Elementy teorii mnogości

Część II

Wojciech Buszkowski

Zakład Teorii Obliczeń
Wydział Matematyki i Informatyki
Uniwersytet im. Adama Mickiewicza

6. Liczby naturalne

Aksjomaty G. Peano, oparte na pojęciach pierwotnych: *liczba naturalna*, *zero*, *następnik liczby naturalnej*.

(1) Zero jest liczbą naturalną.

(2) Następnik liczby naturalnej jest liczbą naturalną.

(3) Zero nie jest następnikiem żadnej liczby naturalnej.

(4) Jeżeli następniki dwóch liczb naturalnych są równe, to te liczby są równe.

(5) Jeżeli X jest zbiorem liczb naturalnych, spełniającym warunki:

(a) zero należy do X,

(b) dla dowolnej liczby naturalnej, jeżeli ta liczba należy do X, to jej następnik należy do X,

to każda liczba naturalna należy do X.

W teorii mnogości można skonstruować obiekty, spełniające aksjomaty Peano. Podamy konstrukcję pochodzącą od J. von Neumanna.

Główna idea: liczba naturalna n jest zbiorem wszystkich liczb naturalnych mniejszych od n.

$0 = \emptyset$

$1 = \{0\} = \{\emptyset\}$

$2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$

$3 = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

Ogólnie: $n = \{0, 1, \ldots, n-1\}$.

Przy tej konstrukcji prawdziwe są równoważności:

$m < n \Leftrightarrow m \in n$,

$m \leq n \Leftrightarrow m \subset n$,

dla dowolnych ustalonych liczb naturalnych m, n.

Zauważmy, że $n+1 = \{0, 1, \ldots, n-1, n\} = n \cup \{n\}$.

Definicja 1. Zbiór $X \cup \{X\}$ nazywamy *następnikiem zbioru* X i oznaczamy $S(X)$.

$S(X) = X \cup \{X\}$.

Definicja 2. Zbiór X nazywamy *indukcyjnym*, jeżeli spełnia warunki:

(a) $\emptyset \in X$,

(b) $\forall_Y (Y \in X \Rightarrow S(Y) \in X)$.

Definicja 3. *Liczbą naturalną* nazywamy zbiór należący do wszystkich zbiorów indukcyjnych.

Zatem liczbami naturalnymi są zbiory: $\emptyset$, $S(\emptyset)$, $S(S(\emptyset))$ itd., które utożsamiamy z liczbami 0, 1, 2 itd.

Aksjomat nieskończoności. Istnieje zbiór indukcyjny.

Fakt 1. Istnieje zbiór wszystkich liczb naturalnych.

Dowód. Na mocy aksjomatu nieskończoności istnieje zbiór indukcyjny. Ustalmy taki zbiór Z. Każda liczba naturalna należy do Z, a więc zbiór:

$\{X \in Z : X \text{ jest liczbą naturalną }\}$

istnieje na mocy aksjomatu wyróżniania i pokrywa się ze zbiorem wszystkich liczb naturalnych. Q.E.D.

Zbiór wszystkich liczb naturalnych oznaczamy symbolem $\mathbb{N}$.

Twierdzenie 1 (zasada indukcji matematycznej I). Jeżeli zbiór $X \subset \mathbb{N}$ spełnia warunki:

(a) $0 \in X$, (b) $\forall_{n\in\mathbb{N}}(n \in X \Rightarrow S(n) \in X)$,

to $X = \mathbb{N}$.

Dowód. Niech $X \subset \mathbb{N}$ spełnia warunki (a) i (b). Wtedy $\emptyset \in X$ oraz $\forall_Y(Y \in X \Rightarrow S(Y) \in X)$. Wobec tego zbiór X jest indukcyjny, a stąd $\mathbb{N} \subset X$. Zatem $X = \mathbb{N}$. Q.E.D.

Wniosek (zasada indukcji matematycznej II). Niech $\varphi(n)$ będzie formułą, dla której prawdziwe są warunki:

(a) $\varphi(0)$, (b) $\forall_{n\in\mathbb{N}}(\varphi(n) \Rightarrow \varphi(S(n)))$.

Wtedy $\forall_{n\in\mathbb{N}}\, \varphi(n)$.

Dowód. Stosujemy Twierdzenie 1 do zbioru $X = \{n \in \mathbb{N} : \varphi(n)\}$. Q.E.D.

Fakt 2. $\forall_{n\in\mathbb{N}}(n \subset \mathbb{N})$.

Słowami: każdy element liczby naturalnej jest liczbą naturalną.

Dowód. Niech $\varphi(n)$ będzie formułą: $n \subset \mathbb{N}$.

I. Krok początkowy: $0 \subset \mathbb{N}$. Tak jest, skoro $0 = \emptyset$.

II. Krok indukcyjny: $\forall_{n\in\mathbb{N}}(n \subset \mathbb{N} \Rightarrow S(n) \subset \mathbb{N})$.

Założenie indukcyjne (ZI): $n \subset \mathbb{N}$ (dla ustalonego $n \in \mathbb{N}$).

Teza indukcyjna (TI): $S(n) \subset \mathbb{N}$ (dla tego samego n).

Dowodzimy (TI). Mamy $S(n) = n \cup \{n\}$. Na mocy ZI $n \subset \mathbb{N}$. Ponadto $n \in \mathbb{N}$, więc $\{n\} \subset \mathbb{N}$. Zatem $S(n) \subset \mathbb{N}$ na mocy praw inkluzji. Q.E.D.

Fakt 3. $\forall_{m,n\in\mathbb{N}}(m \in n \Rightarrow m \subset n)$.

Fakt 4. $\forall_{n\in\mathbb{N}}(n \in S(n))$.

Fakt 5. $\forall_{n\in\mathbb{N}}(n \notin n)$.

Teraz możemy udowodnić wszystkie aksjomaty Peano.

Aksjomaty (1), (2) wynikają z definicji liczby naturalnej.

Aksjomat (3) jest prawdziwy, ponieważ $0 = \emptyset$, a $S(n) \neq \emptyset$ na mocy Faktu 4.

Aksjomat (5) to Twierdzenie 1. Pozostaje udowodnić aksjomat (4).

Fakt 6. $\forall_{m,n\in\mathbb{N}}(S(m) = S(n) \Rightarrow m = n)$.

Dowód. Zakładamy $S(m) = S(n)$. Stąd $m \cup \{m\} = n \cup \{n\}$. Wobec tego $m \in n \cup \{n\}$ i $n \in m \cup \{m\}$.

Przypuśćmy, że $m \neq n$. Wtedy $m \in n$ i $n \in m$. Na mocy Faktu 3 $m \subset n$, a więc $n \in n$, wbrew Faktowi 5. Zatem $m = n$. Q.E.D.

Definicja 4. Relację mniejszości $<$ na zbiorze $\mathbb{N}$ określamy wzorem: $m < n \Leftrightarrow m \in n$.

Otrzymujemy prawa:

$\forall_{k,m,n\in\mathbb{N}}(k < m \wedge m < n \Rightarrow k < n)$ (Fakt 3),

$\forall_{n\in\mathbb{N}}(n < S(n))$ (Fakt 4),

$\forall_{n\in\mathbb{N}}\neg(n < n)$ (Fakt 5),

$\forall_{m,n\in\mathbb{N}}(m < S(n) \Leftrightarrow m < n \vee m = n)$.

$$m < S(n) \leftrightarrow m \in n \cup \{n\} \leftrightarrow m \in n \vee m \in \{n\} \leftrightarrow m < n \vee m = n$$

Twierdzenie 2 (zasada indukcji zupełnej). Niech $\varphi(n)$ będzie formułą, spełniającą warunek:

$\forall_{n\in\mathbb{N}}[\forall_{k\in\mathbb{N}}(k < n \Rightarrow \varphi(k)) \Rightarrow \varphi(n)]$.

Wtedy $\forall_{n\in\mathbb{N}}\,\varphi(n)$.

Twierdzenie 3 (zasada minimum). Niech $\varphi(n)$ będzie formułą. Wtedy:

$\exists_{n\in\mathbb{N}}\varphi(n) \Rightarrow \exists_{n\in\mathbb{N}}[\varphi(n) \wedge \forall_{k\in\mathbb{N}}(k < n \Rightarrow \neg\varphi(k))]$.

Dowód. Zakładamy $\exists_{n\in\mathbb{N}}\varphi(n)$. Stąd $\neg\forall_{n\in\mathbb{N}}\neg\varphi(n)$.

Na mocy Tw. 2 mamy:

$\neg\forall_{n\in\mathbb{N}}[\forall_{k\in\mathbb{N}}(k < n \Rightarrow \neg\varphi(k)) \Rightarrow \neg\varphi(n)]$,

a ta formuła jest logicznie równoważna formule:

$\exists_{n\in\mathbb{N}}[\varphi(n) \wedge \forall_{k\in\mathbb{N}}(k < n \Rightarrow \neg\varphi(k))]$. Q.E.D.

Sformułowanie słowne zasady minimum: Jeżeli istnieje liczba naturalna n taka, że $\varphi(n)$, to istnieje najmniejsza liczba naturalna n taka, że $\varphi(n)$.

$\forall_{m,n\in\mathbb{N}}(m < n \vee m = n \vee n < m)$ (prawo trychotomii)

Twierdzenie 4 (o definicjach indukcyjnych). Dla dowolnych funkcji $f : X \mapsto Y$ i $g : X \times \mathbb{N} \times Y \mapsto Y$ istnieje dokładnie jedna funkcja $h : X \times \mathbb{N} \mapsto Y$, spełniająca równania:

$h(x, 0) = f(x)$, $h(x, S(n)) = g(x, n, h(x, n))$

dla wszelkich $x \in X$, $n \in \mathbb{N}$.

Idea dowodu. Najpierw wykazujemy, że dla każdego $k \in \mathbb{N}$ istnieje dokładnie jedna funkcja $h_k : X \times \{0, 1, \ldots, k\} \mapsto Y$, spełniająca powyższe równania dla wszystkich $n < k$. Następnie definiujemy $h = \bigcup_{k \in \mathbb{N}} h_k$. Q.E.D.

Twierdzenie 4 uzasadnia definicje indukcyjne (albo: rekurencyjne) działań dodawania i mnożenia liczb naturalnych.

$m + 0 = m$, $m + S(n) = S(m + n)$

$m \cdot 0 = 0$, $m \cdot S(n) = (m \cdot n) + m$

Tu $X = Y = \mathbb{N}$.

Fakt 7. $n+1 = S(n)$ dla każdego $n \in \mathbb{N}$.

Dowód. $n+1 = n+S(0) = S(n+0) = S(n)$ Q.E.D.

Fakt 8. $(k+m)+n = k+(m+n)$ dla wszelkich $k, m, n \in \mathbb{N}$.

Dowód. Indukcja względem n (przy ustalonych k, m).

$n = 0$.

Mamy: $(k+m)+0 = k+m = k+(m+0)$

ZI: $(k+m)+n = k+(m+n)$ (dla ustalonego n)

TI: $(k+m)+S(n) = k+(m+S(n))$ (dla tego samego n)

$(k+m)+S(n) = S((k+m)+n) =^{ZI} S(k+(m+n)) =$
$k+S(m+n) = k+(m+S(n))$ Q.E.D.

Inny przykład definicji indukcyjnej:

$a^0 = 1$, $a^{n+1} = a^n \cdot a$ dla $a \in \mathbb{R}$, $n \in \mathbb{N}$.

Tu $X = Y = \mathbb{R}$.

