Wstęp do teorii mnogości

Materiały do wykładu dla 1 roku informatyki
http://www.mimuw.edu.pl/∼urzy/wtm.html

Paweł Urzyczyn
urzy@mimuw.edu.pl
2001–2006

Po co komu teoria mnogości

Fryderyk Engels definiował matematykę jako dziedzinę zajmującą się „stosunkami ilościowymi i formami przestrzennymi świata rzeczywistego”. Definicja ta jest trafna w odniesieniu do pewnych tradycyjnych działów dawnej matematyki (arytmetyka, geometria), które uprawiane były w oparciu o praktyczną obserwację rzeczywistości i podlegały stosunkowo łatwej weryfikacji poprzez doświadczenie. Współczesna matematyka, również ta, której zadaniem jest opis procesów obliczeniowych, posługuje się często modelami abstrakcyjnymi, których związek z obserwowalną rzeczywistością jest mniej bezpośredni. A ponieważ nasza intuicja, pozbawiona obserwacyjnej weryfikacji, bywa zawodna, matematyka od dawna polega na rygorystycznej ścisłości rozumowań, opierających się na możliwie najmniejszej liczbie pojęć pierwotnych i aksjomatów.

Pojęcie zbioru okazuje się tutaj niezwykle użyteczne. Przy całej swojej prostocie, pozwala na łatwe definiowanie w ścisły sposób wielu innych pojęć matematycznych. Dlatego posługujemy się językiem teorii mnogości (*mnogość* to po prostu *zbiór*) dla formułowania i badania rozmaitych teorii matematycznych.

Matematycy, w sposób mniej lub bardziej jawny, posługiwali się zbiorami od dawna. Teoria mnogości jako odrębna dziedzina powstała w XIX wieku, a za jej twórcę uważa sie zwykle Georga Cantora. Podał on taką „definicję” zbioru:

Zbiorem nazywamy zgromadzenie w jedną całość wyraźnie wyróżnionych przedmiotów naszej intuicji lub naszej myśli.

Najważniejszą rzeczą w tej definicji jest następujące założenie. Jeśli tylko potrafimy wyodrębnić pewne przedmioty za pomocą jakiegoś kryterium $K(x)$, to te przedmioty tworzą dobrze określony zbiór $\{x \mid K(x)\}$. Według Cantora, zbiór jest więc *upostaciowieniem* kryterium, które go definiuje (poprzez określenie jego elementów). W gruncie rzeczy zbiór jest pewnym skrótem myślowym: zamiast myśleć i mówić o wszystkich przedmiotach x, spełniających kryterium $K(x)$, wygodniej rozważać tylko jeden przedmiot, właśnie zbiór $\{x \mid K(x)\}$.

Na co dzień zbiory służą nam właśnie do tego. Ale jeśli raz zgodziliśmy się traktować zbiory tak jak wszystkie inne przedmioty, musimy się też zgodzić na konsekwencje, na przykład na zbiory zbiorów. W „naiwnej" teorii mnogości można na przykład rozważać zbiór wszystkich zbiorów: $Z = \{x \mid x \text{ jest zbiorem}\}$. Oczywiście taki zbiór jest swoim własnym elementem (co zapiszemy tak: $Z \in Z$). To jeszcze nic złego, ale co począć z takim zbiorem:

$$R = \{x \mid x \text{ jest zbiorem i } x \notin x\} \ ?$$

Niebezpieczne pytanie: czy $R \in R$? Jeśli $R \in R$, to R musi spełniać warunek $R \notin R$. A jeśli $R \notin R$, to warunek definiujący zbiór nie może być spełniony i mamy $R \in R$. Tak czy owak, jest źle!

Powyższe rozumowanie, zwane *antynomią Russella*, wskazuje na to, że „naiwne" pojmowanie zbiorów prowadzi do sprzeczności. Nie można uprawiać abstrakcyjnej matematyki opierając się wyłącznie na niedoskonałej ludzkiej intuicji. Ale nie wynika stąd, że cała teoria zbiorów jest bezużyteczna. Trzeba ją tylko tak zmodyfikować, ograniczyć, żeby nie groziły nam antynomie. Jak to zrobić? Zastosujemy metodę aksjomatyczną. Ograniczymy się do niewielkiej liczby elementarnych własności zbiorów, a z nich będziemy wnioskować o innych własnościach. Jeśli dobrze wybierzemy aksjomaty, to uda się uniknąć sprzeczności a jednocześnie zachować z „naiwnej" teorii mnogości to, co pożyteczne.

1 Aksjomaty teorii mnogości

Używamy następujących symboli na oznaczenie spójników zdaniowych: znak $\wedge$ oznacza koniunkcję, $\vee$ oznacza alternatywę, $\neg$ to negacja, $\to$ to implikacja i wreszcie $\leftrightarrow$ to równoważność. Kwantyfikatory czytamy tak: „$\forall x$" to „dla każdego x" a „$\exists x$" to „istnieje takie x, że". Stosujemy następujące priorytety:

1. negacja i kwantyfikatory,
2. koniunkcja i alternatywa,
3. implikacja.

Na przykład w $\forall x A(x) \vee B \to C$ domyślne nawiasy są takie: $((\forall x A(x)) \vee B) \to C$. W szczególności kwantyfikator dotyczy tylko $A(x)$. A wyrażenie $A \vee B \wedge C$ jest niepoprawne.

Napis „$x = y$" oznacza, że x i y są nazwami tego samego przedmiotu.

Napis „$x \in y$" czytamy „x jest elementem y" lub „x należy do y".

Język, którym będziemy się posługiwać, składa się z symboli logicznych, i znaków równości i należenia. Wszystkie dodatkowe oznaczenia, które wprowadzimy, będą w istocie *skrótami* stosowanymi dla wygody. Na przykład, zamiast „$\neg x \in y$" i „$\neg x = y$" będziemy często pisać odpowiednio „$x \notin y$" i „$x \neq y$".

Wyrażenie $\forall x{\in}a\, W(x)$ oznacza to samo, co $\forall x\,(x \in a \to W(x))$, a wyrażenie $\exists x{\in}a\, W(x)$ jest skrótem dla $\exists x\,(x \in a \wedge W(x))$. Zamiast $\forall x \forall y \ldots$ piszemy $\forall x, y \ldots$ itd.

Zauważmy, że w naszym języku nie ma specjalnego oznaczenia na stwierdzenie „x jest zbiorem". Wynika to z następującego wygodnego założenia: skoro i tak mówimy przede wszystkim o zbiorach, to tak naprawdę nie ma potrzeby rozważania nic innego niż zbiory. Elementy zbiorów to też zbiory. Nie musimy interesować się ich elementami, jeśli nie ma takiej potrzeby. Ta konwencja może się wydawać dziwna, ale jest wygodnym uproszczeniem. Nic przez to nie tracimy, bo w razie potrzeby można różne rzeczy, np. liczby, zdefiniować jako pewne specyficzne zbiory.

Najważniejszy aksjomat

Najważniejszy aksjomat to *aksjomat jednoznaczności*, zwany także *aksjomatem ekstensjonalności*. Stwierdza on, że zbiór jest jednoznacznie wyznaczony przez wskazanie jego elementów. Sposób, w jaki określamy elementy zbioru (np. porządek, powtórzenia) nie ma znaczenia, ważne jest jedynie to, czy dany przedmiot należy do naszego zbioru, czy nie. Wyrażamy tę własność tak:

1.1 (Aksjomat jednoznaczności)

$$\forall x \forall y (x = y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y))$$

Aby udowodnić, że dwa zbiory a i b są równe, postępujemy więc zwykle tak: pokazujemy, że każdy element zbioru a należy też do b, a każdy element zbioru b należy też do a.

Mówimy, że zbiór x jest *zawarty* w zbiorze y (lub, że jest jego *podzbiorem*) wtedy i tylko wtedy, gdy zachodzi warunek $\forall z (z \in x \to z \in y)$. Piszemy wówczas „$x \subseteq y$". Używamy też następujących skrótów:

$$\text{„}x \not\subseteq y\text{" oznacza „}\neg x \subseteq y\text{";}$$
$$\text{„}x \subsetneq y\text{" oznacza „}x \subseteq y \wedge x \neq y\text{".}$$

Fakt 1.2 $\quad \forall x \forall y (x = y \leftrightarrow x \subseteq y \wedge y \subseteq x)$.

A zatem równość zbiorów to ich wzajemne zawieranie.

Uwaga: Należy odróżniać *zawieranie* ($\subseteq$) od *należenia* ($\in$).

Najważniejszy zbiór

Najważniejsze rzeczy są zawsze najprostsze. Najprostszy jest taki zbiór, który nie ma elementów.

1.3 (Aksjomat zbioru pustego)

$$\exists x \forall y (y \notin x)$$

Zbiór x o własności $\forall y (y \notin x)$ nazywamy zbiorem *pustym*. Istnieje tylko jeden zbiór pusty.

Fakt 1.4 *Jeśli zbiory x_1 i x_2 są puste, to $x_1 = x_2$.*

Dowód: Przypuśćmy, że $\forall y (y \notin x_1)$ oraz $\forall y (y \notin x_2)$. Wtedy

$$\forall y (y \in x_1 \leftrightarrow y \in x_2)$$

co oznacza (z jednoznaczności), że $x_1 = x_2$. ∎

Zbiór pusty oznaczamy symbolem $\emptyset$.

Operacje na zbiorach

Zdefiniujemy teraz kilka operacji na zbiorach. Dla porządku, poprawność tych operacji, tj. istnienie odpowiednich zbiorów, musimy postulować aksjomatami. Aksjomaty poniżej mają taką postać: „dla dowolnych zbiorów x, $y, \ldots$ istnieje zbiór z, który ma dokładnie takie a takie elementy." Z jednoznaczności zawsze wynika, że taki zbiór z jest tylko jeden.

1.5 (Aksjomat pary)

$$\forall x \forall y \exists z \forall t (t \in z \leftrightarrow (t = x \vee t = y))$$

Aksjomat pary czytamy tak: dla dowolnych x, y istnieje zbiór z, którego elementami są x, y i nic więcej. Taki zbiór jest tylko jeden (por. Fakt 1.4) i oznaczamy go przez $\{x, y\}$. Zauważmy, że $\{x, y\} = \{y, x\}$.

Zbiór $\{x, x\}$ zapisujemy po prostu jako $\{x\}$. Ogólniej, zbiór o elementach $x_1, \ldots, x_n$ zapisujemy jako $\{x_1, \ldots, x_n\}$. Kolejność elementów na liście i ich powtórzenia nie mają znaczenia, np. $\{a, b\} = \{b, b, a\}$.

Uwaga: Pamiętajmy, że $\emptyset \neq \{\emptyset\}$.

1.6 (Aksjomat sumy)

$$\forall x \exists y \forall z (z \in y \leftrightarrow \exists t (z \in t \wedge t \in x))$$

Aksjomat sumy mówi, że dla dowolnego zbioru x istnieje zbiór y złożony dokładnie z tych i tylko tych przedmiotów, które są elementami elementów zbioru x. Na mocy jednoznaczności, taki zbiór y jest tylko jeden. Oznaczamy go przez $\bigcup x$ i nazywamy *sumą uogólnioną* rodziny zbiorów x. (Określenie „rodzina zbiorów" oznacza w zasadzie to samo co „zbiór". Używamy go wtedy, gdy chcemy podkreślić, że elementy zbioru x to też zbiory.) Morał do zapamiętania:

$$z \in \bigcup x \leftrightarrow \exists t (z \in t \wedge t \in x).$$

Często stosujemy notację indeksowaną, np. $\bigcup_{i=1}^{n} A_i = \bigcup \{A_1, \ldots, A_n\}$. Zwykła suma dwóch zbiorów jest też szczególnym przypadkiem sumy uogólnionej. Definiujemy ją tak:

$$x \cup y = \bigcup \{x, y\}$$

Fakt 1.7 *Dla dowolnych x, y, z:*

$$(1) \qquad z \in x \cup y \leftrightarrow (z \in x \vee z \in y);$$

$$(2) \qquad z \notin x \cup y \leftrightarrow (z \notin x \wedge z \notin y).$$

Dowód: Oczywiście wystarczy udowodnić część (1), bo część (2) wynika z niej przez proste zastosowanie prawa De Morgana.

($\Rightarrow$) Niech $z \in x \cup y$. Ponieważ $x \cup y = \bigcup \{x, y\}$, oznacza to, że $z \in t$ dla pewnego $t \in \{x, y\}$. Ale wtedy albo[1] $t = x$ albo $t = y$. Zatem $z \in x$ lub $z \in y$.

($\Leftarrow$) Mamy dwa przypadki. Przypuśćmy najpierw, że $z \in x$. Skoro $x \in \{x, y\}$, to $z \in \bigcup \{x, y\}$ z definicji sumy. Przypadek $z \in y$ jest analogiczny. ∎

1.8 (Aksjomat potęgi)

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x)$$

Aksjomat potęgi stwierdza, że dla dowolnego x istnieje zbiór złożony ze wszystkich podzbiorów zbioru x. Oczywiście jest dokładnie jeden taki zbiór. Będziemy go oznaczać przez $\mathbf{P}(x)$. Zapamiętajmy równoważność:

$$z \in \mathbf{P}(x) \leftrightarrow z \subseteq x$$

Na przykład $\mathbf{P}(\emptyset) = \{\emptyset\}$, $\mathbf{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ oraz $\mathbf{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Elementami zbioru $\mathbf{P}(x)$ są zawsze $\emptyset$ i x.

[1]Nie ma różnicy pomiędzy „lub" i „albo". W obu przypadkach mamy na myśli zwykłą alternatywę.

1.9 (Aksjomat podzbiorów (wycinania))

Jeżeli $W(z)$ jest dowolnym warunkiem (kryterium), to

$$\forall x \exists y \forall z (z \in y \leftrightarrow (z \in x \wedge W(z)))$$

Użyte powyżej określenie „warunek” oznacza dowolną własność z wyrażoną za pomocą języka teorii mnogości. Aksjomat podzbiorów, zwany też aksjomatem wycinania, nie jest właściwie pojedynczym aksjomatem ale *schematem* aksjomatu. W istocie mamy po jednym aksjomacie dla dowolnego warunku $W(z)$. Mówi on, że dla dowolnego x istnieje zbiór złożony z tych i tylko tych elementów zbioru x, które spełniają warunek. Jak zwykle, aksjomat jednoznaczności gwarantuje istnienie tylko jednego takiego zbioru. Zapisujemy go tak:

$$\{z \in x \mid W(z)\}, \quad \text{lub tak:} \quad \{z \in x : W(z)\}.$$

Czasami jednak nadużywamy tej notacji, pisząc na przykład $\{\{a, b\} \mid a, b \in A\}$ zamiast poprawnego $\{t \in \mathbf{P}(A) \mid \exists a, b \in A\, (t = \{a, b\})\}$.

Uwaga dla dociekliwych: W tak zwanej teorii mnogości Zermelo-Fraenkla (ZF) przyjmuje się nieco silniejszy aksjomat zwany aksjomatem zastępowania. Nam on na razie nie jest potrzebny.

Aksjomat wycinania jest przydatny przy definiowaniu rozmaitych zbiorów. Na przykład *iloczyn uogólniony* rodziny zbiorów x definiujemy tak:

$$\bigcap x = \{z \in \bigcup x \mid \forall t (t \in x \to z \in t)\}$$

Fakt 1.10 *Jeśli $x \neq \emptyset$ to dla dowolnego z*

$$z \in \bigcap x \leftrightarrow \forall t (t \in x \to z \in t).$$

Dowód: Część ($\Rightarrow$) jest oczywista. W części ($\Leftarrow$) wystarczy wykazać, że $z \in \bigcup x$. Ale skoro $x \neq \emptyset$ to istnieje takie t, że $t \in x$. Ponieważ $\forall t (t \in x \to z \in t)$, więc $z \in t \in x$. Zatem faktycznie $z \in \bigcup x$. ∎

Uwaga: Założenie $x \neq \emptyset$ w Fakcie 1.10 jest istotne. Rzeczywiście, $\bigcap \emptyset = \emptyset$. Tymczasem warunek $\forall t (t \in \emptyset \to z \in t)$ jest spełniony przez dowolne z!

