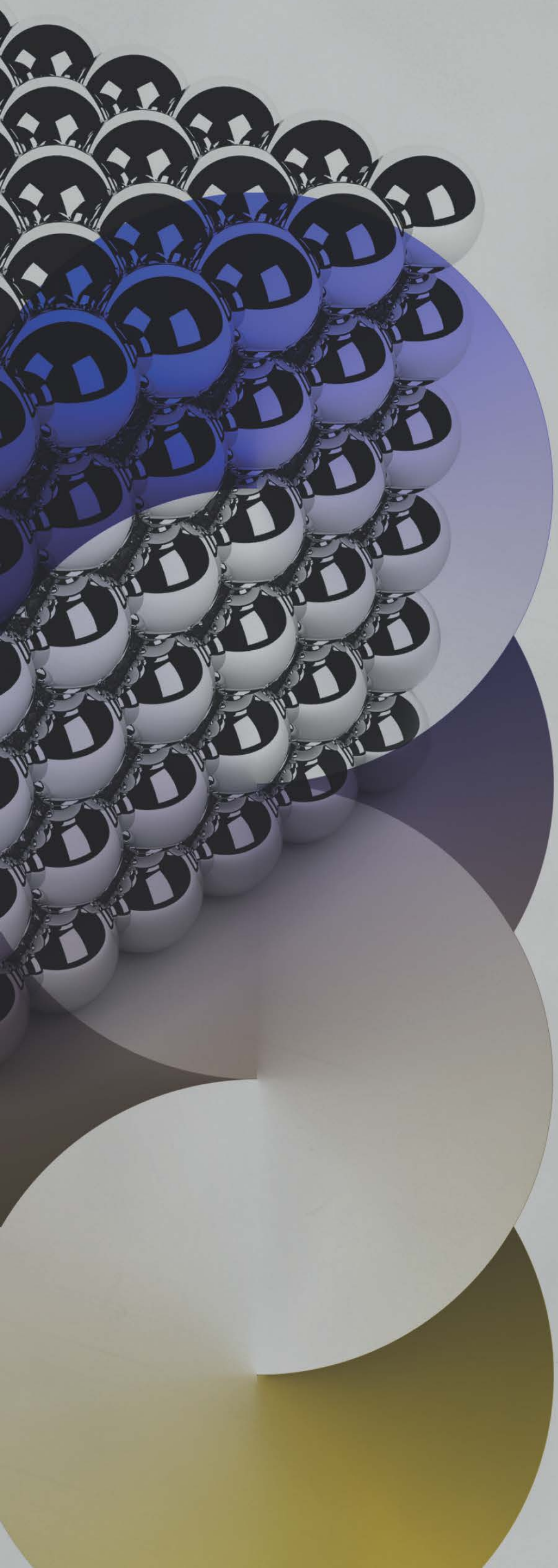


Biblio
theca
Philoso
phica

3(2018)

Marek Nowak

Elementy teorii mnogości

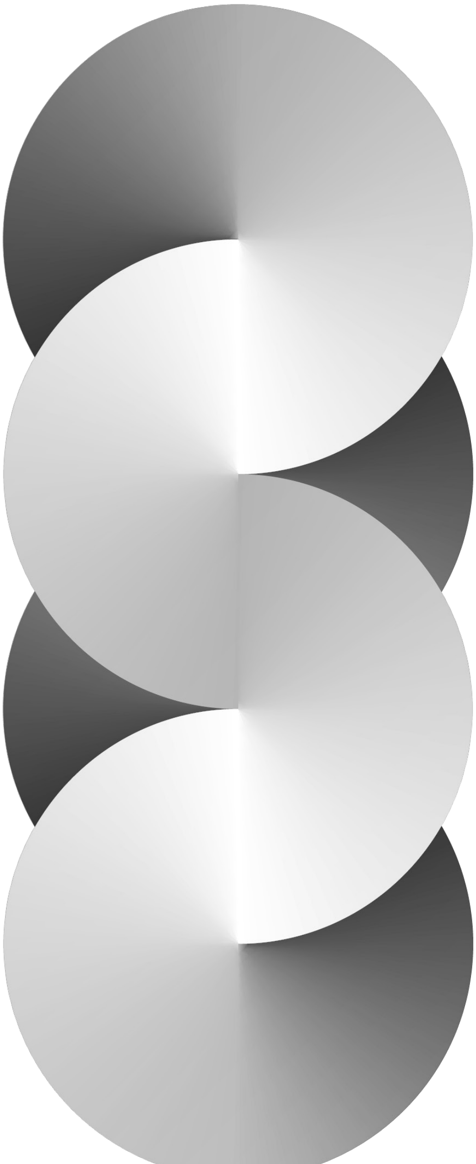
WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

Biblio
theca
Philoso
phica

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

Biblio
theca
Philoso
phica

3(2018)



Marek Nowak

Elementy teorii mnogości

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

Łódź 2018

Marek Nowak – Uniwersytet Łódzki, Wydział Filozoficzno-Historyczny, Instytut Filozofii
Katedra Logiki i Metodologii Nauk, 90-131 Łódź, ul. Lindleya 3/5

RECENZENT
Andrzej Pietruszczak

REDAKTOR INICJUJĄCY
Magdalena Skoneczna

KOREKTA
Paweł M. Sobczak

SKŁAD I ŁAMANIE
Marek Nowak

KOREKTA TECHNICZNA
Leonora Gralka

PROJEKT OKŁADKI
Katarzyna Turkowska

Zdjęcie wykorzystane na okładce: © Depositphotos.com/garloon

Wydrukowano z gotowych materiałów dostarczonych do Wydawnictwa UŁ

Wydane przez Wydawnictwo Uniwersytetu Łódzkiego
Wydanie I. W.08905.18.0.M

Ark. druk. 11,0

ISBN 978-83-8142-520-9
e-ISBN 978-83-8142-521-6

https://doi.org/10.18778/8142-520-9

Wydawnictwo Uniwersytetu Łódzkiego
90-131 Łódź, ul. Lindleya 8
www.wydawnictwo.uni.lodz.pl
e-mail: ksiegarnia@uni.lodz.pl
tel. (42) 665 58 63

Spis treści

Wstęp

Niniejsza praca poświęcona jest teorii mnogości Zermelo-Fraenkla z aksjomatem wyboru, nazywanej w skrócie teorią ZFC (Z, F – pierwsze litery nazwisk jej twórców, C – pierwsza litera wyrazu *choice*, *axiom of choice* – aksjomat wyboru). Jest to teoria pierwszego rzędu, a więc klasa zdań ustalonego języka pierwszego rzędu zamknięta na relację wynikania. Zazwyczaj teoria pierwszego rzędu mająca zastosowanie gdzieś poza teorią modeli podawana jest w postaci aksjomatycznej, tzn. traktowana jako klasa wszystkich zdań ustalonego języka wynikających z ustalonego zbioru zdań zwanych aksjomatami tej teorii. Właśnie w takiej postaci teoria ZFC jest tu prezentowana.

Praca stanowi istotne rozszerzenie części rozdziału 2 z [11]. Przeznaczona jest dla humanistów niebędących matematykami (np. filozofów wykorzystujących teorię mnogości), ma więc charakter elementarny. Niemniej zakładamy znajomość aparatury pojęciowej logiki kwantyfikatorów z identycznością (logiki pierwszego rzędu), w szczególności znajomość języka tej logiki oraz metod dowodzenia zdań tego języka (zob. np. [3], [5], [16], [18], [19]). Bibliografia została ograniczona do pozycji „klasycznych".

Panom profesorom Andrzejowi Indrzejczakowi i Piotrowi Łukowskiemu oraz Recenzentowi tekstu, profesorowi Andrzejowi Pietruszczakowi, serdecznie dziękuję za cenne uwagi, istotnie ulepszające pierwotny tekst. Wyrazy podziękowania składam również pani mgr Beacie Promińskiej za trud włożony w redakcyjne opracowanie tekstu do druku.

§1. Wprowadzenie do zagadnień teorii mnogości

Język teorii mnogości wyposażony jest w jedyny pierwotny predykat 2-argumentowy $\in$ (naturalnie poza predykatem identyczności: $=$, traktowanym jako stała logiczna) i nie zawiera żadnych pierwotnych stałych indywidualnych ani pierwotnych symboli funkcyjnych. Predykat „$\in$" czytamy: „należy do" lub „jest elementem" (używamy zapisu: $x \notin y$ jako równoznacznego z negacją formuły atomowej: $x \in y$).

Teoria ZFC może być więc traktowana jako jedna z teorii ustalających i precyzujących znaczenie terminu: „jest elementem mnogości (zbioru)" czy też „jest częścią mnogości". Historycznie pierwszą z takich teorii formalnych jest tzw. naiwna teoria mnogości, sformułowana nieaksjomatycznie w drugiej połowie XIX stulecia przez Georga Cantora. Miała ona fundamentalny mankament – była sprzeczna. Sformułowanie teorii niesprzecznej, lecz zachowującej podstawowe intuicje znaczeniowe Cantora stało się celem badań na początku XX w. Jednym z owoców tych badań jest właśnie teoria ZFC. Aby przybliżyć owe intuicje Cantora, rozważmy przez chwilę tzw. aksjomatyczną teorię naiwną. Określają ją następujące aksjomaty:

$(Ax =)\ \forall x \forall y (\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$,

$(AxCan)\ \exists y \forall x (x \in y \Leftrightarrow \phi(x))$,

gdzie $\phi(x)$ jest formułą języka teorii, w której x jest przynajmniej jedną zmienną wolną oraz w której y nie jest zmienną wolną.

$(Ax =)$ zwany jest aksjomatem identyczności lub ekstensjonalności. $(AxCan)$ zwany jest aksjomatem lub pewnikiem Cantora. Nie jest to właściwie aksjomat (formuła języka), lecz schemat aksjomatu: w zależności od konkretnej postaci formuły $\phi(x)$ uzyskujemy z $(AxCan)$ konkretny aksjomat teorii.

Oba aksjomaty mają na celu formalnie ujmować następującą intuicję: dla dowolnie pomyślanej własności istnieje zbiór (mnogość) tych i tylko tych obiektów, którym ta własność przysługuje. Owa własność reprezentowana jest formalnie formułą $\phi(x)$ w $(AxCan)$. Właśnie $(AxCan)$ stwierdza istnienie zbioru y tych i tylko tych obiektów x, którym „własność" $\phi(x)$ przysługuje. Jednakże samo wyrażenie $(AxCan)$ nie wystarcza dla oddania owej intuicji. Niejawnie bowiem jest w niej mowa o dokładnie jednym zbiorze tych i tylko tych obiektów, którym dana własność przysługuje. Tymczasem $(AxCan)$ nie gwarantuje wcale istnienia dokładnie jednego zbioru y złożonego z obiektów x, dla których prawdą jest, że $\phi(x)$. Przykładowo rozważmy $\phi(x)$ postaci

$\forall z (x \neq z \Rightarrow x \in z)$,

odpowiadającą własności: jest częścią czegokolwiek różnego od siebie. Wówczas z $(AxCan)$ otrzymujemy zdanie:

$\exists y \forall x (x \in y \Leftrightarrow \forall z (x \neq z \Rightarrow x \in z))$.

Zinterpretujmy je w strukturze relacyjnej $(\{a, b, c\}, \in)$, gdzie a, b, c są różnymi od siebie obiektami oraz relacja $\in$ (nie odróżniana tu symbolicznie od predykatu $\in$) jest taka, że $c \in a$ i $c \in b$. Wówczas łatwo sprawdzić, że prawdziwe są formuły:

$\forall x (x \in a \Leftrightarrow \forall z (x \neq z \Rightarrow x \in z))$ oraz

$\forall x (x \in b \Leftrightarrow \forall z (x \neq z \Rightarrow x \in z))$

(nie odróżniamy tu obiektów a, b od stałych indywidualnych będących ich nazwami w tej interpretacji), tzn. istnieją dwa różne „zbiory" y dla których prawdą jest

$\forall x (x \in y \Leftrightarrow \forall z (x \neq z \Rightarrow x \in z))$.

Dodanie aksjomatu $(Ax{=})$ powoduje, że ów zbiór y, którego istnienie stwierdza $(AxCan)$ jest dokładnie jeden. $(Ax =)$ stwierdza utożsamienie zbiorów mających te same elementy. W podanej tu przykładowo interpretacji oczywiście $(Ax =)$ jest fałszywy, bowiem obiekty a, b mają jedyny element c (jeden i ten sam), nie są zaś identyczne.

Bardziej ogólnie, załóżmy, że w obecności $(Ax =)$, dla ustalonej (konkretnej) formuły $\phi(x)$ prawdziwe są dwie formuły uzyskane z $(AxCan)$:

(1) $\forall x(x \in a \Leftrightarrow \phi(x))$ oraz

(2) $\forall x(x \in b \Leftrightarrow \phi(x))$.

Wówczas mamy:

(3) $\forall x(x \in a \Leftrightarrow x \in b)$.

Weźmy bowiem dowolny x i w celu pokazania równoważności: $x \in a \Leftrightarrow x \in b$, załóżmy, że $x \in a$. Wówczas z (1) mamy: $\phi(x)$, zatem z (2): $x \in b$. Tym samym mamy implikację: $x \in a \Rightarrow x \in b$. Dowód implikacji odwrotnej: $x \in b \Rightarrow x \in a$, jest analogiczny.

(3) w połączeniu z $(Ax =)$ w postaci: $\forall x(x \in a \Leftrightarrow x \in b) \Rightarrow a = b$, prowadzi do: $a = b$. Zatem zbiór, którego istnienie stwierdza $(AxCan)$ (dla ustalonej $\phi(x)$) jest dokładnie jeden.

Niestety, jak wiadomo, intuicja, której formalnym ujęciem są aksjomaty $(Ax =), (AxCan)$ okazuje się naiwna, ponieważ jest nieuzasadniona, by nie rzec fałszywa. Teoria oparta na tych aksjomatach jest bowiem sprzeczna (tzn. jest zbiorem wszystkich zdań swojego języka). Rozważmy mianowicie formułę $\phi(x)$ postaci: $x \notin x$, uzyskując z $(AxCan)$ aksjomat:

$\exists y \forall x(x \in y \Leftrightarrow x \notin x)$.

Oznaczmy ów jedyny zbiór, którego istnienie ta formuła stwierdza symbolem „a". Wówczas

$\forall x(x \in a \Leftrightarrow x \notin x)$, a stąd

$a \in a \Leftrightarrow a \notin a$.

Zdanie to, będące przecież postaci $A \Leftrightarrow \neg A$, w żadnej interpretacji nie jest prawdziwe. Sprzeczność ta nosi nazwę antynomii Russella, przyczyniła się ona do rozwoju badań teoriomnogościowych owocujących innymi niż naiwna teoriami mnogości.

Teoria ZFC nie posiada przedstawionego mankamentu teorii naiwnej. Oparta jest ona na innym zestawie aksjomatów (zachowany jest aksjomat identyczności), jednakże formuły postaci $(AxCan)$ są w niej obecne, choć nie dla wszystkich formuł

$\phi(x)$. Z powodu obecności $(Ax =)$ w ZFC, zbiór y, którego istnienie stwierdza w teorii ZFC formuła $\exists y \forall x (x \in y \Leftrightarrow \phi(x))$, jest jedyny. W ogólności, jest on oznaczany w znany sposób, jako: $\{x : \phi(x)\}$ (zbiór wszystkich takich x, że $\phi(x)$).

Zatem w teorii ZFC również stwierdza się istnienie zbiorów, których elementami są te i tylko te zbiory, którym przysługuje „własność” $\phi(x)$. Jednakże nie dla każdej „własności” taki zbiór istnieje. Przykładowo, można wykazać w ZFC, że, zgodnie z krytyką Russella teorii naiwnej, nie istnieje zbiór wszystkich zbiorów nie będących swoimi elementami ($\phi(x)$ postaci : $x \notin x$), co (w obecności aksjomatu regularności) jest równoważne nieistnieniu zbioru wszystkich zbiorów; innym przykładem jest nieistnienie zbioru wszystkich liczb porządkowych ($\phi(x)$ postaci: x *jest liczbą porządkową*).

Rozdział 1. Aksjomatyka ZFC i podstawowe pojęcia teoriomnogościowe

§1. Aksjomaty teorii mnogości

W literaturze przedmiotu spotyka się różne zestawy aksjomatów teorii ZFC (por. np. [4], [6], [7], [10], [12], [14], [17], [20], [21]). Wybieramy zestaw ośmiu aksjomatów z encyklopedycznej wersji teorii ZFC [20]. Aksjomaty są formułami, w których poza stałymi logicznymi, tzn. spójnikami $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$, kwantyfikatorami $\forall, \exists$ i predykatem identyczności $=$, występują zmienne indywidualne x, y, z, u, v, w oraz jedyny predykat: $\in$.

Adekwatne objaśnienie znaczenia niektórych aksjomatów jest możliwe dopiero po wprowadzeniu do teorii odpowiednich pojęć. Wówczas bowiem jest możliwy inny, równoważny zapis owych aksjomatów, w znacznie krótszej postaci, w której obok predykatu $\in$ pojawiają się symbole tych pojęć.

Aksjomat identyczności (lub ekstensjonalności):

$(Ax =)$ $\forall x \forall y(\forall z(z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$.

Zbiór x jest tożsamy ze zbiorem y, o ile zachodzi $\forall z(z \in x \Leftrightarrow z \in y)$, czyli gdy x, y mają te same elementy.

Aksjomat identyczności umożliwia definiowanie danego zbioru (o ile on istnieje) przez podanie, jakie zbiory są jego elementami. Wiedząc bowiem, jakie zbiory stanowią wszystkie elementy danego zbioru, mamy, dzięki $(Ax =)$, jednoznacznie ten zbiór wyznaczony.

Nie oznacza to, że dany zbiór można utożsamić z sekwencją czy ekspozycją jego elementów. Status ontyczny zbioru eksponowanych elementów jest taki sam jak status każdego z jego elementów (są to obiekty świata zbiorów), lecz różny od statusu ekspozycji.

Aksjomat Zermelo (lub podzbiorów albo selekcji):

$(AxZ)_\phi$ $\forall x(\phi(x) \Rightarrow x \in z) \Rightarrow \exists y \forall x(x \in y \Leftrightarrow \phi(x))$,

gdzie $\phi(x)$ jest dowolną formułą języka teorii, w której x jest przynajmniej jedną zmienną wolną oraz w której y nie jest zmienną wolną.

Podobnie jak rozważany wcześniej aksjomat Cantora, (AxZ) nie jest pojedynczym (konkretnym) aksjomatem teorii, lecz klasą aksjomatów, z której „wyjmuje” się konkretny aksjomat $(AxZ)_\phi$, dla konkretnej formuły $\phi(x)$.

Ponadto, jak widać, zmienna z jest w $(AxZ)_\phi$ zmienną wolną. Jednakże wszystkie formuły teorii ZFC (dotyczy to jakiejkolwiek teorii I rzędu), zatem również jej aksjomaty winny być domknięte, tzn. nie występują w nich zmienne wolne. Fakt, że w $(AxZ)_\phi$ pojawia się co najmniej jedna zmienna wolna z – być może w konkretnie wziętej formule $\phi(x)$ występują jeszcze inne zmienne wolne niż zmienna x, które to zmienne są wolne w całej formule $(AxZ)_\phi$ – jest oparty na powszechnie przyjętej konwencji notacyjnej, według której formułę $\psi(x_1, \ldots x_n)$, w której $x_1, \ldots x_n$ są wszystkimi jej zmiennymi wolnymi postrzega się jako formułę uniwersalnie domkniętą: $\forall x_1 \ldots \forall x_n(\psi(x_1, \ldots x_n))$, tzn. przed ową formułą ze zmiennymi wolnymi „widzi” się kwantyfikatory uniwersalne wiążące wszystkie te zmienne wolne. W przypadku zapisu formuły $(AxZ)_\phi$ zastosowanie owej konwencji notacyjnej jest bardzo wygodne, bowiem to, jakie zmienne mają być wiązane kwantyfikatorami uniwersalnymi umieszczonymi przed $(AxZ)_\phi$ zależy przecież od konkretnej postaci formuły $\phi(x)$.

Widać, że następnik implikacji $(AxZ)_\phi$ jest identyczny z formułą $(AxCan)$. Funkcja jaką spełnia $(AxZ)_\phi$ w teorii ZFC jest więc podobna do tej jaką aksjomat Cantora pełni w naiwnej teorii mnogości. Mianowicie, dla konkretnej formuły $\phi(x)$, z aksjomatu $(AxZ)_\phi$ wnioskujemy również istnienie zbioru y tych i tylko tych zbiorów x, dla których zachodzi $\phi(x)$. Jednakże wnioskowanie to jest uprawnione jedynie wówczas, gdy $\phi(x)$ jest taką formułą, że spełniony jest poprzednik $(AxZ)_\phi : \forall x(\phi(x) \Rightarrow x \in z)$, gdzie z jest jakimś dowolnie wybranym, ustalonym zbiorem.

Stwierdzenie prawdziwości owego poprzednika zabezpiecza klasę aksjomatów (AxZ) przed sprzecznością. Bowiem to, że jest on prawdziwy, oznacza, że elementy zbioru y, którego istnienie stwierdza następnik w $(AxZ)_\phi$ należą do wcześniej danego zbioru z; innymi słowy, $(AxZ)_\phi$ umożliwia utworzenie zbioru y z elementów danego zbioru z, czyli utworzenie *podzbioru* zbioru z. Intuicyjnie rzecz ujmując, nie widać nic absurdalnego czy prowadzącego do sprzeczności w możliwości łączenia niektórych elementów danego zbioru (tutaj oznaczonego symbolem „z”) w całość zwaną zbiorem (tutaj oznaczonym symbolem „y”). To zabezpieczenie przed sprzecznością powoduje jednakże, że siła dedukcyjna klasy formuł (AxZ) jest słabsza niż klasy formuł $(AxCan)$. Stąd teoria ZFC jest wyposażona w inne jeszcze aksjomaty niż teoria naiwna, tak, aby intuicyjnie pojmowany świat zbiorów, który miał być ujęty teorią naiwną, był opisany w teorii ZFC.

Z punktu widzenia historii rozwoju aksjomatyki teorii ZFC należy podkreślić, że aksjomat podany przez Zermelo oraz występujący w literaturze pod nazwą aksjomatu Zermelo ma właściwie postać następującą:

$(AxZer)_\phi$ $\exists y \forall x(x \in y \Leftrightarrow (x \in z \wedge \phi(x)))$.

Łatwo wykazać, że $(AxZ)_\phi$ jest implikowany przez $(AxZer)_\phi$: załóżmy bowiem $(AxZer)_\phi$ oraz poprzednik

(1) $\forall x(\phi(x) \Rightarrow x \in z)$

implikacji $(AxZ)_\phi$. Niech a będzie zbiorem, którego istnienie $(AxZer)_\phi$ stwierdza. Wówczas mamy:

(2) $\forall x(x \in a \Leftrightarrow (x \in z \wedge \phi(x)))$.

Wykazujemy:

(3) $\forall x(x \in a \Leftrightarrow \phi(x))$.

($\Rightarrow$): Niech $x \in a$. Wówczas z (2): $x \in z \wedge \phi(x)$, zatem $\phi(x)$.

($\Leftarrow$): Załóżmy, że zachodzi $\phi(x)$. Wówczas z (1): $x \in z$. Zatem $x \in z \wedge \phi(x)$. Ostatecznie $x \in a$ na mocy (2).

Na podstawie (3) otrzymujemy bezpośrednio następnik implikacji $(AxZ)_\phi : \exists y \forall x(x \in y \Leftrightarrow \phi(x))$.

Równie łatwo jest wykazać, że klasa formuł (AxZ) implikuje $(AxZer)_\phi$ dla dowolnej formuły ϕ: rozważmy bowiem dowolną $\phi(x)$ oraz załóżmy $(AxZ)_\psi$, gdzie $\psi(x)$ jest postaci: $x \in z \wedge \phi(x)$, tzn. załóżmy, że spełniona jest formuła:

(4) $\forall x((x \in z \wedge \phi(x)) \Rightarrow x \in z) \Rightarrow \exists y \forall x(x \in y \Leftrightarrow (x \in z \wedge \phi(x)))$.

Ponieważ poprzednik implikacji (4) jest prawdziwy, mamy więc następnik, czyli $(AxZer)_\phi$.

Aksjomat zbioru potęgowego:

(AxP) $\forall u \exists y \forall x(x \in y \Leftrightarrow \forall z(z \in x \Rightarrow z \in u))$.

Dla dowolnego zbioru u istnieje *zbiór potęgowy* zbioru u, tzn. zbiór, którego elementami są wszystkie podzbiory zbioru u i tylko one (formuła $\forall z(z \in x \Rightarrow z \in u)$ oznacza, że x jest podzbiorem zbioru u).

Aksjomat sumy:

$(Ax\bigcup)$ $\forall u \exists y \forall x(x \in y \Leftrightarrow \exists z(z \in u \wedge x \in z))$.

Dla dowolnego zbioru u istnieje *suma* zbioru u, tzn. zbiór, którego elementami są te i tylko te zbiory, które są elementami jakiegoś elementu zbioru u.

Aksjomat podstawiania (lub zastępowania):

$$(AxSUB)_\psi \ \forall y \exists z(\psi(y,z) \wedge \forall v(\psi(y,v) \Rightarrow v = z)) \Rightarrow$$
$$\exists u \forall z(z \in u \Leftrightarrow \exists y(y \in x \wedge \psi(y,z))),$$

gdzie $\psi(y,z)$ jest dowolną formułą języka teorii, w której y, z są zmiennymi wolnymi, zaś $\psi(y,v)$ jest formułą otrzymaną z $\psi(y,z)$ przez zastąpienie każdego wolnego występowania zmiennej z w $\psi(y,z)$ zmienną v.

Pod pewnymi względami $(AxSUB)_\psi$ zachowuje się analogicznie jak $(AxZ)_\phi$. Jest, jak widać, klasą różnych aksjomatów w zależności od różnych formuł $\psi(y,z)$. Ponadto wnioskujemy z konkretnego aksjomatu $(AxSUB)_\psi$ istnienie pewnego zbioru u, gdy poprzednik implikacji $(AxSUB)_\psi$ jest spełniony.

Ów poprzednik jest spełniony wówczas, gdy formuła $\psi(y,z)$ jest taka, że dla każdego zbioru y istnieje dokładnie jeden zbiór z taki, że zachodzi $\psi(y,z)$. Krótko mówiąc, wówczas, gdy dysponujemy formułą $\psi(y,z)$ ustalającą jakieś przyporządkowanie każdemu zbiorowi y dokładnie jednego zbioru z, mamy gwarancję istnienia zbioru u, o którym mowa w następniku implikacji $(AxSUB)_\psi$. Ów zbiór u jest zależny od jeszcze jednego parametru jakim jest zbiór oznaczony w $(AxSUB)_\psi$ zmienną (wolną) x. Mając więc dowolnie wybrany, ustalony zbiór x, na mocy $(AxSUB)_\psi$ stwierdzamy istnienie zbioru u tych i tylko tych zbiorów z, które są jednoznacznie przyporządkowane elementom zbioru x według formuły ψ.

Aksjomat nieskończoności:

$$(Ax\infty) \ \exists x[\exists y(y \in x \wedge \forall z(z \notin y)) \wedge$$
$$\forall y(y \in x \Rightarrow \exists z(z \in x \wedge \forall u(u \in z \Leftrightarrow (u \in y \vee u = y))))].$$

Jest to jedyny z aksjomatów teorii ZFC, który bezwarunkowo i niezależnie od istnienia innych zbiorów stwierdza istnienie pewnego zbioru, oznaczonego tu zmienną x, o własnościach opisanych formułą w nawiasach kwadratowych, i ze względu na te własności nazywanego zbiorem *indukcyjnym*. Własności te powodują, że zbiór indukcyjny ma nieskończenie wiele elementów. Aksjomat ten stwierdza więc istnienie w świecie zbiorów zbioru nieskończonego (bardziej precyzyjna analiza znaczenia tego aksjomatu podana jest w Rozdziale 7, §5).

Aksjomat regularności (lub ufundowania):

$$(AxR) \ \forall x[\exists y(y \in x) \Rightarrow \exists y(y \in x \wedge \forall z(z \in y \Rightarrow z \notin x))].$$

Każdy *niepusty* zbiór (tzn. taki zbiór x, że $\exists y(y \in x)$) posiada *element minimalny* (tzn. taki element y, który ze zbiorem x nie ma wspólnych elementów: $\forall z(z \in y \Rightarrow z \notin x)$) (rola jaką gra aksjomat regularności w teorii ZFC omówiona jest w Rozdziale 2).

Aksjomat wyboru:

$$(AxC)\ \forall z[\forall x \forall y(x \in z \wedge y \in z \Rightarrow [\exists u(u \in x) \wedge (\exists u(u \in x \wedge u \in y) \Rightarrow x = y)]) \\ \Rightarrow \exists u \forall x(x \in z \Rightarrow \exists v \forall w(w \in u \wedge w \in x \Leftrightarrow w = v))].$$

Dla dowolnego zbioru z takiego, że każdy jego element x jest zbiorem niepustym oraz jakiekolwiek dwa różne jego elementy x, y nie mają wspólnych elementów: $\forall x \forall y(x \in z \wedge y \in z \Rightarrow [\exists u(u \in x) \wedge (\exists u(u \in x \wedge u \in y) \Rightarrow x = y)])$, istnieje zbiór u, który z każdym elementem x zbioru z ma dokładnie jeden element wspólny: $\exists u \forall x(x \in z \Rightarrow \exists v \forall w(w \in u \wedge w \in x \Leftrightarrow w = v))$ (zob. Rozdział 10, §3).

§2. Inkluzja zbiorów

Mimo ubóstwa pojęć pierwotnych, teoria ZFC dysponuje niejakim bogactwem pojęć definiowanych. Tak jak w każdej teorii I rzędu, pojęcia te dzielimy na dwa rodzaje: relacje i operacje (w tym tzw. 0-argumentowe operacje tożsame z wyróżnionymi obiektami). Po stronie językowej odpowiadają tym pojęciom, odpowiednio, predykaty i symbole funkcyjne. W związku z tym mamy dwa rodzaje definicji nominalnych (tzn. definiujących wyrażenia): definicje predykatów oraz definicje symboli funkcyjnych.

Definicja predykatu wprowadza do języka teorii nowy predykat, w ten sposób, że formuła atomowa, zbudowana w oparciu o ten predykat, jest skrótem dla pewnej, zazwyczaj dość złożonej formuły, w której ów nowy predykat naturalnie nie występuje. Relację czy stosunek wyrażony definiowanym predykatem można więc również określić bez jego wprowadzania – przy pomocy owej formuły złożonej. W konsekwencji, kosztem długości zapisu, każdą z relacji rozważanych w teorii (poza pierwotnymi) można by wyrażać bez jej nazwy – predykatu, a wyłącznie przez odwoływanie się do formuł zawierających tylko terminy pierwotne teorii. Czego się naturalnie ze względów praktycznych nie czyni.

W przeciwieństwie do definicji predykatu, definicja symbolu funkcyjnego nie określa żadnego skrótu dla innej formuły, lecz dostarcza nazwy dla operacji, której istnienie jest niejawnie opisane w aksjomatach lub twierdzeniach teorii. Bez takiej definicji nie można operacji z aksjomatów czy twierdzeń „wydobyć”. Jeżeli operacja jest 0-argumentowa, czyli gdy jest ona wyróżnionym obiektem, jego istnienie i jedyność muszą być zagwarantowane w owych aksjomatach czy twierdzeniach. Dopiero po pokazaniu tych gwarancji można definicyjnie wprowadzić stałą indywidualną nazywającą ów obiekt. Podobnie, aksjomaty czy twierdzenia teorii muszą gwarantować istnienie n-argumentowego ($n \geq 1$) przyporządkowania (operacji) dowolnej sekwencji n obiektów dokładnie jednego obiektu, aby można było definicyjnie wprowadzić symbol funkcyjny wyrażający to przyporządkowanie.

Wprowadzanie pojęć niepierwotnych teorii ZFC zaczniemy od 2-argumentowego stosunku *inkluzji.*

Uwaga. Na oznaczanie obiektów opisywanych w teorii, a więc zbiorów, będziemy w dalszym ciągu używać zmiennych indywidualnych w postaci zarówno małych, jak i wielkich liter alfabetu łacińskiego, traktując zmienne postaci x, X jako różne. Stosujemy też zwyczajowo skrót „wtw" dla wyrażenia „wtedy i tylko wtedy, gdy". W dowodach twierdzeń postaci równoważności, znak „($\Rightarrow$)" oznacza, że przystępujemy do dowodu implikacji, której poprzednikiem jest lewy człon, zaś następnikiem prawy człon równoważności; znak „($\Leftarrow$)" oznacza, iż przystępujemy do dowodu implikacji odwrotnej. Zgodnie ze wzmiankowaną w §1 konwencją notacyjną, często nie piszemy kwantyfikatorów uniwersalnych na początku danego twierdzenia, pozostawiając w nim zmienne wolne.

DEFINICJA. Definiujemy 2-argumentowy predykat *inkluzji* $\subseteq$ (*zawierania się zbiorów*): $X \subseteq Y \Leftrightarrow \forall x(x \in X \Rightarrow x \in Y)$.

(Dla dowolnych zbiorów X, Y zbiór X *zawiera się* w zbiorze Y lub X *jest podzbiorem* zbioru Y wtw każdy element zbioru X jest elementem zbioru Y).

TWIERDZENIE 1. $X \subseteq X$.

DOWÓD. Rozważmy dowolny zbiór X. Wówczas prawdziwa jest formuła $\forall x(x \in X \Rightarrow x \in X)$ (biorąc bowiem pod uwagę dowolny zbiór x, prawdziwa jest implikacja $x \in X \Rightarrow x \in X$). Z definicji inkluzji, $X \subseteq X$. □

TWIERDZENIE 2. $(X \subseteq Y \wedge Y \subseteq X) \Rightarrow X = Y$.

DOWÓD. Załóżmy, że
(1) $X \subseteq Y$,
(2) $Y \subseteq X$.

Wykażemy najpierw, że
(3) $\forall x(x \in X \Leftrightarrow x \in Y)$.

Weźmy więc dowolny x. Dowodzimy równoważności $x \in X \Leftrightarrow x \in Y$.

($\Rightarrow$): Niech $x \in X$. Ponieważ na mocy (1) z definicji inkluzji mamy: $\forall x(x \in X \Rightarrow x \in Y)$, zatem również: $x \in X \Rightarrow x \in Y$, więc $x \in Y$.

Analogicznie dowodzimy odwrotnej implikacji korzystając z (2). Skorzystajmy teraz z aksjomatu $(Ax =)$ uzyskując wyrażenie $\forall x(x \in X \Leftrightarrow x \in Y) \Rightarrow X = Y$. Zatem, na mocy (3), $X = Y$. $\square$

Uwaga. Tw. 2 jest bardzo szeroko stosowane dla dowodzenia równości zbiorów. Aby wykazać, że $X = Y$ dowodzi się inkluzji $(\subseteq)$ tzn., że $X \subseteq Y$; następnie inkluzji $(\supseteq)$ tzn., że $Y \subseteq X$. (zob. np. dowód Tw. 6).

Twierdzenie 3. $(X \subseteq Y \wedge Y \subseteq Z) \Rightarrow X \subseteq Z$.

Dowód. Załóżmy, że
(1) $X \subseteq Y$ oraz
(2) $Y \subseteq Z$.

Aby wykazać, że $X \subseteq Z$ musimy zgodnie z definicją inkluzji dowieść, że $\forall x(x \in X \Rightarrow x \in Z)$. Rozważmy więc jakiś zbiór x. Załóżmy, że $x \in X$. Z (1) mamy: $\forall x(x \in X \Rightarrow x \in Y)$. Zatem $x \in Y$. Ale z (2): $\forall x(x \in Y \Rightarrow x \in Z)$, zatem $x \in Z$. $\square$

§3. Zbiór pusty

Weźmy na chwilę pod uwagę aksjomat nieskończoności $(Ax\infty)$; oznaczmy zbiór, którego istnienie on stwierdza symbolem a. Rozważmy następnie aksjomat podzbiorów $(AxZ)_\phi$, taki, że formuła $\phi(x)$ jest postaci $x \neq x$:

$\forall z[\forall x(x \neq x \rightarrow x \in z) \rightarrow \exists y \forall x(x \in y \Leftrightarrow x \neq x)]$ (po dokonaniu uniwersalnego domknięcia).

Stąd otrzymujemy:

$\forall x(x \neq x \Rightarrow x \in a) \Rightarrow \exists y \forall x(x \in y \Leftrightarrow x \neq x)$.

Lecz poprzednik tej implikacji jest spełniony (dla dowolnego x, poprzednik implikacji: $x \neq x \Rightarrow x \in a$ jest fałszywy, zatem jest ona prawdziwa). Stąd prawdziwy w dziedzinie zbiorów jest następnik $\exists y \forall x(x \in y \Leftrightarrow x \neq x)$. Zbiór (dokładnie jeden), którego istnienie on stwierdza oznaczamy symbolem $\emptyset$ i nazywamy zbiorem *pustym*:

Definicja. $\forall x(x \in \emptyset \Leftrightarrow x \neq x)$, lub $\emptyset = \{x : x \neq x\}$.

Uwaga. Symbol $\emptyset$ jest stałą indywidualną wprowadzoną definicyjnie do języka teorii.

TWIERDZENIE 4. $\forall x(x \notin \emptyset)$ (*zbiór pusty nie ma elementów*).

DOWÓD. Załóżmy nie wprost, że $\neg\forall x(x \notin \emptyset)$. Wówczas $\exists x(x \in \emptyset)$, zatem dla jakiegoś zbioru a, $a \in \emptyset$. Wtedy z definicji zbioru $\emptyset$, $a \neq a$ co jest niemożliwe. $\square$

TWIERDZENIE 5. $\emptyset \subseteq X$.

DOWÓD. Rozważmy dowolny zbiór X. Wówczas formuła $\forall x(x \in \emptyset \Rightarrow x \in X)$ jest prawdziwa (biorąc bowiem pod uwagę dowolny zbiór x, na mocy Tw. 4 fałszywy jest poprzednik implikacji $x \in \emptyset \Rightarrow x \in X$, zatem jest ona prawdziwa). Wobec tego z definicji inkluzji, $\emptyset \subseteq X$. $\square$

TWIERDZENIE 6. $\forall x(x \notin X) \Rightarrow X = \emptyset$ (*zbiór $\emptyset$ jest jedynym zbiorem niemającym elementów*).

DOWÓD. Załóżmy, że $\forall x(x \notin X)$. Dowód równości $X = \emptyset$ opieramy na Tw. 2.

($\subseteq$): Wykazujemy, że $X \subseteq \emptyset$, tzn., że $\forall x(x \in X \Rightarrow x \in \emptyset)$. Weźmy więc pod uwagę zbiór x. Na mocy założenia: $x \notin X$, zatem implikacja $x \in X \Rightarrow x \in \emptyset$ jest prawdziwa (fałszywy poprzednik).

($\supseteq$): Należy pokazać, że $\emptyset \subseteq X$, ale to jest oczywistym wnioskiem z Tw. 5.

Ostatecznie na mocy Tw. 2 (w postaci: $(X \subseteq \emptyset \ \wedge\ \emptyset \subseteq X) \Rightarrow X = \emptyset$) wnosimy, że $X = \emptyset$. $\square$

WNIOSEK. *Dla dowolnego zbioru X, $\forall x(x \notin X) \Leftrightarrow X = \emptyset$ (inaczej: $X \neq \emptyset \Leftrightarrow \exists x(x \in X)$).*

DOWÓD. ($\Rightarrow$): Z Tw. 6.

($\Leftarrow$): Z Tw. 4. $\square$

§4. Zbiór potęgowy danego zbioru

Biorąc pod uwagę definicję inkluzji, możemy aksjomat zbioru potęgowego (AxP) zapisać w postaci:

$\forall u \exists y \forall x(x \in y \Leftrightarrow x \subseteq u)$.

Rozważmy więc dowolny zbiór U. Wówczas ten jedyny zbiór y, którego istnienie stwierdza formuła: $\exists y \forall x(x \in y \Leftrightarrow x \subseteq U)$ oznaczamy symbolem $P(U)$ i nazywamy *zbiorem potęgowym zbioru U* (jest to zbiór wszystkich podzbiorów zbioru U):

DEFINICJA. Dla dowolnego zbioru U,
$\forall x(x \in P(U) \Leftrightarrow x \subseteq U)$ lub $P(U) = \{x : x \subseteq U\}$.

Uwaga. Symbol P jest jednoargumentowym symbolem funkcyjnym nazywającym jednoargumentową operację przyporządkowującą każdemu zbiorowi jego zbiór potęgowy.

TWIERDZENIE 7. *Dla dowolnego zbioru* U : $\emptyset, U \in P(U)$.

DOWÓD. Ponieważ $\emptyset \subseteq U$ oraz $U \subseteq U$ (Tw. 5 i Tw. 1), więc z definicji zbioru potęgowego, $\emptyset \in P(U)$ oraz $U \in P(U)$. □

WNIOSEK. *Dla dowolnego zbioru* U, $P(U) \neq \emptyset$.

DOWÓD. Na podstawie Tw. 7 i Wniosku z Tw. 6. □

TWIERDZENIE 8. $X \subseteq Y \Leftrightarrow P(X) \subseteq P(Y)$.

DOWÓD. ($\Rightarrow$): Załóżmy, że $X \subseteq Y$. Niech $A \in P(X)$. Wówczas z definicji zbioru potęgowego, $A \subseteq X$. Zatem z założenia, na mocy Tw. 3, $A \subseteq Y$, czyli $A \in P(Y)$. Wobec dowolności wyboru zbioru A stwierdzamy, że $P(X) \subseteq P(Y)$.

($\Leftarrow$): Załóżmy, że $P(X) \subseteq P(Y)$. Ponieważ $X \in P(X)$ (Tw. 7), więc z założenia otrzymujemy: $X \in P(Y)$. Stąd $X \subseteq Y$. □

TWIERDZENIE 9. $\forall x(x \in P(\emptyset) \Leftrightarrow x = \emptyset)$ (*zbiór potęgowy zbioru pustego ma dokładnie jeden element: zbiór pusty*).

DOWÓD. ($\Rightarrow$): Załóżmy, że $x \in P(\emptyset)$. Zatem $x \subseteq \emptyset$. Wówczas, na mocy Tw. 5 oraz Tw. 2, $x = \emptyset$.

($\Leftarrow$): Na mocy Tw. 7. □

TWIERDZENIE 10. $\forall x[x \in P(P(\emptyset)) \Leftrightarrow (x = \emptyset \vee x = P(\emptyset))]$ (*zbiór potęgowy zbioru potęgowego zbioru pustego ma dokładnie dwa elementy: zbiór pusty oraz zbiór potęgowy zbioru pustego*).

DOWÓD. ($\Rightarrow$): Załóżmy, że $x \in P(P(\emptyset))$. Wówczas

(1) $x \subseteq P(\emptyset)$.

W celu wykazania alternatywy $x = \emptyset \vee x = P(\emptyset)$, załóżmy, że $x \neq \emptyset$.
Wówczas, na mocy Wniosku z Tw. 6, niech

(2) $a \in x$.

Wtedy z (1): $a \in P(\emptyset)$, a więc na mocy Tw. 9 mamy:

(3) $a = \emptyset$.

Wykazujemy teraz, że

(4) $P(\emptyset) \subseteq x$.

Niech więc $y \in P(\emptyset)$. Wówczas na podstawie Tw. 9, $y = \emptyset$. Zatem z (3): $y = a$ i konsekwentnie na mocy (2): $y \in x$.

Z (1) i (4) wnioskujemy, na mocy Tw. 2, iż $x = P(\emptyset)$.

($\Leftarrow$): Na mocy Tw. 7. $\square$

§5. Suma zbioru

Weźmy pod uwagę aksjomat sumy ($Ax\bigcup$) oraz dowolny zbiór u. Ten jedyny zbiór y, którego istnienie stwierdza formuła:

$$\exists y \forall x (x \in y \Leftrightarrow \exists z (z \in u \wedge x \in z))$$

nazywamy *sumą* (*uogólnioną*) $\bigcup u$ zbioru u.

DEFINICJA. Dla dowolnego zbioru u:
$\forall x (x \in \bigcup u \Leftrightarrow \exists z (z \in u \wedge x \in z))$ lub $\bigcup u = \{x : \exists z (z \in u \wedge x \in z)\}$.

Uwaga. Symbol $\bigcup$ jest jednoargumentowym symbolem funkcyjnym nazywającym operację przyporządkowującą każdemu zbiorowi u jego sumę $\bigcup u$, czyli zbiór tych i tylko tych elementów, które należą do przynajmniej jednego elementu zbioru u.

TWIERDZENIE 11. *Dla dowolnego zbioru* u:
(1) $\forall x (x \in u \Rightarrow x \subseteq \bigcup u)$, *czyli* $u \subseteq P(\bigcup u)$,
(2) *dla dowolnego* $y, \forall x (x \in u \Rightarrow x \subseteq y) \Rightarrow \bigcup u \subseteq y$,
(3) $\bigcup P(u) = u$,
(4) $\bigcup \emptyset = \emptyset$.

DOWÓD. Dla (1): Załóżmy, że $x \in u$. Aby wykazać inkluzję $x \subseteq \bigcup u$, niech $y \in x$. Zatem $\exists z (z \in u \wedge y \in z)$. Wobec tego z definicji sumy, $y \in \bigcup u$.

Dla (2): Załóżmy, że y jest takim zbiorem, że $\forall x (x \in u \Rightarrow x \subseteq y)$. Niech $v \in \bigcup u$. Wówczas $\exists z (z \in u \wedge v \in z)$. Zatem dla pewnego zbioru $a, a \in u$ oraz $v \in a$. Wobec tego z założenia mamy: $a \subseteq y$ (bo $a \in u$) skoro więc $v \in a$, to $v \in y$, co dowodzi inkluzji $\bigcup u \subseteq y$.

Dla (3): ($\supseteq$): Na mocy (1) zapisanego dla zbioru $P(u)$ w miejsce u mamy: $u \in P(u) \Rightarrow u \subseteq \bigcup P(u)$, zatem według Tw. 7, $u \subseteq \bigcup P(u)$. Aby dowieść inkluzji przeciwnej zauważmy, że $\forall x (x \in P(u) \Leftrightarrow x \subseteq u)$ i zastosujmy (2), gdzie w miejscu zbioru u wystąpi $P(u)$, zaś w miejscu zbioru y zbiór u. Z (2) mamy wówczas: $\forall x (x \in P(u) \Rightarrow x \subseteq u) \Rightarrow \bigcup P(u) \subseteq u$. Zatem, wobec prawdziwości poprzednika, otrzymujemy: $\bigcup P(u) \subseteq u$.

Dla (4): Załóżmy nie wprost, że $\bigcup\emptyset \neq \emptyset$. Wówczas dla pewnego a, $a \in \bigcup\emptyset$. Zatem $\exists z(z \in \emptyset \wedge a \in z)$ skąd dla pewnego b, $b \in \emptyset$, co jest niemożliwe. □

§6. Para zbiorów, zbiór jednoelementowy

Rozważmy aksjomat podstawiania $(AxSUB)_\psi$ dla formuły $\psi(y,z)$ postaci: $(y = \emptyset \wedge z = X) \vee (y \neq \emptyset \wedge z = Y)$ oraz dla zbioru oznaczonego zmienną x postaci $P(P(\emptyset))$:

$$\forall X \forall Y [\forall y \exists z(\psi(y,z) \wedge \forall v(\psi(y,v) \Rightarrow v = z)) \Rightarrow$$
$$\exists u \forall z(z \in u \Leftrightarrow \exists y(y \in P(P(\emptyset)) \wedge \psi(y,z)))].$$

Weźmy pod uwagę dowolne zbiory X, Y. Wówczas spełniony jest poprzednik implikacji w $(AxSUB)_\psi$, tzn. formuła $\forall y \exists z(\psi(y,z) \wedge \forall v(\psi(y,v) \Rightarrow v = z))$. Weźmy bowiem pod uwagę dowolny zbiór y. Naturalnie $y = \emptyset$ lub $y \neq \emptyset$. Gdy $y = \emptyset$, mamy: $\psi(y,X) \wedge \forall v(\psi(y,v) \Rightarrow v = X)$, gdy zaś $y \neq \emptyset$ wówczas prawdą jest: $\psi(y,Y) \wedge \forall v(\psi(y,v) \Rightarrow v = Y)$.

Formuła $\psi(y,z)$ ustala więc jednoznaczne przyporządkowanie każdemu zbiorowi y dokładnie jednego zbioru z, mianowicie, zbiorowi pustemu przyporządkowany jest zbiór X, zaś każdemu zbiorowi niepustemu przyporządkowany jest zbiór Y.

Prawdziwy jest więc następnik implikacji w $(AxSUB)_\psi$, czyli formuła

(1) $\exists u \forall z(z \in u \Leftrightarrow \exists y(y \in P(P(\emptyset)) \wedge \psi(y,z)))$.

Wyrażenie $\exists y(y \in P(P(\emptyset)) \wedge \psi(y,z))$ jest równoważne na mocy Tw. 10 formule

$$\exists y[(y = \emptyset \vee y = P(\emptyset)) \wedge ((y = \emptyset \wedge z = X) \vee (y \neq \emptyset \wedge z = Y))],$$

która z kolei (bierzemy tu pod uwagę Wniosek z Tw. 7 w postaci: $P(\emptyset) \neq \emptyset$) jest równoważna wyrażeniu $z = X \vee z = Y$. Ostatecznie z (1) otrzymujemy:

$$\exists u \forall z(z \in u \Leftrightarrow (z = X \vee z = Y)).$$

Ów jedyny zbiór u, którego istnienie stwierdza ostatnia formuła oznaczamy w postaci: $\{X, Y\}$ i nazywamy *parą zbiorów* lub, gdy $X \neq Y$ – *zbiorem 2-elementowym*:

Definicja. Dla dowolnych zbiorów X, Y,
$\forall z(z \in \{X,Y\} \Leftrightarrow (z = X \vee z = Y))$ lub $\{X,Y\} = \{z : z = X \vee z = Y\}$.

Ponadto dla dowolnego zbioru X, $\{X\} = \{X, X\}$, tzn. $\{X\} = \{z : z = X\}$ bądź $\forall z(z \in \{X\} \Leftrightarrow z = X)$. Zbiór $\{X\}$ nazywamy *singletonem* lub zbiorem *1-elementowym*, którego jedynym elementem jest X.

Przykład. Na podstawie Tw. 9 i Tw. 10 oraz $(Ax =)$, $P(\emptyset) = \{\emptyset\}$ oraz $P(P(\emptyset)) = \{\emptyset, P(\emptyset)\}$.

§7. Suma dwóch zbiorów

Definicja. Dla dowolnych zbiorów x, y zbiór $\bigcup\{x, y\}$, czyli sumę pary zbiorów $\{x, y\}$ nazywamy *sumą zbiorów* x, y i oznaczamy w postaci: $x \cup y$.

Uwaga. Symbol $\cup$ jest 2-argumentowym symbolem funkcyjnym nazywającym operację przyporządkowującą zbiorom x, y ich sumę $x \cup y$.

Twierdzenie poniżej konstytuuje pojęcie sumy dwóch zbiorów w znany sposób:

Twierdzenie 12. *Dla dowolnych zbiorów* x, y,
$\forall z(z \in x \cup y \Leftrightarrow (z \in x \vee z \in y))$ *(suma dwóch zbiorów jest zbiorem tych i tylko tych zbiorów, które należą do co najmniej jednego z tych dwóch zbiorów).*

Dowód. ($\Rightarrow$): Załóżmy, że $z \in x \cup y$, tzn. $z \in \bigcup\{x, y\}$. Wówczas dla pewnego $a \in \{x, y\}$, $z \in a$. Z definicji pary zbiorów, $a = x$ lub $a = y$. Niech $a = x$. Wówczas $z \in x$, stąd mamy: $z \in x \vee z \in y$. Analogicznie, gdy $a = y$.

($\Leftarrow$): Załóżmy, że $z \in x$ lub $z \in y$. Niech $z \in x$. Ponieważ $x = x$, więc z definicji pary zbiorów, $x \in \{x, y\}$. Zatem $\exists u(u \in \{x, y\} \wedge z \in u)$. Ostatecznie z definicji sumy, $z \in \bigcup\{x, y\}$, tzn. $z \in x \cup y$. Analogicznie, gdy $z \in y$. $\square$

Twierdzenie 13. *Dla dowolnych zbiorów* A, B, X*:*
(1) $A \subseteq A \cup B,\ B \subseteq A \cup B$,
(2) $(A \subseteq X \wedge B \subseteq X) \Rightarrow A \cup B \subseteq X$,
(3) $A \subseteq B \Leftrightarrow A \cup B = B$.

Dowód. Dla (1): Niech $x \in A$. Wówczas $x \in A \vee x \in B$, zatem według Tw. 12, $x \in A \cup B$, czyli $A \subseteq A \cup B$. Analogicznie dla drugiej inkluzji.

Dla (2): Załóżmy, że $A \subseteq X, B \subseteq X$. Niech $x \in A \cup B$. Wówczas $x \in A \vee x \in B$. Załóżmy, że $x \in A$. Wtedy $x \in X$ (skoro $A \subseteq X$). Załóżmy, że $x \in B$. Wówczas również $x \in X$ (bo $B \subseteq X$). Ostatecznie $x \in X$, czyli $A \cup B \subseteq X$.

Dla (3): ($\Rightarrow$): Załóżmy, że $A \subseteq B$. Wykazujemy, że $A \cup B = B$.

($\subseteq$): Niech $x \in A \cup B$. Wówczas $x \in A \vee x \in B$. Musimy wykazać, że $x \in B$. Wystarczy więc rozważyć przypadek, gdy alternatywa ta jest prawdziwa w ten sposób, że jej lewy człon jest prawdziwy, tzn. $x \in A$. Wówczas z założenia ($A \subseteq B$) mamy: $x \in B$.

($\supseteq$): Inkluzja $B \subseteq A \cup B$ zachodzi na mocy (1).

($\Leftarrow$): Załóżmy, że $A \cup B = B$. Niech $x \in A$. Wówczas $x \in A \vee x \in B$. Stąd $x \in A \cup B$. Zatem z założenia, $x \in B$. Ostatecznie $A \subseteq B$. $\square$

§8. Zbiór n-elementowy

Definicja. Dla dowolnego $n = 2, 3, \ldots$, dla dowolnych zbiorów $x_1, \ldots, x_n$, x_{n+1}, $\{x_1, \ldots, x_n, x_{n+1}\} = \{x_1, \ldots, x_n\} \cup \{x_{n+1}\}$.

Gdy wszystkie zbiory $x_1, \ldots, x_n (n \geq 1)$ są różne od siebie, zbiór $\{x_1, \ldots, x_n\}$ nazywamy *n-elementowym*.

Zbiór X nazywamy *skończonym*, gdy $X = \emptyset$ lub istnieje liczba naturalna $n \geq 1$ oraz zbiory $x_1, \ldots, x_n$ takie, że $X = \{x_1, \ldots, x_n\}$. Zbiór nazywamy *nieskończonym*, gdy nie jest on skończony.

Uwaga. Symbol $\{\ldots\}$ traktujemy jako n-argumentowy symbol funkcyjny nazywający n-argumentową operację przyporządkowującą sekwencji n zbiorów zbiór, którego elementami są wszystkie zbiory z tej sekwencji i tylko one. Intuicyjnie rzecz biorąc, ilość elementów zbioru n-elementowego wynosi n. Formalnie, problem ilości elementów zbioru będzie rozważany w Rozdziale 11.

Twierdzenie 14. *Dla dowolnego $n \geq 1$, dla dowolnych zbiorów $x_1, \ldots, x_n$,*
$(\{\})$ $\forall x(x \in \{x_1, \ldots, x_n\} \Leftrightarrow (x = x_1 \vee \ldots \vee x = x_n))$.

Dowód (indukcyjny; o dowodach indukcyjnych będzie mowa w Rozdziale 7, §1). Dla $n = 1$ oraz $n = 2$ warunek $(\{\})$ jest spełniony na mocy definicji singletonu oraz definicji pary zbiorów.

Załóżmy, że dla pewnego $n \geq 1$ warunek $(\{\})$ zachodzi dla dowolnych zbiorów $x_1, \ldots, x_n$. Mamy wykazać, że dla dowolnych zbiorów $x_1, \ldots, x_n, x_{n+1}$,
$\forall x(x \in \{x_1, \ldots, x_n, x_{n+1}\} \Leftrightarrow (x = x_1 \vee \ldots \vee x = x_n \vee x = x_{n+1}))$.

Weźmy więc pod uwagę jakieś zbiory $x_1, \ldots, x_n, x_{n+1}$. Wówczas z definicji zbioru $\{x_1, \ldots, x_n, x_{n+1}\}$, Tw. 12, założenia indukcyjnego oraz definicji singletonu mamy: $x \in \{x_1, \ldots, x_n, x_{n+1}\}$ wtw $x \in \{x_1, \ldots, x_n\}$ lub $x \in \{x_{n+1}\}$ wtw $(x = x_1 \vee \ldots \vee x = x_n)$ lub $x = x_{n+1}$ wtw $x = x_1 \vee \ldots \vee x = x_n \vee x = x_{n+1}$. □

Przykład. $P(\{x, y\}) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$ dla dowolnych zbiorów x, y.

§9. Iloczyn dwóch zbiorów

Rozważmy aksjomat podzbiorów $(AxZ)_\phi$, gdzie formuła $\phi(x)$ jest postaci $x \in u \wedge x \in v$, oraz w którym zbiór oznaczony zmienną z jest zbiorem u:

$$\forall u \forall v[\forall x((x \in u \wedge x \in v) \Rightarrow x \in u) \Rightarrow \exists y \forall x(x \in y \Leftrightarrow (x \in u \wedge x \in v))].$$

Weźmy pod uwagę dowolne zbiory u, v. Wówczas poprzednik implikacji w $(AxZ)_\phi$ jest prawdziwy, mamy zatem następnik

$\exists y \forall x (x \in y \Leftrightarrow (x \in u \wedge x \in v))$,

co prowadzi do definicji *iloczynu* $u \cap v$ zbiorów u, v:

DEFINICJA. Dla dowolnych zbiorów u, v,
$\forall x (x \in u \cap v \Leftrightarrow (x \in u \wedge x \in v))$ lub $u \cap v = \{x : x \in u \wedge x \in v\}$ (iloczyn dwóch zbiorów jest zbiorem tych i tylko tych zbiorów, które należą do każdego z tych dwóch zbiorów).

Zbiory u, v nazywamy *rozłącznymi*, gdy $u \cap v = \emptyset$ (tzn. gdy nie mają one wspólnego elementu).

TWIERDZENIE 15. *Dla dowolnych zbiorów* A, B, X:
(1) $A \cap B \subseteq A,\ A \cap B \subseteq B$,
(2) $(X \subseteq A \wedge X \subseteq B) \Rightarrow X \subseteq A \cap B$,
(3) $A \subseteq B \Leftrightarrow A \cap B = A$.

DOWÓD. Dla (1): Niech $x \in A \cap B$. Wówczas $x \in A \wedge x \in B$. Stąd $x \in A$, ostatecznie $A \cap B \subseteq A$. Analogicznie dla drugiej inkluzji.

Dla (2): Załóżmy, że $X \subseteq A, X \subseteq B$. Niech $x \in X$. Wówczas z założenia, $x \in A, x \in B$, czyli $x \in A \cap B$. Ostatecznie, $X \subseteq A \cap B$.

Dla (3): ($\Rightarrow$): Załóżmy, że $A \subseteq B$. Wykazujemy, że $A \cap B = A$. Inkluzja ($\subseteq$) zachodzi na mocy (1).

($\supseteq$): Niech $x \in A$. Wówczas z założenia, $x \in B$, zatem $x \in A \wedge x \in B$, czyli $x \in A \cap B$.

($\Leftarrow$): Załóżmy, że $A \cap B = A$. Aby dowieść, że $A \subseteq B$ przypuśćmy, że $x \in A$. Wówczas z założenia, $x \in A \cap B$. Stąd $x \in A \wedge x \in B$, a więc $x \in B$. $\square$

§10. Różnica zbiorów, dopełnienie zbioru

Postępując analogicznie z aksjomatem podzbiorów jak powyżej, lecz dla formuły $\phi(x)$ postaci: $x \in u \wedge x \notin v$, uzyskujemy definicję *różnicy* $u - v$ zbiorów u, v:

DEFINICJA. Dla dowolnych zbiorów u, v,
$\forall x (x \in u - v \Leftrightarrow (x \in u \wedge x \notin v))$ lub $u - v = \{x : x \in u \wedge x \notin v\}$.

TWIERDZENIE 16. *Dla dowolnych zbiorów* A, B, X:
(1) $A - B \subseteq A$,
(2) $(A - B) \cap B = \emptyset$,
(3) $(X \subseteq A \wedge X \cap B = \emptyset) \Rightarrow X \subseteq A - B$,
(4) $A \subseteq B \Leftrightarrow A - B = \emptyset$.

DOWÓD. Dla (1): Niech $x \in A - B$. Wówczas $x \in A \wedge x \notin B$. Stąd $x \in A$. Zatem $A - B \subseteq A$.

Dla (2): Załóżmy, że $(A - B) \cap B \neq \emptyset$. Wówczas dla jakiegoś zbioru x, $x \in (A-B)\cap B$. Wtedy $x \in A-B$ oraz $x \in B$. Z definicji różnicy zbiorów, $x \in A \wedge x \notin B$. Stąd $x \notin B$. Sprzeczność.

Dla (3): Załóżmy, że $X \subseteq A$ oraz $X \cap B = \emptyset$. Aby wykazać, że $X \subseteq A-B$, weźmy $x \in X$. Wówczas z założenia, że $X \subseteq A$ mamy: $x \in A$. Ponadto $x \notin B$ (gdyby $x \in B$, to $x \in X \cap B$, zatem $X \cap B \neq \emptyset$, co jest niemożliwe na mocy założenia). Zatem $x \in A - B$, czyli wobec dowolności wyboru elementu x, $X \subseteq A - B$.

Dla (4): ($\Rightarrow$): Załóżmy, że $A \subseteq B$ oraz że $A - B \neq \emptyset$. Wówczas istnieje taki x, że $x \in A - B$, tzn. $x \in A$ oraz $x \notin B$. Lecz skoro $A \subseteq B$ (założenie) oraz $x \in A$, więc $x \in B$. Sprzeczność.

($\Leftarrow$): Załóżmy, że $A - B = \emptyset$. W celu wykazania, że $A \subseteq B$ załóżmy, że $x \in A$. Naturalnie $x \in B \vee x \notin B$. Gdyby $x \notin B$, to $x \in A - B$ i konsekwentnie $A - B \neq \emptyset$, co jest niemożliwe na mocy założenia. Zatem $x \in B$, co dowodzi inkluzji $A \subseteq B$. □

DEFINICJA. Niech U będzie dowolnym zbiorem. Dla dowolnego $A \in P(U)$ niech $-A = U - A$. Przy ustalonym zbiorze U, $-$ jest jednoargumentową operacją zwaną operacją *dopełnienia*, tzn. $-A$ nazywamy dopełnieniem zbioru A (do zbioru U).

TWIERDZENIE 17. *Dla dowolnych* $A, B \in P(U)$:
(1) $-(A \cup B) = -A \cap -B$,
(2) $-(A \cap B) = -A \cup -B$,
(3) $--A = A$,
(4) $A \subseteq B \Leftrightarrow -B \subseteq -A$,
(5) $-A \cup A = U$,
(6) $-A \cap A = \emptyset$,
(7) $-U = \emptyset$,
(8) $-\emptyset = U$.

DOWÓD. Dla (1): ($\subseteq$): Niech $x \in -(A \cup B)$. Wówczas $x \in U$ oraz $x \notin A \cup B$. Stąd $x \notin A$ oraz $x \notin B$. Zatem $x \in -A$ oraz $x \in -B$, czyli $x \in -A \cap -B$.

($\supseteq$): Niech $x \in -A \cap -B$. Zatem $x \in -A$ oraz $x \in -B$, czyli $x \in U$ oraz $x \notin A$ i $x \notin B$. Stąd $x \notin A \cup B$, czyli $x \in -(A \cup B)$.

Dla (2): ($\subseteq$): Niech $x \in -(A \cap B)$. Wówczas $x \in U$ oraz $x \notin A \cap B$. Stąd $x \notin A \vee x \notin B$. Załóżmy, że $x \notin A$. Wtedy $x \in -A$, zaś $-A \subseteq -A \cup -B$, zatem $x \in -A \cup -B$. Załóżmy, że $x \notin B$. Wówczas $x \in -B$, lecz $-B \subseteq -A \cup -B$, więc $x \in -A \cup -B$.

($\supseteq$): Niech $x \in -A \cup -B$. Wówczas $x \in -A \vee x \in -B$. Załóżmy, że $x \in -A$. Wtedy $x \in U$ oraz $x \notin A$. Stąd $x \notin A \vee x \notin B$, czyli $x \notin A \cap B$. Zatem $x \in -(A \cap B)$.

Załóżmy, że $x \in -B$. Wówczas analogicznie jak przed chwilą otrzymujemy: $x \in -(A \cap B)$.

Dla (3): ($\subseteq$): Niech $x \in --A$. Zatem $x \in U$ oraz $x \notin -A$. Ostatnie wyrażenie jest równoważne formule $x \notin U \vee x \in A$. Skoro więc $x \in U$, to $x \in A$.

($\supseteq$): Niech $x \in A$. Ponieważ $A \subseteq U$, więc $x \in U$. Mamy: $x \notin -A$ (gdyby $x \in -A$, to $x \notin A$ wbrew założeniu). Ostatecznie $x \in U-(-A)$, tzn. $x \in --A$.

Dla (4): ($\Rightarrow$): Załóżmy, że $A \subseteq B$. Wówczas na mocy Tw. 13(3), $A \cup B = B$. Zatem $-(A \cup B) = -B$, co na mocy (1) implikuje: $-A \cap -B = -B$, więc również $-B \cap -A = -B$ i konsekwentnie na mocy Tw. 15(3), $-B \subseteq -A$.

($\Leftarrow$): Załóżmy, że $-B \subseteq -A$. Wówczas na mocy przed chwilą dowiedzionej implikacji otrzymujemy: $--A \subseteq --B$, zatem z (3): $A \subseteq B$.

Dla (5): Ponieważ $-A \subseteq U$ oraz $A \subseteq U$, więc na mocy Tw. 13(2), $-A \cup A \subseteq U$. Aby dowieść inkluzji ($\supseteq$) załóżmy, że $x \in U$. Naturalnie $x \in A \vee x \notin A$. Gdy $x \in A$, to oczywiście $x \in -A \cup A$ (bo $A \subseteq -A \cup A$), gdy zaś $x \notin A$, to $x \in -A$, a ponieważ $-A \subseteq -A \cup A$, więc $x \in -A \cup A$.

Dla (6): Załóżmy, że $-A \cap A \neq \emptyset$. Niech $x \in -A \cap A$. Wówczas $x \in -A$ oraz $x \in A$. Jednakże skoro $x \in -A$, to $x \notin A$. Sprzeczność.

Dla (7): Na podstawie (5), (1), (3) i (6) mamy: $-U = -(-A \cup A) = --A \cap -A = A \cap -A = \emptyset$ (bo naturalnie $A \cap -A = -A \cap A$).

Dla (8): Z (7): $-U = \emptyset$, zatem $--U = -\emptyset$, więc na mocy (3), $U = -\emptyset$. $\square$

§11. Przekrój zbioru niepustego

Zastosujmy aksjomat podzbiorów w postaci:

$$(AxZ)_\phi \ \forall u[\forall x(\forall z(z \in u \Rightarrow x \in z) \Rightarrow x \in \bigcup u) \Rightarrow \exists y \forall x(x \in y \Leftrightarrow \forall z(z \in u \Rightarrow x \in z))].$$

Rozważmy dowolny zbiór u. Naturalnie $u = \emptyset$ lub $u \neq \emptyset$. Gdy $u = \emptyset$, wyrażenie $\forall z(z \in u \Rightarrow x \in z)$ (dla ustalonego dowolnego zbioru x) jest prawdziwe, bowiem poprzednik implikacji: $z \in u \Rightarrow x \in z$ dla dowolnego zbioru z jest fałszywy. Tymczasem wyrażenie $x \in \bigcup u$ jest na mocy Tw. 11(4) fałszywe. Ostatecznie, poprzednik implikacji w nawiasach kwadratowych w $(AxZ)_\phi$ jest fałszywy. Nie możemy więc oderwać następnika.

Rozważmy jednakże przypadek: $u \neq \emptyset$. Wówczas ów poprzednik jest prawdziwy. Weźmy bowiem pod uwagę dowolny zbiór x oraz załóżmy, że $\forall z(z \in u \Rightarrow x \in z)$. Skoro $u \neq \emptyset$, więc dla pewnego zbioru a, $a \in u$. Wówczas z założenia, $x \in a$, zatem $\exists z(z \in u \wedge x \in z)$, czyli $x \in \bigcup u$.

Ostatecznie, dla dowolnego niepustego zbioru u odrywamy następnik w implikacji $(AxZ)_\phi$, co prowadzi do definicji *iloczynu* (*uogólnionego*) lub *przekroju* $\bigcap u$

niepustego zbioru u, jako zbioru tych wszystkich zbiorów x, które należą do każdego elementu zbioru u:

DEFINICJA. Dla dowolnego niepustego zbioru u,
$\forall x(x \in \bigcap u \Leftrightarrow \forall z(z \in u \Rightarrow x \in z))$ lub $\bigcap u = \{x : \forall z(z \in u \Rightarrow x \in z)\}$.

Przekrój niepustego zbioru ma analogiczne własności do podanych w Tw. 11(1),(2) dla sumy zbioru:

TWIERDZENIE 18. *Dla dowolnego niepustego zbioru* u:
(1) $\forall x(x \in u \Rightarrow \bigcap u \subseteq x)$,
(2) dla dowolnego y, $\forall x(x \in u \Rightarrow y \subseteq x) \Rightarrow y \subseteq \bigcap u$.

DOWÓD. Dla (1): Załóżmy, że $x \in u$. Niech $a \in \bigcap u$. Wówczas z definicji przekroju, $\forall z(z \in u \Rightarrow a \in z)$. Stąd i z założenia mamy: $a \in x$, co dowodzi inkluzji $\bigcap u \subseteq x$.

Dla (2): Załóżmy, że y jest takim zbiorem, że $\forall x(x \in u \Rightarrow y \subseteq x)$. Niech $a \in y$. Aby wykazać, że $a \in \bigcap u$ (co dowiedzie inkluzji $y \subseteq \bigcap u$) musimy dowieść, że $\forall z(z \in u \Rightarrow a \in z)$. Niech więc $z \in u$. Wówczas z założenia otrzymujemy: $y \subseteq z$ i dalej, skoro $a \in y$, to $a \in z$, co dowodzi wyrażenia $\forall z(z \in u \Rightarrow a \in z)$. $\square$

Przekrój pary zbiorów jest iloczynem jej elementów:

TWIERDZENIE 19. *Dla dowolnych zbiorów* $x, y : \bigcap\{x, y\} = x \cap y$.

DOWÓD. Rozważmy dowolny zbiór a. Mamy: $a \in \bigcap\{x, y\}$ wtw $\forall z(z \in \{x, y\} \Rightarrow a \in z)$ wtw $\forall z((z = x \vee z = y) \Rightarrow a \in z)$ wtw $(a \in x \wedge a \in y)$ wtw $a \in x \cap y$, co dowodzi, że $\forall v(v \in \bigcap\{x, y\} \Leftrightarrow v \in x \cap y)$. Zatem z aksjomatu równości $(Ax =)$ w postaci $\forall v(v \in \bigcap\{x, y\} \Leftrightarrow v \in x \cap y) \Rightarrow \bigcap\{x, y\} = x \cap y$ uzyskujemy: $\bigcap\{x, y\} = x \cap y$. $\square$

§12. Ciało zbiorów

DEFINICJA. Zbiór $\mathcal{C} \subseteq P(U)$ nazywamy *ciałem zbiorów* (dokładniej *ciałem podzbiorów* zbioru U), gdy
(1) $\mathcal{C} \neq \emptyset$,
(2) $\forall X(X \in \mathcal{C} \Rightarrow -X \in \mathcal{C})$,
(3) $\forall X \forall Y((X \in \mathcal{C} \wedge Y \in \mathcal{C}) \Rightarrow X \cap Y \in \mathcal{C})$.

PRZYKŁAD. Zbiór potęgowy $P(U)$ jest ciałem zbiorów (ciałem wszystkich podzbiorów zbioru U), bowiem $P(U) \neq \emptyset$ i gdy $X \in P(U)$, to $-X \in P(U)$ oraz gdy $X, Y \in P(U)$, czyli $X, Y \subseteq U$, to $X \cap Y \subseteq U$, zatem $X \cap Y \in P(U)$.

Innym przykładem ciała podzbiorów zbioru U jest zbiór $\{\emptyset, U\}$. Oczywiście warunek (1) definicji ciała zbiorów jest dla $\mathcal{C} = \{\emptyset, U\}$ spełniony. Warunek (2) jest spełniony na mocy Tw. 17(7),(8), natomiast warunek (3) na mocy oczywistych faktów: $U \cap U = U, \emptyset \cap \emptyset = \emptyset$ oraz $\emptyset \cap U = U \cap \emptyset = \emptyset$.