7. Relacje równoważności

7.1. Relacje równoważności i klasy abstrakcji

Definicja 1. Relację $R \subset A^2$ nazywamy *relacją równoważności na zbiorze* A, jeżeli relacja R jest zwrotna (na zbiorze A), symetryczna i przechodnia.

zwrotna na A: $\forall_{x \in A}(xRx)$

symetryczna: $\forall_{x,y}(xRy \Rightarrow yRx)$

przechodnia: $\forall_{x,y,z}(xRy \wedge yRz \Rightarrow xRz)$

Przykłady.

1. I_A jest relacją równoważności na zbiorze A.

2. Niech $f : X \mapsto Y$. Relacja $R \subset X^2$ określona wzorem:

$xRy \Leftrightarrow f(x) = f(y)$ dla $x, y \in X$

jest relacją równoważności na zbiorze X.

Definicja 2. Niech R będzie relacją równoważności na zbiorze A. Dla elementu $x \in A$ określamy zbiór:

$[x]_R = \{y : xRy\}$ (równoważnie: $[x]_R = \{y \in A : xRy\}$).

Zbiór $[x]_R$ nazywamy *klasą abstrakcji relacji równoważności* R *wyznaczoną przez element* x.

Fakt 1 (własności klas abstrakcji). Niech R będzie relacją równoważnościu na zbiorze A.

(a) $x \in [x]_R$ dla każdego $x \in A$.

(b) $xRy \Leftrightarrow [x]_R = [y]_R$ dla dowolnych $x, y \in A$.

(c) $\neg(xRy) \Leftrightarrow [x]_R \cap [y]_R = \emptyset$ dla dowolnych $x, y \in A$.

Dowód.

(a) Niech $x \in A$. Ponieważ xRx, więc $x \in [x]_R$.

(b) $xRy \Leftrightarrow [x]_R = [y]_R$ dla dowolnych $x, y \in A$

Najpierw udowodnimy:

(1) $xRy \Leftrightarrow \forall_z(xRz \Leftrightarrow yRz)$ dla dowolnych $x, y \in A$.

($\Rightarrow$). Zakładamy xRy. Niech xRz. Stąd yRx i xRz, a więc yRz. Wykazaliśmy: $xRz \Rightarrow yRz$. Niech yRz. Stąd xRy i yRz, a więc xRz. Wykazaliśmy: $yRz \Rightarrow xRz$. Zatem $xRz \Leftrightarrow yRz$ dla każdego z.

($\Leftarrow$). Zakładamy, że $x, y \in A$ i $\forall_z(xRz \Leftrightarrow yRz)$. Stąd dla $z = y$ mamy: $xRy \Leftrightarrow yRy$. Ponieważ yRy, więc xRy.

Mamy: $xRy \leftrightarrow \forall_z(xRz \Leftrightarrow yRz) \leftrightarrow \forall_z(z \in [x]_R \Leftrightarrow z \in [y]_R) \leftrightarrow$

$\leftrightarrow [x]_R = [y]_R$

na mocy (1), definicji klas abstrakcji, aksjomatu ekstensjonalności i prawa równości.

(c) $\neg(xRy) \Leftrightarrow [x]_R \cap [y]_R = \emptyset$ dla dowolnych $x, y \in A$.

Wykażemy logicznie równoważną formułę:

$xRy \Leftrightarrow [x]_R \cap [y]_R \neq \emptyset$ dla dowolnych $x, y \in A$.

($\Rightarrow$). Zakładamy xRy. Wtedy $[x]_R = [y]_R$ na mocy (b), a więc $[x]_R \cap [y]_R = [x]_R$. Ponieważ $x \in [x]_R$ na mocy (a), więc $[x]_R \cap [y]_R \neq \emptyset$.

($\Leftarrow$). Zakładamy $[x]_R \cap [y]_R \neq \emptyset$. Stąd istnieje $z \in [x]_R \cap [y]_R$. Ustalamy takie z. Ponieważ $z \in [x]_R$ i $z \in [y]_R$, więc xRz i yRz. Wobec tego xRz i zRy, a więc xRy. Q.E.D.

Definicja 3. Rodzinę wszystkich klas abstrakcji relacji równoważności R na zbiorze A nazywamy *zbiorem ilorazowym zbioru A przez relację R* i oznaczamy A/R.

$A/R = \{[x]_R : x \in A\}$

Definicja 4. Niech P będzie rodziną podzbiorów zbioru A. Rodzinę P nazywamy *podziałem* zbioru A, jeżeli spełnia warunki:

(a) wszystkie zbiory rodziny P są niepuste,

(b) $\forall_{X,Y\in P}(X \neq Y \Rightarrow X \cap Y = \emptyset)$,

(c) $\bigcup P = A$.

Warunek (b) wyrażamy słowami: P jest rodziną zbiorów *parami rozłącznych*.

Twierdzenie 1 (zasada abstrakcji). Jeżeli R jest relacją równoważności na zbiorze A, to zbiór ilorazowy A/R jest podziałem zbioru A.

Dowód. (a). Niech $X \in A/R$. Wtedy $X = [x]_R$ dla pewnego $x \in A$. Ustalamy takie x. Mamy $x \in [x]_R$ (Fakt 1.(a)), a więc $X \neq \emptyset$.

(b). Niech $X, Y \in A/R$ i $X \neq Y$. Wtedy $X = [x]_R$ i $Y = [y]_R$ dla pewnych $x, y \in A$. Ustalamy takie x, y. Ponieważ $[x]_R \neq [y]_R$, więc $\neg(xRy)$ (Fakt 1.(b)), a stąd $[x]_R \cap [y]_R = \emptyset$ (Fakt 1.(c)). Zatem $X \cap Y = \emptyset$.

(c) Każdy zbiór $X \in A/R$ jest zawarty w A, a więc $\bigcup(A/R) \subset A$. Niech $x \in A$. Wtedy $x \in [x]_R$ i $[x]_R \in A/R$, a więc $x \in \bigcup(A/R)$. Zatem $A \subset \bigcup(A/R)$. Wykazaliśmy $\bigcup(A/R) = A$. Q.E.D.

Definicje przez abstrakcję polegają na określaniu nowych obiektów jako klas abstrakcji pewnej relacji równoważności.

W następnym podrozdziale zdefiniujemy w ten sposób liczby całkowite i wymierne.

7.2. Liczby całkowite i wymierne

Liczby całkowite otrzymujemy przez odejmowanie liczb naturalnych.

$m - n = m' - n' \Leftrightarrow m + n' = m' + n$

Określamy relację R na zbiorze $\mathbb{N} \times \mathbb{N}$:

$\langle m, n\rangle R\langle m', n'\rangle \Leftrightarrow m + n' = m' + n$ dla $m, n, m', n' \in \mathbb{N}$

Wykażemy, że R jest relacją równoważności na $\mathbb{N} \times \mathbb{N}$.

Zwrotność. Mamy: $\langle m, n\rangle R\langle m, n\rangle \Leftrightarrow m + n = m + n$. Zatem $\langle m, n\rangle R\langle m, n\rangle$.

Symetria. Zakładamy $\langle m, n\rangle R\langle m', n'\rangle$. Stąd $m + n' = m' + n$. Wobec tego $m' + n = m + n'$, czyli $\langle m', n'\rangle R\langle m, n\rangle$. Zatem relacja R jest symetryczna.

Przechodniość. Zakładamy, że $\langle m_1, n_1\rangle R\langle m_2, n_2\rangle$ i $\langle m_2, n_2\rangle R\langle m_3, n_3\rangle$. Stąd:

$m_1 + n_2 = m_2 + n_1$ i $m_2 + n_3 = m_3 + n_2$.

Otrzymujemy:

$$m_1 + n_2 + n_3 = m_2 + n_1 + n_3 = m_2 + n_3 + n_1 = m_3 + n_2 + n_1,$$

a więc: $m_1 + n_3 + n_2 = m_3 + n_1 + n_2$. Korzystając z prawa skracania: $m + k = n + k \Rightarrow m = n$, dostajemy: $m_1 + n_3 = m_3 + n_1$. Zatem $\langle m_1, n_1\rangle R\langle m_3, n_3\rangle$. Wykazaliśmy, że relacja R jest przechodnia.

Definiujemy $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/R$.

Liczbie naturalnej n odpowiada liczba całkowita $[\langle n, 0\rangle]_R$.

Określamy: $-n = [\langle 0, n\rangle]_R$ dla $n \in \mathbb{N}$.

Przykłady.

$$0_{\mathbb{Z}} = [\langle 0,0\rangle]_R = \{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,2\rangle, \ldots\} = \{\langle n,n\rangle : n \in \mathbb{N}\}$$

$$1_{\mathbb{Z}} = [\langle 1,0\rangle]_R = \{\langle 1,0\rangle, \langle 2,1\rangle, \langle 3,2\rangle, \ldots\} = \{\langle n+1,n\rangle : n \in \mathbb{N}\}$$

$$-1 = [\langle 0,1\rangle]_R = \{\langle 0,1\rangle, \langle 1,2\rangle, \langle 2,3\rangle, \ldots\} = \{\langle n,n+1\rangle : n \in \mathbb{N}\}$$

$$-2 = [\langle 0,2\rangle]_R = \{\langle 0,2\rangle, \langle 1,3\rangle, \langle 2,4\rangle, \ldots\} = \{\langle n,n+2\rangle : n \in \mathbb{N}\}$$

Wprowadzimy działania dodawania i mnożenia liczb całkowitych jako działania ilorazowe.

Definicja 5. Niech R będzie relacją równoważności na zbiorze A. Niech $*$ będzie binarnym działaniem wewnętrznym na zbiorze A. Mówimy, że relacja R jest *zgodna* z działaniem $*$, jeżeli spełnia warunek:

$$\forall_{x_1,x_2,y_1,y_2\in A}(x_1 R y_1 \wedge x_2 R y_2 \Rightarrow (x_1 * x_2) R (y_1 * y_2)).$$

Definicja 6. Niech R będzie relacją równoważności na zbiorze A zgodną z działaniem $*$. Określamy *działanie ilorazowe* $*_R$ na zbiorze A/R:

$$[x]_R *_R [y]_R = [x * y]_R \text{ dla } x, y \in A.$$

Uwaga. Powyższa definicja działania $*_R$ jest poprawną definicją funkcji wtw, gdy spełniony jest warunek:

$$[x_1]_R = [y_1]_R \wedge [x_2]_R = [y_2]_R \Rightarrow [x_1 * x_2]_R = [y_1 * y_2]_R,$$

który jest równoważny warunkowi zgodności relacji R z działaniem $*$.

$(m-n)+(m'-n')=(m+m')-(n+n')$

Określamy działanie $\oplus$ na zbiorze $\mathbb{N}\times\mathbb{N}$:

$\langle m,n\rangle\oplus\langle m',n'\rangle=\langle m+m',n+n'\rangle$

Wykażemy, że relacja równoważności R, określona na początku, jest zgodna z działaniem $\oplus$.

$\langle k,l\rangle R\langle k',l'\rangle\wedge\langle m,n\rangle R\langle m',n'\rangle\Rightarrow$
$(\langle k,l\rangle\oplus\langle m,n\rangle)R(\langle k',l'\rangle\oplus\langle m',n'\rangle)$

Zakładamy,że $\langle k,l\rangle R\langle k',l'\rangle$ i $\langle m,n\rangle R\langle m',n'\rangle$.

Stąd $k+l'=k'+l$ i $m+n'=m'+n$. Dodajemy te równania stronami.

$k+m+l'+n'=k'+m'+l+n$, a więc
$\langle k+m,l+n\rangle R\langle k'+m',l'+n'\rangle$.

Zatem $(\langle k,l\rangle\oplus\langle m,n\rangle)R(\langle k',l'\rangle\oplus\langle m',n'\rangle)$.

Określamy działanie ilorazowe na zbiorze $\mathbb{Z}$.