Iloczyn dwóch zbiorów definiujemy jako szczególny przypadek iloczynu uogólnionego.

$$x \cap y = \bigcap \{x, y\}.$$

Fakt 1.11 *Dla dowolnych x, y, z:*

$$(1) \quad z \in x \cap y \leftrightarrow (z \in x \wedge z \in y);$$

$$(2) \quad z \notin x \cap y \leftrightarrow (z \notin x \vee z \notin y).$$

Dowód: Łatwy. ∎

Określimy jeszcze jedną często spotykaną operację na zbiorach: *różnicę zbiorów*:

$$x - y = \{z \in x \mid z \notin y\}$$

Uwaga: Często można spotkać się z pojęciem „dopełnienia" danego zbioru a, co zwykle oznacza się przez $-a$. To pojęcie ma sens wtedy, gdy wszystkie zbiory będące przedmiotem rozważań są podzbiorami jednego ustalonego zbioru $\top$, np. wtedy gdy interesują nas wyłącznie zbiory punktów płaszczyzny. Wówczas dopełnieniem zbioru $a \subseteq \top$ (do zbioru $\top$) nazywa się różnicę $\top - a$. Bez ustalonego zbioru $\top$ nie można mówić o operacji dopełnienia.

Regularność *

Dalsze aksjomaty teorii mnogości będziemy omawiać wtedy, kiedy będą nam potrzebne. Teraz jeszcze ciekawostka dla dociekliwych.

1.12 (Aksjomat regularności)

$$\forall x(x \neq \emptyset \to \exists y((y \in x) \wedge (y \cap x = \emptyset)))$$

Sens regularności jest taki: wprawdzie może się zdarzyć, że $v \in y \in x$ oraz $v \in x$, tj. element elementu x może też być elementem x, ale zawsze musi być takie $y \in x$, które nie ma już elementów wspólnych z x. Wynika stąd na przykład to:

Fakt 1.13

$$\forall z(z \notin z)$$

Dowód: Z aksjomatu regularności zastosowanego do zbioru $\{z\}$, wynika, że $z \cap \{z\} = \emptyset$, bo przecież z jest jedynym elementem $\{z\}$. A zatem $z \notin z$, bo inaczej $z \cap \{z\} \neq \emptyset$. ∎

2 Relacje

W matematyce mamy do czynienia z najrozmaitszymi relacjami. Wiele z nich ma podobne własności. Aby jednak mówić o wspólnych cechach rożnych relacji, należy najpierw odpowiedzieć na pytanie co w ogóle uważamy za relację, powiedzmy dwuargumentową. Dla

* Fragmenty oznaczone gwiazdką są przeznaczone dla dociekliwych.

naszych celów dostatecznie dobrym uściśleniem pojęcia relacji jest taka definicja: relacja to po prostu zbiór wszystkich uporządkowanych par tych przedmiotów, pomiędzy ktorymi relacja zachodzi. Istotnie, znając ten zbiór, wiemy w zasadzie wszystko o relacji. No dobrze, ale co to jest para uporządkowana?

Definicja 2.1 *Uporządkowaną parą* przedmiotów a i b nazywamy zbiór:

$$\langle a, b\rangle = \{\{a\}, \{a, b\}\}$$

Definicja 2.1 może się wydawać dziwna. Zauważmy jednak, że to czego naprawdę oczekujemy od pary uporządkowanej to następująca własność: para uporządkowana powinna być jednoznacznie wyznaczona przez swoje współrzędne i ich kolejność. A nasza definicja ma tę własność.

Lemat 2.2 *Dla dowolnych a, b, x, y zachodzi równoważność:*

$$\langle a, b\rangle = \langle x, y\rangle \quad \textit{wtedy i tylko wtedy, gdy} \quad a = x \text{ i } b = y.$$

Dowód: Implikacja z prawej do lewej jest oczywista. Dla dowodu implikacji z lewej do prawej przyjmijmy oznaczenia:

$$L = \langle a, b\rangle = \{\{a\}, \{a, b\}\} \quad \text{oraz} \quad P = \langle x, y\rangle = \{\{x\}, \{x, y\}\},$$

i załóżmy, że $L = P$. Ponieważ $\{a\} \in L$, więc $\{a\} \in P$, czyli $\{a\} = \{x\}$, lub $\{a\} = \{x, y\}$. W obu przypadkach $x \in \{a\}$, a więc $a = x$.

Pozostaje wykazać, że $b = y$. Uwzględniając równość $a = x$, możemy teraz napisać

$$P = \langle x, y\rangle = \{\{a\}, \{a, y\}\}.$$

Skoro $L = P$ to także $\bigcup L = \bigcup P$, czyli $\{a, b\} = \{a, y\}$. Stąd albo $y = b$ (i dobrze) albo $y = a$. Ale wtedy $\{a, y\} = \{a\} = \{a, b\}$, skąd $b \in \{a\} = \{y\}$. A więc też $b = y$. ∎

Definicja 2.3 *Iloczynem kartezjańskim* zbiorów a i b nazywamy taki zbiór $a \times b$, że dla dowolnego t:

$$t \in a \times b \quad \text{wtedy i tylko wtedy, gdy} \quad \exists u \exists v (t = \langle u, v\rangle \wedge u \in a \wedge v \in b).$$

Uwaga: Iloczyn kartezjański $a \times b$ zawsze istnieje i jest dokładnie jeden. Istotnie, można go zdefiniować tak: $a \times b = \{t \in \mathbf{P}(\mathbf{P}(a \cup b)) \mid \exists u \exists v (t = \langle u, v\rangle \wedge u \in a \wedge v \in b)\}$.

Definicja 2.4 Dowolny podzbiór r iloczynu kartezjańskiego $a \times b$ nazywamy *relacją*[2] *ze zbioru a w zbiór b*. Jeśli $a = b$, to mówimy, że r jest relacją *w zbiorze a*.
Piszemy czasami „$x\,r\,y$" zamiast „$\langle x, y\rangle \in r$".

Uwaga: O relacji można mówić wtedy gdy wiadomo w jakim zbiorze jest określona. Inkluzja (zawieranie) dowolnych zbiorów nie jest relacją. Ale dla dowolnej rodziny zbiorów R, zbiór par

$$\subseteq_R = \{\langle x, y\rangle \in R \times R \mid x \subseteq y\}$$

jest relacją w zbiorze R. Dlatego można mówić o „relacji inkluzji w zbiorze R".

Definicja 2.5 Pewne własności relacji dwuargumentowych mają swoje nazwy. Oto niektóre z nich. Mówimy, że relacja r w zbiorze a jest

$$\begin{array}{rll}
\textit{zwrotna} & \text{gdy} & \forall x{\in}a\,(x\,r\,x) \\
\textit{symetryczna} & \text{gdy} & \forall x{\in}a\,\forall y{\in}a\,(x\,r\,y \to y\,r\,x) \\
\textit{przechodnia} & \text{gdy} & \forall x{\in}a\,\forall y{\in}a\,\forall z{\in}a(x\,r\,y \wedge y\,r\,z \to x\,r\,z) \\
\textit{antysymetryczna} & \text{gdy} & \forall x{\in}a\,\forall y{\in}a\,(x\,r\,y \wedge y\,r\,x \to x = y) \\
\textit{spójna} & \text{gdy} & \forall x{\in}a\,\forall y{\in}a\,(x\,r\,y \vee y\,r\,x)
\end{array}$$

Na przykład relacja prostopadłości prostych na płaszczyźnie jest symetryczna, ale nie jest zwrotna, antysymetryczna, przechodnia ani spójna. Natomiast relacja równoległości prostych jest zwrotna, przechodnia i symetryczna, ale nie jest antysymetryczna ani spójna.

Definicja 2.6 Relacją odwrotną do danej relacji $r \subseteq a \times b$ nazywamy zbiór

$$r^{-1} = \{\langle y, x\rangle \mid \langle x, y\rangle \in r\} \subseteq b \times a$$

Jeśli $r \subseteq a \times b$ oraz $s \subseteq b \times c$, to *złożeniem* relacji r i s nazywamy relację $(r\,;s) \subseteq a \times c$, określoną tak:

$$x\,(r\,;s)\,y \quad \text{wtedy i tylko wtedy, gdy} \quad \exists z \in b\,(x\,r\,z \wedge z\,s\,y).$$

3 Funkcje

Funkcja to szczególny rodzaj relacji. Zatem także funkcje są w teorii mnogości rozumiane jako zbiory par argument-wartość. Nie ma tu znaczenia jak dana funkcja jest zdefiniowana, a jedynie jakie wartości są przypisane poszczególnym argumentom.

[2] Ograniczamy się do relacji dwuargumentowych. Relacje trójargumentowe można definiować np. jako podzbiory iloczynów postaci $(a \times b) \times c$.

Definicja 3.1 Relacja $f \subseteq a \times b$ jest *funkcją ze zbioru* a *w zbiór* b (co zapisujemy $f : a \to b$) wtedy i tylko wtedy, gdy:

1) $\forall x{\in}a\, \exists y{\in}b\, (\langle x, y\rangle \in f)$;

2) $\forall x{\in}a\, \forall y{\in}b\, \forall z{\in}b\, (\langle x, y\rangle \in f \wedge \langle x, z\rangle \in f \to y = z)$.

Jedyny element $y \in b$ spełniający warunek $\langle x, y\rangle \in f$ oznaczamy przez $f(x)$. Zbiór a nazywamy *dziedziną* funkcji f i oznaczamy przez $\mathrm{Dom}(f)$. *Zbiorem wartości* funkcji f nazywamy zbiór $\mathrm{Rg}(f) = \{y \in b \mid \exists x{\in}a\, f(x) = y\}$. Zbiór wszystkich funkcyj z a do b oznaczamy przez b^a.

Zauważmy, że aby jednoznacznie określić funkcję $f : a \to b$ potrzeba i wystarcza określić wartość $f(x)$ dla dowolnego $x \in a$. Jeśli f, g są dwoma funkcjami z a w b, to:

$$\begin{array}{lll} f = g & \text{wtedy i tylko wtedy, gdy} & \forall x{\in}a\, f(x) = g(x); \\ f \neq g & \text{wtedy i tylko wtedy, gdy} & \exists x{\in}a\, f(x) \neq g(x). \end{array}$$

Warto też sobie uświadomić, że jeśli f jest dowolnym zbiorem par uporządkowanych, spełniającym warunek (2) powyżęj, to f jest funkcją z pewnego zbioru a w pewien zbiór b. Dociekliwi łatwo zauważą, że dziedzina i zbiór wartości tej funkcji są zawarte w zbiorze $\bigcup\bigcup f$.

Definicja 3.2

- Funkcja $f : a \to b$ jest *różnowartościowa* (notacja $f : a \xrightarrow{1-1} b$) wtedy i tylko wtedy, gdy zachodzi warunek $\forall x, y \in a\, (x \neq y \to f(x) \neq f(y))$, lub równoważnie, gdy $\forall x, y \in a\, (f(x) = f(y) \to x = y)$.
- Funkcja $f : a \to b$ jest *na* b wtedy i tylko wtedy, gdy $\forall y{\in}b\, \exists x{\in}a\, (f(x) = y)$, lub równoważnie, gdy $b = \mathrm{Rg}(f)$. Używamy wtedy zapisu $f : a \xrightarrow{\text{na}} b$.
- Funkcję różnowartościową nazywamy też *injekcją*, funkcję „na” nazywamy *surjekcją*, a funkcję, która jest różnowartościowa i „na” nazywamy *bijekcją*. W przypadku bijekcji stosujemy notację $f : a \xrightarrow[\text{na}]{1-1} b$.

Przykładem funkcji różnowartościowej jest $f : \mathbf{P}(A) \xrightarrow{1-1} \mathbf{P}(A \times A)$, określona wzorem $f(z) = z \times z$, dla $z \subseteq A$. Przykładami surjekcji są *rzutowania* $\pi_1 : A \times B \to A$ oraz $\pi_2 : A \times B \to B$ określone równaniami $\pi_1(\langle x, y\rangle) = x$ i $\pi_2(\langle x, y\rangle) = y$. Zauważmy jednak, że każda funkcja f jest surjekcją na swój zbiór wartości $\mathrm{Rg}(f)$.

Odwracanie i składanie

Jeżeli $f : a \xrightarrow{1-1} b$ to relację f^{-1} nazywamy *funkcją odwrotną* do funkcji f.

Fakt 3.3 *Jeśli $f : a \xrightarrow{1-1} b$, to $f^{-1} : \mathrm{Rg}(f) \xrightarrow[\text{na}]{1-1} a$.*

Dowód: Na początek zauważmy, że $f^{-1} \subseteq \mathrm{Rg}(f) \times a$, bo jeśli $\langle x, y\rangle \in f^{-1}$ to $\langle y, x\rangle \in f$, więc $y \in a$ oraz $x = f(y) \in \mathrm{Rg}(f)$.

Sprawdzamy warunki (1) i (2) Definicji 3.1.

1) Jeśli $x \in \mathrm{Rg}(f)$, to $x = f(y)$ dla pewnego y, więc $\langle x, y\rangle \in f^{-1}$.
2) Jeśli $\langle x, y\rangle \in f^{-1}$ i $\langle x, z\rangle \in f^{-1}$, to $x = f(y)$ i $x = f(z)$, skąd $y = z$, bo funkcja f jest różnowartościowa.

Funkcja f^{-1} jest różnowartościowa, bo gdyby $f^{-1}(x) = f^{-1}(y) = z$ to $x = f(z) = y$. Jest ona także na a, bo dla dowolnego $y \in a$ mamy $y = f^{-1}(f(y))$. ∎

Definicja 3.4 Niech $f : a \to b$ oraz $g : b \to c$. *Złożeniem funkcji f i g* nazywamy funkcję $g \circ f : a \to c$ określoną równaniem $(g \circ f)(x) = g(f(x))$, dla dowolnego $x \in a$.

Uwaga: Jeśli złożenie $g \circ f$ jest określone, to $g \circ f = (f\,; g)$.

Dowody poniższych faktów pozostawione są jako ćwiczenie:

Fakt 3.5

1) *Jeśli $f : a \to b$, $g : b \to c$ i $h : c \to d$, to $h \circ (g \circ f) = (h \circ g) \circ f$.*
2) *Jeśli istnieje f^{-1} to $f^{-1} \circ f = \mathrm{id}_{\mathrm{Dom}(f)}$ oraz $f \circ f^{-1} = \mathrm{id}_{\mathrm{Rg}(f)}$.*
3) *Zawsze $f \circ \mathrm{id}_{\mathrm{Dom}(f)} = f = \mathrm{id}_{\mathrm{Rg}(f)} \circ f$.*

Fakt 3.6

1) *Jeśli $f : a \xrightarrow{1-1} b$ oraz $g : b \xrightarrow{1-1} c$ to $g \circ f : a \xrightarrow{1-1} c$.*
2) *Jeśli $f : a \xrightarrow{\text{na}} b$ oraz $g : b \xrightarrow{\text{na}} c$ to $g \circ f : a \xrightarrow{\text{na}} c$.*

Definicja 3.7 Niech $f : A \to B$. *Obrazem* zbioru $C \subseteq A$ przy przekształceniu f nazywamy zbiór

$$\vec{f}(C) = \{b \in B \mid \exists a \in C\,(f(a) = b)\}.$$

Inaczej można napisać:

$$\vec{f}(C) = \{f(a) \mid a \in C\}.$$

A *przeciwobrazem* zbioru $D \subseteq B$ przy przekształceniu f nazywamy zbiór

$$\vec{f}^{\,-1}(D) = \{a \in A \mid f(a) \in D\}.$$

Na przykład niech $f : \mathbb{N} \to \mathbf{P}(\mathbb{N})$ będzie funkcją przyporządkowującą każdej liczbie $n \in \mathbb{N}$ zbiór jej właściwych (różnych od 1 i od n) dzielników pierwszych, przy czym przyjmijmy, że zero nie ma dzielników pierwszych. Wtedy $\vec{f}(\{1, 3, 4, 6, 9\}) = \{\emptyset, \{2\}, \{3\}, \{2, 3\}\}$, a jeśli P oznacza zbiór liczb pierwszych, to $\vec{f}(P) = \{\emptyset\}$. Natomiast $\vec{f}^{\,-1}(\{\{2\}, \{1, 2, 27, 36\}\}) = \{2^k \mid k \in \mathbb{N} - \{0, 1\}\}$.

Uwaga: Oznaczenie $\vec{f}^{\,-1}(A)$ jest w istocie dwuznaczne. Może tu chodzić o przeciwobraz A przy przekształceniu f lub o obraz A przy przekształceniu f^{-1} (jeśli jest określone). Szczęśliwie, w obu wypadkach chodzi o ten sam zbiór (ćwiczenie).