TWIERDZENIE 20. *Niech $\mathcal{C}$ będzie dowolnym ciałem podzbiorów zbioru U. Wówczas*
(1) $\forall X \forall Y((X \in \mathcal{C} \wedge Y \in \mathcal{C}) \Rightarrow X \cup Y \in \mathcal{C})$,
(2) $\emptyset \in \mathcal{C}$ *oraz* $U \in \mathcal{C}$.

DOWÓD. Niech $\mathcal{C} \subseteq P(U)$ będzie ciałem podzbiorów zbioru U.

Dla (1): Załóżmy, że $X, Y \in \mathcal{C}$. Wówczas na mocy warunku (2) definicji ciała zbiorów, $-X, -Y \in \mathcal{C}$. Stąd, na mocy warunku (3): $-X \cap -Y \in \mathcal{C}$. Wobec tego, na podstawie Tw. 17(1), $-(X \cup Y) \in \mathcal{C}$. Zatem znowu z warunku (2) definicji, $--(X \cup Y) \in \mathcal{C}$, co na mocy Tw. 17(3) daje: $X \cup Y \in \mathcal{C}$.

Dla (2): Na mocy warunku (1) definicji ciała zbiorów, niech $X \in \mathcal{C}$. Wówczas na podstawie warunku (2) tej definicji, $-X \in \mathcal{C}$. Zatem na podstawie warunku (3): $-X \cap X \in \mathcal{C}$, czyli na mocy Tw. 17(6), $\emptyset \in \mathcal{C}$. Konsekwentnie, na mocy (2) definicji ciała zbiorów, otrzymujemy: $-\emptyset \in \mathcal{C}$. Zatem według Tw. 17(8), $U \in \mathcal{C}$. □

WNIOSEK. *Ciało $\{\emptyset, U\}$ jest najmniejszym (w sensie inkluzji) ciałem podzbiorów zbioru U.*

DOWÓD. Na mocy Tw. 20(2) zbiór $\{\emptyset, U\}$ zawiera się w każdym ciele $\mathcal{C}$ podzbiorów zbioru U. □

PRZYKŁAD. Wszystkie ciała podzbiorów zbioru $U = \{a, b, c\}$:
$\{\emptyset, U\}, \{\emptyset, \{a\}, \{b, c\}, U\}, \{\emptyset, \{b\}, \{a, c\}, U\}, \{\emptyset, \{c\}, \{a, b\}, U\}, P(U)$.

Ciało zbiorów jest przykładem zbioru *zamkniętego na operacje*: $\cap, \cup, -$. Mówimy bowiem, że zbiór jest *zamknięty na* daną n-argumentową operację, gdy jej wartość na dowolnej sekwencji (tzn. obiekt przyporządkowany sekwencji) n elementów tego zbioru jest również elementem tego zbioru. Gdy zbiór jest zamknięty na daną operację, to mówimy, iż jest to *operacja* na *tym zbiorze*.

Rozważymy obecnie ilość elementów największego (w sensie inkluzji) ciała podzbiorów danego n-elementowego zbioru U, czyli po prostu ilość wszystkich podzbiorów zbioru U (ilość elementów zbioru potęgowego n-elementowego zbioru). W tym celu sformułujmy pomocniczy fakt, wykorzystywany dalej w dowodzie twierdzenia ustalającego ową ilość. Pojawiające się tu zbiory $\mathcal{A}, \mathcal{B}$ istnieją na mocy aksjomatu podzbiorów.

Lemat. *Niech U będzie dowolnym niepustym zbiorem oraz $a \in U$. Niech ponadto $\mathcal{A} = \{X : X \subseteq U \wedge a \notin X\}, \mathcal{B} = \{X : X \subseteq U \wedge a \in X\}$. Wówczas $\mathcal{A} \cup \mathcal{B} = P(U)$ oraz $\mathcal{A} \cap \mathcal{B} = \emptyset$. Ponadto zbiory $\mathcal{A}, \mathcal{B}$ mają tyle samo elementów.*

Dowód. Dowodzimy pierwszej równości. ($\subseteq$): Niech $X \in \mathcal{A} \cup \mathcal{B}$. Wówczas $X \in \mathcal{A} \vee X \in \mathcal{B}$. Gdy $X \in \mathcal{A}$, to $X \subseteq U$ oraz gdy $X \in \mathcal{B}$, to również $X \subseteq U$ z definicji zbiorów $\mathcal{A}, \mathcal{B}$, zatem ostatecznie $X \in P(U)$, czyli $\mathcal{A} \cup \mathcal{B} \subseteq P(U)$.

($\supseteq$): Załóżmy, że $X \in P(U)$. Wówczas $X \subseteq U$. Naturalnie $a \in X \vee a \notin X$. Gdy $a \in X$, to wówczas $X \in \mathcal{B}$, zatem $X \in \mathcal{A} \vee X \in \mathcal{B}$, czyli $X \in \mathcal{A} \cup \mathcal{B}$. Gdy zaś $a \notin X$, to $X \in \mathcal{A}$, czyli znowu $X \in \mathcal{A} \vee X \in \mathcal{B}$, skąd $X \in \mathcal{A} \cup \mathcal{B}$. Ostatecznie, $P(U) \subseteq \mathcal{A} \cup \mathcal{B}$.

Dowodzimy drugiej równości. Załóżmy, że $\mathcal{A} \cap \mathcal{B} \neq \emptyset$. Niech więc $X \in \mathcal{A} \cap \mathcal{B}$. Wówczas $X \in \mathcal{A}$ oraz $X \in \mathcal{B}$. Zatem $a \notin X$ oraz $a \in X$ z definicji zbiorów $\mathcal{A}, \mathcal{B}$. Sprzeczność.

Aby wykazać, że zbiory $\mathcal{A}, \mathcal{B}$ mają tę samą ilość elementów, weźmy pod uwagę dowolny $X \in \mathcal{A}$. Wówczas $X \subseteq U$ oraz $a \notin X$. Zatem $X \cup \{a\} \in \mathcal{B}$ (bo $X \cup \{a\} \subseteq U$ oraz $a \in X \cup \{a\}$).

Rozważmy przyporządkowanie każdemu elementowi X ze zbioru $\mathcal{A}$ elementu $X \cup \{a\}$ ze zbioru $\mathcal{B}$. Przyporządkowanie to ma dwie następujące własności:
(w1) dla dowolnych $X_1, X_2 \in \mathcal{A}, (X_1 \neq X_2 \Rightarrow X_1 \cup \{a\} \neq X_2 \cup \{a\})$,
(w2) dla dowolnego $Y \in \mathcal{B}$ istnieje $X \in \mathcal{A}$ taki, że $Y = X \cup \{a\}$.

Aby dowieść (w1) załóżmy: $X_1 \cup \{a\} = X_2 \cup \{a\}$ dla jakichś $X_1, X_2 \in \mathcal{A}$ i wykażmy równość $X_1 = X_2$.

($\subseteq$): Niech $x \in X_1$. Wówczas $x \in X_1 \cup \{a\}$. Zatem z założenia, $x \in X_2 \cup \{a\}$, czyli $x \in X_2 \vee x = a$. Lecz $x \neq a$ (gdyby bowiem $x = a$, to $x \notin X_1$, bo $a \notin X_1$ skoro $X_1 \in \mathcal{A}$). Zatem $x \in X_2$. Analogicznie dowodzi się inkluzji ($\supseteq$).

Aby dowieść (w2) rozważmy dowolny $Y \in \mathcal{B}$. Wówczas $Y \subseteq U$ oraz $a \in Y$. Ponieważ $Y - \{a\} \subseteq Y$, więc $Y - \{a\} \subseteq U$. Oczywiście $a \notin Y - \{a\}$. Zatem $Y - \{a\} \in \mathcal{A}$. Ponadto $(Y - \{a\}) \cup \{a\} = Y$. Mamy bowiem: $Y - \{a\} \subseteq Y$ oraz $\{a\} \subseteq Y$ (bo $a \in Y$). Stąd na mocy Tw. 13(2), $(Y - \{a\}) \cup \{a\} \subseteq Y$. Aby dowieść odwrotnej inkluzji załóżmy, że $x \in Y$. Naturalnie $x = a \vee x \neq a$. Jeśli $x = a$, to $x \in \{a\}$, zaś $\{a\} \subseteq (Y - \{a\}) \cup \{a\}$, czyli $x \in (Y - \{a\}) \cup \{a\}$. Gdy $x \neq a$, to $x \notin \{a\}$, zatem $x \in Y - \{a\}$, a ponieważ $Y - \{a\} \subseteq (Y - \{a\}) \cup \{a\}$, więc $x \in (Y - \{a\}) \cup \{a\}$.

Ostatecznie dla wybranego dowolnie $Y \in \mathcal{B}$ znaleźliśmy $X \in \mathcal{A}$ taki, że $Y = X \cup \{a\}$ (ów $X = Y - \{a\}$).

Jak widać, fakt, że zbiory $\mathcal{A}, \mathcal{B}$ mają tyle samo elementów, jest bezpośrednim wnioskiem z (w1) i (w2). Własność (w1) bowiem mówi, że w zbiorze $\mathcal{B}$ nie ma mniej elementów niż w zbiorze $\mathcal{A}$, zaś (w2) mówi, że w $\mathcal{B}$ nie ma więcej elementów niż w $\mathcal{A}$. $\square$

TWIERDZENIE 21. *Dla dowolnej liczby naturalnej n, dla dowolnego n-elementowego zbioru U, zbiór potęgowy $P(U)$ jest 2^n-elementowy.*

DOWÓD (indukcyjny). Dla $n = 0$, $U = \emptyset$. Wówczas $P(U) = \{\emptyset\}$ (Tw. 9), czyli $P(U)$ jest 2^0-elementowy. Ustalmy dowolne $n \geq 0$.

Założenie indukcyjne: dla dowolnego n-elementowego zbioru U, $P(U)$ jest 2^n-elementowy.

Teza indukcyjna (mamy ją dowieść): dla dowolnego $(n+1)$-elementowego zbioru U, zbiór $P(U)$ jest 2^{n+1}-elementowy.

Rozważmy $(n+1)$-elementowy zbiór U. Wówczas $U \neq \emptyset$. Niech $a \in U$ będzie dowolnie wybranym elementem. Oznaczmy:

$\mathcal{A} = \{X : X \subseteq U \wedge a \notin X\}$, $\mathcal{B} = \{X : X \subseteq U \wedge a \in X\}$.

Na mocy lematu mamy natychmiast:
(1) $A \cup \mathcal{B} = P(U)$ oraz
(2) $\mathcal{A} \cap \mathcal{B} = \emptyset$.

Wykażemy:
(3) $\mathcal{A} = P(U - \{a\})$.

Dowód (3) opieramy na następującej równoważności:
(4) $(X \subseteq U \wedge a \notin X)$ wtw $\forall x(x \in X \Rightarrow x \in U - \{a\})$, dla dowolnego zbioru X.

Aby dowieść (4) ($\Rightarrow$) załóżmy, że $X \subseteq U$ oraz $a \notin X$. Weźmy dowolny x. Niech $x \in X$. Wówczas $x \in U$. Ponadto $x \neq a$ (gdyby $x = a$, to $a \in X$ wbrew założeniu), czyli $x \notin \{a\}$. Ostatecznie $x \in U - \{a\}$.

(4) ($\Leftarrow$): Na odwrót, załóżmy, że $\forall x(x \in X \Rightarrow x \in U - \{a\})$. Aby wykazać inkluzję $X \subseteq U$, weźmy $x \in X$. Wówczas z założenia, $x \in U - \{a\}$, czyli $x \in U \wedge x \notin \{a\}$, skąd otrzymujemy, że $x \in U$. Aby wykazać, iż $a \notin X$, przypuśćmy, że $a \in X$. Wówczas z założenia: $a \in U - \{a\}$, co oznacza, że $a \in U \wedge a \notin \{a\}$. W szczególności więc $a \notin \{a\}$, czyli $a \neq a$, co jest niemożliwe.

Wykazujemy teraz (3):

($\subseteq$): Niech $X \in \mathcal{A}$. Wówczas $X \subseteq U \wedge a \notin X$. Zatem na mocy (4), $X \subseteq U - \{a\}$, czyli $X \in P(U - \{a\})$.

($\supseteq$): Na odwrót, załóżmy, że $X \in P(U - \{a\})$, tzn. $X \subseteq U - \{a\}$. Wówczas z (4) mamy natychmiast: $X \subseteq U \wedge a \notin X$, a zatem $X \in \mathcal{A}$.

Bezpośrednio na mocy lematu mamy:
(5) Zbiory $\mathcal{A}, \mathcal{B}$ mają tyle samo elementów.

Ponieważ zbiór $U - \{a\}$ jest n-elementowy, więc stosując do tego zbioru założenie indukcyjne, otrzymujemy: zbiór $P(U - \{a\})$ jest 2^n-elementowy. Zatem, na mocy (3), zbiór $\mathcal{A}$ jest 2^n-elementowy. Wobec tego, zgodnie z (5), zbiór $\mathcal{B}$ jest również 2^n-elementowy. Ostatecznie, w oparciu o (1) i (2) wnosimy, że zbiór $P(U)$ ma $2^n + 2^n$ elementów (bo ilość elementów sumy skończonych rozłącznych zbiorów jest równa sumie ilości elementów tych zbiorów), tzn. zbiór $P(U)$ jest 2^{n+1}-elementowy. $\square$

§13. Algebra Boole'a

Definicja. Dowolny zbiór A wraz z następującymi operacjami na nim, 2-argumentowymi: $\wedge, \vee$, 1-argumentową: $-$, oraz wyróżnionymi elementami: 1, 0, spełniającymi równości:

(1)	$x \wedge x = x$,	$x \vee x = x$,
(2)	$x \wedge y = y \wedge x$,	$x \vee y = y \vee x$,
(3)	$x \wedge (y \wedge z) = (x \wedge y) \wedge z$,	$x \vee (y \vee z) = (x \vee y) \vee z$,
(4)	$x \wedge (x \vee y) = x$,	$x \vee (x \wedge y) = x$,
(5)	$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$,	$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$,
(6)	$x \wedge 1 = x$,	$x \vee 0 = x$,
(7)	$-x \wedge x = 0$,	$-x \vee x = 1$,

nazywamy *algebrą Boole'a.*

Precyzyjniej: dowolny model $(A, \wedge, \vee, -, 1, 0)$ dla powyższych równości (dla języka I rzędu ze stałymi indywidualnymi 1, 0 oraz symbolami funkcyjnymi $\wedge, \vee, -$, bez symboli predykatywnych) nazywamy algebrą Boole'a.

Przykład. Układ $(\{1,0\}, \wedge, \vee, -, 1, 0)$, gdzie $1, 0$ są wartościami logicznymi odpowiednio, prawdy i fałszu oraz $\wedge, \vee, -$ są operacjami na tych wartościach logicznych odpowiadającymi warunkom prawdziwości w logice klasycznej dla spójników odpowiednio, koniunkcji, alternatywy i negacji, tzn. dla dowolnych $x, y \in \{1, 0\}$:

$x \wedge y = 1$, gdy $x = y = 1$, w przeciwnym wypadku $x \wedge y = 0$,

$x \vee y = 0$, gdy $x = y = 0$, w przeciwnym wypadku $x \vee y = 1$,

$-1 = 0, -0 = 1$,

jest 2-elementową algebrą Boole'a.

Twierdzenie 22. *Niech $\mathcal{C} \subseteq P(U)$ będzie ciałem podzbiorów zbioru U. Wówczas $(\mathcal{C}, \cap, \cup, -, U, \emptyset)$, gdzie $\cap, \cup$ są odpowiednio operacjami iloczynu i sumy dwóch zbiorów oraz $-$ jest operacją dopełnienia (do zbioru U) jest algebrą Boole'a.*

Dowód. Rzeczywiście, z definicji ciała zbiorów, $\cap$ oraz $-$ są odpowiednio 2- i 1-argumentowymi operacjami na zbiorze $\mathcal{C}$. Na mocy Tw. 20(1) również $\cup$ jest operacją na zbiorze $\mathcal{C}$, zaś zgodnie z Tw. 20(2), U oraz $\emptyset$ są elementami zbioru $\mathcal{C}$. Aby więc dowieść, że układ $(\mathcal{C}, \cap, \cup, -, U, \emptyset)$ jest algebrą Boole'a należy wykazać, że równości (1)–(7) z definicji algebry Boole'a, zapisane dla operacji $\cap, \cup, -$ oraz elementów wyróżnionych $U, \emptyset$, są spełnione.

Równości (1), (2) oraz (3) są w oczywisty sposób spełnione.

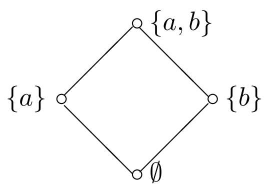
Weźmy dowolne $X, Y, Z \in \mathcal{C}$. Dla równości (4): $X \cap (X \cup Y) \subseteq X$, na mocy Tw. 15(1). Ponieważ $X \subseteq X$ oraz $X \subseteq X \cup Y$ (Tw. 1 oraz Tw. 13(1)), więc zgodnie z Tw. 15(2), $X \subseteq X \cap (X \cup Y)$. Ostatecznie, $X \cap (X \cup Y) = X$. Analogicznie dowodzimy drugą z równości (4).

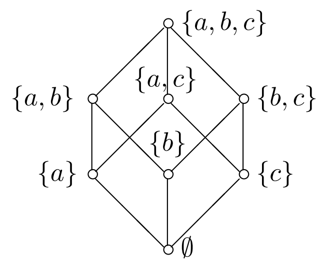
Dla (5): $X \cap Y \subseteq Y$ (Tw. 15(1)) oraz $Y \subseteq Y \cup Z$ (Tw. 13(1)), zatem na mocy Tw. 3, $X \cap Y \subseteq Y \cup Z$. Ponadto $X \cap Y \subseteq X$. Zatem, według Tw. 15(2), $X \cap Y \subseteq X \cap (Y \cup Z)$. Analogicznie wykazuje się, iż $X \cap Z \subseteq X \cap (Y \cup Z)$. Z dwóch ostatnich wyrażeń wnosimy, na mocy Tw. 13(2), iż $(X \cap Y) \cup (X \cap Z) \subseteq X \cap (Y \cup Z)$. Pozostaje dowieść odwrotnej inkluzji. Niech $x \in X \cap (Y \cup Z)$. Wówczas $x \in X$ oraz $x \in Y \cup Z$. Stąd $x \in Y$ lub $x \in Z$. Niech zatem $x \in Y$. Wówczas $x \in X \cap Y$, stąd $x \in (X \cap Y) \cup (X \cap Z)$. Gdy zaś $x \in Z$, to $x \in X \cap Z$, zatem również $x \in (X \cap Y) \cup (X \cap Z)$. Ostatecznie $X \cap (Y \cup Z) \subseteq (X \cap Y) \cup (X \cap Z)$. Analogicznie dowodzimy drugą z równości (5).

Dla (6): Równości: $X \cap U = X$ oraz $X \cup \emptyset = X$ wynikają odpowiednio z Tw. 15(3) (bo oczywiście $X \subseteq U$), oraz równości (2) (przemienność sumy), Tw. 13(3) i Tw. 5.

Równości (7) to Tw. 17(6),(5). □

Przykład. Zbiór potęgowy dowolnego zbioru wraz z odpowiednimi operacjami jest algebrą Boole'a. Ilustracje algebr Boole'a wszystkich podzbiorów zbioru $\{a, b\}$ oraz zbioru $\{a, b, c\}$ są następujące:





Linia łamana prowadząca ku górze (na każdym swoim odcinku) od jednego do drugiego zbioru, oznacza, że zbiór położony niżej jest podzbiorem zbioru będącego wyżej.

O algebrach Boole'a dowodzi się twierdzenia w pewnym sensie odwrotnego do Tw. 22: każda algebra Boole'a ma „strukturę algebraiczną” pewnego ciała zbiorów (zob. np. [22], w kwestii pojęć algebraicznych por. np. [8]).

Rozdział 2. Zbiory nieufundowane. Aksjomat regularności

W niniejszym rozdziale omawiamy rolę aksjomatu regularności w teorii ZFC. W tym celu rozważamy w pierwszych dwóch paragrafach teorię bez tego aksjomatu, zastępując go innym, nie należącym do ZFC (formuła (Ω)) – w ten sposób dopuszczając do istnienia zbiory *niemające elementu minimalnego* oraz tzw. zbiory *nieufundowane* (por. np. [1]). Aby oddać intuicje związane z pojęciami takich zbiorów, wprowadzamy nieformalne pojęcie *nieskończonego zejścia zbiorów*. Twierdzenia 2, 3, 5 tego rozdziału, a więc twierdzenia, w których to pojęcie występuje, należy zatem traktować nieformalnie – nie należą one do ZFC. Ponadto Tw. 1 również nie jest twierdzeniem tej teorii, lecz z innego powodu: jego sformułowanie wymaga aksjomatu (Ω). Natomiast Twierdzenia 4, 6, 7, 8, mimo, że występują w dwóch pierwszych paragrafach, a więc tam, gdzie rozważa się teorię ZFC bez aksjomatu regularności, ale z aksjomatem (Ω), są pełnoprawnymi twierdzeniami ZFC, bowiem w ich sformułowaniu i dowodach nie wykorzystuje się formuły (Ω).

§1. Zbiory niemające elementu minimalnego

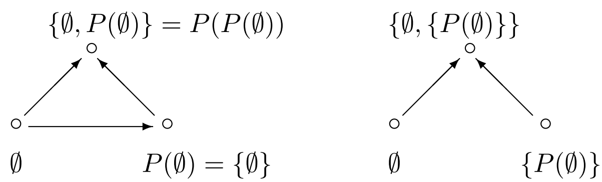
Definicja. Dla dowolnych zbiorów x, y, y jest *elementem minimalnym* zbioru x, gdy $y \in x$ oraz $y \cap x = \emptyset$.

Przykład. Zbiór $\emptyset$ jest (jedynym) elementem minimalnym zbioru $\{\emptyset, P(\emptyset)\}$. Zbiory $\emptyset$, $\{P(\emptyset)\}$ są elementami minimalnymi zbioru $\{\emptyset, \{P(\emptyset)\}\}$.

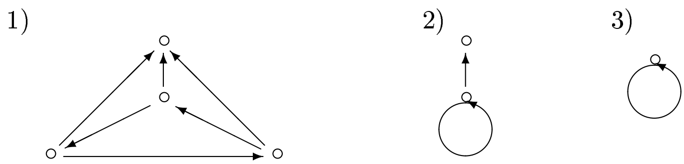
W celu określania elementów minimalnych w danym zbiorze, wygodnie jest posłużyć się ilustracją tzw. grafu zbioru.

Fakt, że $y \in x$ ilustrujemy w postaci: $y \circ \longrightarrow \circ\, x$, tzn. różne zbiory x, y oznaczamy różnymi punktami, a zachodzący między nimi stosunek należenia zaznaczamy odpowiednio strzałką. Przez ilustrację grafu zbioru x będziemy rozumieć rysunek, na którym znajdują się punkty odpowiadające zbiorowi x oraz wszystkim jego elementom, a także strzałki pokazujące wszystkie stosunki należenia, jakie zachodzą między zbiorami, którym odpowiadają owe punkty. Element minimalny zbioru x będzie wówczas oznaczony punktem, do którego nie „wchodzi” żadna strzałka „wychodząca” z jakiegoś elementu tego zbioru.

Przykład. Grafy dwóch zbiorów z przykładu powyżej:



Poniżej podajemy przykłady grafów zbiorów, które nie posiadają elementu minimalnego (gdyby takie zbiory istniały). Każdy z tych zbiorów ilustrowany jest punktem najwyżej na rysunku położonym. Pierwszy z tych zbiorów jest 3-elementowy, pozostałe dwa zbiory są jednoelementowe:



W dalszym ciągu rozważamy teorię ZFC bez aksjomatu regularności, zwykle wówczas oznaczaną jako ZFC$^-$. Ponadto do zestawu jej aksjomatów dodajemy formułę

(Ω) $\exists y \forall x (x \in y \Leftrightarrow x = y)$.

Oznaczmy zbiór, którego istnienie ona stwierdza symbolem Ω. Wówczas mamy:

(1) $\forall x (x \in \Omega \Leftrightarrow x = \Omega)$.

Z (1) otrzymujemy natychmiast: $\Omega \in \Omega$ oraz Ω jest jedynym takim zbiorem x, że $x \in \Omega$. Krótko mówiąc, Ω jest singletonem, którego jedynym elementem jest właśnie Ω. Precyzyjniej, można to wykazać następująco. Z definicji zbioru 1-elementowego mamy:

(2) $\forall x (x \in \{\Omega\} \Leftrightarrow x = \Omega)$.

Zatem z (1) oraz (2): $\forall x (x \in \Omega \Leftrightarrow x \in \{\Omega\})$, skąd przy użyciu aksjomatu identyczności uzyskujemy:

(3) $\Omega = \{\Omega\}$.

Zauważmy, że aksjomat identyczności nie gwarantuje wcale jedyności zbioru, którego istnienie stwierdza formuła (Ω), czyli różnych zbiorów Ω o własności (3) może istnieć więcej niż jeden. Mówiąc dalej o zbiorze Ω, mamy na myśli jakikolwiek ze zbiorów o własności (3). Jak widać, graf takiego zbioru jest przedstawiony powyżej na trzecim diagramie.

TWIERDZENIE 1. *Zbiór Ω nie ma elementu minimalnego.*

DOWÓD. Oczywiście jedynym elementem zbioru Ω jest Ω, lecz Ω nie jest elementem minimalnym zbioru Ω, bowiem $\Omega \cap \Omega \neq \emptyset$, skoro $\Omega \cap \Omega = \Omega = \{\Omega\} \neq \emptyset$. $\square$

DEFINICJA. Sekwencję zbiorów (niekoniecznie różnych) $x_1, x_2, \ldots, x_n, \ldots$ nazwiemy *nieskończonym wejściem* (*zejściem*), gdy $x_1 \in x_2, x_2 \in x_3, \ldots, x_{n-1} \in x_n, x_n \in x_{n+1}, \ldots$ $(\ldots, x_{n+1} \in x_n, x_n \in x_{n-1}, \ldots, x_3 \in x_2, x_2 \in x_1)$.

PRZYKŁAD. Sekwencja zbiorów $\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \ldots, \{..\{\emptyset\}..\}, \ldots$ jest nieskończonym wejściem. Natomiast sekwencja $\Omega, \{\Omega\}, \{\{\Omega\}\}, \ldots, \{..\{\Omega\}..\}, \ldots$ jest jednocześnie nieskończonym wejściem i zejściem. Z definicji singletonu jest bowiem oczywiste, że $\Omega \in \{\Omega\} \in \{\{\Omega\}\} \in \ldots \in \{\ldots\{\Omega\}\ldots\} \in \ldots$. Jednakże również mamy: $\ldots \in \{\ldots\{\Omega\}\ldots\} \in \ldots \in \{\{\Omega\}\} \in \{\Omega\} \in \Omega$, skoro na mocy (3), dowolny singleton $\{\ldots\{\Omega\}\ldots\}$ jest identyczny ze zbiorem Ω, zatem sam jest jedynym swoim elementem (powyższa sekwencja ma oczywiście postać: $\Omega, \Omega, \ldots, \Omega, \ldots$).

Uwaga. Pojęcie nieskończonego zejścia (wejścia), tak jak zostało tu wprowadzone, formalnie nie jest pojęciem teorii ZFC$^-$, bowiem bazuje ono na pojęciu sekwencji zbiorów, które z kolei jest tutaj pojęciem wyłącznie intuicyjnym, pierwotnie zakładanym, a więc nie należącym formalnie do teorii ZFC$^-$. Powodem, dla którego wprowadzamy pojęcie nieskończonego zejścia jest objaśnienie intuicji związanych z pojęciem *zbioru nieufundowanego*.

W dalszym ciągu twierdzenia, w których sformułowaniu bądź dowodzie pojawia się pojęcie nieskończonego zejścia będą oznaczane symbolem *.

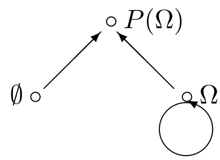
DEFINICJA. Powiemy, że zbiór x ma *nieskończone zejście*, gdy istnieje nieskończone zejście postaci: $x, x_1, x_2, \ldots, x_n, \ldots$. Wówczas będziemy mówić również, że takie nieskończone zejście jest *nieskończonym zejściem zbioru x*.

PRZYKŁAD. Naturalnie zbiór Ω ma nieskończone zejście: $\Omega, \Omega, \ldots, \Omega, \ldots$.

*TWIERDZENIE 2. *Każdy niepusty zbiór niemający elementu minimalnego ma nieskończone zejście.*

DOWÓD. Niech x będzie niepustym zbiorem niemającym elementu minimalnego. Wówczas dla pewnego zbioru y_1 mamy: $y_1 \in x$ (bo $x \neq \emptyset$). Z założenia, y_1 nie jest elementem minimalnym zbioru x, zatem $y_1 \cap x \neq \emptyset$. Istnieje więc zbiór y_2 taki, że $y_2 \in y_1$ oraz $y_2 \in x$. Choć y_2 jest elementem zbioru x, to jednak nie jest jego elementem minimalnym. Zatem istnieje zbiór y_3 taki, że $y_3 \in y_2$ oraz $y_3 \in x$. I tak dalej. Jest widoczne, że sekwencja $x, y_1, y_2, y_3, \ldots$ jest nieskończonym zejściem zbioru x. $\square$

Twierdzenie odwrotne do Tw. 2 nie jest prawdziwe. Istnieją zbiory (oczywiście w ramach ZFC$^-$ z aksjomatem (Ω)) z nieskończonym zejściem mające element minimalny. Na przykład zbiór $P(\Omega)$ ma tę własność: zbiór $\emptyset$ jest jego elementem minimalmym, chociaż sekwencja $\{\emptyset, \Omega\}, \Omega, \Omega, \ldots, \Omega, \ldots$ jest jego nieskończonym zejściem, jak na to wskazuje graf zbioru $P(\Omega)$:



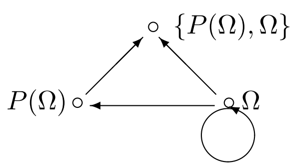
§2. Zbiory nieufundowane i ufundowane

DEFINICJA. Mówimy, że zbiór x jest *ufundowany*, gdy dla dowolnego zbioru y, jeżeli $x \in y$, to y ma element minimalny.

Gdy zbiór nie jest ufundowany, mówimy, że jest on *nieufundowany*. Zatem x jest nieufundowany, gdy jest on elementem pewnego zbioru nie mającego elementu minimalnego.

PRZYKŁAD. Zbiór $\emptyset$ jest ufundowany. Jeśli bowiem $\emptyset \in y$, to $\emptyset$ jest elementem minimalnym zbioru y, bo $\emptyset \cap y = \emptyset$.

Zbiór $P(\Omega)$ nie jest ufundowany. Rozważmy bowiem zbiór $\{P(\Omega), \Omega\}$. Naturalnie $P(\Omega) \in \{P(\Omega), \Omega\}$, lecz zbiór $\{P(\Omega), \Omega\}$ nie ma elementu minimalnego:



*TWIERDZENIE 3. *Każdy zbiór nieufundowany ma nieskończone zejście.*

DOWÓD. Niech x będzie zbiorem nieufundowanym. Wówczas dla pewnego zbioru y, $x \in y$ oraz y nie ma elementu minimalnego. Zatem x nie jest elementem minimalnym zbioru y, czyli $x \cap y \neq \emptyset$. Niech więc $y_1 \in x$ oraz $y_1 \in y$. y_1 nie jest elementem minimalnym zbioru y, zatem $y_1 \cap y \neq \emptyset$. Niech więc $y_2 \in y_1$ oraz $y_2 \in y$. I tak dalej. Naturalnie sekwencja $x, y_1, y_2, \ldots$ jest nieskończonym zejściem zbioru x. $\square$

Jak widać na podstawie Twierdzeń 2 i 3, niepuste zbiory nie mające elementu minimalnego oraz zbiory nieufundowane zachowują się podobnie ze względu na posiadanie nieskończonego zejścia. Spróbujmy bliżej scharakteryzować związki między tymi klasami zbiorów, w ramach teorii ZFC$^-$ z aksjomatem (Ω).

TWIERDZENIE 4. *Każdy niepusty zbiór niemający elementu minimalnego jest zbiorem nieufundowanym.* (*Inaczej: każdy niepusty zbiór ufundowany ma element minimalny.*)

DOWÓD. Niech $x \neq \emptyset$ będzie zbiorem nie mającym elementu minimalnego. Rozważmy zbiór $x \cup \{x\}$. Wówczas naturalnie $x \in x \cup \{x\}$. Wykażemy, że $x \cup \{x\}$ nie ma elementu minimalnego, co skończy dowód. Załóżmy nie wprost, że y jest elementem minimalnym zbioru $x \cup \{x\}$. Wówczas

(1) $y \in x \cup \{x\}$ oraz

(2) $y \cap (x \cup \{x\}) = \emptyset$.

Konsekwencją (2) jest oczywiście

(3) $y \cap x = \emptyset$,

gdyby bowiem dla pewnego z, $z \in y \cap x$, to $z \in y$ oraz $z \in x$, skąd $z \in x \cup \{x\}$, zatem $z \in y \cap (x \cup \{x\})$, co jest niemożliwe wobec (2).

Z (1) mamy natychmiast: $y \in x$ lub $y = x$. Gdy $y \in x$, to wobec (3), y jest elementem minimalnym zbioru x, wbrew założeniu. Gdy zaś $y = x$, to według (3), $x = \emptyset$, co również jest sprzeczne z założeniem. $\square$

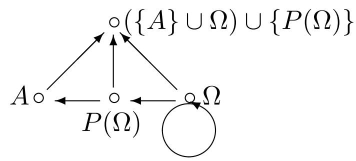
TWIERDZENIE 5. *Twierdzenie odwrotne do Tw. 4 jest fałszywe, tzn. istnieją zbiory nieufundowane posiadające element minimalny.*

DOWÓD. Wykażmy, że zbiór $A = \{\{P(\Omega)\}, P(\Omega)\}$ nie jest ufundowany, lecz posiada element minimalny. Graf zbioru A jest postaci:

$$\begin{tikzcd}
 & \circ A & \\
\{P(\Omega)\}\circ \arrow[ur] & & \circ\, P(\Omega) = \{\emptyset, \Omega\} \arrow[ul] \arrow[ll]
\end{tikzcd}$$

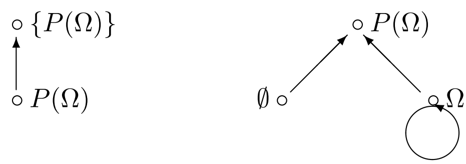
Zatem $P(\Omega)$ jest elementem minimalnym zbioru A.

Oczywiście $A \in (\{A\} \cup \Omega) \cup \{P(\Omega)\}$. Jednakże zbiór $(\{A\} \cup \Omega) \cup \{P(\Omega)\}$ nie ma elementów minimalnych:



Zatem A nie jest ufundowany. □

Nie jest również tak, że zbiór nieufundowany musi mieć element, który nie ma elementów minimalnych. Zbiór A z dowodu Tw. 5 jest nieufundowany, lecz każdy jego element posiada element minimalny. Grafy elementów zbioru A są postaci:



Okazuje się jednak, że zbiór nieufundowany musi mieć element, który nie jest zbiorem ufundowanym:

Twierdzenie 6. *Dla dowolnego zbioru x, jeżeli x nie jest ufundowany, to istnieje zbiór y taki, że $y \in x$ oraz y nie jest ufundowany.* (*Inaczej: jeżeli każdy element zbioru x jest ufundowany, to x jest ufundowany.*)

Dowód. Dowodzimy drugiego sformułowania twierdzenia. Załóżmy, że $\forall y(y \in x \Rightarrow y$ jest ufundowany). Aby wykazać, że x jest ufundowany, załóżmy, że $x \in z$. Wykażemy, że z ma element minimalny. Naturalnie x jest elementem minimalnym zbioru z lub x nie jest elementem minimalnym zbioru z. Załóżmy więc, że x nie jest elementem minimalnym zbioru z. Wówczas $x \cap z \neq \emptyset$. Niech $a \in x$ oraz $a \in z$. Ponieważ z założenia każdy element zbioru x jest ufundowany, więc a jest ufundowany. Zatem, skoro $a \in z$, to z ma element minimalny. □

Twierdzenie odwrotne do Tw. 6 jest również prawdziwe:

Twierdzenie 7. *Dowolny zbiór mający nieufundowany element jest nieufundowany.* (*Inaczej: każdy element dowolnego zbioru ufundowanego jest zbiorem ufundowanym.*)

DOWÓD. Załóżmy, że x, y są zbiorami takimi, że
(1) $y \in x$ oraz
(2) y jest nieufundowany.
Na mocy (2) niech z będzie takim zbiorem, że
(3) $y \in z$ oraz
(4) z nie ma elementu minimalnego.
Rozważmy zbiór $z \cup \{x\}$. Naturalnie $x \in z \cup \{x\}$. Pokażemy że zbiór $z \cup \{x\}$ nie ma elementu minimalnego. Załóżmy nie wprost, że a jest elementem minimalnym tego zbioru, tzn.
(5) $a \in z \cup \{x\}$ oraz
(6) $a \cap (z \cup \{x\}) = \emptyset$.
Wówczas z (5): $a \in z$ lub $a = x$. Załóżmy, że $a \in z$. Na mocy (4), a nie jest elementem minimalnym zbioru z, zatem $a \cap z \neq \emptyset$. Stąd również $a \cap (z \cup \{x\}) \neq \emptyset$; sprzeczność z (6). Załóżmy, że $a = x$. Wówczas z (1) mamy: $y \in a$. Ponadto z (3), $y \in z \cup \{x\}$. Czyli $y \in a \cap (z \cup \{x\})$. Zatem znowu $a \cap (z \cup \{x\}) \neq \emptyset$.
Ostatecznie, x nie jest ufundowany. □

Różnicę między pojęciami zbioru nieufundowanego oraz niepustego zbioru nie posiadającego elementu minimalnego można intuicyjnie wyjaśnić w oparciu o pojęcie nieskończonego zejścia. Choć zarówno zbiór nieufundowany jak i niepusty zbiór niemający elementu minimalnego mają nieskończone zejścia (Tw. 3 i Tw. 2), to jednak zbiór posiadający nieskończone zejście może mieć element minimalny, tymczasem jest on zbiorem nieufundowanym. Bowiem:

**zbiór nieufundowany to taki zbiór, który ma nieskończone zejście.*

Aby to stwierdzenie uzasadnić, weźmy pod uwagę jakikolwiek zbiór x mający nieskończone zejście: $x, y_1, \ldots, y_n, \ldots$ i rozważmy klasę wszystkich zbiorów w tym zejściu (sekwencji) występujących. Zbiór x jest elementem tej klasy, lecz klasa ta nie ma elementu minimalnego, skoro każdy zbiór z tej sekwencji ma element występujący (bezpośrednio za nim) w tej sekwencji. Zatem zbiór x jest nieufundowany.

Uzasadnienie to miałoby nieformalną wartość, gdyby wyrażenie „klasa" można było zastąpić wyrażeniem „zbiór" lub też zmodyfikować definicję zbioru nieufundowanego w sposób następujący: zbiór x jest *nieufundowany*, gdy istnieje klasa (mnogość, ekspozycja) zbiorów, w której x się znajduje oraz każdy zbiór tej klasy ma element w niej występujący.

Pierwsze z tych rozwiązań odrzucamy – nie mamy bowiem w ogólności żadnych gwarancji istnienia zbioru wszystkich zbiorów występujących w jakimś nieskończonym zejściu. Drugie rozwiązanie łatwo akceptujemy, lecz wyłącznie w ramach rozważań nieformalnych (tzn. poza teorią ZFC^-), które przecież od zakończenia dowodu Tw. 7 prowadzimy, skoro posługujemy się pojęciem nieskończonego zejścia.

Łatwo zauważyć, że przy tak zmienionym pojęciu zbioru nieufundowanego, można bez trudności zmodyfikować dowód Tw. 3, aby uzasadnić twierdzenie: **każdy zbiór nieufundowany ma nieskończone zejście.*

Naturalnie w ramach teorii mnogości ZFC^- czy ZFC funkcjonuje to pojęcie zbioru nieufundowanego (czy ufundowanego), które zostało zdefiniowane na początku §2. Nie można w ZFC^- utożsamiać (formalnie) zbioru nieufundowanego ze zbiorem mającym nieskończone zejście, bowiem w ramach tej teorii nie mamy przecież pojęcia nieskończonego zejścia.

Patrząc nieformalnie na zbiory nieufundowane jako na te i tylko te, które posiadają nieskończone zejście, jaśniejsze stają się twierdzenia, które funkcjonują bez pojęcia nieskończonego zejścia:

Tw. 4 – na mocy Tw. 2, **niepusty zbiór nie mający elementu minimalnego ma nieskończone zejście, zatem jest nieufundowany,*

Tw. 5 – **istnieją zbiory mające nieskończone zejście oraz element minimalny,*

Tw. 6 – **jeżeli zbiór* x *ma nieskończone zejście, powiedzmy* $x, y_1, y_2, \ldots, y_n, \ldots$, *to* $y_1 \in x$ *oraz* y_1 *ma nieskończone zejście* $y_1, y_2, \ldots, y_n, \ldots$,

Tw. 7 – **jeżeli* $y \in x$ *oraz* y *ma nieskończone zejście* $y, y_1, y_2, \ldots, y_n, \ldots$, *to zbiór* x *ma nieskończone zejście* $x, y, y_1, y_2, \ldots, y_n, \ldots$.

W teorii ZFC^- klasa wszystkich zbiorów niepustych niemających elementu minimalnego zawiera się w klasie wszystkich zbiorów nieufundowanych (Tw. 4). Zatem, gdyby w ZFC^- nie było zbiorów nieufundowanych, to nie byłoby tam również niepustych zbiorów nie mających elementu minimalnego. Jednakże łatwo zauważyć, że również odwrotnie, gdyby nie było tam niepustych zbiorów bez elementu minimalnego, to nie byłoby również zbiorów nieufundowanych:

TWIERDZENIE 8. *Każdy niepusty zbiór ma element minimalny wtw każdy zbiór jest ufundowany.*

DOWÓD. ($\Rightarrow$): Załóżmy, że każdy niepusty zbiór posiada element minimalny oraz nie wprost, niech a będzie zbiorem, który nie jest ufundowany. Wówczas dla pewnego zbioru y nie mającego elementu minimalnego, $a \in y$. Lecz wtedy $y \neq \emptyset$, zatem z założenia musi mieć element minimalny. Sprzeczność.

($\Leftarrow$): Na mocy Tw. 4. $\square$

§3. Dwie istotne własności zbiorów ufundowanych

Odnotujmy dwie istotne własności zbiorów ufundowanych:

TWIERDZENIE 9. $\forall x(x$ *jest ufundowany* $\Rightarrow x \notin x)$.

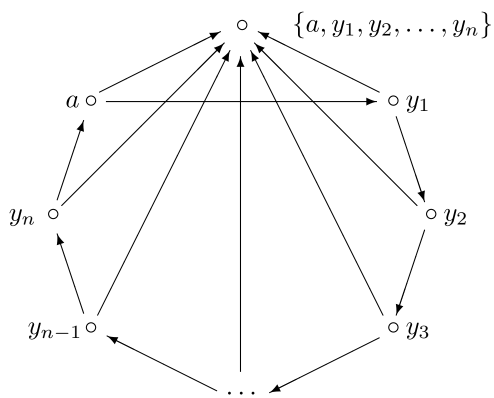
DOWÓD. Załóżmy nie wprost, że a jest ufundowany oraz $a \in a$. Ponieważ $a \in \{a\}$, więc zbiór $\{a\}$ ma element minimalny (z definicji zbioru ufundowanego). Niech b będzie elementem minimalnym zbioru $\{a\}$. Wówczas $b \in \{a\}$ oraz $b \cap \{a\} = \emptyset$. Zatem $b = a$ i konsekwentnie $a \cap \{a\} = \emptyset$. Tymczasem z założenia, $a \in a$. Ponieważ $a \in \{a\}$, więc $a \in a \cap \{a\}$, czyli $a \cap \{a\} \neq \emptyset$. Sprzeczność. □

TWIERDZENIE 10. *Dla dowolnego zbioru x, jeżeli x jest ufundowany, to nie istnieje liczba naturalna n oraz zbiory $y_1, y_2, \ldots, y_n$ takie*, że $x \in y_1 \wedge y_1 \in y_2 \wedge \ldots \wedge y_{n-1} \in y_n \wedge y_n \in x$.

DOWÓD. Załóżmy nie wprost, że a jest zbiorem ufundowanym oraz dla pewnych $y_1, y_2, \ldots, y_n$ mamy:

(1) $a \in y_1 \in y_2 \in \ldots \in y_{n-1} \in y_n \in a$.

Ponieważ a jest ufundowany oraz $a \in \{a, y_1, y_2, \ldots, y_n\}$, więc zbiór $\{a, y_1, y_2, \ldots, y_n\}$ ma element minimalny. Tymczasem na mocy (1), jak wskazuje ilustracja grafu tego zbioru, zbiór ten nie ma elementu minimalnego:



□

§4. Aksjomat regularności i jego konsekwencje

Możemy obecnie sformułować aksjomat regularności (AxR) następująco:

$(AxR)'$ $\forall x(x \neq \emptyset \Rightarrow \exists y(y$ jest elementem minimalnym $x))$,

lub równoważnie na mocy Tw. 8:

$(AxR)''$ $\forall x(x$ jest ufundowany$)$.

W teorii ZFC (z aksjomatem regularności) nie istnieją zbiory takie jak Ω (negacja formuły (Ω) jest twierdzeniem ZFC), czyli zbiory nieufundowane. Według nieformalnych rozważań w §2, takie zbiory nie mają „pełnego fundamentu" co się przejawia w posiadaniu nieskończonego zejścia. Jednakże pojęcie nieskończonego zejścia nie mieści się w ramach, często nieświadomie akceptowanego, atomizmu metodologicznego B. Russella, według którego jakiekolwiek konstrukty formalne winny być na początku budowane z fundamentalnych cegiełek (atomów). Zbiór, jako konstrukt formalny, winien być „rozkładalny" w skończonej ilości kroków na ostateczne elementarne części. Tymczasem zbiór posiadający nieskończone zejście, „rozkładalny" jest w nieskończoność.

W ZFC, na podstawie aksjomatu regularności, otrzymujemy jako wnioski z Tw. 9 oraz Tw. 10 odpowiednio następujące zdania:

Wniosek z Tw. 9. $\forall x(x \notin x)$.

Wniosek z Tw. 10. *Dla dowolnego zbioru x nie istnieje liczba naturalna n oraz zbiory $y_1, y_2, \ldots, y_n$ takie,* że $x \in y_1 \wedge y_1 \in y_2 \wedge \ldots \wedge y_{n-1} \in y_n \wedge y_n \in x$.

Konsekwencją Wniosku z Tw. 9 jest

Twierdzenie 11. $\neg\exists y \forall x(x \in y)$ (*nie istnieje zbiór wszystkich zbiorów*).

Dowód. Załóżmy nie wprost, że $\exists y \forall x(x \in y)$. Wówczas dla pewnego zbioru V mamy: $\forall x(x \in V)$. Zatem $V \in V$, co jest niemożliwe na mocy Wniosku z Tw. 9. □

Naturalnie Tw. 11 jest bezpośrednią konsekwencją nieistnienia zbioru tych i tylko tych zbiorów, które nie są swoimi elementami (por. Wstęp) oraz następującego aksjomatu Zermelo:

$\forall x \ (x \notin x \ \Rightarrow \ x \in V) \ \Rightarrow \ \exists y \forall x \ (x \in y \ \Leftrightarrow \ x \notin x)$, gdzie V jest zbiorem wszystkich zbiorów: $\forall x(x \in V)$. Istnienie zbioru wszystkich zbiorów implikuje istnienie zbioru $R = \{x : x \notin x\}$. Zauważmy, że z drugiej strony, w obecności aksjomatu regularności, a więc wówczas, gdy zachodzi Wniosek z Tw. 9, prawdziwe jest twierdzenie: gdyby istniał zbiór R, to byłby on zbiorem wszystkich zbiorów. Gdy bowiem zachodzi: $\forall x(x \notin x)$, to wówczas, $\forall x(x \in R)$.

Rozdział 3. Relacje binarne

§1. Para uporządkowana. Produkt kartezjański dwóch zbiorów

Dla pary zbiorów $\{x, y\}$ zachodzi, jak łatwo sprawdzić, równość $\{x, y\} = \{y, x\}$. To znaczy, kolejność wymienienia elementów pary zbiorów jest dla jej określenia nieistotna. Wprowadzimy pojęcie *uporządkowanej pary zbiorów*: $<x, y>$ takiej, że $<x, y> \neq <y, x>$ o ile $x \neq y$.

DEFINICJA. Dla dowolnych zbiorów x, y, $<x, y> = \{\{x\}, \{x, y\}\}$.

TWIERDZENIE 1. $<x, y> = <u, v> \Rightarrow (x = u \wedge y = v)$.

DOWÓD. Załóżmy, że $<x, y> = <u, v>$. Wówczas z definicji pary uporządkowanej mamy:
(1) $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$.

Oczywiście $x = y$ lub $x \neq y$. Gdy $x = y$, to $\{\{x\}, \{x, y\}\} = \{\{x\}\}$. Zatem z (1) mamy: $\{\{x\}\} = \{\{u\}, \{u, v\}\}$, co oznacza, że
(2) $\{x\} = \{u\}$ oraz
(3) $\{x\} = \{u, v\}$.

Z (2) otrzymujemy: $x = u$, zaś z (3): $x = u = v$, zatem skoro $y = x$, więc $y = v$.

Załóżmy, że $x \neq y$. Wówczas
(4) $\{x\} \neq \{x, y\}$.

Wtedy na podstawie (1):
$(\{x\} = \{u\}$ lub $\{x\} = \{u, v\})$ oraz $(\{x, y\} = \{u\}$ lub $\{x, y\} = \{u, v\})$.

Gdy $\{x\} = \{u\}$, to $\{x, y\} \neq \{u\}$ na mocy (4), zatem $\{x, y\} = \{u, v\}$. Gdy zaś $\{x\} = \{u, v\}$, to $\{x, y\} \neq \{u, v\}$, czyli $\{x, y\} = \{u\}$. Mamy zatem następujące dwa przypadki:
(5) $\{x\} = \{u\}$ i $\{x, y\} = \{u, v\}$,
(6) $\{x\} = \{u, v\}$ i $\{x, y\} = \{u\}$.

Jednakże przypadek (6) nie może zachodzić, bowiem gdyby zachodził, toby $x = u$ oraz $y = u$, czyli byłoby $x = y$. Zatem zachodzi przypadek (5), co oznacza, że $x = u$, a ponadto skoro $y \neq x$, czyli $y \neq u$, więc $y = v$. $\square$

WNIOSEK. $<x, y> = <y, x> \Rightarrow x = y$.

DOWÓD. Oczywisty na podstawie Tw. 1. $\square$

Wykorzystamy aksjomat podzbiorów, aby dowieść istnienia zbioru wszystkich par uporządkowanych, z których pierwszy element należy do jednego danego zbioru, zaś drugi element pary do drugiego danego zbioru. W tym celu wykazujemy fakt pomocniczy:

LEMAT. $(u \in a \wedge v \in b) \Rightarrow <u, v> \subseteq P(a \cup b)$.

DOWÓD. Załóżmy, że $u \in a$ oraz $v \in b$. Wówczas $\{u\} \subseteq a \subseteq a \cup b$. Ponadto, $\{u, v\} \subseteq a \cup b$. Zatem $\{u\}, \{u, v\} \in P(a \cup b)$, czyli $\{\{u\}, \{u, v\}\} \subseteq P(a \cup b)$, a więc z definicji pary uporządkowanej: $<u, v> \subseteq P(a \cup b)$. $\square$

Rozważmy w aksjomacie podzbiorów $(AxZ)_\phi$ formułę $\phi(x)$ postaci $\exists u \exists v(u \in a \wedge v \in b \wedge x = <u, v>)$ oraz zbiór z postaci $P(P(a \cup b))$, otrzymując wyrażenie

$\forall a \forall b[\forall x(\exists u \exists v(u \in a \wedge v \in b \wedge x = <u, v>) \Rightarrow x \in P(P(a \cup b))) \Rightarrow \exists y \forall x(x \in y \Leftrightarrow \exists u \exists v(u \in a \wedge v \in b \wedge x = <u, v>))]$,

które, wobec prawdziwości poprzednika głównej implikacji (na mocy lematu) prowadzi do definicji *produktu kartezjańskiego* $a \times b$ dla dowolnych zbiorów a, b:

DEFINICJA. Dla dowolnych zbiorów a, b,
$\forall x(x \in a \times b \Leftrightarrow \exists u \exists v(u \in a \wedge v \in b \wedge x = <u, v>))$ lub
$a \times b = \{x : \exists u \exists v(u \in a \wedge v \in b \wedge x = <u, v>)\} = \{<u, v>: u \in a \wedge v \in b\}$.

Produkt kartezjański $a \times b$ zbiorów a, b jest zbiorem wszystkich par uporządkowanych, których pierwszy element należy do zbioru a, zaś drugi do zbioru b.

Produkt $a \times a$ bywa oznaczany jako a^2.

Uwaga. Ostatnia z równości w definicji produktu została uzyskana na podstawie konwencji notacyjnej, w myśl której sekwencja symboli $\{F(x_1, \ldots, x_n) : \psi(x_1, \ldots, x_n)\}$, gdzie F jest symbolem n-argumentowej operacji, zaś $x_1, \ldots, x_n$ zmiennymi wolnymi w formule $\psi(x_1, \ldots, x_n)$, oznacza zbiór wszystkich wartości $F(x_1, \ldots, x_n)$ operacji F na tej sekwencji zbiorów $x_1, \ldots, x_n$, dla której prawdziwe jest $\psi(x_1, \ldots, x_n)$.

Używać również będziemy konwencji notacyjnej polegającej na pisaniu $\{x \in A : \psi(x)\}$ na oznaczenie zbioru $\{x : x \in A \wedge \psi(x)\}$.

Ponadto używać będziemy notorycznie kwantyfikatorów o ograniczonym zakresie: $\forall \alpha(x)(\beta) =_{def} \forall x(\alpha(x) \Rightarrow \beta)$ oraz $\exists \alpha(x)(\beta) =_{def} \exists x(\alpha(x) \wedge \beta)$, gdzie $\alpha(x)$ jest formułą, w której x jest zmienną wolną oraz β jest formułą. Na przykład będziemy pisać $\forall x \in A(x \in B)$ lub po prostu $\forall x \in A,\ x \in B$ zamiast pisać $\forall x(x \in A \Rightarrow x \in B)$. Podobnie będziemy pisać $\exists x \in A(x \in B)$ lub $\exists x \in A,\ x \in B$ zamiast $\exists x(x \in A \wedge x \in B)$.

Wreszcie zamiast pisać $\forall x \forall y$ bądź $\forall x \in A \forall y \in A$ będziemy pisać $\forall x, y$ bądź $\forall x, y \in A$. Analogicznie dla zbitki kwantyfikatorów egzystencjalnych.

§2. Pojęcie relacji binarnej

DEFINICJA. Dla dowolnych zbiorów A, B, dowolny podzbiór $R \subseteq A \times B$ nazywamy *relacją binarną na zbiorach* A, B. Mówimy, że R jest *relacją binarną określoną na zbiorze* A, gdy $R \subseteq A \times A$. Zbiór $\emptyset \subseteq A \times A$ nazywamy relacją *pustą na zbiorze* A, zaś sam produkt $A \times A$ – relacją *pełną na zbiorze* A.

Niech $R \subseteq A \times B$. Zbiór $D(R) = \{x \in A : \exists y \in B(<x, y> \in R)\}$ nazywamy *dziedziną relacji* R, natomiast zbiór $D^{-1}(R) = \{y \in B : \exists x \in A(<x, y> \in R)\}$ nazywamy *przeciwdziedziną relacji* R.

Uwaga. Istnienie dziedziny i przeciwdziedziny danej relacji binarnej jest naturalnie gwarantowane przez aksjomat podzbiorów.

DEFINICJA. Niech $R \subseteq A \times A$. Mówimy, że relacja R jest
zwrotna na $A \Leftrightarrow \forall x \in A, <x, x> \in R$,
przeciwzwrotna na $A \Leftrightarrow \forall x \in A, <x, x> \notin R$,
symetryczna na $A \Leftrightarrow \forall x, y \in A(<x, y> \in R \Rightarrow <y, x> \in R)$,
przeciwsymetryczna na $A \Leftrightarrow \forall x, y \in A(<x, y> \in R \Rightarrow <y, x> \notin R)$,
antysymetryczna na $A \Leftrightarrow \forall x, y \in A((<x, y> \in R \wedge\ <y, x> \in R) \Rightarrow\ x = y)$,
przechodnia na $A \Leftrightarrow \forall x, y, z \in A((<x, y> \in R \wedge\ <y, z> \in R) \Rightarrow <x, z> \in R)$,
spójna na $A \Leftrightarrow \forall x, y \in A(<x, y> \in R \vee <y, x> \in R \vee x = y)$.

Większość z powyższych formalnych własności relacji binarnych daje się zilustrować na diagramie relacji. Napiszmy w postaci *macierzy* wszystkie pary uporządkowane należące do produktu $A \times A$, n-elementowego zbioru $A = \{a_1, a_2, \ldots, a_n\}$:

$$
\begin{array}{l}
< a_1, a_1 >, < a_1, a_2 >, \ldots, < a_1, a_n > \\
< a_2, a_1 >, < a_2, a_2 >, \ldots, < a_2, a_n > \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
< a_n, a_1 >, < a_n, a_2 >, \ldots, < a_n, a_n >.
\end{array}
$$

Każdą niepustą relację binarną określoną na zbiorze A można teraz uwidocznić przez podkreślenie par do niej należących. Nazwijmy ekspozycję podkreślonych par uporządkowanych – diagramem relacji R.

Jasne jest, że relacja R jest zwrotna, gdy przekątna macierzy o końcach $<a_1, a_1>$, $<a_n, a_n>$ zawiera się w diagramie R, natomiast R jest przeciwzwrotna, gdy owa przekątna nie ma wspólnych par z diagramem relacji R.

Ponadto, R jest symetryczna, gdy, ilekroć jakaś para z macierzy jest w jej diagramie, tylekroć „zwierciadlane odbicie” tej pary względem przekątnej (tzn. wartość symetrii osiowej względem przekątnej na tej parze) również należy do diagramu R.

R jest przeciwsymetryczna, gdy, ilekroć jakaś para z macierzy jest w diagramie R, tylekroć „zwierciadlane odbicie” tej pary względem przekątnej nie jest w tym diagramie. W szczególności więc, żadna para z przekątnej nie jest w diagramie takiej relacji (tzn. relacja przeciwsymetryczna jest przeciwzwrotna) skoro zwierciadlanym odbiciem pary z przekątnej jest ona sama.

Relacja R jest antysymetryczna, gdy dla par spoza przekątnej zachowuje się ona jak relacja przeciwsymetryczna, tzn. ilekroć jakaś para spoza przekątnej jest w jej diagramie, tylekroć „zwierciadlane odbicie” tej pary nie znajduje się w diagramie; jednakże, w przeciwieństwie do relacji przeciwsymetrycznej, jakiekolwiek pary z przekątnej mogą należeć dla relacji antysymetrycznej.

Relacja R jest spójna, gdy dla dowolnej pary uporządkowanej poza przekątną, para ta lub jej „zwierciadlane odbicie” względem przekątnej występują w diagramie relacji R.

Widać, że niektóre z wymienionych wyżej własności relacji nie są niezależne od siebie. Przykładowo, związki między przeciwzwrotnością a przeciwsymetrią są postaci:

TWIERDZENIE 2. *Niech R będzie relacją binarną określoną na zbiorze A.*
(1) *Jeżeli R jest przeciwsymetryczna, to R jest przeciwzwrotna.*
(2) *Jeżeli R jest przeciwzwrotna i przechodnia, to R jest przeciwsymetryczna.*

DOWÓD. Dla (1): Załóżmy, że $\forall x, y \in A(<x,y> \in R \Rightarrow <y,x> \notin R)$ oraz nie wprost, że R nie jest przeciwzwrotna, tzn. dla pewnego $x \in A$, $<x,x> \in R$. Wówczas z warunku przeciwsymetrii mamy: $<x,x> \in R \Rightarrow <x,x> \notin R$. Stąd $<x,x> \notin R$. Sprzeczność.

Dla (2): Załóżmy, że $\forall x \in A, <x,x> \notin R$ oraz $\forall x,y,z \in A((<x,y> \in R \wedge <y,z> \in R) \Rightarrow <x,z> \in R)$ i nie wprost, że R nie jest przeciwsymetryczna, tzn. dla pewnych $x, y \in A$, $<x,y> \in R$ oraz $<y,x> \in R$. Z przechodniości mamy: $(<x,y> \in R \wedge <y,x> \in R) \Rightarrow <x,x> \in R$. Stąd $<x,x> \in R$. Jednakże z przeciwzwrotności, $<x,x> \notin R$. Sprzeczność. □

§3. Operacje na relacjach binarnych

DEFINICJA. Niech $R \subseteq A \times B$. Przez *konwers relacji R* (lub *relację odwrotną do R*) rozumiemy relację $R^{\sim} \subseteq B \times A$ określoną następująco: $R^{\sim} = \{<x,y> \in B \times A : <y,x> \in R\}$, tzn. $\forall x \in B \forall y \in A$, $<x,y> \in R^{\sim}$ wtw $<y,x> \in R$.

Niech ponadto $S \subseteq B \times C$. Przez *złożenie* (lub *superpozycję*) relacji R, S rozumiemy relację $R \circ S \subseteq A \times C$ określoną następująco:
$R \circ S = \{<x,y> \in A \times C : \exists z \in B(<x,z> \in R \wedge <z,y> \in S)\}$, tzn. $\forall x \in A \forall y \in C$, $<x,y> \in R \circ S$ wtw $\exists z \in B(<x,z> \in R \wedge <z,y> \in S)$.

Zbiór $\mathrm{id}_A = \{<x,x>: x \in A\} = \{<x,y> \in A^2 : x = y\}$ nazywamy relacją *identycznościową* lub *tożsamościową na zbiorze A*. Inaczej: $\forall x, y \in A, <x,y> \in \mathrm{id}_A$ wtw $x = y$.

Uwaga. Nietrudno zastosować aksjomat podzbiorów dla dowodów istnienia konwersu oraz złożenia relacji jak również relacji identycznościowej.

TWIERDZENIE 3. *Niech* $R \subseteq A \times B,\ S \subseteq B \times C,\ T \subseteq C \times D$. *Wówczas*:
(1) $R \circ (S \circ T) = (R \circ S) \circ T$,
(2) $R \circ \mathrm{id}_B = \mathrm{id}_A \circ R = R$,
(3) $(R \circ S)^{\sim} = S^{\sim} \circ R^{\sim}$.

DOWÓD. Dla (1): Naturalnie $S \circ T \subseteq B \times D$, zaś $R \circ S \subseteq A \times C$. Zatem $R \circ (S \circ T) \subseteq A \times D$ oraz $(R \circ S) \circ T \subseteq A \times D$.

($\subseteq$): Niech dla $a \in A$ i $d \in D$, $<a,d> \in R \circ (S \circ T)$. Wówczas dla pewnego $b \in B$:
(4) $<a,b> \in R$ oraz
(5) $<b,d> \in S \circ T$.

Z (5) dla pewnego $c \in C$:
(6) $<b,c> \in S$ oraz
(7) $<c,d> \in T$.

Zatem z (4) i (6): $<a,c> \in R \circ S$, stąd i z (7): $<a,d> \in (R \circ S) \circ T$.

Dla inkluzji ($\supseteq$) dowód jest analogiczny.

Dla (2): Wykazujemy, że $R \circ \mathrm{id}_B = R$. Niech $a \in A$ oraz $b \in B$.

($\subseteq$): Załóżmy, że $<a,b> \in R \circ \mathrm{id}_B$. Wówczas dla pewnego $x \in B$, $<a,x> \in R$ oraz $<x,b> \in \mathrm{id}_B$. Stąd $x = b$, czyli $<a,b> \in R$.

($\supseteq$): Niech $<a,b> \in R$. Ponieważ $<b,b> \in \mathrm{id}_B$, więc z definicji złożenia relacji mamy: $<a,b> \in R \circ \mathrm{id}_B$.

Analogicznie wykazujemy, że $\mathrm{id}_A \circ R = R$.

Dla (3): Naturalnie $(R \circ S)^{\sim} \subseteq C \times A$ (bo $R \circ S \subseteq A \times C$) oraz $S^{\sim} \circ R^{\sim} \subseteq C \times A$ (bo $S^{\sim} \subseteq C \times B$ oraz $R^{\sim} \subseteq B \times A$).

($\subseteq$): Niech $c \in C$ oraz $a \in A$. Załóżmy, że $<c,a> \in (R \circ S)^{\sim}$. Wówczas $<a,c> \in R \circ S$, zatem dla pewnego $b \in B$, $<a,b> \in R$ i $<b,c> \in S$. Czyli $<c,b> \in S^{\sim}$ oraz $<b,a> \in R^{\sim}$. Ostatecznie, $<c,a> \in S^{\sim} \circ R^{\sim}$.

($\supseteq$): Rozumowanie odwrotne do powyższego. □

TWIERDZENIE 4. *Niech* $R_1, R_2 \subseteq A \times B$ oraz $S \subseteq B \times C$. Wówczas
(1) $R_1 \subseteq R_2 \Rightarrow R_1 \circ S \subseteq R_2 \circ S$,
(2) $(R_1 \cap R_2)^{\sim} = R_1^{\sim} \cap R_2^{\sim}$,
(3) $(R_1 \cup R_2)^{\sim} = R_1^{\sim} \cup R_2^{\sim}$.

Dowód. Dla (1): Załóżmy, że $R_1 \subseteq R_2$. Niech dla $a \in A$ oraz $c \in C$, $<a, c> \in R_1 \circ S$. Wówczas dla pewnego $b \in B$, $<a, b> \in R_1$ oraz $<b, c> \in S$. Z założenia zatem otrzymujemy: $<a, b> \in R_2$ i ostatecznie, $<a, c> \in R_2 \circ S$.

Dla (2): Mamy: $<b, a> \in (R_1 \cap R_2)^\sim$ wtw $<a, b> \in R_1 \cap R_2$ wtw $<a, b> \in R_1$ oraz $<a, b> \in R_2$ wtw $<b, a> \in R_1^\sim$ oraz $<b, a> \in R_2^\sim$ wtw $<b, a> \in R_1^\sim \cap R_2^\sim$, co na mocy aksjomatu identyczności implikuje równość $(R_1 \cap R_2)^\sim = R_1^\sim \cap R_2^\sim$.

Dla (3): Analogicznie jak dla (2). □

Nietrudno zauważyć, że wartości operacji złożenia i konwersu na relacjach binarnych określonych na danym zbiorze A są relacjami na tym zbiorze. Innymi słowy, zbiór wszystkich relacji określonych na zbiorze A, czyli zbiór $P(A \times A)$ jest zamknięty na te dwie operacje. Jako ciało zbiorów, jest on również zamknięty na operacje: $\cap, \cup, -$. Zbiór potęgowy $P(A \times A)$ wyposażony w operacje: $\cap, \cup, -, \circ, ^\sim$ z wyróżnionymi elementami: $\emptyset, A \times A$, id_A nazywamy *algebrą relacji* lub *algebrą relacyjną*.

Operacje na relacjach mogą posłużyć do wyrażenia własności formalnych relacji określonych na danym zbiorze. Przykładowo:

Twierdzenie 5. *Dla dowolnej relacji* $R \subseteq A^2$:
(1) *R jest zwrotna na A wtw* $\mathrm{id}_A \subseteq R$,
(2) *R jest symetryczna na A wtw* $R^\sim = R$
(3) *R jest przechodnia na A wtw* $R \circ R \subseteq R$.

Dowód. Dla (1): Mamy oczywiste równoważności:
R jest zwrotna wtw $\forall x \in A$, $<x, x> \in R$ wtw $\mathrm{id}_A \subseteq R$.

Dla (2): ($\Rightarrow$): Załóżmy, że $\forall x, y \in A(<x, y> \in R \Rightarrow <y, x> \in R)$. Aby wykazać równość $R = R^\sim$, dowodzimy inkluzji ($\subseteq$): niech $<x, y> \in R$. Wówczas na mocy symetrii: $<y, x> \in R$, zatem z definicji konwersu, $<x, y> \in R^\sim$. ($\supseteq$): Niech $<x, y> \in R^\sim$. Wówczas $<y, x> \in R$, zatem z warunku symetrii, $<x, y> \in R$.

($\Leftarrow$): Załóżmy, że $R = R^\sim$. Aby dowieść warunek symetrii weźmy $x, y \in A$ i załóżmy, że $<x, y> \in R$. Wówczas z założenia, $<x, y> \in R^\sim$ skąd $<y, x> \in R$, zatem R jest symetryczna na A.

Dla (3): ($\Rightarrow$): Załóżmy, że $\forall x, y, z \in A((<x, y> \in R \wedge <y, z> \in R) \Rightarrow <x, z> \in R)$. Aby pokazać inkluzję $R \circ R \subseteq R$ załóżmy, że dla jakichś $x, y \in A$, $<x, y> \in R \circ R$. Wówczas z definicji złożenia, $<x, a> \in R$ oraz $<a, y> \in R$ dla pewnego $a \in A$. Zatem z przechodniości otrzymujemy: $(<x, a> \in R \wedge <a, y> \in R) \Rightarrow <x, y> \in R$, skąd mamy natychmiast: $<x, y> \in R$, co kończy dowód inkluzji $R \circ R \subseteq R$.

($\Leftarrow$): Załóżmy, że $R \circ R \subseteq R$. Aby wykazać warunek przechodniości rozważmy $x, y, z \in A$ i załóżmy, że $<x, y> \in R$ oraz $<y, z> \in R$. Wówczas $<x, z> \in R \circ R$, zatem z założenia zachodzi $<x, z> \in R$, co dowodzi przechodniości relacji R na zbiorze A. □

Uwaga. Dla pozostałych formalnych własności relacji binarnych określonych na zbiorze A, tzn. dla przeciwzwrotności, antysymetrii, przeciwsymetrii oraz spójności, można równie łatwo podać ich odpowiedniki w terminach operacji na relacjach.

§4. Relacje porządkujące

Relacje binarne określone na danym zbiorze, w zależności od własności formalnych, które im przysługują, dzieli się na rodzaje. Na przykład wyróżnia się relacje, które są zwrotne, symetryczne i przechodnie, nazywając je relacjami *równoważnościowymi.* Relacje zwrotne i przechodnie zwane są często relacjami *quasi-porządkującymi.* Jeżeli ponadto są one antysymetryczne, to nazywamy je relacjami *częściowo porządkującymi.* Relacje częściowo porządkujące, które są spójne, nazywane są relacjami *liniowo porządkującymi.*

Nazwa: „relacja porządkująca" odnosi się do takiej relacji, która ustala pewien porządek wśród elementów zbioru, na którym jest określona. Naturalnym przykładem relacji porządkującej jest relacja mniejszości $<$, określona na zbiorze liczb naturalnych, ustalająca porządek liczb naturalnych postaci: $0 < 1 < 2 < \ldots$. Jednakże relacji $<$ nie możemy zaliczyć do żadnej z wymienionych wyżej grup relacji porządkujących, nie jest to bowiem relacja zwrotna. Łatwo sprawdzić, że jest to relacja przeciwzwrotna, przechodnia i spójna. Istnieje ścisły związek między relacjami przeciwzwrotnymi i przechodnimi a relacjami częściowo porządkującymi. W naszym przykładzie przeciwzwrotna i przechodnia relacja $<$ wyznacza jednoznacznie częściowo porządkującą relację $\leq$ (mniejsze lub równe) na zbiorze liczb naturalnych. Relacja $\leq$ jest oczywiście postaci: $< \cup \, \mathrm{id}_N$, gdzie N jest zbiorem liczb naturalnych. Na odwrót, odjęcie z relacji częściowo porządkującej $\leq$ relacji identycznościowej id_N daje w efekcie wyjściową relację $<$.