$[\langle m, n\rangle]_R \oplus_R [\langle m', n'\rangle]_R = [\langle m, n\rangle \oplus \langle m'.n'\rangle]_R$

Tak określone działanie odpowiada działaniu dodawania liczb całkowitych.

$1 + (-2) = -1$

$[\langle 1, 0\rangle]_R \oplus_R [\langle 0, 2\rangle]_R = [\langle 1, 2\rangle]_R = [\langle 0, 1\rangle]_R = -1.$

Podobnie określamy mnożenie liczb całkowitych.

$(m - n) \cdot (m' - n') = (m \cdot m' + n \cdot n') - (m \cdot n' + m' \cdot n)$

Określamy: $\langle m, n\rangle \odot \langle m', n'\rangle = \langle mm' + nn', mn' + m'n\rangle.$

Można wykazać, że relacja R jest zgodna z $\odot$.

Określamy: $[\langle m, n\rangle]_R \odot_R [\langle m', n'\rangle]_R = [\langle m, n\rangle \odot \langle m', n'\rangle]_R$

$(-1) \cdot (-2) = 2$

$[\langle 0, 1\rangle]_R \odot_R [\langle 0, 2\rangle]_R = [\langle 2, 0\rangle]_R = 2$

Liczby wymierne otrzymujemy przez dzielenie liczb całkowitych.

$\frac{m}{n} = \frac{m'}{n'} \Leftrightarrow mn' = m'n$ dla $m, n, m', n' \in \mathbb{Z}$, $n, n' \neq 0$.

Określamy relację R na zbiorze $X = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

$\langle m, n\rangle R\langle m', n'\rangle \Leftrightarrow mn' = m'n$

Można wykazać, że R jest relacją równoważności na X.

Określamy: $\mathbb{Q} = X/R$.

Działania dodawania i mnożenia liczb wymiernych określamy jako działania ilorazowe utworzone z działań $\oplus, \odot$ na X.

$\langle m, n\rangle \oplus \langle m', n'\rangle = \langle mn' + m'n, nn'\rangle$

$\langle m, n\rangle \odot \langle m', n'\rangle = \langle mm', nn'\rangle$

Najpierw trzeba sprawdzić, że relacja R jest zgodna z tymi działaniami.

8. Relacje porządkujące

8.1. Relacje porządkujące i liniowo porządkujące

Definicja 1. Relację $R \subset A^2$ nazywamy *relacją (częściowo) porządkującą na zbiorze* A, jeżeli relacja R jest zwrotna (na zbiorze A), antysymetryczna i przechodnia.

antysymetryczna: $\forall_{x,y}(xRy \wedge yRx \Rightarrow x = y)$

Definicja 2. Relację $R \subset A^2$ nazywamy *relacją liniowo porządkującą na zbiorze* A, jeżeli relacja R jest porządkująca i spójna (na zbiorze A).

spójna: $\forall_{x,y\in A}(xRy \vee yRx)$ (dowolne dwa elementy są porównywalne)

Definicja 3. Niech R będzie relacją (odp. liniowo) porządkującą na zbiorze A. Parę (A, R) nazywamy *zbiorem uporządkowanym* (odp. *liniowo uporządkowanym*).

Przykłady.

(1) Relacja I_A jest relacją porządkującą. Jest to najmniejsza (w sensie zawierania) relacja porządkująca na zbiorze A, tzn. relacja I_A jest zawarta w każdej relacji porządkującej na A.

(2) Relacja inkluzji na $\mathcal{P}(U)$, tj. $\{\langle X, Y\rangle \in \mathcal{P}(U)^2 : X \subset Y\}$, jest relacją porządkującą.

(3) Relacja podzielności na zbiorze $\mathbb{N}$ określona wzorem:

$m|n \Leftrightarrow \exists_{k\in\mathbb{N}}\, km = n$ dla $m, n \in \mathbb{N}$

jest relacją porządkującą.

(4) Relacja $\leq$ na zbiorze $\mathbb{N}$ jest relacją liniowo porządkującą. Podobnie $\leq$ na $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

Relacje porządkujące często oznaczamy symbolami $\leq$, $\preceq$, $\sqsubseteq$.

Zamiast ‘relacja (odp. liniowo) porządkująca’ mówimy też: (odp. liniowy) porządek.

Niech $\leq$ bedzie porządkiem na zbiorze A. Określamy relację $< \subset A^2$ wzorem:

$x < y \Leftrightarrow x \leq y \wedge x \neq y$ dla $x, y \in A$.

Tak określona relacja $<$ jest przeciwzwrotna i przechodnia.

Relacje przeciwzwrotne i przechodnie nazywamy *ostrymi (częściowymi) porządkami.*

Niech $<$ będzie ostrym porządkiem na zbiorze A. Określamy relację $\leq \subset A^2$ wzorem:

$x \leq y \Leftrightarrow x < y \vee x = y$ dla $x, y \in A$.

Tak określona relacja $\leq$ jest porządkiem na A.

W ten sposób każdy porządek wyznacza ostry porządek i odwrotnie.

Ostry porządek $< \subset A^2$ nazywamy *ostrym liniowym porządkiem* (na zbiorze A), jeżeli spełnia warunek słabej spójności:

$\forall_{x,y \in A}(x < y \vee x = y \vee y < x)$.

Każdy liniowy porządek wyznacza ostry liniowy porządek i odwrotnie.

Niech $R \subset A^2$ i $X \subset A$. Relację:

$R \cap X^2 = \{\langle x, y\rangle \in R : x \in X \wedge y \in X\}$

nazywamy *ograniczeniem relacji R na zbiór X*.

Fakt 1. Niech (A, R) będzie zbiorem (odp. liniowo) uporządkowanym i $X \subset A$. Wtedy $(X, R \cap X^2)$ jest zbiorem (odp. liniowo) uporządkowanym.

$R \cap X^2$ nazywamy *porządkiem indukowanym na zbiorze X przez porządek R*.

Definicja 4. Niech (A, R) będzie zbiorem uporządkowanym. Zbiór $X \subset A$ nazywamy *łańcuchem* w (A, R), jeżeli $(X, R \cap X^2)$ jest zbiorem liniowo uporządkowanym.

Zauważmy, że zbiór $X \subset A$ jest łańcuchem w (A, R) wtedy i tylko wtedy, gdy $\forall_{x,y \in X}(xRy \vee yRx)$.

Przykłady.

1. Rozważmy zbiór $\mathcal{P}(\{a, b\})$ uporządkowany przez ograniczenie stosunku inkluzji na ten zbiór. Ta relacja nie jest liniowym porządkiem, ponieważ ani $\{a\} \subset \{b\}$, ani $\{b\} \subset \{a\}$ nie zachodzi. Zbiory:

$\{\emptyset, \{a\}, \{a, b\}\}$ i $\{\emptyset, \{b\}, \{a, b\}\}$

są łańcuchami w $\mathcal{P}(\{a, b\})$.

2. Rozważmy zbiór $\{1, 2, 3, 4\}$ z relacją podzielności ograniczoną na ten zbiór. Zbiory $\{1, 2, 4\}$, $\{1, 3\}$, $\{1, 4\}$ są łańcuchami.

Definicja 5. Niech $(A, \leq)$ będzie zbiorem uporządkowanym. Niech $X \subset A$. Element $a \in A$ nazywamy:

elementem najmniejszym w zbiorze X, jeżeli $a \in X$ i $\forall_{x \in X}(a \leq x)$,

elementem największym w zbiorze X, jeżeli $a \in X$ i $\forall_{x \in X}(x \leq a)$,

elementem minimalnym w zbiorze X, jeżeli $a \in X$ i $\neg\exists_{x \in X}(x < a)$,

elementem maksymalnym w zbiorze X, jeżeli $a \in X$ i $\neg\exists_{x \in X}(a < x)$,

ograniczeniem dolnym zbioru X, jeżeli $\forall_{x \in X}(a \leq x)$,

ograniczeniem górnym zbioru X, jeżeli $\forall_{x \in X}(x \leq a)$,

kresem dolnym zbioru X, jeżeli a jest największym ograniczeniem dolnym zbioru X,

kresem górnym zbioru X, jeżeli a jest najmniejszym ograniczeniem górnym zbioru X.

Przykłady.

1. Rozważmy zbiór $\mathbb{R}$ z normalną relacją $\leq$.

W przedziale domkniętym $[a, b]$ liczba a jest elementem najmniejszym, a liczba b jest elementem największym. Każda liczba x taka, że $x \leq a$, jest ograniczeniem dolnym przedziału $[a, b]$, a każda liczba x taka, że $a \leq x$, jest ograniczeniem górnym przedziału $[a, b]$. Zatem a jest kresem dolnym, a b kresem górnym przedziału $[a, b]$.

W przedziale otwartym (a, b) nie istnieje element najmniejszy, ani największy. Ograniczenia dolne i górne przedziału (a, b) są takie jak dla przedziału $[a, b]$. Zatem a jest kresem dolnym, a b kresem górnym przedziału (a, b).

Cały zbiór $\mathbb{R}$ nie ma elementu najmniejszego, ani największego. Żadna liczba nie jest ograniczeniem dolnym, ani górnym tego zbioru.

2. Rozważmy zbiór $\mathbb{N}$ z relacją podzielności. 0 jest elementem największym. a 1 elementem najmniejszym zbioru $\mathbb{N}$. W zbiorze $\{n \in \mathbb{N} : n \geq 2\}$ każda liczba pierwsza jest elementem minimalnym; nie istnieje element najmniejszy, ani największy tego zbioru. Nie istnieją elementy maksymalne tego zbioru.

3. Oczywiście dla zbioru $\mathbb{N}$ z normalną relacją $\leq$ mamy inną sytuację. 0 jest elementem najmniejszym zbioru $\mathbb{N}$.

Fakt 2. Każdy podzbiór zbioru uporządkowanego $(A, \leq)$ ma najwyżej jeden element najmniejszy i najwyżej jeden element największy.

Dowód. Niech $a_1, a_2 \in X$ będą takie, że $\forall_{x \in X}(a_1 \leq x)$ i $\forall_{x \in X}(a_2 \leq x)$. Wtedy $a_1 \leq a_2$ i $a_2 \leq a_1$, a więc $a_1 = a_2$, ponieważ relacja $\leq$ jest antysymetryczna. Podobnie wykazujemy, że istnieje najwyżej jeden element największy zbioru X. Q.E.D.

Wobec tego każdy podzbiór zbioru uporządkowanego ma najwyżej jeden kres dolny i najwyżej jeden kres górny.

Kres dolny zbioru X nazywamy też *infimum* zbioru X i oznaczamy przez $\inf(X)$ lub $\bigwedge X$.

Kres górny zbioru X nazywamy też *supremum* zbioru X i oznaczamy przez $\sup(X)$ lub $\bigvee X$.

Element najmniejszy zbioru X często oznacza się przez $\min(X)$, a element największy zbioru X przez $\max(X)$.

Fakt 3. (a) Element najmniejszy (odp. największy) zbioru X jest jedynym elementem minimalnym (odp. maksymalnym) zbioru X oraz kresem dolnym (odp. górnym) zbioru X.

(b) Jeżeli $(A, \leq)$ jest zbiorem liniowo uporządkowanym, $X \subset A$ i a jest elementem minimalnym (odp. maksymalnym) zbioru X, to a jest elementem najmniejszym (odp. największym) zbioru X.

8.2. Liczby rzeczywiste

Podamy konstrukcję liczb rzeczywistych (R. Dedekind).

Definicja 6. Niech $(A, \leq)$ będzie zbiorem liniowo uporządkowanym. Zbiór $X \subset A$ nazywamy *odcinkiem początkowym* zbioru $(A, \leq)$, jeżeli spełnia warunek:

$\forall_{x,y}(x \in X \wedge y \leq x \Rightarrow y \in X)$.