Rodzina indeksowana i produkt uogólniony

O *rodzinie indeksowanej* $\{A_t\}_{t \in T}$ mówimy wtedy, gdy rozważamy pewne obiekty (zbiory) A_t indeksowane elementami zbioru T, a przy tym możliwe są powtórzenia. Chcemy bowiem odróżnić rodzinę indeksowaną od zbioru $\{A_t \mid t \in T\}$. Najprościej jest przyjąć, że rodzina indeksowana to po prostu odpowiednia funkcja.

Definicja 3.8 *Rodziną indeksowaną* $\{A_t\}_{t \in T}$ nazywamy taką funkcję A, że $\mathrm{Dom}(A) = T$ oraz $A(t) = A_t$, dla dowolnego $t \in T$.

Iloczyn kartezjański (produkt) $A \times B$ zdefiniowaliśmy jako zbiór par. Produkt trzech zbiorów można zdefiniować na przykład jako $(A \times B) \times C$. Podobnie dla czterech i więcej zbiorów. Elementami produktu skończonej liczby zbiorów są więc *krotki* odpowiedniej długości. O takich krotkach można myśleć jak o ciągach skończonych. To podsuwa pomysł jak można zdefiniować produkt rodziny zbiorów indeksowanej liczbami naturalnymi: produktem rodziny $\{A_n\}_{n \in \mathbb{N}}$ powinien być zbiór wszystkich ciągów nieskończonych $a_0, a_1, \ldots$ spełniających warunek $a_n \in A_n$ dla dowolnego $n \in \mathbb{N}$. No dobrze, ale co to jest „ciąg nieskończony"? Funkcja o dziedzinie $\mathbb{N}$. Po tej obserwacji poniższa definicja powinna być oczywista.

Definicja 3.9 *Produktem uogólnionym* (lub po prostu „produktem" albo „iloczynem kartezjańskim") rodziny indeksowanej $\{A_t\}_{t\in T}$ nazywamy zbiór

$$\prod_{t\in T} A_t = \{f \in \mathbf{P}(T \times \bigcup_{t\in T} A_t) \mid (f : T \to \bigcup_{t\in T} A_t) \wedge (\forall t \in T(f(t) \in A_t)\}$$

Zapiszmy inaczej to, co najważniejsze w tej definicji:

$$f \in \prod_{t\in T} A_t \quad \Leftrightarrow \quad f \text{ jest funkcją, } \mathrm{Dom}(f) = T \text{ oraz } \forall t \in T(f(t) \in A_t)$$

Pewnik wyboru

Definicja 3.10 Niech X będzie dowolną rodziną zbiorów. Zbiór $S \subseteq \bigcup X$ nazywamy *selektorem* dla rodziny X, jeżeli S ma dokładnie po jednym elemencie wspólnym z każdym zbiorem rodziny X, tj.:

$$\forall a \in X \exists t \in a\, (S \cap a = \{t\}).$$

Funkcja $f : X \to \bigcup X$ jest *funkcją wyboru* dla X, jeśli $f(a) \in a$ dla dowolnego $a \in X$.

Na przykład zbiór $\{1, 3, 4\}$ jest selektorem dla rodziny $\{\{1, 2\}, \{3, 5\}, \{4, 5\}\}$, a rodzina $\{\{1\}, \{2\}, \{1, 2\}\}$ nie ma selektora.

3.11 (Aksjomat wyboru)

Dla dowolnej rodziny niepustych zbiorów parami rozłącznych[3] *istnieje selektor.*

Następujące twierdzenie jest alternatywnym sformułowaniem aksjomatu wyboru.

Twierdzenie 3.12 *Dla dowolnej rodziny X zbiorów niepustych istnieje funkcja wyboru.*

Dowód: Rozpatrzmy funkcję $F : X \to \mathbf{P}(X \times \bigcup X)$, określoną warunkiem $F(a) = \{a\} \times a$, dla $a \in X$. Niech $Y = \mathrm{Rg}(F)$, tj $Y = \{\{a\} \times a \mid a \in X\}$. Ponieważ X jest rodziną zbiorów niepustych, więc także Y jest rodziną zbiorów niepustych. Co więcej, zbiory należące do Y są parami rozłączne. (Jeśli bowiem $t \in (\{a\} \times a) \cap (\{b\} \times b)$ to $t = \langle a, \xi\rangle = \langle b, \nu\rangle$ dla pewnych $\xi \in a \in X$ i $\nu \in b \in X$. Ale wtedy $a = b$ na mocy Lematu 2.2, więc $\{a\} \times a = \{b\} \times b$.)

A zatem rodzina Y ma selektor S. Udowodnimy, że S jest funkcją wyboru dla X. W tym celu sprawdzimy warunki wymienione w Definicji 3.1.

[3]Mówimy, że rodzina R jest *rozłączna* lub jest rodziną zbiorów *parami rozłącznych*, gdy zachodzi warunek $\forall a, b \in R(a \neq b \to a \cap b = \emptyset)$.

Na początek zauważmy, że $S \subseteq X \times \bigcup X$. Istotnie, $S \subseteq \bigcup Y$, jeśli więc $t \in S$ to $t \in \{a\} \times a$, dla pewnego $a \in X$. Wtedy $t = \langle a, \rho \rangle$ dla pewnego $\rho \in a$, a więc $t \in X \times \bigcup X$, bo $\rho \in a \in X$.

Dalej nietrudno stwierdzić, że zachodzi następujący warunek (nieco silniejszy niż (1) w Definicji 3.1):

1) $\forall a \in X \exists \mu \in a\, (\langle a, \mu \rangle \in S)$

Rzeczywiście, jeśli $a \in X$ to $\{a\} \times a \in Y$ więc jest $t \in S \cap (\{a\} \times a)$. Ale wtedy t musi być postaci $\langle a, \mu \rangle$.

Ponadto mamy:

2) $\forall a \in X \forall \sigma, \tau\, (\langle a, \sigma \rangle \in S \wedge \langle a, \tau \rangle \in S \to \sigma = \tau)$,

a to dlatego, że pary $\langle a, \sigma \rangle$ i $\langle a, \tau \rangle$ należące do jednoelementowego zbioru $S \cap (\{a\} \times a)$ muszą być równe.

A zatem nasz selektor jest funkcją z X do $\bigcup X$. Z warunku (1) powyżej wynika, że zawsze $S(a) \in a$, więc S jest funkcją wyboru. ∎

Pewnik wyboru czasami budzi kontrowersje ze względu na niektóre swoje zaskakujące konsekwencje. Ale następujące dwa twierdzenia stanowią przykłady intuicyjnie oczywistych faktów, których dowody wymagają użycia tego aksjomatu.

Twierdzenie 3.13 *Jeśli $\{A_t\}_{t \in T}$ jest rodziną indeksowaną zbiorów niepustych, to produkt $\Pi_{t \in T} A_t$ jest niepusty.*

Dowód: Niech φ będzie funkcją wyboru dla $\{A_t \mid t \in T\}$ i niech $f : T \to \bigcup\{A_t \mid t \in T\}$ będzie określona przez równanie $f(t) = \varphi(A_t)$, dla $t \in T$. Oczywiście $f \in \prod_{t \in T} A_t$. ∎

Twierdzenie 3.14 *Jeśli $A \neq \emptyset$, to następujące warunki są równoważne:*

1) Istnieje funkcja $f : A \xrightarrow{1-1} B$;

2) Istnieje funkcja $g : B \xrightarrow{\text{na}} A$.

Dowód: (1)⇒(2): Skoro $A \neq \emptyset$, to mamy jakiś element $\alpha \in A$. A skoro funkcja f jest różnowartościowa, to istnieje funkcja odwrotna $f^{-1} : \mathrm{Rg}(f) \xrightarrow[\text{na}]{1-1} A$. Możemy więc tak zdefiniować $g(b)$, dla $b \in B$:

$$g(b) = \begin{cases} f^{-1}(b), & \text{jeśli } b \in \mathrm{Rg}(f); \\ \alpha, & \text{w przeciwnym przypadku.} \end{cases}$$

(2)⇒(1): Dla $a \in A$, niech $F_a = g^{-1}(\{a\})$. Zbiory F_a są niepuste, więc produkt $\Pi_{a\in A}F_a$ jest niepusty, czyli istnieje funkcja $f : A \to B$ (zauważmy, że $\bigcup_{a\in A} F_a \subseteq B$). Ta funkcja jest różnowartościowa bo zbiory $g^{-1}(\{a\})$ są rozłączne. ∎

4 Relacje równoważności

Relacja równoważności jest zazwyczaj zadana przez jakieś kryterium klasyfikacji przedmiotów ze względu na pewną cechę. Przedmioty są w relacji jeśli mają tę cechę wspólną, tj. kryterium ich nie rozróżnia. Zwykle prowadzi to do utożsamiania przedmiotów „nierozróżnialnych" i tworzenia pojęć abstrakcyjnych, np. „wektor swobodny", „kierunek". W tym przypadku słowo „abstrakcja" należy rozumieć jako oderwanie od pozostałych cech przedmiotów, które są nieistotne z punktu widzenia naszego kryterium.

Definicja 4.1 Relacja r w zbiorze a jest *relacją równoważności* wtedy i tylko wtedy, gdy jest zwrotna, symetryczna i przechodnia (Definicja 2.5), to jest:

- $\forall x{\in}a\,(x\,r\,x)$;
- $\forall x{\in}a\,\forall y{\in}a\,(x\,r\,y \to y\,r\,x)$;
- $\forall x{\in}a\,\forall y{\in}a\,\forall z{\in}a(x\,r\,y \wedge y\,r\,z \to x\,r\,z)$.

Klasą abstrakcji relacji r wyznaczoną przez element $x \in a$ nazywamy zbiór

$$[x]_r = \{y \in a \mid x\,r\,y\}.$$

Przykładami relacyj równoważności są równoległość prostych, podobieństwo figur geometrycznych, przystawanie wektorów. Skrajne przykłady relacyj równoważności w dowolnym zbiorze a to relacja identycznościowa $\mathrm{id}_a = \{\langle x, x\rangle \mid x \in a\}$ i relacja pełna (totalna) $a \times a$. Szczególnym przykładem jest *jądro* dowolnego przekształcenia $f : a \to b$, czyli relacja $\ker(f)$ zadana przez

$$\langle x, y\rangle \in \ker(f) \quad\Leftrightarrow\quad f(x) = f(y).$$

Fakt 4.2

1) Jeśli $r \subseteq A \times A$ jest relacją równoważności w zbiorze A oraz $x \in A$ to $x \in [x]_r$.

2) Jeśli $r \subseteq A \times A$ jest relacją równoważności w zbiorze A oraz $x, y \in A$ to następujące warunki są równoważne:

a) $x\,r\,y$;

b) $x \in [y]_r$;

c) $y \in [x]_r$;

d) $[x]_r = [y]_r$;

e) $[x]_r \cap [y]_r \neq \emptyset$.

Dowód: Część (1) wynika natychmiast ze zwrotności relacji r. W części (2) równoważność warunków (a), (b) i (c) wynika wprost z tego, że relacja jest symetryczna.

(a)$\Rightarrow$(d) Załóżmy, że $x\,r\,y$ i niech $t \in [x]_r$. Wtedy $x\,r\,t$, więc z przechodniości i symetrii także $y\,r\,t$. A więc pokazaliśmy inkluzję $[x]_r \subseteq [y]_r$. Inkluzji odwrotnej dowodzimy analogicznie.

(d)$\Rightarrow$(e) Skoro $x \in [x]_r = [y]_r$, to $x \in [x]_r \cap [y]_r$.

(e)$\Rightarrow$(a) Jeśli $t \in [x]_r \cap [y]_r$, to $x\,r\,t$ oraz $y\,r\,t$. Z przechodniości i symetrii wynika $x\,r\,y$. ∎

Definicja 4.3 Zbiór wszystkich klas abstrakcji relacji r oznaczamy przez a/r i nazywamy *zbiorem ilorazowym* relacji r.

Fakt 4.4 *Każda relacja równoważności jest jądrem pewnego przekształcenia.*

Dowód: Niech $r \subseteq A \times A$ będzie relacją równoważności w zbiorze A. Rozpatrzmy „naturalną" surjekcję $\kappa : A \to A/r$, określoną tak:

$$\kappa(a) = [a]_r, \text{ dla } a \in A.$$

Wówczas oczywiście $\ker(\kappa) = r$. ∎

Definicja 4.5 *Podziałem* zbioru A nazywamy dowolną rodzinę $P \subseteq \mathbf{P}(A)$, która spełnia warunki:

- $\forall p{\in}P\,(p \neq \emptyset)$;
- $\forall p, q{\in}P\,(p = q \vee p \cap q = \emptyset)$;
- $\bigcup P = A$, czyli $\forall x{\in}A \exists p{\in}P\,(x \in p)$.

Twierdzenie 4.6 (Zasada abstrakcji)

1) Jeżeli r jest relacją równoważności w zbiorze A to A/r jest podziałem zbioru A.

2) Jeżeli P jest podziałem zbioru A, to istnieje taka relacja równoważności r w A, że $P = A/r$.

Dowód: Część (1) wynika łatwo z Faktu 4.2. Dla dowodu części (2), rozpatrzmy dowolny podział P zbioru A i niech r będzie taką relacją:

$$r = \{\langle x, y\rangle \in A \times A \mid \exists p{\in}P\,(x \in p \wedge y \in p)\}$$

Najpierw zauważmy, że r jest relacją równoważności. Zwrotność wynika z warunku $\bigcup P = A$, a symetria wprost z definicji r. Pozostaje przechodniość. Przypuśćmy więc, że $x\,r\,y$ i $y\,r\,z$. Wtedy są takie $p, q \in P$, że $x, y \in p$ oraz $y, z \in q$. Ale wtedy $p \cap q \neq \emptyset$, więc $p = q$. Skoro więc $x \in p$ i $z \in q = p$, to $x\,r\,z$.

Następna obserwacja jest taka:

$$\textit{Jeśli } x \in p \in P \textit{ to } [x]_r = p. \tag{*}$$

Dla dowodu (*) przypuśćmy, że $x \in p \in P$ i niech $t \in [x]_r$. Wtedy $x, t \in q$ dla pewnego $q \in P$. Ale $q = p$ bo $x \in p \wedge q$. Zatem $t \in p$ i wykazaliśmy już, że $[x]_r \subseteq p$. Na odwrót, jeśli $t \in p$, to $t\,r\,x$ (bo $x \in p$) więc $t \in [x]_r$.

Teraz wreszcie pokażemy, że $P = A/r$.

($\subseteq$): Jeśli $p \in P$, to $p \neq \emptyset$, więc jest $x \in p$. Wtedy $p = [x]_r$ na mocy (*), więc $p \in A/r$.

($\supseteq$): Dla dowolnego $x \in a$ istnieje takie $p \in P$, że $x \in p$. Wtedy $[x]_r = p$. A zatem każda klasa $[x]_r \in A/r$ należy do P. ∎

5 Liczby naturalne

Podobno to Leopold Kronecker twierdził, że liczby naturalne stworzył Pan Bóg, a resztę wymyślili ludzie. Mimo że pojęcie liczby naturalnej jest intuicyjnie oczywiste, matematycy od dawna usiłowali nadać mu bardziej precyzyjny charakter. Można to zrobić na dwa sposoby: aksjomatycznie lub poprzez konstrukcję. Z metodą aksjomatyczną najczęściej wiążemy nazwisko Giuseppe Peano. Aksjomaty Peano liczb naturalnych są takie:

- *Zero* jest liczbą naturalną.
- Każda liczba naturalna ma *następnik*, który jest liczbą naturalną.
- Liczby o tych samych następnikach są równe.
- Zero nie jest następnikiem żadnej liczby naturalnej.
- Jeśli zero ma pewną własność W, oraz
  - z tego że jakaś liczba naturalna ma własność W wynika, że jej następnik też ma własność W,

  to każda liczba naturalna ma własność W.