W ogólności, dowolna relacja R przeciwzwrotna i przechodnia na zbiorze A, jednoznacznie wyznacza relację częściowo porządkującą postaci: $R \cup \mathrm{id}_A$, zaś dowolna relacja częściowo porządkująca R wyznacza jednoznacznie relację przeciwzwrotną i przechodnią postaci: $R - \mathrm{id}_A$:

TWIERDZENIE 6. *Niech R będzie relacją binarną określoną na zbiorze A.*
(1) *Jeżeli R jest przeciwzwrotna i przechodnia na A, to relacja $R \cup \mathrm{id}_A$ jest zwrotna, antysymetryczna i przechodnia na A.*
(2) *Jeżeli R jest zwrotna, antysymetryczna i przechodnia na zbiorze A, to relacja $R - \mathrm{id}_A$ jest przeciwzwrotna i przechodnia na tym zbiorze.*

DOWÓD. Dla (1): Załóżmy, że R jest przeciwzwrotna i przechodnia na A. Ponieważ $\mathrm{id}_A \subseteq R \cup \mathrm{id}_A$, więc na mocy Tw. 5(1) relacja $R \cup \mathrm{id}_A$ jest zwrotna na A. Aby wykazać, że jest ona antysymetryczna, załóżmy, że $<x,y> \in R \cup \mathrm{id}_A$ i $<y,x> \in R \cup \mathrm{id}_A$, oraz nie wprost, że $x \neq y$. Wówczas $<x,y> \in R$ oraz $<y,x> \in R$, zatem z przechodniości relacji R otrzymujemy: $<x,x> \in R$, co przeczy przeciwzwrotności R. W celu wykazania przechodniości relacji $R \cup \mathrm{id}_A$ załóżmy, że
(3) $<x,y> \in R \cup \mathrm{id}_A$ oraz
(4) $<y,z> \in R \cup \mathrm{id}_A$.

Z (3): $<x,y> \in R$ lub $x = y$, zaś z (4): $<y,z> \in R$ lub $y = z$.

Załóżmy, że $< x,y > \in R$ oraz $< y,z > \in R$. Wówczas z przechodniości R mamy: $<x,z> \in R$, lecz $R \subseteq R \cup \mathrm{id}_A$, zatem $<x,z> \in R \cup \mathrm{id}_A$. Załóżmy, że $<x,y> \in R$ oraz $y = z$. Wówczas natychmiast $<x,z> \in R$, co, jak poprzednio, implikuje $<x,z> \in R \cup \mathrm{id}_A$. Załóżmy, że $x = y$ oraz $<y,z> \in R$. Wówczas znowu $<x,z> \in R$. Ostatni przypadek jaki może zachodzić, gdy alternatywy uzyskane z (3), (4) są prawdziwe, jest następujący: $x = y$ oraz $y = z$. Wówczas $x = z$, czyli $<x,z> \in \mathrm{id}_A$, stąd $<x,z> \in R \cup \mathrm{id}_A$.

Dla (2): Załóżmy, że R jest zwrotna, antysymetryczna i przechodnia na A. Jest oczywiste, że relacja $R - \mathrm{id}_A$ jest przeciwzwrotna (zakładany warunek zwrotności relacji R nie jest tu wykorzystywany). W celu wykazania, że $R - \mathrm{id}_A$ jest przechodnia załóżmy, że $<x,y> \in R - \mathrm{id}_A$ oraz $<y,z> \in R - \mathrm{id}_A$. Wówczas mamy:
(5) $<x,y> \in R$,
(6) $x \neq y$,
(7) $<y,z> \in R$.

Z (5), (7) oraz przechodniości relacji R otrzymujemy: $<x,z> \in R$. Ponadto $x \neq z$, gdyby bowiem $x = z$, to z (7) mielibyśmy: $<y,x> \in R$, co wraz z (5) na mocy antysymetrii relacji R dałoby: $x = y$, co jest niemożliwe z racji (6). Ostatecznie $<x,z> \in R - \mathrm{id}_A$. □

Jest oczywiste, że przyporządkowanie postaci: $R \longrightarrow R \cup \mathrm{id}_A$, ustala jedno-jednoznaczną odpowiedniość między relacjami, które są przeciwzwrotne i przechodnie a relacjami częściowo porządkującymi: mianowicie dwóm różnym relacjom przeciwzwrotnym i przechodnim odpowiadają dwie różne relacje częściowo porządkujące.

Ponadto, dowolna relacja częściowo porządkująca R jest, według owego przyporządkowania, przyporządkowana pewnej relacji przeciwzwrotnej i przechodniej, mianowicie relacji $R - \mathrm{id}_A$.

Wobec tej jednoznacznej odpowiedniości, czasem właśnie relacje przeciwzwrotne i przechodnie (są one wówczas również przeciwsymetryczne na mocy Tw. 2(2)) nazywane są relacjami częściowo porządkującymi.

§5. Tranzytywne domknięcie relacji binarnej

Jak widać, we wszystkich wzmiankowanych w §4 rodzajach relacji binarnych określonych na danym zbiorze, bierze się pod uwagę warunek przechodniości. Obecnie poświęcimy mu nieco więcej uwagi.

Łatwo sprawdzić, że dowolny singleton $\{<a,b>\}$ dla $a,b \in A$, jest relacją przechodnią na zbiorze A. Suma dwóch singletonów postaci: $\{<a,b>\} \cup \{<b,a>\}$, gdzie $a \neq b$, relacją przechodnią nie jest. Zatem suma dwóch relacji przechodnich nie musi być relacją przechodnią. W ogólności nie jest tak, że dla dowolnego zbioru $\mathcal{R}$ relacji przechodnich na danym zbiorze A, $\bigcup \mathcal{R}$ jest relacją przechodnią (w przeciwieństwie na przykład do zbioru relacji zwrotnych czy symetrycznych, którego suma zachowuje te własności).

Tymczasem przekrój dowolnego zbioru $\mathcal{R}$ relacji przechodnich na zbiorze A jest relacją przechodnią na tym zbiorze. Jeśli bowiem dla jakichś $x,y,z \in A$, $<x,y>, <y,z> \in \bigcap \mathcal{R}$, to w ten sposób dla każdej relacji $R \in \mathcal{R}$, $<x,y>, <y,z> \in R$, zatem wobec przechodniości każdej relacji $R \in \mathcal{R}$, $<x,z> \in R$ dla wszystkich $R \in \mathcal{R}$, tzn. $<x,z> \in \bigcap \mathcal{R}$.

Rozważmy dowolną relację R określoną na zbiorze A. Weźmy pod uwagę wszystkie relacje przechodnie S na zbiorze A takie, że $R \subseteq S$. Oczywiście takie relacje istnieją, bo sam produkt $A \times A$ jest relacją przechodnią na A. Na mocy aksjomatu podzbiorów, łatwo uzasadnić istnienie zbioru $\mathcal{S}$ wszystkich takich relacji S. Skoro zbiór ten jest niepusty, możemy rozważyć jego przekrój $\bigcap \mathcal{S}$. Jasne jest, że $\bigcap \mathcal{S}$ jest relacją przechodnią. Ponadto z własności przekroju mamy: $R \subseteq \bigcap \mathcal{S}$ (Tw. 18(2), Rozdział 1) oraz $\bigcap \mathcal{S} \subseteq S$ dla każdej $S \in \mathcal{S}$ (Tw. 18(1), Rozdział 1). Ostatecznie, przekrój zbioru wszystkich relacji przechodnich na zbiorze A zawierających daną relację R jest najmniejszą (w sensie zawierania) relacją przechodnią zawierającą R, tzn. ów przekrój, sam będąc relacją przechodnią zawierającą relację R, zawiera się w każdej relacji przechodniej zawierającej R.

Najmniejszą relację przechodnią zawierającą daną relację R określoną na zbiorze A można opisać jeszcze w inny sposób.

Definicja. Niech R będzie dowolną relacją określoną na zbiorze A. Relację R^- określoną na zbiorze A następująco: $\forall x,y \in A$, $<x,y> \in R^-$ wtw dla pewnej liczby naturalnej $n \geq 2$ istnieją $z_1, \ldots, z_n \in A$ takie, że $x = z_1, <z_1,z_2> \in R, <z_2,z_3> \in R, \ldots, <z_{n-1},z_n> \in R, z_n = y$, nazywamy *tranzytywnym* (lub *przechodnim*) *domknięciem relacji R*. (Istnienie tranzytywnego domknięcia gwarantowane jest przez aksjomat podzbiorów.)

TWIERDZENIE 7. *Dla dowolnej relacji binarnej R określonej na zbiorze A,*
(1) *R^- jest relacją przechodnią na A,*
(2) *$R \subseteq R^-$,*
(3) *dla dowolnego $S \subseteq A \times A$, jeżeli $R \subseteq S$ i S jest przechodnia, to $R^- \subseteq S$,*
(4) *$R^- = \bigcap\{S \subseteq A \times A : R \subseteq S \wedge S \text{ jest przechodnia}\}$.*
(Tzn. tranzytywne domknięcie relacji R na zbiorze A jest najmniejszą, w sensie inkluzji, relacją przechodnią na A zawierającą relację R.)

DOWÓD. Dla (1): Załóżmy, że dla $x, y, z \in A$, $<x, y>, <y, z> \in R^-$. Wówczas z definicji relacji R^-, dla pewnego $n \geq 2$ istnieją $z_1, \ldots, z_n \in A$ takie, że $x = z_1, <z_1, z_2> \in R, \ldots, <z_{n-1}, z_n> \in R, z_n = y$, oraz dla pewnego $m \geq 2$ istnieją $z'_1, \ldots, z'_m \in A$ takie, że $y = z'_1, <z'_1, z'_2> \in R, \ldots, <z'_{m-1}, z'_m> \in R, z'_m = z$. Ponieważ $z_n = z'_1$, więc mamy elementy $z_1, \ldots, z_n, z'_2, \ldots, z'_m \in A$ (tutaj $n + m - 1 \geq 2$) takie, że $x = z_1, <z_1, z_2> \in R, \ldots, <z_{n-1}, z_n> \in R$, $<z_n, z'_2> \in R, \ldots, <z'_{m-1}, z'_m> \in R, z'_m = z$. Ostatecznie, $<x, z> \in R^-$ na mocy definicji tranzytywnego domknięcia.

Dla (2): Niech dla $x, y \in A$, $<x, y> \in R$. Wówczas mamy $n = 2$ oraz $z_1, z_2 \in A$ takie, że $x = z_1, <z_1, z_2> \in R, z_2 = y$, zatem $<x, y> \in R^-$.

Dla (3): Załóżmy, że
(5) $R \subseteq S$ oraz
(6) S jest przechodnia.

Niech $<x, y> \in R^-$. Wówczas dla pewnego $n \geq 2$ istnieją $z_1, \ldots, z_n \in A$ takie, że $x = z_1, <z_1, z_2> \in R, \ldots, <z_{n-1}, z_n> \in R, z_n = y$. Wówczas na mocy (5), $<z_1, z_2> \in S, \ldots, <z_{n-1}, z_n> \in S$ i wobec (6) przez $(n-2)$-krotne zastosowanie warunku przechodniości otrzymujemy: $<z_1, z_n> \in S$, czyli $<x, y> \in S$.

Dla (4): Oznaczmy: $\mathcal{S} = \{S \subseteq A \times A : R \subseteq S \wedge S \textit{ jest przechodnia}\}$. Na podstawie (1) i (2), $R^- \in \mathcal{S}$, zatem $\bigcap \mathcal{S} \subseteq R^-$. Z drugiej strony, na podstawie (3), dla dowolnej relacji $S \in \mathcal{S}$, $R^- \subseteq S$, zatem $R^- \subseteq \bigcap \mathcal{S}$. $\square$

Jest oczywiste (por. warunki (2),(3) Tw. 7), że gdy relacja R jest przechodnia, to $R^- = R$ (na przykład tranzytywne domknięcie relacji pustej jest zatem relacją pustą). Wynika stąd między innymi, że operacja $^-$ tranzytywnego domknięcia w banalny sposób zachowuje własność przechodniości. Mniej banalnym faktem jest to, że zachowuje ona własności zwrotności i symetryczności:

TWIERDZENIE 8. *Jeżeli relacja R określona na zbiorze A jest zwrotna i symetryczna na tym zbiorze, to jej tranzytywne domknięcie R^- jest również relacją zwrotną i symetryczną na A.*

DOWÓD. Załóżmy że R jest zwrotna i symetryczna na A. Na mocy Tw. 5(1) oraz Tw. 7(2), $\mathrm{id}_A \subseteq R^-$, zatem R^- jest zwrotna. W celu wykazania, iż R^- jest

symetryczna załóżmy, że dla $x, y \in A$, $<x, y> \in R^-$. Wówczas dla pewnego $n \geq 2$ istnieją $z_1, \ldots, z_n \in A$ takie, że
(1) $x = z_1, y = z_n$ oraz
(2) $<z_1, z_2> \in R, \ldots, <z_{n-1}, z_n> \in R$.

Ponieważ R jest symetryczna, więc z (2) mamy: $< z_n, z_{n-1} > \in R, \ldots,$ $<z_2, z_1> \in R$, co w połączeniu z (1) daje: $<y, x> \in R^-$. $\square$

Rozdział 4. Funkcje

§1. Funkcja jako relacja binarna. Złożenie funkcji

Definicja. Relację binarną f na zbiorach A, B nazywamy *funkcją przekształcającą zbiór A w B* (co zapisujemy $f : A \longrightarrow B$), gdy
(1) $\forall x \in A\ \exists y \in B(<x, y> \in f)$,
(2) $\forall x \in A\ \forall y, z \in B((<x, y> \in f\ \wedge <x, z> \in f) \Rightarrow y = z)$.

Gdy relacja $f \subseteq A \times B$ jest funkcją przekształcającą zbiór A w B, to zapis $<x, y> \in f$ interpretujemy następująco: element y ze zbioru B *jest przyporządkowany według funkcji f* elementowi x ze zbioru A. Wówczas warunek (1) definicji funkcji, równoważny skądinąd wyrażeniu $D(f) = A$, czytamy następująco: każdemu elementowi ze zbioru A jest przyporządkowany według f jakiś element ze zbioru B. Natomiast warunek (2) mówi, iż co najwyżej jeden element ze zbioru B może być przyporządkowany danemu elementowi ze zbioru A. Ostatecznie, biorąc pod uwagę interpretację obu warunków, postrzegamy funkcję f przekształcającą A w B jako *przyporządkowanie* każdemu elementowi zbioru A dokładnie jednego elementu ze zbioru B. Ten jedyny element y taki, że $<x, y> \in f$, tzn. przyporządkowany elementowi x według funkcji f, oznacza się jako $f(x)$ i nazywa *wartością funkcji f dla argumentu x*. Mamy zatem:

$$\forall x \in A\ \forall y \in B(<x, y> \in f \Leftrightarrow y = f(x)).$$

Zbiór wszystkich funkcji przekształcających zbiór A w B oznaczamy: B^A, tzn.

$$B^A = \{f \subseteq A \times B : f \text{ jest funkcją przekształcającą } A \text{ w } B\}.$$

Uwaga. Dla dowolnego zbioru $B, B^{\varnothing} = \{\varnothing\}$ oraz $\varnothing^A = \varnothing$, gdy $A \neq \varnothing$.

Naturalnie zbiór oznaczany powyżej jako B^A istnieje, na podstawie aksjomatu podzbiorów, w którym formuła $\phi(x)$ jest postaci: x jest funkcją przekształcającą A w B, oraz zbiór z jest postaci: $P(A \times B)$.

Pierwsze z twierdzeń tego rozdziału podaje oczywisty warunek konieczny i wystarczający na to, aby dwie funkcje przekształcające jeden zbiór w drugi były jednym i tym samym zbiorem; warunkiem tym jest identyczność wartości tych funkcji na wszystkich argumentach:

Twierdzenie 1. *Dla dowolnych $f, g \in B^A, f = g$ wtw $\forall x \in A, f(x) = g(x)$.*

DOWÓD. Niech $f, g \in B^A$.

($\Rightarrow$): Załóżmy, że $f = g$; weźmy $x \in A$. Wówczas $<x, f(x)> \in f$, zatem $<x, f(x)> \in g$, lecz przecież $<x, g(x)> \in g$. Wobec warunku (2) definicji funkcji, $f(x) = g(x)$.

($\Leftarrow$): Załóżmy, że $\forall x \in A, f(x) = g(x)$. ($\subseteq$): niech $<x, y> \in f$. Wówczas $y = f(x)$, zatem $y = g(x)$; lecz $<x, g(x)> \in g$, więc $<x, y> \in g$. Analogicznie dla inkluzji ($\supseteq$). $\square$

TWIERDZENIE 2. *Niech* $f : A \longrightarrow B$ *oraz* $g : B \longrightarrow C$. *Wówczas* $f \circ g \in C^A$. (*Złożenie dwóch funkcji jest funkcją.*)

DOWÓD. Jest oczywiste, że $f \circ g \subseteq A \times C$.

Wykazujemy warunek (1) definicji funkcji: niech $a \in A$. Wówczas $<a, f(a)> \in f$ oraz $<f(a), g(f(a))> \in g$, zatem $<a, g(f(a))> \in f \circ g$ oraz $g(f(a)) \in C$.

Wykazujemy warunek (2) definicji funkcji: niech $<a, x>, <a, y> \in f \circ g$, gdzie $a \in A, x, y \in C$. Zatem dla pewnych $b, c \in B$, $<a, b> \in f$ i $<b, x> \in g$ oraz $<a, c> \in f$ i $<c, y> \in g$. Stąd, ponieważ f jest funkcją, na podstawie warunku (2) mamy: $b = c$; zatem $<b, x>, <b, y> \in g$. Lecz g jest funkcją, więc $x = y$. $\square$

Ustalmy *explicite* wartość złożenia dwóch funkcji na dowolnym argumencie:

TWIERDZENIE 3. *Niech* $f : A \longrightarrow B$ *oraz* $g : B \longrightarrow C$. *Wówczas* $\forall a \in A$, $(f \circ g)(a) = g(f(a))$.

DOWÓD. Niech $a \in A$. Wówczas dla dowolnego $c \in C$, $c = (f \circ g)(a)$ wtw $<a, c> \in f \circ g$ wtw dla pewnego $b \in B$, $<a, b> \in f$ i $<b, c> \in g$ wtw dla pewnego $b \in B$, $b = f(a)$ i $c = g(b)$ wtw $c = g(f(a))$. Stąd $(f \circ g)(a) = g(f(a))$. $\square$

§2. Bijekcja, funkcja odwrotna

W ogólności nie jest tak, że relacja odwrotna do funkcji $f : A \longrightarrow B$ jest funkcją przekształcającą zbiór B w A. Na przykład relacja odwrotna do funkcji $f : P(P(\varnothing)) \longrightarrow P(P(\varnothing))$ określonej następująco: $f(\varnothing) = f(P(\varnothing)) = \varnothing$, nie spełnia żadnego z warunków (1), (2) definiujących funkcję. Obecnie ograniczymy zbiór B^A wszystkich funkcji przekształcających A w B do zbioru tylko takich funkcji, których konwers należy do zbioru A^B.

DEFINICJA. Funkcja $f : A \longrightarrow B$ jest 1-1 (albo *jedno-jednoznaczna* lub *różnowartościowa*), gdy
$\forall x, y \in A\ (f(x) = f(y) \Rightarrow x = y)$
(tzn. gdy $\forall x, y \in A \forall z \in B(<x, z> \in f \wedge <y, z> \in f \Rightarrow x = y)$).

$f : A \longrightarrow B$ jest *„na"* (dokładniej: *przekształca zbiór A na B*), gdy $\forall y \in B\ \exists x \in A\ (y = f(x))$ (inaczej, gdy $D^{-1}(f) = B$).

$f : A \longrightarrow B$ jest *bijekcją*, gdy f jest 1-1 i *„na"*.

TWIERDZENIE 4. *Relacja identycznościowa id_A jest bijekcją przekształcającą zbiór A na A.*

DOWÓD. Oczywisty. □

TWIERDZENIE 5. *Jeżeli $f : A \longrightarrow B$ jest bijekcją, to $f^{\sim} \in A^B$.*

DOWÓD. Niech $f : A \longrightarrow B$ będzie bijekcją. Wykazujemy, że $f^{\sim}$ jest funkcją przekształcającą B w A.

Warunek (1) definicji funkcji: Niech $b \in B$. Ponieważ f przekształca A na B, więc dla pewnego $a \in A$, $b = f(a)$, tzn. $<a, b> \in f$. Stąd $<b, a> \in f^{\sim}$.

Warunek (2) definicji funkcji: Niech $b \in B, x, y \in A$ oraz $<b, x>, <b, y> \in f^{\sim}$. Zatem $<x, b>, <y, b> \in f$. Ponieważ f jest 1-1, więc $x = y$. □

Gdy relacja odwrotna do funkcji $f \in B^A$ jest funkcją przekształcającą zbiór B w A, wówczas związki miedzy tymi funkcjami są następującej postaci:

TWIERDZENIE 6. *Niech $f \in B^A$. Jeżeli $f^{\sim}$ jest funkcją przekształcającą zbiór B w zbiór A, to:*

(i) *dla dowolnych $b \in B, a \in A$, $f^{\sim}(b) = a$ wtw $b = f(a)$,*

(ii) *$\forall b \in B, f(f^{\sim}(b)) = b$ oraz $\forall a \in A, f^{\sim}(f(a)) = a$,*

(iii) *$f^{\sim} \circ f = id_B$ oraz $f \circ f^{\sim} = id_A$.*

DOWÓD. Niech $f \in B^A$ oraz $f^{\sim} \in A^B$.

Dla (i): $f^{\sim}(b) = a$ wtw $<b, a> \in f^{\sim}$ wtw $<a, b> \in f$ wtw $b = f(a)$.

Dla (ii): Na mocy (i) ponieważ $f^{\sim}(b) \in A$ mamy: $f^{\sim}(b) = f^{\sim}(b)$ wtw $b = f(f^{\sim}(b))$, skąd $b = f(f^{\sim}(b))$ oraz, ponieważ $f(a) \in B$, więc $f^{\sim}(f(a)) = a$ wtw $f(a) = f(a)$, skąd $f^{\sim}(f(a)) = a$.

Dla (iii): (iii) jest wnioskiem z (ii), Tw. 3, definicji relacji (funkcji) identycznościowej oraz Tw. 1. □

Aby wykazać, że ograniczenie zbioru B^A do zbioru bijekcji przekształcających zbiór A na B jest również niezbędne, a nie tylko wystarczające (Tw. 5) na to, by relacje odwrotne do nich były funkcjami przekształcającymi zbiór B w A, wykorzystamy warunek konieczny i wystarczający dla bycia bijekcją, sformułowany w następującym twierdzeniu:

Twierdzenie 7. *Dla dowolnej funkcji $f : A \longrightarrow B$, f jest bijekcją wtw istnieje funkcja $g : B \longrightarrow A$ taka, że $f \circ g = id_A$ oraz $g \circ f = id_B$.*

Dowód. ($\Rightarrow$): na mocy Tw. 5 oraz Tw. 6(iii).

($\Leftarrow$): Niech $f \in B^A$ oraz $g \in A^B$ będą takie, że $f \circ g = \mathrm{id}_A$ oraz $g \circ f = \mathrm{id}_B$. Załóżmy, że $f(x) = f(y)$ dla $x, y \in A$. Wówczas $g(f(x)) = g(f(y))$. Lecz z założenia, $g(f(x)) = x$ oraz $g(f(y)) = y$. Zatem $x = y$, czyli f jest 1-1. Niech $b \in B$. Na mocy założenia, $f(g(b)) = b$ oraz oczywiście $g(b) \in A$. Zatem f przekształca A na B. □

Twierdzenie 8. *Niech $f \in B^A$. f jest bijekcją wtw $f^{\sim} \in A^B$.*

Dowód. ($\Rightarrow$): Tw. 5.

($\Leftarrow$): Niech $f^{\sim}$ będzie funkcją przekształcającą zbiór B w A. Wówczas na mocy Tw. 6(iii) oraz Tw. 7, f jest bijekcją. □

Twierdzenie 9. *Niech $f \in B^A$. Jeżeli $f^{\sim} \in A^B$, to $f^{\sim}$ jest bijekcją.*

Dowód. Niech $f^{\sim} : B \longrightarrow A$. Zastosujmy Tw. 7, kładąc w miejsce funkcji f funkcję $f^{\sim}$ (zamieniając zbiór A na B oraz B na A). Wówczas w oparciu o Tw. 6(iii), wnosimy, iż $f^{\sim}$ jest bijekcją. □

Zakończymy niniejszy paragraf algebraicznym opisem zbioru $\mathrm{Bij}(A)$ wszystkich bijekcji przekształcających zbiór A na siebie (naturalnie istnienie takiego zbioru jest gwarantowane przez aksjomat podzbiorów). W tym celu sformułujmy najpierw twierdzenie mówiące, że operacja złożenia funkcji zachowuje własność bycia bijekcją:

Twierdzenie 10. *Złożenie bijekcji jest bijekcją.*

Dowód. Niech $f : A \longrightarrow B$ oraz $g : B \longrightarrow C$ będą bijekcjami. Niech $x, y \in A$ oraz załóżmy, że $(f \circ g)(x) = (f \circ g)(y)$. Wówczas na mocy Tw. 3, $g(f(x)) = g(f(y))$. Ponieważ g jest 1-1, $f(x) = f(y)$, a stąd $x = y$, bo f jest 1-1. Ostatecznie, $f \circ g$ jest różnowartościowa.

Niech $c \in C$. Wówczas $c = g(b)$ dla jakiegoś $b \in B$, bo g przekształca B na C. Lecz $b = f(a)$ dla jakiegoś $a \in A$, bo f przekształca A na B. Zatem $c = g(f(a)) = (f \circ g)(a)$, czyli $f \circ g$ przekształca A na C. □

Definicja. Dowolny zbiór A z operacjami, 2-argumentową $\circ$, 1-argumentową $-$, oraz wyróżnionym elementem 1 spełniającymi równości, dla dowolnych $x, y, z \in A$:

$(x \circ y) \circ z = x \circ (y \circ z)$,
$x \circ 1 = 1 \circ x = x$,
$x \circ -x = -x \circ x = 1$,
nazywamy *grupą*.

Precyzyjniej, dowolny model $(A, \circ, -, 1)$ dla powyższych równości (dla języka I rzędu ze stałą indywidualną 1 oraz symbolami funkcyjnymi $\circ, -$, bez symboli predykatywnych) nazywamy *grupą*.

TWIERDZENIE 11. $(\mathrm{Bij}(A), \circ, ^\sim, \mathrm{id}_A)$, *gdzie* $\mathrm{Bij}(A)$ *jest zbiorem wszystkich bijekcji przekształcających zbiór* A *na* A, *jest grupą.*

DOWÓD. Na podstawie Tw. 10, operacja złożenia relacji $\circ$ jest operacją na zbiorze $\mathrm{Bij}(A)$. Według Tw. 5 i Tw. 9 operacja konwersu relacji $^\sim$ jest również operacją na zbiorze $\mathrm{Bij}(A)$. Wreszcie, na mocy Tw. 4, $\mathrm{id}_A \in \mathrm{Bij}(A)$.

Równość $(f \circ g) \circ h = f \circ (g \circ h)$ jest prawdziwa już dla dowolnych relacji binarnych f, g, h określonych na zbiorze A (Tw. 3(1), Rozdział 3). Podobnie równości $f \circ \mathrm{id}_A = f$ oraz $\mathrm{id}_A \circ f = f$ zachodzą już dla dowolnej relacji binarnej f na zbiorze A (Tw. 3(2), Rozdział 3). Równości $f \circ f^\sim = \mathrm{id}_A$ oraz $f^\sim \circ f = \mathrm{id}_A$ dla dowolnej $f \in \mathrm{Bij}(A)$, są konsekwencją Tw. 6(iii). $\square$

§3. Obraz i przeciwobraz zbioru

DEFINICJA. Niech $f : A \longrightarrow B$. Dla dowolnego $X \subseteq A$, zbiór $\overrightarrow{f}(X) = \{b \in B : \exists a \in X,\ b = f(a)\} = \{f(a) : a \in X\}$ nazywamy *obrazem zbioru X według funkcji f.*

Dla dowolnego $Y \subseteq B$, zbiór $\overleftarrow{f}(Y) = \{a \in A : f(a) \in Y\}$ nazywamy *przeciwobrazem zbioru Y według funkcji f.*

Uwaga. Naturalnie istnienie obrazu i przeciwobrazu zbioru według danej funkcji jest gwarantowane przez aksjomat podzbiorów.

TWIERDZENIE 12. *Dla dowolnych* $f : A \longrightarrow B,\ X, Y \subseteq A,\ Z \subseteq B$:
(1) $X \subseteq Y \Rightarrow \overrightarrow{f}(X) \subseteq \overrightarrow{f}(Y)$,
(2) $\overrightarrow{f}(X \cup Y) = \overrightarrow{f}(X) \cup \overrightarrow{f}(Y)$,
(3) $\overrightarrow{f}(X \cap Y) \subseteq \overrightarrow{f}(X) \cap \overrightarrow{f}(Y)$,
(4) f *jest* $1{-}1 \Rightarrow \overrightarrow{f}(X \cap Y) = \overrightarrow{f}(X) \cap \overrightarrow{f}(Y)$,
(5) $X \subseteq \overleftarrow{f}(\overrightarrow{f}(X))$,
(6) $\overrightarrow{f}(\overleftarrow{f}(Z)) \subseteq Z$,
(7) f *jest bijekcją* $\Rightarrow (X = \overleftarrow{f}(\overrightarrow{f}(X)) \wedge \overrightarrow{f}(\overleftarrow{f}(Z)) = Z)$.

Dowód. Dla (1): Załóżmy, że $X \subseteq Y$. Weźmy $b \in \overrightarrow{f}(X)$. Wówczas $b = f(a)$ dla pewnego $a \in X$. Zatem z założenia, $a \in Y$, czyli $f(a) \in \overrightarrow{f}(Y)$, tzn. $b \in \overrightarrow{f}(Y)$.

Dla (2): Ponieważ $X \subseteq X \cup Y$ oraz $Y \subseteq X \cup Y$, więc na mocy (1) mamy: $\overrightarrow{f}(X) \subseteq \overrightarrow{f}(X \cup Y)$ oraz $\overrightarrow{f}(Y) \subseteq \overrightarrow{f}(X \cup Y)$, zatem $\overrightarrow{f}(X) \cup \overrightarrow{f}(Y) \subseteq \overrightarrow{f}(X \cup Y)$. Aby dowieść odwrotnej inkluzji załóżmy, że $b \in \overrightarrow{f}(X \cup Y)$. Zatem dla pewnego $a \in X \cup Y$, $b = f(a)$. Mamy więc: $a \in X$ lub $a \in Y$. Gdy $a \in X$, to oczywiście $f(a) \in \overrightarrow{f}(X) \subseteq \overrightarrow{f}(X) \cup \overrightarrow{f}(Y)$, czyli $b \in \overrightarrow{f}(X) \cup \overrightarrow{f}(Y)$. Analogicznie gdy $a \in Y$.

Dla (3): Ponieważ $X \cap Y \subseteq X$ oraz $X \cap Y \subseteq Y$, więc na mocy (1), $\overrightarrow{f}(X \cap Y) \subseteq \overrightarrow{f}(X)$ oraz $\overrightarrow{f}(X \cap Y) \subseteq \overrightarrow{f}(Y)$, zatem $\overrightarrow{f}(X \cap Y) \subseteq \overrightarrow{f}(X) \cap \overrightarrow{f}(Y)$.

Dla (4): Załóżmy, że f jest różnowartościowa. Na mocy (3) wystarczy wykazać inkluzję $\overrightarrow{f}(X) \cap \overrightarrow{f}(Y) \subseteq \overrightarrow{f}(X \cap Y)$. Niech więc $b \in \overrightarrow{f}(X) \cap \overrightarrow{f}(Y)$. Wtedy $b \in \overrightarrow{f}(X)$ oraz $b \in \overrightarrow{f}(Y)$. Zatem dla pewnego $a_1 \in X$, $b = f(a_1)$ oraz dla pewnego $a_2 \in Y$, $b = f(a_2)$. Wówczas, skoro $f(a_1) = f(a_2)$, więc z założenia, $a_1 = a_2$. Zatem $a_1 \in Y$ (bo $a_2 \in Y$). Ostatecznie, $a_1 \in X \cap Y$, skąd $f(a_1) \in \overrightarrow{f}(X \cap Y)$, tzn. $b \in \overrightarrow{f}(X \cap Y)$.

Dla (5): Niech $a \in X$. Wówczas $f(a) \in \overrightarrow{f}(X)$, zatem z definicji przeciwobrazu: $a \in \overleftarrow{f}(\overrightarrow{f}(X))$.

Dla (6): Niech $b \in \overrightarrow{f}(\overleftarrow{f}(Z))$. Wówczas dla pewnego $a \in \overleftarrow{f}(Z)$, $b = f(a)$. Lecz wtedy, z definicji przeciwobrazu, $f(a) \in Z$, zatem $b \in Z$.

Dla (7): Załóżmy, że f jest 1-1 oraz „*na*". Aby wykazać pierwszą z równości wystarczy, na mocy (5), wykazać inkluzję $\overleftarrow{f}(\overrightarrow{f}(X)) \subseteq X$. Niech więc $a \in \overleftarrow{f}(\overrightarrow{f}(X))$. Wówczas $f(a) \in \overrightarrow{f}(X)$, zatem dla pewnego $a_1 \in X$, $f(a) = f(a_1)$. Ponieważ f jest 1-1, więc $a = a_1$, stąd $a \in X$.

Aby wykazać drugą równość wystarczy, na mocy (6) wykazać inkluzję $Z \subseteq \overrightarrow{f}(\overleftarrow{f}(Z))$. Załóżmy więc, że $b \in Z$. Ponieważ funkcja f przekształca zbiór A na B, zaś $Z \subseteq B$, więc dla pewnego $a \in A$, $b = f(a)$. Stąd $f(a) \in Z$, zatem $a \in \overleftarrow{f}(Z)$, co z kolei oznacza, że $f(a) \in \overrightarrow{f}(\overleftarrow{f}(Z))$. Ostatecznie, $b \in \overrightarrow{f}(\overleftarrow{f}(Z))$. □

Tw. 12 nie jest naturalnie wyczerpującym przeglądem własności obrazu i przeciwobrazu zbioru. Można je rozszerzyć, podając na przykład odpowiedniki warunków (1), (2), (3), (4) dla przeciwobrazu:

$U \subseteq V \Rightarrow \overleftarrow{f}(U) \subseteq \overleftarrow{f}(V)$,
$\overleftarrow{f}(U \cup V) = \overleftarrow{f}(U) \cup \overleftarrow{f}(V)$,
$\overleftarrow{f}(U \cap V) = \overleftarrow{f}(U) \cap \overleftarrow{f}(V)$, dla dowolnych $U, V \subseteq B$.

Na koniec tego paragrafu zdefiniujmy jeszcze użyteczne pojęcia obcięcia funkcji oraz ciągu:

Definicja. Niech $f \in B^A$ oraz $X \subseteq A$. Naturalnie zbiór par uporządkowanych $\{<x, f(x)>: x \in X\}$ jest funkcją przekształcającą zbiór X w zbiór B. Nazywamy ją *obcięciem funkcji f do zbioru X* i oznaczamy: $f \upharpoonright X$.

Definicja. Niech A będzie niepustym zbiorem. Dowolną funkcję $a : \{1, ..., n\} \longrightarrow A$ nazywamy *n-wyrazowym ciągiem elementów ze zbioru A* i oznaczamy $(a(1), \ldots, a(n))$.

Dowolną funkcję $a : \{1, 2, \ldots\} \longrightarrow A$ nazywamy *ciągiem (nieskończonym) elementów ze zbioru A* i oznaczamy $(a(1), a(2), \ldots)$.

Wartość ciągu a na argumencie $i \in \{1, \ldots, n, \ldots\}$, czyli $a(i)$, nazywamy *i-tym wyrazem ciągu a.*

§4. Rodziny indeksowane

Definicja. Niech I, U będą dowolnymi niepustymi zbiorami. Dowolną funkcję $f \in P(U)^I$ nazywamy *rodziną indeksowaną zbiorów (podzbiorów zbioru U).*

Oznaczmy dla dowolnego $i \in I, f(i) = A_i$, gdzie $A_i \subseteq U$. Wówczas obraz $\overrightarrow{f}(I)$ zbioru I według funkcji f jest to zbiór $\{A_i : i \in I\}$. Często nieformalnie rodzinę indeksowaną $f : I \longrightarrow P(U)$ utożsamia się z obrazem $\{A_i : i \in I\}$.

Twierdzenie 13. *Niech $\{A_i : i \in I\}, \{B_i : i \in I\}$ będą rodzinami indeksowanymi podzbiorów zbioru U. Wówczas:*

(1) $\bigcup\{A_i : i \in I\} \cup \bigcup\{B_i : i \in I\} = \bigcup\{A_i \cup B_i : i \in I\}$,
(2) $\bigcap\{A_i : i \in I\} \cap \bigcap\{B_i : i \in I\} = \bigcap\{A_i \cap B_i : i \in I\}$,
(3) $U - \bigcup\{A_i : i \in I\} = \bigcap\{U - A_i : i \in I\}$,
(4) $U - \bigcap\{A_i : i \in I\} = \bigcup\{U - A_i : i \in I\}$.

Dowód. Dla (1): ($\subseteq$): Niech $x \in \bigcup\{A_i : i \in I\} \cup \bigcup\{B_i : i \in I\}$. Wówczas $x \in \bigcup\{A_i : i \in I\}$ lub $x \in \bigcup\{B_i : i \in I\}$. Niech $x \in \bigcup\{A_i : i \in I\}$. Wtedy dla pewnego $j \in I$, $x \in A_j$, zatem $x \in A_j \cup B_j$, czyli $x \in \bigcup\{A_i \cup B_i : i \in I\}$. Analogicznie gdy $x \in \bigcup\{B_i : i \in I\}$.

($\supseteq$): Niech $x \in \bigcup\{A_i \cup B_i : i \in I\}$. Wówczas dla pewnego $j \in I, x \in A_j \cup B_j$. Zatem $x \in A_j$ lub $x \in B_j$. Niech $x \in A_j$, wtedy $x \in \bigcup\{A_i : i \in I\}$, zatem $x \in \bigcup\{A_i : i \in I\} \cup \bigcup\{B_i : i \in I\}$. Analogicznie gdy $x \in B_j$.

Dla (2): Mamy: $x \in \bigcap\{A_i : i \in I\} \cap \bigcap\{B_i : i \in I\}$ wtw ($x \in \bigcap\{A_i : i \in I\}$ oraz $x \in \bigcap\{B_i : i \in I\}$) wtw ($\forall i \in I,\ x \in A_i$ oraz $\forall i \in I,\ x \in B_i$) wtw $\forall i \in I(x \in A_i \wedge x \in B_i)$ wtw $\forall i \in I,\ x \in A_i \cap B_i$ wtw $x \in \bigcap\{A_i \cap B_i : i \in I\}$.

Dla (3): ($\subseteq$): Niech $x \in U - \bigcup\{A_i : i \in I\}$, tzn. $x \in U$ oraz $x \notin \bigcup\{A_i : i \in I\}$. Wówczas $\forall i \in I,\ x \notin A_i$, czyli $\forall i \in I,\ x \in U - A_i$, stąd $x \in \bigcap\{U - A_i : i \in I\}$.

($\supseteq$): Odwrotne do powyższego rozumowanie.

Dla (4): ($\subseteq$): Niech $x \in U - \bigcap\{A_i : i \in I\}$, tzn. $x \in U$ oraz $x \notin \bigcap\{A_i : i \in I\}$. Wówczas dla pewnego $j \in I,\ x \notin A_j$. Zatem $x \in U - A_j$. Stąd $x \in \bigcup\{U - A_i : i \in I\}$.

($\supseteq$): Odwrotne do powyższego rozumowanie. $\square$

DEFINICJA. Przez *produkt kartezjański rodziny indeksowanej* $\{A_i : i \in I\}$ rozumiemy zbiór $\{a \in (\bigcup\{A_i : i \in I\})^I : \forall i \in I,\ a(i) \in A_i\}$, oznaczany w postaci: $\Pi\{A_i : i \in I\}$

W przypadku, gdy $I = \{1, \ldots, n\}$, produkt $\Pi\{A_i : i \in I\}$, oznaczamy w postaci: $A_1 \times \ldots \times A_n$. Jest jasne, że elementami tego produktu są wszystkie ciągi n-wyrazowe a elementów zbioru $A_1 \cup \ldots \cup A_n$ takie, że dla każdego $i \in \{1, \ldots, n\},\ a(i) \in A_i$.

Zwróćmy uwagę na to, iż formalnie rzecz biorąc, argumentem operacji Π nie jest obraz $\{A_i : i \in I\}$, lecz sama rodzina indeksowana f – ta, dla której $\vec{f}(I) = \{A_i : i \in I\}$. Przeciwnie niż w przypadku operacji $\bigcup$ stosowanej w Tw. 13 i dalej, gdzie argumentem jest właśnie ów obraz, nie zaś rodzina indeksowana.

Uwaga. W przypadku, gdy $n = 2$, pojęcie produktu kartezjańskiego $A_1 \times A_2$ jako zbioru wszystkich 2-wyrazowych ciągów takich, że pierwszy wyraz ciągu jest elementem zbioru A_1, zaś drugi wyraz ciągu jest elementem A_2 nie jest tożsame z pojęciem produktu kartezjańskiego zbiorów A_1, A_2 jako zbioru wszystkich par uporządkowanych, których pierwszy element należy do A_1, a drugi do A_2. Jednakże jedyna istotna własność par uporządkowanych (zob. Tw. 1, Rozdział 3) przysługuje ciągom 2-wyrazowym:

dla dowolnych ciągów 2-wyrazowych a, b elementów jakiegoś zbioru A, jeżeli $a = b$, to $a(1) = b(1)$ oraz $a(2) = b(2)$ (na mocy Tw. 1).

Zatem we wszelkich zastosowaniach oba pojęcia produktu dwóch zbiorów można traktować jako identyczne.

TWIERDZENIE 14. *Jeżeli* $\forall i \in I,\ A_i = A$, *to* $\Pi\{A_i : i \in I\} = A^I$.

DOWÓD. Jest oczywiste z definicji produktu, że w przypadku, gdy rodzina indeksowana jest funkcją stałą: $\forall i \in I,\ f(i) = A$, to $\Pi\{A_i : i \in I\} = \{a \in (\bigcup\{A\})^I : \forall i \in I, a(i) \in A\} = \{a \in A^I : \forall i \in I, a(i) \in A\} = A^I$. $\square$

Na koniec uogólnijmy pojęcie relacji binarnej (2-argumentowej) do pojęcia relacji n-argumentowej:

dowolny podzbiór R produktu $A_1 \times \ldots \times A_n$ nazywamy *relacją n-argumentową na zbiorach* $A_1, \ldots, A_n$.

Rozdział 5. Zbiory częściowo uporządkowane

§1. Pojęcie zbioru częściowo uporządkowanego, elementy największy i najmniejszy oraz maksymalny i minimalny

DEFINICJA. Relację binarną $\leqslant$ określoną na zbiorze A nazywamy *relacją częściowo porządkującą*, gdy $\leqslant$ jest zwrotna, antysymetryczna i przechodnia na A.

Wówczas parę $<A, \leqslant>$ nazywamy *zbiorem częściowo uporządkowanym.*

TWIERDZENIE 1. *Niech $<A, \leqslant>$ będzie zbiorem częściowo uporządkowanym oraz $B \subseteq A$. Wówczas relacja $\leqslant \cap (B \times B)$ jest relacją częściowo porządkującą na zbiorze B.*

DOWÓD. Jest oczywiste, że warunki zwrotności, antysymetrii oraz przechodniości są spełnione dla relacji $\leqslant \cap (B \times B)$, gdy są one spełnione dla relacji $\leqslant$ (nawet gdy $B = \varnothing$; relacja $\varnothing$ na zbiorze $\varnothing$ jest częściowo porządkująca). $\square$

Uwaga. Gdy $< A, \leqslant>$ jest zbiorem cz. up. oraz $B \subseteq A$, to zbiór cz. up. $< B, \leqslant \cap (B \times B)>$ nazywamy *podzbiorem zbioru cz. up.* $< A, \leqslant>$. Oznaczamy go w skrócie w postaci: $<B, \leqslant>$. Ponadto zamiast pisać $<x, y> \in \leqslant$, zwyczajnie piszemy $x \leqslant y$.

DEFINICJA. Niech $<A, \leqslant>$ – zbiór cz. up. Element $a \in A$ nazywamy *największym* (*najmniejszym*) *w* $<A, \leqslant>$, gdy $\forall x \in A, x \leqslant a$ ($\forall x \in A, a \leqslant x$).

Element $a \in A$ nazywamy *maksymalnym* (*minimalnym*) *w* $<A, \leqslant>$, gdy $\forall x \in A\ (a \leqslant x \Rightarrow a = x)$ ($\forall x \in A\ (x \leqslant a \Rightarrow x = a)$).

TWIERDZENIE 2. *W dowolnym zbiorze cz. up. $<A, \leqslant>$ istnieje co najwyżej jeden element największy i co najwyżej jeden element najmniejszy.*

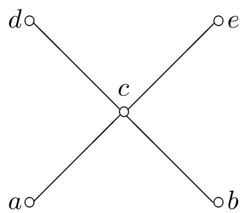
DOWÓD. Załóżmy, że $a, b \in A$ są elementami największymi w $<A, \leqslant>$. Wówczas $\forall x \in A, x \leqslant a$ oraz $\forall x \in A, x \leqslant b$. Zatem $b \leqslant a$ oraz $a \leqslant b$, co wobec antysymetrii relacji $\leqslant$ daje $a = b$. Analogicznie dla elementu najmniejszego. $\square$

TWIERDZENIE 3. *Jeżeli w zbiorze cz. up. $<A, \leqslant>$ istnieje element największy (najmniejszy), to jest on jedynym elementem maksymalnym (minimalnym) w $<A, \leqslant>$.*

DOWÓD. Niech a będzie elementem największym w $<A, \leqslant>$. Załóżmy, że $a \leqslant x$ dla jakiegoś $x \in A$. Ponieważ $x \leqslant a$, więc z antysymetrii relacji $\leqslant$, $a = x$ co dowodzi, że a jest elementem maksymalnym w $< A, \leqslant>$.

Załóżmy, że b jest elementem maksymalnym w $<A, \leqslant>$. Z definicji elementu największego mamy: $b \leqslant a$, zatem z założenia $b = a$, czyli a jest jedynym elementem maksymalnym w $<A, \leqslant>$. Podobnie dla elementu najmniejszego. $\square$

Przykład. Diagram Hassego dla skończonego zbioru cz. up.:



Elementy d, e są elementami maksymalnymi zaś a, b – minimalnymi w zbiorze cz. up. $<\{a, b, c, d, e\}, \leqslant>$, gdzie relacja $\leqslant$ jest określona diagramem w sposób następujący: dla dowolnych różnych elementów x, y tego zbioru, $x \leqslant y$ wtw z punktu x można „przejść” do punktu y wzdłuż łamanej, kierując się na każdym jej odcinku z dołu do góry. Zatem $a \leqslant c$, $a \leqslant e$ oraz $a \leqslant d$. Identycznie dla elementu b (zamiast a). Natomiast $\neg(a \leqslant b)$. Ponadto $\neg(c \leqslant a)$ itd. Zakłada się, czego diagram nie uwidacznia, że każdy ze zbiorów a, b, c, d, e jest sam ze sobą w relacji $\leqslant$.

Znanym przykładem relacji częściowo porządkującej jest relacja inkluzji określona na zbiorze potęgowym danego zbioru:

Twierdzenie 4. *Dla dowolnego zbioru U, $<P(U), \subseteq>$ jest zbiorem częściowo uporządkowanym, w którym U jest elementem największym oraz $\varnothing$ jest elementem najmniejszym.*

Dowód. Oczywisty na mocy twierdzeń: dla dowolnych $X, Y, Z \in P(U)$, $X \subseteq X$, $(X \subseteq Y \wedge Y \subseteq X) \Rightarrow X = Y$, $(X \subseteq Y \wedge Y \subseteq Z) \Rightarrow X \subseteq Z$ oraz $\forall X \in P(U)(X \subseteq U \wedge \varnothing \subseteq X)$. $\square$

Twierdzenie 5. *Dowolny niepusty skończony zbiór cz. up. posiada element maksymalny.*

Dowód. Udowodnimy indukcyjnie wyrażenie:

(1) Dla każdego $n \geqslant 1$, w dowolnym n-elementowym zbiorze cz. up. $<A, \leqslant>$ istnieje element maksymalny.

Dla $n = 1$: oczywiście dowolny zbiór cz. up. jednoelementowy posiada element maksymalny.

Weźmy dowolne $n \geqslant 1$. Założenie indukcyjne:

(2) w dowolnym n-elementowym zbiorze cz. up. $< A, \leqslant >$ istnieje element maksymalny.

Mamy wykazać:

(3) w dowolnym $(n+1)$-elementowym zbiorze cz. up. $< A, \leqslant >$ istnieje element maksymalny.

Rozważmy zatem dowolny zbiór cz. up. $<A, \leqslant>$, $(n+1)$-elementowy. Niech $x \in A$. Wówczas $<A - \{x\}, \leqslant>$ jest zbiorem cz. up. n-elementowym. Na mocy (2), niech a będzie jego elementem maksymalnym. Naturalnie $a \neq x$. Zachodzi: $a \leqslant x$ lub $\neg(a \leqslant x)$.

Jeśli $a \leqslant x$, to x jest elementem maksymalnym w $<A, \leqslant>$. Bowiem gdyby istniał $y \in A$ taki, że $x \leqslant y$ oraz $x \neq y$, to wobec przechodniości relacji $\leqslant$ byłoby: $a \leqslant y$. Ponadto $a \neq y$, gdyby bowiem $a = y$, to wobec antysymetrii relacji $\leqslant$, $a = x$, co jest niemożliwe. Zatem wobec maksymalności elementu a w $<A - \{x\}, \leqslant>$, byłoby: $y \notin A - \{x\}$, tzn. $y = x$, sprzeczność.

Jeśli zaś nie jest tak, że $a \leqslant x$, to oczywiście a jest elementem maksymalnym w $<A, \leqslant>$. $\square$

Definicja. Niech $<A, \leqslant>$ będzie zbiorem cz. up. oraz niech $X \subseteq A$. Element $a \in A$ nazywamy *ograniczeniem górnym* (*dolnym*) *zbioru* X w $<A, \leqslant>$, gdy dla każdego $x \in X$, $x \leqslant a$ (dla każdego $x \in X$, $a \leqslant x$).

Zbiór wszystkich ograniczeń górnych (dolnych) zbioru X będziemy oznaczać $Og(X)$ $(Od(X))$, czyli

$Og(X) = \{a \in A : \forall x \in X,\ x \leqslant a\}$,

$Od(X) = \{a \in A : \forall x \in X,\ a \leqslant x\}$.

Uwaga. Naturalnie istnienie zbiorów $Og(X), Od(X)$ jest gwarantowane przez aksjomat podzbiorów.

Przykład. Dla zbioru cz. up. $< \{a, b, c, d, e\}, \leqslant>$ określonego powyżej diagramem, $Og(\{c, d, e\}) = \varnothing$, $Od(\{c, d, e\}) = \{c, a, b\}$.

W dalszym ciągu elementy największy oraz najmniejszy danego zbioru cz. up. $<A, \leqslant>$, o ile te elementy istnieją, będziemy oznaczać odpowiednio 1 oraz 0.

Twierdzenie 6. *Niech* $<A, \leqslant>$ *będzie zbiorem cz. up. Wówczas*

(1) *Jeżeli w* $<A, \leqslant>$ *istnieje element największy* 1, *to* $Og(A) = \{1\}$,

(2) *Jeżeli w* $<A, \leqslant>$ *nie istnieje element największy, to* $Og(A) = \varnothing$,

(3) *Jeżeli w* $<A, \leqslant>$ *istnieje element najmniejszy* 0, *to* $Od(A) = \{0\}$,

(4) *Jeżeli w* $<A, \leqslant>$ *nie istnieje element najmniejszy, to* $Od(A) = \varnothing$,

(5) $Og(\varnothing) = Od(\varnothing) = A$.

Dowód. Dla (1): Załóżmy, że 1 jest elementem największym w $<A, \leqslant>$.

($\subseteq$): Niech $a \in Og(A)$, czyli $\forall x \in A, x \leqslant a$. Zatem a jest elementem największym w $<A, \leqslant>$, czyli na mocy Tw. 2, $a = 1$, tzn. $a \in \{1\}$.

($\supseteq$): Ponieważ $\forall x \in A, x \leqslant 1$, więc $1 \in Og(A)$.

Dla (2): Załóżmy, że w $<A, \leqslant>$ nie ma elementu największego. Gdyby $Og(A) \neq \varnothing$, to dla jakiegoś $a \in A$ byłoby $a \in Og(A)$, zatem $\forall x \in A, x \leqslant a$, czyli a byłby elementem największym wbrew założeniu.

Dla (3): Analogicznie jak dla (1).

Dla (4): Analogicznie jak dla (2).

Dla (5): Jest oczywiste, że $Og(\varnothing) \subseteq A$. Aby wykazać odwrotną inkluzję załóżmy, że $a \in A$. Ponieważ $a \in Og(\varnothing)$ wtw $\forall x(x \in \varnothing \Rightarrow x \leqslant a)$ oraz zachodzi $\forall x(x \in \varnothing \Rightarrow x \leqslant a)$, więc $a \in Og(\varnothing)$. Identycznie dla $Od(\varnothing)$. □

§2. Zbiór liniowo uporządkowany, lemat Kuratowskiego-Zorna

Definicja. Niech $<A, \leqslant>$ – zbiór cz. up. Elementy $x, y \in A$ nazywamy *porównywalnymi* w $<A, \leqslant>$, gdy $x \leqslant y$ lub $y \leqslant x$. Zbiór cz. up. $<A, \leqslant>$, w którym dowolne dwa elementy są porównywalne nazywamy *łańcuchem*.

Zbiór cz. up. $<A, \leqslant>$, w którym relacja $\leqslant$ jest spójna nazywamy *zbiorem liniowo uporządkowanym*, zaś relację $\leqslant$ – *relacją liniowo porządkującą*.

Twierdzenie 7. *Zbiór cz. up. $<A, \leqslant>$ jest łańcuchem wtw jest on liniowo uporządkowany.*

Dowód. Warunek spójności: $\forall x, y \in A(x \leqslant y$ lub $y \leqslant x$ lub $x = y)$, jest równoważny warunkowi porównywalności: $\forall x, y \in A(x \leqslant y$ lub $y \leqslant x)$. □

Przykład. Zbiór cz. up. $<N, \leqslant>$, gdzie N – zbiór liczb naturalnych oraz $\leqslant$ jest relacją bycia liczbą mniejszą lub równą, jest łańcuchem mającym element najmniejszy – liczbę 0, oraz niemającym elementu największego.

Liniowo uporządkowany zbiór $<N, \leqslant>$ ma ponadto następującą własność: dowolny jego niepusty podzbiór posiada element najmniejszy.

Definicja. Zbiór liniowo uporządkowany $<A, \leqslant>$ taki, że dla dowolnego niepustego $X \subseteq A$ w $<X, \leqslant>$ istnieje element najmniejszy, nazywamy *zbiorem dobrze uporządkowanym*.

Twierdzenie 8. *Jeżeli w łańcuchu $<A, \leqslant>$ istnieje element maksymalny (minimalny), to jest on elementem największym (najmniejszym).*

Dowód. Niech a będzie elementem maksymalym w łańcuchu $<A, \leqslant>$. Weźmy $x \in A$. a, x są zatem porównywalne, tzn. $x \leqslant a$ lub $a \leqslant x$. Gdy $a \leqslant x$, to wobec maksymalności a, $a = x$, czyli $x \leqslant a$ wobec zwrotności relacji $\leqslant$. Ostatecznie $x \leqslant a$, co dowodzi, wobec dowolności wyboru x, że a jest elementem największym w $<A, \leqslant>$. Analogicznie dla elementu minimalnego. □

Wniosek. *Dowolny niepusty skończony łańcuch posiada elementy największy i najmniejszy.*

Dowód. Oczywisty na mocy Twierdzeń 5, 8 w przypadku stwierdzania istnienia elementu największego. Aby uzasadnić istnienie elementu najmniejszego można posłużyć się dualną wersją Tw. 5: *dowolny niepusty skończony zbiór cz. up. posiada element minimalny*, której dowód jest analogiczny do dowodu Tw. 5. □

Lemat Kuratowskiego-Zorna. *Niech $<A, \leqslant>$ będzie zbiorem cz. up. Jeżeli dla dowolnego niepustego łańcucha $Ł \subseteq A$ istnieje w $<A, \leqslant>$ ograniczenie górne (tzn. $Og(Ł) \neq \emptyset$), to w $<A, \leqslant>$ istnieje element maksymalny.*

Lemat Kuratowskiego-Zorna (sformułowanie szczegółowe). *Niech $<A, \leqslant>$ będzie zbiorem cz. up. Jeżeli dla dowolnego niepustego łańcucha $Ł \subseteq A$ istnieje w $<A, \leqslant>$ ograniczenie górne, to dla każdego $a \in A$ w $<A, \leqslant>$ istnieje element maksymalny x taki, że $a \leqslant x$.*

Twierdzenie 9. *Oba sformułowania lematu Kuratowskiego-Zorna są sobie równoważne.*

Dowód. Jest oczywiste, że sformułowanie szczegółowe implikuje sformułowanie pierwsze. Aby dowieść odwrotnej implikacji załóżmy, że zachodzi pierwsze sformułowanie lematu oraz że w jakimś ustalonym zbiorze cz. up. $<A, \leqslant>$ dla dowolnego niepustego łańcucha $Ł \subseteq A$, $Og(Ł) \neq \emptyset$. Niech $a \in A$. Rozważmy zbiór cz. up. $< Og(\{a\}), \leqslant>$, aby zastosować dla niego pierwsze sformułowanie lematu. Niech więc $Ł \subseteq Og(\{a\})$ będzie niepustym łańcuchem. Wówczas $Ł$ jest łańcuchem w $<A, \leqslant>$, bo $Og(\{a\}) \subseteq A$. Zatem z założenia istnieje ograniczenie górne zbioru $Ł$ w $<A, \leqslant>$. Niech b będzie tym ograniczeniem górnym. Skoro $Ł \neq \emptyset$, więc dla jakiegoś $x \in Ł$ mamy: $a \leqslant x$ (bo $Ł \subseteq Og(\{a\})$) oraz $x \leqslant b$, zatem $a \leqslant b$, czyli $b \in Og(\{a\})$, tzn. b jest ograniczeniem górnym łańcucha $Ł$ w $<Og(\{a\}), \leqslant>$. Wobec dowolności wyboru łańcucha $Ł$ w $<Og(\{a\}), \leqslant>$, stosując pierwsze sformułowanie lematu dla zbioru cz. up. $<Og(\{a\}), \leqslant>$, otrzymujemy: w $<Og(\{a\}), \leqslant>$ istnieje element maksymalny. Niech z będzie tym elementem maksymalnym. Jest oczywiste, że $a \leqslant z$. Pozostaje wykazać, że z jest elementem maksymalnym w $<A, \leqslant>$. Przypuśćmy że z nie jest elementem maksymalnym w $<A, \leqslant>$. Wówczas dla jakiegoś $y \in A$, $z \leqslant y$ oraz $z \neq y$. Jednakże wtedy $a \leqslant y$, tzn. $y \in Og(\{a\})$. Zatem z nie byłby maksymalny w $<Og(\{a\}), \leqslant>$. $\square$

Lemat Kuratowskiego-Zorna jest użyteczny w stwierdzaniu istnienia elementów maksymalnych w nieskończonych zbiorach cz. up. Jednakże „pracuje" on również dla skończonych zbiorów cz. up. Mianowicie można go zastosować do dowodu Tw. 5. W tym celu należy wykazać prawdziwość poprzednika implikacji pierwszego sformułowania lematu, tzn. zdania: „w dowolnym niepustym skończonym zbiorze cz. up. każdy niepusty łańcuch ma ograniczenie górne". Można tego dokonać natychmiast w oparciu o Wniosek z Tw. 8. Rozważając bowiem jakiś niepusty łańcuch w skończonym zbiorze cz. up., wobec skończoności tego łańcucha istnieje w nim element największy, zatem jego ograniczenie górne. Naturalnie, użycie tu Wniosku z Tw. 8 zakłada, że jest on wcześniej uzasadniony nie w oparciu o Tw. 5 i Tw. 8, ale inaczej – na przykład dzięki prostemu dowodowi indukcyjnemu.

§3. Pojęcie kraty

DEFINICJA. Niech $<A, \leqslant>$ będzie zbiorem cz. up. oraz $X \subseteq A$. Element najmniejszy w $<Og(X), \leqslant>$ nazywamy *kresem górnym zbioru* X w $<A, \leqslant>$ i oznaczamy: $\sup X$ (*supremum zbioru* X). Element największy w $< Od(X), \leqslant>$ nazywamy *kresem dolnym zbioru* X w $<A, \leqslant>$ i oznaczamy: $\inf X$ (*infimum zbioru* X).

PRZYKŁAD. Dla rozważanego powyżej przykładu zbioru cz. up. zadanego diagramem, $\sup\{c, d, e\}$ nie istnieje, zaś $\inf\{c, d, e\} = c$.

TWIERDZENIE 10. *Niech* $< A, \leqslant>$ *będzie zbiorem cz. up. Wówczas*
(1) *Jeżeli w* $< A, \leqslant>$ *istnieje element największy* 1, *to* $\sup A = 1$ *oraz* $\inf \varnothing = 1$,
(2) *Jeżeli w* $< A, \leqslant>$ *nie istnieje element największy, to nie istnieje* $\sup A$ *oraz nie istnieje* $\inf \varnothing$,
(3) *Jeżeli w* $< A, \leqslant>$ *istnieje element najmniejszy* 0, *to* $\inf A = 0$ *oraz* $\sup \varnothing = 0$,
(4) *Jeżeli w* $< A, \leqslant>$ *nie istnieje element najmniejszy, to nie istnieje* $\inf A$ *oraz nie istnieje* $\sup \varnothing$,
(5) *Dla dowolnego* $x \in A$, $\sup\{x\} = \inf\{x\} = x$,
(6) *Dla dowolnych* $x, y \in A$, $x \leqslant y$ *wtw* $\sup\{x, y\} = y$ *wtw* $\inf\{x, y\} = x$,
(7) *Jeżeli* A *ma więcej niż jeden element, to dla dowolnego* $X \subseteq A$, *jeżeli istnieją kresy* $\sup X, \inf X$ *w* $<A, \leqslant>$, *to* $X \neq \varnothing$ *wtw* $\inf X \leqslant \sup X$.

DOWÓD. Dla (1): Na mocy Tw. 6(1), $Og(A) = \{1\}$, zatem elementem najmniejszym w $<\{1\}, \leqslant>$, czyli $\sup A$ jest element 1. Na mocy Tw. 6(5), $Od(\varnothing) = A$, zatem największym elementem w $<Od(\varnothing), \leqslant>$, czyli $\inf \varnothing$ jest element 1.

Dla (2): Załóżmy, że w $<A, \leqslant>$ nie ma elementu największego. Wówczas na mocy Tw. 6(2), $Og(A) = \varnothing$, zatem w $<Og(A), \leqslant>$ nie ma elementu najmniejszego, bo nie ma tam żadnego elementu. Dlatego $\sup A$ nie istnieje. Również na mocy Tw. 6(5), $Od(\varnothing) = A$, zatem w $<Od(\varnothing), \leqslant>$ nie ma elementu największego, czyli nie istnieje $\inf \varnothing$.

Dla (3): Analogicznie na mocy Tw. 6(3),(5).

Dla (4): Analogicznie na mocy Tw. 6(4),(5).

Dla (5): Niech $x \in A$. Ponieważ $x \in Og(\{x\})$ (relacja $\leqslant$ jest zwrotna) oraz $\forall y \in Og(\{x\}), x \leqslant y$, więc x jest najmniejszym ograniczeniem górnym zbioru $\{x\}$, zatem $x = \sup\{x\}$. Analogicznie wykazujemy, że $x = \inf\{x\}$.

Dla (6): Niech $x, y \in A$.

$(\Rightarrow)$: Załóżmy, że $x \leqslant y$. Ponieważ $y \leqslant y$, więc $y \in Og(\{x, y\})$. Niech $z \in Og(\{x, y\})$. Wówczas $y \leqslant z$, zatem y jest najmniejszym ograniczeniem górnym zbioru $\{x, y\}$, czyli $y = \sup\{x, y\}$.

$(\Leftarrow)$: Załóżmy, że $y = \sup\{x, y\}$. Ponieważ $\sup\{x, y\} \in Og(\{x, y\})$, więc $x \leqslant \sup\{x, y\}$, stąd $x \leqslant y$.

Analogicznie dowodzimy drugiej równoważności.

Dla (7): Niech A ma więcej niż jeden element. Rozważmy $X \subseteq A$, dla którego istnieją kresy górny i dolny w $<A, \leqslant>$.

$(\Rightarrow)$: Załóżmy, że $X \neq \varnothing$. Niech więc $a \in X$. Ponieważ $\inf X$ jest ograniczeniem dolnym zbioru X, więc $\inf X \leqslant a$. Analogicznie, $a \leqslant \sup X$. Zatem z przechodniości relacji $\leqslant$ uzyskujemy: $\inf X \leqslant \sup X$.

$(\Leftarrow)$: Załóżmy, że $\inf X \leqslant \sup X$ oraz nie wprost, że $X = \varnothing$. Wówczas z (2) i (1), $\inf X = 1$, oraz z (4) i (3), $\sup X = 0$, gdzie $1, 0$ są odpowiednio największym i najmniejszym elementem w $<A, \leqslant>$. Z założenia mamy więc: $1 \leqslant 0$. Oczywiście $0 \leqslant 1$, zatem z antysymetrii relacji $\leqslant$ uzyskujemy: $0 = 1$. Jednakże wówczas, wbrew założeniu, A jest zbiorem 1-elementowym, bowiem dla dowolnego $a \in A$, $0 \leqslant a$ oraz $a \leqslant 0$ (skoro $0 = 1$), co implikuje $a = 0$. $\square$

DEFINICJA. Zbiór cz. up. $<A, \leqslant>$, w którym $A \neq \varnothing$ oraz dla każdego $X \subseteq A$ istnieją kresy $\sup X, \inf X$ nazywamy *kratą zupełną*.

TWIERDZENIE 11. *Dla dowolnego zbioru U, zbiór cz. up. $<P(U), \subseteq>$ jest kratą zupełną.*

DOWÓD. Niech $\mathcal{R} \subseteq P(U)$. Wykażemy, że $\bigcup \mathcal{R} = \sup \mathcal{R}$. Naturalnie $\bigcup \mathcal{R} \in P(U)$, bo skoro $\mathcal{R} \subseteq P(U)$, tzn. $\forall A \in \mathcal{R}, A \subseteq U$, więc $\bigcup \mathcal{R} \subseteq U$. Ponieważ $\forall A \in \mathcal{R}, A \subseteq$

$\bigcup\mathcal{R}$, więc $\bigcup\mathcal{R} \in Og(\mathcal{R})$. Niech $Y \in Og(\mathcal{R})$, czyli $\forall A \in \mathcal{R}, A \subseteq Y$. Wówczas naturalnie $\bigcup\mathcal{R} \subseteq Y$ (Tw. 11(2), Rozdział 1), zatem $\bigcup\mathcal{R}$ jest najmniejszym ograniczeniem górnym zbioru $\mathcal{R}$, tzn. $\bigcup\mathcal{R} = \sup\mathcal{R}$.

Gdy $\mathcal{R} = \emptyset$, to zgodnie z Tw. 10(1) oraz Tw. 4, $\inf\mathcal{R} = U$. Niech $\mathcal{R} \neq \emptyset$. Wykażemy, że $\bigcap\mathcal{R} = \inf\mathcal{R}$. Naturalnie $\bigcap\mathcal{R} \in P(U)$, bo dla dowolnego $A \in \mathcal{R}$, $\bigcap\mathcal{R} \subseteq A$, zaś $A \subseteq U$. Ponieważ $\forall A \in \mathcal{R}, \bigcap\mathcal{R} \subseteq A$, więc $\bigcap\mathcal{R} \in Od(\mathcal{R})$. Niech $Y \in Od(\mathcal{R})$, tzn. $\forall A \in \mathcal{R},\ Y \subseteq A$. Wówczas naturalnie $Y \subseteq \bigcap\mathcal{R}$ (Tw. 18(2), Rozdział 1), zatem $\bigcap\mathcal{R}$ jest największym ograniczeniem dolnym zbioru $\mathcal{R}$, czyli $\bigcap\mathcal{R} = \inf\mathcal{R}$. $\square$

TWIERDZENIE 12. *W każdej kracie zupełnej istnieje element największy i najmniejszy.*

DOWÓD. Niech $<A, \leqslant>$ będzie kratą zupełną. Istnieje więc $\sup A$. Zatem na mocy Tw. 10(2) w $<A, \leqslant>$ istnieje element największy. Ponieważ $\inf A$ również istnieje, więc na mocy Tw. 10(4) istnieje w $<A, \leqslant>$ element najmniejszy. $\square$

Okazuje się, że wystarczy stwierdzić istnienie kresów jednego rodzaju dla wszystkich podzbiorów danego zbioru cz. up., aby uznać go za kratę zupełną:

TWIERDZENIE 13. *Niech $<A, \leqslant>$ będzie zbiorem cz. up. Jeżeli dla każdego $X \subseteq A$ istnieje w $<A, \leqslant>$ kres dolny $\inf X$, to $<A, \leqslant>$ jest kratą zupełną.*

DOWÓD. Załóżmy, że dla dowolnego $X \subseteq A$ istnieje $\inf X$. Aby dowieść twierdzenia wystarczy wykazać, że dla każdego $X \subseteq A$ istnieje $\sup X$ w $<A, \leqslant>$. Rozważmy więc dowolny $X \subseteq A$. Wykażemy, że z założenia istniejący w $<A, \leqslant>$ $\inf Og(X)$ (bo $Og(X) \subseteq A$) jest kresem górnym zbioru X w $<A, \leqslant>$.

Wykażmy najpierw, że $\inf Og(X) \in Og(X)$ tzn. że $\forall x \in X,\ x \leqslant \inf Og(X)$. Niech więc $x \in X$. Wówczas $\forall a \in Og(X), x \leqslant a$, zatem x jest ograniczeniem dolnym zbioru $Og(X)$; wobec tego $x \leqslant \inf Og(X)$, bo $\inf Og(X)$ jest największym ograniczeniem dolnym zbioru $Og(X)$.

Niech teraz $y \in Og(X)$. Naturalnie $\inf Og(X) \in Od(Og(X))$, zatem $\inf Og(X) \leqslant y$, co dowodzi, że $\inf Og(X)$ jest najmniejszym ograniczeniem górnym zbioru X, zatem $\inf Og(X) = \sup X$. $\square$

Analogicznie można dowieść twierdzenia mówiącego o istnieniu kresów górnych jako warunku wystarczającym na to, by zbiór cz. up. był kratą zupełną.

TWIERDZENIE 14. *Każdy zbiór dobrze uporządkowany mający element największy jest kratą zupełną.*

Dowód. Niech $<A, \leqslant>$ będzie zbiorem dobrze uporządkowanym z elementem największym 1. Wówczas na podstawie Tw. 10(1) istnieje kres dolny zbioru pustego: $\inf \varnothing = 1$. Niech $\varnothing \neq X \subseteq A$. Oznaczmy symbolem 0 element najmniejszy w $<X, \leqslant>$. Ponieważ $\forall y \in X, 0 \leqslant y$, więc 0 jest ograniczeniem dolnym zbioru X. Gdy zaś dla jakiegoś $z \in A, z$ jest ograniczeniem dolnym zbioru X, to $z \leqslant 0$, bo $0 \in X$. Zatem 0 jest największym ograniczeniem dolnym zbioru X, tzn. $0 = \inf X$. Ostatecznie, na mocy Tw. 13, $<A, \leqslant>$ jest kratą zupełną. □

Definicja. Niepusty zbiór cz. up. $<A, \leqslant>$ nazywamy *kratą*, gdy dla dowolnych $x, y \in A$ istnieją kresy $\inf\{x, y\}, \sup\{x, y\}$.

Naturalnie każda krata zupełna jest kratą.

Twierdzenie 15. *Każdy niepusty łańcuch $<A, \leqslant>$ jest kratą.*

Dowód. Niech $<A, \leqslant>$ będzie niepustym łańcuchem. Ponieważ $\forall x, y \in A$ ($x \leqslant y$ lub $y \leqslant x$), więc na mocy Tw. 10(6), dla dowolnych $x, y \in A$ ($\sup\{x, y\} = y$ oraz $\inf\{x, y\} = x$) lub ($\sup\{x, y\} = x$ oraz $\inf\{x, y\} = y$). □

Przykład. $<N, \leqslant>$, gdzie N – zbiór liczb naturalnych oraz $\leqslant$ – relacja bycia liczbą mniejszą lub równą, jest kratą, choć nie jest kratą zupełną (nie istnieje w $<N, \leqslant>$ element największy – porównaj Tw. 12).

Przykład. Rozważmy na zbiorze $N - \{0\}$ konwers relacji podzielności $|$ określony następująco: $\forall x, y \in N - \{0\}, x \,|^{\smile}\, y$ wtw $\exists k \in N - \{0\},\ y = xk$ (tzn. $x \,|^{\smile}\, y$ wtw y jest podzielne przez x). Wówczas $<N - \{0\}, |^{\smile}>$ jest kratą, w której dla dowolnych $x, y \in N - \{0\},\ \inf\{x, y\} = \mathrm{nwp}(x, y)$ (największy wspólny podzielnik liczb x, y) oraz $\sup\{x, y\} = \mathrm{nww}(x, y)$ (najmniejsza wspólna wielokrotność liczb x, y).