Odcinek początkowy w $(A, \leq)$ różny od A nazywamy *właściwym odcinkiem początkowym* zbioru $(A, \leq)$.

Rozważmy zbiór liniowo uporządkowany $(\mathbb{Q}, \leq)$, gdzie $\leq$ jest normalnym porządkiem na $\mathbb{Q}$.

Liczby rzeczywiste definiujemy jako niepuste, właściwe odcinki początkowe w $(\mathbb{Q}, \leq)$, nie mające elementu największego. $\mathbb{R}$ oznacza zbiór liczb rzeczywistych.

Liczba wymierna q jest reprezentowana przez $\{x \in \mathbb{Q} : x < q\}$.

Mamy: $q = \sup\{x \in \mathbb{Q} : x < q\}$. Zatem liczby wymierne są reprezentowane przez niepuste, właściwe odcinki początkowe w $(\mathbb{Q}, \leq)$, mające kres górny w $(\mathbb{Q}, \leq)$.

Liczby niewymierne odpowiadają niepustym, właściwym odcinkom początkowym w $(\mathbb{Q}, \leq)$, dla których nie istnieje kres górny w $(\mathbb{Q}, \leq)$.

Na przykład, $\sqrt{2}$ to $\{x \in \mathbb{Q} : x < 0 \vee x^2 \leq 2\}$.

Relację $\leq$ na $\mathbb{R}$ definiujemy jako relację inkluzji.

Porządek $\leq$ na $\mathbb{Q}$ jest *gęsty*, tzn. spełnia warunek:

$\forall_{x,y \in \mathbb{Q}}(x < y \Rightarrow \exists_{z \in \mathbb{Q}}(x < z \wedge z < y))$.

Porządek $\leq$ na $\mathbb{R}$ jest gęsty i *ciągły*, tzn. spełnia *warunek ciągłości*:

dla każdego niepustego zbioru $X \subset \mathbb{R}$, jeżeli zbiór X jest ograniczony z góry, to istnieje kres górny zbioru X.

8.3. Zbiory dobrze uporządkowane

Definicja 7. Porządek $\leq$ na zbiorze A nazywamy *dobrym porządkiem*, jeżeli dla każdego niepustego zbioru $X \subset A$ istnieje element najmniejszy w X. Wtedy parę $(X, \leq)$ nazywamy *zbiorem dobrze uporządkowanym*.

Fakt 4. Każdy zbiór dobrze uporządkowany jest liniowo uporządkowany.

Dowód. Zakładamy, że $(A, \leq)$ jest dobrze uporządkowany. Niech $x, y \in A$. Zbiór $\{x, y\}$ jest niepusty, a więc istnieje element najmniejszy w $\{x, y\}$. Jeżeli x jest tym elementem, to $x \leq y$. Jeżeli y jest tym elementem, to $y \leq x$. Zatem $x \leq y$ lub $y \leq x$. Q.E.D.

Fakt 5. Każdy podzbiór zbioru dobrze uporządkowanego jest dobrze uporządkowany (przez porządek indukowany).

Przykłady.

1. Zbiór $(\mathbb{N}, \leq)$, gdzie $\leq$ jest naturalnym porządkiem na $\mathbb{N}$, jest dobrze uporządkowany.

To wynika z Tw. 6.3 (zasada minimum). Niech $X \subset \mathbb{N}$, $X \neq \emptyset$. Wtedy $\exists_{n\in\mathbb{N}}(n \in X)$. Na mocy Tw. 6.3 istnieje liczba $n \in \mathbb{N}$ taka, że $\forall_{k\in\mathbb{N}}(k < n \Rightarrow k \notin X)$. Ta liczba n jest elementem minimalnym zbioru X, a więc jest elementem najmniejszym zbioru X, skoro $(\mathbb{N}, \leq)$ jest liniowo uporządkowany (Fakt 3). Q.E.D.

W konsekwencji każdy podzbiór zbioru $\mathbb{N}$ jest dobrze uporządkowany przez relację $\leq$ ograniczoną na ten podzbiór.

2. Rozważmy zbiór $X = \{\frac{n}{n+1} : n \in \mathbb{N}\} \cup \{1 + \frac{n}{n+1} : n \in \mathbb{N}\}$ z naturalnym porządkiem $\leq$ na $\mathbb{Q}$ ograniczonym na X. Jest to dobry porządek, który można przedstawić tak:

$0 < \frac{1}{2} < \frac{2}{3} < \cdots < 1 < 1 + \frac{1}{2} < 1 + \frac{2}{3} < \cdots$

Zbiory $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ z naturalnymi porządkami nie są dobrze uporządkowane.

Ogólna postać zbioru dobrze uporządkowanego $(X, \leq)$:

$a_0 < a_1 < a_2 < \cdots < b_0 < b_1 < b_2 < \cdots < c_0 < c_1 < c_2 < \cdots,$

gdzie $a_0 = \min(X)$, $a_1 = \min(X \setminus \{a_0\})$, $a_2 = \min(X \setminus \{a_0, a_1\})$ itd. Oczywiście zbiór X może skończyć się w dowolnym miejscu tak tworzonego ciągu *pozaskończonego*.

Rolę standardowych zbiorów dobrze uporządkowanych grają *liczby porządkowe*. Każda liczba porządkowa jest zbiorem wszystkich liczb porządkowych mniejszych od niej, przy czym stosunek mniejszości pokrywa się ze stosunkiem należenia.

Skończone liczby porządkowe to liczby naturalne. $\omega = \mathbb{N}$ jest najmniejszą nieskończoną liczbą porządkową. Następne liczby porządkowe to $S(\omega) = \omega + 1$, $S(S(\omega)) = \omega + 2$ itd.

$0 < 1 < 2 < \cdots < \omega < \omega + 1 < \omega + 2 < \cdots < \omega + \omega < \cdots$

Definicja 8. Niech $(X, \leq_X)$, $(Y, \leq_Y)$ będą zbiorami uporządkowanymi. Mówimy, że funkcja $f : X \mapsto Y$ *zachowuje porządek*, jeżeli spełnia warunek:

$\forall_{a,b \in X}(a \leq_X b \Rightarrow f(a) \leq_Y f(b))$.

Jeżeli funkcja f spełnia silniejszy warunek:

$\forall_{a,b \in X}(a \leq_X b \Leftrightarrow f(a) \leq_Y f(b))$,

to funkcję f nazywamy *zanurzeniem* $(X, \leq_X)$ w $(Y, \leq_Y)$.

Fakt 6. Każde zanurzenie jednego zbioru uporządkowanego w drugi jest iniekcją.

Definicja 9. Bijekcję $f : X \mapsto Y$, która jest zanurzeniem $(X, \leq_X)$ w $(Y, \leq_Y)$, nazywamy *izomorfizmem* zbioru $(X, \leq_X)$ ze zbiorem $(Y, \leq_Y)$. Mówimy, że zbiór $(X, \leq_X)$ *jest izomorficzny* ze zbiorem $(Y, \leq_Y)$ (albo: te zbiory *są izomorficzne*), jeżeli istnieje taki izomorfizm. Wtedy piszemy: $(X, \leq_X) \simeq (Y, \leq_Y)$.

Fakt 7. Dla dowolnych zbiorów uporządkowanych $(X, \leq_X)$, $(Y, \leq_Y)$, $(Z, \leq_Z)$ spełnione są warunki:

(a) $(X, \leq_X) \simeq (X, \leq_X)$,

(b) jeżeli $(X, \leq_X) \simeq (Y, \leq_Y)$, to $(Y, \leq_Y) \simeq (X, \leq_X)$,

(c) jeżeli $(X, \leq_X) \simeq (Y, \leq_Y)$ i $(Y, \leq_Y) \simeq (Z, \leq_Z)$, to $(X, \leq_X) \simeq (Z, \leq_Z)$.

Dowód. (a) Funkcja I_X jest izomorfizmem $(X, \leq_X)$ ze sobą.

(b) Jeżeli $f : X \mapsto Y$ jest izomorfizmem $(X, \leq_X)$ z $(Y, \leq_Y)$, to f^{-1} jest izmorfizmem $(Y, \leq_Y)$ z $(X, \leq_X)$.

(c) Jeżeli $f : X \mapsto Y$ jest izomorfizmem $(X, \leq_X)$ z $(Y, \leq_Y)$ i $g : Y \mapsto Z$ jest izomorfizmem $(Y, \leq_Y)$ z $(Z, \leq_Z)$, to $g \circ f$ jest izomorfizmem $(X, \leq_X)$ z $(Z, \leq_Z)$. Q.E.D.

Lemat 1. Niech $(X, \leq)$ będzie zbiorem dobrze uporządkowanym, a funkcja $f; X \mapsto X$ będzie zanurzeniem $(X, \leq)$ w siebie. Wtedy $a \leq f(a)$ dla każdego $a \in X$.

Dowód. Przypuśćmy, że istnieje $a \in X$ takie, że $\neg(a \leq f(a))$, co jest równoważne $f(a) < a$, skoro $\leq$ jest liniowym porządkiem. Oznaczmy $A = \{a \in X : f(a) < a\}$. Istnieje $b = \min(A)$. Ponieważ $f(b) < b$, więc $f(b) \leq b$ i $f(b) \neq b$. Skoro f jest zanurzeniem, mamy $f(f(b)) \leq f(b)$ i $f(f(b)) \neq f(b)$, czyli $f(f(b)) < f(b)$. Wobec tego $f(b) \in A$, ale $f(b) < b$, co jest sprzeczne z definicją b jako elementu najmniejszego w A. Q.E.D.

Lemat 2. Zbiór dobrze uporządkowany nie jest izomorficzny z żadnym swoim właściwym odcinkiem początkowym.

DOWÓD. Przypuśćmy, że $(X, \leq)$ jest zbiorem dobrze uporządkowanym, $Y \subset X$ jest odcinkiem początkowym $(X, \leq)$, $Y \neq X$ oraz $(X, \leq) \simeq (Y, \leq \cap Y^2)$.

Niech $f : X \mapsto Y$ będzie takim izomorfizmem. Ustalamy $a \in X \setminus Y$. Mamy $y < a$ dla każdego $y \in Y$. Ponieważ $f(a) \in Y$, więc $f(a) < a$, wbrew Lematowi 1. Q.E.D.

Twierdzenie 1 (zasada trychotomii dla zbiorów dobrze uporządkowanych). Niech $(X, \leq_X)$ i $(Y, \leq_Y)$ będą zbiorami dobrze uporządkowanymi. Wtedy prawdziwy jest dokładnie jeden z następujących warunków:

(a) $(X, \leq_X) \simeq (Y, \leq_Y)$,

(b) zbiór $(X, \leq_X)$ jest izomorficzny z właściwym odcinkiem początkowym zbioru $(Y, \leq_Y)$,

(c) zbiór $(Y, \leq_Y)$ jest izomorficzny z właściwym odcinkiem początkowym zbioru $(X, \leq_X)$.

Twierdzenie 2 (zasada indukcji pozaskończonej). Niech $(X, \leq)$ będzie zbiorem dobrze uporządkowanym. Niech $\varphi(x)$ będzie formułą, określoną dla elementów zbioru X i spełniającą warunek:

$\forall_{x \in X}[\forall_{y \in X}(y < x \Rightarrow \varphi(y)) \Rightarrow \varphi(x)]$.

Wtedy $\forall_{x \in X} \varphi(x)$.

Dowód. Przypuśćmy, że istnieje $x \in X$ takie, że $\neg\varphi(x)$. Niech $x_0 = \min\{x \in X : \neg\varphi(x)\}$. Mamy:

$\forall_{y \in X}(y < x_0 \Rightarrow \varphi(y))$.

