$ jest podpierścieniem całkowitym pierścienia całkowitego $(P, +, \cdot, \leqslant)$. Oczywiście $(P_1, +, \cdot, \leqslant|_{P_1})$ jest uporządkowanym podpierścieniem całkowitym uporządkowanego pierścienia całkowitego $(P, +, \cdot, \leqslant)$.

Uwaga: Zamiast $\leqslant|_{P_1}$ będziemy pisać $\leqslant$.

Twierdzenie 3.31
Niech $(P, +, \cdot, \leqslant)$ będzie uporządkowanym pierścieniem całkowitym. Wtedy uporządkowany pierścień $(\mathcal{Z}, +, \cdot, \leqslant)$ liczb całkowitych i uporządkowany pierścień całkowity $(P_1, +, \cdot, \leqslant)$ są izomorficzne.

Dowód. Z twierdzenia 3.4(a_7),(a_4) wynika, że $n \cdot 1 > 0$ dla każdego $n \in \mathcal{N}_1$. Wobec tego pierścienie $(\mathcal{Z}, +, \cdot)$ i $(P_1, +, \cdot)$ są izomorficzne na mocy wniosku 3.26. Na podstawie dowodu twierdzenia 3.25 wnioskujemy, że funkcja $\varphi\colon \mathcal{Z} \longrightarrow P_1$ określona wzorem

$$\varphi(m) = m \cdot 1$$

dla $m \in \mathcal{Z}$, jest izomorfizmem pierścieni $(\mathcal{Z}, +, \cdot)$ i $(P_1, +, \cdot)$. Z twierdzenia 3.4(a_7) i lematu 3.29(a) wynika, że: $m \leqslant n \Longleftrightarrow m \cdot 1 \leqslant n \cdot 1 \Longleftrightarrow \varphi(m) \leqslant \varphi(n)$ dla dowolnych $m, n \in \mathcal{Z}$. Zatem uporządkowane pierścienie $(\mathcal{Z}, +, \cdot, \leqslant)$ i $(P_1, +, \cdot, \leqslant)$ są izomorficzne.

Z twierdzenia 3.31 wynika następujący

Wniosek 3.32
Każdy uporządkowany pierścień całkowity $(P, +, \cdot, \leqslant)$ zawiera, z dokładnością do izomorfizmu, uporządkowany pierścień $(\mathcal{Z}, +, \cdot, \leqslant)$ liczb całkowitych.

Wniosek 3.33
W uporządkowanym pierścieniu $(\mathcal{Z}, +, \cdot, \leqslant)$ liczb całkowitych relacja porządkująca $\leqslant$ jest określona jednoznacznie, tzn. jeśli $(\mathcal{Z}, +, \cdot, \leqslant)$ i $(\mathcal{Z}, +, \cdot, \leqslant^*)$ są uporządkowanymi pierścieniami liczb całkowitych, to relacje $\leqslant$ i $\leqslant^*$ są identyczne.

Dowód. Zauważmy, że $\mathcal{Z}_1 = \{m \cdot 1 \colon m \in \mathcal{Z}\} = \mathcal{Z}$. Na podstawie dowodu twierdzenia 3.31 wiemy, że funkcja $\varphi\colon \mathcal{Z} \longrightarrow \mathcal{Z}$ określona wzorem

$$\varphi(m) = m \cdot 1$$

dla $m \in \mathcal{Z}$, jest izomorfizmem uporządkowanych pierścieni $(\mathcal{Z}, +, \cdot, \leqslant)$ i $(\mathcal{Z}, +, \cdot, \leqslant^*)$. Ponieważ $\varphi(m) = m$ dla $m \in \mathcal{Z}$, więc $m \leqslant n \Longleftrightarrow \varphi(m) \leqslant^* \varphi(n) \Longleftrightarrow m \leqslant^* n$ dla $m, n \in \mathcal{Z}$. Zatem $\leqslant\, = \,\leqslant^*$.

4. Ciało uporządkowane liczb wymiernych

Głównymi pojęciami w tej części artykułu są: ciało uporządkowane, ciało uporządkowane elementów wymiernych ciała uporządkowanego, ciało uporządkowane liczb wymiernych. Podstawowymi twierdzeniami są: twierdzenie o izomorficznym zanurzeniu ciała uporządkowanego liczb wymiernych w dowolnym ciele uporządkowanym, twierdzenie o izomorfizmie ciał uporządkowanych liczb wymiernych.

Definicja 4.1
Jeżeli uporządkowany pierścień całkowity $(K, +, \cdot, \leqslant)$ jest taki, że $(K, +, \cdot)$ jest ciałem, to $(K, +, \cdot, \leqslant)$ nazywamy *ciałem uporządkowanym*.

Izomorfizm ciał uporządkowanych będziemy rozumieć zgodnie z definicją 3.6.

Łatwo udowodnić poniższe cztery lematy o podstawowych własnościach ciał uporządkowanych, które będą wykorzystywane w dalszej części artykułu.

Lemat 4.2
Niech $(K, +, \cdot, \leqslant)$ *będzie ciałem uporządkowanym. Wtedy spełnione są następujące warunki:*
(a) $\forall\, a \in K[a > 0 \Longleftrightarrow a^{-1} > 0]$,
(b) $\forall\, a \in K[a < 0 \Longleftrightarrow a^{-1} < 0]$,
(c) $\forall\, a \in K\, \forall\, b \in K \setminus \{0\}[ab \geqslant 0 \Longleftrightarrow ab^{-1} \geqslant 0]$.

Lemat 4.3
Jeżeli $(K, +, \cdot, \leqslant)$ *jest ciałem uporządkowanym, to zbiór* $(K, \leqslant)$ *jest gęsto uporządkowany.*

Lemat 4.4
Niech $F\colon K \longrightarrow L$ *będzie izomorfizmem ciał uporządkowanych* $(K, +, \cdot, \leqslant)$ *oraz* $(L, +, \cdot, \leqslant)$*, natomiast niech* $G\colon L \longrightarrow M$ *będzie izomorfizmem ciał uporządkowanych* $(L, +, \cdot, \leqslant\ )$ *oraz* $(M, +, \cdot, \leqslant)$*. Wtedy* $G \circ F\colon K \longrightarrow M$ *jest izomorfizmem ciał uporządkowanych* $(K, +, \cdot, \leqslant)$ *i* $(M, +, \cdot, \leqslant)$*.*

Lemat 4.5
Niech $F\colon K \longrightarrow L$ *będzie izomorfizmem ciał uporządkowanych* $(K, +, \cdot, \leqslant)$ *oraz* $(L, +, \cdot, \leqslant)$*. Wtedy* $F^{-1}\colon L \longrightarrow K$ *jest izomorfizmem ciał uporządkowanych* $(L, +, \cdot, \leqslant)$ *i* $(K, +, \cdot, \leqslant)$*.*

W następnym lemacie zostanie użyte pojęcie wartości bezwzględnej w ciele uporządkowanym zgodnie z definicją tego pojęcia zamieszczoną w książce (Cohen, Ehrlich, 1963, definicja 3.6, s. 68).