Twierdzenie 16. *Niech $<A, \leqslant>$ będzie kratą. Wówczas dla dowolnego niepustego skończonego zbioru $X \subseteq A$ istnieją $\inf X$ oraz $\sup X$.*

Dowód. Załóżmy, że $<A, \leqslant>$ jest kratą. Wykażemy indukcyjnie, że dla dowolnego $n = 1, 2, \ldots$, dla dowolnych $x_1, x_2, \ldots, x_n \in A$ istnieje $\sup\{x_1, x_2, \ldots, x_n\}$ w $<A, \leqslant>$.

Dla $n = 1$: naturalnie dla dowolnego singletonu $\{x\} \subseteq A$ istnieje $\sup\{x\}$ (Tw. 10(5)).

Załóżmy, że dla jakiegoś n, dla dowolnych $x_1, x_2, \ldots, x_n \in A$ istnieje $\sup\{x_1, x_2, \ldots, x_n\}$. Mamy wykazać, że dla dowolnych $x_1, \ldots, x_n, x_{n+1} \in A$, istnieje $\sup\{x_1, x_2, \ldots, x_n, x_{n+1}\}$.

Rozważmy więc dowolne $x_1, x_2, \ldots, x_n, x_{n+1} \in A$. Z założenia istnieje kres $\sup\{x_1, x_2, \ldots, x_n\}$. Wykażemy, że $\sup\{x_1, \ldots, x_n, x_{n+1}\} = \sup\{\sup\{x_1, \ldots, x_n\}, x_{n+1}\}$ (ponieważ $<A, \leqslant>$ jest kratą, więc $\sup\{\sup\{x_1, \ldots, x_n\}, x_{n+1}\}$ musi istnieć jeśli tylko istnieje $\sup\{x_1, \ldots, x_n\}$). Oznaczmy $a = \sup\{\sup\{x_1, \ldots, x_n\}, x_{n+1}\}$. Ponieważ dla każdego $i = 1, 2, \ldots, n$, $x_i \leqslant \sup\{x_1, \ldots, x_n\} \leqslant a$ oraz $x_{n+1} \leqslant a$, więc $a \in Og(\{x_1, \ldots, x_n, x_{n+1}\})$. Załóżmy teraz, że $x \in Og(\{x_1, \ldots, x_n, x_{n+1}\})$. Wówczas $x \in Og(\{x_1, \ldots, x_n\})$, zatem $\sup\{x_1, \ldots, x_n\} \leqslant x$. Naturalnie $x_{n+1} \leqslant x$. Zatem $x \in Og(\{\sup\{x_1, \ldots, x_n\}, x_{n+1}\})$. Stąd $a \leqslant x$, co dowodzi, że $a = \sup\{x_1, \ldots,_n, x_{n+1}\}$.

Analogicznie wykazujemy odpowiednik dowodzonego wyrażenia dla kresów dolnych:

dla dowolnego $n = 1, 2, \ldots$, dla dowolnych $x_1, x_2, \ldots, x_n \in A$ istnieje kres $\inf\{x_1, x_2, \ldots, x_n\}$ w $<A, \leqslant>$. □

Wniosek. *Każda krata skończona jest kratą zupełną.*

Dowód. Ponieważ każdy podzbiór kraty skończonej jest skończony, więc wobec Tw. 16 wystarczy wykazać, że w kracie skończonej istnieją $\sup \varnothing$ oraz $\inf \varnothing$.

Niech $<A, \leqslant>$ będzie kratą skończoną. Wówczas istnieje $\sup A$. Zatem na mocy Tw. 10(2), w $<A, \leqslant>$ istnieje element największy 1. Stąd według Tw. 10(1), $\inf \varnothing = 1$, zatem $\inf \varnothing$ istnieje. Ponadto w $<A, \leqslant>$ istnieje $\inf A$. Zatem na mocy Tw. 10(4) w $<A, \leqslant>$ istnieje element najmniejszy 0. Stąd, zgodnie z Tw. 10(3), $\sup \varnothing = 0$, zatem $\sup \varnothing$ istnieje. □

§4. Izomorfizm zbiorów częściowo uporządkowanych

Definicja. Niech $<A_1, \leqslant_1>, <A_2, \leqslant_2>$ będą zbiorami cz. up. Funkcję $f : A_1 \longrightarrow A_2$ taką, że f jest bijekcją przekształcającą A_1 na A_2 oraz taką, że spełniony jest warunek:

(ISO) $\forall x, y \in A_1 (x \leqslant_1 y \text{ wtw } f(x) \leqslant_2 f(y))$,

nazywamy *izomorfizmem zbiorów cz. up.* $<A_1, \leqslant_1>, <A_2, \leqslant_2>$.

Zbiory cz. up. $< A_1, \leqslant_1>, < A_2, \leqslant_2>$, dla których istnieje izomorfizm nazywamy *izomorficznymi*.

Jasne jest, że zbiory cz. up. $<A_1, \leqslant_1>, <A_2, \leqslant_2>$ izomorficzne mają nie tylko taką samą ilość elementów, ale dzięki warunkowi (ISO), również tę samą strukturę uporządkowania, w jednym zbiorze daną relacją $\leqslant_1$, w drugim relacją $\leqslant_2$.

Okazuje się, że każdą strukturę uporządkowania wyznaczoną przez relację częściowego porządku można reprezentować relacją inkluzji w następującym sensie:

TWIERDZENIE 17 (O REPREZENTACJI ZBIORÓW CZ. UP.). *Niech* $<A, \leqslant>$ *będzie dowolnym zbiorem częściowo uporządkownym. Wówczas funkcja* $f : A \longrightarrow \{Od(\{x\}) : x \in A\}$ (*gdzie* $Od(\{x\})$ *jest zbiorem ograniczeń dolnych zbioru* $\{x\}$ *w* $<A, \leqslant>$, *tzn.* $Od(\{x\}) = \{y \in A : y \leqslant x\}$) *określona następująco:* $\forall x \in A, f(x) = Od(\{x\})$, *jest izomorfizmem zbiorów cz. up.* $<A, \leqslant>, <\{Od(\{x\}) : x \in A\}, \subseteq>$.

DOWÓD. Niech $<A, \leqslant>$ będzie dowolnym zbiorem cz. up. Naturalnie $<\{Od(\{x\}) : x \in A\}, \subseteq>$, jako podzbiór zbioru cz. up. $<P(A), \subseteq>$, jest zbiorem cz. up. Z określenia widać, że funkcja f jest „*na*". Wykażmy, że f jest różnowartościowa. Niech zatem $f(x) = f(y)$ dla jakichś $x, y \in A$. Wówczas $Od(\{x\}) = Od(\{y\})$. Ponieważ $x \in Od(\{x\})$, więc $x \in Od(\{y\})$, czyli $x \leqslant y$. Ponieważ $y \in Od(\{y\})$, więc $y \in Od(\{x\})$, czyli $y \leqslant x$, zatem na mocy antysymetrii relacji $\leqslant$ otrzymujemy, $x = y$.

Wykazujemy warunek (ISO). Niech $x, y \in A$.

($\Rightarrow$): Załóżmy, że $x \leqslant y$. Niech $z \in Od(\{x\})$. Wówczas $z \leqslant x$. Zatem z przechodniości relacji $\leqslant$, $z \leqslant y$, czyli $z \in Od(\{y\})$, co oznacza, wobec dowolności wyboru elementu z, że $Od(\{x\}) \subseteq Od(\{y\})$. Zatem $f(x) \subseteq f(y)$.

($\Leftarrow$): Na odwrót, niech $f(x) \subseteq f(y)$, tzn. $Od(\{x\}) \subseteq Od(\{y\})$. Ponieważ $x \in Od(\{x\})$, więc $x \in Od(\{y\})$, zatem $x \leqslant y$. $\square$

Zgodnie z identycznością uporządkowań zbiorów cz. up. izomorficznych, oczekujemy, iż w przypadku, gdy jeden z nich jest kratą zupełną, to i drugi również jest kratą zupełną:

TWIERDZENIE 18. *Niech* $f : A \longrightarrow B$ *będzie izomorfizmem zbiorów cz. up.* $<A, \leqslant_A>$ *oraz* $<B, \leqslant_B>$. *Niech ponadto* $<A, \leqslant_A>$ *będzie kratą zupełną. Wówczas* $<B, \leqslant_B>$ *jest również kratą zupełną taką, że dla dowolnego* $Y \subseteq B, \sup_B Y = f(\sup_A \overleftarrow{f}(Y))$ *oraz* $\inf_B Y = f(\inf_A \overleftarrow{f}(Y))$.

Ponadto dla dowolnego $X \subseteq A$, $f(\sup_A X) = \sup_B \overrightarrow{f}(X)$ *oraz* $f(\inf_A X) = \inf_B \overrightarrow{f}(X)$.

DOWÓD. Załóżmy, że f jest izomorfizmem zbiorów cz. up. $<A, \leqslant_A>$, $<B, \leqslant_B>$ oraz że $<A, \leqslant_A>$ jest kratą zupełną. Niech $Y \subseteq B$. Wówczas $\overleftarrow{f}(Y) \subseteq A$. Niech $y \in Y$. Ponieważ f jest „*na*" rozważmy $x \in A$ taki, że $y = f(x)$. Naturalnie z definicji przeciwobrazu, $x \in \overleftarrow{f}(Y)$. Ponieważ istniejący z założenia $\sup_A \overleftarrow{f}(Y)$ jest ograniczeniem górnym zbioru $\overleftarrow{f}(Y)$ w $<A, \leqslant_A>$, więc $x \leqslant_A \sup_A \overleftarrow{f}(Y)$. Stąd na podstawie (ISO), $f(x) \leqslant_B f(\sup_A \overleftarrow{f}(Y))$, zatem $y \leqslant_B f(\sup_A \overleftarrow{f}(Y))$. Czyli wobec dowolności wyboru elementu y ze zbioru Y, $f(\sup_A \overleftarrow{f}(Y))$ jest ograniczeniem górnym zbioru Y w $<B, \leqslant_B>$.

Załóżmy teraz, że $z \in Og_B(Y)$, tzn. $\forall y \in Y,\ y \leqslant_B z$. Niech $a \in A$ będzie taki, że $z = f(a)$. Wówczas $\forall x \in \overleftarrow{f}(Y),\ x \leqslant_A a$. Weźmy bowiem $x \in \overleftarrow{f}(Y)$. Wtedy $f(x) \in Y$, zatem $f(x) \leqslant_B z$, tzn. $f(x) \leqslant_B f(a)$. Z warunku (ISO) mamy wówczas: $x \leqslant_A a$. Ostatecznie, a jest ograniczeniem górnym zbioru $\overleftarrow{f}(Y)$ w $<A, \leqslant_A>$. Zatem $\sup_A \overleftarrow{f}(Y) \leqslant_A a$ i konsekwentnie z (ISO) otrzymujemy: $f(\sup_A \overleftarrow{f}(Y)) \leqslant_B f(a)$, czyli $f(\sup_A \overleftarrow{f}(Y)) \leqslant_B z$, co oznacza, że $f(\sup_A \overleftarrow{f}(Y))$ jest najmniejszym ograniczeniem górnym zbioru Y w $<B, \leqslant_B>$, czyli $f(\sup_A \overleftarrow{f}(Y)) = \sup_B Y$.

Analogicznie dowodzi się, że $f(\inf_A \overleftarrow{f}(Y))$ jest kresem dolnym zbioru Y w $<B, \leqslant_B>$.

Aby dowieść drugiej części twierdzenia, rozważmy $X \subseteq A$. Ponieważ f jest bijekcją, więc na mocy Tw. 12(7), Rozdział 4, $X = \overleftarrow{f}(\overrightarrow{f}(X))$. Zatem, na podstawie pierwszej części twierdzenia, $\sup_B \overrightarrow{f}(X) = f(\sup_A \overleftarrow{f}(\overrightarrow{f}(X))) = f(\sup_A X)$ oraz $\inf_B \overrightarrow{f}(X) = f(\inf_A \overleftarrow{f}(\overrightarrow{f}(X))) = f(\inf_A X)$. $\square$

Ostatnie twierdzenie tego rozdziału stwierdza możliwość odtworzenia porządku danego zbioru cz. up. na bijektywnym obrazie tego zbioru:

Twierdzenie 19. *Niech $<A, \leqslant_A>$ będzie zbiorem cz. up. oraz niech B będzie dowolnym zbiorem takim, że $B = \overrightarrow{f}(A)$ dla pewnej bijekcji f. Wówczas relacja $\leqslant_B$ zdefiniowana na zbiorze B następująco:*
$\forall x, y \in B,\ x \leqslant_B y$ wtw $f^{\sim}(x) \leqslant_A f^{\sim}(y)$,
jest relacją częściowo porządkującą oraz funkcja f jest izomorfizmem zbiorów częściowo uporządkowanych $<A, \leqslant_A>, <B, \leqslant_B>$.

Ponadto jeśli $< A, \leqslant_A>$ jest liniowo (dobrze) uporządkowany, to również $<B, \leqslant_B>$ jest liniowo (dobrze) uporządkowany.

Dowód. Niech $< A, \leqslant_A>$ będzie zbiorem cz. up. Załóżmy, że $f : A \longrightarrow B$ jest bijekcją. Oczywiście konwers funkcji f jest wówczas funkcją przekształcającą zbiór B na A (Tw. 8, Rozdział 4). Naturalnie dla dowolnego $x \in B$, skoro $\leqslant_A$ jest zwrotna, więc $f^{\sim}(x) \leqslant_A f^{\sim}(x)$. Zatem z definicji relacji $\leqslant_B$, $x \leqslant_B x$, tzn. $\leqslant_B$ jest zwrotna. Aby dowieść jej antysymetrii załóżmy, że dla $x, y \in B$, $x \leqslant_B y$ oraz $y \leqslant_B x$. Wówczas $f^{\sim}(x) \leqslant_A f^{\sim}(y)$ oraz $f^{\sim}(y) \leqslant_A f^{\sim}(x)$, zatem na mocy antysymetrii relacji $\leqslant_A$, $f^{\sim}(x) = f^{\sim}(y)$. Stąd $f(f^{\sim}(x)) = f(f^{\sim}(y))$ i konsekwentnie, $x = y$ (por. Tw. 6(ii), Rozdział 4). Przechodniość relacji $\leqslant_B$ wynika natychmiast z przechodniości relacji $\leqslant_A$.

Aby wykazać, że bijekcja f jest żądanym izomorfizmem należy dowieść warunku (ISO): $\forall a, b \in A : a \leqslant_A b$ wtw $f(a) \leqslant_B f(b)$. Otóż na mocy Tw. 6(ii), Rozdział 4 oraz definicji relacji $\leqslant_B$ mamy: $a \leqslant_A b$ wtw $f^{\sim}(f(a)) \leqslant_A f^{\sim}(f(b))$ wtw $f(a) \leqslant_B f(b)$.

Załóżmy teraz, że $<A, \leqslant_A>$ jest łańcuchem. Rozważmy dowolne $x, y \in B$. Oczywiście $f^{\sim}(x), f^{\sim}(y) \in A$. Zatem z założenia, $f^{\sim}(x) \leqslant_A f^{\sim}(y)$ lub $f^{\sim}(y) \leqslant_A f^{\sim}(x)$, co z definicji relacji $\leqslant_B$ jest równoważne alternatywie: $x \leqslant_B y$ lub $y \leqslant_B x$. Wobec dowolności wyboru elementów x, y stwierdzamy, że $<B, \leqslant_B>$ jest łańcuchem.

Załóżmy wreszcie, że $<A, \leqslant_A>$ nie tylko jest łańcuchem, ale ponadto dla dowolnego niepustego $X \subseteq A$ istnieje element najmniejszy w $<X, \leqslant_A>$. Rozważmy dowolny niepusty podzbiór Y w łańcuchu $<B, \leqslant_B>$. Ponieważ $\varnothing \neq \overleftarrow{f}(Y) \subseteq A$, więc zgodnie z założeniem, niech a będzie elementem najmniejszym zbioru cz. up. $<\overleftarrow{f}(Y), \leqslant_A>$. Czyli

(1) $\forall b \in \overleftarrow{f}(Y), a \leqslant_A b$

oraz $a \in \overleftarrow{f}(Y)$. Stąd oczywiście: $f(a) \in Y$. Rozważmy dowolny $x \in Y$. Naturalnie $f^{\sim}(x) \in \overleftarrow{f}(Y)$, bo $f(f^{\sim}(x)) \in Y$, skoro $f(f^{\sim}(x)) = x$. Zatem na mocy (1), $a \leqslant_A f^{\sim}(x)$, czyli $f^{\sim}(f(a)) \leqslant_A f^{\sim}(x)$ (bo $a = f^{\sim}(f(a))$), co wobec definicji relacji $\leqslant_B$ daje: $f(a) \leqslant_B x$. Wobec dowolności wyboru elementu x ze zbioru Y, świadczy to o tym, iż $f(a)$ jest elementem najmniejszym w zbiorze cz. up. $<\overleftarrow{f}(Y), \leqslant_B>$. Ponieważ $Y \subseteq B$ był dowolnie wybrany, więc łańcuch $<B, \leqslant_B>$ jest dobrze uporządkowany. $\square$

Literatura poświęcona zbiorom częściowo uporządkowanym jest bardzo bogata. W kwestiach fundamentalnych por. np. [18] lub [15]. Pozycje te obejmują również zagadnienia z następnego rozdziału.

Rozdział 6. Relacje równoważnościowe

Jednym z bardzo użytecznych, nie tylko w matematyce, pojęć teoriomnogościowych jest *relacja równoważnościowa*. Wskazuje ona na pewien aspekt, względem którego elementy zbioru, na którym jest określona są do siebie podobne, oraz formalnie reprezentuje to podobieństwo.

W ogólności, gdy jakieś dowolne dwa obiekty są do siebie podobne, to są one podobne zawsze pod pewnym względem. Ów wzgląd czy aspekt to pewna własność bądź własności. Dwa przedmioty są podobne ze względu na daną własność, gdy mają one tę samą „wartość" czy też jakość tej własności. Mówimy na przykład, że dwa przedmioty materialne są podobne ze względu na kształt czy barwę, gdy przedmioty te mają ten sam kształt czy są tej samej barwy.

Otóż podobieństwo ze względu na daną własność, ma wszystkie cechy relacji równoważnościowej:

- zwrotność: dany obiekt jest podobny ze względu na daną własność sam do siebie,

- symetria: jeżeli jeden obiekt jest podobny ze względu na daną własność do drugiego, czyli gdy oba obiekty mają tę samą „wartość" owej własności, to naturalnie ten drugi obiekt jest podobny względem tej własności do pierwszego,

- przechodniość: gdy jeden obiekt jest podobny ze względu na daną własność do drugiego, ten zaś z kolei do trzeciego, to wszystkie trzy obiekty mają tę samą „wartość" własności, w szczególności pierwszy i trzeci, zatem są one podobne względem tej własności.

Z drugiej strony, można uważać, że dowolna relacja równoważności reprezentuje pewien stosunek podobieństwa. Mówiąc precyzyjniej, reprezentuje ona stosunek podobieństwa ze względu na pewną własność, jaki ma miejsce wśród elementów zbioru, na którym relacja jest określona. Własność ta jest konstytuowana przez swoje wartości, jakimi są tu tzw. *klasy abstrakcji* względem tej relacji równoważności. Owe klasy abstrakcji są jednoznacznie przez tę relację określone (por. §2).

§1. Krata relacji równoważności

DEFINICJA. Relację binarną $\approx$ określoną na zbiorze A nazywamy *relacją równoważnościową* (lub *równoważności*), gdy $\approx$ jest zwrotna, symetryczna i przechodnia na A.

Uwaga. Relacja $\varnothing$ jest (jedyną) relacją równoważnościową na zbiorze $\varnothing$.

PRZYKŁAD. Relacje $\mathrm{id}_A, A \times A$ są równoważnościowe na A.

TWIERDZENIE 1. *Relacja* id_A, *gdzie* $A \neq \varnothing$, *jest jedyną relacją równoważnościową i częściowo porządkującą na zbiorze* A.

DOWÓD. Jest oczywiste, że id_A jest jednocześnie relacją równoważnościową i częściowo porządkującą. Załóżmy, że relacja binarna $R \subseteq A \times A$ jest relacją równoważnościową oraz częściowo porządkującą, oraz $R \neq \mathrm{id}_A$. Ponieważ R jest zwrotna, więc $\mathrm{id}_A \subseteq R$. Zatem nie jest tak, że $R \subseteq \mathrm{id}_A$. Niech więc dla $x, y \in A$ będzie tak, że $<x, y> \in R$ oraz $<x, y> \notin \mathrm{id}_A$, tzn. $x \neq y$. Ponieważ R jest symetryczna, więc $<y, x> \in R$. Lecz R jest również antysymetryczna, zatem $x = y$. Sprzeczność. □

TWIERDZENIE 2. *Niech dla dowolnego zbioru* $A, E(A)$ *oznacza zbiór wszystkich relacji równoważności na zbiorze* A. *Wówczas* $<E(A), \subseteq>$ *jest kratą zupełną.*

DOWÓD. Naturalnie $<E(A), \subseteq>$ jest zbiorem cz. up., jako że $E(A) \subseteq P(A \times A)$, zaś $<P(A \times A), \subseteq>$ jest zbiorem cz. up.

Na mocy Tw. 13, Rozdział 5, wystarczy wykazać, że dla dowolnego $\mathcal{R} \subseteq E(A)$ istnieje $\inf \mathcal{R}$ w zbiorze cz. up. $< E(A), \subseteq>$. Ponieważ $< E(A), \subseteq>$ ma element największy: $A \times A$ (ma też on element najmniejszy: id_A, skoro id_A jest podzbiorem każdej relacji zwrotnej na A), więc na mocy Tw. 10(1), Rozdział 5, $\inf \varnothing = A \times A$, a więc $\inf \varnothing$ istnieje.

Weźmy pod uwagę niepusty zbiór $\mathcal{R}$ relacji równoważnościowych na A. Ponieważ $\bigcap \mathcal{R} \subseteq \theta$ dla każdej $\theta \in \mathcal{R}$, oraz dla dowolnej $\approx \in E(A)$ takiej, że $\forall \theta \in \mathcal{R}, \approx \subseteq \theta$ mamy: $\approx \subseteq \bigcap \mathcal{R}$, więc gdy wykażemy, że $\bigcap \mathcal{R}$ jest relacją równoważności na A, to tym samym wykażemy, że $\bigcap \mathcal{R} = \inf \mathcal{R}$.

Jest oczywiste, że $\bigcap \mathcal{R} \subseteq A \times A$. Aby wykazać, że $\bigcap \mathcal{R}$ jest zwrotna, weźmy $x \in A$. Ponieważ dla dowolnej $\theta \in \mathcal{R}, <x, x> \in \theta$ (bo każda relacja $\theta \in \mathcal{R}$ jest zwrotna), więc $<x, x> \in \bigcap \mathcal{R}$.

Weźmy teraz $x, y \in A$ i załóżmy, że $<x, y> \in \bigcap \mathcal{R}$. Zatem $<x, y> \in \theta$ dla każdej $\theta \in \mathcal{R}$. Lecz każda relacja $\theta \in \mathcal{R}$ jest symetryczna. Zatem dla każdej $\theta \in \mathcal{R}, <y, x> \in \theta$, co oznacza, że $<y, x> \in \bigcap \mathcal{R}$, czyli $\bigcap \mathcal{R}$ jest relacją symetryczną na A.

W celu wykazania przechodniości relacji $\bigcap \mathcal{R}$ załóżmy, że dla jakichś $x, y, z \in A, <x, y>, <y, z> \in \bigcap \mathcal{R}$. Wówczas $\forall \theta \in \mathcal{R}, <x, y>, <y, z> \in \theta$. Ponieważ każda $\theta \in \mathcal{R}$ jest przechodnia, więc $\forall \theta \in \mathcal{R}, <x, z> \in \theta$, czyli $<x, z> \in \bigcap \mathcal{R}$, zatem relacja $\bigcap \mathcal{R}$ jest przechodnia (por. §5, Rozdział 3). □

Uwaga. Istnienie zbioru $E(A)$ gwarantuje aksjomat podzbiorów.

Gdy $A = \varnothing$, krata $<E(A), \subseteq>$ jest jednoelementowa – tym jedynym elementem jest relacja $\varnothing$.

Gdy $A \neq \varnothing$, w ogólności nie jest tak, że dla dowolnego $\mathcal{R} \subseteq E(A), \sup \mathcal{R} = \bigcup \mathcal{R}$. W przypadku $\mathcal{R} = \varnothing$, oczywiście $\sup \mathcal{R} \neq \bigcup \mathcal{R}$, bo $\sup \varnothing = \mathrm{id}_A \neq \varnothing$, skoro id_A jest najmniejszym elementem w $< E(A), \subseteq>$; tymczasem $\bigcup \varnothing = \varnothing$. Lecz również w przypadku $\mathcal{R} \neq \emptyset$, na ogół $\sup \mathcal{R} \neq \bigcup \mathcal{R}$, ponieważ nie dla każdego $\mathcal{R} \subseteq E(A)$, $\bigcup \mathcal{R} \in E(A)$, skoro $\bigcup \mathcal{R}$ na ogół nie jest relacją przechodnią (zob. §5, Rozdział 3).

Jednakże $\bigcup \mathcal{R}$ ($\mathcal{R} \neq \emptyset$) jest relacją zwrotną i symetryczną: dla dowolnego $x \in A, <x,x> \in \theta$ dla jakiejś (nawet każdej) $\theta \in \mathcal{R}$, zatem $<x,x> \in \bigcup \mathcal{R}$, czyli $\bigcup \mathcal{R}$ jest zwrotna; gdy zaś dla $x, y \in A, <x,y> \in \bigcup \mathcal{R}$, to $<x,y> \in \theta$ dla pewnej $\theta \in \mathcal{R}$, zatem wobec symetryczności relacji θ mamy: $<y,x> \in \theta$, stąd $<y,x> \in \bigcup \mathcal{R}$, czyli $\bigcup \mathcal{R}$ jest relacją symetryczną na A.

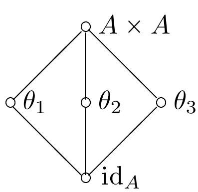
Wobec tego, na mocy Tw. 8, Rozdział 3 oraz Tw. 7(1), Rozdział 3, stwierdzamy, że tranzytywne domknięcie relacji $\bigcup \mathcal{R}$ (gdy $\mathcal{R} \neq \emptyset$) jest relacją równoważnościową, tzn. $(\bigcup \mathcal{R})^- \in E(A)$. Ponadto skoro $\forall \theta \in \mathcal{R},\ \theta \subseteq \bigcup \mathcal{R}$ oraz $\bigcup \mathcal{R} \subseteq (\bigcup \mathcal{R})^-$ (Tw. 7(2), Rozdział 3), więc relacja $(\bigcup \mathcal{R})^-$ jest ograniczeniem górnym zbioru $\mathcal{R}$ w zbiorze częściowo uporządkowanym $<E(A), \subseteq>$. Co więcej, gdy relacja $\approx\, \in E(A)$ jest ograniczeniem górnym zbioru $\mathcal{R}$, a więc gdy $\forall \theta \in \mathcal{R},\ \theta \subseteq\, \approx$, to wówczas (Tw. 11(2), Rozdział 1) $\bigcup \mathcal{R} \subseteq\, \approx$, zatem wobec przechodniości relacji $\approx$, na podstawie Tw. 7(3), Rozdział 3, otrzymujemy: $(\bigcup \mathcal{R})^- \subseteq\, \approx$. Ostatecznie, tranzytywne domknięcie $(\bigcup \mathcal{R})^-$ jest najmniejszym ograniczeniem górnym zbioru $\mathcal{R}$ w $<E(A), \subseteq>$, tzn. $(\bigcup \mathcal{R})^- = \sup \mathcal{R}$ (dla $\mathcal{R} = \emptyset$ równość ta nie zachodzi; tranzytywne domknięcie relacji $\bigcup \emptyset$, a więc tranzytywne domknięcie relacji pustej jest relacją pustą – por. §5, Rozdział 3).

Jak należało oczekiwać, w przypadku, gdy $\bigcup \mathcal{R}$ jest relacją równoważnościową (łatwo sprawdzić, że $\bigcup \mathcal{R} \in E(A)$, gdy $\mathcal{R}$ jest łańcuchem), tzn. w przypadku, gdy $\bigcup \mathcal{R}$ jest relacją przechodnią, $(\bigcup \mathcal{R})^- = \bigcup \mathcal{R}$, zatem wówczas $\bigcup \mathcal{R} = \sup \mathcal{R}$.

Ostatecznie, korzystając z definicji tranzytywnego domknięcia, otrzymujemy jawną postać kresu górnego dowolnego niepustego podzbioru $\mathcal{R}$ w kracie zupełnej $<E(A), \subseteq>$:

dla dowolnych $x, y \in A, <x,y> \in \sup \mathcal{R}$ wtw $<x,y> \in (\bigcup \mathcal{R})^-$ wtw dla pewnego $n \geqslant 2$ istnieją $z_1, z_2, \ldots, z_n \in A$ oraz $\theta_1, \theta_2, , \theta_{n-1} \in \mathcal{R}$ (niekoniecznie różne) takie, że $x = z_1, <z_1, z_2> \in \theta_1, <z_2, z_3> \in \theta_2, \ldots, <z_{n-1}, z_n> \in \theta_{n-1}, z_n = y$.

Przykład. Niech $A = \{a, b, c\}$. Wówczas krata $<E(A), \subseteq>$ ma postać:



gdzie $\theta_1 = \mathrm{id}_A \cup \{<a,b>, <b,a>\}, \theta_2 = \mathrm{id}_A \cup \{<a,c>, <c,a>\}$ oraz $\theta_3 = \mathrm{id}_A \cup \{<b,c>, <c,b>\}$.

§2. Klasa abstrakcji, zbiór ilorazowy, podział zbioru

DEFINICJA. Niech $\approx$ będzie relacją równoważnościową na A. Dla dowolnego $a \in A$, zbiór $[a]_\approx = \{x \in A : a \approx x\}$ nazywamy *klasą abstrakcji elementu* a (bądź *której reprezentantem jest element* a) *względem relacji równoważnościowej* $\approx$. (Podobnie jak w przypadku relacji częściowo porządkujących będziemy pisać: $x \approx y$ zamiast $<x, y> \in \approx$.)

Zbiór $A/\approx = \{[a]_\approx : a \in A\}$ nazywamy *zbiorem ilorazowym zbioru* A *względem relacji* $\approx$.

Relację równoważności $\approx$ określoną na zbiorze A można postrzegać jako stosunek podobieństwa ze względu na własność reprezentowania klasy abstrakcji. Prawdziwe jest bowiem wyrażenie:

dla dowolnych $x, y \in A$, elementy x, y są podobne ze względu na taką własność wtw $x \approx y$.

Albowiem spełnione są równoważności: elementy $x, y \in A$ są podobne ze względu na tak pojmowaną własność wtw mają one tę samą jej wartość wtw reprezentują one tę samą klasę abstrakcji (tzn. $[x]_\approx = [y]_\approx$), co jest równoważne temu (zob. Tw. 3(2)), iż $x \approx y$.

W dalszym ciągu, jeśli na uwadze będziemy mieli jedną ustaloną relację równoważnościową $\approx$, będziemy pisać $[a]$ zamiast $[a]_\approx$.

TWIERDZENIE 3. *Niech $\approx$ będzie dowolną relacją równoważności na zbiorze A. Wówczas dla dowolnych $x, y \in A$,*
(1) $x \in [x]$,
(2) $x \approx y$ *wtw* $[x] = [y]$,
(3) $[x] \cap [y] \neq \varnothing \Rightarrow [x] = [y]$,
(4) $\bigcup(A/\approx) = A$.

DOWÓD. Rozważmy $x, y \in A$.

Dla (1): Ponieważ $\approx$ jest relacją zwrotną, więc $x \approx x$, zatem $x \in [x]$.

Dla (2): ($\Rightarrow$): Załóżmy, że $x \approx y$. ($\subseteq$): Niech $z \in [x]$. Wówczas $x \approx z$. Ponieważ z symetrii relacji $\approx$ mamy: $y \approx x$, więc na mocy przechodniości, $y \approx z$, zatem $z \in [y]$. ($\supseteq$): Na odwrót, niech $z \in [y]$, tzn. $y \approx z$. Wówczas z założenia i z przechodniości, $x \approx z$, czyli $z \in [x]$.

($\Leftarrow$): Załóżmy, że $[x] = [y]$. Na mocy (1), $y \in [y]$, zatem z założenia, $y \in [x]$, czyli $x \approx y$.

Dla (3): Załóżmy, że $[x] \cap [y] \neq \varnothing$. Niech więc $a \in [x] \cap [y]$, tzn. $a \in [x]$ oraz $a \in [y]$. Zatem $x \approx a$ i $y \approx a$. Wówczas z symetrii relacji $\approx$ mamy: $a \approx y$, zatem z przechodniości, $x \approx y$, co na mocy (2) implikuje równość $[x] = [y]$.

Dla (4): Ponieważ dla dowolnego $x \in A, [x] \subseteq A$, więc $\bigcup(A/\approx) \subseteq A$. Aby dowieść odwrotnej inkluzji załóżmy, że $x \in A$. Wówczas na mocy (1), $x \in [x]$, zaś $[x] \in A/\approx$. Zatem $\exists Z(Z \in A/\approx \wedge x \in Z)$, czyli $x \in \bigcup(A/\approx)$. $\square$

Stosunek podobieństwa ze względu na daną własność, jaki zachodzi między obiektami jest ściśle związany z podziałem czy klasyfikacją tych obiektów.

Z jednej strony, mając dany stosunek podobieństwa ze względu na pewną własność, wszystkie te obiekty, które są podobne do siebie, a więc mające tę samą „wartość" własności, „wrzucamy do jednego worka", odróżniając je czy wydzielając od pozostałych. Otrzymujemy tyle różnych „worków", ile jest różnych „wartości" własności, ze względu na którą obiekty są do siebie podobne.

Z drugiej strony, mając dany podział klasy obiektów na rozłączne części („worki"), możemy zdefiniować stosunek podobieństwa między tymi obiektami ze względu na pewną własność: dwa obiekty są do siebie podobne, gdy należą do tej samej części podziału. Zazwyczaj podział obiektów na części opiera się na jakimś kryterium wskazującym pewną własność przysługującą obiektom w różnym stopniu czy natężeniu. Obiekty, którym własność ta przysługuje w tym samym stopniu tworzą część podziału. Tym samym podobieństwo określone przez podział jest podobieństwem ze względu na własność wskazaną w kryterium tego podziału.

Na przykład, biorąc pod uwagę podział wszelkich nauk, dokonany przez K. Ajdukiewicza w [2], na nauki aprioryczne, empiryczne i humanistyczne, możemy określić podobieństwo między dwiema naukami ze względu na status ich ostatecznych przesłanek (zob. [2]). Dwie nauki są do siebie podobne, gdy albo są aprioryczne, albo empiryczne, albo humanistyczne, co ma miejsce dokładnie wtedy, gdy mają one ten sam status ostatecznych przesłanek (kryterium podziału jest tu własność określona jako status ostatecznych przesłanek).

Zarysowany tu związek między podobieństwem a podziałem będzie przedmiotem teoriomnogościowych rozważań w następnym paragrafie. Aby te rozważania umożliwić, dysponując już pojęciem relacji równoważności jako formalnym reprezentantem stosunku podobieństwa, potrzebujemy jeszcze teoriomnogościowego odpowiednika pojęcia podziału.

Definicja. Zbiór Π podzbiorów zbioru A nazywamy *podziałem zbioru A*, gdy
(1) $\forall X \in \Pi, X \neq \varnothing$,
(2) $\forall X, Y \in \Pi \ (X \cap Y \neq \varnothing \Rightarrow X = Y)$,
(3) $\bigcup \Pi = A$.

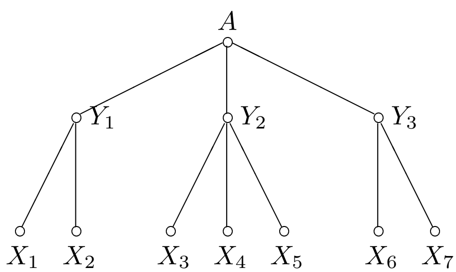
Uwaga. Istnieje dokładnie jeden podział zbioru $\emptyset$. Jest nim zbiór $\Pi = \emptyset$.

Przykład. Zbiory $\{\{a\} : a \in A\}, \{A\}$ są podziałami niepustego zbioru A.

Dowolny zbiór Π taki, że $\forall X \in \Pi, X \neq \emptyset$ oraz $\forall X, Y \in \Pi\ (X \cap Y \neq \emptyset \Rightarrow X = Y)$ jest podziałem zbioru $\bigcup \Pi$.

Definicja. Dla dowolnego zbioru A niech $Part(A)$ będzie zbiorem wszystkich podziałów zbioru A. Niech $\Pi, \mathcal{Q} \in Part(A)$. Mówimy, że podział Π *jest drobniejszy niż* $\mathcal{Q}$ wtw $\forall Y \in \mathcal{Q}\ \exists \mathcal{R} \in Part(Y),\ \mathcal{R} \subseteq \Pi$. (Podział Π jest drobniejszy niż podział $\mathcal{Q}$ wtw dla każdego elementu Y podziału $\mathcal{Q}$ znajdziemy wśród elementów podziału Π takie, że ich zbiór jest podziałem zbioru Y.)

Przykład. Poniższy rysunek przedstawia podziały $\Pi = \{X_1, X_2, \ldots, X_7\}$ oraz $\mathcal{Q} = \{Y_1, Y_2, Y_3\}$ zbioru A takie, że Π jest drobniejszy niż $\mathcal{Q}$. Podzbiory $\{X_1, X_2\}$, $\{X_3, X_4, X_5\}, \{X_6, X_7\}$ podziału Π są podziałami odpowiednio następujących elementów podziału $\mathcal{Q} : Y_1, Y_2, Y_3$.



Lemat. *Dla dowolnych podziałów* $\Pi, \mathcal{Q}$ *zbioru* A, Π *jest drobniejszy niż* $\mathcal{Q}$ *wtw* $\forall X \in \Pi\ \exists Y \in \mathcal{Q},\ X \subseteq Y$.

Dowód. ($\Rightarrow$): Załóżmy że Π jest podziałem drobniejszym niż $\mathcal{Q}$. Niech $X \in \Pi$. Ponieważ $X \neq \emptyset$, więc niech $a \in X$. Skoro $\bigcup \mathcal{Q} = A$ oraz $a \in A$, więc $a \in \bigcup \mathcal{Q}$. Niech zatem $Y \in \mathcal{Q}$ będzie taki, że $a \in Y$. Wykażemy, że $X \subseteq Y$ co skończy dowód tej części lematu. Rozważmy na mocy założenia podział $\mathcal{R}$ zbioru Y taki, że $\mathcal{R} \subseteq \Pi$. Wówczas $\bigcup \mathcal{R} = Y$, zatem $a \in \bigcup \mathcal{R}$. Wobec tego dla pewnego $X_1 \in \mathcal{R} : a \in X_1$. Lecz $X_1 \in \Pi$ (bo $\mathcal{R} \subseteq \Pi$). Mamy więc: $a \in X \cap X_1$, stąd $X \cap X_1 \neq \emptyset$, czyli $X_1 = X$. Ale $X_1 \subseteq \bigcup \mathcal{R}$ (bo $X_1 \in \mathcal{R}$), zatem $X \subseteq \bigcup \mathcal{R}$. Jednakże $\bigcup \mathcal{R} = Y$, więc $X \subseteq Y$.

($\Leftarrow$): Załóżmy, że $\forall X \in \Pi\ \exists Y \in \mathcal{Q},\ X \subseteq Y$. Rozważmy dowolny $Y \in \mathcal{Q}$. Niech $\mathcal{R}_Y = \{X \in \Pi : X \subseteq Y\}$. Jest jasne, że $\mathcal{R}_Y \subseteq \Pi$. Wykażemy, że $\mathcal{R}_Y \in Part(Y)$ co zakończy dowód. Warunki: $\forall X \in \mathcal{R}_Y, X \neq \emptyset$ oraz $\forall X_1, X_2 \in \mathcal{R}_Y (X_1 \cap X_2 \neq \emptyset \Rightarrow X_1 = X_2)$ są oczywiście spełnione, bo $\mathcal{R}_Y \subseteq \Pi$. Wykażemy, że $\bigcup \mathcal{R}_Y = Y$. Inkluzja

($\subseteq$) jest oczywista, bo skoro $\forall X \in \mathcal{R}_Y, X \subseteq Y$, to $\bigcup \mathcal{R}_Y \subseteq Y$. Aby dowieść inkluzji odwrotnej załóżmy, że $a \in Y$. Naturalnie $a \in A$. Ponieważ $\bigcup \Pi = A$, więc $a \in \bigcup \Pi$, czyli dla pewnego $X \in \Pi, a \in X$. Wówczas z założenia niech $Y_0 \in \mathcal{Q}$ będzie taki, że $X \subseteq Y_0$. Wtedy $a \in Y_0$, więc $a \in Y \cap Y_0$, czyli $Y \cap Y_0 \neq \emptyset$. Jednakże $Y, Y_0 \in \mathcal{Q}$. Zatem $Y_0 = Y$. Stąd $X \subseteq Y$. Ponieważ $X \in \Pi$, więc z definicji zbioru $\mathcal{R}_Y$ mamy: $X \in \mathcal{R}_Y$. Ponadto $a \in X$. Ostatecznie, $a \in \bigcup \mathcal{R}_Y$. $\square$

TWIERDZENIE 4. *Relacja $\leqslant$ określona na zbiorze Part(A) wszystkich podziałów zbioru A następująco*: $\Pi \leqslant \mathcal{Q}$ *wtw* $\forall X \in \Pi\ \exists Y \in \mathcal{Q},\ X \subseteq Y$, *jest relacją częściowo porządkującą.* (*Na mocy lematu relacja $\leqslant$ jest relacją bycia drobniejszym.*)

DOWÓD. Niech $\Pi \in Part(A)$. Weźmy $X \in \Pi$. Wówczas oczywiście $X \subseteq X$, zatem $\exists Y \in \Pi, X \subseteq Y$, stąd $\Pi \leqslant \Pi$, tzn. relacja $\leqslant$ jest zwrotna na $Part(A)$.

Aby wykazać, że $\leqslant$ jest antysymetryczna, załóżmy, że dla $\Pi, \mathcal{Q} \in Part(A)$, $\Pi \leqslant \mathcal{Q}$ oraz $\mathcal{Q} \leqslant \Pi$. Wykazujemy równość $\Pi = \mathcal{Q}$.

($\subseteq$): Niech $Z \in \Pi$. Ponieważ $\Pi \leqslant \mathcal{Q}$, więc $Z \subseteq Y$ dla pewnego $Y \in \mathcal{Q}$. Skoro $Y \in \mathcal{Q}$ oraz $\mathcal{Q} \leqslant \Pi$, to $Y \subseteq X$ dla pewnego $X \in \Pi$. Skoro $Z \subseteq Y$ oraz $Y \subseteq X$, więc $Z \subseteq X$, czyli $Z \cap X = Z$. Na mocy warunku (1) definicji podziału, $Z \neq \emptyset$, czyli $Z \cap X \neq \emptyset$. Ponadto $Z, X \in \Pi$, zatem na mocy warunku (2) definicji podziału mamy: $Z = X$. A więc nie tylko $Z \subseteq Y$, lecz również $Y \subseteq Z$ (bo $Y \subseteq X$). Stąd $Z = Y$. Lecz $Y \in \mathcal{Q}$, zatem $Z \in \mathcal{Q}$.

Inkluzję ($\supseteq$) dowodzimy analogicznie.

Aby wykazać, że relacja $\leqslant$ jest przechodnia na $Part(A)$ załóżmy, że dla $\Pi, \mathcal{Q}, \mathcal{R} \in Part(A)$, $\Pi \leqslant \mathcal{Q}$ oraz $\mathcal{Q} \leqslant \mathcal{R}$. Mamy wykazać, że $\Pi \leqslant \mathcal{R}$.

Weźmy więc $X \in \Pi$. Ponieważ $\Pi \leqslant \mathcal{Q}$, więc $X \subseteq Y$ dla pewnego $Y \in \mathcal{Q}$. Skoro jednak $\mathcal{Q} \leqslant \mathcal{R}$, więc $Y \subseteq Z$ dla pewnego $Z \in \mathcal{R}$. Ostatecznie $X \subseteq Z$ oraz $Z \in \mathcal{R}$, czyli $\Pi \leqslant \mathcal{R}$. $\square$

§3. Relacje równoważności a podziały

W niniejszym paragrafie uzasadnimy intuicyjnie oczywisty fakt, iż z praktycznego puntu widzenia pojęcia podziału oraz relacji równoważności mogą być utożsamione.

Dowolna relacja równoważności określona na danym zbiorze wyznacza podział tego zbioru jak następuje:

TWIERDZENIE 5 (ZASADA ABSTRAKCJI). *Dla dowolnej relacji równoważności $\approx$ na zbiorze A, zbiór ilorazowy $A/\approx$ jest podziałem zbioru A.*

DOWÓD. Warunek (1) definicji podziału zachodzi dla $A/\approx$ na mocy Tw. 3(1), warunek (2) na podstawie Tw. 3(3) oraz warunek (3) – na mocy Tw. 3(4). $\square$

Uwaga. Tw. 5 jest prawdziwe dla $A = \varnothing$. Wówczas bowiem $\approx \; = \varnothing$ oraz $A/\!\approx \; = \varnothing$ jest podziałem zbioru $\varnothing$.

Dowolny podział zbioru wyznacza relację równoważności na tym zbiorze:

TWIERDZENIE 6. *Dla dowolnego podziału* Π *zbioru* A *relacja binarna* $\approx_\Pi$ *określona na* A *następująco*: $x \approx_\Pi y$ *wtw* $\exists Y \in \Pi \; (x \in Y \wedge y \in Y)$, *jest relacją równoważności.*

DOWÓD. Niech Π będzie podziałem zbioru A. Weźmy $x \in A$. Z warunku (3) definicji podziału mamy: $x \in \bigcup \Pi$. Niech więc $Y \in \Pi$ będzie taki, że $x \in Y$. Stąd $x \approx_\Pi x$, czyli $\approx_\Pi$ jest zwrotna.

Aby wykazać symetrię relacji $\approx_\Pi$ załóżmy, że $x \approx_\Pi y$. Czyli dla pewnego $Y \in \Pi$, $x, y \in Y$. Wobec tego $y \approx_\Pi x$.

Załóżmy, że $x \approx_\Pi y$ oraz $y \approx_\Pi z$. Wówczas $x, y \in Y_1$ oraz $y, z \in Y_2$ dla pewnych $Y_1, Y_2 \in \Pi$. Jak widać $Y_1 \cap Y_2 \neq \varnothing$ (bo $y \in Y_1 \cap Y_2$). Zatem z warunku (2) definicji podziału mamy: $Y_1 = Y_2$. Stąd $x, z \in Y_1$ i konsekwentnie $x \approx_\Pi z$, co dowodzi, że $\approx_\Pi$ jest przechodnia. $\square$

Uwaga. Tw. 6 jest prawdziwe, gdy $A = \varnothing$. Wówczas jedyny podział Π zbioru A jest zbiorem pustym i wyznacza on relację $\approx_\Pi \; = \varnothing$.

Dowolna relacja równoważności na danym zbiorze jest relacją wyznaczoną przez wyznaczony przez siebie podział:

TWIERDZENIE 7. *Dla dowolnej relacji równoważności* $\approx$ *na* A, $\approx \; = \; \approx_{A/\approx}$.

DOWÓD. Dla dowolnych $a, b \in A$, $a \approx_{A/\approx} b$ wtw dla pewnego $x \in A$, $a \in [x]$ oraz $b \in [x]$ co jest równoważne temu, że $a \approx b$. Jeśli bowiem $a, b \in [x]$, to $x \approx a$ i $x \approx b$, zatem z symetrii i przechodniości relacji $\approx$ otrzymujemy: $a \approx b$. Na odwrót, gdy $a \approx b$, to $b \in [a]$ oraz na mocy Tw. 3(1), $a \in [a]$. Zatem istnieje $x \in A$ taki, że $b \in [x]$ oraz $a \in [x]$. $\square$

Dowolny podział danego zbioru jest podziałem wyznaczonym przez wyznaczoną przez siebie relację równoważności:

TWIERDZENIE 8. *Dla dowolnego podziału* Π *zbioru* A, $\Pi = A/\!\approx_\Pi$.

DOWÓD. Niech $Y \in \Pi$. Wykażemy najpierw:
(*) dla dowolnego $a \in Y$, $Y = [a]_{\approx_\Pi}$.

Weźmy $a \in Y$. $(\subseteq)$: Niech $x \in Y$. Wówczas z definicji relacji $\approx_\Pi$ skoro $a \in Y$ mamy: $a \approx_\Pi x$, zatem $x \in [a]_{\approx_\Pi}$.

($\supseteq$): Niech $x \in [a]_{\approx_\Pi}$. Wówczas $a \approx_\Pi x$, czyli dla pewnego $Z \in \Pi$, $x, a \in Z$. Lecz $a \in Y$, czyli $Y \cap Z \neq \varnothing$, stąd na mocy warunku (2) definicji podziału, $Z = Y$. Lecz $x \in Z$, zatem $x \in Y$.

Inkluzja $\Pi \subseteq A/{\approx_\Pi}$ wynika bezpośrednio z (*) oraz warunku (1) definicji podziału. Aby dowieść inkluzji odwrotnej, rozważmy $a \in A$. Ponieważ Π jest podziałem zbioru A, więc na mocy warunku (3) definicji podziału, $a \in Y$ dla pewnego $Y \in \Pi$. Wówczas jednak na mocy (*), $Y = [a]_{\approx_\Pi}$, co oznacza, że $[a]_{\approx_\Pi} \in \Pi$. □

TWIERDZENIE 9. *Dla dowolnego zbioru A, zbiory częściowo uporządkowane $<E(A), \subseteq>$ oraz $<Part(A), \leqslant>$ są izomorficzne.*

DOWÓD. Zauważmy najpierw, że w przypadku $A = \varnothing$, $E(A) = \{\varnothing\}$ oraz $Part(\mathrm{A}) = \{\varnothing\}$, zatem $<E(A), \subseteq>$, $< Part(\mathrm{A}), \leqslant>$ są izomorficzne.

Niech $A \neq \varnothing$. Pokażemy, że funkcja $\phi : E(A) \longrightarrow Part(A)$ określona następująco: $\phi(\approx) = A/{\approx}$, jest żądanym izomorfizmem. Rozważmy funkcję ψ: $Part(A) \longrightarrow E(A)$ określoną następująco: $\psi(\Pi) = {\approx_\Pi}$. Wtedy $(\phi \circ \psi)(\approx) = \psi(\phi(\approx)) = \psi(A/{\approx}) = {\approx_{A/\approx}} = {\approx}$ na mocy Tw. 7, oraz $(\psi \circ \phi)(\Pi) = \phi(\psi(\Pi)) = \phi(\approx_\Pi) = A/{\approx_\Pi} = \Pi$ na mocy Tw. 8. Zatem $\phi \circ \psi = \mathrm{id}_{E(A)}$ oraz $\psi \circ \phi = \mathrm{id}_{Part(A)}$. Stąd, na mocy Tw. 7, Rozdział 4, wnosimy, że ϕ jest bijekcją.

Teraz wykazujemy warunek (ISO): dla dowolnych $\approx, \simeq \in E(A)$, ${\approx} \subseteq {\simeq}$ wtw $\phi(\approx) \leqslant \phi(\simeq)$.

($\Rightarrow$): Załóżmy, że ${\approx} \subseteq {\simeq}$. Musimy wykazać, że $A/{\approx} \leqslant A/{\simeq}$. Niech zatem $X \in A/{\approx}$. Wówczas $X = [a]_\approx$ dla pewnego $a \in A$. Lecz $[a]_\approx \subseteq [a]_\simeq$, na mocy założenia (jeśli bowiem $x \in [a]_\approx$, tzn. $a \approx x$, to ponieważ ${\approx} \subseteq {\simeq}$, więc $a \simeq x$, czyli $x \in [a]_\simeq$). Zatem $X \subseteq [a]_\simeq$. Lecz $[a]_\simeq \in A/{\simeq}$. Ostatecznie, $A/{\approx} \leqslant A/{\simeq}$.

($\Leftarrow$): Załóżmy, że $\phi(\approx) \leqslant \phi(\simeq)$, tzn. $A/{\approx} \leqslant A/{\simeq}$. Aby wykazać inkluzję ${\approx} \subseteq {\simeq}$, załóżmy, że $a \approx b$. Wówczas $b \in [a]_\approx$. Skoro $[a]_\approx \in A/{\approx}$, więc z założenia, $[a]_\approx \subseteq X$ dla pewnego $X \in A/{\simeq}$. Naturalnie $X = [x]_\simeq$ dla pewnego $x \in A$. Mamy więc: $[a]_\approx \subseteq [x]_\simeq$. Zatem $b \in [x]_\simeq$ (bo $b \in [a]_\approx$) oraz $a \in [x]_\simeq$ (bo $a \in [a]_\approx$). Dlatego $x \simeq b$ oraz $x \simeq a$, skąd na mocy symetrii i przechodniości relacji $\simeq$ otrzymujemy: $a \simeq b$. Ostatecznie ${\approx} \subseteq {\simeq}$. □

Uwaga. Elementy najmniejszy i największy w $< E(A), \subseteq>$ to odpowiednio, $\mathrm{id}_A, A \times A$. Elementy najmniejszy i największy w $<Part(\mathrm{A}), \leqslant>$ to $\phi(\mathrm{id}_A) = \{\{a\} : a \in A\}$ oraz $\phi(A \times A) = \{A\}$, gdzie ϕ jest izomorfizmem zdefiniowanym w dowodzie Tw. 9.

TWIERDZENIE 10. *Dla dowolnego zbioru A zbiór cz. up. $<Part(A), \leqslant>$ jest kratą zupełną.*

Dowód. Ponieważ $< E(A), \subseteq>$ jest kratą zupełną (Tw. 2) oraz $< E(A), \subseteq>$ i $< Part(A), \leqslant>$ są izomorficzne (Tw. 9), więc na mocy Tw. 18, Rozdział 5, $< Part(A), \leqslant>$ jest kratą zupełną. $\square$

Przykład. Kratę zupełną $< Part(\{a,b,c\}), \leqslant>$ wszystkich podziałów zbioru $\{a,b,c\}$ można zilustrować analogicznym diagramem jak powyżej w przykładzie diagramu kraty $< E(\{a,b,c\}), \subseteq>$. Tutaj $\{a,b,c\}/\theta_1 = \{\{a,b\},\{c\}\}$; $\{a,b,c\}/\theta_2 = \{\{a,c\},\{b\}\}$ oraz $\{a,b,c\}/\theta_3 = \{\{b,c\},\{a\}\}$.

§4. Relacje równoważności a funkcje

Dowolna funkcja wyznacza na swojej dziedzinie relację równoważności oraz dowolna relacja równoważności wyznacza funkcję o dziedzinie będącej zbiorem, na którym ta relacja jest określona, jak następuje:

Twierdzenie 11. *Dla dowolnej funkcji $f : A \longrightarrow B$ relacja binarna $\simeq_f$ określona na A następująco: dla dowolnych $x, y \in A$, $x \simeq_f y$ wtw $f(x) = f(y)$, jest relacją równoważności.*

Dla dowolnej relacji równoważności $\approx$ na zbiorze A, funkcja $k_\approx : A \longrightarrow A/\approx$ taka, że dla każdego $x \in A$, $k_\approx(x) = [x]_\approx$ jest „na”.

Dowód. Niech $f \in B^A$. Łatwo sprawdzić, że relacja $\simeq_f$ jest równoważnościowa na zbiorze A.

Jest oczywiste, że dla dowolnej relacji równoważności $\approx$ na A, dla dowolnego elementu ze zbioru ilorazowego $A/\approx$, czyli dla dowolnej klasy abstrakcji można wybrać jej reprezentanta i wówczas ta klasa abstrakcji jest wartością funkcji $k_\approx$ na tym reprezentancie, czyli $k_\approx$ jest „*na*”. $\square$

Łatwo zauważyć, że każda relacja równoważności $\approx$ określona na zbiorze A jest relacją postaci: $\simeq_f$, tzn. jest wyznaczona, w myśl Tw. 11, przez pewną funkcję, mianowicie $\approx\, = \,\simeq_{k_\approx}$. Albowiem dla dowolnych $a, b \in A$, $a \simeq_{k_\approx} b$ wtw $k_\approx(a) = k_\approx(b)$ wtw $[a]_\approx = [b]_\approx$ wtw $a \approx b$, na mocy Tw. 3(2).

Naturalnie nie każda funkcja $f: A \longrightarrow B$ jest wyznaczona w analogicznym sensie przez relację równoważności, mianowicie nie jest w ogólności tak, że $f = k_\approx$ dla pewnej relacji równoważności $\approx$ określonej na A. Jest przecież jasne, że przeciwdziedziną funkcji $k_\approx$ jest zbiór ilorazowy $A/\approx$, tymczasem przeciwdziedziną funkcji f jest podzbiór zbioru B, który może być zadany niezależnie od zbioru A.

Jednakże w innym, bliskim poprzedniego sensie, każda funkcja $f : A \longrightarrow B$ jest wyznaczona przez pewną relację równoważności na zbiorze A, mianowicie przez relację $\simeq_f$. Otóż, można łatwo znaleźć jedno-jednoznaczną odpowiedniość między elementami przeciwdziedziny funkcji $k_{\simeq_f}$ (czyli zbiorem ilorazowym $A/\simeq_f$) a elementami przeciwdziedziny funkcji f (tzn. obrazem $\overrightarrow{f}(A)$), pozwalającą „utożsamić” obie przeciwdziedziny. Precyzyjniej zaś, mając ową jedno-jednoznaczną odpowiedniość w postaci funkcji $g : A/{\simeq_f} \longrightarrow B$, można funkcję f przedstawić jako złożenie $k_{\simeq_f} \circ g$. Innymi słowy, dowolna funkcja $f : A \longrightarrow B$ jest wyznaczona przez relację równoważności $\simeq_f$ w następujący sposób: istnieje funkcja różnowartościowa $g : A/{\simeq_f} \longrightarrow B$ taka, że $f = k_{\simeq_f} \circ g$:

Twierdzenie 12. *Dla dowolnej funkcji $f : A \longrightarrow B$ przekształcającej zbiór A na zbiór B, funkcja $g : A/{\simeq_f} \longrightarrow B$ określona następująco: dla dowolnego $x \in A, g([x]) = f(x)$, jest bijekcją oraz $k_{\simeq_f} \circ g = f$:*

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "k_{\simeq_f}"'] & & B \\ & A/{\simeq_f} \arrow[ur, "g"'] & \end{tikzcd}$$

Dowód. Najpierw wykażmy, że g jest dobrze określona, tzn., że jej wartość na danej klasie abstrakcji nie zależy od wyboru reprezentanta tej klasy abstrakcji. Niech więc $[x] = [y]$ dla jakichś $x, y \in A$. Wówczas, na mocy Tw. 3(2), $x \simeq_f y$, zatem z definicji relacji $\simeq_f$, $f(x) = f(y)$, stąd $g([x]) = g([y])$.

Aby wykazać, że g jest 1-1 załóżmy, że $g([x]) = g([y])$. Wówczas z określenia funkcji g mamy: $f(x) = f(y)$, zatem $x \simeq_f y$, stąd $[x] = [y]$. Aby wykazać, że g jest „*na*”, rozważmy dowolny $b \in B$. Ponieważ z założenia funkcja f jest „*na*”, niech więc $a \in A$ będzie taki, że $b = f(a)$. Lecz $g([a]) = f(a)$. Zatem $b = g([a])$ i $[a] \in A/{\simeq_f}$, czyli g jest „*na*”. Ostatecznie g jest bijekcją.

Ponadto dla dowolnego $x \in A$, $(k_{\simeq_f} \circ g)(x) = g(k_{\simeq_f}(x)) = g([x]) = f(x)$, co dowodzi, że $k_{\simeq_f} \circ g = f$. $\square$

Z dowodu Tw. 12 wynika, że można je sformułować w wersji ogólniejszej – rozważając dowolną funkcję $f : A \longrightarrow B$, niekoniecznie „*na*”. Wówczas w twierdzeniu będzie mowa nie o bijekcji $g : A/{\simeq_f} \longrightarrow B$, lecz o funkcji 1-1. Pozostałe wyrażenia twierdzenia nie ulegną zmianie.

Jasne jest, że taka funkcja g ustala ową jedno-jednoznaczną odpowiedniość między przeciwdziedzinami funkcji $k_{\simeq_f}$ oraz f, przy czym $f = k_{\simeq_f} \circ g$.

Zakończymy niniejszy rozdział użytecznym w logice formalnej twierdzeniem:

Twierdzenie 13. *Dla dowolnej relacji zwrotnej i przechodniej R na zbiorze A, $R \cap R^{\smile}$ jest relacją równoważności na A.*

Relacja $\leqslant$ określona na zbiorze ilorazowym $A/(R \cap R^{\smile})$ następująco: dla dowolnych $x, y \in A$, $[x] \leqslant [y]$ wtw $<x, y> \in R$ jest relacją częściowo porządkującą.

DOWÓD. Niech R będzie zwrotna oraz przechodnia na A. Wówczas dla dowolnego $x \in A$: $<x, x> \in R$ oraz $<x, x> \in R^{\sim}$, zatem $R \cap R^{\sim}$ jest zwrotna. Załóżmy, że $<x, y>, <y, z> \in R \cap R^{\sim}$ dla jakichś $x, y, z \in A$. Wówczas $<x, y>, <y, z> \in R$ oraz $<y, x>, <z, y> \in R$. Zatem z przechodniości relacji R mamy: $<x, z> \in R$ oraz $<z, x> \in R$, czyli $<x, z> \in R^{\sim}$ i ostatecznie $<x, z> \in R \cap R^{\sim}$, co oznacza, że $R \cap R^{\sim}$ jest przechodnia. W celu wykazania symetrii, załóżmy, że $<x, y> \in R \cap R^{\sim}$. Wówczas $<x, y> \in R$ oraz $<x, y> \in R^{\sim}$, zatem $<y, x> \in R$ oraz $<y, x> \in R^{\sim}$. Ostatecznie, $<y, x> \in R \cap R^{\sim}$, tzn. $R \cap R^{\sim}$ jest symetryczna.

Aby dowieść drugiej części twierdzenia, najpierw wykażmy, że relacja $\leqslant$ jest dobrze określona na zbiorze ilorazowym $A/(R \cap R^{\sim})$, tzn. nie zależy od wyboru reprezentantów klas abstrakcji. Niech więc $[x] = [a]$ oraz $[y] = [b]$ dla pewnych $a, b \in A$. Wykażemy, że na mocy definicji relacji $\leqslant$ zachodzi: $[x] \leqslant [y]$ wtw $[a] \leqslant [b]$. Załóżmy więc, że $[x] \leqslant [y]$. Wówczas z definicji relacji $\leqslant$, $<x, y> \in R$. Ponieważ z założenia, $[x] = [a]$, więc (Tw. 3(2)) $<x, a> \in R \cap R^{\sim}$, skąd $<x, a> \in R^{\sim}$, czyli $<a, x> \in R$. Z przechodniości relacji R, $<a, y> \in R$. Jednakże również $[y] = [b]$, czyli $<y, b> \in R \cap R^{\sim}$. Stąd $<y, b> \in R$. Zatem z przechodniości R otrzymujemy: $<a, b> \in R$, czyli $[a] \leqslant [b]$. Odwrotną implikację dowodzimy analogicznie.

Rozważmy dowolny element $[x] \in A/(R \cap R^{\sim})$. Wówczas $[x] \leqslant [x]$ skoro $<x, x> \in R$ wobec zwrotności relacji R. Zatem relacja $\leqslant$ jest zwrotna. Załóżmy, że $[x] \leqslant [y]$ oraz $[y] \leqslant [x]$. Wówczas $<x, y> \in R$ oraz $<y, x> \in R$, czyli $<x, y> \in R^{\sim}$, zatem $<x, y> \in R \cap R^{\sim}$, a stąd $[x] = [y]$ (Tw. 3(2)), co dowodzi antysymetrii relacji $\leqslant$. W celu wykazania przechodniości relacji $\leqslant$ załóżmy, że $[x] \leqslant [y]$ oraz $[y] \leqslant [z]$. Wówczas $<x, y> \in R$ oraz $<y, z> \in R$, zatem z przechodniości R, $<x, z> \in R$, co daje $[x] \leqslant [z]$. $\square$

Rozdział 7. Liczby naturalne

§1. Arytmetyka elementarna

Arytmetyka elementarna jest najprostszą z teorii liczb naturalnych. Ujmuje ona liczby naturalne bez uwzględnienia działań dodawania i mnożenia.

Arytmetyka elementarna jest teorią I rzędu zdefiniowaną aksjomatycznie w języku z jedną pierwotną stałą indywidualną „0” reprezentującą liczbę zero oraz jednym pierwotnym 1-argumentowym symbolem funkcyjnym „s”, reprezentującym tzw. operację następnika (której wartością na danej liczbie naturalnej jest liczba następna po niej tzn. o jeden większa, zwana właśnie następnikiem danej liczby).

Aksjomaty:

(AN1) $\forall x(s(x) \neq 0)$,

Liczba zero nie jest następnikiem żadnej liczby naturalnej.

(AN2) $\forall x \forall y(s(x) = s(y) \Rightarrow x = y)$,

Dowolne dwie liczby naturalne są identyczne, jeśli ich następniki są identyczne.

(Aksjomat indukcji) $[\psi(0) \wedge \forall x(\psi(x) \Rightarrow \psi(s(x)))] \Rightarrow \forall x(\psi(x))$,

gdzie $\psi(x)$ jest formułą języka, w której x jest przynajmniej jedną zmienną wolną, zaś $\psi(0)$ oraz $\psi(s(x))$ są formułami uzyskanymi z $\psi(x)$ przez zastąpienie każdego wolnego występowania zmiennej x w $\psi(x)$ odpowiednio termami: 0 oraz $s(x)$.

Każda liczba naturalna x spełnia formułę $\psi(x)$, o ile liczba 0 ją spełnia oraz jest tak, że następnik dowolnej liczby spełnia $\psi(x)$, ilekroć ta liczba ją spełnia.

Aksjomat indukcji, podobnie jak niektóre aksjomaty teorii ZFC czy też pewnik Cantora, jest schematem dla aksjomatów, z którego uzyskujemy właściwy aksjomat (formułę języka), wstawiając w miejsce $\psi(x)$ konkretną formułę języka teorii.

Praktycznie wyprowadzamy przy użyciu aksjomatu indukcji wszystkie twierdzenia arytmetyki elementarnej o postaci: $\forall x(\psi(x))$, a więc stwierdzające przysługiwanie pewnych własności wszystkim liczbom naturalnym. Mówimy wówczas, że dowody takich twierdzeń są indukcyjne.

Aby dowieść indukcyjnie twierdzenia postaci $\forall x(\psi(x))$, wykazujemy prawdziwość poprzednika w aksjomacie indukcji dla tej konkretnej postaci formuły $\psi(x)$. Twierdzenie $\forall x(\psi(x))$ otrzymujemy jako następnik w tym aksjomacie. Ponieważ ów poprzednik jest koniunkcją, wykazujemy więc każdy z jej członów:

(1) $\psi(0)$ (tzw. zerowy krok indukcyjny),

(2) $\forall x(\psi(x) \Rightarrow \psi(s(x))$.

Aby dowieść (2), wybieramy dowolne x oraz zakładamy, że $\psi(x)$ (tzw. założenie indukcyjne). Następnie dążymy do wykazania: $\psi(s(x))$ (tzw. teza indukcyjna).

Wyprowadzimy, przy użyciu aksjomatu indukcji, dwa twierdzenia. Pierwsze mówi, że następnik dowolnej liczby naturalnej jest od niej różny. Drugie, że jakakolwiek liczba naturalna różna od zera jest następnikiem jakiejś liczby.

tw. 1. $\forall x(s(x) \neq x)$.

DOWÓD. Jako $\psi(x)$ kładziemy w aksjomacie indukcji formułę: $s(x) \neq x$. Zastosowanie tego aksjomatu w tym dowodzie będzie możliwe po wykazaniu prawdziwości dwóch wyrażeń, których koniunkcja jest poprzednikiem aksjomatu indukcji zapisanego dla owej konkretnej formuły $\psi(x)$. Dowodzimy zatem:
(1) $s(0) \neq 0$ (zerowy krok indukcyjny) oraz
(2) $\forall x(s(x) \neq x \Rightarrow s(s(x)) \neq s(x))$.

Naturalnie (1) jest bezpośrednim wnioskiem z (AN1). Aby wykazać (2), załóżmy, że $s(x) \neq x$ (założenie indukcyjne) dla dowolnie wybranego x. Musimy wykazać tezę indukcyjną postaci $s(s(x)) \neq s(x)$. Załóżmy nie wprost, że $s(s(x)) = s(x)$. Wówczas na mocy (AN2), $s(x) = x$. Sprzeczność z założeniem indukcyjnym. $\square$

tw. 2. $\forall x(x = 0 \vee \exists y(x = s(y)))$.

DOWÓD. Krok zerowy: $0 = 0 \vee \exists y(0 = s(y))$, jest oczywiście spełniony.

Założenie indukcyjne: $x = 0 \vee \exists y(x = s(y))$, dla dowolnie wybranego, ustalonego x. Dowodzimy tezy indukcyjnej postaci: $s(x) = 0 \vee \exists y(s(x) = s(y))$.

Niech założenie indukcyjne będzie prawdziwe w ten sposób, że $x = 0$. Wówczas $s(x) = s(0)$, więc $\exists y(s(x) = s(y))$. Zatem $s(x) = 0 \vee \exists y(s(x) = s(y))$. Niech założenie indukcyjne będzie prawdziwe w ten sposób, że $\exists y(x = s(y))$. Wówczas dla pewnego a, $x = s(a)$ i konsekwentnie $s(x) = s(s(a))$, stąd $\exists y(s(x) = s(y))$, a więc $s(x) = 0 \vee \exists y(s(x) = s(y))$. $\square$

W ogólności dla dowolnego zbioru formuł domkniętych A danego języka I rzędu $\mathcal{L}$, każdą interpretację dla tego języka, w której wszystkie formuły z A są prawdziwe, nazywamy *modelem dla zbioru formuł* A. Łatwo stwierdzić (porównaj dalej tw. 5, §3), że dowolny model dla zbioru aksjomatów danej teorii jest modelem dla tej teorii. Teoria, której zbiorem aksjomatów jest A, jest bowiem zbiorem wszystkich zdań (formuł domkniętych) języka, które wynikają ze zbioru A, tzn. są prawdziwe w każdej interpretacji, w której prawdziwe są wszystkie zdania ze zbioru A.

Nietrudno zauważyć, że wszystkie obiekty nazywane termami: $0, s(0), s(s(0))$, $s(s(s(0))), \ldots$ (traktowane jako różne od siebie) i tylko one są elementami dziedziny modelu dla arytmetyki elementarnej. W dziedzinie tej występuje obiekt 0, który nie jest wartością operacji s na żadnym innym obiekcie – prawdziwy jest więc w tejże dziedzinie aksjomat AN1 – oraz każdy z obiektów różnych od 0 jest wartością iluśkrotnego złożenia operacji s na obiekcie 0, przy czym różnokrotne złożenia operacji s na 0 dają różne obiekty. Stąd wynika prawdziwość aksjomatu AN2. Aby lepiej zdać sobie z tego sprawę, rozpatrzmy obiekty dziedziny w kolejności, w jakiej zostały wyżej zapisane, tzn. w kolejności wzrastania krotności złożenia operacji s (obiekt $s(x)$ występuje bezpośrednio za obiektem x). Gdy dwa obiekty x, y są różne od siebie, to jeden z nich, powiedzmy x, występuje w owej sekwencji na prawo od drugiego – y (tzn. jest on wartością złożenia s o większej krotności, niż krotność złożenia, której wartością jest obiekt y, w szczególności y może w ogóle nie być wartością owego złożenia, tzn. może być 0). Ponieważ $s(x), s(y)$ występują w sekwencji bezpośrednio na prawo od odpowiednio x oraz y, więc obiekt $s(x)$ jest „równie odległy na prawo" od $s(y)$, jak x jest „odległy" od y. W konsekwencji $s(x) \neq s(y)$.

Pozostaje wykazanie prawdziwości aksjomatu indukcji. Niech więc $\psi(x)$ będzie formułą języka arytmetyki elementarnej. Załóżmy, że w rozważanej dziedzinie prawdziwy jest poprzednik aksjomatu indukcji dla tejże $\psi(x)$. Zatem obiekt 0 spełnia formułę $\psi(x)$ oraz prawdą jest, że jakikolwiek obiekt dziedziny spełnia $\psi(x)$, o ile obiekt bezpośrednio go poprzedzający w powyższej sekwencji, spełnia tę formułę. Zastosujmy ostatnią obserwację kolejno do każdego obiektu z sekwencji. Skoro 0 spełnia $\psi(x)$, a bezpośrednio poprzedza obiekt $s(0)$, więc $s(0)$ spełnia $\psi(x)$; skoro $s(0)$ spełnia $\psi(x)$, a bezpośrednio poprzedza $s(s(0))$, więc $s(s(0))$ spełnia $\psi(x)$, skoro … itd. Wniosek: każdy z obiektów z sekwencji spełnia $\psi(x)$.