Stąd, na mocy założonego warunku, otrzymujemy $\varphi(x_0)$, wbrew definicji x_0. Q.E.D.

8.4. Aksjomat wyboru

Aksjomat wyboru. (AC) Dla dowolnej rodziny zbiorów niepustych i parami rozłącznych istnieje zbiór zawarty w sumie tej rodziny i mający z każdym zbiorem tej rodziny dokładnie jeden element wspólny.

Taki zbiór nazywamy *selektorem* danej rodziny zbiorów.

Przykład. Niech $A = \{\{a, b\}, \{c, d\}\}$. Zbiory $\{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}$ są selektorami rodziny A.

Powyższy przykład dotyczy rodziny skończonej. Bez aksjomatu wyboru można udowodnić, że dla każdej skończonej rodziny zbiorów niepustych i parami rozłącznych istnieje selektor.

Aksjomat wyboru jest potrzebny, gdy mamy do czynienia z nieskończoną rodziną zbiorów niepustych i parami rozłącznych, dla której nie znamy warunku wyróżniającego elementy pewnego selektora tej rodziny.

Definicja 10. Niech A będzie rodziną zbiorów niepustych. Funkcję $F : A \mapsto \bigcup A$ taką, że $F(X) \in X$ dla każdego $X \in A$, nazywamy *funkcją wyboru* dla rodziny A.

Twierdzenie 3. Dla dowolnej rodziny zbiorów niepustych istnieje funkcja wyboru.

Dowód. Niech A będzie rodziną zbiorów niepustych. Określamy rodzinę $B = \{\{X\} \times X : X \in A\}$. B jest rodziną zbiorów niepustych i parami rozłącznych. Na mocy aksjomatu wyboru istnieje selektor Z rodziny B. Dla każdego $X \in A$ istnieje dokładnie jeden element $x \in X$ taki, że $\langle X, x\rangle \in Z$. Zatem Z jest funkcją wyboru dla rodziny A. Q.E.D.

Faktycznie Twierdzenie 3 jest równoważnikiem aksjomatu wyboru, tzn. jest równoważne aksjomatowi wyboru na gruncie pozostałych aksjomatów.

Podamy dwa inne, ważne równoważniki aksjomatu wyboru.

Twierdzenie 4 (lemat Kuratowskiego-Zorna). (LKZ) Jeżeli zbiór uporządkowany $(X, \leq)$ spełnia *warunek łańcucha*:

(WŁ) dla każdego łańcucha w $(X, \leq)$ istnieje ograniczenie górne tego łańcucha,

to istnieje element maksymalny w $(X, \leq)$.

Krótko: Każdy zbiór częściowo uporządkowany, w którym każdy łańcuch ma ograniczenie górne, ma element maksymalny.

Twierdzenie 5 (twierdzenie Zermelo o dobrym uporządkowaniu). (TZ) Dla każdego zbioru istnieje dobry porządek na tym zbiorze.

Krótko: Każdy zbiór można dobrze uporządkować.

Wykażemy: (LKZ) $\Rightarrow$ (AC).

Zakładamy (LKZ). Niech A będzie rodziną zbiorów niepustych i parami rozłącznych. Rozważamy rodzinę $\mathcal{S}$, składającą się ze wszystkich częściowych selektorów rodziny A, tzn. wszystkich zbiorów $Z \subset \bigcup A$ takich, że dla każdego $X \in A$ zbiór $X \cap Z$ jest pusty lub jednoelementowy. Relacja inkluzji ograniczona na $\mathcal{S}$ jest porządkiem.

Wykażemy (WŁ). Niech $\mathcal{T} \subset \mathcal{S}$ będzie łańcuchem w $\mathcal{S}$, tzn.

$\forall_{Z_1, Z_2 \in \mathcal{T}}(Z_1 \subset Z_2 \vee Z_2 \subset Z_1)$.

Wtedy $\bigcup \mathcal{T} \in \mathcal{S}$. Przypuśćmy, że tak nie jest. Wtedy istnieją $X \in A$ oraz różne elementy x, y takie, że $x, y \in X \cap \bigcup \mathcal{T}$. Stąd $x, y \in X$ oraz $x \in Z_1$, $y \in Z_2$ dla pewnych $Z_1, Z_2 \in \mathcal{T}$. Mamy: $Z_1 \subset Z_2$ lub $Z_2 \subset Z_1$. W pierwszym przypadku $x, y \in Z_2$, a stąd $x, y \in X \cap Z_2$, co jest niemożliwe, skoro $Z_2 \in \mathcal{S}$. Podobnie wykluczamy drugi przypadek.

Dla każdego $Z \in \mathcal{T}$ mamy $Z \subset \bigcup \mathcal{T}$. Zatem $\bigcup \mathcal{T}$ jest ograniczeniem górnym łańcucha $\mathcal{T}$ w $\mathcal{S}$.

Na mocy (LKZ) istnieje element maksymalny $Z \in \mathcal{S}$, tzn. taki zbiór $Z \in \mathcal{S}$, dla którego nie istnieje $Z_1 \in \mathcal{S}$ taki, że $Z \subset Z_1$ i $Z \neq Z_1$. Ustalamy taki zbiór Z.

Wykażemy, że Z jest selektorem rodziny A. Przypuśćmy, że nie jest. Wtedy istnieje $X \in A$ taki, że $X \cap Z = \emptyset$. Ponieważ $X \neq \emptyset$, więc istnieje $x \in X$. Określamy $Z_1 = Z \cup \{x\}$. Oczywiście $Z \subset Z_1$, $Z \neq Z_1$ i $Z_1 \in \mathcal{S}$, wbrew maksymalności Z. Q.E.D.

Podobnie można wykazać: (LKZ) $\Rightarrow$ (TZ).

9. Liczby kardynalne

9.1. Równoliczność zbiorów i liczby kardynalne

Definicja 1. Mówimy, że zbiór X *jest równoliczny* ze zbiorem Y, jeżeli istnieje bijekcja $f : X \mapsto Y$. Wtedy piszemy: $X \sim Y$.

Fakt 1. Dla dowolnych zbiorów X, Y, Z:

(a) $X \sim X$,

(b) jeżeli $X \sim Y$, to $Y \sim X$,

(c) jeżeli $X \sim Y$ i $Y \sim Z$, to $X \sim Z$.

Dowód. (a) I_X jest bijekcją zbioru X na zbiór X.

(b) Jeżeli $f : X \mapsto Y$ jest bijekcją, to $f^{-1} : Y \mapsto X$ jest bijekcją.

(c) Jeżeli $f : X \mapsto Y$ i $g : Y \mapsto Z$ są bijekcjami, to $g \circ f : X \mapsto Z$ jest bijekcją. Q.E.D.

Każdemu zbiorowi X przyporządkowujemy pewien obiekt $\overline{\overline{X}}$ w taki sposób, że prawdziwa jest równoważność:

$$X \sim Y \Leftrightarrow \overline{\overline{X}} = \overline{\overline{Y}}$$

dla dowolnych zbiorów X, Y.

Definicja 2. Obiekt $\overline{\overline{X}}$ nazywamy *mocą* lub *liczbą kardynalną* zbioru X.

G. Frege definiował $\overline{\overline{X}} = [X]_\sim$, czyli jako zbiór wszystkich zbiorów równolicznych z X. Dzisiaj wiemy, że taki zbiór nie istnieje, jeżeli $X \neq \emptyset$. Dlatego w teorii mnogości przyjmuje się, że liczba kardynalna zbioru X jest pewnym ustalonym zbiorem równolicznym z X, tj. pewnym reprezentantem klasy $[X]_\sim$.

W teorii mnogości z aksjomatem wyboru liczby kardynalne można zdefiniować jako *początkowe* liczby porządkowe (nierównoliczne z żadną liczbą porządkową mniejszą od danej liczby).

Definicja 3. Zbiór nazywamy *skończonym*, jeżeli jest równoliczny z pewną liczbą naturalną. Zbiór nazywamy *nieskończonym*, jeżeli nie jest skończony.

Można udowodnić, że różne liczby naturalne nie są równoliczne. Zatem dla każdego skończonego zbioru X istnieje dokładnie jedna liczba $n \in \mathbb{N}$ taka, że $X \sim n$; przyjmujemy, że ta jedyna liczba n jest liczbą kardynalną danego zbioru X. Wobec tego liczby naturalne są liczbami kardynalnymi zbiorów skończonych (skończonymi liczbami kardynalnymi).

Fakt 2.

(a) Każdy podzbiór zbioru skończonego jest skończony.

(b) Suma dwóch zbiorów skończonych jest zbiorem skończonym.

(c) Suma skończonej rodziny zbiorów skończonych jest zbiorem skończonym.

Fakt 3. $\mathbb{N}$ jest zbiorem nieskończonym.

Dowód. Każdy niepusty, skończony zbiór liniowo uporządkowany ma element najmniejszy i element największy (ćwiczenia!). $\mathbb{N}$ z naturalnym porządkiem jest liniowo uporządkowany. Gdyby zbiór $\mathbb{N}$ był skończony, to istniałaby największa liczba naturalna. Tak nie jest, ponieważ $n < S(n)$ dla każdego $n \in \mathbb{N}$. Q.E.D.

Nieskończone liczby kardynalne to liczby kardynalne zbiorów nieskończonych.

Definicja 3. $\aleph_0 = \overline{\overline{\mathbb{N}}}$.

$\aleph$ (alef) to pierwsza litera alfabetu hebrajskiego.

$\overline{\overline{X}} = \aleph_0 \Leftrightarrow X \sim \mathbb{N}$

$\aleph_0$ jest pierwszą nieskończoną liczbą kardynalną.

Przykłady. Podamy trzy inne przykłady zbiorów mocy $\aleph_0$.

1. $A_k = \{n \in \mathbb{N} : n \geq k\}$, gdzie $k \in \mathbb{N}^+$. Odwzorowanie $f : \mathbb{N} \mapsto A_k$ określone wzorem:

$$f(n) = n + k \text{ dla } n \in \mathbb{N}$$

jest bijekcją. Zatem $\mathbb{N} \sim A_k$, a więc $\overline{\overline{A_k}} = \overline{\overline{N}} = \aleph_0$.

2. $P = \{n \in \mathbb{N} : \exists_{k \in \mathbb{N}}(n = 2k)\}$ (zbiór liczb naturalnych parzystych). Odwzorowanie $f : \mathbb{N} \mapsto P$ określone wzorem: $f(n) = 2n$ dla $n \in \mathbb{N}$, jest bijekcją.

3. $\mathbb{N}^2$. Odwzorowanie $\pi : \mathbb{N}^2 \mapsto \mathbb{N}$ określone wzorem:

$$\pi(m, n) = 2^m(2n + 1) - 1 \text{ dla } m, n \in \mathbb{N}$$

jest bijekcją. Wystarczy wykazać, że dla każdego $k \in \mathbb{N}$ istnieje dokładnie jedna para $\langle m, n\rangle \in \mathbb{N}^2$ taka, że $\pi(m, n) = k$, czyli $2^m(2n + 1) = k + 1$. Funkcję π nazywamy *funkcją pary*.