Lemat 4.6
Niech $F\colon K \longrightarrow L$ *będzie izomorfizmem ciał uporządkowanych* $(K, +, \cdot, \leqslant)$ *oraz* $(L, +, \cdot, \leqslant)$*. Wtedy*
$$\forall\, a \in K[F(|a|) = |F(a)|.$$

Dowód. Niech $a \in K$. Jeżeli $a \geqslant 0$, to $F(a) \geqslant 0$. Stąd $F(|a|) = F(a) = |F(a)|$. Jeżeli $a < 0$, to $F(a) < 0$. Stąd $F(|a|) = F(-a) = -F(a) = |F(a)|$.

Lemat 4.7
Niech $(K, +, \cdot, \leqslant)$ *i* $(L, +, \cdot, \leqslant)$ *będą ciałami uporządkowanymi. Niech* $F\colon K \longrightarrow L$ *będzie injekcją taką, że:*
(a) $\forall\, a, b \in K[F(a + b) = F(a) + F(b)]$,
(b) $\forall\, a \in K[a \in K^+ \Longleftrightarrow F(a) \in L^+]$.
Wtedy
$$\forall\, a, b \in K[a < b \Longleftrightarrow F(a) < F(b)].$$

Dowód. Zauważmy, że $F(0) = F(0+0) = F(0)+F(0)$, czyli $F(0) = 0$. Niech $a \in K$ i $F(a) = 0$. Wtedy $F(a) = 0 = F(0)$, stąd $a = 0$. Uzasadnimy, że $F(-a) = -F(a)$ dla każdego $a \in K$. Istotnie, $0 = F(0) = F(a + (-a)) = F(a) + F(-a)$. Stąd $F(-a) = -F(a)$. Wykażemy, że $F(a - b) = F(a) - F(b)$ dla dowolnych $a, b \in K$. Rzeczywiście, $F(a - b) = F(a + (-b)) = F(a) + F(-b) = F(a) - F(b)$. Dla dowolnych $a, b \in K$ mamy: $a < b \Longleftrightarrow b - a > 0 \Longleftrightarrow F(b - a) > 0 \Longleftrightarrow F(b) - F(a) > 0 \Longleftrightarrow F(a) < F(b)$.

Na bazie arytmetyki liczb całkowitych możemy skonstruować za pomocą odpowiedniej relacji równoważności zbiór $\mathcal{Q}_Z$ liczb wymiernych. W zbiorze $\mathcal{Q}_Z$ określamy dodawanie $+$, mnożenie $\cdot$ oraz relację $\leqslant$ liniowego porządku.

Na podstawie konstrukcji liczb wymiernych i twierdzeń zamieszczonych w książce (Chronowski, 1999b, podrozdziały 1.1-1.3), możemy sformułować następujące twierdzenie.

Twierdzenie 4.8
System $(\mathcal{Q}_Z, +, \cdot, \leqslant)$ jest ciałem uporządkowanym.

Uwaga: W książce (Chronowski, 1999b) zamiast symbolu $\mathcal{Q}_Z$ występuje symbol Q zbioru liczb wymiernych.

Lemat 4.9
Niech $(K, +, \cdot, \leqslant)$ będzie ciałem uporządkowanym. Niech

$$\mathcal{Q}_K = \left\{ \frac{m \cdot 1}{n \cdot 1} : \frac{m}{n} \in \mathcal{Q}_Z \right\}.$$

Wtedy $(\mathcal{Q}_K, +, \cdot, \leqslant |_{\mathcal{Q}_K})$ jest podciałem uporządkowanym ciała uporządkowanego $(K, +, \cdot, \leqslant)$.

Dowód. Zamiast $\leqslant |_{\mathcal{Q}_K}$ będziemy pisać $\leqslant$. Niech $\frac{m \cdot 1}{n \cdot 1}, \frac{k \cdot 1}{l \cdot 1} \in \mathcal{Q}_K$.
Korzystając z lematów 3.22 i 3.23 otrzymujemy:

(a) $\frac{m \cdot 1}{n \cdot 1} - \frac{k \cdot 1}{l \cdot 1} = \frac{(m \cdot 1)(l \cdot 1) - (k \cdot 1)(n \cdot 1)}{(n \cdot 1)(l \cdot 1)} = \frac{(ml - kn) \cdot 1}{(nl) \cdot 1} \in \mathcal{Q}_K$.

(b) $\frac{m \cdot 1}{n \cdot 1} \cdot \frac{k \cdot 1}{l \cdot 1} = \frac{(mk) \cdot 1}{(nk) \cdot 1} \in \mathcal{Q}_K$.

(c) Niech $m \neq 0$. Wtedy $(\frac{m \cdot 1}{n \cdot 1})^{-1} = \frac{n \cdot 1}{m \cdot 1} \in \mathcal{Q}_K$.

Zatem $(\mathcal{Q}_K, +, \cdot, \leqslant)$ jest podciałem uporządkowanym ciała uporządkowanego $(K, +, \cdot, \leqslant)$.

Na mocy lematu 4.9 możemy przyjąć następującą definicję.

Definicja 4.10
Ciało uporządkowane $(\mathcal{Q}_K, +, \cdot, \leqslant)$ nazywamy *ciałem uporządkowanym elementów wymiernych* ciała uporządkowanego $(K, +, \cdot, \leqslant)$.

Twierdzenie 4.11
Niech $(K, +, \cdot, \leqslant)$ będzie ciałem uporządkowanym. Wtedy ciało uporządkowane $(\mathcal{Q}_Z, +, \cdot, \leqslant)$ liczb wymiernych i ciało uporządkowane elementów wymiernych $(\mathcal{Q}_K, +, \cdot, \leqslant)$ są izomorficzne.

Dowód. Określamy funkcję $F\colon \mathcal{Q}_Z \longrightarrow \mathcal{Q}_K$ następująco:

$$F\left(\frac{m}{n}\right) = \frac{m \cdot 1}{n \cdot 1}$$

dla $\frac{m}{n} \in \mathcal{Q}_Z$. Korzystając z lematów 3.20, 3.22, 3.23 dla dowolnych $\frac{m}{n}, \frac{k}{l} \in \mathcal{Q}_Z$ otrzymujemy:

(a) $F(\frac{m}{n} + \frac{k}{l}) = F(\frac{ml+kn}{nl}) = \frac{(ml+kn)\cdot 1}{(nl)\cdot 1} = \frac{(m\cdot 1)(l\cdot 1)+(k\cdot 1)(n\cdot 1)}{(n\cdot 1)(l\cdot 1)} = \frac{m\cdot 1}{n\cdot 1} + \frac{k\cdot 1}{l\cdot 1} = F(\frac{m}{n}) + F(\frac{k}{l})$;

(b) $F(\frac{m}{n} \cdot \frac{k}{l}) = F(\frac{mk}{nl}) = \frac{(mk)\cdot 1}{(nl)\cdot 1} = \frac{(m\cdot 1)(k\cdot 1)}{(n\cdot 1)(l\cdot 1)} = \frac{m\cdot 1}{n\cdot 1} \cdot \frac{k\cdot 1}{l\cdot 1} = F(\frac{m}{n}) \cdot F(\frac{k}{l})$.