Opisany model arytmetyki elementarnej liczb naturalnych nosi nazwę *standardowego* (w kwestii niestandardowych modeli zob. np. [9]).

Stosowane zwyczajowo nazewnictwo obiektów z dziedziny standardowego modelu ma oczywiście postać: $1 =_{def} s(0),\ 2 =_{def} s(s(0)),\ 3 =_{def} s(s(s(0)))$ itd.

§2. Arytmetyka liczb naturalnych z dodawaniem i mnożeniem

Arytmetyka liczb naturalnych z dodawaniem jest teorią I rzędu określoną aksjomatycznie na języku arytmetyki elementarnej rozszerzonym o 2-argumentowy symbol funkcyjny „+", interpretowany w modelu standardowym arytmetyki elementarnej jako operacja „zwykłego" dodawania.

Oprócz aksjomatów arytmetyki elementarnej (AN1), (AN2), (Aksjomat indukcji) występują tu dwa aksjomaty, nadające znaczenie symbolowi „+” :

(AN3) $\forall y(0 + y = y)$,

(AN4) $\forall x \forall y(s(x) + y = s(x + y))$.

Aksjomaty te określają wartość operacji dodawania na dowolnych liczbach naturalnych (tzn. obiektach modelu standardowego) w sposób następujący: w myśl tw. 2, §1, każda liczba naturalna jest bądź liczbą 0, bądź następnikiem jakiejś liczby naturalnej; (AN3) ustala wartość operacji dodawania dla ciągu $(0, y)$, gdzie y jest dowolną liczbą naturalną, zaś (AN4) określa wartość tej operacji w pozostałych przypadkach, a więc wówczas, gdy pierwszym argumentem operacji dodawania jest jakakolwiek liczna naturalna różna od 0 (liczba $s(x)$) oraz drugim dowolna liczba naturalna y. Aby w myśl (AN4) obliczyć wartość operacji dodawania na ciągu $(s(x), y)$, trzeba wcześniej znać wartość tej operacji na ciągu (x, y). Aby ją z kolei obliczyć, bierzemy pod uwagę (AN3), gdy $x = 0$, co zakończy obliczenie, albo znowu (AN4), gdy $x \neq 0$, a więc $x = s(z)$ dla pewnej liczby naturalnej z. Wówczas jednak należy znać wartość operacji dodawania na ciągu (z, y), a więc znowu korzystamy z (AN3), gdy $z = 0$ (obliczenie skończone), bądź z (AN4), gdy $z \neq 0$ itd. aż do chwili, gdy pierwszy argument operacji będzie liczbą 0, zatem do obliczeń zastosujemy (AN3). Przykładowo:

$2+3 =_{wg\ def}\ s(s(0))+s(s(s(0))) =_{wg\ (AN4)} s(s(0)+s(s(s(0)))) =_{wg\ (AN4)}\ s(s(0+s(s(s(0))))) =_{wg\ (AN3)} s(s(s(s(s(0))))) =_{wg\ def}\ 5$.

Naturalnie wszystkie twierdzenia arytmetyki elementarnej są twierdzeniami arytmetyki z dodawaniem, choć nie na odwrót. Arytmetyka z dodawaniem jest „bogatszą” teorią, zaś dowodzenie jej twierdzeń opisujących operację dodawania jest trudniejsze niż dowodzenie twierdzeń w arytmetyce elementarnej. Przykładowo wykażemy, że dodawanie jest operacją przemienną:

tw. 3. $\forall x \forall y(x + y = y + x)$.

DOWÓD. Połóżmy $\phi(x) := \forall y(x + y = y + x)$. Wówczas dowodzone twierdzenie jest następnikiem aksjomatu indukcji, którego poprzednik ma postać:
(1) $\forall y(0 + y = y + 0) \wedge \forall x[\forall y(x + y = y + x) \Rightarrow \forall y(s(x) + y = y + s(x))]$.

Aby wykazać (1) najpierw indukcyjnie dowodzimy
(2) $\forall y(0 + y = y + 0)$, tzn. $\phi(0)$.

Połóżmy więc $\psi(y) := 0 + y = y + 0$. Wówczas (2) jest następnikiem aksjomatu indukcji, którego poprzednikiem jest
(3) $0 + 0 = 0 + 0 \wedge \forall y(0 + y = y + 0 \Rightarrow 0 + s(y) = s(y) + 0)$.

Naturalnie pierwszy człon koniunkcji (3) (formuła $\psi(0)$) jest spełniony. Aby wykazać prawdziwość drugiego członu, tzn. formuły: $\forall y(\psi(y) \Rightarrow \psi(s(y)))$, weźmy dowolną liczbę y i załóżmy, że $0 + y = y + 0$. Na mocy (AN3) mamy wówczas: $y = y + 0$, zatem $s(y) = s(y + 0)$. Stąd na mocy (AN4), $s(y) = s(y) + 0$. Lecz z drugiej strony, na podstawie (AN3), $0 + s(y) = s(y)$, zatem $0 + s(y) = s(y) + 0$. W ten sposób wykazaliśmy (3), a więc w konsekwencji również (2), czyli wykonaliśmy zerowy krok indukcyjny w dowodzie twierdzenia.

Aby dowieść drugiego członu koniunkcji (1), tzn. formuły: $\forall x(\phi(x) \Rightarrow \phi(s(x)))$, rozważmy dowolną ustaloną liczbę x oraz załóżmy

(4) $\forall y(x + y = y + x)$.

Aby wykazać

(5) $\forall y(s(x) + y = y + s(x))$,

połóżmy $\chi(y) := s(x) + y = y + s(x)$. Dowód (5) będzie więc indukcyjny. Musimy wykazać

(6) $s(x) + 0 = 0 + s(x)$ (tzn. $\chi(0)$) oraz

(7) $\forall y(s(x) + y = y + s(x) \Rightarrow s(x) + s(y) = s(y) + s(x))$ (tzn. $\forall y(\chi(y) \Rightarrow \chi(s(y)))$).

Formuła (6) jest oczywistym wnioskiem z (2). Dowodzimy więc formuły (7). Weźmy dowolną liczbę y i załóżmy, że

(8) $s(x) + y = y + s(x)$.

Wówczas $s(x) + s(y) =_{na\ mocy\ (AN4)} s(x + s(y)) =_{na\ mocy\ (4)} s(s(y) + x) =_{na\ mocy\ (AN4)} s(s(y + x)) =_{na\ mocy\ (4)} s(s(x + y)) =_{na\ mocy\ (AN4)} s(s(x) + y) =_{na\ mocy\ (8)} s(y + s(x)) =_{na\ mocy\ (AN4)} s(y) + s(x)$.

W ten sposób wykazano prawdziwość formuły (5), wobec czego również formuły (1), więc na mocy aksjomatu indukcji dowód twierdzenia jest zakończony. □

Aksjomat indukcji zazwyczaj wykorzystywany jest dla dowodów indukcyjnych w bardziej popularnej postaci, możliwej do napisania dopiero w języku arytmetyki z dodawaniem:

$$(\psi(0) \wedge \forall x(\psi(x) \Rightarrow \psi(x + 1))) \Rightarrow \forall x(\psi(x)).$$

Traktujemy powyższe wyrażenie jako twierdzenie, będące oczywistym wnioskiem z formuły (Aksjomat indukcji) oraz twierdzenia:

tw. 4. $\forall x(s(x) = x + s(0))$.

Dowód. Rozważmy dowolną liczbę x. Wówczas na mocy tw. 3 oraz (AN4), (AN3) mamy: $x + s(0) = s(0) + x = s(0 + x) = s(x)$. □

Arytmetyka liczb naturalnych z dodawaniem i mnożeniem jest teorią I rzędu określoną aksjomatycznie na języku arytmetyki z dodawaniem rozszerzonym o 2-argumentowy symbol funkcyjny $\cdot$, interpretowany w modelu standardowym jako operacja mnożenia.

Aksjomatyka tej teorii złożona jest z aksjomatów arytmetyki z dodawaniem oraz dwóch kolejnych aksjomatów opisujących operację mnożenia, analogicznie jak aksjomaty (AN3), (AN4) opisują dodawanie:

(AN5) $\forall y(0 \cdot y = 0)$,

(AN6) $\forall x \forall y(s(x) \cdot y = (x \cdot y) + y)$.

Przez *standardowy model* dla arytmetyki z dodawaniem i mnożeniem rozumiemy standardowy model dla arytmetyki elementarnej (opisany w §1), wyposażony w „zwykłe" operacje dodawania i mnożenia. Istnieją *niestandardowe* (nieizomorficzne ze standardowym) modele arytmetyki z dodawaniem i mnożeniem (zob. np. [9]), jednakże ich opis wymaga aparatu pojęciowego teorii modeli, w szczególności tzw. konstrukcji ultraproduktu, co wykracza poza ramy tej elementarnej monografii.

§3. Pewne metalogiczne własności arytmetyk liczb naturalnych

Arytmetyka elementarna oraz arytmetyka z dodawaniem różnią się od arytmetyki liczb naturalnych z dodawaniem i mnożeniem bardzo ważną własnością metalogiczną: te dwie pierwsze teorie są *zupełne*, podczas gdy arytmetyka z dodawaniem i mnożeniem jest teorią *niezupełną*. Aby objaśnić pojęcie *zupełności* teorii I rzędu, wprowadzimy teraz kilka prostych pojęć z teorii modeli oraz podamy pewne elementarne fakty z tej teorii.

Niech będzie dany jakiś język $\mathcal{L}$ pierwszego rzędu, w postaci ustalonej listy predykatów, symboli funkcyjnych oraz stałych indywidualnych.

Dla dowolnego zbioru zdań A (formuł domkniętych) języka $\mathcal{L}$ oznaczmy symbolem $\mathrm{Th}(A)$ teorię I rzędu aksjomatyzowaną przez zbiór A, tzn. $\mathrm{Th}(A)$ jest zbiorem wszystkich zdań α języka $\mathcal{L}$, które wynikają ze zbioru A, czyli $\alpha \in \mathrm{Th}(A)$ wtw dla dowolnej interpretacji $\mathcal{M}$ języka $\mathcal{L}, \alpha$ jest prawdziwe w $\mathcal{M}$, o ile każde zdanie β ze zbioru A jest prawdziwe w $\mathcal{M}$.

Ponadto, dla dowolnej interpretacji $\mathcal{M}$ języka $\mathcal{L}$, niech $\mathrm{Ver}(\mathcal{M})$ oznacza zbiór wszystkich zdań języka $\mathcal{L}$, które są prawdziwe w $\mathcal{M}$.

Według powyższej notacji mamy oczywisty związek: dla dowolnego zdania α, $\alpha \in \mathrm{Th}(A)$ wtw dla dowolnej interpretacji $\mathcal{M}$, jeśli $A \subseteq \mathrm{Ver}(\mathcal{M})$, to $\alpha \in \mathrm{Ver}(\mathcal{M})$. Stąd uzasadnione jest twierdzenie:

tw. 5. *Dla dowolnej interpretacji* $\mathcal{M}$ *oraz zbioru zdań* A *języka* $\mathcal{L}$, *jeżeli* $A \subseteq \mathrm{Ver}(\mathcal{M})$, *to* $\mathrm{Th}(A) \subseteq \mathrm{Ver}(\mathcal{M})$.

(*Jeżeli aksjomaty teorii są prawdziwe w danej interpretacji, to każde twierdzenie tej teorii jest prawdziwe w tejże interpretacji; innymi słowy, dowolny model dla aksjomatów teorii jest modelem dla tej teorii.*)

Rozważmy przypadek: $A = \mathrm{Ver}(\mathcal{M})$ dla ustalonej interpretacji $\mathcal{M}$ języka $\mathcal{L}$. Na mocy tw. 5 mamy natychmiast: $\mathrm{Th}(\mathrm{Ver}(\mathcal{M})) \subseteq \mathrm{Ver}(\mathcal{M})$. Z drugiej strony, z definicji teorii $\mathrm{Th}(B)$ aksjomatyzowanej przez zbiór zdań B, $B \subseteq \mathrm{Th}(B)$, zatem można sformułować twierdzenie:

tw. 6. *Dla dowolnej interpretacji* $\mathcal{M}$ *języka* $\mathcal{L}$, $\mathrm{Th}(\mathrm{Ver}(\mathcal{M})) = \mathrm{Ver}(\mathcal{M})$.

Zbiór wszystkich zdań prawdziwych w danej interpretacji jest więc teorią (opisującą strukturę relacyjno-algebraiczną tej interpretacji).

Można rozważać teorie nie tylko pojedynczych struktur relacyjno-algebraicznych, lecz ich klas. Niech $\mathbf{K}$ będzie dowolną klasą (mnogością) interpretacji dla języka $\mathcal{L}$. Oznaczmy symbolem $\mathrm{Ver}(\mathbf{K})$ zbiór wszystkich zdań języka $\mathcal{L}$ prawdziwych w każdej interpretacji $\mathcal{M} \in \mathbf{K}$, tzn. $\mathrm{Ver}(\mathbf{K}) = \bigcap\{\mathrm{Ver}(\mathcal{M}) : \mathcal{M} \in \mathbf{K}\}$. Wówczas mamy:

tw. 7. *Dla dowolnej klasy interpretacji* $\mathbf{K}$ *dla języka* $\mathcal{L}$, $\mathrm{Th}(\mathrm{Ver}(\mathbf{K})) = \mathrm{Ver}(\mathbf{K})$.

DOWÓD. Wystarczy wykazać inkluzję $\mathrm{Th}(\mathrm{Ver}(\mathbf{K})) \subseteq \mathrm{Ver}(\mathbf{K})$. Niech więc $\alpha \in \mathrm{Th}(\mathrm{Ver}(\mathbf{K}))$, czyli

(1) $\forall\mathcal{M}(\mathrm{Ver}(\mathbf{K}) \subseteq \mathrm{Ver}(\mathcal{M}) \Rightarrow \alpha \in \mathrm{Ver}(\mathcal{M}))$.

Aby wykazać, że $\alpha \in \mathrm{Ver}(\mathbf{K})$ rozważmy dowolną interpretację $\mathcal{M} \in \mathbf{K}$. Wówczas oczywiście $\mathrm{Ver}(\mathbf{K}) \subseteq \mathrm{Ver}(\mathcal{M})$, zatem na mocy (1), $\alpha \in \mathrm{Ver}(\mathcal{M})$ i ostatecznie, wobec dowolności wyboru interpretacji $\mathcal{M}$ z klasy $\mathbf{K}$, otrzymujemy: $\alpha \in \mathrm{Ver}(\mathbf{K})$. $\square$

DEFINICJA. Teorię $\mathrm{Th}(A)$ nazywamy *zupełną*, gdy dla dowolnego zdania α języka $\mathcal{L}$, $\alpha \in \mathrm{Th}(A)$ lub $\neg\alpha \in \mathrm{Th}(A)$.

tw. 8. *Dla dowolnej interpretacji* $\mathcal{M}$ *języka* $\mathcal{L}$, *teoria* $\mathrm{Ver}(\mathcal{M})$ *jest zupełna.*

DOWÓD. Załóżmy nie wprost, że dla pewnej interpretacji $\mathcal{M}$, $\mathrm{Ver}(\mathcal{M})$ nie jest zupełna. Wówczas dla pewnego zdania α, $\alpha \notin \mathrm{Ver}(\mathcal{M})$ oraz $\neg\alpha \notin \mathrm{Ver}(\mathcal{M})$. Na podstawie warunku prawdziwości dla spójnika negacji $\neg$: $\neg\alpha \in \mathrm{Ver}(\mathcal{M})$ wtw $\alpha \notin \mathrm{Ver}(\mathcal{M})$, otrzymujemy sprzeczność. $\square$

W ogólności teoria klasy struktur $\mathrm{Ver}(\mathbf{K})$ nie musi być zupełna. Argument zastosowany w dowodzie tw. 8 oczywiście nie „pracuje" dla teorii $\mathrm{Ver}(\mathbf{K})$. Banalnym przykładem jest tu teoria $\mathrm{Ver}(\mathbf{K}_0)$, gdzie $\mathbf{K}_0$ jest klasą wszystkich interpretacji dla języka $\mathcal{L}$. Oczywiście $\mathrm{Ver}(\mathbf{K}_0)$ jest zbiorem wszystkich zdań tautologicznych w języku $\mathcal{L}$, zaś w jakimkolwiek języku I rzędu występują takie zdania, że ani one, ani ich negacje nie są tautologiami w tym języku, zatem $\mathrm{Ver}(\mathbf{K}_0)$ nie jest teorią zupełną.

Przykładem teorii niezupełnej (tzn. nie będącej zupełną) jest teoria ZFC. Oto na przykład tzw. *hipoteza continuum* (zob. §4, Rozdział 11) jest takim zdaniem w języku ZFC, że ani ono ani jego negacja nie należą ZFC. Dowodzi się bowiem po pierwsze, że *hipoteza continuum* jest niezależna względem aksjomatów ZFC (tzn. z nich nie wynika) oraz po drugie, że dodanie jej do aksjomatów ZFC daje teorię niesprzeczną, tzn. $\mathrm{Th}(Ax)$, gdzie Ax jest zbiorem aksjomatów ZFC wraz z *hipotezą continuum*, jest teorią niesprzeczną. Stąd *hipoteza continuum* nie należy do ZFC, skoro nie wynika z aksjomatów ZFC, oraz negacja *hipotezy continuum* nie jest twierdzeniem teorii ZFC, gdyby bowiem była, to byłaby również twierdzeniem teorii $\mathrm{Th}(Ax)$, skoro $\mathrm{ZFC} \subseteq \mathrm{Th}(Ax)$; wówczas jednak $\mathrm{Th}(Ax)$ byłaby sprzeczna.

tw. 9. *Dla dowolnego zbioru zdań A języka $\mathcal{L}$ oraz interpretacji $\mathcal{M}$ dla $\mathcal{L}$ takich, że $A \subseteq \mathrm{Ver}(\mathcal{M})$, teoria $\mathrm{Th}(A)$ jest zupełna wtw $\mathrm{Th}(A) = \mathrm{Ver}(\mathcal{M})$.*

(*Jeżeli $\mathcal{M}$ jest modelem dla aksjomatów jakiejś teorii, to teoria ta jest zupełna dokładnie wtedy, gdy jest teorią struktury z $\mathcal{M}$.*)

Dowód. Załóżmy, że
(1) $A \subseteq \mathrm{Ver}(\mathcal{M})$.
($\Rightarrow$): Niech
(2) $\mathrm{Th}(A)$ jest zupełna,
oraz załóżmy nie wprost, że
(3) $\mathrm{Th}(A) \neq \mathrm{Ver}(\mathcal{M})$.
Wówczas z (1) na mocy tw. 5 mamy:
(4) $\mathrm{Th}(A) \subseteq \mathrm{Ver}(\mathcal{M})$,
zatem na podstawie (3) stwierdzamy, iż nie jest tak, że $\mathrm{Ver}(\mathcal{M}) \subseteq \mathrm{Th}(A)$. Niech więc α będzie takim zdaniem, że
(5) $\alpha \in \mathrm{Ver}(\mathcal{M})$ oraz
(6) $\alpha \notin \mathrm{Th}(A)$.
Wtedy z (2) i (6) otrzymujemy: $\neg\alpha \in \mathrm{Th}(A)$, co wraz z (4) implikuje: $\neg\alpha \in \mathrm{Ver}(\mathcal{M})$, a to z kolei oznacza, iż $\alpha \notin \mathrm{Ver}(\mathcal{M})$. Sprzeczność z (5).
($\Leftarrow$): na mocy tw. 8. □

Dowodzi się (stosując metodę tzw. skolemizacji zdań, zob np. [9]), że arytmetyka z dodawaniem i mnożeniem nie jest teorią zupełną. Na mocy tw. 9 oznacza to, iż arytmetyka ta jest zbiorem twierdzeń różnym od zbioru wszystkich zdań prawdziwych w jej standardowym modelu. Zatem, skoro na mocy tw. 5 wszystkie jej twierdzenia są prawdziwe w standardowym modelu, istnieć więc muszą również zdania, które prawdziwe są w standardowym modelu i które twierdzeniami arytmetyki nie są, tzn. nie wynikają z jej aksjomatów. Innymi słowy, istnieć musi taki model (niestandardowy) arytmetyki z dodawaniem i mnożeniem, w którym pewne, w standardowym modelu prawdziwe zdanie, jest fałszywe.

Tymczasem okazuje się, że arytmetyka elementarna, jak również arytmetyka z dodawaniem, są teoriami zupełnymi. Na mocy tw. 9, obie te teorie są więc odpowiednio zbiorami wszystkich zdań prawdziwych w swoich modelach standardowych.

§4. Operacja następnika w teorii ZFC

Głównym celem niniejszego rozdziału jest interpretacja arytmetyki elementarnej w teorii ZFC. Polega ona na wykazaniu, że każde twierdzenie arytmetyki elementarnej jest twierdzeniem teorii mnogości ZFC, o ile wcześniej, po pierwsze, ustalono do jakich zbiorów (opisywanych w ZFC) odnoszą się kwantyfikatory w języku arytmetyki, czyli jakie zbiory mają być postrzegane jako liczby naturalne, oraz po drugie, zinterpretowano w ZFC pierwotne pojęcia arytmetyki elementarnej: liczbę zero oraz następnik, tzn. określono jaki wyróżniony zbiór (wśród zbiorów określonych jako liczby naturalne) odpowiada stałej 0 oraz jaka operacja na zbiorach (określonych jako liczby naturalne) odpowiada symbolowi funkcyjnemu s.

Naturalnie, aby wykazać, że każde twierdzenie arytmetyki elementarnej jest twierdzeniem teorii ZFC, wystarczy wykazać, że każdy aksjomat arytmetyki (po zinterpretowaniu) jest twierdzeniem ZFC.

Na początek zdefiniujmy jednoargumentową operację S zwaną operacją następnika, określoną dla wszystkich zbiorów:

Definicja. Dla dowolnego zbioru x, $S(x) = x \cup \{x\}$. To znaczy, $\forall y(y \in S(x) \Leftrightarrow (y \in x \vee y = x))$.

Następnik $S(x)$ zbioru x jest więc takim zbiorem, że jednocześnie $x \in S(x)$ oraz $x \subseteq S(x)$.

Twierdzenie 1. *Dla dowolnego zbioru x, $S(x)$ jest najmniejszym zbiorem (względem inkluzji) wśród wszystkich zbiorów y takich, że $x \in y$ oraz $x \subseteq y$.*

Dowód. Załóżmy, że $x \in y$ oraz $x \subseteq y$. Wówczas $\{x\} \subseteq y$, zatem $x \cup \{x\} \subseteq y$, czyli $S(x) \subseteq y$. □

Zauważmy ponadto, że dla dowolnego zbioru x nie istnieje taki zbiór y, że $x \in y$ oraz $y \in S(x)$. Gdyby bowiem taki y istniał, to byłoby: $y \in x$ lub $y = x$, lecz oba człony tej alternatywy są zabronione, na mocy Wniosków z odpowiednio Tw. 10, Rozdział 2 i Tw. 9, Rozdział 2.

Kolejne dwa twierdzenia charakteryzujące operację S, wskazują na możliwość jej wykorzystania jako interpretacji symbolu funkcyjnego „s" z języka arytmetyki:

TWIERDZENIE 2. $\forall x(S(x) \neq \varnothing)$.

DOWÓD. Oczywisty na mocy definicji operacji następnika. □

TWIERDZENIE 3. $\forall x \forall y(S(x) = S(y) \Rightarrow x = y)$.

DOWÓD. Załóżmy, że $S(x) = S(y)$. Ponieważ według Wniosku z Tw. 10, Rozdział 2, wykluczona jest koniunkcja $x \in y \wedge y \in x$, więc prawdziwa jest alternatywa $x \notin y \vee y \notin x$. Załóżmy, że $x \notin y$. Ponieważ $x \in S(x)$, więc z założenia dowodu uzyskujemy: $x \in S(y)$, zatem $x \in y \vee x = y$, skąd $x = y$. Analogicznie postępujemy przy założeniu, że $y \notin x$. □

Jak widać, Tw. 2 jest interpretacją aksjomatu (AN1), o ile zbiór pusty uznamy za interpretację stałej 0. Naturalnie Tw. 3 jest interpretacją aksjomatu (AN2) arytmetyki elementarnej. Na uwagę zasługuje fakt, że kwantyfikatory pojawiające się w tych dwóch twierdzeniach odnoszą się do wszelkich zbiorów, zatem również do tych, które później określimy jako liczby naturalne.

Ograniczenie kwantyfikacji przy interpretacji aksjomatów arytmetyki w ZFC do specjalnej klasy zbiorów, okazuje się konieczne. Nie oczekujmy bowiem, że interpretacja aksjomatu indukcji, w której kwantyfikatory odnoszą się do wszelkich zbiorów oraz interpretacjami 0 i s są odpowiednio $\varnothing, S$ – nawet przy jakimś rozsądnym ograniczeniu klasy formuł $\psi(x)$, teraz będących formułami języka ZFC – okaże się twierdzeniem teorii ZFC. Gdyby tak było, to każde twierdzenie arytmetyki elementarnej, według tejże interpretacji (której dziedziną jest klasa wszystkich zbiorów), byłoby twierdzeniem ZFC. Tak jednakże nie jest. Rozważmy na przykład tw. 2 (§1), po zinterpretowaniu w postaci: $\forall x(x = \varnothing \vee \exists y(x = S(y)))$. Bynajmniej nie jest to twierdzenie teorii mnogości. Weźmy bowiem pod uwagę zbiór $\{\{\varnothing\}\}$. Wówczas prawdą jest, że $\{\{\varnothing\}\} \neq \varnothing \wedge \neg\exists y(\{\{\varnothing\}\} = S(y))$. Gdyby bowiem dla pewnego zbioru $y : \{\{\varnothing\}\} = S(y)$, to mielibyśmy: $y \in \{\{\varnothing\}\}$, zatem $y = \{\varnothing\}$; lecz wówczas $S(y) = y \cup \{y\} = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}$ i ostatecznie $\{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}$, co jest absurdalne.

To, że kluczową rolę w interpretacji arytmetyki elementarnej odgrywa aksjomat indukcji jest widoczne na podstawie faktu, iż same Twierdzenia 2 oraz 3 nie są wystarczające do uznania, że jedyną możliwą interpretacją symbolu „s" z języka arytmetyki jest operacja następnika S. Gdyby na przykład interpretować ów symbol jako operację zbioru potęgowego P (oraz 0 jako zbiór $\varnothing$), z aksjomatów (AN1), (AN2) otrzymujemy twierdzenia teorii ZFC:

$\forall x(P(x) \neq \varnothing)$ (Wniosek z Tw. 7, Rozdział 1),

$\forall x \forall y(P(x) = P(y) \Rightarrow x = y)$ (na mocy Twierdzeń 1, 8, 2 z Rozdziału 1).

W następnym paragrafie dokonamy interpretacji aksjomatu indukcji, w której symbol „s" reprezentuje operację S, uzyskując z tego aksjomatu twierdzenie ZFC.

Obecnie skupimy uwagę na innych własnościach operacji następnika, choć nie wykorzystywanych przy interpretowaniu arytmetyki elementarnej w ZFC, to jednak użytecznych później, w teorii liczb porządkowych von Neumanna (Rozdziały 8 i 9). Okazuje się, że w tej teorii operacja sumy $\bigcup$ pełni równie ważną funkcję, w szczególności zachowuje się dla niektórych zbiorów w pewnym sensie dualnie do operacji następnika. Podamy więc obecnie pewne związki między tymi dwiema operacjami.

Twierdzenie 4. *$\bigcup S(x) = x \cup \bigcup x$.*

Dowód. ($\subseteq$): Niech $y \in \bigcup S(x)$. Zatem $y \in z$ dla pewnego $z \in x \cup \{x\}$. Niech $z \in x$. Wówczas $y \in \bigcup x$. Gdy zaś $z = x$, to $y \in x$. W obu przypadkach $y \in x \cup \bigcup x$.

($\supseteq$): Załóżmy, że $y \in x \cup \bigcup x$. Niech $y \in x$. Ponieważ $x \in S(x)$, więc $y \in \bigcup S(x)$. Niech $y \in \bigcup x$. Wtedy $y \in z$ dla pewnego $z \in x$. Stąd $z \in S(x)$, zatem $y \in \bigcup S(x)$. $\square$

Twierdzenie 5. *$\bigcup x = x$ wtw $x \in S(\bigcup x)$.*

Dowód. ($\Rightarrow$): Załóżmy, że $\bigcup x = x$. Wówczas natychmiast $x \in S(\bigcup x)$, bo $x \in S(x)$.

($\Leftarrow$): Załóżmy, że $x \in S(\bigcup x)$. Wówczas $x \in \bigcup x \cup \{\bigcup x\}$. Gdyby $x \in \bigcup x$, to $x \in y$ dla pewnego $y \in x$, co jest niemożliwe (Wniosek z Tw. 10, Rozdział 2). Zatem $x \in \{\bigcup x\}$, tzn. $x = \bigcup x$. $\square$

Twierdzenie 6. *$x \subseteq \bigcup x$ wtw $\bigcup S(x) \in S(\bigcup x)$.*

Dowód. ($\Rightarrow$): Załóżmy, że $x \subseteq \bigcup x$. Wówczas $x \cup \bigcup x = \bigcup x$ (Tw. 13(3), Rozdział 1). Zatem na mocy Tw. 4, $\bigcup S(x) = \bigcup x$, a ponieważ $\bigcup x \in S(\bigcup x)$, więc $\bigcup S(x) \in S(\bigcup x)$.

($\Leftarrow$): Załóżmy, że $\bigcup S(x) \in S(\bigcup x)$. Zatem według Tw. 4, $x \cup \bigcup x \in S(\bigcup x)$, tzn. $x \cup \bigcup x \in \bigcup x$ lub $x \cup \bigcup x = \bigcup x$. Gdyby $x \cup \bigcup x \in \bigcup x$, to skoro $\bigcup x \subseteq x \cup \bigcup x$, więc byłoby: $x \cup \bigcup x \in x \cup \bigcup x$, co jest niemożliwe (Wniosek z Tw. 9, Rozdział 2). Zatem $x \cup \bigcup x = \bigcup x$, co implikuje: $x \subseteq \bigcup x$. $\square$

TWIERDZENIE 7. $\bigcup x \in x$ *wtw* $S(\bigcup x) \subseteq \bigcup S(x)$.

DOWÓD. ($\Rightarrow$): Załóżmy, że $\bigcup x \in x$. Wówczas $\{\bigcup x\} \subseteq x$, zaś $x \subseteq x \cup \bigcup x$, zatem $\{\bigcup x\} \subseteq x \cup \bigcup x$. Oczywiście $\bigcup x \subseteq x \cup \bigcup x$. Ostatecznie, $\bigcup x \cup \{\bigcup x\} \subseteq x \cup \bigcup x$. Stąd, na mocy Tw. 4 oraz definicji następnika, $S(\bigcup x) \subseteq \bigcup S(x)$.

($\Leftarrow$): Załóżmy, że $S(\bigcup x) \subseteq \bigcup S(x)$. Wówczas, ponieważ $\bigcup x \in S(\bigcup x)$, więc $\bigcup x \in \bigcup S(x)$, tzn. (Tw. 4) $\bigcup x \in x \cup \bigcup x$. Zatem $\bigcup x \in x$ lub $\bigcup x \in \bigcup x$. Lecz drugi z członów tej alternatywy jest fałszywy (Wniosek z Tw. 9, Rozdział 2). Dlatego $\bigcup x \in x$. □

TWIERDZENIE 8. *Dla dowolnego zbioru x, jeżeli $x = \bigcup x$, to x nie jest następnikiem żadnego zbioru, tzn.* $\forall y(x \neq S(y))$.

DOWÓD. Załóżmy, że $x = \bigcup x$ oraz nie wprost, niech $x = S(y)$ dla pewnego zbioru y. Wówczas $\bigcup x = \bigcup S(y) = y \cup \bigcup y$ na mocy Tw. 4. Zatem z założenia, $x = y \cup \bigcup y$. Lecz z założenia nie wprost, $x = y \cup \{y\}$, skąd $y \in x$. Wówczas $y \in y \cup \bigcup y$, co jest niemożliwe. □

Odwrotne twierdzenie w ogólności nie jest prawdziwe. Rozważmy na przykład $x = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$. Gdyby $x = S(y)$ dla jakiegoś y, to y musiałby być elementem zbioru x. Lecz $S(\varnothing) = \{\varnothing\} \neq x$, $S(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\} \neq x$, wreszcie $S(\{\{\varnothing\}\}) = \{\{\varnothing\}, \{\{\varnothing\}\}\} \neq x$. Zatem x nie jest następnikiem żadnego zbioru y. Natomiast $\bigcup x = \{\varnothing, \{\varnothing\}\} \neq x$.

§5. Interpretacja arytmetyki elementarnej w teorii ZFC

Dysponując operacją następnika, jesteśmy w stanie zapisać aksjomat nieskończoności w krótszej postaci:

$(Ax\,\infty)'$ $\exists x(\varnothing \in x \wedge \forall y(y \in x \Rightarrow S(y) \in x))$.

Zbiór, którego istnienie ów aksjomat stwierdza, nosi nazwę zbioru indukcyjnego:

DEFINICJA. Dla dowolnego zbioru x, x jest *indukcyjny*, gdy $\varnothing \in x$ oraz $\forall y(y \in x \Rightarrow S(y) \in x)$.

Zbiór jest więc indukcyjny, gdy jego elementem jest zbiór $\varnothing$ oraz gdy jest on zamknięty na operację następnika.

W ten sposób uzyskujemy najprostszą postać aksjomatu nieskończoności:

$(Ax\,\infty)''$ $\exists x(x$ jest indukcyjny$)$.

Pojęcie zbioru indukcyjnego umożliwia wyodrębnienie spośród zbiorów tych, których mnogość stanowić będzie dziedzinę modelu dla aksjomatów arytmetyki elementarnej. Zbiory te nazwiemy więc liczbami naturalnymi. Właśnie do tych zbiorów ograniczymy kwantyfikację interpretując aksjomaty arytmetyki elementarnej.

Definicja. Dla dowolnego zbioru x, x jest *liczbą naturalną*, gdy $\forall y$(y jest indukcyjny $\Rightarrow x \in y$) (zbiór jest liczbą naturalną, gdy jest elementem każdego zbioru indukcyjnego).

Wprost z definicji liczby naturalnej oraz zbioru indukcyjnego otrzymujemy:

Twierdzenie 9. *Zbiór $\varnothing$ jest liczbą naturalną.*

Mnogość liczb naturalnych jest zamknięta na operację następnika:

Twierdzenie 10. $\forall x$(x *jest liczbą naturalną* $\Rightarrow S(x)$ *jest liczbą naturalną*).

Dowód. Załóżmy, że zbiór x jest liczbą naturalną, tzn. $\forall y$(y jest indukcyjny $\Rightarrow x \in y$). Aby wykazać, że $S(x)$ jest liczbą naturalną, rozważmy dowolny zbiór indukcyjny y. Wówczas z założenia, $x \in y$. Zatem z definicji zbioru indukcyjnego mamy: $S(x) \in y$, co wobec dowolności wyboru zbioru y dowodzi, że $S(x)$ jest liczbą naturalną. $\square$

Wykażemy teraz, że owa mnogość liczb naturalnych jest po prostu zbiorem (tzn. obiektem, którego istnienie jest dowodliwe w ZFC). W tym celu rozważmy w aksjomacie podzbiorów formułę $\phi(x)$ postaci: x jest liczbą naturalną. Oznaczmy symbolem „A" jakikolwiek ze zbiorów, których istnienie stwierdza aksjomat nieskończoności, uzyskując prawdziwe zdanie: A jest indukcyjny. Wówczas natychmiast z definicji liczby naturalnej otrzymujemy prawdziwy poprzednik implikacji $(AxZ)_\phi$,

$\forall x$(x jest liczbą naturalną $\Rightarrow x \in A$),

zatem również prawdziwy następnik w aksjomacie podzbiorów,

$\exists y \forall x$($x \in y \Leftrightarrow x$ jest liczbą naturalną),

co w konsekwencji prowadzi do definicji zbioru liczb naturalnych N:

Definicja. $\forall x$($x \in N \Leftrightarrow x$ jest liczbą naturalną) lub $N = \{x : x$ jest liczbą naturalną$\}$.

Jako bezpośredni wniosek z Tw. 9 oraz Tw. 10 uzyskujemy:

TWIERDZENIE 11. *N jest indukcyjny.*

Dzięki Tw. 11, symbole funkcyjne $0, s$ występujące w aksjomatach arytmetyki elementarnej możemy interpretować jako odpowiednio, zbiór $\varnothing$ oraz operacja następnika S (skoro $\varnothing \in N$ oraz zbiór N jest zamknięty na tę operację). Jest oczywiste, że na podstawie Tw. 2 oraz Tw. 3 mamy:

$\forall x \in N\ (S(x) \neq \varnothing)$, oraz

$\forall x, y \in N\ (S(x) = S(y) \Rightarrow x = y)$,

czyli dwa pierwsze aksjomaty arytmetyki elementarnej są prawdziwe w dziedzinie N (są one przecież prawdziwe w dziedzinie wszystkich zbiorów). Aby wykazać, że aksjomat indukcji jest również prawdziwy w dziedzinie N dowiedźmy najpierw, iż zbiór liczb naturalnych jest najmniejszym (względem inkluzji) zbiorem indukcyjnym.

TWIERDZENIE 12. $\forall x(x$ *jest indukcyjny* $\Rightarrow N \subseteq x)$.

DOWÓD. Załóżmy, że x jest indukcyjny. Niech $y \in N$. Skoro więc y jest liczbą naturalną, to $y \in x$, co dowodzi inkluzji: $N \subseteq x$. $\square$

Interpretacja aksjomatu indukcji ma postać:

TWIERDZENIE 13. *Dla dowolnej formuły $\psi(x)$ języka teorii* ZFC,
$[\psi(\varnothing) \wedge \forall x \in N(\psi(x) \Rightarrow \psi(S(x)))] \Rightarrow \forall x \in N(\psi(x))$.

DOWÓD. Załóżmy, że
(1) $\psi(\varnothing)$ oraz
(2) $\forall x \in N(\psi(x) \Rightarrow \psi(S(x)))$.

Wstawmy w aksjomacie podzbiorów $(AxZ)_\phi$ jako $\phi(x)$ formułę $x \in N \wedge \psi(x)$, uzyskując poprzednik tego aksjomatu w postaci:
$\forall x((x \in N \wedge \psi(x)) \Rightarrow x \in N)$.

Oderwijmy więc następnik:
$\exists y \forall x(x \in y \Leftrightarrow (x \in N \wedge \psi(x)))$.

Stąd dla pewnego zbioru B,
(3) $\forall x(x \in B \Leftrightarrow (x \in N \wedge \psi(x)))$.

Wykażmy, że B jest zbiorem indukcyjnym. Ponieważ $\varnothing \in N$, więc na mocy (1) i (3), $\varnothing \in B$. Załóżmy, że $y \in B$. Wówczas z (3), $y \in N$ oraz $\psi(y)$. Zatem z założenia (2), $\psi(S(y))$. Ponadto, skoro $y \in N$, więc $S(y) \in N$ (Tw. 10). Ostatecznie z (3), $S(y) \in B$, czyli B jest indukcyjny.

Zatem na podstawie Tw. 12 otrzymujemy:
(4) $N \subseteq B$.

Aby więc dowieść, że $\forall x \in N(\psi(x))$ rozważmy dowolny $x \in N$. Wówczas $x \in B$ na mocy (4), czyli, biorąc pod uwagę (3), zachodzi $\psi(x)$. $\square$

Warto podkreślić, że w interpretacji aksjomatu indukcji jaką jest Tw. 13, nie ma żadnych ograniczeń dla formuł $\psi(x)$. Zastosujmy Tw. 13 w przypadku, gdy formuła $\psi(x)$ nie ma swojego odpowiednika w języku arytmetyki elementarnej:

TWIERDZENIE 14. *Każdy element dowolnej liczby naturalnej jest liczbą naturalną, tzn.* $\forall x \in N\ \forall y(y \in x \Rightarrow y \in N)$.

DOWÓD. Połóżmy $\psi(x) := \forall y(y \in x \Rightarrow y \in N)$. Wówczas dowodzone twierdzenie jest następnikiem implikacji Tw. 13 (aksjomatu indukcji). Udowodnijmy więc poprzednik. Formuła $\psi(\varnothing)$, a więc formuła postaci: $\forall y(y \in \varnothing \Rightarrow y \in N)$ jest naturalnie prawdziwa.

Weźmy dowolne $x \in N$ oraz przyjmijmy założenie indukcyjne, że $\psi(x)$, tzn. $\forall y(y \in x \Rightarrow y \in N)$. W celu wykazania, że prawdą jest $\psi(S(x))$, tzn. formuła postaci: $\forall y(y \in S(x) \Rightarrow y \in N)$, weźmy dowolny y i załóżmy, że $y \in S(x)$. Wówczas $y \in x$ lub $y = x$. Gdy $y \in x$, to z założenia indukcyjnego mamy: $y \in N$, gdy zaś $y = x$, to oczywiście $y \in N$ (bo $x \in N$). $\square$

Rozdział 8. Pojęcie liczby porządkowej

§1. Liczby naturalne a liczby porządkowe

Oto cztery pierwsze liczby naturalne zapisane według różnych czterech notacji w porządku od najmniejszej do największej:

$\varnothing,\ S(\varnothing),\ S(S(\varnothing)),\ S(S(S(\varnothing)))$

$\varnothing,\ \{\varnothing\},\ \{\varnothing,\{\varnothing\}\},\ \{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}$

$0,\ 1,\ 2,\ 3$

$0,\ \{0\},\ \{0,1\},\{0,1,2\}.$

Widać, że sekwencja czterech pierwszych liczb naturalnych ma następującą własność:

(*) Każdy ze zbiorów tej sekwencji jest zbiorem wszystkich tych i tylko tych zbiorów, które w tej sekwencji są wcześniej od niego.

Rozszerzmy sekwencję czterech pierwszych liczb naturalnych do nieskończoności:

(1) $\varnothing,\ S(\varnothing),\ S(S(\varnothing)),\ S(S(S(\varnothing))),\ \ldots$ lub

(1)′ $\varnothing,\ \{\varnothing\},\ \{\varnothing,\{\varnothing\}\},\ \{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\},\ \ldots$

tak, aby sekwencja ta miała własność (*), tzn. piąty wyraz tej sekwencji jest zbiorem dokładnie poprzednich czterech zbiorów, szósty jej wyraz jest zbiorem dokładnie pięciu poprzedzających zbiorów itd.

Jest oczywiste, na mocy Twierdzeń 9 oraz 10, Rozdział 7, że każdy zbiór pojawiający się w tejże sekwencji jest liczbą naturalną. Nie jest wszakże oczywiste, że każda liczba naturalna (w myśl definicji teoriomnogościowej) występuje w tej sekwencji. Jednakże tak właśnie jest. Innymi słowy, zbiór N jest dziedziną standardowego (precyzyjniej: izomorficznego ze standardowym) modelu arytmetyki elementarnej. Załóżmy bowiem, że tak nie jest. Niech zatem $\lambda_0 \in N$ będzie zbiorem, który w sekwencji (1) nie występuje. Interpretacja teoriomnogościowa tw. 2, §1, Rozdział 7, a więc zdanie: $\forall x \in N(x = \varnothing \vee \exists y \in N(x = S(y)))$ jest twierdzeniem ZFC. Ponieważ $\lambda_0 \neq \varnothing$, więc na mocy tego twierdzenia: $\lambda_0 = S(\lambda_1)$ dla pewnego zbioru $\lambda_1 \in N$. Gdyby λ_1 występował w sekwencji (1), to również λ_0 (jako następnik λ_1) występowałby w tejże sekwencji, a tak nie jest. Zatem λ_1 nie występuje w sekwencji. Zatem znowu $\lambda_1 \neq \varnothing$ i na mocy tw. 2: $\lambda_1 = S(\lambda_2)$ dla pewnego zbioru $\lambda_2 \in N$, który nie występuje w sekwencji itd. Ponieważ $\lambda_1 \in \lambda_0, \lambda_2 \in \lambda_1, \ldots$, więc sekwencja: $\lambda_0, \lambda_1, \lambda_2, \ldots$ jest nieskończonym zejściem zbioru λ_0 (Rozdział 2), co oznacza, że λ_0 jest zbiorem nieufundowanym; zaś zgodnie z aksjomatem regularności takich zbiorów w ZFC nie ma.

Skoro więc (1) jest sekwencją wszystkich liczb naturalnych oraz sekwencja ta ma własność (*), zatem każda liczba naturalna jest zbiorem wszystkich liczb naturalnych mniejszych (wcześniejszych) od niej.

Rozważmy przez chwilę jakąkolwiek sekwencję zbiorów mającą własność (*). Niech A będzie dowolnie wybranym zbiorem z tej sekwencji. Wówczas zbiór A ma następującą własność: dla dowolnego $a \in A$: $a \subseteq A$. Jest tak dlatego, ponieważ dowolny element a zbioru A (gdy $A \neq \varnothing$) znajduje się w powyższej sekwencji przed A, zatem każdy element zbioru a, będąc przed a jest tym samym przed zbiorem A, tzn. należy do A. Zbiór A o takiej własności nazywamy *tranzytywnym*.

Jest zatem jasne, że własność (*) sekwencji zbiorów implikuje to, że każdy ze zbiorów tej sekwencji jest zbiorem tranzytywnym.

Nietrudno zorientować się, że własność (*) implikuje ponadto, że każdy element jakiegokolwiek zbioru A z tej sekwencji jest zbiorem tranzytywnym. Jeśli bowiem rozważymy jakiś $a \in A$, to przecież a musi znajdować się (przed A) w tej sekwencji, zatem a jest zbiorem tranzytywnym.

Zbiór tranzytywny, którego każdy element jest zbiorem tranzytywnym nazywamy *liczbą porządkową*. Zatem własność (*) sekwencji zbiorów implikuje to, że każdy ze zbiorów tej sekwencji jest liczbą porządkową.

Wniosek: każda liczba naturalna jest liczbą porządkową (tzn. jest zbiorem tranzytywnym oraz każdy jej element jest zbiorem tranzytywnym – naturalnie drugi człon tejże koniunkcji jest również wnioskiem z członu pierwszego oraz Tw. 14, Rozdział 7).

Powstaje pytanie czy jedynymi liczbami porządkowymi są liczby naturalne. Odpowiemy przecząco, gdy podamy jakąkolwiek sekwencję zbiorów mającą własność (*) i w której wystąpi chociaż jeden zbiór niebędący liczbą naturalną.

Aby podać taką sekwencję, zastanówmy się najpierw nad warunkami konstrukcji jakiejkolwiek sekwencji mającej własność (*).

Otóż, po pierwsze, taka sekwencja zbiorów musi mieć początek (pierwszy wyraz). Gdyby bowiem go nie miała, to wybierając dowolny zbiór z takiej sekwencji i układając wszystkie zbiory z tej sekwencji występujące przed tym wybranym zbiorem w odwrotnej kolejności, uzyskalibyśmy nieskończone zejście, które, jak wiadomo skądinąd (por. Rozdział 2), nie może istnieć.

Po drugie, pierwszy wyraz takiej sekwencji musi być zbiorem pustym, skoro pierwszy wyraz jest, jak każdy, zbiorem, którego elementami są te i tylko te zbiory, które go w sekwencji poprzedzają, a przecież żadne zbiory pierwszego jej wyrazu nie poprzedzają.

Po trzecie, dla dowolnego A, jeżeli A jest zbiorem występującym w takiej sekwencji oraz A nie jest jej ostatnim wyrazem, to bezpośrednio następującym po A wyrazem tej sekwencji jest zbiór $S(A)$. Bowiem z definicji operacji następnika, zbiór $S(A)$ jest jedynym zbiorem, którego elementami są wszystkie elementy zbioru A oraz sam zbiór A. Jeśli więc A nie jest ostatnim wyrazem sekwencji, to po nim musi w tej sekwencji wystąpić zbiór tych i tylko tych zbiorów, które go w tej sekwencji poprzedzają, a poprzedzają go w tej sekwencji zbiór A i te zbiory, które są wcześniej niż A tzn. wszystkie elementy zbioru A.

Po czwarte, jakakolwiek sekwencja skończona mająca własność (*) jest sekwencją początkowych n wyrazów sekwencji (1) dla pewnego n. Jest to oczywisty wniosek z warunków drugiego i trzeciego, jakie musi spełniać konstrukcja jakiejkolwiek sekwencji zbiorów o własności (*).

Po piąte, jakakolwiek sekwencja nieskończona o własności (*) musi „zawierać" sekwencję (1) i jeżeli nie jest z nią tożsama, to musi ją „zawierać" jako swoją początkową część właściwą. Jest to wniosek oparty na tych samych argumentach, na których był oparty warunek czwarty, tzn. pierwszym wyrazem nieskończonej sekwencji o własności (*) jest zbiór $\varnothing$ oraz bezpośrednim następnikiem jakiegokolwiek zbioru A tej sekwencji, który nie jest jej ostatnim wyrazem, jest zbiór $S(A)$.

Widać wyraźnie, że znajdziemy liczbę porządkową niebędącą liczbą naturalną wówczas, gdy skonstruujemy nieskończoną sekwencję spełniającą (*), której początkową częścią właściwą jest sekwencja (1) wszystkich liczb naturalnych. Żeby taką sekwencję podać, należy najpierw określić, jaki to zbiór winien w niej występować bezpośrednio po wszystkich zbiorach sekwencji (1) i czy w ogóle taki zbiór istnieje. Otóż zgodnie z warunkiem (*) musi to być zbiór tych i tylko tych zbiorów, które występują w konstruowanej sekwencji przed nim, a więc zbiór, którego elementami są wszystkie liczby naturalne i tylko one. Krótko mówiąc, jest to zbiór liczb naturalnych N. Jeżeli N nie jest ostatnim wyrazem konstruowanej sekwencji, to naturalnie bezpośrednio następnym jej wyrazem jest zbiór: $S(N)$. Sekwencja nieskończona spełniająca (*), której ostatnim wyrazem jest $S(N)$ ma więc postać:

$$\varnothing,\ S(\varnothing),\ S(S(\varnothing)),\ S(S(S(\varnothing))),\ \ldots,\ N,\ S(N).$$

Oczywiście zarówno N, jak również $S(N)$ są liczbami porządkowymi niebędącymi liczbami naturalnymi.

Jest jasne, że nie musimy kończyć konstruowanej sekwencji na wyrazie $S(N)$, lecz możemy rozważyć nieskończoną sekwencję o własności (*) bez ostatniego wyrazu, postaci:

$$\varnothing,\ S(\varnothing),\ S(S(\varnothing)),\ S(S(S(\varnothing))),\ \ldots,\ N,\ S(N),\ S(S(N)),\ S(S(S(N))),\ \ldots$$

która wskazuje na nieskończenie wiele liczb porządkowych niebędących liczbami naturalnymi.

Widać wyraźnie, że pojęcie liczby porządkowej jest uogólnieniem teoriomnogościowego pojęcia liczby naturalnej. Formalnie zajmiemy się liczbami porządkowymi w następnych paragrafach.

§2. Zbiory tranzytywne

DEFINICJA. Dowolny zbiór x nazywamy *zbiorem tranzytywnym*, gdy $\forall y(y \in x \Rightarrow y \subseteq x)$. Zbiór jest więc tranzytywny, gdy każdy jego element jest jego podzbiorem.

Na mocy definicji inkluzji zbiorów, warunek definiujący tranzytywność zbioru x można zapisać w postaci: $\forall y(y \in x \Rightarrow \forall z(z \in y \Rightarrow z \in x))$ lub równoważnie: $\forall y \forall z((z \in y \wedge y \in x) \Rightarrow z \in x)$. Z powodu podobieństwa ostatniej formuły do warunku przechodniości dla relacji należenia do zbioru wywodzi się nazwa „tranzytywny” – od ang. *transitive* – przechodni. Często w literaturze przedmiotu zbiór tranzytywny nazywany bywa przechodnim. Na użytek tej monografii odróżnimy jednak pojęcia zbioru tranzytywnego i zbioru przechodniego.

DEFINICJA. Zbiór x nazwiemy *przechodnim*, gdy $\forall y, z, v \in x\ ((y \in z \wedge z \in v) \Rightarrow y \in v)$, czyli gdy relacja należenia do zbioru określona na zbiorze x jest relacją przechodnią.

PRZYKŁAD. Zbiór $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$ jest tranzytywny, lecz nie jest zbiorem przechodnim. Z drugiej strony, każdy singleton jest oczywiście zbiorem przechodnim, lecz niekoniecznie tranzytywnym, na przykład singleton: $\{\{\varnothing\}\}$ nie jest zbiorem tranzytywnym.

Na podstawie Tw. 14, Rozdział 7 mamy: $\forall x \in N(x \subseteq N)$, zatem zbiór liczb naturalnych jest zbiorem tranzytywnym. N jest również zbiorem przechodnim.

W dalszym ciągu okaże się przydatne rozważanie pewnych klas czy mnogości zbiorów, tzn. takich „zespołów” zbiorów, które zbiorami w teorii ZFC nie są. Przykładem takiej klasy zbiorów niebędącej zbiorem (jak później to wykażemy) jest mnogość wszystkich zbiorów tranzytywnych.

Uogólnijmy pojęcia tranzytywności oraz przechodniości zbioru, aby stosowały się one do dowolnego zespołu zbiorów:

Powiemy, że *klasa zbiorów jest tranzytywna*, gdy dowolny ze zbiorów tej klasy jest taki, iż każdy jego element jest również zbiorem z tej klasy.

Powiemy, że *klasa zbiorów jest przechodnia*, gdy dla dowolnych zbiorów x, y, z z tej klasy zachodzi: $(x \in y \wedge y \in z) \Rightarrow x \in z$.

Rozważmy dla przykładu klasę wszystkich zbiorów tranzytywnych. Zbiór $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ (por. przykład powyżej) jest zbiorem z tej klasy, lecz jego element $\{\{\emptyset\}\}$ nie jest zbiorem z tej klasy (tzn. nie jest zbiorem tranzytywnym). Zatem klasa wszystkich zbiorów tranzytywnych nie jest tranzytywna. Jednakże klasa ta jest przechodnia:

TWIERDZENIE 1. *Dla dowolnych zbiorów tranzytywnych* x, y, z, $(x \in y \wedge y \in z) \Rightarrow x \in z$.

DOWÓD. Niech $x \in y$ oraz $y \in z$. Ponieważ z jest tranzytywny, więc $y \subseteq z$, zatem $x \in z$. $\square$

Następujące twierdzenie charakteryzuje pojęcie zbioru tranzytywnego przy użyciu operacji P, $\bigcup$, S:

TWIERDZENIE 2. *Dla dowolnego zbioru x następujące warunki są równoważne:*
(i) *x jest tranzytywny,*
(ii) $x \subseteq P(x)$,
(iii) $\bigcup x \subseteq x$,
(iv) $x = \bigcup S(x)$.

DOWÓD. Równoważność (i) $\Leftrightarrow$ (ii) jest bezpośrednią konsekwencją definicji zbioru tranzytywnego.

(i) $\Rightarrow$ (iii): Załóżmy, że x jest tranzytywny. Niech $y \in \bigcup x$. Wówczas $y \in z$ dla pewnego $z \in x$. Wtedy z założenia $z \subseteq x$, więc $y \in x$.

(iii) $\Rightarrow$ (i): Załóżmy, że $\bigcup x \subseteq x$. Niech $y \in x$. W celu wykazania, że $y \subseteq x$ weźmy $z \in y$. Wówczas $z \in \bigcup x$, zatem z założenia: $z \in x$.

Równoważność (iii) $\Leftrightarrow$ (iv) jest bezpośrednią konsekwencją Tw. 4, Rozdział 7 oraz Tw. 13(3), Rozdział 1. $\square$

Jest oczywiste, że zbiór pusty jest zbiorem tranzytywnym. Okazuje się, że jest on elementem każdego niepustego zbioru tranzytywnego:

TWIERDZENIE 3. *Dla dowolnego niepustego tranzytywnego zbioru* x : $\emptyset \in x$.

DOWÓD. Niech x będzie tranzytywny i niepusty. Na mocy aksjomatu regularności niech y będzie elementem minimalnym zbioru x, tzn. $y \in x$ oraz $y \cap x = \emptyset$. Z tranzytywności zbioru x mamy: $y \subseteq x$, zatem $y \cap x = y$. Ostatecznie $y = \emptyset$, czyli $\emptyset \in x$. $\square$

Twierdzenie 4. *Jeżeli x jest tranzytywny, to $S(x)$ jest tranzytywny.*

Dowód. Załóżmy, że x jest tranzytywny. Na mocy Tw. 2, $x = \bigcup S(x)$, lecz $x \subseteq S(x)$, zatem $\bigcup S(x) \subseteq S(x)$, czyli znowu według Tw. 2, $S(x)$ jest tranzytywny. □

Twierdzenie 5. *Jeżeli x jest tranzytywny, to $\bigcup x$ jest zbiorem tranzytywnym.*

Dowód. Załóżmy, że x jest tranzytywny. Wówczas na mocy Tw. 2, $\bigcup x \subseteq x$. Niech $y \in \bigcup x$. Zatem $y \in x$, skąd (Tw. 11(1), Rozdział 1) $y \subseteq \bigcup x$, co świadczy o tym, że $\bigcup x$ jest zbiorem tranzytywnym. □

Twierdzenie 6. *Dla dowolnego zbioru tranzytywnego x następujące warunki są równoważne:*
(i) $\bigcup x = x$,
(ii) $x \in S(\bigcup x)$,
(iii) $\bigcup S(x) \in S(\bigcup x)$.

Dowód. Równoważność (i) $\Leftrightarrow$ (ii) zachodzi dla dowolnego zbioru x (Tw. 5, Rozdział 7).

Równoważność (ii) $\Leftrightarrow$ (iii) zachodzi dla dowolnego zbioru tranzytywnego x, ponieważ wówczas $x = \bigcup S(x)$ (Tw. 2). □

Twierdzenie 7. *Dla dowolnego zbioru tranzytywnego x,*
$\bigcup x \in x$ *wtw* $S(\bigcup x) \subseteq x$.

Dowód. Jest to bezpośredni wniosek z Tw. 7, Rozdział 7 oraz Tw. 2(i)$\Leftrightarrow$(iv). □

§3. Liczba naturalna jako liczba porządkowa

Definicja. Zbiór x nazywamy *liczbą porządkową*, gdy x jest tranzytywny oraz każdy element zbioru x jest zbiorem tranzytywnym.

Twierdzenie 8. *Zbiór $\varnothing$ jest liczbą porządkową.*

Dowód. Skoro prawdziwa jest formuła $\forall y(y \in \varnothing \Rightarrow y \subseteq \varnothing)$, więc $\varnothing$ jest zbiorem tranzytywnym. Naturalnie również prawdziwa jest formuła $\forall y(y \in \varnothing \Rightarrow y$ jest tranzytywny). Stąd $\varnothing$ jest liczbą porządkową. □

Twierdzenie 9. $\forall x(x$ *jest liczbą porządkową* $\Rightarrow S(x)$ *jest liczbą porządkową*) (*Następnik liczby porządkowej jest liczbą porządkową, lub inaczej: klasa liczb porządkowych jest zamknięta na operację następnika.*)

Dowód. Niech x będzie liczbą porządkową. Wobec Tw. 4 wystarczy wykazać, że każdy element zbioru $S(x)$ jest zbiorem tranzytywnym. Niech $y \in S(x)$. Wówczas $y \in x$ lub $y = x$. Gdy $y \in x$, to wobec założenia, że x jest liczbą porządkową: y jest tranzytywny. Gdy zaś $y = x$, to naturalnie y jest tranzytywny, bo x jest tranzytywny jako liczba porządkowa. □

Twierdzenia 8 oraz 9 stanowią podstawę do sformułowania twierdzenia, iż każda liczba naturalna jest liczbą porządkową:

Twierdzenie 10. $\forall x (x \in N \Rightarrow x$ *jest liczbą porządkową*$)$.

Dowód. Połóżmy w Tw. 13, Rozdział 7 (interpretacja aksjomatu indukcji dla liczb naturalnych) formułę $\psi(x)$ postaci: x jest liczbą porządkową. Wówczas dowodzone twierdzenie jest następnikiem tak uzyskanej implikacji. Jej poprzednik: $\varnothing$ jest liczbą porządkową $\wedge\ \forall x \in N(x$ jest liczbą porządkową $\Rightarrow S(x)$ jest liczbą porządkową), jest prawdziwy na mocy Tw. 8 i Tw. 9. □

Przykład. Zbiór $\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$, choć tranzytywny, nie jest liczbą porządkową. Jego element $\{\{\varnothing\}\}$ nie jest bowiem zbiorem tranzytywnym.

Na mocy Tw. 14, Rozdział 7, zbiór liczb naturalnych N jest tranzytywny, zaś na mocy Tw. 10 każdy element zbioru N jest tranzytywny, zatem N jest liczbą porządkową. Ponadto jest to liczba porządkowa, która nie jest liczbą naturalną (bo $N \notin N$).

§4. Warianty definicyjne dla pojęcia liczby porządkowej

Paragraf ten poświęcimy innym niż definicyjne, lecz równoważnym mu, sformułowaniom pojęcia liczby porządkowej.

Twierdzenie 11. *Dla dowolnego zbioru x, x jest liczbą porządkową wtw x jest tranzytywny i przechodni.*

Dowód. $(\Rightarrow)$: Załóżmy, że x jest liczbą porządkową. Naturalnie x jest wtedy zbiorem tranzytywnym. Ponieważ każdy element zbioru x jest tranzytywny, więc, na mocy Tw. 1, x jest zbiorem przechodnim.

$(\Leftarrow)$: Załóżmy, że x jest zbiorem tranzytywnym i przechodnim. Aby wykazać, że każdy element zbioru x jest tranzytywny, załóżmy, że

(1) $y \in x$ oraz

(2) $z \in y$.

Mamy wykazać, że $z \subseteq y$. Niech więc

(3) $v \in z$.

Z tranzytywności zbioru x oraz (1) wnosimy, iż $y \subseteq x$, zatem z (2) otrzymujemy:
(4) $z \in x$.

Z (4) i z tranzytywności zbioru x mamy: $z \subseteq x$, zatem z (3) uzyskujemy:
(5) $v \in x$.

Ostatecznie z przechodniości zbioru x, na podstawie (5), (4), (1), (3), (2) wnosimy, że $v \in y$. □

Analogicznie jak własność przechodniości zbioru, zdefiniujmy jego spójność:

DEFINICJA. Zbiór x nazywamy *spójnym*, gdy $\forall y, z \in x\ (y \in z \vee z \in y \vee y = z)$.

TWIERDZENIE 12. *Dla dowolnego zbioru x, x jest liczbą porządkową wtw x jest tranzytywny oraz spójny.*

DOWÓD. ($\Leftarrow$): Załóżmy, że x jest tranzytywny i spójny oraz nie wprost, że x nie jest liczbą porządkową. Wówczas istnieje $y \in x$, który nie jest zbiorem tranzytywnym. Czyli dla pewnego zbioru z mamy:
(1) $z \in y$ oraz
(2) $z \nsubseteq y$.

Z tranzytywności zbioru x wynika, że $y \subseteq x$, zatem z (1), $z \in x$, co implikuje:
(3) $z \subseteq x$.

Na mocy (2) istnieje zbiór u taki, że
(4) $u \in z$ oraz
(5) $u \notin y$. Ponadto
(6) $u \neq y$.

Gdyby bowiem $u = y$, to z (4) byłoby: $y \in z$, co wobec (1) i Wniosku z Tw. 10, Rozdział 2, jest niemożliwe.

Na mocy (3) i (4), $u \in x$, zatem y, u są elementami zbioru x, dlatego ze spójności tego zbioru, wobec (5) i (6) otrzymujemy:
(7) $y \in u$.

Lecz (7), (4), (1) wraz z Wnioskiem z Tw. 10, Rozdział 2, prowadzą do sprzeczności.

Implikacja odwrotna do udowodnionej, a dokładniej mówiąc, zdanie „liczba porządkowa jest zbiorem spójnym", okaże się bezpośrednim wnioskiem z następnych twierdzeń tego rozdziału (dla dowodu których Tw. 12 nie jest wykorzystywane). □

Najbardziej istotne poza definicyjnymi, czy też konstytutywne (w sensie, który za chwilę wyjaśnimy) dla klasy liczb porządkowych są dwa warunki, które teraz podamy w postaci Tw. 13 i Tw. 14:

TWIERDZENIE 13. $\forall x(x$ *jest liczbą porządkową* $\Rightarrow \forall y(y \in x \Rightarrow y$ *jest liczbą porządkową*)) (*Każdy element dowolnej liczby porządkowej jest liczbą porządkową.*)

DOWÓD. Niech x będzie liczbą porządkową oraz niech $y \in x$. Wówczas y jest zbiorem tranzytywnym. Aby dowieść, że jest on liczbą porządkową, musimy wykazać, że każdy jego element jest zbiorem tranzytywnym. Niech więc $z \in y$. Ponieważ x jest liczbą porządkową, więc x jest tranzytywny. Skoro więc $y \in x$, to $y \subseteq x$, zatem $z \in x$. Stąd z jest tranzytywny jako element liczby porządkowej. $\square$

TWIERDZENIE 14. *Dla dowolnych liczb porządkowych* x, y, z: $(x \in y \wedge y \in z) \Rightarrow x \in z$.

DOWÓD. Oczywisty na podstawie Tw. 1. $\square$

Oczywiście Tw. 13 można interpretować jako stwierdzenie, iż klasa wszystkich liczb porządkowych jest tranzytywna; natomiast według Tw. 14, klasa ta jest przechodnia. Obecnie wykażemy, że klasa wszystkich liczb porządkowych jest największą tranzytywną i przechodnią klasą zbiorów.

Niech $W(x)$ będzie formułą języka ZFC z dokładnie jedną zmienną wolną x, dla której spełnione są dwa warunki:

(war1) $\forall x(W(x) \Rightarrow \forall y(y \in x \Rightarrow W(y))$,

(war2) $\forall x \forall y \forall z(W(x) \wedge W(y) \wedge W(z) \Rightarrow (x \in y \wedge y \in z \Rightarrow x \in z))$.

Predykat 1-argumentowy W reprezentuje własność przysługującą zbiorom. Według (war1) jeżeli własność ta przysługuje danemu zbiorowi, to przysługuje ona każdemu elementowi tego zbioru. Według (war2) relacja należenia do zbioru $\in$ jest przechodnia na klasie wszystkich takich zbiorów x, że $W(x)$.

Nigdzie nie zakładamy, że istnieje zbiór postaci: $\{x : W(x)\}$, gdzie $W(x)$ spełnia (war1), (war2). Jednakże będziemy mówić o klasie czy mnogości takich zbiorów x, że $W(x)$. Jest jasne, że według (war1) taka klasa jest tranzytywna, zaś zgodnie z (war2), klasa zbiorów x takich, że $W(x)$ jest przechodnia.

Gdyby jednak istniał dla jakiejś formuły $W(x)$, zbiór $A = \{x : W(x)\}$, to, jak widać, (war1) byłby równoważny stwierdzeniu: $\forall x(x \in A \Rightarrow \forall y(y \in x \Rightarrow y \in A))$, czyli $\forall x(x \in A \Rightarrow x \subseteq A)$, co jest równoważne temu, że A jest zbiorem tranzytywnym. Z kolei (war2) jest wówczas równoważny stwierdzeniu, że zbiór A jest przechodni.

W ten sposób, wobec Tw. 11, uzyskaliśmy przykład formuły $W(x)$, dla której zachodzą (war1) i (war2). Wystarczy mianowicie za $W(x)$ przyjąć „$x \in A$", dla jakiejkolwiek liczby porządkowej A. W szczególności więc, dla liczby porządkowej

$N = \{x : x$ jest liczbą naturalną$\}$. Zatem dla $W(x)$ postaci: „x jest liczbą naturalną”, warunki (war1), (war2) są prawdziwe (oczywiście tutaj warunek (war1) to Tw. 14, Rozdział 7).

Na mocy Tw. 13 oraz Tw. 14 widać, że dla formuły $W(x)$ postaci: „x jest liczbą porządkową”, warunki (war1) oraz (war2) są prawdziwe. Wykażemy, że klasa wszystkich liczb porządkowych, tzn. klasa tych wszystkich x, że $W(x)$, gdzie $W(x)$ jest postaci: „x jest liczbą porządkową”, jest największą ze wszystkich klas zbiorów x takich, że $W(x)$, gdzie W jest dowolną własnością spełniającą (war1), (war2). Innymi słowy, wykażemy, że klasa wszystkich liczb porządkowych jest największą tranzytywną i przechodnią klasą zbiorów.

W tym celu wykazujemy, że dla dowolnej formuły $W(x)$, dla której spełnione są (war1), (war2) zachodzi:

(*) $\forall x(W(x) \Rightarrow x$ jest liczbą porządkową$)$.

Dowodzimy najpierw, że

(1) $\forall x(W(x) \Rightarrow x$ jest tranzytywny$)$.

Załóżmy nie wprost, że dla pewnego x prawdą jest, że $W(x)$ oraz x nie jest tranzytywny, co oznacza, że dla pewnego $y \in x : \ y \nsubseteq x$; zatem istnieje z takie, że $z \in y$ oraz $z \notin x$. Na mocy (war1) mamy $W(y)$ i konsekwentnie $W(z)$. Wówczas z (war2) skoro $z \in y$ oraz $y \in x$, więc $z \in x$. Sprzeczność.

Pozostaje dowieść:

(2) $\forall x(W(x) \Rightarrow \forall y(y \in x \Rightarrow y$ jest tranzytywny$))$.

Załóżmy nie wprost, że dla pewnych x, y jest tak, że $W(x)$, $y \in x$ oraz y nie jest tranzytywny. Na mocy (war1) mamy: $W(y)$, zatem dalej rozumowanie przebiega tak samo jak w dowodzie dla (1) tyle, że dla zbioru y nie x.

Oczywiście (1) i (2) bezpośrednio implikują (*).

Warunek (*) ma jednoznaczną wymowę: dowolna klasa zbiorów x takich, że $W(x)$, dla W spełniającego warunki (war1), (war2), a więc dowolna klasa zbiorów tranzytywna i przechodnia, jest mnogością liczb porządkowych. Stąd oraz na podstawie faktu, że mnogość wszystkich liczb porządkowych sama jest przecież klasą tranzytywną i przechodnią, wynika, iż jest ona największą (w sensie zawierania) spośród wszystkich tranzytywnych i przechodnich klas zbiorów.

Na podstawie powyższych rozważań jasne jest, że warunki (war1), (war2) charakteryzują pojęcie liczby porządkowej w następujący sposób:

Twierdzenie 15. *Dla dowolnego zbioru z, z jest liczbą porządkową wtw istnieje formuła $W(x)$ (z dokładnie jedną zmienną wolną x) spełniająca* (war1), (war2) *taka, że zachodzi $W(z)$.*

Dowód. ($\Rightarrow$): na mocy Tw. 13, Tw. 14 ($W(x)$ ma postać: „x jest liczbą porządkową”).

($\Leftarrow$): na mocy (*). $\square$

Inaczej mówiąc, to właśnie Twierdzenia 13, 14 konstytuują pojęcie liczby porządkowej, w takim oto sensie: możemy je traktować jako aksjomatyczną definicję klasy liczb porządkowych (precyzyjniej – predykatu „jest liczbą porządkową”).

Okazuje się, że tę definicję można zmodyfikować, analogicznie jak Tw. 12 jest modyfikacją charakterystyki pojęcia liczby porządkowej podanej w Tw. 11, tzn. zamienić Tw. 14 (warunek (war2)) mówiące, że klasa wszystkich liczb porządkowych jest przechodnia, na warunek stwierdzający, że klasa wszystkich liczb porządkowych jest spójna. Wcześniej naturalnie należy uogólnić pojęcie spójności zbioru do pojęcia spójności dowolnej mnogości zbiorów:

powiemy, że klasa (mnogość) zbiorów jest *spójna*, gdy dla dowolnych zbiorów x, y z tej klasy zachodzi: $x \in y$ lub $y \in x$ lub $x = y$.

W dalszym ciągu (lecz dopiero w §6), udowodnimy, że Tw. 13 i Tw. 14 implikują spójność klasy wszystkich liczb porządkowych. W dowodzie tym wymagane jest zastosowanie jednego z najważniejszych twierdzeń teorii liczb porządkowych, jakim jest twierdzenie o indukcji pozaskończonej (któremu wobec tego wcześniej musimy poświęcić uwagę (§5)). Twierdzenie to jest bezpośrednią konsekwencją Twierdzeń 13, 14.

Natomiast obecnie pokażemy, że spójność dowolnej klasy zbiorów implikuje przechodniość tej klasy:

Twierdzenie 16. *Warunek:*
(war3) $\forall x \forall y((W(x) \wedge W(y)) \Rightarrow (x \in y \vee y \in x \vee x = y))$
implikuje warunek (war2).