9.2. Uporządkowanie liczb kardynalnych

Definicja 4. Określamy stosunki $\leq$ i $<$ między liczbami kardynalnymi:

$$\overline{\overline{X}} \leq \overline{\overline{Y}} \Leftrightarrow \exists_Z (Z \subset Y \wedge X \sim Z)$$

Równoważnie:

$$\overline{\overline{X}} \leq \overline{\overline{Y}} \Leftrightarrow \exists_f (f : X \mapsto Y \text{ jest iniekcją})$$

$$\overline{\overline{X}} < \overline{\overline{Y}} \Leftrightarrow \overline{\overline{X}} \leq \overline{\overline{Y}} \wedge \overline{\overline{X}} \neq \overline{\overline{Y}}$$

Te definicje są poprawne, ponieważ zachodzą warunki zgodności:

$$X_1 \sim Y_1 \wedge X_2 \sim Y_2 \Rightarrow (\overline{\overline{X_1}} \leq \overline{\overline{X_2}} \Rightarrow \overline{\overline{Y_1}} \leq \overline{\overline{Y_2}})$$

i podobnie dla $<$. Wykażemy pierwszy warunek. Niech $X_1 \sim Y_1$ i $X_2 \sim Y_2$. Niech $f : X_1 \mapsto X_2$ będzie iniekcją. Istnieją bijekcje $g : X_1 \mapsto Y_1$ i $h : X_2 \mapsto Y_2$. Wtedy $h \circ f \circ g^{-1} : Y_1 \mapsto Y_2$ jest iniekcją.

Wykażemy drugi warunek. Niech $X_1 \sim Y_1$ i $X_2 \sim Y_2$. Niech $\overline{\overline{X_1}} < \overline{\overline{X_2}}$. Stąd $\overline{\overline{X_1}} \leq \overline{\overline{X_2}}$ i $X_1 \not\sim X_2$ (tzn. $\neg(X_1 \sim X_2)$). Na mocy pierwszego warunku $\overline{\overline{Y_1}} \leq \overline{\overline{Y_2}}$. Gdyby $Y_1 \sim Y_2$, to mielibyśmy $X_1 \sim X_2$. Wobec tego $Y_1 \not\sim Y_2$. Zatem $\overline{\overline{Y_1}} < \overline{\overline{Y_2}}$.

Fakt 4. Dla dowolnych zbiorów X, Y, Z:

(a) $\overline{\overline{X}} \leq \overline{\overline{X}}$,

(b) jeżeli $\overline{\overline{X}} \leq \overline{\overline{Y}}$ i $\overline{\overline{Y}} \leq \overline{\overline{Z}}$, to $\overline{\overline{X}} \leq \overline{\overline{Z}}$.

Dowód. (a) $\mathrm{I}_X : X \mapsto X$ jest iniekcją.

(b) Jeżeli $f : X \mapsto Y$ i $g : Y \mapsto Z$ są iniekcjami, to $g \circ f : X \mapsto Z$ jest iniekcją. Q.E.D.

Uwaga. Dla liczb naturalnych tak określone stosunki $\leq$ i $<$ pokrywają się z naturalnymi porządkami: nieostrym i ostrym na $\mathbb{N}$. Ponadto $n < \aleph_0$ dla każdego $n \in \mathbb{N}$.

Twierdzenie 1 (tw. Cantora). $\overline{\overline{X}} < \overline{\overline{\mathcal{P}(X)}}$ dla każdego zbioru X.

Dowód. Najpierw wykażemy: $\overline{\overline{X}} \leq \overline{\overline{\mathcal{P}(X)}}$. Określamy funkcję $f : X \mapsto \mathcal{P}(X)$:

$f(a) = \{a\}$ dla $a \in X$.

Oczywiście tak określona funkcja jest różnowartościowa.

Wykażemy, że $X \not\sim \mathcal{P}(X)$. Przypuśćmy, że istnieje bijekcja $g : X \mapsto \mathcal{P}(X)$. Określamy zbiór:

$Z = \{a \in X : a \notin g(a)\}$.

Ponieważ $Z \in \mathcal{P}(X)$ i g jest suriekcją, więc istnieje $b \in X$ takie, że $g(b) = Z$. Ustalamy takie b. Mamy:

$b \in g(b) \leftrightarrow b \in Z \leftrightarrow b \notin g(b)$.

Otrzymaliśmy formułę logicznie fałszywą: $b \in g(b) \Leftrightarrow b \notin g(b)$. Q.E.D.

Wniosek. Istnieje nieskończenie wiele nieskończonych liczb kardynalnych.

Dowód. Na mocy tw. Cantora mamy:

$\overline{\overline{\mathbb{N}}} < \overline{\overline{\mathcal{P}(\mathbb{N})}} < \overline{\overline{\mathcal{P}(\mathcal{P}(\mathbb{N}))}} < \cdots$

Wszystkie liczby kardynalne w tym ciągu są nieskończone i różne. Q.E.D.

Lemat 1 (lemat o trzech zbiorach). Niech X, Y, Z będą zbiorami takimi, że $X \subset Y \subset Z$ oraz $X \sim Z$. Wtedy $X \sim Y$ i $Y \sim Z$.

Dowód. Ustalamy bijekcję $f : Z \mapsto X$. Określamy nieskończony ciąg zbiorów $(A_n)_{n\in\mathbb{N}}$.

$A_0 = Z \setminus Y$, $A_{n+1} = f[A_n]$

Określamy zbiór $A = \bigcup_{n\in\mathbb{N}} A_n$. Oczywiście $A \subset Z$. Ponadto:

$f[A] = f[\bigcup_{n\in\mathbb{N}} A_n] = \bigcup_{n\in\mathbb{N}} f[A_n] = \bigcup_{n\in\mathbb{N}} A_{n+1} \subset A.$

Określamy funkcję $g : Z \mapsto Z$.

$g(a) = f(a)$ dla $a \in A$, $g(a) = a$ dla $a \in Z \setminus A$.

(1) $g : Z \mapsto Y$, tzn. $D^*(g) \subset Y$.

Niech $a \in Z$. Rozważamy dwa przypadki. 1°. $a \in A$. Wtedy $g(a) = f(a) \in X$, a stąd $g(a) \in Y$. 2°. $a \notin A$. Wtedy $a \notin A_0 = Z \setminus Y$, czyli $a \in Y$. Zatem $g(a) = a \in Y$.

(2) Funkcja g jest różnowartościowa.

Niech $a_1, a_2 \in Z$, $a_1 \neq a_2$. Wykażemy $g(a_1) \neq g(a_2)$. Rozważamy cztery przypadki. 1°. $a_1, a_2 \in A$. Wtedy $g(a_1) = f(a_1)$, $g(a_2) = f(a_2)$. Mamy $f(a_1) \neq f(a_2)$, a stąd $g(a_1) \neq g(a_2)$. 2°. $a_1, a_2 \notin A$. Wtedy $g(a_1) = a_1$, $g(a_2) = a_2$, a więc $g(a_1) \neq g(a_2)$. 3°. $a_1 \in A$, $a_2 \notin A$. Wtedy $g(a_2) = a_2 \notin A$, ale $g(a_1) = f(a_1) \in f[A]$, a stąd $g(a_1) \in A$. Zatem $g(a_1) \neq g(a_2)$. 4°. $a_1 \notin A$, $a_2 \in A$. Rozumujemy podobnie jak poprzednio.

(3) Odwzorowanie $g : Z \mapsto Y$ jest suriekcją.

Niech $b \in Y$. Stąd $b \notin A_0$. Mamy dwa przypadki. 1°. $b \in A$. Wtedy $b \in A_n$ dla pewnego $n > 0$, czyli $b \in A_{k+1}$ dla pewnego $k \in \mathbb{N}$. Skoro $A_{k+1} = f[A_k]$, istnieje $a \in A_k$ takie, że $b = f(a)$. Mamy $g(a) = f(a) = b$. 2°. $b \notin A$. Wtedy $g(b) = b$.

Wykazaliśmy, że $g : Z \mapsto Y$ jest bijekcją. Stąd $Z \sim Y$, czyli $Y \sim Z$. Ponieważ $X \sim Z$, więc także $X \sim Y$. Q.E.D.

Twierdzenie 2 (tw. Cantora-Bernsteina). Dla dowolnych zbiorów X, Y, jeżeli $\overline{\overline{X}} \leq \overline{\overline{Y}}$ i $\overline{\overline{Y}} \leq \overline{\overline{X}}$, to $\overline{\overline{X}} = \overline{\overline{Y}}$.

Dowód. Zakładamy, że $X \sim Z$ dla pewnego $Z \subset Y$ oraz $Y \sim V$ dla pewnego $V \subset X$. Ustalamy takie zbiory Z, V oraz bijekcję $f : X \mapsto Z$. Mamy $f[V] \subset Z \subset Y$ oraz $Y \sim V$ i $V \sim f[V]$, a stąd $Y \sim f[V]$. Na mocy Lematu 1, $Z \sim Y$, a więc $X \sim Y$. Q.E.D.

Twierdzenie 3. $\forall_{X,Y}(\overline{\overline{X}} \leq \overline{\overline{Y}} \vee \overline{\overline{Y}} \leq \overline{\overline{X}})$.

Dowód. Niech X, Y będą dowolnymi zbiorami. Na mocy tw. Zermelo istnieją dobre porządki $\leq_X$ na X i $\leq_Y$ na Y. Na mocy zasady trychotomii dla zbiorów dobrze uporządkowanych, zbiór $(X, \leq_X)$ jest izomorficzny z odcinkiem początkowym zbioru $(Y, \leq_Y)$ lub odwrotnie. Ponieważ każdy izomorfizm jest bijekcją, więc zbiór X jest równoliczny z podzbiorem zbioru Y lub odwrotnie. Q.E.D.

Twierdzenie 4. Zbiór X jest nieskończony wtedy i tylko wtedy, gdy $\aleph_0 \leq \overline{\overline{X}}$.

Dowód. ($\Leftarrow$). Zakładamy $\aleph_0 \leq \overline{\overline{X}}$. Wtedy zbiór $\mathbb{N}$ jest równoliczny z pewnym zbiorem $Z \subset X$. Ponieważ zbiór $\mathbb{N}$ jest nieskończony, więc zbiór Z jest nieskończony. Wobec tego zbiór X jest nieskończony (Fakt 2(a)).

($\Rightarrow$). Zakładamy, że zbiór X jest nieskończony, czyli nie jest równoliczny z żadną liczbą naturalną. Wtedy $X \neq \emptyset$. Niech F będzie funkcją wyboru dla rodziny wszystkich niepustych podzbiorów zbioru X (F istnieje na mocy Tw. 8.3).

Określamy funkcję $f : \mathbb{N} \mapsto X$.

$f(n) = F(X \setminus f[n])$ dla $n \in \mathbb{N}$

Jest to definicja indukcyjna: $f(n) = F(X \setminus \{f(k) : k < n\})$.

Przez indukcję względem n można udowodnić, że dla każdego n wartość $f(n)$ jest określona i różna od wszystkich $f(k)$ dla $k < n$.

Wobec tego $f : \mathbb{N} \mapsto X$ jest iniekcją, a stąd $\overline{\overline{\mathbb{N}}} \leq \overline{\overline{X}}$. Q.E.D.

Wniosek. Zbiór X jest skończony wtedy i tylko wtedy, gdy $\overline{\overline{X}} < \aleph_0$.

9.3. Zbiory przeliczalne

Definicja 5. Zbiór X nazywamy *przeliczalnym*, jeżeli $\overline{\overline{X}} \leq \aleph_0$.

Mamy: $\overline{\overline{X}} \leq \aleph_0 \Leftrightarrow \overline{\overline{X}} < \aleph_0 \vee \overline{\overline{X}} = \aleph_0$.

Zatem zbiór jest przeliczalny wtw, gdy jest skończony lub mocy $\aleph_0$.

Fakt 5. Zbiór jest mocy $\aleph_0$ wtw, gdy jest nieskończony i przeliczalny.

Sformułujemy użyteczne kryteria przeliczalności.

Fakt 6. Zbiór jest mocy $\aleph_0$ wtw, gdy jest zbiorem wszystkich wyrazów pewnego ciągu nieskończonego bez powtórzeń.