Uzasadnimy, że F jest injekcją. Niech $F(\frac{m}{n}) = F(\frac{k}{l})$, gdzie $\frac{m}{n}, \frac{k}{l} \in \mathcal{Q}_Z$. Korzystając z lematów 3.22, 3.23 i 3.27(c) otrzymujemy:

$$\begin{aligned}
F\left(\frac{m}{n}\right) = F\left(\frac{k}{l}\right) &\Longrightarrow \frac{m \cdot 1}{n \cdot 1} = \frac{k \cdot 1}{l \cdot 1} \\
&\Longrightarrow (m \cdot 1)(l \cdot 1) = (k \cdot 1)(n \cdot 1) \\
&\Longrightarrow (ml) \cdot 1 = (kn) \cdot 1 \Longrightarrow (ml) \cdot 1 - (kn) \cdot 1 = 0 \\
&\Longrightarrow (ml - kn) \cdot 1 = 0 \Longrightarrow ml - kn = 0 \\
&\Longrightarrow ml = kn \\
&\Longrightarrow \frac{m}{n} = \frac{k}{l}.
\end{aligned}$$

Łatwo zauważyć, że F jest surjekcją, a więc F jest bijekcją. Wykażemy, że: $\frac{m}{n} \leqslant \frac{k}{l} \Longleftrightarrow F(\frac{m}{n}) \leqslant F(\frac{k}{l})$ dla dowolnych $\frac{m}{n}, \frac{k}{l} \in \mathcal{Q}_Z$. Korzystając z lematów 3.22, 3.23, 3.27, 4.2(c) otrzymujemy:

$$\begin{aligned}
F\left(\frac{m}{n}\right) \leqslant F\left(\frac{k}{l}\right) &\Longleftrightarrow \frac{m \cdot 1}{n \cdot 1} \leqslant \frac{k \cdot 1}{l \cdot 1} \\
&\Longleftrightarrow \frac{k \cdot 1}{l \cdot 1} - \frac{m \cdot 1}{n \cdot 1} \geqslant 0 \\
&\Longleftrightarrow \frac{(k \cdot 1)(n \cdot 1) - (l \cdot 1)(m \cdot 1)}{(l \cdot 1)(n \cdot 1)} \geqslant 0 \\
&\Longleftrightarrow \frac{(kn - lm) \cdot 1}{(ln) \cdot 1} \geqslant 0 \\
&\Longleftrightarrow [(kn - lm) \cdot 1][(ln) \cdot 1]^{-1} \geqslant 0 \\
&\Longleftrightarrow [(kn - lm) \cdot 1][(ln) \cdot 1] \geqslant 0 \\
&\Longleftrightarrow [(kn - lm)(ln)] \cdot 1 \geqslant 0 \\
&\Longleftrightarrow (kn - lm)(ln) \geqslant 0 \\
&\Longleftrightarrow (kn - lm)(ln)^{-1} \geqslant 0 \\
&\Longleftrightarrow \frac{kn - lm}{ln} \geqslant 0 \\
&\Longleftrightarrow \frac{k}{l} - \frac{m}{n} \geqslant 0 \\
&\Longleftrightarrow \frac{m}{n} \leqslant \frac{k}{l}.
\end{aligned}$$

Zatem F jest izomorfizmem ciał uporządkowanych $(\mathcal{Q}_Z, +, \cdot, \leqslant)$ i $(\mathcal{Q}_K, +, \cdot, \leqslant)$.

Z twierdzenia 4.11 wynika następujący

Wniosek 4.12
Każde ciało uporządkowane $(K, +, \cdot, \leqslant)$ zawiera, z dokładnością do izomorfizmu, ciało uporządkowane $(\mathcal{Q}_Z, +, \cdot, \leqslant)$ liczb wymiernych.

Na podstawie twierdzenia 4.11 możemy przyjąć następującą definicję.

Definicja 4.13
Każde ciało uporządkowane $(K, +, \cdot, \leqslant)$ takie, że $K = \mathcal{Q}_K$ nazywamy *uporządkowanym ciałem liczb wymiernych.*

Na mocy twierdzenia 4.11 oraz lematów 4.4 i 4.5 możemy sformułować następujące wnioski:

Wniosek 4.14
Dowolne dwa ciała uporządkowane liczb wymiernych są izomorficzne.

Wniosek 4.15
Istnieje tylko jedno, z dokładnością do izomorfizmu, ciało uporządkowane liczb wymiernych.

Na mocy wniosku 4.15 możemy przyjąć tradycyjny zapis $(\mathcal{Q}, +, \cdot, \leqslant)$ dla ciała uporządkowanego liczb wymiernych.

Z wniosków 4.12 i 4.15 wynika następujący

Wniosek 4.16
Każde ciało uporządkowane $(K, +, \cdot, \leqslant)$ zawiera, z dokładnością do izomorfizmu, ciało uporządkowane $(\mathcal{Q}, +, \cdot, \leqslant)$ liczb wymiernych.

Wniosek 4.17
W ciele uporządkowanym $(\mathcal{Q}, +, \cdot, \leqslant)$ liczb wymiernych relacja porządkująca $\leqslant$ jest określona jednoznacznie, tzn. jeśli $(\mathcal{Q}, +, \cdot, \leqslant)$ i $(\mathcal{Q}, +, \cdot, \leqslant^*)$ są ciałami uporządkowanymi liczb wymiernych, to relacje $\leqslant$ i $\leqslant^*$ są identyczne.

Dowód. Zauważmy, że

$$\mathcal{Q}_Q = \left\{ \frac{m \cdot 1}{n \cdot 1} : \frac{m}{n} \in \mathcal{Q} \right\} = \mathcal{Q}.$$

Na podstawie dowodu twierdzenia 4.11 wiemy, że funkcja $F \colon \mathcal{Q} \longrightarrow \mathcal{Q}$ określona wzorem

$$F\left(\frac{m}{n}\right) = \frac{m \cdot 1}{n \cdot 1}$$

dla $\frac{m}{n} \in \mathcal{Q}$, jest izomorfizmem ciał uporządkowanych $(\mathcal{Q}, +, \cdot, \leqslant)$ i $(\mathcal{Q}, +, \cdot, \leqslant^*)$. Ponieważ $F(\frac{m}{n}) = \frac{m}{n}$ dla $\frac{m}{n} \in \mathcal{Q}$, więc $\frac{m}{n} \leqslant \frac{k}{l} \Longleftrightarrow F(\frac{m}{n}) \leqslant^* F(\frac{k}{l}) \Longleftrightarrow \frac{m}{n} \leqslant^* \frac{k}{l}$ dla $\frac{m}{n}, \frac{k}{l} \in \mathcal{Q}$. Zatem $\leqslant \, = \, \leqslant^*$.