Dowód. Załóżmy (war3) oraz nie wprost, że (war2) nie zachodzi, czyli dla pewnych zbiorów x, y, z takich, że $W(x), W(y), W(z)$ mamy:
(1) $x \in y$,
(2) $y \in z$,
(3) $x \notin z$.

Wówczas zachodzi również
(4) $x \neq z$.

Gdyby bowiem $x = z$, to na mocy (2) byłoby: $y \in x$, co wraz z (1) i Wnioskiem z Tw. 10, Rozdział 2, dałoby sprzeczność.

Na mocy (war3) z (3) i (4) otrzymujemy: $z \in x$ co wraz z (1) i (2) daje cykl: $x \in y \in z \in x$, zabroniony na mocy Wniosku z Tw. 10, Rozdział 2. $\square$

§5. Twierdzenie o indukcji pozaskończonej

Dla klasy zbiorów x takich, że $W(x)$, gdzie $W(x)$ spełnia (war1), (war2), oraz dla dowolnej formuły $\phi(x)$ języka ZFC z przynajmniej jedną wolną zmienną x zachodzi twierdzenie:

(**) $\forall x[W(x) \Rightarrow (\forall y(y \in x \Rightarrow \phi(y)) \Rightarrow \phi(x))] \Rightarrow \forall x(W(x) \Rightarrow \phi(x))$

(jeżeli dla dowolnego zbioru x z tej klasy zachodzi $\phi(x)$, o ile ϕ jest spełnione dla każdego elementu zbioru x, to $\phi(x)$ zachodzi dla wszystkich x z tej klasy).

Intuicyjność tego twierdzenia jest widoczna w przypadku, gdy ograniczymy je do klasy (zbioru) liczb naturalnych:

($**N$) $\forall x[x \in N \Rightarrow (\forall y(y \in x \Rightarrow \phi(y)) \Rightarrow \phi(x))] \Rightarrow \forall x(x \in N \Rightarrow \phi(x))$.

Ograniczymy się do udowodnienia twierdzenia (**) dla jednej postaci formuły $W(x)$: x jest liczbą porządkową, czyli dla największej klasy zbiorów x takich, że $W(x)$, dla $W(x)$ spełniającego (war1), (war2). Korzystać będziemy w tym dowodzie wyłącznie z Tw. 13 i Tw. 14, czyli z warunków (war1) i (war2) dla tej specjalnej postaci formuły $W(x)$. Każdy łatwo odtworzy dowód ogólnego twierdzenia (**) w oparciu o te warunki, na podstawie poniższego dowodu.

TWIERDZENIE O INDUKCJI POZASKOŃCZONEJ.
$\forall x[x$ *jest liczbą porządkową* $\Rightarrow (\forall y(y \in x \Rightarrow \phi(y)) \Rightarrow \phi(x))] \Rightarrow$
$\forall x(x$ *jest liczbą porządkową* $\Rightarrow \phi(x))$.

DOWÓD. Załóżmy poprzednik dowodzonej implikacji oraz nie wprost niech a będzie taką liczbą porządkową, że $\neg\phi(a)$. Na mocy aksjomatu podzbiorów, skoro prawdą jest:
$\forall x((x \in a \wedge \neg\phi(x)) \Rightarrow x \in a)$, więc
$\exists y \forall x(x \in y \Leftrightarrow (x \in a \wedge \neg\phi(x)))$.

Zatem niech b będzie takim zbiorem, że

(1) $\forall x(x \in b \Leftrightarrow (x \in a \wedge \neg\phi(x)))$.

Wówczas oczywiście:

(2) $b \neq \varnothing$ wtw $\exists y(y \in a \wedge \neg\phi(y))$.

Z założenia, ponieważ a jest liczbą porządkową, więc: $\forall y(y \in a \Rightarrow \phi(y)) \Rightarrow \phi(a)$. Jednakże $\neg\phi(a)$, zatem $\exists y(y \in a \wedge \neg\phi(y))$, co na mocy (2) daje: $b \neq \varnothing$. Niech więc na mocy aksjomatu regularności, c będzie elementem minimalnym zbioru b. Wówczas z (1) mamy:
(3) $c \in a$ oraz
(4) $\neg\phi(c)$.

Ponieważ a jest liczbą porządkową, więc na mocy (3) oraz Tw. 13, c jest również liczbą porządkową. Zatem na mocy założenia oraz (4), postępując analogicznie jak poprzednio dla liczby porządkowej a, otrzymujemy:
(5) $\exists y(y \in c \wedge \neg\phi(y))$.

Mamy więc d takie, że
(6) $d \in c$ oraz
(7) $\neg\phi(d)$.

Na mocy (6) i Tw. 13, d jest liczbą porządkową, zatem według (3),(6) i Tw. 14, $d \in a$. Ostatecznie na mocy (7) i (1), $d \in b$, czyli $d \in c \cap b$, skąd $c \cap b \neq \varnothing$, co jednak jest niemożliwe, bo c jest elementem minimalnym zbioru b. □

§6. Spójność relacji ∈ oraz relacja inkluzji dla liczb porządkowych

Jedną z ważnych konsekwencji twierdzenia o indukcji pozaskończonej, a więc konsekwencji Tw. 13 i Tw. 14, jest własność spójności relacji $\in$ na klasie liczb porządkowych; innymi słowy, klasa wszystkich liczb porządkowych jest spójna:

TWIERDZENIE 17. *Dla dowolnych liczb porządkowych* x, z, $x = z \vee x \in z \vee z \in x$.

DOWÓD. Dowodzimy formuły:
$\forall x[x$ jest liczbą porządkową $\Rightarrow \forall z(z$ jest liczbą porządkową $\Rightarrow (x = z \vee x \in z \vee z \in x))]$,
korzystając z twierdzenia o indukcji pozaskończonej, gdzie formuła $\phi(x)$ jest postaci:
(1) $\forall z(z$ jest liczbą porządkową $\Rightarrow (x = z \vee x \in z \vee z \in x))$.

Wystarczy więc wykazać poprzednik w twierdzeniu o indukcji pozaskończonej:
$\forall x[x$ jest liczbą porządkową $\Rightarrow (\forall y(y \in x \Rightarrow \phi(y)) \Rightarrow \phi(x))]$.

Załóżmy więc, że x jest liczbą porządkową oraz
(2) $\forall y(y \in x \Rightarrow \phi(y))$.

Mamy wykazać, że $\phi(x)$. W tym celu zapiszmy $\phi(x)$ z (1) w postaci:
(3) $\forall z(z$ jest liczbą porządkową $\Rightarrow \psi(z))$,
gdzie $\psi(z) :=\ x = z \vee x \in z \vee z \in x$. Lecz (3) jest następnikiem w twierdzeniu o indukcji pozaskończonej postaci:
(4) $\forall z[z$ jest liczbą porządkową $\Rightarrow (\forall y(y \in z \Rightarrow \psi(y)) \Rightarrow \psi(z))] \Rightarrow$
$\forall z(z$ jest liczbą porządkową $\Rightarrow \psi(z))$.

Aby zatem uzyskać (3), dowiedźmy poprzednik implikacji (4), tzn. wykazujemy:
(5) $\forall z[z$ jest liczbą porządkową $\Rightarrow (\forall y(y \in z \Rightarrow \psi(y)) \Rightarrow \psi(z))]$.

Załóżmy zatem, że z jest liczbą porządkową oraz
(6) $\forall y(y \in z \Rightarrow \psi(y))$.

Aby wykazać $\psi(z)$, czyli formułę: $x = z \vee x \in z \vee z \in x$, załóżmy, że $x \neq z$. Wówczas, na mocy Tw. 2, Rozdział 1:
(7) $x \nsubseteq z \vee z \nsubseteq x$.

Niech alternatywa (7) będzie prawdziwa w ten sposób, iż $x \nsubseteq z$ jest prawdziwe. Wówczas dla pewnego c mamy
(8) $c \in x$ oraz
(9) $c \notin z$.

Z (8) i (2) mamy natychmiast: $\phi(c)$. Stąd (zob. postać (1)), odłączając kwantyfikator dla wziętej wcześniej liczby porządkowej z, mamy: $c = z \vee c \in z \vee z \in c$. Zatem na mocy (9), $c = z$ lub $z \in c$. Niech $c = z$. Wówczas z (8) otrzymujemy: $z \in x$, skąd konsekwentnie: $x \in z \vee z \in x$. Niech teraz $z \in c$. Na mocy (8) oraz Tw. 13, c jest liczbą porządkową, zatem $z \in x$ zgodnie z (8) i Tw. 14. Konsekwentnie, $x \in z \vee z \in x$.

Teraz wykazujemy, że $x \in z \vee z \in x$ zakładając drugi człon alternatywy (7). Wówczas dla pewnego d,
(10) $d \in z$ oraz
(11) $d \notin x$.

Na mocy (10) i (6) mamy: $\psi(d)$, tzn. $x = d \vee x \in d \vee d \in x$. Z (11), $x = d$ lub $x \in d$. Niech $x = d$. Wówczas z (10), $x \in z$, co daje alternatywę: $x \in z \vee z \in x$. Niech teraz $x \in d$. Ponieważ z jest liczbą porządkową, więc na mocy Tw. 13 oraz (10), d jest liczbą porządkową. Zatem na mocy Tw. 14 oraz (10), $x \in z$, co znowu prowadzi do: $x \in z \vee z \in x$. □

Jest oczywiste, że Tw. 17 można wzmocnić do stwierdzenia:

dla dowolnych liczb porządkowych x, z, *albo* $x = z$ *albo* $x \in z$ *albo* $z \in x$,

tzn. dokładnie jeden z członów alternatywy z Tw. 17 jest prawdziwy dla dowolnych liczb porządkowych x, z.

Jest jasne, że nie tylko Tw. 13 i Tw. 14 implikują Tw. 17, lecz ponadto, na mocy Tw. 16 zastosowanego dla predykatu W postaci „jest liczbą porządkową", Tw. 17 implikuje Tw. 14. Oznacza to, że koniunkcja Twierdzeń 13, 14 (tzn. aksjomatyczna definicja liczby porządkowej) jest równoważna koniunkcji Twierdzeń 13, 17.

Skądinąd jest również oczywiste, że dowód Tw. 17 w oparciu o Twierdzenia 13, 14 (pośrednio w oparciu o twierdzenie o indukcji pozaskończonej) można przełożyć na dowód warunku (war3) z Tw. 16 w oparciu o warunki (war1), (war2) (pośrednio w oparciu o twierdzenie (**)). Skoro więc warunki (war1), (war2) implikują (war3), to stosując te warunki dla fomuły $W(x)$ postaci: $x \in A$, uzyskujemy twierdzenie:

dowolny zbiór tranzytywny i przechodni jest zbiorem spójnym,

skąd, na mocy Tw. 11, uzyskujemy implikację:

dowolna liczba porządkowa jest zbiorem spójnym – por. Tw. 12 i uwagę po pierwszej części jego dowodu.

Jedną z konsekwencji aksjomatu regularności jest to, że relacja $\in$ na mnogości liczb porządkowych (skoro na klasie wszystkich zbiorów) ma własność przeciwzwrotności. Tw. 14 wskazuje na własność przechodniości. Stąd, według Tw. 6(1), Rozdział 3, relacja, w jakiej są dwie liczby porządkowe x, y wówczas, gdy $x \in y \vee x = y$, jest stosunkiem o własnościach częściowego porządku. Okazuje się, iż ów stosunek jest po prostu relacją inkluzji:

TWIERDZENIE 18. *Dla dowolnych liczb porządkowych x, y : $(x \in y$ lub $x = y)$ wtw $x \subseteq y$ (inaczej: $x \in S(y) \Leftrightarrow x \subseteq y$).*

DOWÓD. Niech x, y będą liczbami porządkowymi.

($\Rightarrow$): Załóżmy, że $x \in y$ lub $x = y$. Niech $x \in y$. Ponieważ y jest tranzytywny, więc $x \subseteq y$. Gdy zaś $x = y$, to naturalnie $x \subseteq y$.

($\Leftarrow$): Załóżmy, że $x \subseteq y$ oraz nie wprost niech $x \notin y$ oraz $x \neq y$. Z Tw. 17 mamy natychmiast: $y \in x$. Ponieważ x jest tranzytywny, więc $y \subseteq x$, co wraz z założeniem prowadzi do równości: $x = y$. Sprzeczność. $\square$

WNIOSEK. *Dla dowolnych liczb porządkowych x, y, $x \in y$ wtw $(x \subseteq y \wedge x \neq y)$.*

DOWÓD. Niech x, y będą dowolnymi liczbami porządkowymi.

($\Rightarrow$): Załóżmy, że $x \in y$. Wówczas z Tw. 18: $x \subseteq y$. Oczywiście $x \neq y$. Gdyby bowiem $x = y$, to byłoby: $x \in x$, co jest niemożliwe.

($\Leftarrow$): oczywisty na mocy Tw. 18. $\square$

Na podstawie Tw. 17 i Tw. 18 jasne jest, że relacja inkluzji ograniczona do klasy wszystkich liczb porządkowych ma własność spójności: dla dowolnych liczb porządkowych x, y : $x \subseteq y$ lub $y \subseteq x$ lub $x = y$. Jak widać, relacja $\subseteq$ na klasie wszystkich liczb porządkowych jest liniowo porządkująca. Ponadto, okazuje się, że klasa wszystkich liczb porządkowych z relacją inkluzji ma własność dobrego uporządkowania, co będzie pokazane w kolejnym paragrafie.

§7. Najmniejsza liczba porządkowa x taka, że $\phi(x)$

Rozważmy dowolną formułę $\phi(x)$ języka ZFC, w której x jest zmienną wolną oraz wszystkie te liczby porządkowe x, dla których spełnione jest $\phi(x)$. Gdyby istniał zbiór: $A = \{x : x \text{ jest liczbą porządkową} \wedge \phi(x)\}$, wówczas najmniejszy element w zbiorze częściowo uporządkowanym $<A, \subseteq>$ nazwalibyśmy zasadnie najmniejszą liczbą porządkową x taką, że $\phi(x)$. W ogólności nie mamy gwarancji istnienia takiego zbioru A dla dowolnej formuły $\phi(x)$ (np. gdy $\phi(x)$ ma postać „x jest liczbą naturalną", to zbiór A istnieje, jest nim zbiór N). Jednakże pojęcie najmniejszej liczby porządkowej x takiej, że $\phi(x)$ można wysłowić niezależnie od istnienia owego zbioru A, podając stosowne warunki definicyjne dla najmniejszego elementu w zbiorze częściowo uporządkowanym:

Definicja. Niech $\phi(x)$ będzie dowolną formułą języka ZFC, w której x jest zmienną wolną. Mówimy, że liczba porządkowa x_0 jest *najmniejszą liczbą porządkową x taką, że $\phi(x)$* wtw $\phi(x_0) \wedge \forall y[(y \text{ jest liczbą porządkową} \wedge \phi(y)) \Rightarrow x_0 \subseteq y]$.

Twierdzenie 19. *Niech x_0 będzie dowolną liczbą porządkową oraz $\phi(x)$ – formułą. Następujące warunki są równoważne*:

(i) *x_0 jest najmniejszą liczbą porządkową x taką, że $\phi(x)$*,

(ii) $\phi(x_0) \wedge \forall y[(y \text{ jest liczbą porządkową} \wedge y \neq x_0 \wedge \phi(y)) \Rightarrow x_0 \in y]$,

(iii) $\phi(x_0) \wedge \forall y(y \in x_0 \Rightarrow \neg\phi(y))$.

Dowód. (i) $\Rightarrow$ (ii): Załóżmy, że x_0 jest najmniejszą liczbą porządkową x taką, że $\phi(x)$. Wówczas naturalnie mamy: $\phi(x_0)$. Załóżmy, że y jest liczbą porządkową taką, że $y \neq x_0$ oraz $\phi(y)$. Wówczas z założenia, $x_0 \subseteq y$ i konsekwentnie na mocy Tw. 18, $x_0 \in y$ lub $x_0 = y$. Ponieważ z założenia drugi człon alternatywy nie zachodzi, więc $x_0 \in y$.

(ii) $\Rightarrow$ (i): Załóżmy (ii) oraz niech y jest liczbą porządkową taką, że $\phi(y)$. Oczywiście $x_0 = y$ lub $x_0 \neq y$. Gdy $x_0 = y$, to naturalnie $x_0 \subseteq y$. Gdy zaś $x_0 \neq y$, to na mocy (ii), $x_0 \in y$. Zatem według Tw. 18, $x_0 \subseteq y$.

(ii) $\Rightarrow$ (iii): Załóżmy (ii) oraz nie wprost niech dla pewnego y_0 : $y_0 \in x_0$ oraz $\phi(y_0)$. Skoro $y_0 \in x_0$ zaś x_0 jest liczbą porządkową, więc y_0 jest również liczbą porządkową. Ponieważ $x_0 \neq y_0$ ($x_0 = y_0$ implikuje $y_0 \in y_0$, co jest niemożliwe), więc na mocy (ii), $x_0 \in y_0$. Istniałby zatem cykl: $x_0 \in y_0, y_0 \in x_0$, co jest niemożliwe.

(iii) $\Rightarrow$ (ii): Załóżmy (iii). Weźmy liczbę porządkową y taką, że $y \neq x_0$ oraz $\phi(y)$. Gdyby $y \in x_0$, to na podstawie (iii) byłoby: $\neg\phi(y)$. Zatem $y \notin x_0$. Ostatecznie, na mocy Tw. 17, $x_0 \in y$. $\square$

Twierdzenie 20. *Dla dowolnej formuły $\phi(x)$ istnieje co najwyżej jedna najmniejsza liczba porządkowa x taka, że $\phi(x)$.*

Dowód. Załóżmy, że x_0, x_1 są najmniejszymi liczbami porządkowymi x takimi, że $\phi(x)$. Wówczas z definicji najmniejszej liczby porządkowej x takiej, że $\phi(x)$ otrzymujemy:

(1) $\phi(x_0) \wedge \forall y(y$ jest liczbą porządkową $\wedge\ \phi(y) \Rightarrow x_0 \subseteq y)$ oraz

(2) $\phi(x_1) \wedge \forall y(y$ jest liczbą porządkową $\wedge\ \phi(y) \Rightarrow x_1 \subseteq y)$.

Wówczas z (1) mamy: $x_0 \subseteq x_1$, z (2) zaś: $x_1 \subseteq x_0$. Ostatecznie $x_0 = x_1$. $\square$

Fakt, że relacja inkluzji jest na klasie wszystkich liczb porządkowych relacją liniowo porządkującą, oraz poniższe twierdzenie, świadczą o tym, iż klasa ta jest przez relację inkluzji dobrze uporządkowana.

Twierdzenie 21. *Jeżeli istnieje liczba porządkowa x, dla której zachodzi $\phi(x)$, to istnieje najmniejsza liczba porządkowa x taka, że $\phi(x)$.*

Dowód. Udowodnimy transpozycję: jeżeli nie istnieje najmniejsza liczba porządkowa x taka, że $\phi(x)$, to $\forall x(x$ jest liczbą porządkową $\Rightarrow \neg\phi(x))$. Załóżmy więc, że nie istnieje najmniejsza liczba porządkowa x taka, że $\phi(x)$, co na mocy Tw. 19(i)$\Leftrightarrow$(iii) oznacza, iż $\neg\exists x[x$ jest liczbą porządkową $\wedge\ \phi(x)\ \wedge\ \forall y(y \in x \Rightarrow \neg\phi(y))]$, równoważnie:

(1) $\forall x[(x$ jest liczbą porządkową $\wedge\ \phi(x)) \Rightarrow \exists y(y \in x \wedge\ \phi(y))]$.

Następnik dowodzonej implikacji jest, jak widać, również następnikiem w twierdzeniu o indukcji pozaskończonej dla formuły ze zmienną wolną x postaci: $\neg\phi(x)$. Wystarczy więc pokazać następujący poprzednik w tym twierdzeniu:

(2) $\forall x[x$ jest liczbą porządkową $\Rightarrow (\forall y(y \in x \Rightarrow \neg\phi(y)) \Rightarrow \neg\phi(x))]$.

Załóżmy nie wprost, że (2) nie zachodzi. Wówczas dla pewnej liczby porządkowej x_0 mamy:

(3) $\forall y(y \in x_0 \Rightarrow \neg\phi(y))$ oraz

(4) $\phi(x_0)$.

Wtedy z (1) oraz (4) otrzymujemy: $\exists y(y \in x_0 \wedge \phi(y))$. Stąd dla pewnego a, $a \in x_0$ oraz $\phi(a)$ co daje sprzeczność z (3). $\square$

Jako przykład zastosowania pojęcia najmniejszej liczby porządkowej x takiej, że $\phi(x)$ udowodnimy następujące

Twierdzenie 22. *Zbiór $\varnothing$ jest najmniejszą liczbą porządkową (precyzyjnie choć przesadnie: zbiór $\varnothing$ jest najmniejszą liczbą porządkową x taką, że x jest liczbą porządkową).*

DOWÓD. Na mocy Tw. 8 oraz definicji najmniejszej liczby porządkowej x takiej, że $\phi(x)$, gdzie $\phi(x)$ ma postać: x jest liczbą porządkową. $\square$

TWIERDZENIE 23. $\forall x(x$ *jest liczbą porządkową* $\wedge\ x \neq \emptyset \Rightarrow \emptyset \in x)$.

DOWÓD. Na podstawie Tw. 3 lub na podstawie Tw. 22 i Tw. 19(i)$\Leftrightarrow$(ii). $\square$

Rozdział 9. Zbiory liczb porządkowych. Liczby porządkowe izolowane i graniczne

§1. Kresy względem $\subseteq$ dowolnego zbioru liczb porządkowych

Poświęcimy teraz uwagę przede wszystkich kratowym własnościom klasy wszystkich liczb porządkowych. Według Tw. 14, Rozdział 5, każdy zbiór dobrze uporządkowany z elementem największym jest kratą zupełną. Naturalnie nie zamierzamy twierdzić, że klasa wszystkich liczb porządkowych wraz z relacją inkluzji jest kratą zupełną, i to nie tylko z tego powodu, że klasa ta nie jest zbiorem (można by przecież, wykraczając poza teorię ZFC, odpowiednio uogólnić pojęcie kraty zupełnej, aby stosowało się ono do wszelkich mnogości zbiorów), lecz dlatego, iż w klasie wszystkich liczb porządkowych nie ma elementu największego, tzn. nie ma takiej liczby porządkowej, w której każda liczba porządkowa się zawiera. Gdyby bowiem taka liczba istniała, to jej następnik, będący na mocy Tw. 9, Rozdział 8 liczbą porządkową, zawierałby się w niej, zatem, wobec przeciwnej inkluzji, byłby jej równy, co jest niemożliwe.

Jednakże pokażemy, że dla dowolnego niepustego zbioru (nie jakiejkolwiek mnogości, lecz właśnie zbioru) liczb porządkowych, w klasie wszystkich liczb porządkowych uporządkowanej relacją inkluzji istnieją jego kresy dolny i górny, tzn. wykażemy, że dla dowolnego niepustego zbioru z liczb porządkowych istnieją takie liczby porządkowe a, b, że

$\forall y \in z,\ a \subseteq y,$
$\forall x[x \text{ jest liczbą porządkową } \Rightarrow\ ((\forall y \in z,\ x \subseteq y) \Rightarrow x \subseteq a)],$
(wtedy właśnie $a = \inf z$) oraz

$\forall y \in z,\ y \subseteq b,$
$\forall x[x \text{ jest liczbą porządkową } \Rightarrow\ ((\forall y \in z,\ y \subseteq x) \Rightarrow b \subseteq x)]$
(wtedy $b = \sup z$).

Rozważmy dowolny niepusty zbiór z liczb porządkowych oraz formułę $\phi(x)$ postaci: $x \in z$. Wówczas na mocy Tw. 21, Rozdział 8 istnieje najmniejsza liczba porządkowa x taka, że $x \in z$, czyli najmniejsza liczba porządkowa w zbiorze z. Na mocy Tw. 20, Rozdział 8 wprowadźmy jednoargumentową operację *nlp* przyporządkowującą każdemu niepustemu zbiorowi z liczb porządkowych najmniejszą liczbę porządkową w zbiorze z. Wówczas z definicji najmniejszej liczby porządkowej x takiej, że $\phi(x)$ mamy: $nlp(z) \in z$ oraz $\forall y \in z$, $nlp(z) \subseteq y$, co natychmiast prowadzi do konkluzji: $nlp(z) = \inf z$.

Jest oczywiste na podstawie Tw. 23, Rozdział 8, że w przypadku, gdy z jest liczbą porządkową (niepustą), $nlp(z) = \varnothing$.

Uwaga. Wprowadzamy operację *nlp* w celu zaznaczenia, że term „$nlp(z)$” nazywa pewną liczbę porządkową. Można by nie wprowadzać do teorii tej operacji, lecz wyrażać najmniejszą liczbę porządkową w danym zbiorze w inny, skądinąd znany sposób. Mianowicie, skoro $nlp(z) \in z$, więc na mocy Tw. 18(1), Rozdział 1, $\bigcap z \subseteq nlp(z)$. Skoro zaś $\forall y \in z,\ nlp(z) \subseteq y$, to zgodnie z Tw. 18(2), Rozdział 1, $nlp(z) \subseteq \bigcap z$. Ostatecznie $nlp(z) = \bigcap z$.

Naturalnie dla dowolnego niepustego zbioru z liczb porządkowych (w szczególności dla niepustej liczby porządkowej), zbiór częściowo uporządkowany $<z, \subseteq>$ jest dobrze uporządkowany (dla dowolnego niepustego $y \subseteq z$, $nlp(y)$ jest elementem najmniejszym w $<y, \subseteq>$).

Zwróćmy jeszcze uwagę na to, iż operacja *nlp* ma, na mocy Tw. 19(i)$\Leftrightarrow$(iii), Rozdział 8, następującą własność: $nlp(z) \in z \wedge \forall y(y \in nlp(z) \Rightarrow y \notin z)$, co świadczy o tym, iż $nlp(z)$ jest elementem minimalnym zbioru z. Co więcej, jak mówi o tym następne twierdzenie, jest to jedyny element minimalny zbioru z:

TWIERDZENIE 1. *Dla dowolnego niepustego zbioru z liczb porządkowych oraz dowolnej liczby porządkowej y, y jest elementem minimalnym zbioru z wtw $y = nlp(z)$.*

DOWÓD. Niech z będzie zbiorem liczb porządkowych oraz y – liczbą porządkową.

($\Rightarrow$): Załóżmy, że

(1) $y \in z$ oraz

(2) $y \cap z = \varnothing$.

Rozważmy dowolny $x \in z$. Wówczas z (2): $x \notin y$. Stąd, ponieważ x, y są liczbami porządkowymi, na mocy Twierdzeń 17 i 18, Rozdział 8, otrzymujemy: $y \subseteq x$. Ostatecznie, wobec (1) i dowolności wyboru zbioru x ze zbioru z, $y = nlp(z)$.

($\Leftarrow$): oczywisty. □

Aby opisać kres górny dowolnego zbioru liczb porządkowych, rozważmy sumę tego zbioru:

TWIERDZENIE 2. *Suma dowolnego zbioru liczb porządkowych jest liczbą porządkową.*

DOWÓD. Niech z będzie zbiorem liczb porządkowych.

Wykazujemy, że $\bigcup z$ jest zbiorem tranzytywnym. Niech więc $x \in \bigcup z$. Wówczas dla pewnego a, $a \in z$ oraz $x \in a$. Aby wykazać, że $x \subseteq \bigcup z$ rozważmy $y \in x$.

Z założenia a jest liczbą porządkową, zatem na mocy Tw. 13, Rozdział 8, x jest liczbą porządkową, a więc konsekwentnie, również y jest liczbą porządkową. Na mocy Tw. 14, Rozdział 8 mamy zatem: $y \in a$. Ostatecznie, z definicji sumy, $y \in \bigcup z$.

Wykazujemy, że $\forall x(x \in \bigcup z \Rightarrow x$ jest tranzytywny$)$. Niech więc $x \in \bigcup z$. Wówczas $x \in a$ oraz $a \in z$ dla pewnego a. Na mocy założenia, a jest liczbą porządkową, więc skoro $x \in a$, to x jest tranzytywny. $\square$

WNIOSEK. $\forall x(x$ *jest liczbą porządkową* $\Rightarrow \bigcup x$ *jest liczbą porządkową*$)$ (*suma liczby porządkowej jest liczbą porządkową*).

DOWÓD. Niech x będzie liczbą porządkową. Na mocy Tw. 13, Rozdział 8, x jest zbiorem liczb porządkowych, zatem na mocy Tw. 2, $\bigcup x$ jest liczbą porządkową. $\square$

Skoro dla dowolnego zbioru z liczb porządkowych, $\bigcup z$ jest liczbą porządkową oraz na mocy Twierdzeń 11(1), 11(2) z Rozdziału 1, mamy:

(1) $\forall y \in z,\ y \subseteq \bigcup z$ oraz

(2) $\forall x[x$ jest liczbą porządkową $\Rightarrow ((\forall y \in z, y \subseteq x) \Rightarrow \bigcup z \subseteq x)]$,

więc $\bigcup z = \sup z$.

Zauważmy ponadto, że według Tw. 18, Rozdział 8, warunek (1) jest równoważny wyrażeniu $\forall y \in z,\ y \in S(\bigcup z)$, które z kolei jest równoważne formule:

(1)′ $z \subseteq S(\bigcup z)$.

Rozumując analogicznie stwierdzamy, że (2) jest równoważne wyrażeniu:

(2)′ $\forall x[x$ jest liczbą porządkową $\Rightarrow (z \subseteq S(x) \Rightarrow \bigcup z \subseteq x)]$.

Bezpośrednią konsekwencją (1)′ i (2)′ oraz Tw. 2 jest

TWIERDZENIE 3. *Dla dowolnego zbioru z liczb porządkowych, $\bigcup z$ jest najmniejszą liczbą porządkową x taką, że $z \subseteq S(x)$.*

§2. Kresy względem $\in$ dowolnego zbioru liczb porządkowych

Rozważmy teraz, dla dowolnego ustalonego zbioru z liczb porządkowych, formułę $\phi(x)$ postaci: $z \subseteq x$. Na mocy Tw. 2 (§1) oraz Tw. 9, Rozdział 8, $S(\bigcup z)$ jest liczbą porządkową, zatem według Tw. 3, istnieje liczba porządkowa x taka, że $\phi(x)$. Zatem, na mocy Tw. 21, Rozdział 8, istnieje najmniejsza liczba porządkowa x taka, że $z \subseteq x$. Następujące twierdzenie podaje jej postać:

Twierdzenie 4. *Dla dowolnego zbioru z liczb porządkowych, $\bigcup S(z)$ jest najmniejszą liczbą porządkową x taką, że $z \subseteq x$.*

Dowód. Rozważmy dowolny zbiór liczb porządkowych z. Na mocy Tw. 4, Rozdział 7, $\bigcup S(z) = z \cup \bigcup z$, zatem $z \subseteq \bigcup S(z)$.

Wykazujemy, że $\bigcup S(z)$ jest liczbą porządkową. Na mocy Tw. 2, $\bigcup z$ jest liczbą porządkową, zatem według Tw. 13, Rozdział 8 – zbiorem liczb porządkowych. Wobec tego $z \cup \bigcup z$ jest zbiorem liczb porządkowych, zatem każdy jego element, będąc liczbą porządkową, jest zbiorem tranzytywnym. Okazuje się, że również sam zbiór $z \cup \bigcup z$ jest tranzytywny. Weźmy bowiem dowolny $y \in z \cup \bigcup z$. Wówczas $y \in z$ lub $y \in \bigcup z$. Gdy $y \in z$, to $y \subseteq \bigcup z$ (Tw. 11(1), Rozdział 1). Gdy zaś $y \in \bigcup z$, to na mocy Tw. 18, Rozdział 8, $y \subseteq \bigcup z$ (bo $y, \bigcup z$ są liczbami porządkowymi). W obu przypadkach: $y \subseteq z \cup \bigcup z$.

Ostatecznie $z \cup \bigcup z$ (tzn. $\bigcup S(z)$) jest liczbą porządkową.

Weźmy pod uwagę formułę $\phi(x)$ postaci: $z \subseteq x$. Wykazaliśmy do tej pory, że $\bigcup S(z)$ jest liczbą porządkową taką, że $\phi(\bigcup S(z))$. Aby wykazać, że $\bigcup S(z)$ jest najmniejszą liczbą porządkową x taką, że $\phi(x)$, rozważmy dowolną liczbę porządkową y taką, że $\phi(y)$, tzn.

(1) $z \subseteq y$.

Wówczas

(2) $\bigcup z \subseteq y$.

Weźmy bowiem dowolny $x \in \bigcup z$. Zatem $x \in a$ dla pewnej liczby porządkowej $a \in z$. Z (1), $a \in y$. Ponieważ x jest liczbą porządkową (Tw. 13, Rozdział 8), więc na mocy Tw. 14, Rozdział 8, $x \in y$.

Z (1) i (2) mamy: $z \cup \bigcup z \subseteq y$, tzn. $\bigcup S(z) \subseteq y$. □

W przypadku, gdy z jest liczbą porządkową, na podstawie Tw. 2, Rozdział 8 mamy: $\bigcup S(z) = z$, i oczywiście najmniejszą liczbą porządkową x taką, że $z \subseteq x$ jest z.

Rozważmy teraz dla dowolnego zbioru z liczb porządkowych oraz dowolnej liczby porządkowej a następujące warunki:

(3) $\forall y \in z,\ y \in a$,

(4) $\forall x[x$ jest liczbą porządkową $\Rightarrow ((\forall y \in z, y \in x) \Rightarrow a \in x \vee a = x)]$.

Jest sensowne nazwać liczbę porządkową a, dla której spełnione są warunki (3), (4) – kresem górnym zbioru z ze względu na relację porządkującą $\in$. Pewne wątpliwości może tu budzić następnik implikacji $(\forall y \in z, y \in x) \Rightarrow a \in x \vee a = x$ w warunku (4), bowiem dla nazwania liczby a kresem górnym ze względu na $\in$, ów następnik powinien być postaci: $a \in x$. Jednakże wówczas warunek (3) z tak zmodyfikowanym warunkiem (4), niczego nie definiują – nie istnieje bowiem liczba porządkowa a, która by takie warunki spełniała (jeśli mamy a takie, że zachodzi (3), to według zmodyfikowanego warunku (4), $a \in a$, co jest niemożliwe).

Jest jasne na mocy definicji najmniejszej liczby porządkowej x takiej, że $\phi(x)$ oraz Tw. 4 i Twierdzeń 20, 18, Rozdział 8, że dla dowolnego zbioru z liczb porządkowych istnieje dokładnie jedna liczba porządkowa a, dla której spełnione są warunki (3), (4), mianowicie $a = \bigcup S(z)$. W literaturze przedmiotu właśnie $\bigcup S(z)$ nazywana jest kresem górnym zbioru z w klasie liczb porządkowych. Dla odróżnienia od kresu górnego $\sup z$ względem inkluzji, oznaczmy kres górny względem $\in$ jako $\sup_\in z$. Zatem $\sup_\in z = \bigcup S(z) = z \cup \bigcup z$. Ponieważ $\sup z = \bigcup z$, więc $\sup z \subseteq \sup_\in z$, czyli $\sup z \in \sup_\in z$ lub $\sup z = \sup_\in z$. W zależności od postaci zbioru z, każdy z tych dwóch przypadków, jeden bądź drugi, jest realizowany. Naturalnie równość obu kresów ma miejsce dokładnie wówczas, gdy $z \subseteq \bigcup z$:

(= sup) $\sup z = \sup_\in z$ wtw $z \subseteq \bigcup z$.

Zatem w przypadku, gdy z jest liczbą porządkową, czyli z jest zbiorem tranzytywnym, a więc $\bigcup z \subseteq z$ (Tw. 2, Rozdział 8) mamy:

(= sup lp) $\sup z = \sup_\in z$ wtw $\bigcup z = z$.

Ponadto, dla z będącego liczbą porządkową, $\sup z \in \sup_\in z$ wtw $\sup z \neq \sup_\in z$ wtw $z \nsubseteq \bigcup z$ wtw $\neg(z \in \bigcup z \vee z = \bigcup z)$ wtw $z \notin \bigcup z \wedge z \neq \bigcup z$ wtw $\bigcup z \in z$, na mocy Twierdzeń 18, 17, Rozdział 8. Ostatecznie:

($\in$ sup lp) $\sup z \in \sup_\in z$ wtw $\bigcup z \in z$.

Na przykład dla $z = \varnothing$, $\sup z = \sup_\in z$ oraz dla dowolnej niepustej liczby naturalnej z, $\sup z \in \sup_\in z$, bo, jak łatwo sprawdzić, wówczas $z = S(\bigcup z)$, zaś $\bigcup z \in S(\bigcup z)$.

Weźmy pod uwagę przykład zbioru z liczb porządkowych, który nie jest liczbą porządkową, powiedzmy, $z = N - \{0\}$. Tutaj $\sup z = \sup_\in z$, bowiem $z \subseteq \bigcup z$: jeśli $x \in N - \{0\}$, to również $S(x) \in N - \{0\}$, lecz $x \in S(x)$, zatem $x \in \bigcup(N - \{0\})$.

Niech $z = \{1, 2\}$, tzn. $z = 3 - \{0\}$. Oczywiście z nie jest liczbą porządkową. W tym przypadku, $\sup z \in \sup_\in z$. Bowiem $\bigcup z = \bigcup\{1, 2\} = 1 \cup 2 = 2$, stąd $2 \notin \bigcup z$, jednakże $2 \in z$, zatem $z \nsubseteq \bigcup z$, czyli zgodnie z warunkiem (= sup), $\sup z \neq \sup_\in z$. Zauważmy, że tutaj zachodzi: $\bigcup z \in z$. Wykażemy w następnym paragrafie, że warunek ($\in$ sup lp) jest prawdziwy dla dowolnego zbioru z liczb porządkowych (nie tylko dla dowolnej liczby porządkowej z).

W ogólności kres dolny $\inf_\in z$ niepustego zbioru z ze względu na porządek $\in$, może nie istnieć. Kres ten winien być bowiem liczbą porządkową spełniającą warunki:

$\forall y \in z,\ \inf_\in z \in y$,

$\forall x[x$ jest liczbą porządkową $\Rightarrow ((\forall y \in z,\ x \in y) \Rightarrow x \subseteq \inf_\in z)]$.

Pierwszy z tych warunków jest równoważny formule:

$\inf_\in z \in \bigcap z$,

drugi zaś wyrażeniu:

$\forall x[x$ jest liczbą porządkową $\Rightarrow (x \in \bigcap z \Rightarrow x \subseteq \inf_\in z)]$.

Lecz $\bigcap z = nlp(z)$ (zobacz poprzednią uwagę). Zatem $\inf_\in z$ byłby największą liczbą porządkową (ze względu na inkluzję) należącą do liczby porządkowej $nlp(z)$. Taka zaś liczba porządkowa dla pewnych zbiorów z liczb porządkowych nie istnieje. Na przykład, gdy z jest dowolną niepustą liczbą porządkową, to $nlp(z) = \varnothing$, więc nie istnieje największa liczba porządkowa należąca do $nlp(z)$.

§3. Suma następnika i następnik sumy dowolnego zbioru liczb porządkowych

Powyżej, dla dowolnego zbioru z liczb porządkowych, porównaliśmy ze sobą dwie liczby porządkowe (kresy górne zbioru z) : $\bigcup z$, $\bigcup S(z)$, mianowicie w ogólności, $\bigcup z \subseteq \bigcup S(z)$. Twierdzenia 3, 4 umożliwiają dokonanie porównania innej pary liczb porządkowych: $\bigcup S(z), S(\bigcup z)$. Skoro $\bigcup S(z)$ jest najmniejszą liczbą porządkową x taką, że $z \subseteq x$, zaś $z \subseteq S(\bigcup z)$, więc $\bigcup S(z) \subseteq S(\bigcup z)$. Ostatecznie mamy następujący

Wniosek. *Dla dowolnego zbioru z liczb porządkowych,*
(1) $\bigcup z \subseteq \bigcup S(z) \subseteq S(\bigcup z)$,
(2) $z \subseteq \bigcup S(z) \subseteq S(\bigcup z)$.

Jedną z konsekwencji tego Wniosku jest alternatywa rozłączna:

(*) albo $\bigcup S(z) \in S(\bigcup z)$, albo $\bigcup S(z) = S(\bigcup z)$,

dla dowolnego zbioru z liczb porządkowych (na mocy Tw. 18, Rozdział 8).

Przypadek $\bigcup S(z) \in S(\bigcup z)$ jest, według Tw. 6, Rozdział 7, równoważny warunkowi $z \subseteq \bigcup z$, a ten z kolei, na mocy (= sup), warunkowi $\bigcup z = \bigcup S(z)$. Zatem, jeżeli $\bigcup S(z) \in S(\bigcup z)$, to na mocy Wniosku,

$$z \subseteq \bigcup z = \bigcup S(z) \in S(\bigcup z).$$

W szczególności, gdy zbiór liczb porządkowych z jest liczbą porządkową, a więc gdy $\bigcup z \subseteq z$, warunek $\bigcup S(z) \in S(\bigcup z)$ jest równoważny równości $z = \bigcup z$, co już wcześniej zostało ustalone w Tw. 6, Rozdział 8. Gdy więc ów warunek zachodzi, to:

$$\bigcup z = z = \bigcup S(z) \in S(\bigcup z).$$

Z kolei przypadek $\bigcup S(z) = S(\bigcup z)$ jest, jak pokazuje następujące twierdzenie, równoważny warunkowi $\bigcup z \in z$:

TWIERDZENIE 5. *Dla dowolnego zbioru z liczb porządkowych, $\bigcup z \in z$ wtw $\bigcup S(z) = S(\bigcup z)$.*

DOWÓD. Niech z będzie zbiorem liczb porządkowych.

($\Rightarrow$): Załóżmy, że $\bigcup z \in z$. Wówczas na mocy Tw. 7, Rozdział 7, $S(\bigcup z) \subseteq \bigcup S(z)$. Ponieważ przeciwna inkluzja zachodzi (por. Wniosek), więc $\bigcup S(z) = S(\bigcup z)$.

($\Leftarrow$): oczywisty na mocy Tw. 7, Rozdział 7. □

Jeśli więc $\bigcup S(z) = S(\bigcup z)$, to na mocy Wniosku oraz Tw. 5,

$$\bigcup z \in z \subseteq \bigcup S(z) = S(\bigcup z),$$

w szczególności zaś, gdy z jest liczbą porządkową, to:

$$\bigcup z \in z = \bigcup S(z) = S(\bigcup z).$$

Przy okazji zauważmy, że skoro warunek $\bigcup S(z) \in S(\bigcup z)$ jest równoważny inkluzji $z \subseteq \bigcup z$, oraz warunek $\bigcup S(z) = S(\bigcup z)$ jest równoważny temu, że $\bigcup z \in z$, więc, na mocy (*), mamy dla dowolnego zbioru z liczb porządkowych prawdziwą alternatywę rozłączną:

(**) albo $z \subseteq \bigcup z$, albo $\bigcup z \in z$.

Pierwszy z członów tej alternatywy, co już dawno ustalono, jest równoważny równości $\sup z = \sup_\in z$, drugi zaś wyrażeniu $\sup z \in \sup_\in z$. Jeśli bowiem $\bigcup z \in z$, to ponieważ $z \subseteq \bigcup S(z)$, więc $\bigcup z \in \bigcup S(z)$, to znaczy $\sup z \in \sup_\in z$. Jeśli zaś $\bigcup z \notin z$, to prawdziwy jest pierwszy z członów alternatywy (**), co oznacza równość obu kresów, zatem wówczas $\sup z \notin \sup_\in z$. Krótko mówiąc, warunek ($\in \sup lp$) jest prawdziwy dla dowolnego zbioru z liczb porządkowych.

Zauważmy ponadto, że z alternatywy (**) uzyskujemy wyrażenie: dla dowolnej liczby porządkowej z: albo $\bigcup z = z$ albo $\bigcup z \in z$.

Inną, oczywistą konsekwencją wyżej sformułowanego Wniosku jest wyrażenie:

dla dowolnego zbioru z liczb porządkowych istnieje liczba porządkowa x taka, że $z \subseteq x$,

z którego wynika

TWIERDZENIE 6. *Nie istnieje zbiór wszystkich liczb porządkowych.*

DOWÓD. Załóżmy, że z jest zbiorem wszystkich liczb porządkowych. Niech x będzie liczbą porządkową taką, że $z \subseteq x$. Wówczas, skoro x jest liczbą porządkową, zaś z zbiorem wszystkich liczb porządkowych, więc $x \in z$. Wtedy jednak $x \in x$, co jest niemożliwe. $\square$

Naturalnie nie istnieje również zbiór wszystkich zbiorów tranzytywnych. Gdyby bowiem istniał, to stosując aksjomat podzbiorów z formułą $\phi(x)$ postaci: x jest liczbą porządkową, oraz zmienną wolną z oznaczającą właśnie ów zbiór, uzyskalibyśmy istnienie zbioru wszystkich liczb porządkowych.

§4. Liczby porządkowe izolowane i graniczne

Następujący fakt jest odpowiednikiem Tw. 6, Rozdział 8:

TWIERDZENIE 7. *Dla dowolnej liczby porządkowej x następujące warunki są równoważne:*
(i) $\bigcup x \in x$,
(ii) $x = S(\bigcup x)$,
(iii) $\bigcup S(x) = S(\bigcup x)$.

DOWÓD. Niech x będzie dowolną liczbą porządkową.
(i) $\Leftrightarrow$ (iii): Na mocy Tw. 5, x jest bowiem zbiorem liczb porządkowych.
(ii) $\Leftrightarrow$ (iii): na mocy Tw. 2(i)$\Leftrightarrow$(iv), Rozdział 8, x jest bowiem zbiorem tranzytywnym. $\square$

Tw. 6, Rozdział 8 jest oczywiście prawdziwe dla każdej liczby porządkowej x. Zauważmy, że według alternatywy (*) z poprzedniego paragrafu, dla dowolnej liczby porządkowej x przynajmniej jeden z warunków (iii) z Tw. 6, Rozdział 8 oraz Tw. 7 musi być spełniony. Jest oczywiste, że jednocześnie oba te warunki nie mogą być prawdziwe.

Podobnie, skoro według Tw. 3, $x \subseteq S(\bigcup x)$, więc na mocy Tw. 18, Rozdział 8, dla dowolnej liczby porządkowej x prawdziwa jest alternatywa:

(***) $x \in S(\bigcup x)$ lub $x = S(\bigcup x)$,

tzn. dla dowolnej liczby porządkowej x dokładnie jeden z warunków (ii) Tw. 6, Rozdział 8 oraz Tw. 7 jest prawdziwy.

Konsekwentnie, biorąc pod uwagę Tw. 6, Rozdział 8 oraz Tw. 7, możemy podzielić klasę liczb porządkowych na dwie grupy: w jednej grupie znajdują się te liczby porządkowe, dla których prawdziwe są warunki z Tw. 6, Rozdział 8, w drugiej grupie te liczby porządkowe, dla których prawdziwe są warunki Tw. 7.

Definicja. Mówimy, że liczba porządkowa x jest *izolowana*, gdy istnieje liczba porządkowa y taka, że $x = S(y)$. Liczbę porządkową, która nie jest izolowana, nazywamy *graniczną*.

Twierdzenie 8. (1) *Dla dowolnej liczby porządkowej x następujące warunki są równoważne:*
(i) $\bigcup x \in x$,
(ii) $x = S(\bigcup x)$,
(iii) $\bigcup S(x) = S(\bigcup x)$,
(iv) $\sup x \in \sup_{\in} x$,
(v) *x jest izolowana.*

(2) *Dla dowolnej liczby porządkowej x następujące warunki są równoważne*:
(i) $\bigcup x = x$,
(ii) $x \in S(\bigcup x)$,
(iii) $\bigcup S(x) \in S(\bigcup x)$,
(iv) $\sup x = \sup_{\in} x$,
(v) *x jest graniczna.*

Dowód. Pierwsze trzy warunki z (1) oraz (2) są naturalnie równoważne na mocy Tw. 7 oraz Tw. 6, Rozdział 8. Równoważności (i) $\Leftrightarrow$ (iv) z (1) oraz z (2) to warunki, odpowiednio, $(\in \sup lp)$, $(= \sup lp)$ z §2.

Na mocy Tw. 8, Rozdział 7, warunek (2)(i) implikuje warunek (2)(v). Jest oczywiste, że warunek (1)(ii) implikuje warunek (1)(v). Stąd prawdą jest, że jeżeli x jest liczbą porządkową graniczną (tzn. x nie jest izolowana), to $x \neq S(\bigcup x)$. Zatem na mocy (***), $x \in S(\bigcup x)$, co dowodzi, że warunek (2)(v) implikuje warunek (2)(ii). Zatem 2(v) jest równoważny każdemu z pozostałych warunków z (2).

Analogicznie, zakładając, że x jest izolowana (a więc nie jest graniczna) mamy na mocy równoważności z (2), iż $x \notin S(\bigcup x)$, co daje (według (***)): $x = S(\bigcup x)$.

Tak więc, warunek (1)(v) implikuje warunek 1(ii). Zatem (1)(v) jest równoważny każdemu z pozostałych warunków z (1). □

Przykładem liczby porządkowej granicznej jest zbiór $\varnothing$ (bo $\bigcup \varnothing = \varnothing$, zob. Tw. 8(2)). Przykładem liczby porządkowej izolowanej jest jakakolwiek niepusta liczba naturalna. Prawdziwa jest bowiem interpretacja tw. 2 arytmetyki elementarnej, §1 Rozdział 7, w teorii ZFC: $\forall x \in N(x = \varnothing \vee \exists y \in N(x = S(y)))$.

Rozważymy teraz najmniejsze liczby porządkowe x takie, że $\phi(x)$ dla następujących formuł $\phi(x)$:
$y \in x$,
$y \subseteq x$,
$y \in x \wedge y \subseteq x$,
gdzie y jest dowolną ustaloną liczbą porządkową.

Oczywiście najmniejszą liczbą porządkową x taką, że $y \subseteq x$ jest liczba porządkowa y.

Formuła $y \in x \wedge y \subseteq x$, na mocy Tw. 18, Rozdział 8, jest równoważna formule $y \in x$. Zatem najmniejsza liczba porządkowa x taka, że $y \in x$ jest najmniejszą liczbą porządkową x taką, że $y \in x \wedge y \subseteq x$. Biorąc pod uwagę Tw. 1 Rozdział 7, oczekujemy więc, że najmniejszą liczbą porządkową x taką, że $y \in x$ jest $S(y)$:

Twierdzenie 9. *Dla dowolnej liczby porządkowej y, $S(y)$ jest najmniejszą liczbą porządkową x taką, że $y \in x$.*

Dowód. Niech y będzie dowolną liczbą porządkową. Naturalnie, na mocy Tw. 9, Rozdział 8, $S(y)$ jest liczbą porządkową. Wystarczy teraz powołać się na Tw. 1, Rozdział 7, aby skończyć dowód. Niemniej jednak wykonajmy ten dowód, odwołując się do warunku (iii) Tw. 19, Rozdział 8. Naturalnie $y \in S(y)$, tzn. spełnione jest $\phi(S(y))$, gdzie $\phi(x)$ jest postaci: $y \in x$.

Wykazujemy, że $\forall z(z \in S(y) \Rightarrow y \notin z)$. Załóżmy nie wprost, że dla pewnego $z : z \in S(y)$ oraz $y \in z$. Wówczas z pierwszego wyrażenia, na mocy Tw. 18, Rozdział 8 (z jest liczbą porządkową) mamy: $z \subseteq y$. Stąd oraz z drugiego wyrażenia, $y \in y$, co jest niemożliwe. □

Wniosek. *Dla dowolnej liczby porządkowej y nie istnieje taka liczba porządkowa x, że $y \in x$ oraz $x \in S(y)$.*

Dowód. Rozważmy dowolną liczbę porządkową y i załóżmy nie wprost, że dla pewnej liczby porządkowej z:
(1) $y \in z$ oraz
(2) $z \in S(y)$.

Wówczas z (1) mamy: $\phi(z)$. Ponadto, skoro na mocy Tw. 9, $S(y)$ jest najmniejszą liczbą porządkową x taką, że $\phi(x)$ (gdzie $\phi(x) := y \in x$), więc według Tw. 19(i)⇔(iii), Rozdział 8 z (2) otrzymujemy: $\neg\phi(z)$; sprzeczność (por. również uwagę po dowodzie Tw. 1, Rozdział 7, §4). □

Jak widać, nazwa „następnik liczby porządkowej y” dla zbioru $S(y)$ jest uzasadniona. $S(y)$ następuje bezpośrednio po y w porządku wyznaczonym przez relację należenia do zbioru.

Rozważmy, analogicznie jak powyżej, następujące trzy formuły $\phi(x)$ dla ustalonej liczby porządkowej y:
$y \in S(x)$,
$y \subseteq S(x)$,
$y \in S(x) \wedge y \subseteq S(x)$.

Jest oczywiste, że dla liczby porządkowej x formuły: $y \in S(x)$ oraz $y \in S(x) \wedge y \subseteq S(x)$ są równoważne. Ponadto wyrażenie $y \in S(x)$ jest na mocy Tw. 18, Rozdział 8, równoważne formule $y \subseteq x$. Zatem najmniejszą liczbą porządkową x taką, że $y \in S(x)$ (oraz taką, że $y \in S(x) \wedge y \subseteq S(x)$) jest liczba porządkowa y.

Interesujący jest więc jedynie przypadek formuły $\phi(x)$ postaci: $y \subseteq S(x)$. Na mocy Tw. 3 mamy natychmiast:

WNIOSEK 1. *Dla dowolnej liczby porządkowej y, najmniejszą liczbą porządkową x taką, że $y \subseteq S(x)$ jest $\bigcup y$.*

Stąd oraz na podstawie Wniosku z Tw. 9 otrzymujemy kolejny wniosek, analogiczny do Wniosku z Tw. 9:

WNIOSEK 2. *Dla dowolnej liczby porządkowej y nie istnieje taka liczba porządkowa x, że $\bigcup y \in x$ oraz $x \in y$.*

DOWÓD. Rozważmy dowolną liczbę porządkową y i załóżmy nie wprost, że dla pewnej liczby porządkowej z mamy:
(1) $\bigcup y \in z$ oraz
(2) $z \in y$.

Na mocy Wniosku 1 (por. również alternatywę (***)), $y \subseteq S(\bigcup y)$. Zatem z (2), $z \in S(\bigcup y)$. Lecz to, wraz z (1) jest, na mocy Wniosku z Tw. 9 ($\bigcup y$ jest liczbą porządkową), niemożliwe. □

Jest jasne, że w przypadku, gdy y jest liczbą porządkową izolowaną, a więc gdy $y = S(\bigcup y)$ (Tw. 8(1)), liczba porządkowa $\bigcup y$ jest *bezpośrednim poprzednikiem* liczby y w porządku liczb porządkowych wyznaczonym relacją $\in$.

W przypadku, gdy y jest liczbą graniczną, $y = \bigcup y$ (Tw. 8(2)) i wówczas y nie ma bezpośredniego poprzednika. Gdyby bowiem x był takim bezpośrednim poprzednikiem liczby y, to y byłby jego następnikiem: $y = S(x)$. Oznaczałoby to, że y jest, wbrew założeniu, liczbą porządkową izolowaną:

y jest izolowana: $$\underset{\bigcup y}{\circ} \longrightarrow \overset{S(\bigcup y)}{\underset{y}{\circ}} \longrightarrow \underset{S(y)}{\circ}$$

y jest graniczna: $$\overset{\bigcup y}{\underset{y}{\circ}} \longrightarrow \overset{S(\bigcup y)}{\underset{S(y)}{\circ}}$$

Naturalnie, jeżeli y jest niepustą liczbą porządkową graniczną, to y jest zbiorem indukcyjnym. Istotnie, $\varnothing \in y$ (Tw. 23, Rozdział 8) oraz gdy $x \in y$, to na mocy Tw. 9, $S(x) \subseteq y$, co implikuje $S(x) \in y$, skoro y jest graniczna ($y \neq S(x)$).

Jest również oczywiste, że jeżeli liczba porządkowa jest zbiorem indukcyjnym, to jest ona graniczna. Izolowana liczba y nie jest bowiem takim zbiorem, skoro $\bigcup y \in y$, zaś $S(\bigcup y) \notin y$.

Gdy y jest izolowana, to sytuacja postaci:

$$\ldots \in \bigcup^n y \in \ldots \in \bigcup\bigcup y \in \bigcup y \in y$$

nie ma miejsca. Gdyby bowiem zachodziła, to y miałby nieskończone zejście: $y, \bigcup y, \bigcup\bigcup y, \ldots, \bigcup^n y, \ldots$. Dokładniej zanalizujmy możliwość takiej sytuacji w oparciu o następujące twierdzenia.

Twierdzenie 10. *Dla dowolnego zbioru z liczb porządkowych granicznych, $\bigcup z$ jest liczbą porządkową graniczną.*

Dowód. Niech z będzie zbiorem liczb porządkowych granicznych. Załóżmy nie wprost, że $\bigcup z$ jest izolowana. Wówczas dla pewnej liczby porządkowej x:
(1) $\bigcup z = S(x)$.

Skoro $x \in S(x)$, więc $x \in \bigcup z$, zatem z definicji sumy, dla pewnego u mamy:
(2) $x \in u$ oraz
(3) $u \in z$.

Oczywiście z (3) na mocy Tw. 11(1), Rozdział 1, otrzymujemy:
(4) $u \subseteq \bigcup z$.

Na mocy Tw. 9, z (2), $S(x) \subseteq u$ (według (3) u jest liczbą porządkową), co wraz z (1) daje $\bigcup z \subseteq u$ i konsekwentnie z (4) otrzymujemy: $\bigcup z = u$. Lecz według (3), u jest graniczna, zatem $\bigcup z$ jest graniczna. Sprzeczność z założeniem. $\square$

TWIERDZENIE 11. *Dla dowolnej liczby porządkowej izolowanej, wśród wszystkich liczb granicznych do niej należących, istnieje liczba największa.*

DOWÓD. Niech y będzie dowolną liczbą porządkową izolowaną. Rozważmy aksjomat podzbiorów dla formuły $\phi(x)$ postaci: x *jest liczbą porządkową graniczną* $\wedge\ x \in y$. Na podstawie tego aksjomatu natychmiast stwierdzamy istnienie zbioru $z = \{x : x \text{ jest graniczna} \wedge x \in y\}$ wszystkich liczb porządkowych granicznych będących elementami zbioru y. Naturalnie $z \neq \varnothing$ (bo $\varnothing \in z$) oraz

(1) $z \subseteq y$.

Wykażemy, że $\bigcup z$ jest elementem największym w zbiorze liniowo uporządkowanym $<z, \subseteq>$. W tym celu rozważmy prawdziwą alternatywę:

(2) albo $\bigcup z \in z$ albo $z \subseteq \bigcup z$ (zobacz (**), §3).

Załóżmy, że zachodzi:

(3) $z \subseteq \bigcup z$.

Wówczas naturalnie $\bigcup z$ jest najmniejszą liczbą porządkową x taką, że $z \subseteq x$ (taka najmniejsza liczba porządkowa jest według Tw. 4 postaci $\bigcup S(z)$, co jest równe $z \cup \bigcup z$, co z kolei jest równe $\bigcup z$; por. również (= sup) z §3). Zatem z (1) otrzymujemy: $\bigcup z \subseteq y$, czyli $\bigcup z \in y$ lub $\bigcup z = y$ (Tw. 18, Rozdział 8). Lecz z jest zbiorem liczb granicznych, więc według Tw. 10, $\bigcup z$ jest graniczna, tymczasem y jest izolowana. Wobec tego $\bigcup z \neq y$ i konsekwentnie $\bigcup z \in y$. Wówczas jednak, z definicji zbioru z, $\bigcup z \in z$, co wobec (3) oznacza, że $\bigcup z \in \bigcup z$, a to jest niemożliwe (jest skądinąd wiadome, że obydwa człony alternatywy (2) nie mogą być prawdziwe).

Skoro nie jest prawdą, że $z \subseteq \bigcup z$, więc z (2) otrzymujemy: $\bigcup z \in z$. Lecz przecież $\forall u \in z, u \subseteq \bigcup z$ (Tw. 11(1), Rozdział 1). Ostatecznie $\bigcup z$ jest największą liczbą porządkową w zbiorze z. □

Weźmy pod uwagę dowolną liczbę porządkową izolowaną y. Na mocy Tw. 11, niech $ng(y)$ będzie największą liczbą porządkową graniczną należącą do y. Rozważmy zbiór $y - S(ng(y))$. Dla dowolnej liczby porządkowej x mamy: $x \in y - S(ng(y))$ wtw ($x \in y$ i $x \notin S(ng(y))$) wtw ($x \in y$ i $x \notin ng(y)$ i $x \neq ng(y)$) wtw ($x \in y$ i $ng(y) \in x$). Ostatecznie,

$$y - S(ng(y)) = \{x : ng(y) \in x \in y\}.$$

Zauważmy, że

(ng) $\forall x \in y - S(ng(y)),\ x$ jest izolowana.

Gdyby bowiem pewna liczba x_0 taka, że $ng(y) \in x_0 \in y$ była graniczna, to byłoby $x_0 \subseteq ng(y)$ i jednocześnie $ng(y) \subseteq x_0$ oraz $ng(y) \neq x_0$ (Wniosek z Tw. 18, Rozdział 8), co jest niemożliwe.

Połóżmy dla dowolnej liczby porządkowej x, $S^0(x) = x$ oraz $S^{n+1}(x) = S(S^n(x))$ dla $n = 0, 1, \ldots$.

Lemat. *Dla dowolnej liczby porządkowej x oraz dowolnej liczby naturalnej n:* $S^{n+1}(x) = x \cup \{x, S(x), S^2(x), \ldots, S^n(x)\}$.

Dowód (indukcyjny). Niech x będzie dowolną liczbą porządkową (lub po prostu dowolnym zbiorem). Dla $n = 0$ powyższa równość jest spełniona na mocy definicji następnika. Załóżmy, że dla jakiegoś n równość ta jest spełniona. Wówczas $S^{(n+1)+1}(x) = S(S^{n+1}(x)) = S^{n+1}(x) \cup \{S^{n+1}(x)\} = x \cup \{x, S(x), S^2(x), \ldots, S^n(x)\} \cup \{S^{n+1}(x)\} = x \cup \{x, S(x), S^2(x), \ldots, S^n(x), S^{n+1}(x)\}$. $\square$

Twierdzenie 12. *Dla dowolnej izolowanej liczby y, zbiór $y - S(ng(y)) = \{x : ng(y) \in x \in y\}$ jest skończony.*

Dowód. Załóżmy nie wprost, że y jest taką liczbą porządkową izolowaną, że $\{x : ng(y) \in x \in y\}$ nie jest zbiorem skończonym. Weźmy pod uwagę zbiór $z = \{ng(y)\} \cup \{x : ng(y) \in x \in y\} = \{x : ng(y) \subseteq x \in y\}$.

Wykażmy indukcyjnie, że

(1) dla dowolnego $n = 0, 1, \ldots, S^n(ng(y)) \in z$.

Jest oczywiste, że $ng(y) \in z$, zatem $S^0(ng(y)) \in z$. Załóżmy, że dla jakiegoś $n \in N, S^n(ng(y)) \in z$. Stąd

(2) $S^n(ng(y)) \in y$.

Z (2) i przechodniości relacji $\in$, ponieważ $ng(y) \in S(ng(y)) \in S^2(ng(y)) \in \ldots \in S^n(ng(y))$, otrzymujemy:

(3) $\{S(ng(y)), \ldots, S^n(ng(y))\} \subseteq \{x : ng(y) \in x \in y\}$.

Ponieważ $S(S^n(ng(y))$ jest najmniejszą liczbą porządkową x taką, że $S^n(ng(y)) \in x$ (Tw. 9), więc z (2), $S(S^n(ng(y))) \subseteq y$. Dlatego $S(S^n(ng(y))) \in y$ lub $S(S^n(ng(y))) = y$ (Tw. 18, Rozdział 8). Lecz równość $S(S^n(ng(y))) = y$ wraz z (3) oznacza (zob. Wniosek z Tw. 9), że $\{S(ng(y)), \ldots, S^n(ng(y))\}$ jest zbiorem wszystkich liczb porządkowych x takich, że $ng(y) \in x \wedge x \in y$, czyli zbiór $y - S(ng(y))$ byłby skończony wbrew założeniu. Zatem $S(S^n(ng(y))) \in y$, tzn. $S^{n+1}(ng(y)) \in y$. Naturalnie $ng(y) \subseteq S^{n+1}(ng(y))$, ostatecznie $S^{n+1}(ng(y)) \in z$, co kończy dowód wyrażenia (1).

Z kolei, dzięki (1) można rozważyć funkcję (ciąg) $f : N \longrightarrow z$ postaci: $\forall n \in N, f(n) = S^n(ng(y))$.

Wykazujemy, że

(4) zbiór $ng(y) \cup \vec{f}(N)$ jest liczbą porządkową.

Oczywiście elementami tego zbioru są wyłącznie liczby porządkowe, zatem zbiory tranzytywne, wystarczy więc wykazać, że $ng(y) \cup \vec{f}(N)$ jest zbiorem tranzytywnym. Niech więc $x \in ng(y) \cup \vec{f}(N)$. Gdy $x \in ng(y)$, to oczywiście $x \subseteq ng(y)$, zatem $x \subseteq ng(y) \cup \vec{f}(N)$. Niech $x \in \vec{f}(N)$. Wówczas $x = S^n(ng(y))$, dla pewnego $n \in N$. Zatem $x = ng(y)$, gdy $n = 0$, oraz $x = ng(y) \cup \{ng(y), S(ng(y)), \ldots, S^{n-1}(ng(y))\}$, gdy $n \neq 0$ (zobacz lemat powyżej). Ostatecznie, $x \subseteq ng(y) \cup \vec{f}(N)$, bo gdy $n \neq 0$, to $\{ng(y), S(ng(y)), \ldots, S^{n-1}(ng(y))\} \subseteq \vec{f}(N)$.

Połóżmy: $u = ng(y) \cup \vec{f}(N)$. Na mocy (4), $\bigcup u \subseteq u$ (Tw. 2, Rozdział 8). Wykazujemy teraz, że $u \subseteq \bigcup u$, co daje równość $\bigcup u = u$ i dowodzi (Tw. 8(2)), że

(5) u jest graniczna.

Niech więc $x \in u$. Zatem $x \in ng(y)$ lub $x \in \vec{f}(N)$. Gdy $x \in ng(y)$, to $S(x) \in ng(y)$, bo $ng(y)$ jest graniczna (tzn. $S(x) \neq ng(y)$, zaś $S(x) \subseteq ng(y)$), stąd $S(x) \in u$. Podobnie, gdy $x \in \vec{f}(N)$, czyli $x = S^n(ng(y))$ dla pewnego $n \in N$, mamy: $S(x) = S^{n+1}(ng(y)) \in \vec{f}(N)$, zatem $S(x) \in u$. Ostatecznie, skoro $x \in S(x)$ oraz $S(x) \in u$, więc $x \in \bigcup u$. (Krótko mówiąc, wykazaliśmy tu, że zbiór u jest zamknięty na operację S, a ponieważ $\varnothing \in u$, więc u jest liczbą porządkową, która jest zbiorem indukcyjnym, zatem u nie jest izolowana.)

Naturalnie $\vec{f}(N) \subseteq z \subseteq y$, z definicji funkcji f oraz zbioru z. Oczywiście $ng(y) \subseteq y$ (bo $ng(y) \in y$). Zatem $ng(y) \cup \vec{f}(N) \subseteq y$, tzn. $u \subseteq y$. Stąd zaś $u \in y$ lub $u = y$ (Tw. 18, Rozdział 8). Lecz wobec (5) i założenia, że y jest izolowana, $u \neq y$. Zatem $u \in y$. Stąd, ponieważ $ng(y) \in u$ (bo $f(0) = ng(y)$, zaś $f(0) \in u$), otrzymujemy: $u \in \{x : ng(y) \in x \in y\}$, co, wobec (5), jest sprzeczne z wyrażeniem (ng). $\square$

Wniosek. *Dla dowolnej liczby izolowanej y istnieje liczba naturalna n taka, że $y = ng(y) \cup \{ng(y), S(ng(y)), \ldots, S^n(ng(y))\} = S^{n+1}(ng(y))$.*

Dowód. Niech y będzie izolowana. Wykazujemy, że dla pewnego $n \in N$ pierwsza z równości jest spełniona. Druga jest bezpośrednią konsekwencją lematu powyżej.

Naturalnie $y = S(ng(y)) \cup (y - S(ng(y))$. Stąd

(1) $y = ng(y) \cup \{ng(y)\} \cup \{x : ng(y) \in x \in y\}$.

Zbiór $\{x : ng(y) \in x \in y\}$, na mocy Tw. 12, jest skończony, zatem

(2) $\{x : ng(y) \in x \in y\} = \varnothing$ lub

(3) dla pewnego $k \geqslant 1, \{x : ng(y) \in x \in y\}$ jest k-elementowy.

Gdy zachodzi (2), to z (1) mamy:

(4) $y = ng(y) \cup \{S^0(ng(y))\}$.

Gdy zachodzi (3), to mamy:

(5) $\{x : ng(y) \in x \in y\} = \{S(ng(y)), \ldots, S^k(ng(y))\}$,

bowiem $ng(y) \in S(ng(y)) \in \ldots \in S^k(ng(y)) \in y$, oraz $S(ng(y)), \ldots, S^k(ng(y))$ są jedynymi liczbami x takimi, że $ng(y) \in x \in y$, gdy zbiór $\{x : ng(y) \in x \in y\}$ jest k-elementowy.

Na mocy (1) i (5) otrzymujemy:
$y = ng(y) \cup \{ng(y), S(ng(y)), \ldots, S^k(ng(y))\}$. $\square$

§5. Niepuste liczby porządkowe graniczne

Powyższe ustalenia mogą wydawać się nieco zbyt abstrakcyjne, w sytuacji, gdy jedynym przykładem liczby granicznej, jakim do tej pory dysponujemy, jest zbiór $\varnothing$. Aby dostarczyć przykładów niepustych liczb granicznych, rozważymy najpierw najmniejszą liczbę porządkową niebędącą liczbą naturalną.

Weźmy pod uwagę $\phi(x)$ postaci: $\neg(x$ jest liczbą naturalną), lub $x \notin N$. Ponieważ zachodzi $\phi(N)$ oraz N jest liczbą porządkową, więc na mocy Tw. 21, Rozdział 8 istnieje najmniejsza liczba porządkowa x taka, że x nie jest liczbą naturalną. Oznaczamy ją symbolem ω. Na mocy Tw. 19(i)$\Leftrightarrow$(iii), Rozdział 8 mamy zatem:

(ω1) $\omega \notin N$ oraz

(ω2) $\forall y(y \in \omega \Rightarrow y \in N)$.

Wyrażenie (ω2) jest równoważne temu, iż $\omega \subseteq N$. Ponieważ zarówno ω jak N są liczbami porządkowymi, więc na mocy Tw. 18, Rozdział 8, $\omega \in N$ lub $\omega = N$, co wraz z (ω1) prowadzi do wniosku:

WNIOSEK. $\omega = N$, *tzn. najmniejszą liczbą porządkową niebędącą liczbą naturalną jest zbiór liczb naturalnych* N.

TWIERDZENIE 13. ω *jest najmniejszą niepustą liczbą porządkową graniczną.*

DOWÓD. Mamy wykazać, że ω jest najmniejszą liczbą porządkową x taką, że $\phi(x)$, gdzie $\phi(x)$ jest postaci: $x \neq \varnothing \wedge x$ jest graniczna. Oczywiście $\omega \neq \varnothing$.

Wykazujemy, że ω jest graniczna. Załóżmy, że tak nie jest. Wówczas ω jest izolowana, czyli $\omega = S(a)$, dla pewnej liczby porządkowej a. Ponieważ $a \in S(a)$, więc $a \in \omega$, tzn. (według powyższego Wniosku) $a \in N$, czyli a jest liczbą naturalną. Na mocy Tw. 10, Rozdział 7, $S(a)$ jest liczbą naturalną, zatem $\omega \in N$, tzn. $N \in N$, co jest niemożliwe.

Zatem spełniona jest formuła $\phi(\omega)$. Na mocy Tw. 19(i)$\Leftrightarrow$(iii), Rozdział 8 wystarczy teraz wykazać, że $\forall y(y \in \omega \Rightarrow \neg\phi(y))$, czyli $\forall y(y \in \omega \Rightarrow (y = \varnothing \vee y$ jest izolowana)). Weźmy więc pod uwagę dowolny $y \in \omega$ taki, że $y \neq \varnothing$. Wówczas y jest niepustą liczbą naturalną, zatem jest następnikiem jakiejś liczby naturalnej

a, tzn. $y = S(a)$ dla pewnej liczby porządkowej a, czyli y jest liczbą porządkową izolowaną. $\square$

ω nie jest jedyną niepustą liczbą graniczną. Aby podać następną z kolei liczbę graniczną, a więc najmniejszą liczbę graniczną x taką, że $\omega \in x$ musimy rozważyć aksjomat podstawiania $(AxSUB)_\psi$, w którym formuła $\psi(y,z)$ jest postaci:

(ψ) $(y \notin \omega \wedge z = y) \vee (y \in \omega \wedge z = S^y(\omega))$.