Pomysł na definicję liczb naturalnych, którą teraz podamy, pochodzi od Johna von Neumanna. Liczbę naturalną rozumiemy jako liczbę elementów pewnego zbioru skończonego. A zatem jako definicję np. liczby naturalnej 5 można przyjąć po prostu pewien ustalony, wzorcowy zbiór o pięciu elementach. Oczywiście zero to musi być zbiór pusty. A pozostałe liczby najprościej zdefiniować tak: liczba naturalna to zbiór wszystkich liczb mniejszych od niej. Następnikiem liczby n jest wtedy $n \cup \{n\}$. A więc:

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

Żeby jednak „zalegalizować” istnienie zbioru wszystkich liczb naturalnych potrzebujemy odpowiedniego aksjomatu.

Definicja 5.1 Każdy zbiór N, spełniający warunek

$$\emptyset \in N \land \forall z\, (z \in N \to z \cup \{z\} \in N)$$

nazywamy zbiorem *induktywnym*.

5.2 (Aksjomat nieskończoności) *Istnieje zbiór induktywny.*

Tak sformułowany aksjomat to jeszcze trochę za mało. Zbiorów induktywnych może być wiele i mogą one mieć dodatkowe „niepotrzebne” elementy. Nam jest potrzebny zbiór induktywny, który składa się tylko z zera i tych rzeczy, które można z niego otrzymać przez stosowanie operacji następnika.

Lemat 5.3 *Jeśli $\mathcal{R}$ jest niepustą rodziną zbiorów induktywnych, to $\bigcap \mathcal{R}$ jest zbiorem induktywnym.*

Dowód: Ponieważ $\emptyset \in N$, dla dowolnego $N \in \mathcal{R}$, to $\emptyset \in \bigcap \mathcal{R}$. Przypuśćmy, że $z \in \bigcap \mathcal{R}$. Wtedy $z \in N$, a więc także $z \cup \{z\} \in N$, dla dowolnego $N \in \mathcal{R}$. Stąd $z \cup \{z\} \in \bigcap \mathcal{R}$. ∎

Twierdzenie 5.4 *Istnieje (dokładnie jeden) najmniejszy zbiór induktywny, tj. taki zbiór induktywny $\mathbb{N}$, że $\mathbb{N} \subseteq N$ dla dowolnego zbioru induktywnego N.*

Dowód: Niech M będzie dowolnym zbiorem induktywnym. Połóżmy

$$\mathcal{R} = \{N \in \mathbf{P}(M) \mid N \text{ jest induktywny}\}$$

i niech $\mathbb{N} = \bigcap \mathcal{R}$. Na mocy Lematu 5.3, zbiór $\mathbb{N}$ jest induktywny. Ponadto jest to najmniejszy zbiór induktywny. Rzeczywiście, przypuśćmy, że N jest induktywny. Wtedy iloczyn $N \cap M$ jest induktywny (znowu na mocy Lematu 5.3) i należy do rodziny $\mathcal{R}$. A zatem $N \cap M$ zawiera iloczyn tej rodziny, czyli $\mathbb{N}$.

Na koniec zauważmy jeszcze, że najmniejszy zbiór induktywny może być tylko jeden. Gdyby były dwa, to by się nawzajem zawierały, a więc i tak byłby tylko jeden. ∎

Definicja 5.5 *Elementy zbioru* $\mathbb{N}$*, o którym mowa w Twierdzeniu 5.4 nazywamy liczbami naturalnymi. Funkcję* $s : \mathbb{N} \to \mathbb{N}$*, określoną warunkiem* $s(n) = n \cup \{n\}$ *nazywamy następnikiem.*

Twierdzenie 5.6 (Zasada indukcji)

Jeśli $A \subseteq \mathbb{N}$ *ma takie własności:*

1) $0 \in A$;

2) $\forall n\, (n \in A \to s(n) \in A)$,

to $A = \mathbb{N}$.

Dowód: Wtedy A jest induktywny, zatem $\mathbb{N} \subseteq A$. ∎

Fakt 5.7 *Jeśli* $n \in \mathbb{N}$ *to* $n \subseteq \mathbb{N}$.

Dowód: Skorzystamy z zasady indukcji (udowodnimy, że zbiór $A = \{n \in \mathbb{N} \mid n \subseteq \mathbb{N}\}$ jest induktywny.)

1) Ponieważ $0 \in \mathbb{N}$, oraz $0 = \emptyset \subseteq \mathbb{N}$ więc $0 \in A$.

2) Niech $n \in A$, czyli $n \subseteq \mathbb{N}$ (korzystamy z *założenia indukcyjnego*). Wtedy także $s(n) = n \cup \{n\} \subseteq \mathbb{N}$, bo $n \subseteq \mathbb{N}$ i $\{n\} \subseteq \mathbb{N}$. ∎

Fakt 5.8 *Jeśli* $m \in n \in \mathbb{N}$ *to* $m \subseteq n$.

Dowód: Udowodnimy, że zbiór $A = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N}\, (m \in n \to m \subseteq n)\}$ jest induktywny, tj. wykonamy dowód przez indukcję „ze względu na n".

1) Jeśli $m \in \emptyset$ to „walkowerem" $m \subseteq \emptyset$ więc $0 = \emptyset \in A$.

2) Niech $n \in A$. Przypuśćmy, że $m \in n \cup \{n\}$. Jeśli $m \in n$ to $m \subseteq n$ z założenia indukcyjnego, a jeśli $m \in \{n\}$ to $m = n$, czyli też $m \subseteq n$. ∎

Fakt 5.9 *Jeśli* $m, n \in \mathbb{N}$ *oraz* $s(m) = s(n)$ *to* $m = n$.

Dowód: Załóżmy, że $s(m) = s(n)$, czyli, że $m \cup \{m\} = n \cup \{n\}$. Wtedy $m \in n \cup \{n\}$, więc albo $m \in n$ albo $m = n$. Na mocy Faktu 5.8, w obu przypadkach $m \subseteq n$. Podobnie dowodzimy, że $n \subseteq m$. ∎

Morał: Konstrukcja liczb von Neumanna spełnia aksjomaty Peano, jest więc poprawną „implementacją" pojęcia liczby naturalnej. Istotnie:

- $0 = \emptyset \in \mathbb{N}$, bo $\mathbb{N}$ jest induktywny.
- Jeśli $n \in \mathbb{N}$ to $s(n) = n \cup \{n\} \in \mathbb{N}$, bo $\mathbb{N}$ jest induktywny.
- Zero nie jest następnikiem, bo zbiór $n \cup \{n\}$ jest zawsze niepusty.
- Następnik jest funkcją różnowartościową, na mocy Faktu 5.9.
- Ostatni aksjomat jest spełniony na mocy zasady indukcji 5.6.

Definiowanie przez indukcję

Definicja 5.10 Jeśli $f : A \to B$ i $C \subseteq A$, to *obcięciem* funkcji f do zbioru C nazywamy funkcję $f|_C : C \to B$, określoną warunkiem $f|_C(x) = f(x)$, dla $x \in C$.

Twierdzenie 5.11

1) *Istnieje dokładnie jedna funkcja* $D : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, *spełniająca warunki:*

   a) $D(0, m) = m$;

   b) $D(s(k), m) = s(D(k, m))$,

   dla dowolnych $k, m \in \mathbb{N}$.

2) *Istnieje dokładnie jedna funkcja* $M : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, *spełniająca warunki:*

   a) $M(0, m) = 0$;

   b) $M(s(k), m) = D(M(k, m), m)$.

   dla dowolnych $k, m \in \mathbb{N}$.

Dowód:* (1) Na potrzeby tego dowodu, przyjmijmy, że funkcja $D : A \times \mathbb{N} \to \mathbb{N}$, gdzie $A \subseteq \mathbb{N}$, jest *dobra*, wtedy i tylko wtedy, gdy spełnia warunki (a) i (b) dla dowolnych $m \in \mathbb{N}$ i takich k, że $s(k) \in A$. Najpierw przez indukcję pokażemy, że dla dowolnego $n \in \mathbb{N}$ istnieje dokładnie jedna dobra funkcja $D_n : s(n) \times \mathbb{N} \to \mathbb{N}$.

Oczywiście funkcja D_0 jest jednoznacznie określona warunkiem $D_0(0, m) = m$. Załóżmy więc, że istnieje dobra funkcja $D_n : s(n) \times \mathbb{N} \to \mathbb{N}$. Określamy funkcję $D_{s(n)} : s(s(n)) \times \mathbb{N} \to \mathbb{N}$ w ten sposób:

$$D_{s(n)}(k,m) = \begin{cases} D_n(k,m), & \text{jeśli } k \in s(n); \\ s(D_n(n,m)), & \text{jesli } k = s(n). \end{cases}$$

Ta funkcja jest dobra, co wynika z definicji i z założenia indukcyjnego o funkcji D_n. Przypuśćmy, że istnieje jeszcze inna dobra funkcja $D : s(s(n))\times\mathbb{N} \to \mathbb{N}$. Wtedy funkcja $D|_{s(n)\times\mathbb{N}} : s(n)\times\mathbb{N} \to \mathbb{N}$ też musi być dobra. Z założenia indukcyjnego funkcje D_n i $D|_{s(n)\times\mathbb{N}}$ są równe, a stąd $D_{s(n)}(k,m) = D_n(k,m) = D|_{s(n)\times\mathbb{N}}(k,m)$ dla wszystkich $k \in s(n)$. Ponadto $D_{s(n)}(s(n),m) = s(D_n(n,m)) = s(D|_{s(n)\times\mathbb{N}}(n,m)) = D(s(n),m))$, więc funkcje $D_{s(n)}$ i D są identyczne.

Określimy teraz funkcję $D : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ warunkiem

$$D(k,m) = D_k(k,m).$$

Sprawdźmy, że ta funkcja jest dobra. Po pierwsze $D(0,m) = D_0(0,m) = m$, po drugie $D(s(k),m) = D_{s(k)}(s(k),m) = s(D_k(k,m)) = s(D(k,m))$. Gdyby istniała inna dobra funkcja $D' : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, to każda z funkcji $D'|_{s(n)\times\mathbb{N}} : s(n) \times \mathbb{N} \to \mathbb{N}$ byłaby dobra, a zatem identyczna z D_n. Stąd, dla każdego n, mielibyśmy $D'(n) = (D'|_{s(n)\times\mathbb{N}})(n) = D_n(n) = D(n)$.

(2) Dowód tej części jest bardzo podobny do powyższego. ∎

Definicja 5.12 Funkcje D i M, o których mowa w Twierdzeniu 5.11, nazywamy odpowiednio *dodawaniem* i *mnożeniem* liczb naturalnych. Zamiast $D(k,m)$ piszemy $k+m$, a zamiast $M(k,m)$ piszemy $k \cdot m$ lub km.

Przykład 5.13 $2 \cdot 2 = 1 \cdot 2 + 2 = (0 \cdot 2 + 2) + 2 = (0 + 2) + 2 = 2 + 2 = s(1 + 2) = s(s(0 + 2)) = s(s(2)) = s(s(s(s(0)))) = 4$.

Dodawanie i mnożenie są przykładami funkcji, które można zdefiniować za pomocą tzw. *rekursji prostej*. Ogólny schemat rekursji prostej wygląda tak:

$$\begin{aligned} f(0,n_1,\ldots,n_k) &= g(n_1,\ldots,n_k); \\ f(s(m),n_1,\ldots,n_k) &= h(m,n_1,\ldots,n_k,f(m,n_1,\ldots,n_k)). \end{aligned}$$

Tutaj definiujemy funkcję f przez indukcję ze względu na pierwszy argument, z pomocą już określonych funkcji g i h. Bardziej ogólny schemat definicji indukcyjnej jest taki (dla uproszczenia ograniczmy się do funkcji dwuargumentowej):

$$f(m,n) = h(m,n,f|_{m\times\mathbb{N}}),$$

gdzie $h : \mathbb{N} \times \mathbb{N} \times \mathbf{P}((\mathbb{N} \times \mathbb{N}) \times \mathbb{N})) \to \mathbb{N}$. Chodzi tu o to, że dla określenia $f(m,n)$ można korzystać ze wszystkich wartości $f(k,r)$, gdzie $k \in m$ i $r \in \mathbb{N}$.

Definicja 5.14 Relację (nieostrej) nierówności pomiędzy liczbami naturalnymi definiujemy za pomocą dodawania:

$$m \leq n \quad \text{wtedy i tylko wtedy, gdy} \quad \exists k(m + k = n).$$

Nierówność ostra jest pojęciem wtórnym w stosunku do relacji $\leq$:

$$m < n \quad \text{wtedy i tylko wtedy, gdy} \quad m \leq n \text{ ale } m \neq n.$$

Następujący lemat będzie nam potrzebny do opisania pewnych własności relacji $\leq$.

Lemat 5.15 *Dla dowolnych liczb $m, k, l \in \mathbb{N}$:*

a) $m + (k + l) = (m + k) + l$*;*

b) Jeśli $m + k = m$ *to* $k = 0$*;*

c) Jeśli $k + l = 0$ *to* $k = 0$*;*

d) $m + 0 = m$*;*

e) $s(m) + k = m + s(k)$*;*

f) $m + k = k + m$*.*

Dowód: (a) Indukcja ze względu na m. Po pierwsze $0 + (k + l) = (k + l) = ((0 + k) + l)$, po drugie z warunku $m + (k + l) = (m + k) + l$ wynika $s(m) + (k + l) = s(m + (k + l)) = s((m + k) + l) = s(m + k) + l = (s(m) + k) + l$.

(b) Indukcja ze względu na m. Po pierwsze $0 + k = k$, a więc warunek $0 + k = 0$ oznacza, że $k = 0$. Po drugie równość $s(m) + k = s(m)$ implikuje $s(m + k) = s(m)$ (bo $s(m) + k = s(m + k)$). Zatem $m + k = m$, a więc $k = 0$ z założenia indukcyjnego.

(c) Gdyby $k + l = 0$ i $k \neq 0$, to $k = s(k')$, dla pewnego k'. Zatem $0 = k + l = s(k') + l = s(k' + l) \neq 0$, sprzeczność.

(d) Indukcja ze względu na m. Po pierwsze $0 + 0 = 0$ z definicji, po drugie $s(m) + 0 = s(m + 0) = s(m)$, wprost z założenia indukcyjnego.

(e) Indukcja ze względu na m. Po pierwsze $s(0)+k = s(0+k) = s(k) = 0+s(k)$. Po drugie, z równości $s(m)+k = m+s(k)$ wynika $s(s(m))+k = s(s(m)+k) = s(m+s(k)) = s(m)+s(k)$.

(f) Indukcja ze względu na m. Dla $m = 0$ wynika natychmiast z częsci (d). Krok indukcyjny wynika z częsci (e): $s(m) + k = s(m + k) = s(k + m) = s(k) + m = k + s(m)$. ∎

Lemat 5.16 *Następujące warunki są równoważne dla dowolnych $m, n \in \mathbb{N}$:*

a) $m < n$*;*

b) $\exists k(m + k = n \wedge k \neq 0)$*;*

c) $s(m) \leq n$*;*

d) $m \in n$.

Dowód: (a)$\Rightarrow$(b) Mamy $m + k = n$ ale $m \neq n$. Zatem $k \neq 0$ na mocy Lematu 5.15(d).

(b)$\Rightarrow$(c) Skoro $m + k = n$ i $k \neq 0$ to $n = m + s(k') = s(m) + k'$ dla pewnego k'. Użyliśmy Lematu 5.15(e).

(c)$\Rightarrow$(d) Przez indukcję ze względu na k pokażemy, że dla dowolnych m i n, warunek $n = s(m) + k$ implikuje $m \in n$. Jeśli $k = 0$ to $n = s(m) = m \cup \{m\}$, więc $m \in n$. Niech więc $n = s(m) + s(k)$. Wtedy $n = s(s(m) + k) = (s(m) + k) \cup \{s(m) + k\}$. Z założenia indukcyjnego $m \in s(m) + k \subseteq n$.

(d)$\Rightarrow$(a) Indukcja ze względu na n. Jeśli $n = 0$ to warunek $m \in n$ nigdy nie zachodzi, możemy więc śmiało twierdzić, że *każdy* element zera spełnia warunek $m < 0$. Niech więc $m < n$ dla wszystkich $m \in n$ i przypuśćmy, że $m \in s(n) = n \cup \{n\}$. Jeśli $m \in n$ to z założenia indukcyjnego mamy $m < n$, skąd $m + k = n$, dla pewnego k. Z Lematu 5.15(e) wynika, że wtedy $m + s(k) = s(m) + k = s(m + k) = s(n)$, a więc $m < s(n)$ na mocy części (b) tego lematu. Jeśli zaś $m = n$ to $m < s(n)$ bo $s(n) = s(0 + n) = s(0) + n = n + s(0) = n + 1$. Użyliśmy znowu Lematu 5.15(e). ∎

Twierdzenie 5.17 *Relacja $\leq$ jest zwrotna, przechodnia, antysymetryczna i spójna.*[4]

Dowód: Zwrotność wynika wprost z Lematu 5.15(d).