5. Ciało uporządkowane liczb rzeczywistych

Głównymi pojęciami w tej części artykułu są: archimedesowskie ciało uporządkowane, ciało uporządkowane zupełne, ciało uporządkowane w sposób ciągły, ciało uporządkowane liczb rzeczywistych. Podstawowymi twierdzeniami są: twierdzenie o izomorficznym zanurzeniu archimedesowskiego ciała uporządkowanego w ciele uporządkowanym liczb rzeczywistych, twierdzenie o izomorfizmie ciał uporządkowanych w sposób ciągły.

Materiał przedstawiony w tej części artykułu jest w sposób istotny oparty na książce (Cohen, Ehrlich, 1963), w szczególności wykorzystane są treści zawarte w rozdziałach 3-5. Podstawowe pojęcia i twierdzenia dotyczące ciał uporządkowanych: zbiór gęsty w zbiorze uporządkowanym, ciąg, ciąg podstawowy (spełniający warunek Cauchy'ego), ciąg zbieżny, granica ciągu, własności granic ciągów, ciąg dodatni, są stosowane w tym artykule dokładnie według książki (Cohen, Ehrlich, 1963). Jeżeli ciąg (x_n) o wyrazach w ciele uporządkowanym $(K, +, \cdot, \leqslant)$ ma granicę $a \in K$, to piszemy $\mathcal{L}(x_n) = a$, zamiast tradycyjnego zapisu $\lim\limits_{n\to\infty} x_n = a$ (również wzorując się na książce (Cohen, Ehrlich, 1963)).

Lemat 5.1

Niech $F\colon K \longrightarrow L$ *będzie izomorfizmem ciał uporządkowanych* $(K, +, \cdot, \leqslant)$ *oraz* $(L, +, \cdot, \leqslant)$. *Niech* (a_n) *będzie ciągiem takim, że* $a_n \in K$ *dla każdego* $n \in \mathcal{N}_1$. *Wtedy spełnione są następujące warunki:*
(a) Ciąg (a_n) *jest ciągiem podstawowym w ciele* K *wtedy i tylko wtedy, gdy* $(F(a_n))$ *jest ciągiem podstawowym w ciele* L.
(b) $\mathcal{L}(a_n) = a \Longleftrightarrow \mathcal{L}(F(a_n)) = F(a)$, *gdzie* $a \in K$.
(c) Ciąg (a_n) *jest ciągiem dodatnim w ciele* K *wtedy i tylko wtedy, gdy* $(F(a_n))$ *jest ciągiem dodatnim w ciele* L.

Dowód. (a) Zakładamy, że ciąg (a_n) jest ciągiem podstawowym w ciele K. Niech $e \in L^+$. Przyjmijmy $e_1 = F^{-1}(e)$, oczywiście $e_1 \in K^+$. Wobec tego

$$\exists\, n_{e_1} \in \mathcal{N}_1\ \forall\, m, n \in \mathcal{N}_1 [(m \geqslant n_{e_1} \wedge n \geqslant n_{e_1}) \Longrightarrow |a_n - a_m| < e_1].$$

Stąd otrzymujemy:

$$\begin{aligned} |a_n - a_m| < e_1 &\implies F(|a_n - a_m|) < F(e_1) \\ &\implies |F(a_n - a_m)| < e \\ &\implies |F(a_n) - F(a_m)| < e. \end{aligned}$$

Przyjmując $n_e = n_{e_1}$ mamy:

$$\forall\, e \in L^+\ \exists\, n_e \in \mathcal{N}_1\ \forall\, m, n \in \mathcal{N}_1 [(m \geqslant n_e \wedge n \geqslant n_e) \Longrightarrow |F(a_n) - F(a_m)| < e].$$

Zatem $(F(a_n))$ jest ciągiem podstawowym w ciele L.

Odwrotnie, niech $(F(a_n))$ będzie ciągiem podstawowym w ciele L. Niech $e \in K^+$. Przyjmijmy $e_1 = F(e)$, oczywiście $e_1 \in L^+$. Wobec tego

$$\exists\, n_{e_1} \in \mathcal{N}_1\ \forall\, m, n \in \mathcal{N}_1 [(m \geqslant n_{e_1} \wedge n \geqslant n_{e_1}) \Longrightarrow |F(a_n) - F(a_m)| < e_1].$$

Stąd otrzymujemy:

$$\begin{aligned}|F(a_n)-F(a_m)|<e_1 &\Longrightarrow F^{-1}(|F(a_n)-F(a_m)|)<F^{-1}(e_1)\\ &\Longrightarrow |F^{-1}(F(a_n)-F(a_m))|<e\\ &\Longrightarrow |F^{-1}(F(a_n))-F^{-1}(F(a_m))|<e\\ &\Longrightarrow |a_n-a_m|<e.\end{aligned}$$

Przyjmując $n_e = n_{e_1}$ mamy:

$$\forall\, e\in K^+\ \exists\, n_e\in\mathcal{N}_1\ \forall\, m,n\in\mathcal{N}_1[(m\geqslant n_e\wedge n\geqslant n_e)\Longrightarrow |a_n-a_m|<e].$$

Zatem (a_n) jest ciągiem podstawowym w ciele K.

Dowody własności (b) i (c), które są podobne do dowodu własności (a), pozostawiamy Czytelnikowi.

Lemat 5.2
Niech (a_n) będzie ciągiem zbieżnym w ciele uporządkowanym $(K,+,\cdot,\leqslant)$. Ciąg (a_n) jest dodatni w $(K,+,\cdot,\leqslant)$ wtedy i tylko wtedy, gdy $\mathcal{L}(a_n)>0$ w $(K,+,\cdot,\leqslant)$.

Dowód. Zakładamy, że ciąg (a_n) jest dodatni w $(K,+,\cdot,\leqslant)$. Wobec tego

$$\exists\, e\in K^+\ \exists\, k\in\mathcal{N}_1\ \forall\, n\in\mathcal{N}_1[n\geqslant k\Longrightarrow a_n\geqslant e].$$

Przypuśćmy, że $\mathcal{L}(a_n)=a\leqslant 0$, gdzie $a\in K$. Ponieważ ciąg (a_n) jest zbieżny, więc

$$\exists\, k_1\in\mathcal{N}_1\ \forall\, n\in\mathcal{N}_1[n\geqslant k_1\Longrightarrow |a_n-a|<e].$$

Stąd $a-e<a_n<a+e$ dla $n\geqslant k_1$. Ponieważ $a\leqslant 0$, więc $a+e\leqslant e$, czyli $a_n<e$ dla $n\geqslant k_1$. Otrzymaliśmy sprzeczność. Zatem $\mathcal{L}(a_n)>0$.