Fakt 7. Zbiór jest niepusty i przeliczalny wtw, gdy jest zbiorem wszystkich wyrazów pewnego ciągu nieskończonego.

Przykłady. Podamy dalsze przykłady zbiorów mocy $\aleph_0$.

1. Zbiór liczb całkowitych $\mathbb{Z}$. Wszystkie liczby całkowite można ustawić w ciąg nieskończony bez powtórzeń.

$0, -1, 1, -2, 2, -3, 3, \ldots$

Jest to ciąg $(a_n)_{n\in\mathbb{N}}$ określony następująco:

$a_n = k$ jeżeli $n = 2k$, $a_n = -(k+1)$ jeżeli $n = 2k+1$.

2. Zbiór wszystkich dodatnich liczb wymiernych $\mathbb{Q}^+$. Wszystkie ułamki $\frac{m}{n}$, gdzie $m, n \in \mathbb{N}^+$, można ustawić w tablicę nieskończoną.

$$\begin{array}{llll} \frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \ldots \\ \frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \ldots \\ \frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \ldots \\ \vdots & & & \end{array}$$

Wyrazy tej tablicy można ustawić w ciąg nieskończony wedle krótkich przekątnych, skierowanych od prawej do lewej ukośnie w dół.

$$\overbrace{\frac{1}{1}}\ ,\overbrace{\frac{1}{2},\frac{2}{1}},\overbrace{\frac{1}{3},\frac{2}{2},\frac{3}{1}},\ldots$$

Usuwając z tego ciągu ułamki skracalne, otrzymamy nieskończony ciąg bez powtórzeń, którego zbiór wyrazów jest równoliczny z $\mathbb{Q}^+$.

3. Zbiór wszystkich liczb wymiernych $\mathbb{Q}$. Pokazaliśmy, że $\mathbb{Q}^+$ jest zbiorem wyrazów pewnego ciągu nieskończonego bez powtórzeń $(q_n)_{n\in\mathbb{N}}$. W takim razie zbiór ujemnych liczb wymiernych $\mathbb{Q}^-$ można ustawić w analogiczny ciąg: $(-q_n)_{n\in\mathbb{N}}$. Ostatecznie cały zbiór $\mathbb{Q}$ można ustawić w ciąg następującej postaci.

$0, -q_0, q_0, -q_1, q_1, -q_2, q_2, \ldots$

Fakt 8. (a) Każdy podzbiór zbioru przeliczalnego jest przeliczalny. (b) Suma przeliczalnej rodziny zbiorów przeliczalnych jest zbiorem przeliczalnym.

Dowód. (a) Jeżeli $\overline{\overline{X}} \leq \aleph_0$ i $Y \subset X$, to $\overline{\overline{Y}} \leq \overline{\overline{X}} \leq \aleph_0$.

(b) Niech A będzie przeliczalną rodziną zbiorów przeliczalnych. Niech B będzie rodziną wszystkich niepustych zbiorów rodziny A. Wtedy $\bigcup B = \bigcup A$. Ponieważ $B \subset A$, więc rodzina B jest przeliczalna, na mocy (a). Jeżeli $B \neq \emptyset$, to $\bigcup B = \emptyset$, czyli $\bigcup B$ jest zbiorem przeliczalnym.

Zakładamy, że $B \neq \emptyset$. Wtedy zbiory rodziny B można ustawić w ciąg nieskończony $(B^{(n)})_{n\in\mathbb{N}}$, na mocy Faktu 7. Każdy zbiór $B^{(n)}$ można ustawić w ciąg nieskończony $(b_k^{(n)})_{k\in\mathbb{N}}$. Wszystkie elementy zbioru $\bigcup B$ można ustawić w ciąg nieskończony:

$b_0^{(0)}, b_1^{(0)}, b_0^{(1)}, b_2^{(0)}, b_1^{(1)}, b_0^{(2)}, \ldots$ Q.E.D.

Fakt 9. Jeżeli zbiory A, B są przeliczalne, to $A \times B$ jest zbiorem przeliczalnym.

Dowód. Niech A, B będą zbiorami przeliczalnymi. Jeżeli $A = \emptyset$ lub $B = \emptyset$, to $A \times B = \emptyset$, czyli zbiór $A \times B$ jest przeliczalny.

Zakładamy, że $A \neq \emptyset$ i $B \neq \emptyset$. Wtedy elementy zbioru A można ustawić w ciąg nieskończony $(a_n)_{n\in\mathbb{N}}$, a elementy zbioru B w ciąg nieskończony $(b_n)_{n\in\mathbb{N}}$. Wszystkie elementy zbioru $A \times B$ można ustawić w ciąg nieskończony:

$\langle a_0, b_0\rangle, \langle a_0, b_1\rangle, \langle a_1, b_0\rangle, \langle a_0, b_2\rangle, \langle a_1, b_1\rangle, \langle a_2, b_0\rangle, \ldots$ Q.E.D.

Symbolem A^* oznaczamy zbiór wszystkich skończonych ciągów, których wyrazy należą do zbioru A.

Fakt 10. Jeżeli A jest zbiorem przeliczalnym, to zbiór A^* jest przeliczalny.

DOWÓD. Niech A będzie zbiorem przeliczalnym. Przez $A^{(n)}$ oznaczamy zbiór wszystkich ciągów długości n, których wyrazy należą do A. Oczywiście $A^* = \bigcup_{n\in\mathbb{N}} A^{(n)}$.

Mamy: $A^{(0)} = \{\emptyset\}$. Jeżeli $A = \emptyset$, to $A^* = A^{(0)}$, czyli A^* jest zbiorem przeliczalnym.

Zakładamy, że $A \neq \emptyset$. Dla każdego $n \geq 1$ mamy $A^{(n)} \sim A^n$. Przez indukcję względem n można wykazać, że każdy zbiór A^n jest przeliczalny (korzystamy z Faktu 9). Stąd każdy zbiór $A^{(n)}$ jest przeliczalny.

Wobec tego $\{A^{(n)} : n \in \mathbb{N}\}$ jest przeliczalną rodziną zbiorów przeliczalnych. Na mocy Faktu 8(b), A^* jest zbiorem przeliczalnym. Q.E.D.

Liczbą algebraiczną nazywamy liczbę rzeczywistą, która jest pierwiastkiem pewnego wielomianu jednej zmiennej o współczynnikach całkowitych. Dowolna liczba wymierna $\frac{m}{n}$ jest liczbą algebraiczną, ponieważ jest pierwiastkiem wielomianu $nx - m$. Ponadto liczbami algebraicznymi są takie liczby niewymierne jak np. $\sqrt{2}$ (jest pierwiastkiem wielomianu $x^2 - 2$), $\sqrt[3]{2}$ (jest pierwiastkiem wielomianu $x^3 - 2$).

Wykażemy, że zbiór wszystkich liczb algebraicznych jest przeliczalny. Niezerowy wielomian $n-$tego stopnia jednej zmiennej o współczynnikach całkowitych można zapisać w postaci:

$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, gdzie $a_0, \ldots, a_n \in \mathbb{Z}$, $a_n \neq 0$.

Zbiór wszystkich niezerowych wielomianów jest równoliczny ze zbiorem wszystkich ciągów $(a_0, a_1, \ldots, a_n)$ takich, że $n \in \mathbb{N}$, $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ i $a_n \neq 0$.

Ten zbiór ciągów jest zawarty w $\mathbb{Z}^*$, a więc jest przeliczalny. Wobec tego zbiór wszystkich takich wielomianów jest przeliczalny (i niepusty), toteż można te wielomiany ustawić w ciąg nieskończony $(w_n)_{n\in\mathbb{N}}$.

Przez P_n oznaczmy zbiór wszystkich pierwiastków rzeczywistych wielomianu w_n. Wiadomo, że każdy zbiór P_n jest skończony.

Ponieważ zbiór liczb algebraicznych pokrywa się z $\bigcup_{n\in\mathbb{N}} P_n$, więc jest przeliczalny. Q.E.D.

W następnym podrozdziale wykażemy, że zbiór liczb rzeczywistych $\mathbb{R}$ jest *nieprzeliczalny*, tzn. nie jest przeliczalny.

9.4. Działania na liczbach kardynalnych. Zbiory nieprzeliczalne

Dla liczb kardynalnych rezerwujemy zmienne κ, μ, ν.

W tej symbolice prawa uporządkowania liczb kardynalnych przyjmują postać.

$\forall_\kappa(\kappa \leq \kappa)$ (prawo zwrotności)

$\forall_{\kappa,\mu}(\kappa \leq \mu \wedge \mu \leq \kappa \Rightarrow \kappa = \mu)$ (prawo antysymetrii; tw. C-B)

$\forall_{\kappa,\mu,\nu}(\kappa \leq \mu \wedge \mu \leq \nu \Rightarrow \kappa \leq \nu)$ (prawo przechodniości)

$\forall_{\kappa,\mu}(\kappa \leq \mu \vee \mu \leq \kappa)$ (prawo spójności)

Definicja 6. Niech $\kappa = \overline{\overline{X}}$, $\mu = \overline{\overline{Y}}$. Określamy działania dodawania, mnożenia i potęgowania liczb kardynalnych:

$\kappa + \mu = \overline{\overline{X \cup Y}}$, jeżeli $X \cap Y = \emptyset$,

$\kappa \cdot \mu = \overline{\overline{X \times Y}}$,

$\mu^\kappa = \overline{\overline{Y^X}}$.

Te definicje są poprawne, ponieważ zachodzą odpowiednie warunki zgodności.

$X_1 \sim Y_1 \wedge X_2 \sim Y_2 \Rightarrow X_1 \cup X_2 \sim Y_1 \cup Y_2$, pod warunkiem, że $X_1 \cap X_2 = Y_1 \cap Y_2 = \emptyset$

$X_1 \sim Y_1 \wedge X_2 \sim Y_2 \Rightarrow X_1 \times X_2 \sim Y_1 \times Y_2$

$X_1 \sim Y_1 \wedge X_2 \sim Y_2 \Rightarrow (X_1)^{X_2} \sim (Y_1)^{Y_2}$

Wykażemy pierwszy warunek. Niech $X_1 \cap X_2 = Y_1 \cap Y_2 = \emptyset$. Niech $f; X_1 \mapsto Y_1$ i $g : X_2 \mapsto Y_2$ będą bijekcjami. Wtedy funkcja $h : X_1 \cup X_2 \mapsto Y_1 \cup Y_2$ określona wzorem:

$h(a) = f(a)$ dla $a \in X_1$, $h(a) = g(a)$ dla $a \in X_2$

jest bijekcją (łatwe ćwiczenie).

Podobnie z dwóch bijekcji $f : X_1 \mapsto Y_1$ i $g : X_2 \mapsto Y_2$ tworzymy bijekcję $h : X_1 \times X_2 \mapsto Y_1 \times Y_2$, daną wzorem:
$h(\langle a, b\rangle) = \langle f(a), g(b)\rangle$ dla $\langle a, b\rangle \in X_1 \times X_2$.

Wreszcie z dwóch bijekcji $f : X_1 \mapsto Y_1$ i $g : X_2 \mapsto Y_2$ tworzymy bijekcję $H : (X_1)^{X_2} \mapsto (Y_1)^{Y_2}$, daną wzorem:

$H(h) = f \circ h \circ g^{-1}$ dla funkcji $h : X_2 \mapsto X_1$.

Oczywiście $H(h) : Y_2 \mapsto Y_1$.

Wiadomo, że $f^{-1} \circ f = \mathrm{I}_{X_1}$, $f \circ f^{-1} = \mathrm{I}_{Y_1}$ i podobnie dla g.