Przechodniość: przypuśćmy, że $m \leq n$ i $n \leq p$. Wtedy $m + k = n$ i $n + l = p$ dla pewnych k, l. Zatem $m + (k + l) = (m + k) + l = n + l = p$, na mocy Lematu 5.15(a), więc $m \leq p$.

Antysymetria: przypuśćmy, że $m \leq n$ i $n \leq m$. Wtedy $m + k = n$ i $n + l = m$ dla pewnych k, l. Zatem $m + (k + l) = (m + k) + l = n + l = m$. Zatem $k + l = 0$ i dalej $k = 0$ (Lemat 5.15(b,c)). Stąd $m = m + 0 = n$, na mocy Lematu 5.15(d).

Spójność: przez indukcję pokażemy, że każde $n \in \mathbb{N}$ spełnia warunek:

$$\forall m \in \mathbb{N}(m \leq n \vee n \leq m)$$

Dla $n = 0$ mamy zawsze $n \leq m$, bo $m = 0 + m$. Załóżmy więc, że $\forall m \in \mathbb{N}(m \leq n \vee n \leq m)$ i pokażmy, że wtedy także $\forall m \in \mathbb{N}(m \leq s(n) \vee s(n) \leq m)$. Niech $m \in \mathbb{N}$. Jeśli $m \leq n$, czyli $m + k = n$, dla pewnego k, to $m + s(k) = s(m) + k = s(m + k) = s(n)$, na mocy Lematu 5.15(e). W przeciwnym razie mamy $n \leq m$, a w istocie $n < m$ bo przypadek $n = m$ już jest rozpatrzony. Nierówność $s(n) \leq m$ wynika wtedy z Lematu 5.16. ∎

Twierdzenie 5.18 (Zasada minimum) *Każdy niepusty podzbiór A zbioru $\mathbb{N}$ ma element najmniejszy, tj. taki element $a \in A$, że $\forall b\,(b \in A \to a \leq b)$.*

[4] Relację o takich własnościach nazywamy relacją *liniowego porządku.*

Dowód: Przypuśćmy, że $A \subseteq \mathbb{N}$ nie ma najmniejszego elementu. Niech

$$B = \{n \in \mathbb{N} \mid \forall k(k \in A \to n < k)\}.$$

Pokażemy, że B jest induktywny. Stąd wyniknie, że $B = \mathbb{N}$, a zatem $A = \emptyset$.

Najpierw zauważmy, że $0 \notin A$. W przeciwnym razie 0 byłoby oczywiście najmniejszym elementem (zawsze $0 \leq m$ bo $0 + m = m$). A więc $0 \in B$ bo $\forall k(k \in A \to 0 < k)$.

Załóżmy, że $n \in B$. Skoro $\forall k(k \in A \to n < k)$ to $\forall k(k \in A \to s(n) \leq k)$, na mocy Lematu 5.16. Gdyby więc $s(n) \in A$ to $s(n)$ byłoby najmniejszym elementem A. No to $s(n) \notin A$ i warunek można wzmocnić: $\forall k(k \in A \to s(n) < k)$. ∎

Wniosek 5.19 (Zasada indukcji) *Jeśli $B \subseteq \mathbb{N}$, oraz $\forall n \in \mathbb{N}(n \subseteq B \to n \in B)$, to $B = \mathbb{N}$.*

Dowód: Niech $A = \mathbb{N} - B$. Jeśli $B \neq \mathbb{N}$ to $A \neq \emptyset$, ma więc element najmniejszy n. Wtedy $n \subseteq B$ ale $n \notin B$, co jest sprzeczne z założeniem. ∎

Inne sformułowanie powyższej zasady jest takie: Aby udowodnić, że każda liczba naturalna spełnia pewien warunek (należy do pewnego zbioru B), wystarczy stwierdzić taką prawidłowość: *jeśli wszystkie liczby mniejsze od pewnego n należą do B, to także $n \in B$.*

Konstrukcja liczb całkowitych

Rozpatrzmy następującą relację w zbiorze $\mathbb{N} \times \mathbb{N}$:

$$\langle m, n\rangle \sim \langle m', n'\rangle \quad \text{wtedy i tylko wtedy, gdy} \quad m + n' = m' + n.$$

Nietrudno zauważyć, że to jest relacja równoważności. Klasy abstrakcji relacji $\sim$ nazwiemy *liczbami całkowitymi.* Zbiorem wszystkich liczb całkowitych jest więc $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/_\sim$. Działania na liczbach całkowitych określamy tak:

$$\begin{aligned} [\langle m, n\rangle]_\sim + [\langle m_1, n_1\rangle]_\sim &= [\langle m + m_1, n + n_1\rangle]_\sim \\ [\langle m, n\rangle]_\sim \cdot [\langle m_1, n_1\rangle]_\sim &= [\langle mm_1 + nn_1, mn_1 + nm_1\rangle]_\sim; \\ -[\langle m, n\rangle]_\sim &= [\langle n, m\rangle]_\sim \end{aligned}$$

Uwaga: Te definicje są poprawne, bo jeśli $\langle m, n\rangle \sim \langle m', n'\rangle$ i $\langle m_1, n_1\rangle \sim \langle m_1', n_1'\rangle$, to:

- $\langle m + m_1, n + n_1\rangle \sim \langle m' + m_1', n' + n_1'\rangle$;
- $\langle mm_1 + nn_1, mn_1 + nm_1\rangle \sim \langle m'm_1' + n'n_1', m'n_1' + n'm_1'\rangle$;
- $\langle n, m\rangle \sim \langle n', m'\rangle$.

Zbiór wszystkich liczb całkowitych nie zawiera w sobie zbioru wszystkich liczb naturalnych. Ale możemy się umówić, że tak jest. Mamy bowiem *włożenie* $i : \mathbb{N} \xrightarrow{1-1} \mathbb{Z}$ określone warunkiem

$$i(n) = [\langle n, 0 \rangle]_{\sim}$$

i z dużym powodzeniem możemy utożsamiać każdą liczbę naturalną n z liczbą całkowitą $i(n)$. Zauważmy na przykład, że $i(m+n) = i(m) + i(n)$ oraz $i(m \cdot n) = i(m) \cdot i(n)$, a więc arytmetykę liczb naturalnych (a o nią tu przecież chodzi) możemy uprawiać bez przeszkód w zbiorze $\mathrm{Rg}(i) \subseteq \mathbb{Z}$.

6 Równoliczność

Definicja 6.1 Mówimy, że zbiory A i B są równoliczne (i piszemy $A \sim B$) wtedy i tylko wtedy, gdy istnieje bijekcja $f : A \xrightarrow[\text{na}]{1-1} B$.

Powyższa definicja opiera się na tym samym pomyśle, którego używają dzieci nie znające arytmetyki do podzielenia się po równo kasztanami, jabłkami itp. Wystarczy dawać każdemu po jednym, aż do wyczerpania zasobów.

Przykład 6.2

- Przedziały otwarte (a, b) i (c, d) są równoliczne bo funkcja $f : (a, b) \xrightarrow[\text{na}]{1-1} (c, d)$ może być określona wzorem $f(x) = \frac{d-c}{b-a} \cdot x + \frac{bc-ad}{b-a}$.
- Przedział $(-\frac{\pi}{2}, \frac{\pi}{2})$ (a zatem także każdy inny przedział otwarty) jest równoliczny ze zbiorem $\mathbb{R}$ wszystkich liczb rzeczywistych. Dla dowodu wystarczy użyć funkcji tangens.
- Przedziały $(0, 1]$ i $(0, 1)$ są równoliczne, bo mamy taką funkcję $f : (0, 1] \xrightarrow[\text{na}]{1-1} (0, 1)$:

$$f(x) = \begin{cases} \frac{1}{n+1}, & \text{jeśli } x = \frac{1}{n}, \text{ dla pewnego } n \in \mathbb{N}; \\ x, & \text{w przeciwnym przypadku.} \end{cases}$$

- Zbiór $\mathbb{R}$ jest równoliczny ze zbiorem wszystkich liczb rzeczywistych dodatnich, a równoliczność ustala np. funkcja logarytm.

Fakt 6.3 *Dla dowolnych zbiorów A, B, C,*

- *$A \sim A$;*

- *Jeśli* $A \sim B$ *to* $B \sim A$*;*
- *Jeśli* $A \sim B$ *i* $B \sim C$ *to* $A \sim C$*.*

Uwaga: Równoliczność zbiorów nie jest relacją, z tych samych powodów, dla których relacjami nie są równość ani inkluzja (por. odp. uwagę w treści Wykładu 2). Ale równoliczność ograniczoną do elementów ustalonej rodziny zbiorów można oczywiście utożsamiać z odpowiednią relacją równoważności w tej rodzinie.

Zbiory skończone

Definicja 6.4 Zbiór A nazywamy *skończonym*, gdy $A \sim n$, dla pewnej liczby naturalnej n. W przeciwnym razie zbiór A jest *nieskończony*.

Lemat 6.5 *Niech* $a \notin A$ *i* $b \notin B$*. Wówczas:*

- $A \cup \{a\} \sim B \cup \{b\}$ *wtedy i tylko wtedy, gdy* $A \sim B$*.*
- *Injekcja* $f : A \cup \{a\} \xrightarrow{1-1} B \cup \{b\}$ *istnieje wtedy i tylko wtedy, gdy istnieje injekcja* $f : A \xrightarrow{1-1} B$*.*

Dowód: Jeśli $f : A \xrightarrow{1-1} B$, to wtedy $g = f \cup \{\langle a, b\rangle\}$ jest injekcją z $A \cup \{a\}$ do $B \cup \{b\}$. Jeśli na dodatek funkcja f była na B, to także g jest „na”. To dowodzi implikacji ($\Leftarrow$) w obu częściach lematu. Przypuśćmy więc, że $f : A \cup \{a\} \xrightarrow{1-1} B \cup \{b\}$. Określimy funkcję $h : A \to B$ definicją warunkową:

$$h(x) = \begin{cases} f(a), & \text{jeśli } f(x) = b; \\ f(x), & \text{w przeciwnym przypadku.} \end{cases}$$

Nietrudno zauważyć, że h jest funkcją różnowartościową, a jeśli f jest „na” to także h jest „na”. ∎

Lemat 6.6 *Dla dowolnych* $n, m \in \mathbb{N}$*:*

1) *Nie istnieje* $f : s(n) \xrightarrow{1-1} n$*.*
2) *Nie istnieje* $f : n \xrightarrow{\text{na}} s(n)$*.*
3) *Jeśli* $m \sim n$ *to* $m = n$*.*

Dowód: (1) Indukcja. Oczywiste dla $n = 0$. Krok indukcyjny wynika natychmiast z Lematu 6.5.

(2) Ta część łatwo wynika z poprzedniej i z Twierdzenia 3.14. Ale można ją też udowodnić bezpośrednio (bez pomocy pewnika wyboru) co zalecane jest jako ćwiczenie.

(3) Przez indukcję ze względu na n, dowodzimy własności

$$\forall m \in \mathbb{N}(m \sim n \to m = n) \qquad (*)$$

Warunek jest oczywisty dla $n = 0$, bo tylko zbiór pusty jest równoliczny ze zbiorem pustym. Załóżmy więc, że zachodzi (*) i niech $m \sim s(n)$, czyli $m \sim n \cup \{n\}$. Wtedy na pewno $m \neq 0$, więc $m = s(m') = m' \cup \{m'\}$, dla pewnego m'. Z Lematu 6.5 wynika, że $m' \sim n$ a więc $m' = n$. W konsekwencji $m = s(n)$. ∎

Jeśli $n \in \mathbb{N}$ to piszemy $\overline{\overline{A}} = n$ gdy $A \sim n$. Poprawność tego oznaczenia wynika z Lematu 6.6. Oczywiście mówimy wtedy, że A ma n elementów. Z tego samego lematu wynika też następujący użyteczny fakt:

Twierdzenie 6.7 *Jeśli A jest zbiorem skończonym, oraz $f : A \to A$ to f jest różnowartościowa wtedy i tylko wtedy, gdy jest na A.*

Dowód: ($\Rightarrow$) Przypuśćmy, że f jest różnowartościowa, ale nie jest „na", tj. istnieje $a \in A - \mathrm{Rg}(f)$. To w szczególności oznacza, że $A \neq \emptyset$. Wiemy, że A jest skończony, czyli równoliczny z pewną liczbą naturalną. Skoro $A \neq \emptyset$, to ta liczba nie jest zerem, ma więc postać $s(n)$, dla pewnego n. Przedstawiając zbiór A w postaci sumy $A = (A - \{a\}) \cup \{a\}$ i korzystając z Lematu 6.5, otrzymujemy równoliczność $A - \{a\} \sim n$. Istnieją więc funkcje $h : n \xrightarrow[\text{na}]{1-1} A - \{a\}$ oraz $g : s(n) \xrightarrow[\text{na}]{1-1} A$. Zatem $h^{-1} \circ f \circ g : s(n) \xrightarrow{1-1} n$, co jest sprzeczne z Lematem 6.6(1).

($\Leftarrow$) Przypuśćmy, że $f : A \xrightarrow{\text{na}} A$ nie jest różnowartościowa. Wtedy są takie $a, b \in A$, że $f(a) = f(b)$. Zbiór A musi być niepusty i możemy powtórzyć rozumowanie z poprzedniej części dowodu, wnioskując o istnieniu funkcyj $h : n \xrightarrow[\text{na}]{1-1} A - \{a\}$ i $g : s(n) \xrightarrow[\text{na}]{1-1} A$. Otrzymujemy $g^{-1} \circ (f|_{A-\{a\}}) \circ h : n \xrightarrow{\text{na}} s(n)$. Możemy się teraz powołać na Lemat 6.6(2) i otrzymać sprzeczność. ∎

Następujące twierdzenie zbiera kilka ważnych własności zbiorów skończonych.

Fakt 6.8

0) Jeśli A jest skończony, to $A \cup \{a\}$ jest skończony.

1) Każdy podzbiór zbioru skończonego jest skończony.

2) Jeśli A jest nieskończony i B jest skończony, to $A - B \neq \emptyset$.

3) Jeśli A jest skończony i $f : A \xrightarrow{\text{na}} B$, to B jest skończony.

4) Suma i iloczyn kartezjański dwóch zbiorów skończonych są skończone.

Dowód: (0) Jeśli $\overline{\overline{A}} = n$ oraz $a \notin A$ to $\overline{\overline{A \cup \{a\}}} = s(n)$.

(1) Na początek udowodnimy, że każdy podzbiór dowolnej liczby naturalnej jest skończony. Zrobimy to przez indukcję. Oczywiście każdy podzbiór zbioru pustego jest pusty, więc warunek jest spełniony przez liczbę zero. Załóżmy, że każdy podzbiór liczby n jest skończony i niech $B \subseteq s(n) = n \cup \{n\}$. Jeśli $B \subseteq n$ to dobrze. W przeciwnym razie $n \in B$ i możemy napisać $B = (B - \{n\}) \cup \{n\}$. Zbiór $B - \{n\}$ jest skończony na mocy założenia indukcyjnego, a z części (0) wynika, że B też jest skończony.

Jeśli teraz $B \subseteq A$ i A jest skończony, to mamy bijekcję $f : A \xrightarrow[\text{na}]{1-1} n$, dla pewnego $n \in \mathbb{N}$. Zbiór B jest więc równoliczny z podzbiorem $\vec{f}(B)$ liczby n. Skoro ten jest skończony, to B też jest skończony.

(2) W przeciwnym razie $A \subseteq B$ i A byłby skończony na mocy części (1).