Odwrotnie, zakładamy, że $\mathcal{L}(a_n)=a>0$, gdzie $a\in K$. Ponieważ zbiór $(K,\leqslant)$ jest gęsto uporządkowany, więc istnieje $e_1\in K$ takie, że $0<e_1<a$. Wobec tego

$$\exists\, n_{e_1}\in\mathcal{N}_1\ \forall\, n\in\mathcal{N}_1[n\geqslant n_{e_1}\Longrightarrow |a_n-a|<e_1].$$

Stąd $a-e_1<a_n<a+e_1$ dla $n\geqslant n_{e_1}$. Przyjmijmy $e=a-e_1$ i $k=n_{e_1}$. Oczywiście $e>0$. Wówczas

$$\exists\, e\in K^+\ \exists\, k\in\mathcal{N}_1\ \forall\, n\in\mathcal{N}_1[n\geqslant k\Longrightarrow a_n\geqslant e].$$

Zatem ciąg (a_n) jest dodatni w $(K,+,\cdot,\leqslant)$.

Lemat 5.3
Niech $(L,+,\cdot,\leqslant)$ będzie podciałem uporządkowanym ciała uporządkowanego $(K,+,\cdot,\leqslant)$ takim, że zbiór L jest gęsty w zbiorze $(K,\leqslant)$. Zakładamy, że (a_n) jest ciągiem takim, że $a_n\in L$ dla każdego $n\in\mathcal{N}_1$. Następujące warunki są równoważne:

(a) $\forall\, e\in L^+\ \exists\, n_e\in\mathcal{N}_1\ \forall\, n,m\in\mathcal{N}_1[(m\geqslant n_e\wedge n\geqslant n_e)\Longrightarrow |a_n-a_m|<e]$,

(b) $\forall\, e\in K^+\ \exists\, n_e\in\mathcal{N}_1\ \forall\, n,m\in\mathcal{N}_1[(m\geqslant n_e\wedge n\geqslant n_e)\Longrightarrow |a_n-a_m|<e]$.

Dowód. Ponieważ $L^+ \subseteq K^+$, więc oczywiście z warunku (b) wynika warunek (a). Wystarczy zatem wykazać, że z warunku (a) wynika warunek (b). Niech $e \in K^+$, czyli $0 < e$. Z założenia o gęstości zbioru L w zbiorze $(K, \leqslant)$ wynika, że istnieje element $e_1 \in L$ taki, że $0 < e_1 < e$. Na mocy warunku (a) mamy:

$$\exists\, n_{e_1} \in \mathcal{N}_1\, \forall\, n, m \in \mathcal{N}_1 [(m \geqslant n_{e_1} \wedge n \geqslant n_{e_1}) \Longrightarrow |a_n - a_m| < e_1].$$

Wobec tego przyjmując $n_e = n_{e_1}$ otrzymujemy:

$$\forall\, e \in K^+\, \exists\, n_e \in \mathcal{N}_1\, \forall\, n, m \in \mathcal{N}_1 [(m \geqslant n_e \wedge n \geqslant n_e) \Longrightarrow |a_n - a_m| < e].$$

Zatem spełniony jest warunek (b).

Dowody dwóch następnych lematów, które są podobne do dowodu lematu 5.3, pozostawiamy Czytelnikowi.

Lemat 5.4
Niech $(L, +, \cdot, \leqslant)$ będzie podciałem uporządkowanym ciała uporządkowanego $(K, +, \cdot, \leqslant)$ takim, że zbiór L jest gęsty w zbiorze $(K, \leqslant)$. Zakładamy, że (a_n) jest ciągiem takim, że $a_n \in L$ dla każdego $n \in \mathcal{N}_1$. Niech $a \in K$. Następujące warunki są równoważne:
(a) $\forall\, e \in L^+\, \exists\, n_e \in \mathcal{N}_1\, \forall\, n \in \mathcal{N}_1 [n \geqslant n_e \Longrightarrow |a_n - a| < e]$,
(b) $\forall\, e \in K^+\, \exists\, n_e \in \mathcal{N}_1\, \forall\, n \in \mathcal{N}_1 [(n \geqslant n_e \Longrightarrow |a_n - a| < e]$.

Lemat 5.5
Niech $(L, +, \cdot, \leqslant)$ będzie podciałem uporządkowanym ciała uporządkowanego $(K, +, \cdot, \leqslant)$ takim, że zbiór L jest gęsty w zbiorze $(K, \leqslant)$. Zakładamy, że (a_n) jest ciągiem takim, że $a_n \in L$ dla każdego $n \in \mathcal{N}_1$. Następujące warunki są równoważne:
(a) $\exists\, e \in L^+\, \exists\, k \in \mathcal{N}_1\, \forall\, n \in \mathcal{N}_1 [n \geqslant k \Longrightarrow a_n \geqslant e]$,
(b) $\exists\, e \in K^+\, \exists\, k \in \mathcal{N}_1\, \forall\, n \in \mathcal{N}_1 [n \geqslant k \Longrightarrow a_n \geqslant e]$.

Definicja 5.6
Ciało uporządkowane $(K, +, \cdot, \leqslant)$ nazywamy *archimedesowskim*, jeżeli

$$\forall\, a, b \in K\, \exists\, n \in \mathcal{N}_1 [0 < a < b \Longrightarrow b \leqslant n \cdot a].$$

Twierdzenie 5.7
Ciało uporządkowane $(K, +, \cdot, \leqslant)$ jest archimedesowskie wtedy i tylko wtedy, gdy zbiór $\mathcal{Q}_K$ elementów wymiernych ciała K jest gęsty w ciele K.

Twierdzenie i jego dowód można znaleźć w książce (Cohen, Ehrlich, 1963, s. 87-88).

Łatwo udowodnić następujący

Lemat 5.8
Jeżeli ciało uporządkowane $(K, +, \cdot, \leqslant)$ jest archimedesowskie, to

$$\mathcal{L}\left(\frac{1}{n}\right) = 0.$$

TWIERDZENIE 5.9
Ciało uporządkowane $(K, +, \cdot, \leqslant)$ *jest archimedesowskie wtedy i tylko wtedy, gdy każdy element ciała* K *jest granicą pewnego ciągu elementów wymiernych należących do ciała* $\mathcal{Q}_K$.

Dowód. Zakładamy, że ciało uporządkowane $(K, +, \cdot, \leqslant)$ jest archimedesowskie. Niech $a \in K$ i $n \in \mathcal{N}_1$. Wówczas $-\frac{1}{n} < \frac{1}{n}$, a stąd $a - \frac{1}{n} < a + \frac{1}{n}$. Z twierdzenia 5.7 wynika, że dla każdego $n \in \mathcal{N}_1$ istnieje $a_n \in \mathcal{Q}_K$ takie, że $a - \frac{1}{n} < a_n < a + \frac{1}{n}$. Wobec tego

$$|a_n - a| < \frac{1}{n} \tag{7}$$

dla każdego $n \in \mathcal{N}_1$. Z lematu 5.8 wynika, że $\mathcal{L}(\frac{1}{n}) = 0$. Niech $e \in K^+$. Wtedy istnieje $n_e \in \mathcal{N}_1$ takie, że $\frac{1}{n} < e$ dla każdego $n \geqslant n_e$. Stąd i z warunku (7) wynika, że

$$|a_n - a| < e$$

dla każdego $n \geqslant n_e$. Zatem $\mathcal{L}(a_n) = a$.