Wykazujemy, że H jest iniekcją. Niech $H(h_1) = H(h_2)$. Wtedy:

$h_1 = f^{-1} \circ H(h_1) \circ g = f^{-1} \circ H(h_2) \circ g = h_2$.

Wykazujemy, że odwzorowanie H jest suriekcją. Rozważmy dowolną funkcję $\bar{h} : Y_2 \mapsto Y_1$. Wtedy $f^{-1} \circ \bar{h} \circ g : X_2 \mapsto X_1$. Mamy:

$H(f^{-1} \circ \bar{h} \circ g) = f \circ f^{-1} \circ \bar{h} \circ g \circ g^{-1} = \bar{h}$.

Uwaga. Dla liczb naturalnych te działania pokrywają się z normalnymi działaniami dodawania, mnożenia i potęgowania liczb naturalnych.

Fakt 11. $\mathcal{P}(X) \sim \{0,1\}^X$ dla dowolnego zbioru X.

Dowód. Każdemu zbiorowi $A \subset X$ odpowiada *funkcja charakterystyczna* zbioru A, tj. funkcja $c_A : X \mapsto \{0,1\}$ określona wzorem:

$c_A(a) = 1$ dla $a \in A$, $c_A(a) = 0$ dla $a \notin A$.

Oczywiście odwzorowanie $F : \mathcal{P}(X) \mapsto \{0,1\}^X$ określone wzorem: $F(A) = c_A$ dla $A \subset X$, jest bijekcją. Q.E.D.

Wniosek. Jeżeli $\overline{\overline{X}} = \kappa$, to $\overline{\overline{\mathcal{P}(X)}} = 2^\kappa$.

W szczególności $\overline{\overline{\mathcal{P}(\mathbb{N})}} = 2^{\aleph_0}$, $\overline{\overline{\mathcal{P}(\mathcal{P}(\mathbb{N}))}} = 2^{(2^{\aleph_0})}$ itd.

Z tw. Cantora otrzymujemy: $\kappa < 2^\kappa$ dla dowolnego κ.

Definicja 7. Liczbę kardynalną $2^{\aleph_0}$ nazywamy *mocą continuum* i oznaczamy symbolem $\mathfrak{c}$.

Z definicji $\mathfrak{c}$, jest to moc zbioru $\{0,1\}^{\mathbb{N}}$, czyli zbioru wszystkich nieskończonych ciągów binarnych. Na mocy Faktu 11, tę samą moc ma zbiór $\mathcal{P}(\mathbb{N})$, czyli zbiór potęgowy zbioru $\mathbb{N}$.

Twierdzenie 5. $\overline{\overline{\mathbb{R}}} = \mathfrak{c}$.

Dowód. Określamy funkcję $f : \{0,1\}^{\mathbb{N}^+} \mapsto [0,1)$ (przedział domknięto-otwarty):

$f((a_n)_{n\geq 1}) = 0, a_1 a_2 a_3 \ldots$.

Ta funkcja jest różnowartościowa, ponieważ dwa różne ułamki dziesiętne nie zawierające okresu (9) odpowiadają różnym liczbom rzeczywistym. Z drugiej strony liczby rzeczywiste można określić jako pewne podzbiory zbioru $\mathbb{Q}$ (patrz 8.2). Mamy:

$2^{\aleph_0} \leq \overline{\overline{[0,1)}} \leq \overline{\overline{\mathbb{R}}} \leq \overline{\overline{\mathcal{P}(\mathbb{Q})}} = 2^{\aleph_0}$.

Zatem $\overline{\overline{\mathbb{R}}} = 2^{\aleph_0}$. Przy okazji $\overline{\overline{[0,1)}} = 2^{\aleph_0}$. Q.E.D.

Podstawowe prawa arytmetyki liczb kardynalnych

$\forall_{\kappa,\mu}(\kappa+\mu=\mu+\kappa)$, bo $X\cup Y=Y\cup X$.

$\forall_{\kappa,\mu,\nu}((\kappa+\mu)+\nu=\kappa+(\mu+\nu))$, bo $(X\cup Y)\cup Z=X\cup(Y\cup Z)$.

$\forall_{\kappa,\mu}(\kappa\cdot\mu=\mu\cdot\kappa)$, bo $X\times Y\sim Y\times X$.

$\forall_{\kappa,\mu,\nu}((\kappa\cdot\mu)\cdot\nu=\kappa\cdot(\mu\cdot\nu))$, bo $(X\times Y)\times Z\sim X\times(Y\times Z)$.

$\forall_{\kappa,\mu,\nu}(\kappa\cdot(\mu+\nu)=\kappa\cdot\mu+\kappa\cdot\nu)$, bo
$X\times(Y\cup Z)=(X\times Y)\cup(X\times Z)$.

$\forall_{\kappa,\mu,\nu}(\kappa^{\mu}\cdot\kappa^{\nu}=\kappa^{\mu+\nu})$, bo $X^Y\times X^Z\sim X^{Y\cup Z}$, jeśli $Y\cap Z=\emptyset$.

$\forall_{\kappa,\mu,\nu}(\kappa^{\nu}\cdot\mu^{\nu}=(\kappa\cdot\mu)^{\nu})$, bo $X^Z\times Y^Z\sim(X\times Y)^Z$.

$\forall_{\kappa,\mu,\nu}((\kappa^{\mu})^{\nu}=\kappa^{\mu\cdot\nu})$, bo $(X^Y)^Z\sim X^{Y\times Z}$.

Wykażemy: $\kappa^\mu \cdot \kappa^\nu = \kappa^{\mu+\nu}$. Niech $\kappa = \overline{\overline{X}}$, $\mu = \overline{\overline{Y}}$, $\nu = \overline{\overline{Z}}$, przy czym $Y \cap Z = \emptyset$. Wtedy:

$\kappa^\mu \cdot \kappa^\nu = \overline{\overline{X^Y \times X^Z}}$, $\kappa^{\mu+\nu} = \overline{\overline{X^{Y \cup Z}}}$.

Wystarczy wykazać: $X^Y \times X^Z \sim X^{Y \cup Z}$. Określamy funkcję $H : X^Y \times X^Z \mapsto X^{Y \cup Z}$ wzorem:

$H(\langle f, g\rangle) = f \cup g$ dla $\langle f, g\rangle \in X^Y \times X^Z$.

Ponieważ $Y \cap Z = \emptyset$, więc $f \cup g$ jest funkcją, której dziedziną jest $Y \cup Z$, a zbiór wartości zawiera się w X. Ponadto $(f \cup g)|Y = f$ i $(f \cup g)|Z = g$. Wykażemy, że H jest iniekcją. Niech $H(\langle f, g\rangle) = H(\langle f', g'\rangle)$. Wtedy $f \cup g = f' \cup g'$, a więc:

$f = (f \cup g)|Y = (f' \cup g')|Y = f'$,
$g = (f \cup g)|Z = (f' \cup g')|Z = g'$.

Zatem $\langle f, g\rangle = \langle f', g'\rangle$. H jest suriekcją, ponieważ dla dowolnej funkcji $h : Y \cup Z \mapsto X$ mamy $h = H(\langle h|Y, h|Z\rangle)$.

$\aleph_0 + \aleph_0 = \aleph_0$. Tak jest, ponieważ zbiór $\mathbb{Z}$ (mocy $\aleph_0$) jest sumą dwóch zbiorów rozłącznych mocy $\aleph_0$, np. zbioru liczb naturalnych i zbioru liczb całkowitych ujemnych.

$\aleph_0 \cdot \aleph_0 = \aleph_0$. Tak jest, ponieważ $\mathbb{N} \times \mathbb{N}$ jest mocy $\aleph_0$.

$\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$. Mamy: $2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0}$.

Zatem $\overline{\overline{\mathbb{R} \times \mathbb{R}}} = \mathfrak{c}$ (moc zbioru wszystkich punktów płaszczyzny).

Podobnie $\mathbb{R}^n$ jest mocy $\mathfrak{c}$ dla dowolnego $n \geq 1$.

$\mathfrak{c}^{\aleph_0} = \mathfrak{c}$. Mamy: $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$.

Zatem $\overline{\overline{\mathbb{R}^{\mathbb{N}}}} = \mathfrak{c}$ (moc zbioru wszystkich nieskończonych ciągów liczb rzeczywistych).

$\aleph_0 \cdot \mathfrak{c} = \mathfrak{c}$. Mamy: $\mathfrak{c} \leq \aleph_0 \cdot \mathfrak{c} \leq \mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$.

$\mathfrak{c}^{\mathfrak{c}} = 2^{\mathfrak{c}}$. Mamy: $(2^{\aleph_0})^{\mathfrak{c}} = 2^{\aleph_0 \cdot \mathfrak{c}} = 2^{\mathfrak{c}}$.

Zatem $\overline{\overline{\mathbb{R}^{\mathbb{R}}}} = 2^{\mathfrak{c}}$ (moc zbioru wszystkich funkcji rzeczywistych).

Dla dowolnych $a, b \in \mathbb{R}$, $a < b$ mamy: $\overline{\overline{[a,b)}} = \mathfrak{c}$. W dowodzie Tw. 5 wykazaliśmy, że $\overline{\overline{[0,1)}} = \mathfrak{c}$. Określamy funkcję $f : [0,1) \mapsto [a,b)$ wzorem:

$f(x) = (b-a)x + a$ dla $0 \leq x < 1$.

Jest to funkcja liniowa, a więc różnowartościowa. Z równania $y = (b-a)x + a$ otrzymujemy: $x = \frac{y-a}{b-a}$; ponadto, jeżeli $a \leq y < b$, to $0 \leq x < 1$. Zatem f jest bijekcją przedziału $[0,1)$ na przedział $[a,b)$.

Dowolny przedział otwarty (a,b), gdzie $a < b$, jest mocy continuum. Mamy: $[\frac{a+b}{2}, b) \subset (a,b) \subset [a,b)$, a stąd $\mathfrak{c} \leq \overline{\overline{(a,b)}} \leq \mathfrak{c}$.

Każdy zbiór $X \subset \mathbb{R}$ zawierający jakiś przedział otwarty (a,b) jest mocy continuum. Mamy: $(a,b) \subset X \subset \mathbb{R}$, a stąd $\mathfrak{c} \leq \overline{\overline{X}} \leq \mathfrak{c}$.

W szczególności $\overline{\overline{[a,b]}} = \mathfrak{c}$.

Twierdzenie 6 (tw. Hessenberga). $\kappa \cdot \kappa = \kappa$ dla każdej nieskończonej liczby kardynalnej κ.

To twierdzenie jest równoważnikiem aksjomatu wyboru. Dowód wykorzystuje zbiory dobrze uporządkowane. Szczegóły pomijamy.

Wniosek. Dla dowolnych nieskończonych liczb kardynalnych κ, μ $\kappa + \mu = \kappa \cdot \mu = \max\{\kappa, \mu\}$.

Dowód. Zakładamy $\kappa \leq \mu$. Wtedy $\max\{\kappa, \mu\} = \mu$. Mamy: $\mu \leq \kappa + \mu \leq \mu + \mu \leq \mu \cdot \mu = \mu$ oraz $\mu \leq \kappa \cdot \mu \leq \mu \cdot \mu = \mu$. Podobnie rozumujemy dla $\mu \leq \kappa$. Q.E.D.

Z kolei potęgowanie nieskończonych liczb kardynalnych stwarza szereg nierozwiązanych problemów.

Hipoteza continuum. Nie istnieje κ takie, że $\aleph_0 < \kappa < \mathfrak{c}$.

Uogólniona hipoteza continuum. Dla żadnej nieskończonej liczby kardynalnej μ nie istnieje κ takie, że $\mu < \kappa < 2^\mu$.