(3) Z Twierdzenia 3.14 wynika, że istnieje wtedy funkcja $g : B \xrightarrow{1-1} A$, a więc B jest równoliczny ze zbiorem $\mathrm{Rg}(g) \subseteq A$, który musi być skończony, jako podzbiór zbioru skończonego.[5]

(4) Ćwiczenie. Wskazówka: przez indukcję należy wykazać, że suma dwóch *rozłącznych* zbiorów, które mają n i m elementów, jest zbiorem o $n + m$ elementach. Podobnie dla iloczynu kartezjańskiego i mnożenia. ∎

Moce zbiorów

Twierdzenie 6.1 *Każdemu zbiorowi A można przypisać pewien obiekt $\overline{\overline{A}}$, zwany* mocą *lub* liczbą kardynalną *zbioru A, i można to zrobić w taki sposób, że*

$$\forall AB\,(A \sim B \Leftrightarrow \overline{\overline{A}} = \overline{\overline{B}}).$$

W szczególności, jeśli zbiór A jest skończony, to jego liczbą kardynalną jest ta liczba naturalna, z którą zbiór A jest równoliczny.

[5] Tę część można też udowodnić bez pomocy Twierdzenia 3.14. Wskazówka: zacząć od przypadku $A \in \mathbb{N}$.

Dowód: Dowód tego twierdzenia pomijamy.[6] W istocie, liczba kardynalna $\overline{\overline{A}}$ jest zawsze pewnym zbiorem równolicznym z A. Liczby naturalne są szczególnym przypadkiem liczb kardynalnych, a poprawność tego wyboru wynika z Lematu 6.6(3). ∎

7 Zbiory przeliczalne

Fakt 7.1 *Jeśli $n \in \mathbb{N}$ to nie istnieje funkcja $f : \mathbb{N} \xrightarrow{1-1} n$. W szczególności zbiór liczb naturalnych $\mathbb{N}$ jest nieskończony.*

Dowód: Gdyby taka funkcja istniała, to $f|_{s(n)} : s(n) \xrightarrow{1-1} n$, a to być nie może z powodu Lematu 6.6(1). ∎

Definicja 7.2 Liczbę kardynalną zbioru $\mathbb{N}$ oznaczamy symbolem $\aleph_0$ („alef zero"). Mówimy, że zbiór A jest *przeliczalny* wtedy i tylko wtedy, gdy jest skończony lub jest zbiorem mocy $\aleph_0$. W przeciwnym razie zbiór A jest *nieprzeliczalny*.

Moc $\aleph_0$ jest najmniejszą mocą nieskończoną, w następującym sensie:

Twierdzenie 7.3 *Zbiór A jest nieskończony wtedy i tylko wtedy, gdy ma podzbiór mocy $\aleph_0$.*

Dowód: ($\Rightarrow$) Niech ϑ będzie funkcją wyboru dla rodziny $\mathbf{P}(A) - \{\emptyset\}$. Określimy funkcję $f : \mathbb{N} \to A$, za pomocą takiej definicji indukcyjnej:

$$f(n) = \vartheta(A - \vec{f}(n)) \qquad (*)$$

Poprawność tej definicji nie jest oczywista i wymaga takiej obserwacji: Skoro n jest zbiorem skończonym, to $\vec{f}(n)$ też jest skończone (na mocy Faktu 6.8(3)) a zatem zbiór $A - \vec{f}(n)$ jest niepusty (na mocy Faktu 6.8(2)) i dlatego prawa strona równania ma sens. Istnienie dokładnie jednej funkcji spełniającej równanie (*) można teraz udowodnić metodami podobnymi do użytych w dowodzie Twierdzenia 5.11.

Zauważmy, że funkcja f jest różnowartościowa. W rzeczy samej, jeśli $m \neq n$, to na przykład $m \in n$. Wtedy $f(m) \in \vec{f}(n)$, a więc wartość $f(n)$, wybierana z dopełnienia zbioru $\vec{f}(n)$, musi być różna od $f(m)$. Zatem $f : \mathbb{N} \xrightarrow[\text{na}]{1-1} \mathrm{Rg}(f)$. Zbiór $\mathrm{Rg}(f)$ ma więc moc $\aleph_0$ i jest podzbiorem A.

[6] Uwaga dla dociekliwych: Konstrukcja liczb kardynalnych wymaga dodatkowego (schematu) aksjomatu, zwanego *aksjomatem zastępowania*.

($\Leftarrow$) Jeżeli $\mathbb{N} \sim B \subseteq A$ i $\overline{\overline{A}} = n \in \mathbb{N}$, to istnieją funkcje $f : \mathbb{N} \xrightarrow[\text{na}]{1-1} B$ i $g : A \xrightarrow[\text{na}]{1-1} n$. Stąd $g \circ f : \mathbb{N} \xrightarrow{1-1} n$, co jest sprzeczne z Faktem 7.1. ∎

Wniosek 7.4 *Zbiór jest nieskończony wtedy i tylko wtedy, gdy jest równoliczny z pewnym swoim podzbiorem właściwym.*

Dowód: ($\Leftarrow$) Ta część wynika wprost z Twierdzenia 6.7.

($\Rightarrow$) Skorzystamy z poprzedniego twierdzenia. Jeśli zbiór A jest nieskończony to ma podzbiór B o mocy $\aleph_0$. Mamy więc funkcję $f : \mathbb{N} \xrightarrow[\text{na}]{1-1} B$ i możemy określić $g : A \to A$ warunkiem

$$g(x) = \begin{cases} f(f^{-1}(x)+1), & \text{jeśli } x \in B; \\ x, & \text{w przeciwnym przypadku.} \end{cases}$$

Łatwo zauważyć, że funkcja g jest różnowartościowa. Ale ta funkcja nie jest na A bo element $f(0)$ nie należy do $\mathrm{Rg}(g)$. Zatem $A \sim \mathrm{Rg}(g) \subsetneq A$. ∎

Dla $B \subseteq \mathbb{N}$, przez $\min B$ oznaczymy najmniejszy element zbioru B. Taki element zawsze istnieje, jeśli tylko B jest niepusty. (Twierdzenie 5.18.)

Fakt 7.5 *Każdy podzbiór zbioru przeliczalnego jest przeliczalny.*

Dowód: Niech C będzie podzbiorem zbioru przeliczalnego B. Jeśli C jest skończony, to dobrze, więc niech C będzie nieskończony. Wtedy zbiór B też musi być nieskończony, a skoro B jest przeliczalny, to mamy funkcję $g : B \xrightarrow[\text{na}]{1-1} \mathbb{N}$. Zbiór C jest więc równoliczny z podzbiorem $\vec{g}(C)$ zbioru $\mathbb{N}$. A zatem wystarczy udowodnić, że każdy nieskończony podzbiór zbioru $\mathbb{N}$ jest przeliczalny.

Niech A będzie takim podzbiorem. Definiujemy przez indukcję funkcję $f : \mathbb{N} \to A$:

$$f(n) = \min(A - \vec{f}(n)) \qquad (*)$$

Ta definicja jest poprawna, a funkcja f jest różnowartościowa, z powodów podobnych do omawianych w dowodzie Twierdzenia 7.3. Pozostaje stwierdzić, że f jest na A. Przypuśćmy, że nie, tj. że istnieje jakieś $m \in A - \mathrm{Rg}(f)$. Wtedy dla dowolnego n mamy jednocześnie $m \in A - \vec{f}(n)$ i $m \neq f(n)$, a więc $m > f(n)$. Stąd $\mathrm{Rg}(f) \subseteq m$ czyli $\mathrm{Rg}(f)$ jest zbiorem skończonym. To niemożliwe, bo f jest różnowartościowa, więc $\mathrm{Rg}(f) \sim \mathbb{N}$. ∎

Następujący fakt uzasadnia nazwę „zbiór przeliczalny”. Zbiór jest przeliczalny, gdy jego elementy można *przeliczać* (niekoniecznie *przeliczyć*), tj. ustawić je w ciąg nieskończony.

Wniosek 7.6 *Niepusty zbiór A jest przeliczalny wtedy i tylko wtedy, gdy istnieje surjekcja $f : \mathbb{N} \xrightarrow{\text{na}} A$.*

Dowód: ($\Rightarrow$) Jeśli $\overline{\overline{A}} = \aleph_0$ to taka funkcja istnieje z definicji i nawet jest różnowartościowa. Jeśli $\overline{\overline{A}} = n \in \mathbb{N}$, to $n \neq 0$ i mamy funkcję $g : n \xrightarrow[\text{na}]{1-1} A$, którą można poprawić tak:

$$h(m) = \begin{cases} g(m), & \text{jeśli } m \in n; \\ g(0), & \text{w przeciwnym przypadku.} \end{cases}$$

($\Leftarrow$) Niech $f : \mathbb{N} \xrightarrow{\text{na}} A$. Wtedy funkcja $g : A \xrightarrow{1-1} \mathbb{N}$ może być określona tak: $g(a) = \min\{i \in \mathbb{N} \mid f(i) = a\}$. Zbiór A jest więc równoliczny z podzbiorem $\mathrm{Rg}(g)$ zbioru $\mathbb{N}$, a zatem przeliczalny. ∎

Lemat 7.7 *Jeśli zbiór A jest przeliczalny i $f : A \xrightarrow{\text{na}} B$, to B jest przeliczalny.*

Dowód: Na mocy Wniosku 7.6 istnieje surjekcja $g : \mathbb{N} \xrightarrow{\text{na}} A$. Wtedy $f \circ g : \mathbb{N} \xrightarrow{\text{na}} B$, więc na mocy tego samego wniosku zbiór B jest przeliczalny. ∎

Fakt 7.8 *Jeśli zbiory A i B są przeliczalne to $A \cup B$ i $A \times B$ też są przeliczalne.*

Dowód: Jeśli któryś ze zbiorów A i B jest pusty to teza jest oczywista. Załóżmy więc, że A i B są niepuste. Na mocy Wniosku 7.6 istnieją więc funkcje $f : \mathbb{N} \xrightarrow{\text{na}} A$ i $g : \mathbb{N} \xrightarrow{\text{na}} B$. Możemy teraz określić funkcję $\varphi : \mathbb{N} \xrightarrow{\text{na}} A \cup B$ wzorem

$$\varphi(n) = \begin{cases} f(k), & \text{jeśli } n = 2k, \text{ dla pewnego } k; \\ g(k), & \text{jeśli } n = 2k+1, \text{ dla pewnego } k \end{cases}$$

A zatem $A \cup B$ jest zbiorem przeliczalnym, co też wynika z Wniosku 7.6. Aby określić funkcję $\psi : \mathbb{N} \xrightarrow{\text{na}} A \times B$, skorzystamy z jednoznaczności rozkładu liczb naturalnych na czynniki pierwsze.[7] Każdą liczbę $n \neq 0$ możemy jednoznacznie zapisać w postaci

$$n = 2^i 3^j q,$$

gdzie q nie jest podzielne ani przez 2 ani przez 3. Przyjmujemy

$$\psi(n) = \begin{cases} \langle f(0), g(0) \rangle, & \text{jeśli } n = 0; \\ \langle f(i), g(j) \rangle, & \text{jeśli } n = 2^i 3^j q \text{ oraz } q \text{ nie dzieli się przez 2 ani 3} \end{cases}$$

Funkcja ψ jest „na", bo dla dowolnych $a \in A$, $b \in B$ istnieją takie liczby i, j, że $f(i) = a$ i $f(j) = b$. A więc $\langle a, b \rangle = \psi(2^j 3^j)$. ∎

[7] Przedmiotem tego wykładu jest teoria mnogości. Dlatego interesuje nas to, jak można na gruncie tej teorii zdefiniować liczby naturalne. Ale własności arytmetyczne liczb naturalnych, które wynikają z aksjomatów Peano (takie jak przywołana tu jednoznaczność rozkładu), już przecież znamy.

Przykład 7.9 Funkcja $t : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ dana wzorem $f(n,m) = 2^n 3^m$ jest różnowartościowa. Natomiast następujące funkcje $u, v : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ są nawet bijekcjami.[8]

$$u(m,n) = 2^m(2n+1) - 1$$

$$v(m,n) = \frac{(m+n)(m+n+1)}{2} + m$$

Sprawdzenie, że tak jest w istocie, pozostawiamy jako ćwiczenie. Wskazówka: pierwszy składnik w definicji $v(m,n)$ przedstawia sumę liczb naturalnych od zera do $m+n$.

Przykłady zbiorów przeliczalnych

- Zbiór $\mathbb{N} \times \mathbb{N}$ jest przeliczalny.
- Zbiór $\mathbb{Z}$ wszystkich liczb całkowitych jest przeliczalny. Skoro bowiem $\mathbb{Z} = (\mathbb{N}\times\mathbb{N})/_\sim$ to mamy funkcję $\kappa : \mathbb{N}\times\mathbb{N} \xrightarrow{\text{na}} \mathbb{Z}$ określoną warunkiem $\kappa(m,n) = [\langle m,n\rangle]_\sim$. (Mówiąc po ludzku, chodzi o funkcję $\kappa(m,n) = m - n$. Każda liczba całkowita jest różnicą dwóch liczb naturalnych.)
- Zbiór $\mathbb{Q}$ wszystkich liczb wymiernych definiujemy podobnie jak zbiór $\mathbb{Z}$. Rozważamy relację równoważności $\approx$ w zbiorze par $\mathbb{Z} \times (\mathbb{Z} - \{0\})$, daną warunkiem

  $$\langle x,y\rangle \approx \langle u,v\rangle \quad \text{wtedy i tylko wtedy, gdy} \quad x \cdot v = u \cdot y,$$

  i przyjmujemy $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} - \{0\}))/_\approx$. Po sprawdzeniu, że warunki $\langle x,y\rangle \approx \langle x',y'\rangle$ i $\langle u,v\rangle \approx \langle u',v'\rangle$ implikują

  $$\langle xv+yu, yv\rangle \approx \langle x'v'+y'u', y'v'\rangle \text{ oraz } \langle xu, yv\rangle \approx \langle x'u', y'v'\rangle,$$

  możemy zdefiniować operacje na liczbach wymiernych:

  $$[\langle x,y\rangle]_\approx + [\langle u,v\rangle]_\approx = [\langle xv+yu, yv\rangle]_\approx$$

  $$[\langle x,y\rangle]_\approx \cdot [\langle u,v\rangle]_\approx = [\langle xu, yv\rangle]_\approx$$

  Liczby całkowite interpretujemy jako liczby wymierne za pomocą włożenia

  $$j(z) = [\langle z,1\rangle]_\approx.$$

  Oczywiście zamiast $[\langle x,y\rangle]_\approx$ piszemy odtąd $\frac{x}{y}$. Ponieważ $\kappa : \mathbb{Z} \times (\mathbb{Z} - \{0\}) \xrightarrow{\text{na}} \mathbb{Q}$, gdzie $\kappa(x,y) = \frac{x}{y}$, więc zbiór wszystkich liczb wymiernych jest przeliczalny.
- A więc przeliczalny jest też np. zbiór wszystkich punktów płaszczyzny o współrzędnych wymiernych. Utożsamiamy go przecież ze zbiorem $\mathbb{Q} \times \mathbb{Q}$.

Twierdzenie 7.10 *Suma przeliczalnej rodziny zbiorów przeliczalnych jest przeliczalna.*

[8] Czasami o bijekcji z $\mathbb{N} \times \mathbb{N}$ na $\mathbb{N}$ mówimy *funkcja pary.* Taka funkcja pozwala na zakodowanie dwóch liczb naturalnych za pomocą jednej.

Dowód: Niech $\mathcal{A}$ będzie przeliczalną rodziną zbiorów przeliczalnych. Bez straty ogólności możemy założyć, że:

- $\mathcal{A} \neq \emptyset$, bo inaczej $\bigcup \mathcal{A} = \emptyset$, czyli teza jest oczywista;
- $\emptyset \notin \mathcal{A}$, bo $\bigcup \mathcal{A} = \bigcup (\mathcal{A} - \{\emptyset\})$, więc zamiast $\mathcal{A}$ możemy wziąć $\mathcal{A} - \{\emptyset\}$.

A więc, na mocy Wniosku 7.6 mamy funkcję:

$$F : \mathbb{N} \xrightarrow{\text{na}} \mathcal{A},$$

a ponieważ elementy $\mathcal{A}$ są też przeliczalne, więc dla dowolnego $m \in \mathbb{N}$ jest też funkcja

$$f_m : \mathbb{N} \xrightarrow{\text{na}} F(m).$$

Wtedy $G : \mathbb{N} \times \mathbb{N} \xrightarrow{\text{na}} \bigcup \mathcal{A}$, gdzie $G(m, n) = f_m(n)$. Sprawdźmy, że funkcja G jest faktycznie „na”. Ponieważ F jest „na”, więc każdy element $a \in \bigcup \mathcal{A}$ należy do pewnego $F(m)$. Zatem a jest postaci $f_m(n)$, bo f_m też jest „na”. Wnioskujemy, że $\bigcup \mathcal{A}$ jest zbiorem przeliczalnym, jako obraz zbioru przeliczalnego (Lemat 7.7). ∎

Uwaga: * Choć nie widać tego na pierwszy rzut oka, dowód powyższego twierdzenia w istotny sposób opiera się na pewniku wyboru. Przypisujemy bowiem każdej liczbie m pewną funkcję $f_m : \mathbb{N} \xrightarrow{\text{na}} F(m)$, a więc *implicite* stosujemy funkcję wyboru dla rodziny $\mathcal{A}$. Ściślej, powołujemy się tu na Twierdzenie 3.13 o niepustości produktu zbiorów niepustych.