Następnie zakładamy, że każdy element ciała K jest granicą pewnego ciągu elementów wymiernych należących do ciała $\mathcal{Q}_K$. Niech $a, b \in K$ i $a < b$. Ponieważ zbiór $(K, \leqslant)$ jest gęsto uporządkowany, więc istnieje element $c \in K$ taki, że $a < c < b$. Stąd $c - a > 0$ i $b - c > 0$. Z założenia wynika, że $c = \mathcal{L}(c_n)$ dla pewnego ciągu takiego, że $c_n \in \mathcal{Q}_K$ dla każdego $n \in \mathcal{N}_1$. Przyjmujemy, że $e = \min\{c - a, b - c\}$. Niech $e = c - a$. Wtedy istnieje $n_e \in \mathcal{N}_1$ takie, że $|c_n - c| < c - a$ dla każdego $n \geqslant n_e$. Stąd otrzymujemy: $-c + a < c_n - c < c - a$, czyli $a < c_n$ dla każdego $n \geqslant n_e$. Z definicji elementu e wynika, że $|c_n - c| < b - c$ dla każdego $n \geqslant n_e$. Stąd $-b + c < c_n - c < b - c$, czyli $c_n < b$ dla każdego $n \geqslant n_e$. Wobec tego $a < c_n < b$ dla każdego $n \geqslant n_e$.

Rozumowanie w przypadku, gdy $e = b - c$ jest analogiczne.

Z powyższych rozważań wynika, że zbiór $\mathcal{Q}_K$ jest gęsty w ciele K, więc na podstawie twierdzenia 5.7 ciało uporządkowane $(K, +, \cdot, \leqslant)$ jest archimedesowskie. Dowód twierdzenia został zakończony.

Na bazie arytmetyki liczb wymiernych możemy skonstruować za pomocą odpowiedniej relacji równoważności określonej w zbiorze wymiernych ciągów podstawowych zbiór $\mathcal{R}_C$ liczb rzeczywistych. Zastosowana metoda konstrukcji zbioru $\mathcal{R}_C$ liczb rzeczywistych nosi nazwę *konstrukcji Cantora*. W zbiorze $\mathcal{R}_C$ określamy dodawanie $+$, mnożenie $\cdot$ oraz relację $\leqslant$ liniowego porządku.

Na podstawie konstrukcji Cantora zbioru liczb rzeczywistych i twierdzeń zamieszczonych w książce (Chronowski, 1999b, podrozdziały 2.1-2.5), możemy sformułować następujące twierdzenie.

TWIERDZENIE 5.10
System $(\mathcal{R}_C, +, \cdot, \leqslant)$ *jest archimedesowskim ciałem uporządkowanym.*

Uwaga: W książce (Chronowski, 1999b) zamiast symbolu $\mathcal{R}_C$ występuje symbol R zbioru liczb rzeczywistych.

Zbiór $\mathcal{Q}$ liczb wymiernych jest zbiorem gęstym w zbiorze $(\mathcal{R}_C, \leqslant)$ liczb rzeczywistych (zob. Chronowski, 1999b, wniosek 5.12, s. 54).

TWIERDZENIE 5.11
Każde archimedesowskie ciało uporządkowane $(K, +, \cdot, \leqslant)$ jest, z dokładnością do izomorfizmu, uporządkowanym podciałem ciała uporządkowanego $(\mathcal{R}_C, +, \cdot, \leqslant)$ liczb rzeczywistych.

Dowód. Niech $(\mathcal{Q}_K, +, \cdot, \leqslant)$ będzie podciałem uporządkowanym elementów wymiernych archimedesowskiego ciała uporządkowanego $(K, +, \cdot, \leqslant)$. Z twierdzenia 5.7 wynika, że zbiór $\mathcal{Q}_K$ jest gęsty w ciele K. Na podstawie twierdzenia 4.11 i wniosku 4.15 istnieje funkcja $\varphi\colon \mathcal{Q}_K \longrightarrow \mathcal{Q}$, będąca izomorfizmem ciał uporządkowanych $(\mathcal{Q}_K, +, \cdot, \leqslant)$ i $(\mathcal{Q}, +, \cdot, \leqslant)$. Określimy funkcję $F\colon K \longrightarrow \mathcal{R}_C$. Niech $a \in K$. Z twierdzenia 5.9 wynika, że $a = \mathcal{L}(x_n)$ dla pewnego ciągu (x_n) takiego, że $x_n \in \mathcal{Q}_K$ dla każdego $n \in \mathcal{N}_1$. Z twierdzenia 3.22 (Cohen, Ehrlich, 1963, s. 75) wynika, że (x_n) jest ciągiem podstawowym w ciele K. Na mocy lematu 5.3 (x_n) jest ciągiem podstawowym w ciele $\mathcal{Q}_K$. Stosując lemat 5.1(a) wnioskujemy, że $(\varphi(x_n))$ jest ciągiem podstawowym w ciele $\mathcal{Q}$ i w konsekwencji $(\varphi(x_n))$ jest ciągiem podstawowym w ciele $\mathcal{R}_C$ na mocy lematu 5.3. Na podstawie twierdzenia 5.17 (Chronowski, 1999b, s. 55) otrzymujemy, że $(\varphi(x_n))$ jest ciągiem zbieżnym w ciele $\mathcal{R}_C$.

Na podstawie powyższych rozważań przyjmujemy następującą definicję funkcji $F\colon K \longrightarrow \mathcal{R}_C$:

$$F(a) = \mathcal{L}(\varphi(x_n)), \tag{8}$$

gdzie $a \in K$, $a = \mathcal{L}(x_n)$, $x_n \in \mathcal{Q}_K$ dla każdego $n \in \mathcal{N}_1$. Stąd wynika, że

$$F(\mathcal{L}(x_n)) = \mathcal{L}(\varphi(x_n)).$$

Udowodnimy, że funkcja F jest dobrze określona. Niech $a = \mathcal{L}(y_n)$ dla pewnego ciągu (y_n) takiego, że $y_n \in \mathcal{Q}_K$ dla każdego $n \in \mathcal{N}_1$. Uzasadnimy, że $\mathcal{L}(\varphi(x_n)) = \mathcal{L}(\varphi(y_n))$. W ciele K mamy:

$$\mathcal{L}(x_n) = \mathcal{L}(y_n) \Longrightarrow \mathcal{L}(x_n) - \mathcal{L}(y_n) = 0 \Longrightarrow \mathcal{L}(x_n - y_n) = 0.$$

Z lematu 5.4 wynika, że $\mathcal{L}(x_n - y_n) = 0$ w ciele $\mathcal{Q}_K$. Stąd w ciele $\mathcal{Q}$ na podstawie lematu 5.1(b) mamy:

$$\varphi(\mathcal{L}(x_n - y_n)) = 0 \Longrightarrow \mathcal{L}(\varphi(x_n - y_n)) = 0 \Longrightarrow \mathcal{L}(\varphi(x_n) - \varphi(y_n)) = 0.$$