Na pierwszy rzut oka można by mieć wątpliwości (mogły one już pojawić się poprzednio przy okazji operowania definicją termu $S^n(x)$) czy (ψ) jest formułą języka teorii ZFC, a to z tego powodu, że ciąg symboli: „$S^y(\omega)$”, gdzie y jest przecież zbiorem, nie wydaje się być termem tego języka. Oznaczenie „$S^n(\omega)$” ma sens, ale wówczas, gdy n nie jest żadnym zbiorem, lecz ilością zastosowań operacji S. Aby rozwiać te wątpliwości, rozważmy skończony zbiór

$A_\omega = \{\omega, S(\omega), S(S(\omega)), \ldots, S(\ldots(S(\omega))\ldots)\}$.

Niech w ostatnim z wypisanych termów ilość wystąpień symbolu S wynosi n. Rozważmy liczbę naturalną (zbiór)

$\{\varnothing, S(\varnothing), S(S(\varnothing)), \ldots, S(\ldots(S(\varnothing))\ldots)\}$

taką, że ilość wystąpień S w ostatnim termie również wynosi n. Zgodnie z ustaloną konwencją notacyjną, taką liczbę naturalną oznaczamy $S(n)$, gdzie n jest teraz liczbą naturalną będącą zbiorem. Weźmy pod uwagę funkcję $f^\omega_n : S(n) \longrightarrow A_\omega$, mianowicie $f^\omega_n = \{<\varnothing, \omega>, <S(\varnothing), S(\omega)>, <S(S(\varnothing)), S(S(\omega))>, \ldots, <S(\ldots(S(\varnothing))\ldots), S(\ldots(S(\omega))\ldots)>\}$. Oznaczmy teraz dla dowolnego $y \in S(n)$, $S^y(\omega) = f^\omega_n(y)$, w szczególności więc $S^n(\omega) = f^\omega_n(n)$ (n jest tutaj zbiorem). Naturalnie w ten sam sposób mamy również dla dowolnej liczby porządkowej (czy w ogóle dowolnego zbioru) $x : S^n(x) = f^x_n(n)$, gdzie n jest zbiorem ($f^x_n : S(n) \longrightarrow A_x$).

Jest zatem jasne, że formuła $\psi(y,z)$ ma właściwie postać następującą:

$(y \notin \omega \wedge z = y) \vee (y \in \omega \wedge z = f^\omega_y(y))$,

w której nie mamy już do czynienia ze zbiorem y postrzeganym jako ilość zastosowań operacji S. W dalszym ciągu będziemy rozważać postać (ψ), pamiętając, że mamy tam do czynienia z pewnym skrótem definicyjnym.

Formuła $\psi(y,z)$ ustala przyporządkowanie każdemu zbiorowi y – jego samego, gdy $y \notin \omega$, oraz zbioru $S^y(\omega)$, gdy $y \in \omega$. Spełniony jest więc poprzednik implikacji $(AxSUB)_\psi$: $\forall y \exists z[\psi(y,z) \wedge \forall v(\psi(y,v) \Rightarrow v = z)]$. Wobec tego mamy następnik postaci:

$\exists u \forall z(z \in u \Leftrightarrow \exists y(y \in \omega \wedge \psi(y,z))$.

Biorąc pod uwagę aksjomat identyczności, mamy jedyny zbiór u, którego istnienie stwierdza powyższa formuła. Ponieważ wyrażenie $y \in \omega \wedge \psi(y,z)$ jest równoważne formule $y \in \omega \wedge z = S^y(\omega)$, więc ów zbiór, oznaczając go symbolem $S^\omega(\omega)$, możemy określić następująco:

$$\forall z(z \in S^\omega(\omega) \Leftrightarrow \exists y(y \in \omega \wedge z = S^y(\omega))).$$

Istnieje zatem zbiór, który nieformalnie zapisalibyśmy w postaci: $S^\omega(\omega) = \{\omega, S(\omega), \ldots, S^n(\omega), \ldots\}$.

Twierdzenie 14. *Zbiór $\omega \cup S^\omega(\omega)$ jest najmniejszą liczbą porządkową x taką, że x jest graniczna i $\omega \in x$.*

Dowód. Wykazanie faktu, że $\omega \cup S^\omega(\omega)$ jest liczbą porządkową graniczną przebiega analogicznie jak wykazanie warunków (4), (5) w dowodzie Tw. 12. Zamiast liczby granicznej $ng(y)$ mamy teraz liczbę graniczną ω, oraz zamiast obrazu $\overrightarrow{f}(N)$ – zbiór $S^\omega(\omega)$, który jest również obrazem zbioru N według funkcji $g : N \longrightarrow S^\omega(\omega)$ przyporządkowującej każdej liczbie naturalnej n zbiór $S^n(\omega)$.

Oczywiście $\omega \in \omega \cup S^\omega(\omega)$. Niech teraz x będzie dowolną liczbą graniczną taką, że $\omega \in x$. Aby wykazać, że $\omega \cup S^\omega(\omega) \subseteq x$, co skończy dowód, wykazujemy, że
(1) $\omega \subseteq x$ oraz
(2) $S^\omega(\omega) \subseteq x$.

(1) jest oczywiste, skoro $\omega \in x$ (Tw. 18, Rozdział 8). Wykazanie, że zachodzi (2) sprowadza się do indukcyjnego dowodu faktu, iż $\forall n \in \omega, S^n(\omega) \in x$. Dowód ten jest podobny do wykazania waruku (1) z dowodu Tw. 12. Oczywiście $S^0(\omega) \in x$. Zakładamy, że dla jakiegoś n, $S^n(\omega) \in x$. Wówczas, na mocy Tw. 9, $S(S^n(\omega)) \in x$ lub $S(S^n(\omega)) = x$. Lecz ostatnia równość nie może zachodzić, skoro x jest graniczna. Zatem $S^{n+1}(\omega) \in x$. □

Zauważmy, że zastosowanie aksjomatu podstawiania dla stwierdzenia istnienia zbioru $S^\omega(\omega)$, można uogólnić dla dowolnej operacji jednoargumentowej F oraz dowolnego zbioru X, tak, aby ustalić istnienie zbioru $F^\omega(X)$. Wystarczy wziąć pod uwagę ten aksjomat z formułą $\psi(y,z)$ postaci: $(y \notin \omega \wedge z = y) \vee (y \in \omega \wedge z = F^y(X))$, aby uzyskać istnienie zbioru:

$$F^\omega(X) = \{z : \exists y(y \in \omega \wedge z = F^y(X))\},$$

nieformalnie zapisywanego w postaci: $\{X, F(X), \ldots, F^n(X), \ldots\}$.

Jasne jest więc, że możemy ustalić kolejne liczby porządkowe graniczne, mianowicie: $\omega_2 = \omega_1 \cup S^\omega(\omega_1)$, gdzie $\omega_1 = \omega \cup S^\omega(\omega)$, $\omega_3 = \omega_2 \cup S^\omega(\omega_2)$, $\ldots$, $\omega_n = \omega_{n-1} \cup S^\omega(\omega_{n-1})$, $\ldots$, przy czym $\omega \in \omega_1 \in \omega_2 \in \ldots \in \omega_n \in \ldots$ oraz między nimi, w porządku ustalonym relacją $\in$, nie ma innych liczb granicznych.

Rozdział 10. Ciągi pozaskończone. Aksjomat wyboru

§1. Ciąg pozaskończony

W dalszym ciągu dla odróżnienia liczb porządkowych od innych zbiorów, o których nie będzie zakładane, iż są liczbami porządkowymi, będziemy liczby porządkowe oznaczać małymi greckimi literami: $\alpha, \beta, \gamma, \delta, \xi$.

Gdy $\alpha \in \beta$, to będziemy mówić, że α jest mniejsza niż β, gdy zaś $\alpha \subseteq \beta$, to mówimy, że α jest mniejsza lub równa β.

Definicja. Niech α będzie dowolną liczbą porządkową oraz X – dowolnym niepustym zbiorem. Dowolną funkcję $f : \alpha \longrightarrow X$ nazywamy *ciągiem pozaskończonym typu* lub *długości* α (*elementów zbioru* X).

Jest widoczne, że powyższa definicja jest uogólnieniem definicji ciągu. Według obecnej terminologii, ciąg pozaskończony typu ω jest dawnym ciągiem, zaś ciąg pozaskończony typu α, gdzie $\alpha \in \omega$, jest ciągiem skończonym.

Aktualna definicja dopuszcza ciąg pozaskończony typu $\varnothing$. Ponieważ $X^{\varnothing} = \{\varnothing\}$, więc istnieje dokładnie jeden ciąg pozaskończony typu $\varnothing$, mianowicie zbiór $\varnothing$.

Zazwyczaj ciąg kojarzony jest z sekwencją jego wyrazów (wartości). W przypadku ciągu pozaskończonego typu α, kolejność wyrazów w kojarzonej z nim sekwencji jest ustalona liniowo porządkującą relacją $\in$ na zbiorze α.

Rozważmy dowolną liczbę porządkową α oraz dowolny niepusty zbiór X. Niech ponadto β będzie liczbą porządkową taką, że $\beta \subseteq \alpha$. Jest oczywiste, że każdy ciąg pozaskończony f typu β elementów zbioru X jest podzbiorem produktu kartezjańskiego $\beta \times X$. Ponieważ $\beta \times X \subseteq \alpha \times X$, więc $f \subseteq \alpha \times X$, czyli $f \in P(\alpha \times X)$. Stąd, $X^{\beta} \subseteq P(\alpha \times X)$ i konsekwentnie, $X^{\beta} \in P(P(\alpha \times X))$. Istnieje więc zbiór $\{X^{\beta} : \beta \subseteq \alpha\}$ jako podzbiór zbioru $P(P(\alpha \times X))$. Bardziej formalnie należałoby uzasadnić jego istnienie, odwołując się do aksjomatu podzbiorów w postaci:

$$\forall x(\phi(x) \Rightarrow x \in P(P(\alpha \times X))) \Rightarrow \exists y \forall x(x \in y \Leftrightarrow \phi(x)),$$

gdzie $\phi(x) := \exists \beta(\beta \subseteq \alpha \ \wedge \ x = X^{\beta})$. Wobec prawdziwości poprzednika mamy:

$$\exists y \forall x(x \in y \Leftrightarrow \exists \beta(\beta \subseteq \alpha \wedge x = X^{\beta})).$$

Jak widać, formuła ta stwierdza istnienie zbioru $\{X^{\beta} : \beta \subseteq \alpha\}$. W konsekwencji, $\bigcup\{X^{\beta} : \beta \subseteq \alpha\}$ jest zbiorem. Jest to zbiór wszystkich ciągów pozaskończonych elementów zbioru X typu mniejszego lub równego α.

Niech Cg będzie 2-argumentową operacją przyporządkowującą dowolnej liczbie porządkowej α oraz niepustemu zbiorowi X zbiór $\bigcup\{X^\beta : \beta \subseteq \alpha\}$, tzn.

$$Cg(\alpha, X) = \bigcup\{X^\beta : \beta \subseteq \alpha\}.$$

TWIERDZENIE 1. *Niech X będzie dowolnym niepustym zbiorem. Wówczas*:
(1) $Cg(\varnothing, X) = \{\varnothing\}$,
(2) *Dla dowolnej liczby porządkowej* α : $\varnothing \in Cg(\alpha, X)$,
(3) *Dla dowolnych liczb porządkowych* α, β: $\beta \in \alpha \Rightarrow Cg(\beta, X) \subseteq Cg(\alpha, X)$.

DOWÓD. Dla (1): $Cg(\varnothing, X) = \bigcup\{X^\beta : \beta \subseteq \varnothing\} = \bigcup\{X^\varnothing\} = X^\varnothing = \{\varnothing\}$.
Dla (2): Ponieważ $\varnothing \in X^\varnothing$, więc $\varnothing \in \bigcup\{X^\beta : \beta \subseteq \alpha\}$, czyli $\varnothing \in Cg(\alpha, X)$.
Dla (3): Niech $\beta \in \alpha$. Weźmy $f \in Cg(\beta, X)$. Wówczas $f \in X^\gamma$ dla pewnego $\gamma \subseteq \beta$. Skoro α, β są liczbami porządkowymi oraz $\beta \in \alpha$, to $\beta \subseteq \alpha$. Zatem $\gamma \subseteq \alpha$. Stąd $f \in \bigcup\{X^\xi : \xi \subseteq \alpha\}$, czyli $f \in Cg(\alpha, X)$. □

§2. Funkcja definiowana przez indukcję pozaskończoną

Rozważmy ciąg $\mathrm{id}_\alpha \in Cg(\alpha, \alpha)$, gdzie α jest dowolną niepustą liczbą porządkową. Ciąg ten ma następującą własność: każdy jego wyraz $\mathrm{id}_\alpha(\beta)$ dla $\beta \in \alpha$, krótko mówiąc, wyraz β, jest jednoznacznie wyznaczony przez wszystkie wyrazy go poprzedzające, bowiem β jest zbiorem wszystkich tych wyrazów.

W ogólności, rozważać teraz będziemy ciągi $f : \alpha \longrightarrow X$ elementów zbioru X takie, że każdy ich wyraz $f(\beta)$ dla $\beta \in \alpha$ jest jednoznacznie wyznaczony przez wyrazy $f(\gamma)$ dla $\gamma \in \beta$.

Sposób wyznaczania danego wyrazu ciągu przez poprzedzające go w tym ciągu wyrazy, jest zupełnie dowolny. Aby go więc możliwie ogólnie określić, rozważa się dowolną funkcję $h : Cg(\alpha, X) \longrightarrow X$ przyporządkowującą każdemu ciągowi typu mniejszego lub równego α jakiś element ze zbioru X. Wartość $f(\beta)$ ciągu f dla $\beta \in \alpha$ można wtedy uzależnić od wartości funkcji h na ciągu wszystkich wyrazów poprzedzających wyraz $f(\beta)$, czyli na sekwencji elementów $f(\gamma)$ dla $\gamma \in \beta$, tzn. formalnie na ciągu: $f \restriction \beta$, następująco:

(din) $f(\beta) = h(f \restriction \beta)$.

Naturalnie pierwszy wyraz tak określanego ciągu f, czyli element $f(\varnothing)$ (inaczej $f(0)$), nie jest jednoznacznie wyznaczony przez wyrazy go poprzedzające, bo takowe nie istnieją. Zatem musi on być arbitralnie podany. Jednakże można tego dokonać pozostając przy równości (din), biorąc pod uwagę wartość funkcji h na ciągu $\varnothing$: $f(\varnothing) = h(f \restriction \varnothing) = h(\varnothing)$.

Oczywiście drugi wyraz ciągu f jest określony przez (din): $f(1) = f(\{\varnothing\}) = h(f \restriction \{\varnothing\})$. Ciąg $f \restriction \{\varnothing\}$ długości 1 (jednowyrazowy ciąg $(f(0))$) jest już wcześniej określony – jego jedyna wartość $f(\varnothing)$ wynosi $h(\varnothing)$. Zatem mając wcześniej zdefiniowaną funkcję h, znamy jej wartość na tym ciągu. Analogicznie, trzeci wyraz ciągu f jest określony przez wartość funkcji h na określonym już dwuwyrazowym ciągu: $f \restriction \{0,1\} = (f(0), f(1)) = (h(\varnothing), h(f \restriction \{\varnothing\}))$ itd.

Rozważany przed chwilą ciąg id_α można zdefiniować równością (din) przy pomocy funkcji $h : Cg(\alpha,\alpha) \longrightarrow \alpha$ zadanej następująco: $h(\varnothing) = \varnothing$ oraz dla dowolnego niepustego ciągu $g \in Cg(\alpha,\alpha)$, $h(g) = \vec{g}(\beta)$, gdzie β jest długością ciągu g (dziedziną tego ciągu). Wówczas bowiem $\mathrm{id}_\alpha(\beta) = h(\mathrm{id}_\alpha \restriction \beta)$ dla każdej $\beta \in \alpha$. Istotnie, $\mathrm{id}_\alpha(\varnothing) = \varnothing = h(\varnothing) = h(\mathrm{id}_\alpha \restriction \varnothing)$ oraz dla dowolnej niepustej $\beta \in \alpha$, $\mathrm{id}_\alpha(\beta) = \beta = \{\mathrm{id}_\alpha(\gamma) : \gamma \in \beta\} = \vec{id}_\alpha\,(\beta) = (\overrightarrow{id_\alpha \restriction \beta})\,(\beta) = h(\mathrm{id}_\alpha \restriction \beta)$.

Rozważmy jeszcze jeden przykład. Niech $h : Cg(\omega,\omega) \longrightarrow \omega$ będzie funkcją określoną następująco: $h(\varnothing) = \gamma$, gdzie γ jest dowolnie ustaloną liczbą naturalną, oraz $h(g) = S(g(\bigcup\beta))$ dla dowolnego ciągu g długości β, gdzie $\varnothing \neq \beta \in \omega$. Ponadto, co nie będzie dalej istotne, lecz jest wymagane dla poprawności definicji funkcji h, niech $h(g) = g(\varnothing)$, gdy g jest długości ω.

Istotny tu jest przypadek niepustego ciągu długości $\beta \in \omega$. Funkcja h przyporządkowuje takiemu ciągowi następnik (w sekwencji liczb naturalnych) jego ostatniego wyrazu. Bowiem suma niepustej a więc izolowanej liczby naturalnej β, będąc jej bezpośrednim poprzednikiem w sekwencji liczb naturalnych (por. §4, Rozdział 9), jest w tej sekwencji ostatnim ze wszystkich jej elementów.

Napiszmy kilka pierwszych wyrazów ciągu $f : \omega \longrightarrow \omega$ definiowanego według (din) przez funkcję h:

(0) $f(0) = h(\varnothing) = \gamma,$
(1) $f(1) = h(f \restriction 1) = S((f \restriction 1)(\bigcup 1)) = S((f \restriction 1)(0)) = S(f(0)) = S(\gamma),$
(2) $f(2) = h(f \restriction 2) = S((f \restriction 2)(\bigcup 2)) = S((f \restriction 2)(1)) = S(f(1)) = S(S(\gamma)).$

W ogólności dla $\varnothing \neq \beta \in \omega$ mamy:

(β) $f(\beta) = h(f \restriction \beta) = S((f \restriction \beta)(\bigcup\beta)) = S(f(\bigcup\beta)),$

a stąd, nic nie tracąc na ogólności, dla dowolnego $\beta \in \omega$:

($S(\beta)$) $f(S(\beta)) = S(f(\bigcup S(\beta))) = S(f(\beta))$, (bo oczywiście $\bigcup S(\beta) = \beta$).

Jest jasne, że dla dowolnego $n \in \omega$, $f(n) = S^n(\gamma)$, gdzie n po prawej stronie równości jest ilością aplikacji operacji S. Oznacza to, że w ograniczonym wypadku, tj. wtedy, gdy $\gamma \in \omega$, można zdefiniować niekontrowersyjnie (zob. uwagi dotyczące poprawności formuły (ψ) służącej do zdefiniowania zbioru $S^\omega(\omega)$ w §5, Rozdział 9) zbiór $S^n(\gamma)$ jako: $S^n(\gamma) := f(n)$, gdzie f jest określona (din) przez opisaną wyżej funkcję h.

W bardziej ogólnym przypadku, gdy γ jest dowolną liczbą porządkową, aby analogicznie zdefiniować zbiór $S^n(\gamma)$, należałoby rozważyć funkcję $h : Cg(\omega, \alpha) \longrightarrow \alpha$, gdzie $\gamma \in \alpha$ oraz α jest graniczna (co jest niemożliwe do przeprowadzenia w §5, Rozdział 9 przed wprowadzeniem liczb ω_1, ω_2 itd.).

Kontynuując dalej nasz przykład, rozważmy funkcję $g : \omega \longrightarrow \omega$ zdefiniowaną następująco: dla dowolnej $\beta \in \omega$, $g(\beta) = \beta + \gamma$. Tutaj, formalnie rzecz biorąc, interpretujemy symbol funkcyjny „+" jako 2-argumentową operację na zbiorach, zdefiniowaną być może niepoprawnie. Jest to bowiem ta operacja, dla której aksjomaty (AN3), (AN4) arytmetyki z dodawaniem (por. §2, Rozdział 7) w interpretacji teoriomnogościowej:

(AN3)$'$ $\forall\delta \in \omega(0 + \delta = \delta)$

(AN4)$'$ $\forall\beta \in \omega\forall\delta \in \omega(S(\beta) + \delta = S(\beta + \delta))$

są prawdziwymi zdaniami w ZFC. Wadliwość takiej definicji polega na braku pewności, czy definiowana w ten sposób operacja + istnieje – postulat prawdziwości (AN3)$'$, (AN4)$'$ w ZFC nie gwarantuje przecież jej istnienia (w przypadku arytmetyki z dodawaniem, istnienie operacji dodawania jest gwarantowane postulowaną prawdziwością formuł (AN3), (AN4), bo są to aksjomaty tej teorii; oczywiście pod warunkiem, że istotnie w jakiejś interpretacji są one prawdziwe, tzn. nie są one sprzeczne).

Przyjmijmy jednak na chwilę, że dysponujemy w ZFC operacją +, która zachowuje się tak, jak mówią o tym formuły (AN3)$'$, (AN4)$'$. Wówczas z definicji funkcji g, na mocy (AN3)$'$ mamy:

$$g(0) = 0 + \gamma = \gamma$$

oraz według (AN4)$'$:

$$g(S(\beta)) = S(\beta) + \gamma = S(\beta + \gamma) = S(g(\beta)).$$

Widać więc, na mocy (0), ($S(\beta)$), że funkcja g spełnia dokładnie te warunki, które, dzięki funkcji h, definiowały funkcję f. Intuicyjnie było jasne, że funkcja h definiuje według (din), tzn. zgodnie z (0) oraz (β), czy też według (0) i ($S(\beta)$), dokładnie jedną funkcję f. Pozostaniemy więc w zgodzie z intuicją, twierdząc, że $g = f$.

Funkcja $f : \omega \longrightarrow \omega$ definiowana według (din) przez funkcję h jest więc 1-argumentową operacją dodawania do ustalonej liczby naturalnej γ.

Sugeruje to możliwość zdefiniowania operacji dodawania na solidniejszych podstawach niż postulat prawdziwości (AN3)$'$, (AN4)$'$. Mianowicie, dla wszystkich liczb naturalnych γ określmy każdy z ciągów $f_\gamma : \omega \longrightarrow \omega$ według (din) przy użyciu funkcji $h_\gamma : Cg(\omega, \omega) \longrightarrow \omega$, zdefiniowanej identycznie jak poprzednio funkcja h (tzn. dla każdej $\gamma \in \omega$, $h_\gamma(\varnothing) = \gamma$ oraz $h_\gamma(g') = S(g'(\bigcup \beta))$ dla ciągu g' długości β, gdzie $\varnothing \neq \beta \in \omega$). Definicje ciągów f_γ dla $\gamma \in \omega$ są więc następujące (zob. warunki (0) oraz $(S(\beta))$):

(+0) $\forall\gamma \in \omega(f_\gamma(0) = \gamma)$ oraz

$(+S(\beta))$ $\forall\beta \in \omega\forall\gamma \in \omega(f_\gamma(S(\beta)) = S(f_\gamma(\beta)))$.

Obecnie możemy standardowo zdefiniować 2-argumentową operację $+$ na zbiorze ω, kładąc dla dowolnych $\beta, \gamma \in \omega$:

(+) $\beta + \gamma = f_\gamma(\beta)$.

Pozostaje pytanie, na jakiej podstawie możemy uznać poprawnie już teraz zdefiniowaną operację $+$, za operację dodawania liczb naturalnych. Jedynym kryterium takiego uznania jest prawdziwość wyrażeń (AN3)$'$, (AN4)$'$ jako twierdzeń ZFC. Rzeczywiście, pozbywając się według definicji (+) symbolu „f_γ” na rzecz symbolu „+” w definicjach (+0), $(+S(\beta))$, uzyskujemy z nich odpowiednio formuły (AN3)$'$, (AN4)$'$. Są to więc twierdzenia ZFC uzyskane bezpośrednio z definicji $(+), (+0), (+S(\beta))$, dlatego często w literaturze są one postrzegane jako właśnie definicja (tzw. indukcyjna) operacji dodawania.

Wracając do rozważań ogólnych, weźmy pod uwagę funkcję $f : \alpha \longrightarrow X$ określoną równością (din) przez funkcję $h : Cg(\alpha, X) \longrightarrow X$, dla liczby porządkowej α oraz niepustego zbioru X.

Zauważmy najpierw, że równość (din) umożliwia rozszerzenie funkcji f na dziedzinę $S(\alpha)$, tzn. można wykorzystać (din) dla określenia wartości $f(\alpha)$ funkcji f na argumencie α, mianowicie, $f(\alpha) = h(f \restriction \alpha)$. Albowiem ciąg $f \restriction \alpha$ jest przecież tożsamy z funkcją f określoną już przez (din) na dziedzinie α, zatem wartość funkcji h na tym ciągu jest dana. Innymi słowy, ciąg f określony na dziedzinie α, wyznacza, dzięki funkcji h, następny wyraz – ciągu określonego już na dziedzinie $S(\alpha)$. Naturalnie ten nowy, dłuższy ciąg przy użyciu h już nie wyznacza kolejnego wyrazu. Funkcja h jest bowiem określona na ciągach długości mniejszej lub równej α, zatem nie jest określona na ciągu długości $S(\alpha)$.

Tak więc, trzy parametry: liczba porządkowa α, niepusty zbiór X oraz funkcja $h : Cg(\alpha, X) \longrightarrow X$, określają funkcję (ciąg pozaskończony) $f : S(\alpha) \longrightarrow X$ taką, że $\forall\beta \in S(\alpha)$, $f(\beta) = h(f \restriction \beta)$. Funkcja f nazywana jest *funkcją definiowaną przez indukcję pozaskończoną.*

Tak podane określenie funkcji definiowanej przez indukcję, jak sama nazwa na to wskazuje, nie jest tzw. *definicją wyraźną*, czyli taką definicją funkcji, która podaje wyraźnie, *explicite*, wartość funkcji dla jej argumentu (definicjami wyraźnymi są na przykład definicje operacji złożenia czy konwersu relacji bądź teoriomnogościowa definicja następnika). Równość: $f(\beta) = h(f \restriction \beta)$ nie podaje wyraźnie wartości funkcji f dla argumentu β, bowiem w prawym jej termie występuje symbol f definiowanej funkcji.

Aby więc formalnie wprowadzić do teorii pojęcie funkcji definiowanej przez indukcję, należy postępować tak, jak w przypadku operacji, których istnienie i jedyność są gwarantowane przez aksjomaty ZFC. Najpierw należy więc wykazać istnienie i jedyność takiej funkcji, czyli dowieść, skądinąd intuicyjnie oczywistego twierdzenia, mówiącego, że dla dowolnych trzech parametrów: α, X, h istnieje dokładnie jedna funkcja $f : S(\alpha) \longrightarrow X$ taka, że $\forall\beta \in S(\alpha), f(\beta) = h(f \restriction \beta)$.

LEMAT. *Dla dowolnych, niepustego zbioru X, liczby porządkowej α oraz funkcji $h : Cg(\alpha, X) \longrightarrow X$ istnieje co najwyżej jedna funkcja $f : S(\alpha) \longrightarrow X$ (to znaczy ciąg pozaskończony typu $S(\alpha)$ elementów zbioru X) taka, że $\forall\beta \in S(\alpha)(f(\beta) = h(f \restriction \beta))$.*

DOWÓD. Niech X będzie niepustym zbiorem, α – liczbą porządkową oraz $h \in X^{Cg(\alpha,X)}$. Załóżmy, że istnieją funkcje f, g takie, że

(1) $\forall\beta \in S(\alpha)(f(\beta) = h(f \restriction \beta))$,

(2) $\forall\beta \in S(\alpha)(g(\beta) = h(g \restriction \beta))$.

Aby wykazać, że $f = g$ skorzystamy z twierdzenia o indukcji pozaskończonej w postaci (**), §5, Rozdział 8, gdzie $W(x)$ jest postaci: $x \in S(\alpha)$ (spełnione są wówczas warunki (war1), (war2) z §4, Rozdział 8, bowiem $S(\alpha)$ jest liczbą porządkową) oraz $\phi(x)$ jest postaci: $f(x) = g(x)$. Zastępując w twierdzeniu o indukcji pozaskończonej zmienne związane x, y odpowiednio zmiennymi β, γ mamy:

$\forall\beta[\beta \in S(\alpha) \Rightarrow (\forall\gamma(\gamma \in \beta \Rightarrow f(\gamma) = g(\gamma)) \Rightarrow f(\beta) = g(\beta))] \Rightarrow$
$\forall\beta(\beta \in S(\alpha) \Rightarrow f(\beta) = g(\beta))$.

Oczywiście równość $f = g$ jest równoważna następnikowi powyższej implikacji. Wykazujemy więc poprzednik. Niech

(3) $\beta \in S(\alpha)$ oraz

(4) $\forall\gamma(\gamma \in \beta \Rightarrow f(\gamma) = g(\gamma))$.

Z (3), $\beta \subseteq S(\alpha)$. Postrzegając liczbę porządkową β jako podzbiór dziedziny funkcji f, g otrzymujemy z (4): $f \restriction \beta = g \restriction \beta$. Stąd natychmiast: $h(f \restriction \beta) = h(g \restriction \beta)$. Zatem na podstawie (1), (2), $f(\beta) = g(\beta)$. □

TWIERDZENIE O DEFINIOWANIU PRZEZ INDUKCJĘ POZASKOŃCZONĄ. *Dla dowolnych, niepustego zbioru X, liczby porządkowej α oraz funkcji $h : Cg(\alpha, X) \longrightarrow X$ istnieje dokładnie jedna funkcja f: $S(\alpha) \longrightarrow X$ taka, że $\forall\beta \in S(\alpha)(f(\beta) = h(f\restriction\beta))$.*

Dowód. Na mocy lematu wystarczy wykazać, że
$\forall X \neq \emptyset\ \forall\alpha\ \forall h \in X^{Cg(\alpha,X)}\ \exists f \in X^{S(\alpha)}\ \forall\beta \in S(\alpha)\ (f(\beta) = h(f \restriction \beta))$.

Weźmy dowolny $X \neq \emptyset$. Dla dowolnej liczby porządkowej α połóżmy
(1) $\psi(\alpha) := \forall h \in X^{Cg(\alpha,X)}\ \exists f \in X^{S(\alpha)}\ \forall\beta \in S(\alpha)\ (f(\beta) = h(f \restriction \beta))$.

Należy więc dowieść, że $\forall\alpha(\psi(\alpha))$. Załóżmy nie wprost, że $\exists\alpha(\neg\psi(\alpha))$. Na mocy Tw. 21, Rozdział 8, niech α_0 będzie najmniejszą liczbą porządkową α taką, że $\neg\psi(\alpha)$. Wówczas mamy (Tw. 19(i)$\Leftrightarrow$(iii), Rozdział 8):
(2) $\neg\psi(\alpha_0)$ oraz
(3) $\forall\gamma(\gamma \in \alpha_0 \Rightarrow \psi(\gamma))$.

Wykażemy sprzeczność z (2), tzn. wykażemy, że zachodzi $\psi(\alpha_0)$. W tym celu, według (1), rozważmy dowolną funkcję $h : Cg(\alpha_0, X) \longrightarrow X$. Skonstruujemy funkcję $f : S(\alpha_0) \longrightarrow X$ taką, że $\forall\gamma \in S(\alpha_0)\ (f(\gamma) = h(f \restriction \gamma))$.

Najpierw określimy funkcję f na dziedzinie α_0. Weźmy pod uwagę dowolną ustaloną liczbę porządkową $\gamma \in \alpha_0$. Na mocy (3) mamy natychmiast: $\psi(\gamma)$. Ponadto według Tw. 1(3), $Cg(\gamma, X) \subseteq Cg(\alpha_0, X)$. Rozważmy więc obcięcie $h \restriction Cg(\gamma, X)$, które oznaczmy jako h_γ. Naturalnie wprost z definicji obcięcia funkcji zachodzi:
(4) $h_\gamma(f') = h(f')$ dla dowolnego ciągu $f' \in Cg(\gamma, X)$.

Zastosujmy wyrażenie $\psi(\gamma)$ dla $h_\gamma \in X^{Cg(\gamma,X)}$. Wówczas z prawdziwości $\psi(\gamma)$ (zob. (1)) oraz na mocy lematu zastosowanego dla zbioru X, liczby porządkowej γ oraz h_γ, istnieje dokładnie jedna funkcja $f_\gamma : S(\gamma) \longrightarrow X$ taka, że $\forall\beta \in S(\gamma)(f_\gamma(\beta) = h_\gamma(f_\gamma \restriction \beta))$. Ostatecznie więc, na mocy (4) mamy:
(5) dla dowolnej $\gamma \in \alpha_0$ istnieje dokładnie jedna funkcja $f_\gamma : S(\gamma) \longrightarrow X$ taka, że $\forall\beta \in S(\gamma)(f_\gamma(\beta) = h(f_\gamma \restriction \beta))$.

Rozważmy teraz liczby porządkowe δ, γ takie że $\delta \in \gamma$ oraz $\gamma \in \alpha_0$. Naturalnie wówczas $\delta \in \alpha_0$. Na mocy (5) mamy dokładnie jedną funkcję $f_\delta : S(\delta) \longrightarrow X$ spełniającą warunek
(6) $\forall\beta \in S(\delta)(f_\delta(\beta) = h(f_\delta \restriction \beta))$,
oraz dokładnie jedną funkcję $f_\gamma : S(\gamma) \longrightarrow X$ taką, że
(7) $\forall\beta \in S(\gamma)(f_\gamma(\beta) = h(f_\gamma \restriction \beta))$.

Ponieważ $\delta \in \gamma$, więc $S(\delta) \subseteq S(\gamma)$ (bo $S(\delta)$ jest, według Tw. 9, Rozdział 9, najmniejszą liczbą porządkową γ taką, że $\delta \in \gamma$, zaś $\delta \in S(\gamma)$), możemy zatem rozważyć obcięcie $f_\gamma{\restriction}S(\delta)$. Oczywiście wówczas
$\forall\beta \in S(\delta)(f_\gamma(\beta) = (f_\gamma{\restriction}S(\delta))(\beta))$, oraz
$\forall\beta \in S(\delta)(f_\gamma \restriction \beta = (f_\gamma {\restriction}S(\delta)) \restriction \beta)$.

Zatem z (7) mamy:
(8) $\forall\beta \in S(\delta)((f_\gamma{\restriction}S(\delta))(\beta) = h((f_\gamma{\restriction}S(\delta)) \restriction \beta))$.

Na mocy (4) można wyrażenia (6), (8) zapisać odpowiednio w postaci:
(9) $\forall\beta \in S(\delta)(f_\delta(\beta) = h_\delta(f_\delta{\restriction} \beta))$,
(10) $\forall\beta \in S(\delta)((f_\gamma{\restriction}S(\delta))(\beta) = h_\delta((f_\gamma{\restriction}S(\delta)){\restriction} \beta))$.

Ponieważ $h_\delta \in X^{Cg(\delta,X)}$, więc można dla liczby porządkowej δ oraz funkcji h_δ zastosować lemat, uzyskując na podstawie (9) i (10) równość:
(11) $f_\gamma \restriction S(\delta) = f_\delta$.
Wobec (11) zachodzi:
(12) dla dowolnych liczb porządkowych $\delta, \gamma \in \alpha_0$: $\delta \in \gamma \Rightarrow f_\gamma(\delta) = f_\delta(\delta)$.
Zdefiniujmy teraz funkcję $g : \alpha_0 \longrightarrow X$ następująco:
(13) $\forall \gamma \in \alpha_0,\ g(\gamma) = f_\gamma(\gamma)$.
Naturalnie $g \in Cg(\alpha_0, X)$, więc $h(g) \in X$. Zdefiniujmy więc funkcję $f : S(\alpha_0) \longrightarrow X$ jak następuje:
(14) $\forall \gamma \in \alpha_0,\ f(\gamma) = g(\gamma)$ oraz
(15) $f(\alpha_0) = h(g)$.
Z określenia (14) mamy natychmiast: $f \restriction \alpha_0 = g$, zatem na mocy określenia (15) otrzymujemy:
(16) $f(\alpha_0) = h(f \restriction \alpha_0)$.
Wystarczy więc jeszcze wykazać, że $\forall \gamma \in \alpha_0\ (f(\gamma) = h(f \restriction \gamma))$, aby skończyć dowód. W tym celu rozważmy dowolną liczbę porządkową $\gamma \in \alpha_0$. Na mocy (14) i (13), $f(\gamma) = f_\gamma(\gamma)$. Lecz na podstawie (5), $f_\gamma(\gamma) = h(f_\gamma \restriction \gamma)$, a zatem $f(\gamma) = h(f_\gamma \restriction \gamma)$. Wystarczy więc wykazać, że $f \restriction \gamma = f_\gamma \restriction \gamma$. Dowodzimy, iż
$\forall \delta \in \gamma, (f \restriction \gamma)(\delta) = (f_\gamma \restriction \gamma)(\delta)$.
Niech więc $\delta \in \gamma$. Oczywiście $\delta \in \alpha_0$. Wówczas z jednej strony mamy: $(f \restriction \gamma)(\delta) = f(\delta) = g(\delta) = f_\delta(\delta)$, na mocy (14) i (13). Z drugiej strony, $(f_\gamma \restriction \gamma)(\delta) = f_\gamma(\delta) = f_\delta(\delta)$, na mocy (12). $\square$

Definicja. Niech α będzie dowolną liczbą porządkową, X – dowolnym niepustym zbiorem oraz $h : Cg(\alpha, X) \longrightarrow X$ dowolną funkcją. Wówczas funkcję f, (której istnienie i jedyność stwierdza twierdzenie o definiowaniu przez indukcję pozaskończoną) spełniającą warunek: $\forall \beta \in S(\alpha), f(\beta) = h(f \restriction \beta)$, nazywamy *funkcją definiowaną przez indukcję pozaskończoną*.

Dla precyzji wprowadźmy 3-argumentową operację din, której wartością $\mathrm{din}(\alpha, X, h)$, jest funkcja definiowana przez indukcję pozaskończoną, tzn.
$\forall \beta \in S(\alpha),\ \mathrm{din}(\alpha, X, h)(\beta) = h(\mathrm{din}(\alpha, X, h) \restriction \beta)$.

Twierdzenie 2. *Dla dowolnych liczb porządkowych α, β, dowolnego zbioru niepustego X oraz funkcji $h : Cg(\alpha, X) \longrightarrow X$:*
$\beta \in \alpha \Rightarrow \mathrm{din}(\alpha, X, h) \restriction S(\beta) = \mathrm{din}(\beta, X, (h \restriction Cg(\beta, X)))$.

Dowód. Niech α, β będą liczbami porządkowymi takimi, że $\beta \in \alpha$. Wówczas naturalnie $S(\beta) \subseteq S(\alpha)$ oraz na podstawie Tw. 1(3), $Cg(\beta, X) \subseteq Cg(\alpha, X)$. Oznaczmy: $f = \mathrm{din}(\alpha, X, h) \restriction S(\beta)$. Rozważmy dowolną liczbę porządkową $\gamma \in S(\beta)$. Wówczas mamy:
$f(\gamma) = (\mathrm{din}(\alpha, X, h) \restriction S(\beta))(\gamma) = \mathrm{din}(\alpha, X, h)(\gamma) = h(\mathrm{din}(\alpha, X, h) \restriction \gamma)$.

Lecz $\mathrm{din}(\alpha, X, h) \restriction \gamma = (\mathrm{din}(\alpha, X, h) \restriction S(\beta)) \restriction \gamma$ bo $\gamma \subseteq S(\beta)$. Zatem $f(\gamma) = h(f \restriction \gamma)$. Ponadto $f \restriction \gamma \in X^\gamma$, zaś $\gamma \subseteq \beta$, zatem $f \restriction \gamma \in Cg(\beta, X)$. Wobec tego, $h(f \restriction \gamma) = h'(f \restriction \gamma)$, gdzie $h' = h \restriction Cg(\beta, X)$. Ostatecznie więc, $\forall \gamma \in S(\beta)(f(\gamma) = h'(f \restriction \gamma))$, tzn. funkcja $f : S(\beta) \longrightarrow X$ jest definiowana przez indukcję pozaskończoną dla liczby porządkowej β, zbioru X oraz funkcji $h' : Cg(\beta, X) \longrightarrow X$. Na mocy twierdzenia o definiowaniu przez indukcję istnieje dokładnie jedna funkcja definiowana przez indukcję dla powyższych parametrów – jest nią $\mathrm{din}(\beta, X, h')$. Zatem $f = \mathrm{din}(\beta, X, h')$, tzn. $\mathrm{din}(\alpha, X, h) \restriction S(\beta) = \mathrm{din}(\beta, X, (h \restriction Cg(\beta, X)))$. $\square$

§3. Aksjomat wyboru, funkcja wyboru

Zapiszmy aksjomat wyboru (AxC) (zob. §1, Rozdział 1) bardziej czytelnie:

$(AxC)'$ $\forall z[\forall x, y \in z(x \neq \varnothing \wedge (x \cap y \neq \varnothing \Rightarrow x = y)) \Rightarrow$
$\exists u \forall x \in z \exists v(u \cap x = \{v\})]$.

Wykazujemy, że $(AxC)'$ jest równoważny wyrażeniu:

$(AxC)''$ Dla dowolnego $z \neq \varnothing$ oraz dowolnego podziału Π zbioru z:
$\exists u \forall x \in \Pi \exists v(u \cap x = \{v\})$.

(Dla dowolnego podziału zbioru niepustego istnieje zbiór, który z każdym elementem tego podziału ma dokładnie jeden element wspólny.)

$(AxC)' \Rightarrow (AxC)''$: Załóżmy $(AxC)'$. Niech $z \neq \varnothing$ oraz Π będzie podziałem zbioru z. Wówczas z definicji podziału mamy:

$\forall x, y \in \Pi(x \neq \varnothing \wedge (x \cap y \neq \varnothing \Rightarrow x = y))$.

Zatem z $(AxC)'$ otrzymujemy:

$\exists u \forall x \in \Pi \exists v(u \cap x = \{v\})$.

$(AxC)'' \Rightarrow (AxC)'$: Załóżmy $(AxC)''$. Niech z będzie dowolnym zbiorem. Gdy $z = \varnothing$, to naturalnie następnik implikacji w (AxC)$'$ jest prawdziwy (np. dla $u = \varnothing$ prawdą jest, że $\forall x \in \varnothing \exists v(u \cap x = \{v\})$), co dowodzi prawdziwości $(AxC)'$.

Niech $z \neq \varnothing$. Załóżmy poprzednik implikacji w $(AxC)'$. Stąd mamy natychmiast:

(1) $\forall x \in z(x \neq \varnothing)$,

(2) $\forall x, y \in z(x \cap y \neq \varnothing \Rightarrow x = y)$,

co oznacza, że z jest podziałem niepustego zbioru: $\bigcup z$ (ponieważ $z \neq \emptyset$, więc pewien $x \in z$, lecz z (1), $x \neq \emptyset$, zaś $x \subseteq \bigcup z$, stąd $\bigcup z \neq \emptyset$). Stosując $(AxC)''$ dla niepustego zbioru $\bigcup z$ i jego podziału z, otrzymujemy następnik implikacji w $(AxC)'$.

Tak więc, dla dowolnego niepustego zbioru Π niepustych i parami rozłącznych zbiorów (tzn. podziału Π niepustego zbioru $\bigcup \Pi$) aksjomat wyboru gwarantuje istnienie takiego zbioru u, który z każdym elementem zbioru Π ma dokładnie jeden wspólny element.

Zwróćmy uwagę na to, że w nazwie „teoria ZFC" litera „C" oznacza, iż formuła (AxC) jest aksjomatem teorii (por. Wstęp). Teoria Zermelo-Fraenkla bez aksjomatu wyboru oznaczana jest symbolem „ZF". To specjalne wyróżnienie aksjomatu wyboru wśród aksjomatów ZFC, spowodowane jest tym, że w historii rozwoju teorii mnogości aksjomat ten nie był powszechnie akceptowany. Aby wyjaśnić dlaczego, dokonajmy pewnego porównania aksjomatu wyboru z pozostałymi aksjomatami teorii.

Wśród wszystkich tych aksjomatów ZFC, które, na ogół po spełnieniu pewnych warunków wstępnych, postulują istnienie pewnego zbioru, każdy z następujących czterech: $(AxZ)_\phi$, (AxP), $(Ax\bigcup)$, $(AxSUB)$, w obecności aksjomatu identyczności, gwarantuje istnienie dokładnie jednego zbioru dla ustalonych warunków wstępnych (w przypadku (AxP) i $(Ax\bigcup)$ warunki wstępne sprowadzają się do ustalenia uwagi na jakimś zbiorze). Co więcej, każdy z tych czterech aksjomatów w pełni określa ów jedyny zbiór, którego istnienie stwierdza, przez jawne podanie jego elementów. Mówi się, że taki jedyny zbiór jest, dla danych warunków wstępnych, *konstruowalny*. Pozostałe dwa aksjomaty z tej grupy, aksjomat nieskończoności oraz właśnie aksjomat wyboru, bez względu na obecność aksjomatu identyczności, nie gwarantują wcale istnienia dokładnie jednego zbioru ($(Ax\infty)$ bezwarunkowo, zaś (AxC) przy warunku wstępnym jakim jest ustalenie uwagi na niepustym zbiorze niepustych, parami rozłącznych zbiorów). Aksjomat nieskończoności nie zapewnia przecież istnienia dokładnie jednego zbioru indukcyjnego. Jednakże użytek, jaki czyni się w teorii z tego aksjomatu polega, z jednej strony, na zagwarantowaniu niepustości świata zbiorów (czego potrzeba nie może być kwestionowana), z drugiej zaś strony, na *konstrukcji*, przy wykorzystaniu aksjomatu podzbiorów, pewnego, jedynego zbioru indukcyjnego, mianowicie, najmniejszego zbioru indukcyjnego, jakim jest zbiór liczb naturalnych (por. Twierdzenia 11, 12, Rozdział 7). Choć więc aksjomat nieskończoności nie wyróżnia żadnego spośród tych wszystkich zbiorów, których istnienie stwierdza, to jednak własności każdego z nich są takie, że zastosowanie aksjomatu podzbiorów powoduje jednak wyróżnienie wśród nich dokładnie jednego – tego, który dalej w teorii, jako jedyny spośród wszystkich tych zbiorów, jest istotny.

Podobnie, aksjomat wyboru nie zapewnia istnienia dokładnie jednego zbioru, który z każdym elementem danego podziału ma dokładnie jeden element wspólny. Lecz w przeciwieństwie do aksjomatu nieskończoności, nie widać w jaki sposób aksjomat wyboru miałby choć umożliwić wyróżnienie jednego spośród tych zbiorów, których istnienie stwierdza. Co więcej, w zastosowaniach tego aksjomatu w teorii, żadnego z takich zbiorów nawet nie próbuje się wyróżniać. Krótko mówiąc, aksjomat wyboru stwierdza istnienie *niekonstruowalnych* zbiorów, z których teoria dalej robi użytek.

Nie każdy dopuszcza do istnienia niezupełnie dookreślone, czy wręcz nieokreślone twory. Stąd niektórzy kwestionują zasadność uznania (AxC) za aksjomat teorii mnogości. Niektórzy zaś, akceptując aksjomat wyboru, odróżniają jednak te twierdzenia, których dowody ów aksjomat umożliwia, od pozostałych twierdzeń, podkreślając w ten sposób jakby inną ich wartość. Naturalnie z formalno-logicznego punktu widzenia, aksjomat wyboru jest zwyczajnym zdaniem ustalonego języka I rzędu, jeśli więc tylko nie prowadzi do sprzeczności, to z owego punktu widzenia, jest aksjomatem teorii równoprawnym pozostałym.

Warto jeszcze zwrócić uwagę na fakt, że niedookreśloności zbioru, który ma dokładnie jeden element wspólny z każdym elementem danego podziału, nie należy wiązać z niewystępowaniem w aksjomacie wyboru charakterystyki tych elementów tego zbioru, które do żadnego z elementów podziału nie należą. Można bowiem w banalny sposób taką charakterystykę podać – twierdząc, że takich elementów nie ma. Mianowicie, nietrudno wykazać, że w obecności aksjomatu podzbiorów, aksjomat wyboru jest równoważny następującemu wyrażeniu:

$(AxC)'''$ Dla dowolnego $z \neq \varnothing$ oraz dowolnego podziału Π zbioru z:
$\exists u(u \subseteq z \wedge \forall x \in \Pi \exists v(u \cap x = \{v\}))$.

(Dla dowolnego podziału zbioru niepustego istnieje taki podzbiór tego zbioru, który z każdym elementem tego podziału ma dokładnie jeden element wspólny.)

Implikacja $(AxC)''' \Rightarrow (AxC)''$ jest oczywista. Aby wykazać implikację odwrotną, załóżmy $(AxC)''$ i rozważmy dowolny podział Π niepustego zbioru z. Na mocy założenia, niech A będzie takim zbiorem, że

(3) $\forall x \in \Pi \exists v(A \cap x = \{v\})$.

Ponieważ poprzednik aksjomatu podzbiorów:

$\forall v(\phi(v) \Rightarrow v \in A) \Rightarrow \exists y \forall v(v \in y \Leftrightarrow \phi(v))$,

dla $\phi(v) := \exists x(x \in \Pi \wedge A \cap x = \{v\})$, jest spełniony, niech więc B będzie tym jedynym (dla ustalonego zbioru A) zbiorem określonym przez następnik w tym aksjomacie, to znaczy

(4) $\forall v(v \in B \Leftrightarrow \exists x(x \in \Pi \wedge A \cap x = \{v\}))$.

Wówczas

(5) $B \subseteq z$.

Niech bowiem $v \in B$. Wtedy z (4), dla pewnego $x \in \Pi$, $A \cap x = \{v\}$. Zatem $v \in x$. Ostatecznie $v \in \bigcup \Pi$, czyli $v \in z$, bo Π jest podziałem zbioru z.

Ponadto,

(6) $\forall x \in \Pi \exists v(B \cap x = \{v\})$.

Niech bowiem $x \in \Pi$. Wówczas z (3), niech w będzie takim zbiorem, że

(7) $A \cap x = \{w\}$.

Stąd, $w \in x$ oraz według (4), $w \in B$. Zatem $\{w\} \subseteq B \cap x$. Aby dowieść inkluzji przeciwnej, co zakończy dowód (6), załóżmy, że $v \in B$ oraz $v \in x$. Wówczas z (4), niech $y \in \Pi$ będzie taki, że $A \cap y = \{v\}$. Zatem $v \in y$. Lecz skoro $v \in x$, więc $x \cap y \neq \varnothing$. Ponieważ x, y są elementami podziału Π, więc $y = x$. Zatem $A \cap x = \{v\}$, co wobec (7) implikuje $\{v\} = \{w\}$, tzn. $v \in \{w\}$. Wobec dowolności wyboru v, $B \cap x \subseteq \{w\}$.

Ostatecznie, z (5) i (6) bezpośrednio wynika formuła $\exists u(u \subseteq z \wedge \forall x \in \Pi \exists v(u \cap x = \{v\}))$.

Jak widać, dla dowolnego podziału niepustego zbioru, aksjomat wyboru w postaci $(AxC)'''$ zapewnia istnienie pewnego podzbioru tego zbioru, a więc jest pod tym względem podobny do aksjomatu podzbiorów. Lecz, w przeciwieństwie do tego aksjomatu, nie gwarantuje on (w obecności aksjomatu identyczności) istnienia dokładnie jednego podzbioru, przez co nie podaje *konstruktywnie* elementów żadnego z tych podzbiorów, których istnienie stwierdza. W tym sensie są one obiektami niedookreślonymi.

W dalszym ciągu aksjomat wyboru posłuży nam do wykazania faktu (skądinąd równoważnego temu aksjomatowi) mówiącego, że dla dowolnego niepustego zbioru istnieje tzw. *stowarzyszona z nim funkcja wyboru*, co w konsekwencji, wraz z zastosowaniem definiowania przez indukcję pozaskończoną, umożliwia wykazanie innego faktu, iż dla dowolnego niepustego zbioru istnieje liczba porządkowa mająca tyle samo elementów co ten zbiór. To z kolei prowadzi do definicji liczby kardynalnej zbioru.

DEFINICJA. Niech u będzie dowolnym niepustym zbiorem. Przez *funkcję wyboru dla zbioru u* (lub *stowarzyszoną ze zbiorem u*) rozumiemy dowolną funkcję $f\colon P(u) \longrightarrow u$ taką, że $\forall y \in P(u) - \{\varnothing\}, f(y) \in y$.

Uwaga. Zdefiniowany tu został nie symbol funkcyjny, lecz predykat „*jest funkcją wyboru*”, stąd dowody istnienia i jedyności są niepotrzebne. Niemniej jednak, w dalszym ciągu wykazujemy, że istnieją obiekty teoriomnogościowe, o których można zgodnie z prawdą ten predykat orzec.

Przykład. Istnieją dokładnie cztery funkcje wyboru f_1, f_2, f_3, f_4 dla 2-elementowego zbioru $\{a, b\}$:

$f_1(\varnothing) = a,\ f_1(\{a\}) = a,\ f_1(\{b\}) = b,\ f_1(\{a, b\}) = a,$
$f_2(\varnothing) = a,\ f_2(\{a\}) = a,\ f_2(\{b\}) = b,\ f_2(\{a, b\}) = b,$
$f_3(\varnothing) = b,\ f_3(\{a\}) = a,\ f_3(\{b\}) = b,\ f_3(\{a, b\}) = a,$
$f_4(\varnothing) = b,\ f_4(\{a\}) = a,\ f_4(\{b\}) = b,\ f_4(\{a, b\}) = b.$

Istnienie funkcji wyboru dla każdego niepustego zbioru u jest gwarantowane przez aksjomat wyboru. Istotnie, niech y będzie dowolnym niepustym podzbiorem zbioru u. Wówczas oczywiście $\{y\} \times y \subseteq P(u) \times u$, czyli $\{y\} \times y \in P(P(u) \times u)$. Rozważmy aksjomat podzbiorów z formułą $\phi(x)$ postaci:

$\exists y(y \in P(u) - \{\varnothing\} \wedge x = \{y\} \times y).$

Ponieważ zachodzi:

$\forall x(\phi(x) \Rightarrow x \in P(P(u) \times u)),$

więc z owego aksjomatu otrzymujemy:

$\exists z \forall x(x \in z \Leftrightarrow \exists y(y \in P(u) - \{\varnothing\} \wedge x = \{y\} \times y)).$

Oznaczmy symbolem „Π” ten (jedyny) zbiór, którego istnienie stwierdza powyższa formuła. Mamy więc:

$\forall x(x \in \Pi \Leftrightarrow \exists y(y \in P(u) - \{\varnothing\} \wedge x = \{y\} \times y))$, lub równoważnie:

$\Pi = \{\{y\} \times y : y \in P(u) - \{\varnothing\}\}.$

Jest oczywiste, że $\varnothing \notin \Pi$. Ponadto spełniony jest warunek:

$\forall v, w \in \Pi(v \cap w \neq \varnothing \Rightarrow v = w).$

Jeśli bowiem $v, w \in \Pi$, to wówczas $v = \{y_1\} \times y_1, w = \{y_2\} \times y_2$ dla pewnych niepustych $y_1, y_2 \subseteq u$. Wtedy $v = \{<y_1, x>: x \in y_1\}$ oraz $w = \{<y_2, x>: x \in y_2\}$. Zatem założenie $v \cap w \neq \varnothing$ implikuje $<y_1, x_1> = <y_2, x_2>$ dla pewnych $x_1 \in y_1, x_2 \in y_2$. Stąd $y_1 = y_2$ i konsekwentnie $v = w$.

Tak więc, Π jest podziałem niepustego zbioru $\bigcup \Pi$. Na mocy aksjomatu wyboru $(AxC)''$ niech A będzie zbiorem takim, że

$\forall x \in \Pi \exists z (A \cap x = \{z\})$.

Weźmy więc pod uwagę dowolny $x \in \Pi$. Wówczas $x = \{y\} \times y$, gdzie $\emptyset \neq y \subseteq u$. Zatem iloczyn $A \cap (\{y\} \times y)$ jest zbiorem 1-elementowym $\{z\}$. Wówczas z jest postaci $<y, v>$, gdzie $v \in y$, przy czym v jest jedynym elementem zbioru y takim, że $<y, v> \in A$. Konsekwentnie zbiór par uporządkowanych:

$\{<\emptyset, v_0>\} \cup (\bigcup \Pi \cap A) = \{<\emptyset, v_0>\} \cup (\{<y, v>: y \in P(u) - \{\emptyset\} \wedge v \in y\} \cap A)$,

gdzie $v_0 \in u$ jest dowolnie wybranym elementem $(u \neq \emptyset)$, jest funkcją $f : P(u) \longrightarrow u$ taką, że dla dowolnego $y \in P(u) - \{\emptyset\}$, $f(y) \in y$ (bowiem $f(y)$ jest tym jedynym elementem zbioru y, że $<y, f(y)> \in A$).

Dla pewnych zbiorów, na przykład dla zbiorów liczb porządkowych, aby uzasadnić istnienie stowarzyszonych z nimi funkcji wyboru, nie musimy odwoływać się do aksjomatu wyboru:

TWIERDZENIE 3. *Niech x będzie dowolnym niepustym zbiorem liczb porządkowych. Wówczas funkcja $f : P(x) \longrightarrow x$ określona następująco: $f(\emptyset) = nlp(x), \forall y \in P(x) - \{\emptyset\}, f(y) = nlp(y)$, jest funkcją wyboru dla zbioru x.*

DOWÓD. Oczywisty na mocy definicji funkcji wyboru oraz najmniejszej liczby porządkowej w danym zbiorze liczb porządkowych. □

DEFINICJA. Dla dowolnego niepustego zbioru x liczb porządkowych niech wb będzie 1-argumentową operacją przyporządkowującą zbiorowi x funkcję wyboru dla zbioru x określoną w Tw. 3, tzn. $wb(x)(\emptyset) = nlp(x)$ oraz $wb(x)(y) = nlp(y)$ dla każdego niepustego $y \subseteq x$.

$wb(x)$ nazwijmy *funkcją wyboru zbioru liczb porządkowych x.*

§4. Funkcja definiowana przez indukcję pozaskończoną wyznaczona przez funkcję wyboru dla dowolnego zbioru

Niech teraz X będzie dowolnym niepustym zbiorem oraz f dowolną funkcją wyboru dla zbioru X. Niech ponadto α będzie dowolną liczbą porządkową. Te trzy parametry wyznaczają jednoznacznie funkcję $h : Cg(\alpha, X) \longrightarrow X$ następująco: $h(\emptyset) = f(\emptyset)$ oraz $h(g) = f(X - \overrightarrow{g}(\beta))$ dla dowolnej niepustej liczby porządkowej $\beta \subseteq \alpha$ (gdy $\alpha \neq \emptyset$), i dowolnego ciągu $g : \beta \longrightarrow X$. Dalej, tak określona funkcja h, jako zależna od owych trzech parametrów, będzie oznaczana w postaci $h(\alpha, X, f)$.

Przykład. Funkcja wyboru f_1 dla zbioru $X = \{a, b\}$ z poprzedniego przykładu (§3) oraz liczba porządkowa ω wyznaczają funkcję $h(\omega, X, f_1) : Cg(\omega, X) \longrightarrow X$ w następujący sposób: $h(\omega, X, f_1)(\varnothing) = f_1(\varnothing) = a$ oraz dla dowolnego ciągu $g : \beta \longrightarrow X$ dla $\varnothing \neq \beta \subseteq \omega$:

$$h(\omega, X, f_1)(g) = f_1(X - \vec{g}(\beta)) = \begin{cases} b, & \text{gdy dla każdej } \gamma \in \beta,\ g(\gamma) = a \\ a, & \text{gdy dla pewnej } \gamma \in \beta,\ g(\gamma) = b. \end{cases}$$

Twierdzenie 4. *Dla dowolnych liczb porządkowych α, β, dowolnego zbioru $X \neq \varnothing$ oraz dowolnej funkcji wyboru f dla X:*
$\beta \in \alpha \Rightarrow h(\beta, X, f) = h(\alpha, X, f) \restriction Cg(\beta, X)$.

Dowód. Niech $\beta \in \alpha$. Wówczas na mocy Tw. 1(3), $Cg(\beta, X) \subseteq Cg(\alpha, X)$, zatem sensownie jest rozważać obcięcie $h(\alpha, X, f) \restriction Cg(\beta, X)$. Mamy więc: $(h(\alpha, X, f) \restriction Cg(\beta, X))(\varnothing) = h(\alpha, X, f)(\varnothing) = f(\varnothing) = h(\beta, X, f)(\varnothing)$. I dalej, dla dowolnego ciągu $g \in Cg(\beta, X)$ takiego, że $g : \gamma \longrightarrow X$, gdzie $\varnothing \neq \gamma \subseteq \beta$: $(h(\alpha, X, f) \restriction Cg(\beta, X))(g) = h(\alpha, X, f)(g) = f(X - \vec{g}(\gamma)) = h(\beta, X, f)(g)$. □

Kolejne fakty dotyczą dowolnego niepustego zbioru X oraz dowolnej funkcji wyboru f dla X. Traktujemy te dwa parametry jako ustalone. Dla dowolnej liczby porządkowej α oznaczmy $d_\alpha := \mathrm{din}(\alpha, X, h(\alpha, X, f))$. Wówczas

(*) $d_\alpha(\varnothing) = h(\alpha, X, f)(d_\alpha \restriction \varnothing) = h(\alpha, X, f)(\varnothing) = f(\varnothing)$ oraz

(**) $d_\alpha(\beta) = h(\alpha, X, f)(d_\alpha \restriction \beta) = f(X - \overrightarrow{(d_\alpha \restriction \beta)}\,(\beta)) = f(X - \vec{d_\alpha}\,(\beta))$,

gdy $\varnothing \neq \beta \in S(\alpha)$.

Twierdzenie 5. *Dla dowolnych liczb porządkowych α, β:*
(1) $\beta \in \alpha \Rightarrow d_\alpha \restriction S(\beta) = d_\beta$,
(2) $\beta \in \alpha \Rightarrow d_\alpha(\beta) = d_\beta(\beta)$.

Dowód. Dla (1): Załóżmy, że $\beta \in \alpha$. Wówczas, na mocy Tw. 2, mamy: $\mathrm{din}(\alpha, X, h(\alpha, X, f)) \restriction S(\beta) = \mathrm{din}(\beta, X, (h(\alpha, X, f) \restriction Cg(\beta, X)))$. Lecz na mocy Tw. 4, $h(\alpha, X, f) \restriction Cg(\beta, X) = h(\beta, X, f)$, zatem $d_\alpha \restriction S(\beta) = \mathrm{din}(\beta, X, h(\beta, X, f))$ $= d_\beta$.

(2) jest bezpośrednią konsekwencją (1). □

Twierdzenie 6. *Dla dowolnej liczby porządkowej α, jeżeli d_α: $S(\alpha) \longrightarrow X$ nie przekształca zbioru $S(\alpha)$ na zbiór X, to d_α jest różnowartościowa.*

Dowód. Załóżmy, że $X - \overrightarrow{d_\alpha}(S(\alpha)) \neq \varnothing$. Rozważmy liczby porządkowe $\beta, \gamma \in S(\alpha)$ takie, że $\beta \neq \gamma$. Wówczas albo $\beta \in \gamma$ albo $\gamma \in \beta$. Załóżmy, że $\beta \in \gamma$. Naturalnie wtedy $\gamma \neq \varnothing$, zatem z (**) mamy:

(1) $d_\alpha(\gamma) = f(X - \overrightarrow{d_\alpha}(\gamma))$.

Ponieważ $\gamma \subseteq S(\alpha)$ (bo $\gamma \in S(\alpha)$), więc $\overrightarrow{d_\alpha}(\gamma) \subseteq \overrightarrow{d_\alpha}(S(\alpha))$. Zatem $X - \overrightarrow{d_\alpha}(S(\alpha)) \subseteq X - \overrightarrow{d_\alpha}(\gamma)$, czyli na mocy założenia, $X - \overrightarrow{d_\alpha}(\gamma) \neq \varnothing$. Wówczas z definicji funkcji wyboru, $f(X - \overrightarrow{d_\alpha}(\gamma)) \in X - \overrightarrow{d_\alpha}(\gamma)$, więc z (1), $d_\alpha(\gamma) \notin \overrightarrow{d_\alpha}(\gamma)$. Lecz skoro $\beta \in \gamma$, to $d_\alpha(\beta) \in \overrightarrow{d_\alpha}(\gamma)$, zatem $d_\alpha(\beta) \neq d_\alpha(\gamma)$. Gdy $\gamma \in \beta$, dowód przebiega analogicznie. □

Twierdzenie 7. *Dla dowolnej liczby porządkowej* α:

(1) $\forall \gamma \in S(\alpha)$ [*jeżeli* $X - \overrightarrow{d_\alpha}(\gamma) \neq \varnothing$, *to* $d_\alpha(\gamma) \notin \overrightarrow{d_\alpha}(\gamma)$],

(2) $\forall \gamma \in S(\alpha)$ [*jeżeli* $X - \overrightarrow{d_\alpha}(\gamma) \neq \varnothing$, *to* $\forall \beta(\beta \in \gamma \Rightarrow d_\alpha(\beta) \neq d_\alpha(\gamma))$],

(3) *jeżeli* $X - \overrightarrow{d_\alpha}(\alpha) \neq \varnothing$, *to* $\forall \beta(\beta \in \alpha \Rightarrow d_\alpha(\beta) \neq d_\alpha(\alpha))$,

(4) *jeżeli* $X - \overrightarrow{d_\alpha}(\alpha) \neq \varnothing$, *to* $\forall \beta(\beta \in \alpha \Rightarrow d_\beta(\beta) \neq d_\alpha(\alpha))$.

Dowód. Dla (1): Niech $\gamma \in S(\alpha)$. Załóżmy, że $X - \overrightarrow{d_\alpha}(\gamma) \neq \varnothing$.

Gdy $\gamma = \varnothing$, to naturalnie $\overrightarrow{d_\alpha}(\gamma) = \varnothing$, więc $d_\alpha(\gamma) \notin \overrightarrow{d_\alpha}(\gamma)$.

Niech $\gamma \neq \varnothing$. Wówczas na mocy (**), $d_\alpha(\gamma) = f(X - \overrightarrow{d_\alpha}(\gamma))$. Z założenia, $f(X - \overrightarrow{d_\alpha}(\gamma)) \in X - \overrightarrow{d_\alpha}(\gamma)$, zatem $d_\alpha(\gamma) \notin \overrightarrow{d_\alpha}(\gamma)$.

Dla (2): Niech $\gamma \in S(\alpha)$. Załóżmy, że $X - \overrightarrow{d_\alpha}(\gamma) \neq \varnothing$ oraz weźmy liczbę porządkową β taką, że $\beta \in \gamma$. Wówczas z (1) mamy: $d_\alpha(\gamma) \notin \overrightarrow{d_\alpha}(\gamma)$. Jednakże $d_\alpha(\beta) \in \overrightarrow{d_\alpha}(\gamma)$, zatem $d_\alpha(\beta) \neq d_\alpha(\gamma)$.

(3) jest bezpośrednią konsekwencją (2), gdy $\gamma = \alpha$.

(4) jest bezpośrednią konsekwencją (3) oraz Tw. 5(2). □

Twierdzenie 8. *Istnieje liczba porządkowa* α *taka, że* $X \subseteq \overrightarrow{d_\alpha}(\alpha)$.

Dowód. Załóżmy nie wprost, iż dla każdej liczby porządkowej α, $X \nsubseteq \overrightarrow{d_\alpha}(\alpha)$. Zatem $X - \overrightarrow{d_\alpha}(\alpha) \neq \varnothing$, dla każdej α. Wobec tego, na mocy Tw. 7(4) otrzymujemy:

(1) $\forall \alpha \forall \beta(\beta \in \alpha \Rightarrow d_\beta(\beta) \neq d_\alpha(\alpha))$.

Wówczas spełniony jest warunek:

(2) dla dowolnych liczb porządkowych α, β : $\alpha \neq \beta \Rightarrow d_\alpha(\alpha) \neq d_\beta(\beta)$.

Załóżmy, bowiem, że $\alpha \neq \beta$. Wtedy $\beta \in \alpha$ lub $\alpha \in \beta$. Gdy $\beta \in \alpha$, to z (1), $d_\beta(\beta) \neq d_\alpha(\alpha)$. Gdy zaś $\alpha \in \beta$, rozumowanie przebiega analogicznie – wystarczy w (1) zamienić α na β oraz β na α.

Weźmy teraz pod uwagę aksjomat podzbiorów $(\mathrm{AxZ})_\phi$ w postaci:
$\forall x(\exists\alpha(x = d_\alpha(\alpha)) \Rightarrow x \in X) \Rightarrow \exists y \forall x(x \in y \Leftrightarrow \exists\alpha(x = d_\alpha(\alpha)))$.

Ponieważ dla dowolnej liczby porządkowej $\alpha, d_\alpha(\alpha) \in X$, więc poprzednik powyższej implikacji jest spełniony. Mamy więc następnik, a stąd istnienie zbioru:
$L = \{x : \exists\alpha(x = d_\alpha(\alpha))\} = \{d_\alpha(\alpha) : \alpha \text{ jest liczbą porządkową}\}$.

Rozważać teraz będziemy aksjomat podstawiania $(AxSUB)_\psi$, w którym poprzednik ma postać:
(3) $\forall y \exists z(\psi(y, z) \wedge \forall v(\psi(y, v) \Rightarrow v = z))$,
gdzie $\psi(y, z)$ jest postaci:
$(y \notin L \wedge z = y) \vee \exists\alpha(\alpha \text{ jest liczbą porządkową} \wedge y = d_\alpha(\alpha) \wedge z = \alpha)$.

Wykażmy, że (3) jest spełnione. Weźmy pod uwagę dowolny zbiór y. Oczywiście $y \notin L \vee y \in L$.

Niech $y \notin L$. Połóżmy $z_0 = y$. Wówczas zachodzi $\psi(y, z_0)$. Aby dowieść, iż $\forall v(\psi(y, v) \Rightarrow v = z_0)$, załóżmy, że $\psi(y, v)$. Prawdziwość prawego członu alternatywy $\psi(y, v)$ oznaczałaby, że $y \in L$. Lecz $y \notin L$. Zatem lewy jej człon jest prawdziwy, czyli $y \notin L \wedge v = y$. Stąd oczywiście $v = z_0$. Ostatecznie $\exists z(\psi(y, z) \wedge \forall v(\psi(y, v) \Rightarrow v = z))$.

Niech teraz $y \in L$. Zatem $y = d_{\alpha_0}(\alpha_0)$ dla pewnej liczby porządkowej α_0. Połóżmy $z_0 = \alpha_0$. Wówczas prawdą jest, że $\exists\alpha(\alpha \text{ jest liczbą porządkową} \wedge y = d_\alpha(\alpha) \wedge z_0 = \alpha)$, czyli zachodzi $\psi(y, z_0)$. Wykazując, iż $\forall v(\psi(y, v) \Rightarrow v = z_0)$, załóżmy, że $\psi(y, v)$. Wówczas naturalnie prawdziwy jest prawy człon alternatywy $\psi(y, v) :\ \exists\alpha(\alpha \text{ jest liczbą porządkową} \wedge y = d_\alpha(\alpha) \wedge v = \alpha)$. Zatem dla pewnej liczby porządkowej β, $y = d_\beta(\beta) \wedge v = \beta$. Lecz jednocześnie $y = d_{\alpha_0}(\alpha_0)$, zatem $d_{\alpha_0}(\alpha_0) = d_\beta(\beta)$. Wobec tego na mocy (2) otrzymujemy: $\beta = \alpha_0$ i konsekwentnie $v = \alpha_0 = z_0$, co kończy dowód (3).

Ostatecznie, formuła $\psi(y, z)$ ustala na mocy (3) jednoznaczną odpowiedniość między elementami zbioru L postaci $d_\alpha(\alpha)$ a liczbami porządkowymi α (jak również między zbiorami nienależącymi do L a nimi samymi, co nie jest interesujące). Możemy więc z aksjomatu podstawiania oderwać następnik, postaci:
$\exists u \forall z(z \in u \Leftrightarrow \exists y(y \in L \wedge \psi(y, z)))$,
w ten sposób uzyskując istnienie zbioru:
$\{z : \exists y(y \in L \wedge \psi(y, z))\}$.

Wyrażenie $y \in L \wedge \psi(y, z)$ jest równoważne koniunkcji:
$y \in L \wedge \exists\alpha(\alpha \text{ jest liczbą porządkową} \wedge y = d_\alpha(\alpha) \wedge z = \alpha)$,
która z kolei, według definicji zbioru L, jest równoważna swojemu prawemu członowi.

Konsekwentnie na mocy aksjomatu podstawiania, uzyskaliśmy istnienie zbioru: $\{z : \exists y \exists \alpha(\alpha \text{ jest liczbą porządkową } \wedge\, y = d_\alpha(\alpha) \wedge z = \alpha)\}$.