Definicja 7.11 *Słowo* nad alfabetem A to dowolny skończony ciąg elementów zbioru A. Dokładniej, jest to dowolna funkcja $w : n \to A$, gdzie n jest pewną liczbą naturalną. Liczbę tę nazywamy *długością* słowa w, i zapisujemy to tak: $n = |w|$. A więc słowo *baba* to funkcja $w : 4 \to \{a, b\}$, spełniająca warunki

$$w(i) = \begin{cases} b, & \text{jeśli } i \text{ jest parzyste;} \\ a, & \text{jeśli } i \text{ jest nieparzyste} \end{cases}$$

Zbiór wszystkich słów n-literowych nad A (słów nad A o długości n) pokrywa się więc ze zbiorem A^n wszystkich funkcji z n do A. Zbiór wszystkich słów nad A oznaczamy przez A^*. Szczególnym słowem jest jedyne słowo o długości 0. Jest to *słowo puste*, czyli funkcja pusta. Oznaczamy je przez ε.

Fakt 7.12 *Jeśli alfabet A jest przeliczalny to zbiór wszystkich słów A^* też jest przeliczalny.*

Dowód: Nietrudno pokazać przez indukcję, że każdy ze zbiorów A^n jest przeliczalny. Istotnie, zbiór $A^0 = \{\varepsilon\}$ jest jednoelementowy, a krok indukcyjny wynika z łatwej równoliczności $A^{n+1} \sim A^n \times A$. Skoro A^* jest sumą wszystkich A^n, dla $n \in \mathbb{N}$, to teza wynika z Twierdzenia 7.10. ∎

8 Nierówności pomiędzy mocami

Lemat 8.1 *Jeżeli* $A \sim B$ *i* $C \sim D$ *oraz istnieje injekcja* $f : A \xrightarrow{1-1} C$*, to istnieje też injekcja* $g : B \xrightarrow{1-1} D$.

Dowód: Istnieją bijekcje $\varphi : B \xrightarrow[\text{na}]{1-1} A$ oraz $\psi : C \xrightarrow[\text{na}]{1-1} D$. Zatem $\psi \circ f \circ \varphi : B \xrightarrow{1-1} D$. Tę konstrukcję przedstawia poniższy diagram:

$$\begin{tikzcd}
A \arrow[r, "f"] & C \arrow[d, "\psi"] \\
B \arrow[u, "\varphi"] \arrow[r, dotted] & D
\end{tikzcd}$$

∎

Definicja 8.2 Mówimy, że moc zbioru A jest *mniejsza lub równa* mocy zbioru B (i piszemy $\overline{\overline{A}} \leq \overline{\overline{B}}$), wtedy i tylko wtedy, gdy istnieje injekcja $f : A \xrightarrow{1-1} B$. Jeżeli $\overline{\overline{A}} \leq \overline{\overline{B}}$ ale zbiory A i B nie są równoliczne, to piszemy $\overline{\overline{A}} < \overline{\overline{B}}$ i mówimy, że zbiór A jest mocy *mniejszej* niż zbiór B.

Uwaga:

- Poprawność powyższej definicji wynika z Lematu 8.1.
- Jeśli $\mathfrak{m}, \mathfrak{n}$ są liczbami kardynalnymi to $\mathfrak{m} \leq \mathfrak{n}$ oznacza, że $\overline{\overline{A}} \leq \overline{\overline{B}}$, dla $\overline{\overline{A}} = \mathfrak{m}$, $\overline{\overline{B}} = \mathfrak{n}$.
- Jeśli $f : A \xrightarrow{1-1} B$, ale f nie jest bijekcją, to nie znaczy, że $\overline{\overline{A}} < \overline{\overline{B}}$. Na przykład funkcja następnika jest injekcją z $\mathbb{N}$ w $\mathbb{N}$ i nie jest „na”, ale przecież $\overline{\overline{\mathbb{N}}} \not< \overline{\overline{\mathbb{N}}}$.

Przykład 8.3

- Jeśli $A \subseteq B$, to $\overline{\overline{A}} \leq \overline{\overline{B}}$.
- Dla dowolnej liczby naturalnej n zachodzi $n < \aleph_0$.
- Dla dowolnego zbioru A zachodzi $\overline{\overline{A}} \leq \overline{\overline{\mathbf{P}(A)}}$. Istotnie, mamy $\zeta : A \xrightarrow{1-1} \mathbf{P}(A)$, gdzie $\zeta(a) = \{a\}$ dla $a \in A$.
- Zbiór A jest nieskończony wtedy i tylko wtedy, gdy $\aleph_0 \leq \overline{\overline{A}}$ (Twierdzenie 7.3).

Fakt 8.4 *Dla dowolnych niepustych zbiorów A, B następujące warunki są równoważne:*

1) $\overline{\overline{A}} \leq \overline{\overline{B}}$;
2) *Istnieje* $g : B \xrightarrow{\text{na}} A$;
3) *Zbiór A jest równoliczny z pewnym podzbiorem zbioru B.*

Dowód: Równoważność warunków (1) i (2) to dokładnie treść Twierdzenia 3.14. Równoważność (1) i (3) wynika z następujących obserwacji:

- Jeśli $f : A \xrightarrow{1-1} B$ to $A \sim \mathrm{Rg}(f)$.
- Jeśli $f : A \xrightarrow[\text{na}]{1-1} C \subseteq B$ to $f : A \xrightarrow{1-1} B$. ∎

Fakt 8.5 *Dla dowolnych zbiorów A, B, C:*

- $\overline{\overline{A}} \leq \overline{\overline{A}}$;
- *Jeśli* $\overline{\overline{A}} \leq \overline{\overline{B}}$ *i* $\overline{\overline{B}} \leq \overline{\overline{C}}$ *to* $\overline{\overline{A}} \leq \overline{\overline{C}}$.

O ile powyższy fakt jest całkiem oczywisty, to antysymetria nierówności

$$\textit{Jeśli } \overline{\overline{A}} \leq \overline{\overline{B}} \textit{ i } \overline{\overline{B}} \leq \overline{\overline{A}} \textit{ to } \overline{\overline{A}} = \overline{\overline{B}}$$

(zwana twierdzeniem Cantora-Bernsteina) nie jest już oczywista. Udowodnimy ją najpierw w takiej wersji:

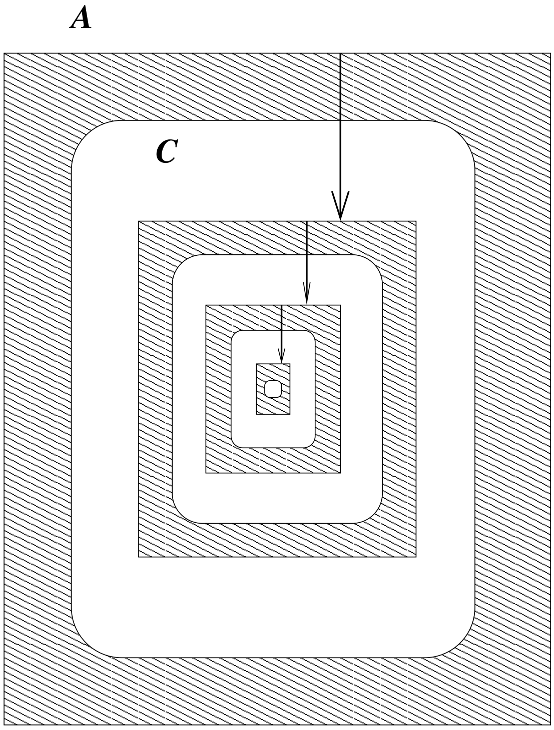
Lemat 8.6 *Jeśli* $\varphi : A \xrightarrow{1-1} C \subseteq A$ *to* $C \sim A$.

Dowód: Zaczniemy od określenia ciągu zbiorów X_n, dla $n \in \mathbb{N}$.

$$\begin{aligned} X_0 &= A - C; \\ X_{n+1} &= \vec{\varphi}(X_n). \end{aligned}$$

Niech $X = \bigcup\{X_n \mid n \in \mathbb{N}\}$ i niech $Y = A - X$. Zauważmy, że $C = A - X_0 = (X \cup Y) - X_0 = (X - X_0) \cup Y$, bo $Y \cap X_0 = \emptyset$. Określimy bijekcję $\psi : A \xrightarrow[\text{na}]{1-1} C$ jak następuje:

$$\psi(x) = \begin{cases} x, & \text{jeśli } x \in Y; \\ \varphi(x), & \text{jeśli } x \in X \end{cases}$$



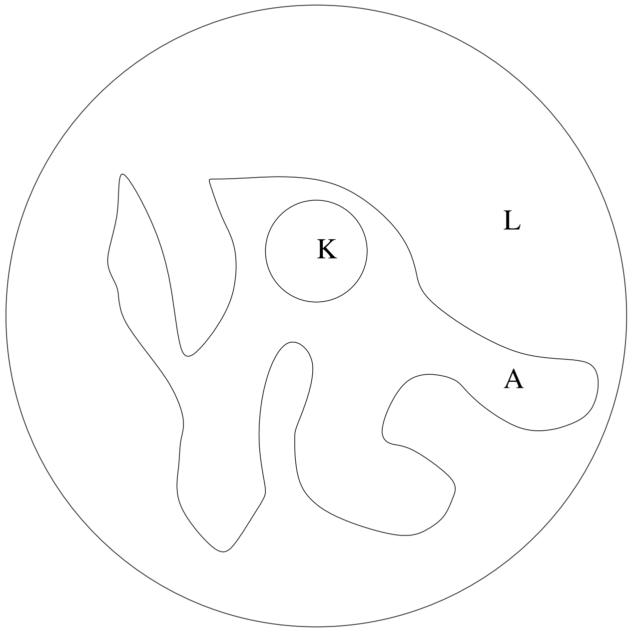
Rysunek 1: Dowód Lematu 8.6

Inaczej, $\psi = \varphi|_X \cup \mathrm{id}_Y$. Na Rysunku 1 zbiór X odpowiada obszarowi zakreskowanemu, a zbiór Y to cała reszta. Poszczególne zakreskowane składowe to zbiory X_n. A zatem funkcja ψ jest identycznością na obszarze białym, a każdą z zakreskowanych składowych przekształca w następną. Funkcja ψ jest różnowartościowa, ponieważ $\mathrm{id}_Y : Y \xrightarrow{1-1} Y$ oraz $\varphi|_X : X \xrightarrow{1-1} X$ są są funkcjami różnowartościowymi, a przy tym X i Y są rozłączne. Ponadto ψ jest na C. Jeśli bowiem $c \in C$, to są dwie możliwości. Albo $c \in Y$ i wtedy $c = \psi(c)$, albo $c \in X - X_0$ i mamy $c \in X_{n+1}$ dla pewnego n. A wtedy $c = \varphi(x) = \psi(x)$ dla pewnego $x \in X_n$. ∎

Twierdzenie 8.7 (Cantora-Bernsteina) *Jeśli* $\overline{\overline{A}} \leq \overline{\overline{B}}$ *i* $\overline{\overline{B}} \leq \overline{\overline{A}}$ *to* $\overline{\overline{A}} = \overline{\overline{B}}$.

Dowód: Z założenia istnieją funkcje $f : A \xrightarrow{1-1} B$ i $g : B \xrightarrow{1-1} A$. Zbiór $C = \mathrm{Rg}(g)$ jest oczywiście równoliczny z B. Jeśli teraz $\varphi = g \circ f$ to $\varphi : A \xrightarrow{1-1} C$. Na mocy Lematu 8.6, zbiór A jest równoliczny z C, a więc także z B. ∎

Twierdzenie Cantora-Bernsteina jest niezwykle użytecznym narzędziem do badania mocy zbiorów. Zwykle znacznie łatwiej jest wskazać dwie funkcje różnowartościowe, jedną z A do B i drugą z B do A, niż bijekcję pomiędzy A i B. Na przykład moc dziwnej figury na Rysunku 2 jest taka sama jak moc każdego z dwóch kół (otwartych). Mamy bowiem



Rysunek 2: Zastosowanie twierdzenia Cantora-Bernsteina

$\overline{\overline{\mathrm{K}}} \leq \overline{\overline{\mathrm{A}}} \leq \overline{\overline{\mathrm{L}}}$, bo $\mathrm{K} \subseteq \mathrm{A} \subseteq \mathrm{L}$. Ponieważ łatwo zauważyć, że dowolne dwa koła otwarte są równoliczne, więc mamy $\overline{\overline{\mathrm{K}}} = \overline{\overline{\mathrm{L}}}$, i możemy użyć twierdzenia Cantora-Bernsteina.

Twierdzenie 8.8 (Cantora) *Dla dowolnego zbioru A zachodzi $\overline{\overline{A}} < \overline{\overline{\mathbf{P}(A)}}$.*

Dowód: Już poprzednio zauważyliśmy, że $\overline{\overline{A}} \leq \overline{\overline{\mathbf{P}(A)}}$, należy więc pokazać, że nie istnieje bijekcja $F : A \xrightarrow[\text{na}]{1-1} \mathbf{P}(A)$. Przypuśćmy, że taka jest, i niech $B = \{x \in A \mid x \notin F(x)\}$. Skoro F jest „na", to istnieje takie $b \in A$, że $F(b) = B$. Pytamy, czy $b \in B$. Jeśli $b \in B$, to z definicji zbioru B mamy $b \notin F(b) = B$. Ale jeśli $b \notin B$, to też źle, bo wtedy warunek $b \notin F(b)$ nie powinien zachodzić, czyli mielibyśmy właśnie $b \in B$. Otrzymana sprzeczność wynikła z założenia, że $F : A \xrightarrow[\text{na}]{1-1} \mathbf{P}(A)$, a więc takiej funkcji nie ma. ∎

Rozumowanie użyte w dowodzie twierdzenia Cantora stosuje tzw. *metodę przekątniową* (rozważamy dwuargumentowy predykat „$x \notin F(y)$" dla $x = y$). Do sprzeczności doprowadziło nas zjawisko podobne do *paradoksu kłamcy*,[9] znane też z anegdoty o wojskowym fryzjerze, któremu polecono golić tych i tylko tych żołnierzy, co sami się nie golą. Porównajmy dwa, niemożliwe do spełnienia, warunki:

$$\forall x \in A(x \in F(b) \Leftrightarrow x \notin F(x))$$

$$\forall x(b \text{ goli } x \Leftrightarrow x \text{ nie goli } x)$$

[9] Stwierdzenie *„To zdanie jest fałszywe"* nie może być ani prawdziwe ani fałszywe.

a zobaczymy, że chodzi tu o ten sam paradoks, często wykorzystywany tam, gdzie należy udowodnić, że coś jest niemożliwe.

Wniosek 8.9

1) Nie istnieje zbiór wszystkich zbiorów, tj. zbiór Ω spełniający warunek $\forall x (x \in \Omega)$.

2) Istnieją zbiory nieprzeliczalne, na przykład $\mathbf{P}(\mathbb{N})$.

3) Istnieje nieskończenie wiele liczb kardynalnych.

Dowód: (1) Gdyby Ω był zbiorem wszystkich zbiorów, to także każdy podzbiór Ω byłby jego elementem, mielibyśmy więc $\mathbf{P}(\Omega) \subseteq \Omega$, skąd $\overline{\overline{\mathbf{P}(\Omega)}} \leq \overline{\overline{\Omega}}$.

(2) Oczywiste.