Na mocy lematu 5.4 w ciele $\mathcal{R}_C$ otrzymujemy:

$$\mathcal{L}(\varphi(x_n) - \varphi(y_n)) = 0 \Longrightarrow \mathcal{L}(\varphi(x_n)) - \mathcal{L}(\varphi(y_n)) = 0 \Longrightarrow \mathcal{L}(\varphi(x_n)) = \mathcal{L}(\varphi(y_n)).$$

Następnie udowodnimy, że funkcja F jest injekcją. Niech $F(a) = F(b)$, gdzie $a, b \in K$. Wobec tego $a = \mathcal{L}(x_n)$ i $b = \mathcal{L}(y_n)$ dla pewnych ciągów (x_n) i (y_n)

o wyrazach z ciała $\mathcal{Q}_K$. Na mocy lematów 5.1(b) i 5.4 otrzymujemy:

$$\begin{aligned} F(a)=F(b) &\Longrightarrow \mathcal{L}(\varphi(x_n))=\mathcal{L}(\varphi(y_n)) \\ &\Longrightarrow \mathcal{L}(\varphi(x_n))-\mathcal{L}(\varphi(y_n))=0 \\ &\Longrightarrow \mathcal{L}(\varphi(x_n)-\varphi(y_n))=0 \\ &\Longrightarrow \mathcal{L}(\varphi(x_n-y_n))=0 \\ &\Longrightarrow \varphi(\mathcal{L}(x_n-y_n))=0 \\ &\Longrightarrow \mathcal{L}(x_n-y_n)=0 \\ &\Longrightarrow \mathcal{L}(x_n)-\mathcal{L}(y_n)=0 \\ &\Longrightarrow \mathcal{L}(x_n)=\mathcal{L}(y_n) \\ &\Longrightarrow a=b. \end{aligned}$$

Następnie uzasadnimy, że

$$F(a+b)=F(a)+F(b)$$

dla $a,b\in K$. Niech $a=\mathcal{L}(x_n)$ i $b=\mathcal{L}(y_n)$ dla pewnych ciągów (x_n) i (y_n) o wyrazach z ciała $\mathcal{Q}_K$. Zauważmy, że $a+b=\mathcal{L}(x_n)+\mathcal{L}(y_n)=\mathcal{L}(x_n+y_n)$. Wobec tego mamy: $F(a+b)=F(\mathcal{L}(x_n+y_n))=\mathcal{L}(\varphi(x_n+y_n))=\mathcal{L}(\varphi(x_n)+\varphi(y_n))=\mathcal{L}(\varphi(x_n))+\mathcal{L}(\varphi(y_n))=F(a)+F(b)$.

Analogicznie możemy uzasadnić, że

$$F(a\cdot b)=F(a)\cdot F(b)$$

dla $a,b\in K$.

W końcu udowodnimy, że

$$a<b\Longleftrightarrow F(a)<F(b) \tag{9}$$

dla $a,b\in K$. Niech $a=\mathcal{L}(x_n)$ dla pewnego ciągu (x_n) o wyrazach z ciała $\mathcal{Q}_K$. Zakładamy, że $a>0$. Stąd $\mathcal{L}(x_n)>0$. Z lematu 5.2 wynika, że (x_n) jest ciągiem dodatnim w ciele K. Stosując lemat 5.5 wnioskujemy, że (x_n) jest ciągiem dodatnim w ciele $\mathcal{Q}_K$. Na mocy lematu 5.1(c) mamy, że $(\varphi(x_n))$ jest ciągiem dodatnim w ciele $\mathcal{Q}$. Ponownie stosując lemat 5.5 wnioskujemy, że $(\varphi(x_n))$ jest ciągiem dodatnim w ciele $\mathcal{R}_C$. Z lematu 5.2 wynika, że $\mathcal{L}(\varphi(x_n))>0$, czyli $F(a)>0$. Analogicznie można udowodnić, że jeżeli $F(a)>0$, to $a>0$. Na mocy lematu 4.7 otrzymujemy, że warunek (9) jest spełniony. Aby zakończyć dowód wystarczy zastosować lemat 3.7.

Definicja 5.12 (Cohen, Ehrlich, 1963, def. 4.3, s. 85)
Ciało uporządkowane $(K,+,\cdot,\leqslant)$ nazywamy *zupełnym*, jeżeli każdy ciąg podstawowy w ciele K jest zbieżny w tym ciele.

Definicja 5.13 (Błaszczyk, 2012)
Jeżeli ciało uporządkowane $(K,+,\cdot,\leqslant)$ jest archimedesowskie i zupełne, to mówimy, że $(K,+,\cdot,\leqslant)$ jest *ciałem uporządkowanym w sposób ciągły*.

Z twierdzeń 5.14 (Chronowski, 1999b, s. 54) i 5.17 (Chronowski, 1999b, s. 55) oraz z definicji 5.13 wynika następujący wniosek.

Wniosek 5.14
Ciało uporządkowane $(\mathcal{R}_C, +, \cdot, \leqslant)$ *liczb rzeczywistych jest ciałem uporządkowanym w sposób ciągły.*

Twierdzenie 5.15
Każde ciało uporządkowane $(K, +, \cdot, \leqslant)$ *w sposób ciągły jest izomorficzne z ciałem uporządkowanym* $(\mathcal{R}_C, +, \cdot, \leqslant)$ *liczb rzeczywistych.*

Dowód. Udowodnimy, że funkcja F określona wzorem (8) jest izomorfizmem ciał uporządkowanych $(K, +, \cdot, \leqslant)$ i $(\mathcal{R}_C, +, \cdot, \leqslant)$. W tym celu wystarczy jedynie uzasadnić, że F jest surjekcją. Niech $r \in \mathcal{R}_C$. Istnieje ciąg podstawowy (y_n) o wyrazach w ciele $\mathcal{Q}$ taki, że $r = \mathcal{L}(y_n)$. Niech $x_n = \varphi^{-1}(y_n)$ dla każdego $n \in \mathcal{N}_1$, gdzie φ jest izomorfizmem określonym w dowodzie twierdzenia 5.11. Na podstawie lematu 5.1(a) wnioskujemy, że (x_n) jest ciągiem podstawowym w ciele $\mathcal{Q}_K$. Stosując lemat 5.3 wnioskujemy, że (x_n) jest ciągiem podstawowym w ciele K. Ponieważ ciało K jest zupełne, więc ciąg (x_n) jest zbieżny w ciele K. Przyjmijmy, że $a = \mathcal{L}(x_n)$. Wobec tego na mocy definicji funkcji F mamy:

$$F(a) = \mathcal{L}(\varphi(x_n) = \mathcal{L}(\varphi(\varphi^{-1}(y_n)) = \mathcal{L}(y_n) = r.$$

Zatem F jest izomorfizmem ciał uporządkowanych $(K, +, \cdot, \leqslant)$ i $(\mathcal{R}_C, +, \cdot, \leqslant)$. Dowód twierdzenia został zakończony.