Widać, iż jest to zbiór, którego elementami są wszystkie liczby porządkowe i tylko one, co przeczy Tw. 6, Rozdział 9. $\square$

Możemy obecnie sformułować twierdzenie, umożliwiające określenie rozważanego w następnym rozdziale pojęcia liczby kardynalnej:

TWIERDZENIE 9. *Dla dowolnego niepustego zbioru X, dla dowolnej funkcji wyboru f dla zbioru X istnieje liczba porządkowa α taka, że funkcja $din(\alpha, X, h(\alpha, X, f))\restriction \alpha : \alpha \longrightarrow X$ jest bijekcją.*

DOWÓD. Niech $X \neq \varnothing$ oraz f będzie funkcją wyboru dla X. Na mocy Tw. 8 oraz Tw. 21, Rozdział 8, niech α_0 będzie najmniejszą liczbą porządkową α taką, że $X \subseteq \overrightarrow{d_\alpha}(\alpha)$, gdzie, jak poprzednio, $d_\alpha = \mathrm{din}(\alpha, X, h(\alpha, X, f))$. Wykażemy, że właśnie $d_{\alpha_0}\restriction\alpha_0 : \alpha_0 \longrightarrow X$ jest bijekcją.

Skoro α_0 jest najmniejszą liczbą porządkową α taką, że $X \subseteq \overrightarrow{d_\alpha}(\alpha)$, więc według Tw. 19(i)$\Rightarrow$(iii), Rozdział 8 mamy:

(1) $X \subseteq \overrightarrow{d_{\alpha_0}}(\alpha_0)$ oraz

(2) $\forall \beta(\beta \in \alpha_0 \Rightarrow X \nsubseteq \overrightarrow{d_\beta}(\beta))$.

Ponieważ z definicji funkcji d_{α_0}, $\overrightarrow{d_{\alpha_0}}(S(\alpha_0)) \subseteq X$ oraz naturalnie $\overrightarrow{d_{\alpha_0}}(\alpha_0) \subseteq \overrightarrow{d_{\alpha_0}}(S(\alpha_0))$ (bo $\alpha_0 \subseteq S(\alpha_0)$), więc na mocy (1) otrzymujemy: $\overrightarrow{d_{\alpha_0}}(\alpha_0) = X$. Oznacza to, że funkcja $d_{\alpha_0}\restriction\alpha_0$ przekształca α_0 na zbiór X.

Aby wykazać, że $d_{\alpha_0}\restriction\alpha_0$ jest różnowartościowa, załóżmy nie wprost, że dla pewnych liczb porządkowych $\beta, \gamma \in \alpha_0$, $(d_{\alpha_0}\restriction\alpha_0)(\beta) = (d_{\alpha_0}\restriction\alpha_0)(\gamma)$ oraz $\beta \neq \gamma$. Wówczas z definicji obcięcia funkcji mamy:

(3) $d_{\alpha_0}(\beta) = d_{\alpha_0}(\gamma)$.

Ponadto z (2), odłączając kwantyfikator dla β oraz γ, uzyskujemy:

(4) $X - \overrightarrow{d_\beta}(\beta) \neq \varnothing$ oraz

(5) $X - \overrightarrow{d_\gamma}(\gamma) \neq \varnothing$.

Ponieważ $\beta \neq \gamma$, więc $\beta \in \gamma$ lub $\gamma \in \beta$. Załóżmy, że

(6) $\beta \in \gamma$.

Na mocy (5), (6) oraz Tw. 7(4) mamy:

(7) $d_\beta(\beta) \neq d_\gamma(\gamma)$.

Jednakże na mocy Tw. 5(2) mamy ponadto:

(8) $d_{\alpha_0}(\beta) = d_\beta(\beta)$ oraz

(9) $d_{\alpha_0}(\gamma) = d_\gamma(\gamma)$.

Z (8), (9) i (7) otrzymujemy: $d_{\alpha_0}(\beta) \neq d_{\alpha_0}(\gamma)$, co jest sprzeczne z (3).

Gdy $\gamma \in \beta$ dowód przebiega analogicznie. Korzystamy wówczas z (4) zamiast z (5) i wszędzie zamieniamy β na γ oraz γ na β. □

§5. Funkcja definiowana przez indukcję pozaskończoną wyznaczona przez funkcję wyboru zbioru liczb porządkowych

Kolejne dwa fakty dotyczą dowolnego niepustego zbioru x liczb porządkowych. Pierwszy z nich jest odpowiednikiem Tw. 7(2). Dla dowolnej liczby porządkowej α oznaczmy $d^*_\alpha := \mathrm{din}(\alpha, x, h(\alpha, x, wb(x)))$. Naturalnie d^*_α jest funkcją, którą do tej pory oznaczaliśmy jako d_α. Symbol „*" ma tu oznaczać, iż funkcja d_α zależy nie od dowolnie ustalonej funkcji wyboru f dla zbioru x liczb porządkowych, lecz od funkcji wyboru $wb(x)$.

Twierdzenie 10. *Dla dowolnej liczby porządkowej* α:
$\forall\gamma \in \alpha[x - \overrightarrow{d^*_\alpha}(\gamma) \neq \varnothing \Rightarrow \forall\delta(\delta \in \gamma \Rightarrow d^*_\alpha(\delta) \in d^*_\alpha(\gamma))]$.

Dowód. Załóżmy, że $\gamma \in \alpha$ oraz $x - \overrightarrow{d^*_\alpha}(\gamma) \neq \varnothing$. Niech ponadto $\delta \in \gamma$. Wówczas z Tw. 7(2) (oczywiście $\gamma \in S(\alpha)$) mamy natychmiast:
(1) $d^*_\alpha(\delta) \neq d^*_\alpha(\gamma)$.

Skoro $\delta \in \gamma$, więc $\delta \subseteq \gamma$. Naturalnie również $\gamma \subseteq \alpha$. Zatem $\overrightarrow{d^*_\alpha}(\delta) \subseteq \overrightarrow{d^*_\alpha}(\gamma)$, co implikuje:
(2) $x - \overrightarrow{d^*_\alpha}(\gamma) \subseteq x - \overrightarrow{d^*_\alpha}(\delta)$.

Na podstawie (**) z §4 prawdziwe są równości:
(3) $d^*_\alpha(\gamma) = wb(x)(x - \overrightarrow{d^*_\alpha}(\gamma))$ oraz
(4) $d^*_\alpha(\delta) = wb(x)(x - \overrightarrow{d^*_\alpha}(\delta))$,
o ile $\delta \neq \varnothing$.

Z (3), założenia, definicji funkcji wyboru oraz z (2) otrzymujemy:
(5) $d^*_\alpha(\gamma) \in x - \overrightarrow{d^*_\alpha}(\delta)$.

Lecz na mocy (4) i definicji funkcji wyboru $wb(x)$:
$d^*_\alpha(\delta) = nlp(x - \overrightarrow{d^*_\alpha}(\delta))$,
tzn. $d^*_\alpha(\delta)$ jest najmniejszą liczbą porządkową β taką, że $\beta \in x - \overrightarrow{d^*_\alpha}(\delta)$. Zatem wobec (5), z definicji najmniejszej liczby porządkowej otrzymujemy: $d^*_\alpha(\delta) \subseteq d^*_\alpha(\gamma)$, co wobec (1) implikuje $d^*_\alpha(\delta) \in d^*_\alpha(\gamma)$.

Wykorzystaliśmy tu równość (4), która jest spełniona, gdy $\delta \neq \varnothing$. Gdyby $\delta = \varnothing$, to wówczas zamiast (4) otrzymujemy na mocy (*) z §4 oraz definicji funkcji wyboru $wb(x)$:

$d^*_\alpha(\delta) = d^*_\alpha(\varnothing) = wb(x)(\varnothing) = nlp(x)$.

Zatem, skoro $d^*_\alpha(\gamma) \in x$ oraz $nlp(x)$ jest najmniejszą liczbą porządkową β taką, że $\beta \in x$, więc znowu mamy inkluzję $d^*_\alpha(\delta) \subseteq d^*_\alpha(\gamma)$, co wobec (1) implikuje $d^*_\alpha(\delta) \in d^*_\alpha(\gamma)$. $\square$

TWIERDZENIE 11. *Dla dowolnej liczby porządkowej α:*
$\forall\gamma[(\gamma \in \alpha \wedge x - \overrightarrow{d^*_\alpha}(\gamma) \neq \varnothing) \Rightarrow \gamma \subseteq d^*_\alpha(\gamma)]$.

DOWÓD. Niech α będzie dowolnie ustaloną liczbą porządkową. Korzystamy z wariantu twierdzenia o indukcji pozaskończonej w postaci (**), §5, Rozdział 8, gdzie zmienne związane x, y zostały zamienione na zmienne γ, δ:
(1) $\forall\gamma[W(\gamma) \Rightarrow (\forall\delta(\delta \in \gamma \Rightarrow \phi(\delta)) \Rightarrow \phi(\gamma))] \Rightarrow \forall\gamma(W(\gamma) \Rightarrow \phi(\gamma))$,
gdzie $W(\gamma) :=\ \gamma \in \alpha \wedge x - \overrightarrow{d^*_\alpha}(\gamma) \neq \varnothing$, oraz $\phi(\gamma) :=\ \gamma \subseteq d^*_\alpha(\gamma)$.

Aby uznać (1) za wariant twierdzenia o indukcji pozaskończonej w postaci (**) należy wykazać, że powyżej określony predykat W spełnia warunki:
(war1) $\forall\gamma(W(\gamma) \Rightarrow \forall\delta(\delta \in \gamma \Rightarrow W(\delta)))$,
(war2) $\forall\gamma\forall\delta\forall\beta(W(\gamma) \wedge W(\delta) \wedge W(\beta) \Rightarrow (\gamma \in \delta \wedge \delta \in \beta \Rightarrow \gamma \in \beta))$.

Aby wykazać (war1) załóżmy, że $W(\gamma)$, tzn. $\gamma \in \alpha$ oraz $x - \overrightarrow{d^*_\alpha}(\gamma) \neq \varnothing$. Niech $\delta \in \gamma$. Wówczas, ponieważ γ jako element liczby porządkowej α jest liczbą porządkową, więc z przechodniości porządku liczb porządkowych (Tw. 14, Rozdział 8) mamy: $\delta \in \alpha$. Naturalnie, ponieważ $\delta \in \gamma$, więc $\delta \subseteq \gamma$. Zatem $\overrightarrow{d^*_\alpha}(\delta) \subseteq \overrightarrow{d^*_\alpha}(\gamma)$, stąd $x - \overrightarrow{d^*_\alpha}(\gamma) \subseteq x - \overrightarrow{d^*_\alpha}(\delta)$, a więc $x - \overrightarrow{d^*_\alpha}(\delta) \neq \varnothing$. Ostatecznie zachodzi $W(\delta)$.

Aby wykazać (war2) wystarczy zauważyć, że zakładając $W(\gamma), W(\delta)$, $W(\beta)$ mamy: $\gamma, \delta, \beta \in \alpha$. Zatem γ, δ, β są liczbami porządkowymi, a więc implikacja $\gamma \in \delta \wedge\ \delta \in \beta\ \Rightarrow \gamma \in \beta$ jest spełniona.

Dowodzone twierdzenie jest, jak widać, następnikiem implikacji (1). Wystarczy więc wykazać jej poprzednik. Załóżmy zatem, iż
(2) $\gamma \in \alpha$,
(3) $x - \overrightarrow{d^*_\alpha}(\gamma) \neq \varnothing$,
(4) $\forall\delta(\delta \in \gamma \Rightarrow \delta \subseteq d^*_\alpha(\delta))$ oraz nie wprost:
(5) $\gamma \nsubseteq d^*_\alpha(\gamma)$.

Ponieważ $\gamma, d^*_\alpha(\gamma)$ są liczbami porządkowymi, więc ze spójności porządku liczb porządkowych, na mocy (5) mamy:
(6) $d^*_\alpha(\gamma) \in \gamma$.

Wówczas z (6) i (4) otrzymujemy:
(7) $d^*_\alpha(\gamma) \subseteq d^*_\alpha(d^*_\alpha(\gamma))$.

Tymczasem z (2),(3),(6) na mocy Tw. 10, $d^*_\alpha(d^*_\alpha(\gamma)) \in d^*_\alpha(\gamma)$, co wraz z (7) oznacza, iż $d^*_\alpha(d^*_\alpha(\gamma)) \in d^*_\alpha(d^*_\alpha(\gamma))$, a to jest niemożliwe. $\square$

Rozdział 11. Liczby kardynalne

§1. Równoliczność zbiorów

Definicja. Dla dowolnych zbiorów x, y : *x jest równoliczny z y*, gdy istnieje funkcja $f : x \longrightarrow y$, która jest bijekcją.

Zauważmy, że funkcja $f : \varnothing \longrightarrow y$, gdzie $y \neq \varnothing$, tzn. $f = \varnothing$ nie jest bijekcją, gdyż nie przekształca zbioru $\varnothing$ „*na*” niepusty zbiór y. Zatem zbiór $\varnothing$ nie jest równoliczny z żadnym niepustym zbiorem. Tymczasem, gdy $y = \varnothing$, funkcja $f : \varnothing \longrightarrow \varnothing$, a więc znowu $f = \varnothing$, jest bijekcją, zatem zbiór pusty jest równoliczny wyłącznie sam ze sobą. W ogólności mamy:

Twierdzenie 1. *X jest równoliczny z X.*

Dowód. Oczywisty na podstawie Tw. 4, Rozdział 4. $\square$

Twierdzenie 2. *X jest równoliczny z $Y \Rightarrow Y$ jest równoliczny z X.*

Dowód. Oczywisty na podstawie Twierdzeń 8, 9, Rozdział 4. $\square$

Twierdzenie 3. *X jest równoliczny z $Y \wedge Y$ jest równoliczny z $U \Rightarrow X$ jest równoliczny z U.*

Dowód. Oczywisty na mocy Tw. 10, Rozdział 4. $\square$

Jako przydatne ćwiczenie udowodnimy następujące

Twierdzenie 4. *Dla dowolnego zbioru X : X jest równoliczny z $S(X)$ wtw $S(X)$ jest równoliczny z $S(S(X))$.*

Dowód. ($\Rightarrow$): Załóżmy, że X *jest równoliczny z* $S(X)$. Niech zatem $f : X \longrightarrow S(X)$ będzie bijekcją. Jest jasne, że wówczas funkcja $g : X \cup \{X\} \longrightarrow S(X) \cup \{S(X)\}$ zdefiniowana następująco: $\forall a \in X,\ g(a) = f(a)$ oraz $g(X) = S(X)$, jest bijekcją. Zatem $S(X)$ jest równoliczny z $S(S(X))$.

($\Leftarrow$): Załóżmy, że $S(X)$ jest równoliczny z $S(S(X))$. Niech więc $f_1 : X \cup \{X\} \longrightarrow S(X) \cup \{S(X)\}$ będzie bijekcją. Jeśli $f_1(X) = S(X)$, to naturalnie $f_1 \restriction X : X \longrightarrow S(X)$ jest bijekcją, zatem X jest równoliczny z $S(X)$.

Przypuśćmy, że $f_1(X) \neq S(X)$. Wówczas oczywiście:
(1) $f_1(X) \in S(X)$.

Jednakże, ponieważ f_1 jest „*na*”, więc dla pewnego $a \in X \cup \{X\}$ mamy:
(2) $f_1(a) = S(X)$.

Naturalnie z (2), $a \neq X$, skoro $f_1(X) \neq S(X)$. Zatem
(3) $a \in X$.

Ponadto,
(4) $\forall y \in X(y \neq a \Rightarrow f_1(y) \in S(X))$.

Gdyby bowiem dla jakiegoś $y \in X$ było tak, że $y \neq a$ oraz $f_1(y) \notin S(X)$, to wówczas $f_1(y) = S(X)$. Zatem z (2) byłoby $f_1(y) = f_1(a)$, co implikuje $y = a$, bo f_1 jest 1-1; sprzeczność.

Na mocy (1), (3), (4) możemy określić funkcję $g_1 : X \longrightarrow S(X)$ jak następuje: dla dowolnego $y \in X$,

$$g_1(y) = \begin{cases} f_1(X) & \text{gdy } y = a \\ f_1(y) & \text{gdy } y \neq a. \end{cases}$$

Jak widać, funkcja g_1 przyjmuje na wszystkich elementach swojej dziedziny, oprócz elementu a, te same wartości co funkcja f_1 na tych elementach, zatem
(5) $g_1 \restriction (X - \{a\}) = f_1 \restriction (X - \{a\})$.

Ponadto,
(6) $g_1(a) = f_1(X)$.

Skoro $f_1 : S(X) \longrightarrow S(X) \cup \{S(X)\}$ jest bijekcją, więc, na mocy (2), obcięcie $f_1 \restriction (S(X) - \{a\})$ jest bijekcją przekształcającą zbiór $S(X) - \{a\}$ na zbiór $S(X)$. Lecz z (3), $S(X) - \{a\} = (X - \{a\}) \cup \{X\}$, zaś $f_1 \restriction ((X - \{a\}) \cup \{X\}) = (f_1 \restriction (X - \{a\})) \cup \{<X, f_1(X)>\}$. Skoro więc $(f_1 \restriction (X - \{a\})) \cup \{<X, f_1(X)>\}$ jest bijekcją przekształcającą zbiór $(X - \{a\}) \cup \{X\}$ na zbiór $S(X)$, to na mocy (5), funkcja $(g_1 \restriction (X - \{a\})) \cup \{<a, f_1(X)>\}$ jest bijekcją przekształcającą zbiór X na $S(X)$. Jednakże według (6), $(g_1 \restriction (X - \{a\})) \cup \{<a, f_1(X)>\} = g_1$, zatem g_1 jest bijekcją przekształcającą X na $S(X)$; ostatecznie X jest równoliczny z $S(X)$. □

§2. Liczba kardynalna zbioru

Jest jasne, na podstawie Twierdzeń 1, 2, 3, że relacja równoliczności na klasie wszystkich zbiorów ma wszystkie własności relacji równoważnościowej. Wskazuje więc ona pewien aspekt, względem którego dwa zbiory równoliczne są podobne (por. Rozdział 6). Oczywiście tym aspektem czy własnością jest ilość elementów w zbiorze. Zatem dwa zbiory są w relacji równoliczności wtw mają tę samą „wartość” ilości wtw mają tę samą ilość elementów. Już wcześniej, na przykład w dowodzie lematu do Tw. 21, Rozdział 1, wykorzystaliśmy fakt istnienia bijekcji przekształcającej jeden zbiór na drugi dla stwierdzenia, że zbiory te mają taką samą ilość elementów.

Oczywiście informacja, że dane zbiory mają tę samą ilość elementów, nie mówi nam nic o tym, ile jest elementów w każdym z tych zbiorów. Podobnie, wiedząc jedynie, że dwa ciała materialne mają tę samą temperaturę, nie wiemy jaką te ciała mają temperaturę. W tym przypadku jednak dysponujemy miarą temperatury, mianowicie mamy takie ciała (np. rtęć czy alkohol w termometrach), z dołączoną do nich skalą, dzięki której odczytujemy ich temperaturę. Wiedząc, że ciało w termometrze ma tę samą temperaturę co dane inne ciało, jesteśmy w stanie podać temperaturę tego danego ciała. W przypadku zbiorów potrzebujemy właśnie takiej miary, czyli takich zbiorów (odpowiedników ciał występujących w termometrach), których ilość elementów jest znana i które można porównywać pod względem ilości elementów z innymi zbiorami. Takimi specjalnymi zbiorami są pewne liczby porządkowe.

TWIERDZENIE 5. *Dla dowolnego niepustego zbioru X istnieje liczba porządkowa α z nim równoliczna.*

DOWÓD. Oczywisty na mocy Tw. 9, Rozdział 10 oraz faktu, że dla dowolnego niepustego zbioru istnieje funkcja wyboru. $\square$

Niech X będzie dowolnym niepustym zbiorem. Na mocy Tw. 5 istnieje liczba porządkowa α równoliczna z X. Istnieje więc (Tw. 21, Rozdział 8) najmniejsza liczba porządkowa α taka, że α jest równoliczna z X.

DEFINICJA. Dla dowolnego niepustego zbioru X najmniejszą liczbę porządkową α taką, że α jest równoliczna z X nazywamy *liczbą kardynalną zbioru* X. Liczbę porządkową $\varnothing$ nazywamy liczbą kardynalną zbioru $\varnothing$. Jest to również najmniejsza (bo jedyna) liczba porządkowa równoliczna ze zbiorem $\varnothing$.

Dla dowolnego zbioru X wprowadzamy 1-argumentową operację *card* przyporządkowującą każdemu zbiorowi X jego liczbę kardynalną. Zatem $card(X)$ jest najmniejszą liczbą porządkową równoliczną z X, czyli $card(X)$ jest równoliczna z X oraz dla dowolnej liczby porządkowej α, jeżeli α jest równoliczna z X, to $card(X) \subseteq \alpha$.

Liczbę porządkową α nazywamy *liczbą kardynalną*, gdy dla pewnego zbioru X, $\alpha = card(X)$.

Liczba kardynalna jest więc wyróżnionym zbiorem wśród wszystkich zbiorów mających tę samą co ona ilość elementów. Innymi słowy, jest ona wyróżnionym reprezentantem klasy abstrakcji względem relacji równoliczności. Formalnie nie wprowadzamy do teorii ZFC pojęcia klasy abstrakcji względem relacji równoliczności, ponieważ taka klasa abstrakcji, zależnie od jej reprezentanta, na ogół nie jest zbiorem. Sama przecież „relacja" równoliczności nie jest w ZFC relacją binarną (równoważnościową), nie istnieje bowiem zbiór, na którym by była ona określona (zbiór wszystkich zbiorów nie istnieje). Niemniej, biorąc pod uwagę Tw. 3(2), Rozdział 6, można by nieformalnie napisać:

dla dowolnych zbiorów X, Y : X *jest równoliczny z* Y *wtw* $[X] = [Y]$,

gdzie $[X], [Y]$ byłyby klasami abstrakcji względem relacji równoliczności. Dysponując wyróżnionym reprezentantem klasy abstrakcji $[X]$, jakim jest $card(X)$, można zupełnie poprawnie pod względem formalnym sformułować odpowiednik powyższego twierdzenia:

TWIERDZENIE 6. *Dla dowolnych zbiorów* X, Y : X *jest równoliczny z* Y *wtw* $card(X) = card(Y)$.

DOWÓD. Niech X, Y będą dowolnymi zbiorami.

($\Rightarrow$): Załóżmy, że X jest równoliczny z Y. Z definicji liczby kardynalnej mamy:
(1) $card(X)$ jest równoliczna z X,
(2) $\forall\alpha(\alpha$ jest liczbą porządkową $\wedge$ α jest równoliczna z $X \Rightarrow card(X) \subseteq \alpha)$,
(3) $card(Y)$ jest równoliczna z Y,
(4) $\forall\alpha(\alpha$ jest liczbą porządkową $\wedge$ α jest równoliczna z $Y \Rightarrow card(Y) \subseteq \alpha)$.

Zatem z założenia oraz (1), na mocy Tw. 3, $card(X)$ jest równoliczna z Y, co wraz z (4) implikuje inkluzję $card(Y) \subseteq card(X)$. Ponadto, z założenia, na mocy Tw. 2, Y jest równoliczny z X, dlatego wobec (3), na mocy Tw. 3, $card(Y)$ jest równoliczna z X. Zatem z (2), $card(X) \subseteq card(Y)$. Ostatecznie, $card(X) = card(Y)$.

($\Leftarrow$): Załóżmy, że $card(X) = card(Y)$. Wówczas, skoro $card(X)$ jest równoliczny z X, więc $card(Y)$ jest równoliczny z X, czyli na mocy Tw. 2, X jest zbiorem równolicznym z $card(Y)$. Lecz $card(Y)$ jest równoliczny z Y. Zatem na mocy Tw. 3, X jest równoliczny z Y. □

WNIOSEK. *Dla dowolnego zbioru* X, $card(card(X)) = card(X)$.

DOWÓD. Ponieważ zbiór $card(X)$ jest równoliczny z X, więc na mocy Tw. 6, $card(card(X)) = card(X)$. □

Oczekujemy, że wyróżnienie spośród wszystkich zbiorów mających tę samą ilość elementów – jednego zbioru, zwanego ich liczbą kardynalną, umożliwi odpowiedź na pytanie, ile jest elementów w każdym z tych zbiorów. Biorąc pod uwagę wzmiankowaną analogię z temperaturą, wyróżnienie wśród wszystkich ciał mających identyczną temperaturę tego ciała, które znajduje się w termometrze, ma sens dlatego, że jest do niego dołączona skala wskazująca jego temperaturę. Czy zatem „techniczne" przecież wyróżnienie liczby kardynalnej jest sensowne dlatego, że znana jest ilość jej elementów? Aby odpowiedzieć na to pytanie, należałoby wcześniej rozważyć pojęcie „ilości elementów w zbiorze".

Na gruncie teorii mnogości ZFC każdy obiekt teoriomnogościowy jest zbiorem. Jeżeli więc w ramach ZFC rozważamy formułę postaci „*x jest ilością elementów zbioru A*" lub „*ilość elementów zbioru A wynosi x*", to symbol „x" musi być nazwą jakiegoś zbioru. Co więcej, różne „ilości elementów" muszą być ze sobą porównywalne. Jeśli zatem uznać te dwa czynniki: bycie zbiorem oraz porównywalność, jako minimalną charakterystykę pojęcia „ilości elementów", to wówczas można by utożsamić ilość elementów zbioru z jego liczbą kardynalną. Przesłankami dla tego utożsamienia są: Tw. 6, które mówi, że dwa zbiory mają tę samą ilość elementów wtw mają one tę samą liczbę kardynalną, oraz fakt, że liczby kardynalne jako liczby porządkowe są porównywalne (według relacji porządkującej $\in$). Uzasadnienie dla utożsamienia ilości elementów zbioru z jego liczbą kardynalną można wzmocnić przez odwołanie się do analogii z temperaturą. Ostatecznie skala temperatury jest przecież ustalona niemal zupełnie arbitralnie. Prawdziwe stwierdzenie, że wartość temperatury danego ciała wynosi x stopni według danej skali, można zastąpić prawdziwym stwierdzeniem, że wartość temperatury tego ciała wynosi y stopni w innej skali. To, co uznamy za wartość temperatury nie jest istotne. Istotne jest, aby te wartości można było porównywać oraz odnosić do wartości innych parametrów termodynamicznych.

W ten sposób, na pytanie, czy znana jest ilość elementów liczby kardynalnej, odpowiedzielibyśmy następująco: tak, bowiem tą ilością jest ona sama (por. również Wniosek powyżej). Konsekwentnie, wyróżnienie wśród wszystkich zbiorów równolicznych ich liczby kardynalnej jest sensowne dlatego, że w ten sposób wyróżniamy ten zbiór, który jest ilością (reprezentuje w ZFC ilość) elementów w każdym z tych zbiorów.

Jednakże utożsamienie ilości elementów zbioru z jego liczbą kardynalną, precyzyjniej, sformalizowanie czy reprezentowanie na gruncie ZFC pojęcia „ilości elementów zbioru" w postaci liczby kardynalnej tego zbioru, może budzić pewne wątpliwości. Oto przecież wyrażenie: „ilość obiektów", przynajmniej wówczas gdy tych obiektów jest skończenie wiele, ma w języku potocznym zupełnie precyzyjne znaczenie. To, jaka jest ta ilość, nie jest wcale kwestią wyboru jakiejś skali. Skala jest jedna: ciąg liczb naturalnych. Oczywiście wyrażenie „ilość" w sformułowaniu „ilość elementów w zbiorze" ma mieć to samo znaczenie, co w języku potocznym. W §8, Rozdział 1, definiując zbiór n-elementowy, gdzie n jest liczbą naturalną, *implicite* wyraziliśmy fakt, że ilość (w sensie potocznym) elementów w takim zbiorze wynosi n, gdzie n jest liczbą naturalną. Jest oczywiste, że jakiekolwiek dwa zbiory n-elementowe są równoliczne. Powstaje pytanie, czy ich liczba kardynalna wynosi n. Jeśli nie, to reprezentacja ilości elementów w zbiorze w postaci liczby kardynalnej tego zbioru jest bezwartościowa. Powyższe pytanie ma sens oczywiście wówczas, gdy liczbę naturalną n postrzegamy nie jako abstrakcyjny obiekt służący do zliczania (ze standardowego modelu arytmetyki liczb naturalnych), lecz obiekt teoriomnogościowy, tzn. jako liczbę porządkową (zbiór n-elementowy) $n = \{0, 1, \ldots, n-1\}$, gdzie $0 = \varnothing$, $1 = S(\varnothing)$ itd. Natychmiast stwierdzamy równoliczność dowolnego n-elementowego zbioru z taką liczbą n. Pytanie nasze sprowadza się więc do następującego: czy $card(n) = n$? Intuicyjnie jest jasne (biorąc pod uwagę definicję liczby kardynalnej), że odpowiedź jest twierdząca. Uzasadnimy ją w następnym paragrafie, poświęconym w ogólności liczbom kardynalnym liczb porządkowych (zob. Tw. 15).

W przypadku zbioru nieskończonego, nie widać przeszkód ze strony potocznego rozumienia słowa „ilość" dla pojmowania liczby kardynalnej takiego zbioru jako ilości jego elementów.

Zauważmy jeszcze, że podobieństwo między danym zbiorem X a jego liczbą kardynalną $card(X)$, ze względu na ilość elementów, pociąga za sobą podobieństwo tych zbiorów pod innym jeszcze względem – uporządkowania elementów. Ponieważ $card(X)$ jest liczbą porządkową, więc $<card(X), \subseteq>$ jest zbiorem dobrze uporządkowanym (por. §1, Rozdział 9). Porządek ten jest odtwarzalny w zbiorze X, jak wskazuje dowód następującego twierdzenia:

TWIERDZENIE 7. *Dla dowolnego niepustego zbioru X istnieje relacja częściowo porządkująca $\leqslant$ na X taka, że $<X, \leqslant>$ jest zbiorem dobrze uporządkowanym.*

DOWÓD. Niech X będzie dowolnym niepustym zbiorem. Rozważmy dobrze uporządkowany zbiór $<card(X), \subseteq>$. Skoro zbiory $card(X)$, X są równoliczne, niech więc $f : card(X) \longrightarrow X$ będzie bijekcją. Wówczas naturalnie $X = \vec{f}(card(X))$. Zatem, według Tw. 19, Rozdział 5, relacja $\leqslant$ zdefiniowana na X następująco: $\forall a, b \in X(a \leqslant b \text{ wtw } f^{\sim}(a) \subseteq f^{\sim}(b))$, jest relacją częściowo porządkującą oraz $<X, \leqslant>$ jest zbiorem dobrze uporządkowanym. □

Aby podać charakterystykę pojęcia liczby kardynalnej w oparciu o liczby porządkowe, porównajmy najpierw dowolną liczbę porządkową z jej liczbą kardynalną:

TWIERDZENIE 8. *Dla dowolnej liczby porządkowej α: $card(\alpha) \subseteq \alpha$ (tzn. $card(\alpha) \in \alpha$ lub $card(\alpha) = \alpha$).*

DOWÓD. Z definicji liczby kardynalnej mamy:
$\forall \beta(\beta$ jest równoliczna z $\alpha \Rightarrow card(\alpha) \subseteq \beta)$.

Na mocy Tw. 1, α jest równoliczna z α, zatem $card(\alpha) \subseteq \alpha$. □

TWIERDZENIE 9. *Dla dowolnej liczby porządkowej α następujące warunki są równoważne:*
(i) *α jest liczbą kardynalną (tzn. dla pewnego $X, \alpha = card(X)$),*
(ii) $card(\alpha) = \alpha$,
(iii) $\forall\beta(\beta \in \alpha \Rightarrow card(\beta) \in card(\alpha))$.

DOWÓD. Niech α będzie dowolną liczbą porządkową.
(i)⇒(ii): Oczywisty na mocy Wniosku z Tw. 6.
(ii)⇒(i): Oczywisty.
(ii)⇒(iii): Załóżmy, że $card(\alpha) = \alpha$ oraz $\beta \in \alpha$. Zatem $\beta \in card(\alpha)$. Według Tw. 8, $card(\beta) \in \beta$ lub $card(\beta) = \beta$. Stąd (Tw. 14, Rozdział 8) $card(\beta) \in card(\alpha)$.
(iii)⇒(ii): Załóżmy (iii) oraz nie wprost, że $card(\alpha) \neq \alpha$. Wówczas z Tw. 8, $card(\alpha) \in \alpha$. Zatem z (iii) uzyskujemy: $card(card(\alpha)) \in card(\alpha)$ i konsekwentnie, na mocy wniosku z Tw. 6, $card(\alpha) \in card(\alpha)$, co jest niemożliwe. □

Jak widać, liczby kardynalne to te liczby porządkowe α, dla których zachodzi równość $card(\alpha) = \alpha$, natomiast liczby porządkowe niebędące liczbami kardynalnymi to te liczby α, dla których zachodzi: $card(\alpha) \in \alpha$ (na mocy Tw. 8).

Uogólniamy Tw. 8 do następującego twierdzenia:

TWIERDZENIE 10. *Dla dowolnego zbioru liczb porządkowych x oraz dowolnej liczby porządkowej β, $x \subseteq \beta \Rightarrow card(x) \subseteq \beta$.*

DOWÓD. Gdy $x = \varnothing$, to $card(x) = \varnothing$, a zatem prawdą jest, że $x \subseteq \beta \Rightarrow card(x) \subseteq \beta$ dla dowolnej β.
Niech więc $x \neq \varnothing$. Załóżmy, że
(1) $x \subseteq \beta$ oraz
(2) $card(x) \nsubseteq \beta$,
dla pewnej liczby porządkowej β. Z (2) mamy natychmiast:
(3) $\beta \in card(x)$.
Na mocy Tw. 9, Rozdział 10, niech α będzie liczbą porządkową taką, że funkcja $\mathrm{din}(\alpha, x, h(\alpha, x, wb(x)))\restriction\alpha$ jest bijekcją przekształcającą zbiór α na zbiór liczb porządkowych x. Oznaczmy jak poprzednio, $d^*_\alpha = \mathrm{din}(\alpha, x, h(\alpha, x, wb(x)))$. Ponieważ α jest równoliczna z x, więc na mocy Tw. 6, $card(\alpha) = card(x)$. Zatem z Tw. 8 mamy: $card(x) \subseteq \alpha$, skąd wobec (3), otrzymujemy:
(4) $\beta \in \alpha$.
Ponieważ $\overrightarrow{d^*_\alpha}(\alpha) = x$, więc na mocy (4), $d^*_\alpha(\beta) \in x$. Zatem z (1),
(5) $d^*_\alpha(\beta) \in \beta$.
Lecz jednocześnie na mocy (4), $\beta \subseteq \alpha$ oraz $\beta \neq \alpha$. Zatem dla pewnej $\gamma:\ \gamma \in \alpha$ oraz $\gamma \notin \beta$. Przypuszczenie, że $d^*_\alpha(\gamma) \in \overrightarrow{d^*_\alpha}(\beta)$ prowadzi do równości $d^*_\alpha(\gamma) = d^*_\alpha(\delta)$,

dla pewnej $\delta \in \beta$. Wówczas jednak, $\gamma = \delta$, bo $d^*_\alpha \restriction \alpha$ jest różnowartościowa, zatem $\gamma \in \beta$, co jest niemożliwe. Ostatecznie $d^*_\alpha(\gamma) \notin \overrightarrow{d^*_\alpha}(\beta)$, lecz $d^*_\alpha(\gamma) \in x$ (bo $\gamma \in \alpha$), zatem $x - \overrightarrow{d^*_\alpha}(\beta) \neq \emptyset$. Stąd i z (4), na mocy Tw. 11, Rozdział 10, otrzymujemy: $\beta \subseteq d^*_\alpha(\beta)$, skąd wobec (5), $d^*_\alpha(\beta) \in d^*_\alpha(\beta)$, co jest niemożliwe. □

Obecnie podamy kilka faktów charakteryzujących liczby kardynalne dowolnych zbiorów. Najpierw wykorzystamy Tw. 10 w dowodzie, jeśli nie oczywistego, to przynajmniej zgodnego z intuicjami twierdzenia, mówiącego, że operacja *card* jest monotoniczna:

TWIERDZENIE 11. *Dla dowolnych zbiorów* $X, Y : X \subseteq Y \Rightarrow card(X) \subseteq card(Y)$.

DOWÓD. Niech $X \subseteq Y$. Ponieważ Y jest równoliczny z $card(Y)$, więc niech $f \colon Y \longrightarrow card(Y)$ będzie bijekcją. Wówczas naturalnie obcięcie $f \restriction X : X \longrightarrow \overrightarrow{(f \restriction X)}(X)$ jest bijekcją. Zatem zbiory X oraz $\overrightarrow{(f \restriction X)}(X)$ są równoliczne, czyli na mocy Tw. 6 mamy:

(1) $card(\overrightarrow{(f \restriction X)}(X)) = card(X)$. Lecz

(2) $\overrightarrow{(f \restriction X)}(X) = \overrightarrow{f}(X) \subseteq card(Y)$.

Z (2), na mocy Tw. 10 (oczywiście $\overrightarrow{(f \restriction X)}(X)$ jako podzbiór liczby porządkowej $card(Y)$ jest zbiorem liczb porządkowych) otrzymujemy: $card(\overrightarrow{(f \restriction X)}(X)) \subseteq card(Y)$, co wobec (1) daje: $card(X) \subseteq card(Y)$. □

Następne twierdzenie jest odpowiednikiem Tw. 6:

TWIERDZENIE 12. *Dla dowolnych zbiorów* X, Y, $card(X) \subseteq card(Y)$ *wtw istnieje funkcja* $f : X \longrightarrow Y$, *która jest różnowartościowa.*

DOWÓD. ($\Rightarrow$): Załóżmy, że $card(X) \subseteq card(Y)$. Naturalnie $card(Y)$ jest równoliczna z Y. Niech więc $g : card(Y) \longrightarrow Y$ będzie bijekcją. Na mocy założenia, rozważmy jej obcięcie $g \restriction card(X)$. Niewątpliwie $g \restriction card(X)$ jest bijekcją przekształcającą $card(X)$ na zbiór $\overrightarrow{g}(card(X))$, będący podzbiorem zbioru Y. Skoro X jest równoliczny z $card(X)$, niech więc $h : X \longrightarrow card(X)$ będzie bijekcją. Wówczas złożenie bijekcji $h \circ (g \restriction card(X)) : X \longrightarrow \overrightarrow{g}(card(X))$ jest bijekcją (Tw. 10, Rozdział 4). Zatem, ponieważ $\overrightarrow{g}(card(X)) \subseteq Y$, więc $h \circ (g \restriction card(X)) : X \longrightarrow Y$ jest różnowartościowa.

($\Leftarrow$): Załóżmy, że $f : X \longrightarrow Y$ jest funkcją różnowartościową. Wówczas $f\colon X \longrightarrow \overrightarrow{f}(X)$ jest bijekcją, czyli zbiory X, $\overrightarrow{f}(X)$ są równoliczne. Konsekwentnie, według Tw. 6, $card(X) = card(\vec{f}(X))$. Lecz $\vec{f}(X) \subseteq Y$, zatem na mocy Tw. 11, $card(\vec{f}(X)) \subseteq card(Y)$. Ostatecznie $card(X) \subseteq card(Y)$. □

TWIERDZENIE 13. *Dla dowolnych zbiorów X, Y, jeżeli $f : X \longrightarrow Y$ jest funkcją przekształcającą X na Y, to $card(Y) \subseteq card(X)$.*

DOWÓD. Załóżmy, że $f : X \longrightarrow Y$ jest „*na*". Gdy $X = \varnothing$, to wówczas z założenia również $Y = \varnothing$ (bo gdyby $Y \neq \varnothing$, to jedyna funkcja $f \in Y^{\varnothing}$, tzn. $f = \varnothing$ nie byłaby „*na*"), zatem $card(Y) \subseteq card(X)$. Załóżmy, że $X \neq \varnothing$. Na mocy Tw. 12, Rozdział 6, rozważmy bijekcję $g : X/\simeq_f \longrightarrow Y$ taką, że dla dowolnego $a \in X$, $g([a]_{\simeq_f}) = f(a)$, gdzie $\simeq_f$ jest relacją równoważności na X wyznaczoną przez funkcję f (tzn. $a \simeq_f b$ wtw $f(a) = f(b)$). Naturalnie funkcja odwrotna do g, a więc $g^{\sim}$ jest bijekcją przekształcającą zbiór Y na zbiór ilorazowy $X/\simeq_f$ (Tw. 8, 9, Rozdział 4).

Ponadto $X/\simeq_f$ jest podziałem zbioru X (Tw. 5, Rozdział 6). Rozważmy więc aksjomat wyboru w wersji $(AxC)''$ (§3, Rozdział 10) dla podziału $X/\simeq_f$ niepustego zbioru X. Wówczas stwierdzamy istnienie zbioru U takiego, że dla dowolnego $Z \in X/\simeq_f$, zbiór $U \cap Z$ ma dokładnie jeden element. Dla każdego $Z \in X/\simeq_f$ oznaczmy ten jedyny element zbioru $U \cap Z$ jako a_Z. Rozważyć więc można funkcję $h : X/\simeq_f \longrightarrow X$ określoną następująco: dla dowolnego $Z \in X/\simeq_f$, $h(Z) = a_Z$ (naturalnie $a_Z \in X$, bo $a_Z \in Z \subseteq X$). Funkcja h jest różnowartościowa, bowiem gdy $Z_1 \neq Z_2$ dla $Z_1, Z_2 \in X/\simeq_f$, to $Z_1 \cap Z_2 = \varnothing$, zatem skoro $a_{Z_1} \in Z_1$ oraz $a_{Z_2} \in Z_2$, więc $a_{Z_1} \neq a_{Z_2}$, czyli $h(Z_1) \neq h(Z_2)$. Dlatego funkcja $h : X/\simeq_f \longrightarrow \vec{h}(X/\simeq_f)$ jest bijekcją.

Na mocy Tw. 10, Rozdział 4, złożenie $g^{\sim} \circ h : Y \longrightarrow \vec{h}(X/\simeq_f)$ jest bijekcją. Stąd, ponieważ $\vec{h}(X/\simeq_f) \subseteq X$, funkcja: $g^{\sim} \circ h : Y \longrightarrow X$ jest różnowartościowa. Ostatecznie, na mocy Tw. 12, otrzymujemy: $card(Y) \subseteq card(X)$. □

Zilustrujmy użyteczność powyższych twierdzeń, formułując następujący

LEMAT. *Dla dowolnych zbiorów X, Y, jeżeli $card(X) = card(Y) = \omega$, to $card(X \cup Y) = \omega$.*

DOWÓD. Załóżmy, że zbiory X, Y są takie, że $card(X) = card(Y) = \omega$.

Niech więc $f_1 : \omega \longrightarrow X$, $f_2 : \omega \longrightarrow Y$ będą bijekcjami. Określmy funkcję $g : \omega \longrightarrow X \cup Y$ następująco: dla dowolnej $\alpha \in \omega$, $g(2\alpha) = f_1(\alpha)$ oraz $g(2\alpha + 1) = f_2(\alpha)$, gdzie 2α jest liczbą naturalną postaci $S^{2n}(\varnothing)$ i $2\alpha + 1$ jest liczbą postaci $S^{2n+1}(\varnothing)$, gdy α ma postać $S^n(\varnothing)$ (n jest tu ilością aplikacji operacji S).

Jest jasne, że g jest funkcją „*na*". Bowiem dla dowolnego $a \in X \cup Y$, gdy $a \in X$, to liczba naturalna $\alpha = 2(f_1^{\sim}(a))$ jest taka, że $g(\alpha) = a$, gdy zaś $a \in Y$, to liczba naturalna $\alpha = 2(f_2^{\sim}(a)) + 1$ jest taka, że $g(\alpha) = a$.

Na mocy Tw. 13 otrzymujemy: $card(X \cup Y) \subseteq card(\omega)$. Zatem według Tw. 8, $card(X \cup Y) \subseteq \omega$. Z drugiej strony, skoro $X \subseteq X \cup Y$, więc zgodnie z Tw. 11, $card(X) \subseteq card(X \cup Y)$, czyli z założenia, $\omega \subseteq card(X \cup Y)$. Ostatecznie $card(X \cup Y) = \omega$. $\square$

Oczywiście powyższy lemat pojmujemy w tej chwili całkiem dosłownie, a więc hipotetycznie – nie rozstrzyga on wcale kwestii, czy istnieją takie zbiory, których liczbą kardynalną jest ω.

§3. Liczby kardynalne liczb porządkowych

Najpierw zajmiemy się liczbami kardynalnymi liczb naturalnych, następnie zaś liczbami kardynalnymi liczb porządkowych większych lub równych ω.

Dowód wzmiankowanego wcześniej faktu, iż liczba kardynalna dowolnej liczby naturalnej jest właśnie tą liczbą naturalną, oprzemy między innymi na następującym twierdzeniu:

TWIERDZENIE 14. $\forall \alpha \in \omega$, *$\alpha$ nie jest równoliczna z $S(\alpha)$.* (*Żadna liczba naturalna nie jest równoliczna ze swoim następnikiem.*)

DOWÓD. Indukcyjny, na podstawie Tw. 13, Rozdział 7.

Naturalnie $\varnothing$ nie jest równoliczny z $S(\varnothing)$. Niech $\alpha \in \omega$. Załóżmy, że α nie jest równoliczna z $S(\alpha)$. Wówczas, na mocy Tw. 4, $S(\alpha)$ nie jest równoliczna z $S(S(\alpha))$. Ostatecznie (Tw. 13, Rozdział 7), $\forall \alpha \in \omega$, α nie jest równoliczna z $S(\alpha)$. $\square$

TWIERDZENIE 15. $\forall \alpha \in \omega$, $card(\alpha) = \alpha$. (*Każda liczba naturalna jest liczbą kardynalną.*)

DOWÓD. Indukcyjny, na podstawie Tw. 13, Rozdział 7.

Naturalnie $card(\varnothing) = \varnothing$. Niech $\alpha \in \omega$. Załóżmy, że $card(\alpha) = \alpha$. Na mocy Tw. 8,

(1) $card(S(\alpha)) \in S(\alpha)$ lub $card(S(\alpha)) = S(\alpha)$.

Przypuśćmy, że $card(S(\alpha)) \in S(\alpha)$. Wówczas z definicji następnika mamy:

(2) $card(S(\alpha)) \in \alpha$ lub $card(S(\alpha)) = \alpha$.

Przypuśćmy, że $card(S(\alpha)) \in \alpha$. Jednakże $\alpha \subseteq S(\alpha)$, zatem według Tw. 11, $card(\alpha) \subseteq card(S(\alpha))$, czyli z założenia indukcyjnego, $\alpha \subseteq card(S(\alpha))$, co wraz z naszym przypuszczeniem implikuje $card(S(\alpha)) \in card(S(\alpha))$, a to jest niemożliwe. Zatem, na mocy (2), $card(S(\alpha)) = \alpha$. Jednakże wówczas, skoro $card(S(\alpha))$ jest równoliczna z $S(\alpha)$, to α jest równoliczna z $S(\alpha)$, a to jest również niemożliwe, na mocy Tw. 14. Ostatecznie, alternatywa (2) nie jest prawdziwa, zatem według (1), otrzymujemy: $card(S(\alpha)) = S(\alpha)$, co kończy dowód. $\square$

TWIERDZENIE 16. $card(\omega) = \omega$.

DOWÓD. Na mocy Tw. 8 wystarczy wykazać, że $card(\omega) \notin \omega$. Załóżmy nie wprost, że $card(\omega) \in \omega$. Wówczas $card(\omega)$ jest liczbą naturalną, zatem jej następnik $S(card(\omega))$ jest również liczbą naturalną (Tw. 10, Rozdział 7), tzn. $S(card(\omega)) \in \omega$. Stąd, z jednej strony, $S(card(\omega)) \subseteq \omega$, i według Tw. 11, $card(S(card(\omega))) \subseteq card(\omega)$. Z drugiej strony, na mocy Tw. 15, $card(S(card(\omega))) = S(card(\omega))$. Dlatego $S(card(\omega)) \subseteq card(\omega)$, a ponieważ $card(\omega) \in S(card(\omega))$, więc $card(\omega) \in card(\omega)$, co jest niemożliwe. $\square$

Dowód Tw. 16 można uogólnić do dowodu następującego twierdzenia:

TWIERDZENIE 17. *Dla dowolnej liczby porządkowej α, jeżeli $card(\alpha) \in \alpha$, to $card(\alpha)$ jest graniczna. (Liczba kardynalna liczby porządkowej niebędącej liczbą kardynalną jest liczbą graniczną.)*

DOWÓD. Załóżmy, że
(1) $card(\alpha) \in \alpha$
oraz nie wprost: $card(\alpha)$ jest izolowana. Wtedy dla pewnej liczby porządkowej β,
(2) $card(\alpha) = S(\beta)$.

Z (2), $\beta \in card(\alpha)$, skoro więc $card(\alpha)$ jest najmniejszą liczbą porządkową równoliczną z α, to według Tw. 19(i)⇔(iii), Rozdział 8 uzyskujemy wyrażenie:
(3) β nie jest równoliczna z α.

Na mocy (1) i Tw. 9, Rozdział 9, $S(card(\alpha)) \subseteq \alpha$, zatem zgodnie z Tw. 11 otrzymujemy:
(4) $card(S(card(\alpha))) \subseteq card(\alpha)$.

Z drugiej strony, $card(\alpha) \subseteq S(card(\alpha))$. Zatem na podstawie Tw. 11 oraz Wniosku z Tw. 6,
(5) $card(\alpha) \subseteq card(S(card(\alpha)))$.

Z (4) i (5) otrzymujemy równość $card(S(card(\alpha))) = card(\alpha)$, co na mocy Tw. 6 implikuje, że $S(card(\alpha))$ jest równoliczny z α. Stąd $S(card(\alpha))$ jest równoliczny z $card(\alpha)$, czyli z (2), $S(S(\beta))$ jest równoliczny z $S(\beta)$. Wówczas jednak, na mocy Tw. 4, $S(\beta)$ jest równoliczny z β, tzn. według (2), $card(\alpha)$ jest równoliczny z β i konsekwentnie α jest równoliczne z β; sprzeczność z (3). $\square$

Na podstawie Tw. 17 i Tw. 8 można sformułować oczywiste wnioski:

WNIOSEK 1. *Jeżeli liczba kardynalna jakiejś liczby porządkowej jest liczbą izolowaną, to jest ona równa tej liczbie porządkowej.*

WNIOSEK 2. *Dla dowolnej liczby porządkowej α, jeżeli α jest graniczna, to $card(\alpha)$ jest graniczna.*

DOWÓD. Załóżmy, że α jest graniczna. Na mocy Tw. 8, $card(\alpha) \in \alpha$ lub $card(\alpha) = \alpha$. Jeśli spełniony jest drugi człon tej alternatywy, to naturalnie $card(\alpha)$ jest graniczna. Jeśli zaś pierwszy, to na mocy Tw. 17, $card(\alpha)$ jest graniczna. $\square$

Zauważmy jeszcze, że Tw. 16 wynika bezpośrednio z Wniosku 2 i Tw. 8 tego rozdziału oraz z Tw. 13, Rozdział 9 i faktu, że $card(\omega) \neq \emptyset$.

TWIERDZENIE 18. *Dla dowolnej liczby porządkowej α, jeżeli $\omega \subseteq \alpha$, to α jest równoliczna z $S(\alpha)$.*

DOWÓD. Niech α będzie liczbą porządkową taką, że $\omega \subseteq \alpha$. Zatem $\omega \cup (\alpha - \omega) = \alpha$ oraz $\omega \cap (\alpha - \omega) = \emptyset$. Rozważmy funkcję $f : \alpha \cup \{\alpha\} \longrightarrow \alpha$ określoną następująco: $\forall \beta \in \omega,\ f(\beta) = S(\beta),\ \forall \beta \in \alpha - \omega,\ f(\beta) = \beta$ oraz $f(\alpha) = 0$. Zauważmy, że $\vec{f}(\alpha \cup \{\alpha\}) = \alpha$. Weźmy bowiem dowolną liczbę $\beta \in \alpha$. Gdy $\beta = 0$, to $\beta = f(\alpha)$ i $\alpha \in \alpha \cup \{\alpha\}$, gdy zaś $0 \neq \beta \in \omega$, to $\beta = S(\bigcup \beta) = f(\bigcup \beta)$ i $\bigcup \beta \in \omega \subseteq \alpha \cup \{\alpha\}$. Wreszcie, gdy $\beta \in \alpha - \omega$, to $\beta = f(\beta)$ i oczywiście $\beta \in \alpha \cup \{\alpha\}$. Ponadto, z określenia funkcji f oraz faktu, że ω jest zbiorem indukcyjnym (zamkniętym na operację następnika) wynika, że f jest różnowartościowa. Skoro więc $f : S(\alpha) \longrightarrow \alpha$ jest bijekcją, to liczby porządkowe α, $S(\alpha)$ są równoliczne. $\square$

WNIOSEK. *Dla dowolnej liczby porządkowej α, jeżeli $\omega \subseteq \alpha$, to dla dowolnej liczby naturalnej n, α jest równoliczna z $S^n(\alpha)$.*

DOWÓD (indukcyjny). Załóżmy, że $\omega \subseteq \alpha$. Na mocy Tw. 1, α jest równoliczna z $S^0(\alpha)$. Załóżmy, że dla jakiegoś n, α jest równoliczna z $S^n(\alpha)$. Ponieważ $\alpha \subseteq S^n(\alpha)$ (zob. lemat przed Tw. 12, Rozdział 9), więc $\omega \subseteq S^n(\alpha)$, zatem na mocy Tw. 18, $S^n(\alpha)$ jest równoliczna z $S^{n+1}(\alpha)$. Stąd, na mocy założenia indukcyjnego oraz Tw. 3, α jest równoliczna z $S^{n+1}(\alpha)$. $\square$

TWIERDZENIE 19. *Dla dowolnej liczby izolowanej α niebędącej liczbą naturalną, $card(\alpha) = card(ng(\alpha))$, gdzie $ng(\alpha)$ jest największą liczbą graniczną należącą do α (por. §4, Rozdział 9).*

DOWÓD. Niech α będzie liczbą izolowaną taką, że $\alpha \notin \omega$. Wówczas oczywiście (Tw. 17, Rozdział 8), $\omega \in \alpha$ lub $\omega = \alpha$, a ponieważ α jest izolowana zaś ω – graniczna, więc mamy:

(1) $\omega \in \alpha$.

Na mocy Wniosku z Tw. 12, Rozdział 9,

(2) $\alpha = S^{n+1}(ng(\alpha))$ dla pewnego n.

Ponieważ $ng(\alpha)$ jest największą liczbą graniczną należącą do α, więc według (1) otrzymujemy: $\omega \subseteq ng(\alpha)$. Stąd, na mocy Wniosku z Tw. 18, $ng(\alpha)$ jest równoliczna z $S^{n+1}(ng(\alpha))$. Zatem z (2), $ng(\alpha)$ jest równoliczna z α, co na mocy Tw. 6 daje: $card(\alpha) = card(ng(\alpha))$. $\square$

Na mocy Tw. 19 oraz Wniosku 2 z Tw. 17 liczba kardynalna dowolnej liczby izolowanej niebędącej liczbą naturalną jest liczbą graniczną. Biorąc pod uwagę Tw. 15, stwierdzamy więc, że wśród wszystkich liczb kardynalnych tylko liczby naturalne są liczbami izolowanymi. Gdyby bowiem jakaś liczba kardynalna α była izolowana i nie była liczbą naturalną, to będąc liczbą kardynalną samej siebie, musiałaby być jednocześnie liczbą graniczną. Sformułujmy więc

WNIOSEK. *Każda liczba kardynalna niebędąca liczbą naturalną jest graniczna.*

Aby wykazać, że powyższy Wniosek nie zależy od jawnej postaci liczby izolowanej niebędącej liczbą naturalną – podanej we Wniosku z Tw. 12, Rozdział 9 i wykorzystywanej w dowodzie Tw. 19 – wykonajmy jego dowód bez opierania się na Tw. 19.

DOWÓD. Załóżmy, że
(1) $\alpha = card(\alpha)$
oraz $\alpha \notin \omega$. Stąd oczywiście $\omega \subseteq \alpha$. Załóżmy nie wprost, że α jest izolowana, czyli dla pewnej β, $\alpha = S(\beta)$. Mamy więc:
(2) $\omega \subseteq S(\beta)$.

Według Tw. 3, Rozdział 9 (dokładniej Wniosku 1 z tego twierdzenia, §4, Rozdział 9), $\bigcup \omega$ jest najmniejszą liczbą porządkową x taką, że $\omega \subseteq S(x)$. Zatem z (2), $\bigcup \omega \subseteq \beta$. Lecz $\bigcup \omega = \omega$ (Tw. 8(2), Rozdział 9), bo ω jest graniczna. Ostatecznie, $\omega \subseteq \beta$. Wobec tego, na mocy Tw. 18, β jest równoliczna z $S(\beta)$, czyli β jest równoliczna z α. Stąd
(3) $card(\beta) = card(\alpha)$.

Z drugiej strony jednak, $\beta \in S(\beta)$, czyli $\beta \in \alpha$. Stąd zaś, na mocy (1) i Tw. 9(ii)$\Leftrightarrow$(iii) otrzymujemy: $card(\beta) \in card(\alpha)$, co jest niemożliwe wobec (3). □

Spróbujmy obliczyć liczby kardynalne liczb granicznych oznaczonych w §5, Rozdział 9 jako $\omega_1, \omega_2, \ldots, \omega_n, \ldots$, gdzie $\omega_1 = \omega \cup S^{\omega}(\omega)$ oraz $\omega_i = \omega_{i-1} \cup S^{\omega}(\omega_{i-1})$ dla $i = 2, 3, \ldots$.

W tym celu zauważmy, że

dla dowolnej liczby porządkowej α, zbiór $S^{\omega}(\alpha) = \{z : \exists y(y \in \omega \wedge z = S^{y}(\alpha))\}$ jest równoliczny z ω.

Funkcja $f : \omega \longrightarrow S^{\omega}(\alpha)$ określona następująco: $\forall y \in \omega,\ f(y) = S^{y}(\alpha)$, jest bowiem bijekcją. Z definicji zbioru $S^{\omega}(\alpha)$ mamy przecież natychmiast: $S^{\omega}(\alpha) = \vec{f}(\omega)$, czyli f jest „*na*". Ponadto, gdy $m \neq n$ dla jakichś $m, n \in \omega$, a więc gdy $m \in n$ lub $n \in m$, to odpowiednio $S^{m}(\alpha) \in S^{n}(\alpha)$ lub $S^{n}(\alpha) \in S^{m}(\alpha)$ – według lematu z §4, Rozdział 9. Zatem $S^m(\alpha) \neq S^n(\alpha)$, tzn. $f(m) \neq f(n)$, czyli f jest różnowartościowa.

Ostatecznie, na mocy Twierdzeń 6, 16, dla dowolnej liczby porządkowej α, $card(S^\omega(\alpha)) = \omega$. Stąd oraz na mocy Tw. 16 i lematu z §2: $card(\omega_1) = card(\omega \cup S^\omega(\omega)) = \omega$ oraz dla $i = 2, 3, \ldots,$ $card(\omega_i) = card(\omega_{i-1} \cup S^\omega(\omega_{i-1})) = \omega$ (oczywisty dowód indukcyjny pomijamy).

Liczby graniczne $\omega_1, \omega_2, \ldots$ nie są więc liczbami kardynalnymi. Nie należy stąd jednak wysuwać przypuszczenia, że jedynymi liczbami kardynalnymi, które nie są izolowanymi liczbami porządkowymi, są liczby: $\varnothing$ oraz ω. Bogactwo liczb kardynalnych (naturalnie będących liczbami granicznymi) jest, jak wykażemy w następnym paragrafie, cokolwiek przerażające.

§4. Liczby kardynalne większe od ω

Fundamentalnym dla ustalenia istnienia liczb kardynalnych α takich, że $\omega \in \alpha$ jest następujące

TWIERDZENIE CANTORA. *Dla dowolnego zbioru X, $card(X) \in card(P(X))$. (Ilość elementów zbioru jest mniejsza od ilości elementów jego zbioru potęgowego.)*

DOWÓD. Rozważmy funkcję $f : X \longrightarrow P(X)$ określoną następująco: $\forall y \in X, f(y) = \{y\}$. Jest widoczne, że f jest różnowartościowa. Zatem $f : X \longrightarrow \vec{f}(X)$ jest bijekcją, co implikuje, że zbiory X, $\vec{f}(X)$ są równoliczne, czyli na mocy Tw. 6, $card(X) = card(\vec{f}(X))$. Jednakże $\vec{f}(X) \subseteq P(X)$, zatem na mocy Tw. 11, $card(\vec{f}(X)) \subseteq card(P(X))$. Wobec tego, $card(X) \subseteq card(P(X))$, tzn. $card(X) \in card(P(X))$ lub $card(X) = card(P(X))$. Aby zakończyć dowód wystarczy więc wykazać, że $card(X) \neq card(P(X))$.

Załóżmy nie wprost, że $card(X) = card(P(X))$. Wówczas na mocy Tw. 6, X jest równoliczny z $P(X)$. Niech więc funkcja $g : X \longrightarrow P(X)$ będzie bijekcją. Rozważmy aksjomat podzbiorów $\forall x(\phi(x) \Rightarrow x \in X) \Rightarrow \exists y \forall x(x \in y \Leftrightarrow \phi(x))$, gdzie $\phi(x)$ jest postaci: $x \in X \wedge x \notin g(x)$. Ponieważ poprzednik powyższej implikacji jest spełniony, istnieje więc zbiór $Z = \{x : \phi(x)\}$, tzn. $Z = \{x : x \in X \wedge x \notin g(x)\}$. Oczywiście $Z \subseteq X$, czyli $Z \in P(X)$. Ponieważ funkcja g przekształca X na zbiór $P(X)$, więc niech $x_0 \in X$ będzie takim elementem, że $g(x_0) = Z$. Wówczas otrzymujemy: $x_0 \in Z \Leftrightarrow x_0 \notin Z$, czyli sprzeczność. Jeśli bowiem $x_0 \in Z$, to z definicji zbioru Z, $x_0 \notin g(x_0)$, zatem $x_0 \notin Z$. Jeśli zaś $x_0 \notin Z$, to, ponieważ $x_0 \in X$, więc $x_0 \in g(x_0)$, zatem $x_0 \in Z$. $\square$

WNIOSEK. $\omega \in card(P(\omega))$.

Dowód. Oczywisty na podstawie Tw. Cantora i Tw. 16. $\square$

Jak widać, $card(P(\omega))$ jest liczbą kardynalną większą od ω. Lecz ponadto, według Tw. Cantora, $card(P(\omega)) \in card(P(P(\omega)))$ itd., tzn. mamy liczby kardynalne ω, $card(P(\omega))$, $card(P(P(\omega))), \ldots, card(P^n(\omega)), \ldots$ takie, że

$$\omega \in card(P(\omega)) \in card(P(P(\omega))) \in \ldots \in card(P^n(\omega)) \in \ldots$$

Co więcej, weźmy pod uwagę zbiór $P^\omega(\omega) = \{z : \exists y(y \in \omega \wedge z = P^y(\omega))\}$ (jego istnienie gwarantuje aksjomat podstawiania – zob. w §5, Rozdział 9 zastosowanie tego aksjomatu dla stwierdzenia istnienia zbioru $F^\omega(X)$ dla dowolnej operacji jednoargumentowej F oraz dowolnego zbioru X). Następujący fakt stwierdza istnienie liczby kardynalnej większej od każdej liczby kardynalnej z powyższej sekwencji:

Twierdzenie 20. $\forall n \in \omega, card(P^n(\omega)) \in card(\bigcup P^\omega(\omega))$.

Dowód. Ponieważ z definicji zbioru $P^\omega(\omega)$, $\forall n \in \omega$, $P^n(\omega) \in P^\omega(\omega)$, więc $\forall n \in \omega, P^n(\omega) \subseteq \bigcup P^\omega(\omega)$ (Tw. 11(1), Rozdział 1). Stąd, według Tw. 11 otrzymujemy:
(1) $\forall n \in \omega,\ card(P^n(\omega)) \subseteq card(\bigcup P^\omega(\omega))$.

Na mocy (1) oraz Tw. 18, Rozdział 8, aby dowieść twierdzenia, wystarczy wykazać, że $\forall n \in \omega,\ card(P^n(\omega)) \neq card(\bigcup P^\omega(\omega))$. Załóżmy więc nie wprost, że dla pewnego $n \in \omega$,
(2) $card(P^n(\omega)) = card(\bigcup P^\omega(\omega))$.

Z Tw. Cantora, $card(P^n(\omega)) \in card(P(P^n(\omega)))$. Zatem z (2) uzyskujemy:
(3) $card(\bigcup P^\omega(\omega)) \in card(P(P^n(\omega)))$.

Lecz $card(P(P^n(\omega))) = card(P^{n+1}(\omega))$, więc według (1), $card(P(P^n(\omega))) \subseteq card(\bigcup P^\omega(\omega))$, co wraz z (3) prowadzi do absurdu: $card(\bigcup P^\omega(\omega)) \in card(\bigcup P^\omega(\omega))$. $\square$

Ponieważ nic nie stoi na przeszkodzie zastosować Tw. Cantora dla zbiorów $\bigcup P^\omega(\omega), P(\bigcup P^\omega(\omega)), \ldots, P^n(\bigcup P^\omega(\omega)), \ldots$, więc otrzymujemy kolejną sekwencję liczb kardynalnych:

$$card(\bigcup P^\omega(\omega)) \in card(P(\bigcup P^\omega(\omega))) \in \ldots \in card(P^n(\bigcup P^\omega(\omega))) \in \ldots.$$

Co więcej, analogicznie jak poprzednio, można rozważyć zbiór $P^\omega(\bigcup P^\omega(\omega))$, aby, identycznie dowodząc, otrzymać analogon Tw. 20:

$$\forall n \in \omega,\ card(P^n(\bigcup P^\omega(\omega)) \in card(\bigcup P^\omega(\bigcup P^\omega(\omega)))$$

i znowu zastosować Tw. Cantora dla zbiorów $P^n(\bigcup P^\omega(\bigcup P^\omega(\omega))$ dla $n \in \omega$ itd. w nieskończoność.

Na koniec rozważmy jeszcze interesujący problem związany z najmniejszą liczbą kardynalną większą od ω, precyzyjniej, najmniejszą liczbą porządkową α taką, że α jest liczbą kardynalną i $\omega \in \alpha$.

Na mocy Tw. 21, Rozdział 8, niech α_0 będzie najmniejszą liczbą kardynalną większą od liczby ω. Według Wniosku z Tw. Cantora oraz Wniosku z Tw. 6, niewątpliwie $\alpha_0 \subseteq card(P(\omega))$, zatem $\alpha_0 \in card(P(\omega))$ lub $\alpha_0 = card(P(\omega))$. Okazuje się, że w ramach teorii ZFC nie można rozstrzygnąć, który z członów tej alternatywy jest twierdzeniem teorii. Równość $\alpha_0 = card(P(\omega))$, czyli supozycja, że najmniejszą liczbą kardynalną większą od ω jest liczba $card(P(\omega))$, zwana jest *hipotezą continuum* (od nazwy liczby kardynalnej $card(P(\omega))$, zwanej liczbą *continuum*) – por. §3, Rozdział 7.

Bibliografia

[1] Aczel P., **Non-Well-Founded Sets**, CSLI, Lecture Notes 14, Stanford 1988.

[2] Ajdukiewicz K., *Metodologiczne typy nauk*, [w:] K. Ajdukiewicz, **Język i poznanie**, t. 1, PWN, Warszawa 1985, s. 287–313.

[3] Bell J. L., Slomson A. B., **Models and Ultraproducts**, North Holland, Amsterdam 1969.

[4] Beth E. W., **The Foundations of Mathematics**, North Holland, Amsterdam 1959.

[5] Chang C. C., Keisler H. J., **Model Theory**, North Holland, Amsterdam 1973.

[6] Fraenkel A. A., **Abstract Set Theory**, North Holland, Amsterdam 1976.

[7] Fraenkel A. A., Bar-Hillel J., Levy A., **Foundations of Set Theory**, North Holland, Amsterdam 1973.

[8] Grätzer G., **Universal Algebra**, Springer-Verlag, New York 1979.

[9] Grzegorczyk A., **Zarys arytmetyki teoretycznej**, PWN, Warszawa 1971.

[10] Guzicki W., Zbierski P., **Podstawy teorii mnogości**, PWN, Warszawa 1978.

[11] Indrzejczak A., Nowak M., **Metody logiki, dedukcja**, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2016.

[12] Jech T. J., **Lectures in Set Theory**, Lectures Notes in Mathematics 217, Springer-Verlag 1971.

[13] Kuratowski K., **Wstęp do teorii mnogości i topologii**, PWN, Warszawa 1975.

[14] Kuratowski K., Mostowski A., **Teoria mnogości**, PWN, Warszawa 1978.

[15] Lipski W., Marek W., **Analiza kombinatoryczna**, PWN, Warszawa 1986.

[16] Mendelson E., **Introduction to Mathematical Logic**, Van Nostrand, Princeton 1964.

[17] Morse A. P., **A Theory of Sets**, Academic Press, Orlando 1986.

[18] Rasiowa H., **Wstęp do matematyki współczesnej**, PWN, Warszawa 1979.

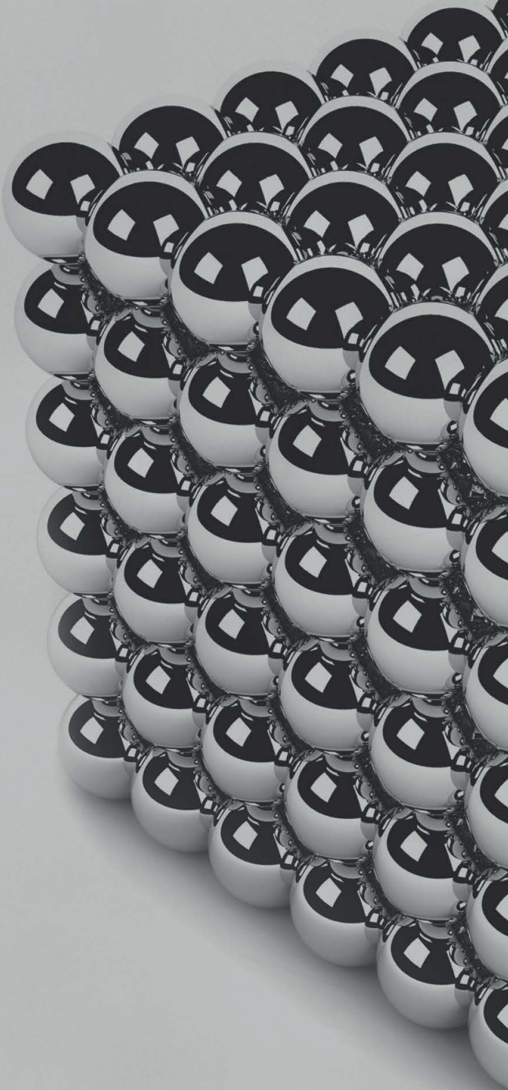
[19] Schoenfield J. R., **Mathematical Logic**, Addison-Wesley, Menlo Park 1967.

[20] Schoenfield J. R., *Axioms of set theory*, [w:] **Handbook of Mathematical Logic** (ed. J. Barwise), North Holland, Amsterdam 1977, s. 321–344.

[21] Takeuti G., Zaring W. M., **Introduction to Axiomatic Set Theory**, Springer-Verlag, New York 1971.

[22] Traczyk T., **Wstęp do teorii algebr Boole'a**, PWN, Warszawa 1970.

Monografia zawiera najważniejsze elementy aksjomatycznej teorii mnogości Zermelo-Fraenkla z aksjomatem wyboru: aksjomatykę, definicje podstawowych pojęć, teorie relacji binarnych, częściowo porządkujących, równoważnościowych, funkcji, liczb porządkowych oraz liczb kardynalnych. Powstała na podstawie wieloletnich wykładów prowadzonych przez autora dla studentów filozofii Uniwersytetu Łódzkiego. Nie wymaga więc gruntownego przygotowania matematycznego, wystarcza pewne „wyrobienie" logiczne w zakresie umiejętności dowodzenia twierdzeń, a właściwie znajomość takich stałych logicznych, jak spójniki boolowskie i kwantyfikatory. Może służyć nie tylko matematykom i studentom matematyki, lecz także humanistom chcącym ugruntować swoją wiedzę o zbiorach, wykorzystywaną często w różnych zabiegach formalizacyjnych. Tym bardziej, że pewne wątki mają charakter filozoficzny, m.in. dyskusje na temat aksjomatu regularności i pojęcia ufundowania zbioru, relacji równoważnościowej, liczby porządkowej czy aksjomatu wyboru.



WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

wydawnictwo.uni.lodz.pl
ksiegarnia@uni.lodz.pl
(42) 665 58 63

Książka dostępna również jako e-book

ISBN 978-83-8142-520-9
9 788381 425209