Na podstawie twierdzenia 5.15 możemy przyjąć następującą definicję.

Definicja 5.16 (Błaszczyk, 2012)
Ciało uporządkowane w sposób ciągły nazywamy *ciałem liczb rzeczywistych.*

Uwaga: Własność, że ciało liczb rzeczywistych jest archimedesowske i zupełne, jest równoważna zasadzie ciągłości sformułowanej we *Wstępie* tego artykułu (zob. Cohen, Ehrlich, 1963, s. 95).

Z twierdzenia 5.15 i lematów 4.4 i 4.5 wynika następujący

Wniosek 5.17
Każde dwa ciała uporządkowane w sposób ciągły są izomorficzne.

Z wniosku 5.17 i definicji 5.16 wynika następujący

Wniosek 5.18
Istnieje, z dokładnością do izomorfizmu, tylko jedno ciało uporządkowane liczb rzeczywistych.

Na mocy wniosku 5.18 możemy przyjąć tradycyjny zapis $(\mathcal{R}, +, \cdot, \leqslant)$ dla ciała uporządkowanego liczb rzeczywistych.

Z twierdzenia 5.11 i wniosku 5.18 wynika następujący

Wniosek 5.19
Każde archimedesowskie ciało uporządkowane $(K, +, \cdot, \leqslant)$ *jest, z dokładnością do izomorfizmu, uporządkowanym podciałem ciała uporządkowanego* $(\mathcal{R}, +, \cdot, \leqslant)$ *liczb rzeczywistych.*

Wniosek 5.20
W ciele uporządkowanym $(\mathcal{R}, +, \cdot, \leqslant)$ *liczb rzeczywistych relacja porządkująca* $\leqslant$ *jest określona jednoznacznie, tzn. jeśli* $(\mathcal{R}, +, \cdot, \leqslant)$ *i* $(\mathcal{R}, +, \cdot, \leqslant^*)$ *są ciałami uporządkowanymi liczb rzeczywistych, to relacje* $\leqslant$ *i* $\leqslant^*$ *są identyczne.*

Dowód. Niech $(\mathcal{R}, +, \cdot, \leqslant)$ i $(\mathcal{R}, +, \cdot, \leqslant^*)$ będą ciałami uporządkowanymi liczb rzeczywistych. Rozważmy podciała uporządkowane $(\mathcal{Q}, +, \cdot, \leqslant|_{\mathcal{Q}})$ i $(\mathcal{Q}, +, \cdot, \leqslant^*|_{\mathcal{Q}})$ odpowiednio ciał uporządkowanych $(\mathcal{R}, +, \cdot, \leqslant)$ i $(\mathcal{R}, +, \cdot, \leqslant^*)$ (zob. wniosek 4.16). Z wniosku 4.17 wynika, że $\leqslant|_{\mathcal{Q}} = \leqslant^*|_{\mathcal{Q}}$. Wobec tego funkcja identycznościowa $\varphi\colon \mathcal{Q} \longrightarrow \mathcal{Q}$ jest izomorfizmem ciał uporządkowanych $(\mathcal{Q}, +, \cdot, \leqslant^*|_{\mathcal{Q}})$ oraz $(\mathcal{Q}, +, \cdot, \leqslant|_{\mathcal{Q}})$. Na podstawie dowodów twierdzeń 5.11 i 5.15 wiemy, że funkcja $F\colon \mathcal{R} \longrightarrow \mathcal{R}$ określona wzorem (8), czyli

$$F(a) = \mathcal{L}(\varphi(x_n)),$$

gdzie $a \in \mathcal{R}$, $a = \mathcal{L}(x_n)$, $x_n \in \mathcal{Q}$ dla każdego $n \in \mathcal{N}_1$, jest izomorfizmem ciał uporządkowanych $(\mathcal{R}, +, \cdot, \leqslant^*)$ i $(\mathcal{R}, +, \cdot, \leqslant)$. Zauważmy, że $F(a) = \mathcal{L}(x_n) = a$ dla każdego $a \in \mathcal{R}$. Wobec tego dla dowolnych $a, b \in \mathcal{R}$ mamy: $a \leqslant^* b \Longleftrightarrow F(a) \leqslant F(b) \Longleftrightarrow a \leqslant b$. Zatem relacje $\leqslant$ i $\leqslant^*$ są identyczne.

Zakończyliśmy prezentację podstawowych zagadnień związanych z kategorycznością uporządkowanych systemów liczb naturalnych, całkowitych, wymiernych i rzeczywistych.

Wiemy (zob. np. Kurosz, 1965, s. 319), że ciała liczb zespolonych nie można uporządkować liniowo.

Literatura

Błaszczyk, P.: 2012, O ciałach uporządkowanych, *Annales Academiae Paedagogicae Cracoviensis. Studia ad Didacticam Mathematicae Pertinentia* **IV**, 15-30.

Chronowski, A.: 1999a, *Podstawy arytmetyki szkolnej. Liczby naturalne i całkowite,* cz. 1, Wydawnictwo Kleks, Bielsko-Biała.

Chronowski, A.: 1999b, *Podstawy arytmetyki szkolnej. Liczby wymierne, rzeczywiste i zespolone,* cz. 2, Wydawnictwo Kleks, Bielsko-Biała.

Cohen, L. C., Ehrlich, G.: 1963, *The Structure of the Real Number System*, Toronto-New York-London.

Guzicki, W., Zakrzewski, P.: 2005, *Wykłady ze wstępu do matematyki. Wprowadzenie do teorii mnogości*, Wydawnictwo Naukowe UAM, Poznań.

Hilbert, D.: 2012, O pojęciu liczby, *Annales Academiae Paedagogicae Cracoviensis. Studia ad Didacticam Mathematicae Pertinentia* **IV**, 199-202. Über den Zahlbegriff, Jahresbericht der Deutschen Mathematiker-Vereinigung 8, 1900, 180-184; tłum. J. Pogonowski.

Kurosz, A. G.: 1965, *Algebra ogólna*, PWN, Warszawa.

Murawski, R.: 2005, *Filozofia matematyki. Zarys dziejów*, Wydawnictwo Naukowe PWN, Warszawa.

Semadeni, Z.: 2002, Trojaka natura matematyki: idee głębokie, formy powierzchniowe, modele formalne, *Roczniki Polskiego Towarzystwa Matematycznego, Seria V, Dydaktyka Matematyki* **24**, 41-92.

Semadeni, Z.: 2005, Idee głębokie struktur matematycznych określonych aksjomatycznie, *Roczniki Polskiego Towarzystwa Matematycznego, Seria V, Dydaktyka Matematyki* **28**, 275-310.

Instytut Matematyki
Uniwersytet Pedagogiczny
ul. Podchorążych 2
PL-30-084 Kraków
e-mail: chron@up.krakow.pl