(3) Łatwo widzieć, że $\overline{\overline{\mathbb{N}}} < \overline{\overline{\mathbf{P}(\mathbb{N})}} < \overline{\overline{\mathbf{P}(\mathbf{P}(\mathbb{N}))}} < \overline{\overline{\mathbf{P}(\mathbf{P}(\mathbf{P}(\mathbb{N})))}} < \cdots$ ∎

Liczby rzeczywiste

Zanim zajmiemy się mocą zbioru wszystkich liczb rzeczywistych, zobaczmy jak można zdefiniować liczby rzeczywiste na gruncie teorii mnogości. Funkcję $f : \mathbb{N} \to \mathbb{Q}$ nazwiemy *ciągiem Cauchy'ego*, gdy

$$\forall \varepsilon \in \mathbb{Q}\, (\varepsilon > 0 \to \exists n \in \mathbb{N}\, \forall k \geq n (f(n) - \varepsilon < f(k) < f(n) + \varepsilon))$$

W zbiorze $\mathcal{C}$ wszystkich ciągów Cauchy'ego określimy relację równoważności $\equiv$.

$$f \equiv g \quad \Leftrightarrow \quad \forall \varepsilon \in \mathbb{Q}\, (\varepsilon > 0 \to \exists n \in \mathbb{N}\, \forall k \geq n (f(k) - \varepsilon < g(k) < f(k) + \varepsilon)).$$

Zbiór $\mathbb{R}$ wszystkich liczb rzeczywistych definiujemy jako $\mathcal{C}/_{\equiv}$. Działania na liczbach rzeczywistych definiujemy „po współrzędnych". Wynikiem dodawania $[f]_{\equiv} + [g]_{\equiv}$ jest więc klasa abstrakcji ciągu h określonego równaniem $h(n) = f(n) + g(n)$. Przyjmujemy, że $\mathbb{Q} \subseteq \mathbb{R}$ poprzez identyfikację każdej liczby wymiernej $q \in \mathbb{Q}$ z ciągiem stałym o wartości q.

Definicja 8.10 Moc zbioru wszystkich liczb rzeczywistych nazywamy *continuum* i oznaczamy przez $\mathfrak{C}$.

Przypomnijmy, że $2^{\mathbb{N}}$ to zbiór wszystkich funkcji z $\mathbb{N}$ do $2 = \{0, 1\}$, inaczej — zbiór wszystkich nieskończonych ciągów zerojedynkowych.

Fakt 8.11 $\mathfrak{C} = \overline{\overline{\mathbf{P}(\mathbb{N})}} = \overline{\overline{2^{\mathbb{N}}}}$.

Dowód: Najpierw zauważmy, że $F : 2^{\mathbb{N}} \xrightarrow[\text{na}]{1-1} \mathbf{P}(\mathbb{N})$, gdzie $F(f) = \vec{f}^{\,-1}(1)$. Istotnie, dla $f \neq g$ istnieje jakieś n, dla którego $f(n) = 1$ i $g(n) = 0$ albo na odwrót. Zatem $n \in F(f)$ i $n \notin F(g)$ albo na odwrót, funkcja F jest więc różnowartościowa. Jest też na $\mathbf{P}(\mathbb{N})$, bo jeśli $B \subseteq \mathbb{N}$ to $B = F(\chi_B)$, gdzie χ_B to *funkcja charakterystyczna* zbioru B, czyli:

$$\chi_B(n) = \begin{cases} 1, & \text{jeśli } n \in B; \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

A zatem zbiory $\mathbf{P}(\mathbb{N})$ i $2^{\mathbb{N}}$ są tej samej mocy. Aby pokazać, że jest to moc continuum, skorzystamy z Twierdzenia 8.7, tj. udowodnimy dwie nierówności: $\overline{\overline{2^{\mathbb{N}}}} \leq \mathfrak{C}$ i $\mathfrak{C} \leq \overline{\overline{\mathbf{P}(\mathbb{N})}}$.

[$\overline{\overline{2^{\mathbb{N}}}} \leq \mathfrak{C}$] Niech $H : 2^{\mathbb{N}} \to \mathbb{R}$ przyporządkowuje każdemu ciągowi zerojedynkowemu liczbę rzeczywistą z przedziału $(0, 1)$, której zapis *dziesiętny* po przecinku odpowiada temu ciągowi. A więc na przykład $H(01100011100\ldots) = 0,01100011100\ldots$ Dokładniej, dla dowolnego $f \in 2^{\mathbb{N}}$

$$H(f) = \sum_{i=0}^{\infty} \frac{f(i)}{10^{i+1}}$$

Aby sprawdzić, że funkcja H jest różnowartościowa, przypuśćmy, że $f \neq g$. Niech $n = \min\{i \mid f(i) \neq g(i)\}$. Wtedy $\sum_{i<n} \frac{f(i)}{10^{i+1}} = \sum_{i<n} \frac{g(i)}{10^{i+1}}$. Oznaczmy tę sumę przez b i przypuśćmy na przykład, że $f(n) = 0$ i $g(n) = 1$. Wtedy

$$H(f) = b + \sum_{i=n+1}^{\infty} \frac{f(i)}{10^{i+1}} < b + \frac{1}{10^{n+1}} \leq H(g)$$

[$\mathfrak{C} \leq \overline{\overline{\mathbf{P}(\mathbb{N})}}$] Niech $\alpha : \mathbb{N} \xrightarrow[\text{na}]{1-1} \mathbb{Q}$ będzie dowolną ustaloną bijekcją, i niech

$$G(x) = \{n \in \mathbb{N} \mid \alpha(n) < x\},$$

dla dowolnego $x \in \mathbb{R}$. W ten sposób określiliśmy funkcję $G : \mathbb{R} \to \mathbf{P}(\mathbb{N})$. Ta funkcja jest różnowartościowa, bo jeśli $x \neq y$ to na przykład $x < y$, a wtedy istnieje liczba wymierna q spełniająca nierówności $x < q < y$. Mamy więc $\alpha^{-1}(q) \in G(y) - G(x)$. ∎

9 Arytmetyka liczb kardynalnych

Lemat 9.1 *Niech* $\overline{\overline{A}} \leq \overline{\overline{B}}$ *i* $\overline{\overline{C}} \leq \overline{\overline{D}}$. *Wtedy:*

1) *Jeśli* $A \cap C = \emptyset$ *i* $B \cap D = \emptyset$, *to* $\overline{\overline{A \cup C}} \leq \overline{\overline{B \cup D}}$.

2) $\overline{\overline{A \times C}} \leq \overline{\overline{B \times D}}$.

3) *Jeśli* $C \neq \emptyset$, *to* $\overline{\overline{A^C}} \leq \overline{\overline{B^D}}$.

Dowód: Istnieją funkcje $f : A \xrightarrow{1-1} B$ i $g : C \xrightarrow{1-1} D$.

(1) Ponieważ dziedziny funkcyj f i g są rozłączne, więc suma $f \cup g$ jest funkcją ze zbioru $A \cup C$ do $B \cup D$. Łatwo zauważyć, że jest to funkcja różnowartościowa.

(2) Funkcja $F : A \times C \xrightarrow{1-1} B \times D$ może być określona warunkiem $F(a, c) = \langle f(a), g(c) \rangle$. Różnowartościowość F łatwo wynika z różnowartościowości f i g.

(3) Ponieważ $C \neq \emptyset$, więc istnieje funkcja $h : D \xrightarrow{\text{na}} C$. Funkcję $G : A^C \to B^D$ określimy równaniem $G(\alpha) = f \circ \alpha \circ h$. Rysunek poniżej objaśnia tę definicję:

$$\begin{tikzcd}
C \arrow[r, "\alpha"] & A \arrow[d, "f"] \\
D \arrow[u, "h"] \arrow[r, dotted, "G(\alpha)"'] & B
\end{tikzcd}$$

Sprawdźmy, że funkcja G jest różnowartościowa. Jeśli $\alpha, \beta \in A^C$ oraz $\alpha \neq \beta$, to $\alpha(c) \neq \beta(c)$, dla pewnego $c \in C$. Funkcja h jest „na", więc istnieje takie $d \in D$, że $h(d) = c$. Z różnowartościowości funkcji f wnioskujemy, że $G(\alpha)(d) = f(\alpha(h(d))) = f(\alpha(c)) \neq f(\beta(c)) = f(\beta(h(d))) = G(\beta)(d)$, czyli, że $G(\alpha) \neq G(\beta)$. ∎

Wniosek 9.2 *Jeśli* $\overline{\overline{A}} = \overline{\overline{B}}$ *i* $\overline{\overline{C}} = \overline{\overline{D}}$ *to*

- $\overline{\overline{A \times C}} = \overline{\overline{B \times D}}$;
- $\overline{\overline{A^C}} = \overline{\overline{B^D}}$.

Jeśli ponadto $A \cap C = \emptyset$ *i* $B \cap D = \emptyset$ *to*

- $\overline{\overline{A \cup C}} = \overline{\overline{B \cup D}}$

Dowód: Łatwa konsekwencja Lematu 9.1. Uwaga: należy zauważyć, że $\overline{\overline{A^\emptyset}} = 1$ dla dowolnego zbioru A. ∎

Z Wniosku 9.2 wynika poprawność następującej definicji:

Definicja 9.3

Sumą $\mathfrak{m} + \mathfrak{n}$ liczb kardynalnych $\mathfrak{m}$ i $\mathfrak{n}$ nazywamy moc dowolnego zbioru postaci $A \cup C$, gdzie $\overline{\overline{A}} = \mathfrak{m}$, $\overline{\overline{C}} = \mathfrak{n}$, oraz $A \cap C = \emptyset$.

Iloczynem $\mathfrak{m} \cdot \mathfrak{n}$ liczb kardynalnych $\mathfrak{m}$ i $\mathfrak{n}$ nazywamy moc dowolnego zbioru postaci $A \times C$, gdzie $\overline{\overline{A}} = \mathfrak{m}$, $\overline{\overline{C}} = \mathfrak{n}$.

Potęgą $\mathfrak{m}^\mathfrak{n}$ o podstawie $\mathfrak{m}$ i wykładniku $\mathfrak{n}$ nazywamy moc dowolnego zbioru postaci A^C, gdzie $\overline{\overline{A}} = \mathfrak{m}$, $\overline{\overline{C}} = \mathfrak{n}$.

Uwaga: Zwykłe działania na liczbach naturalnych pokrywają się z działaniami określonymi powyżej.

Przykład 9.4

- $\aleph_0 + \aleph_0 = \aleph_0$, bo $\mathbb{Z} \sim \mathbb{N}$.
- $\aleph_0 \cdot \aleph_0 = \aleph_0$, bo $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.
- $2^{\aleph_0} = \mathfrak{C}$, na mocy Faktu 8.11.
- Przyjmijmy $\beth_0 = \aleph_0$ i dalej $\beth_{n+1} = 2^{\beth_n}$. (Hebrajską literę $\beth$ czytamy „bet".) Wtedy $\overline{\overline{\mathbf{P}(\mathbb{N})}} = \overline{\overline{\mathbb{R}}} = \beth_1$, $\overline{\overline{\mathbf{P}(\mathbf{P}(\mathbb{N}))}} = \beth_2$, itd.

Fakt 9.5 *Jeśli* $\mathfrak{m} \geq \aleph_0$ *to* $\mathfrak{m} + \aleph_0 = \mathfrak{m}$.

Dowód: Niech $\overline{\overline{A}} = \mathfrak{m}$ i $\overline{\overline{C}} = \aleph_0$, a przy tym $A \cap C = \emptyset$. Na mocy Twierdzenia 7.3, istnieje podzbiór $B \subseteq A$, o mocy $\aleph_0$. Wtedy $A \cup C = (A - B) \cup (B \cup C) \sim (A - B) \cup B = A$, ponieważ $B \cup C$ też jest mocy $\aleph_0$. A zatem $\mathfrak{m} + \aleph_0 = \overline{\overline{A \cup C}} = \overline{\overline{A}} = \mathfrak{m}$. ∎

Wiele praw arytmetyki liczb naturalnych można uogólnić na dowolne liczby kardynalne. W szczególności, dla dowolnych liczb kardynalnych $\mathfrak{m}$, $\mathfrak{n}$ i $\mathfrak{p}$, zachodzą następujące równości:

- $\mathfrak{m} + 0 = \mathfrak{m}$ (bo $A \cup \emptyset = A$).
- $\mathfrak{m} + \mathfrak{n} = \mathfrak{n} + \mathfrak{m}$ (bo $A \cup B = B \cup A$).

- $(\mathfrak{m}+\mathfrak{n})+\mathfrak{p}=\mathfrak{m}+(\mathfrak{n}+\mathfrak{p})$ (bo $(A\cup B)\cup C=A\cup(B\cup C)$).
- $\mathfrak{m}\cdot 1=\mathfrak{m}$ (bo $A\times 1\sim A$).
- $\mathfrak{m}\cdot 0=0$ (bo $A\times\emptyset=\emptyset$).
- $\mathfrak{m}\cdot\mathfrak{n}=\mathfrak{n}\cdot\mathfrak{m}$ (bo $A\times B\sim B\times A$).
- $(\mathfrak{m}\cdot\mathfrak{n})\cdot\mathfrak{p}=\mathfrak{m}\cdot(\mathfrak{n}\cdot\mathfrak{p})$ (bo $(A\times B)\times C\sim A\times(B\times C)$).
- $\mathfrak{m}\cdot(\mathfrak{n}+\mathfrak{p})=\mathfrak{m}\cdot\mathfrak{n}+\mathfrak{m}\cdot\mathfrak{p}$ (bo $A\times(B\cup C)\sim(A\times B)\cup(A\times C)$).
- $\mathfrak{m}^0=1$ (bo tylko $\emptyset$ należy do $A^{\emptyset}$).
- $\mathfrak{m}^1=\mathfrak{m}$ (bo elementy A^1 to funkcje stałe).
- $1^{\mathfrak{m}}=1$ (bo funkcja należąca do $\{0\}^A$ musi być stale równa zero).
- $0^{\mathfrak{m}}=0$, o ile $\mathfrak{m}\neq 0$ (bo nie ma funkcji ze zbioru niepustego w pusty).

Mniej oczywiste są trzy prawa potęgowania.

Fakt 9.6 *Dla dowolnych liczb kardynalnych $\mathfrak{m}$, $\mathfrak{n}$ i $\mathfrak{p}$, zachodzą następujące równości:*

1) $\mathfrak{m}^{\mathfrak{n}}\cdot\mathfrak{m}^{\mathfrak{p}}=\mathfrak{m}^{(\mathfrak{n}+\mathfrak{p})}$;

2) $\mathfrak{m}^{\mathfrak{n}}\cdot\mathfrak{p}^{\mathfrak{n}}=(\mathfrak{m}\cdot\mathfrak{p})^{\mathfrak{n}}$;

3) $(\mathfrak{m}^{\mathfrak{n}})^{\mathfrak{p}}=\mathfrak{m}^{\mathfrak{n}\cdot\mathfrak{p}}$.

Dowód: W części (1) należy pokazać, że $A^B\times A^C\sim A^{B\cup C}$, przy założeniu, że $B\cap C=\emptyset$. Bijekcję $F: A^B\times A^C \xrightarrow[\text{na}]{1-1} A^{B\cup C}$ można określić wzorem $F(f,g)=f\cup g$, dla $f: B\to A$ i $g: C\to A$.

Dla dowodu części (2) potrzebna jest bijekcja $G: A^B\times C^B \xrightarrow[\text{na}]{1-1} (A\times C)^B$, którą zdefiniujemy tak: $G(f,g)(b)=\langle f(b),g(b)\rangle$, dla $f: B\to A$, $g: B\to C$ i $b\in B$.

W części (3) posłużymy się bijekcją $H: (A^B)^C \xrightarrow[\text{na}]{1-1} A^{B\times C}$, która jest określona wzorem $H(\varphi)(b,c)=\varphi(c)(b)$, dla $\varphi: C\to A^B$ i dla $c\in C$, $b\in B$. Dowód, że jest to istotnie bijekcja, podobnie jak funkcje określone w (1) i (2) pozostawiamy jako ćwiczenie. ∎

Lemat 9.1 stwierdza, że działania na liczbach kardynalnych są operacjami monotonicznymi w następującym sensie. Jeśli $\mathfrak{m}\leq\mathfrak{n}$ i $\mathfrak{p}\leq\mathfrak{q}$, to:

- $\mathfrak{m}+\mathfrak{p}\leq\mathfrak{n}+\mathfrak{q}$;

- $\mathfrak{m} \cdot \mathfrak{p} \leq \mathfrak{n} \cdot \mathfrak{q}$;
- $\mathfrak{m}^{\mathfrak{p}} \leq \mathfrak{n}^{\mathfrak{q}}$, pod warunkiem, że $\mathfrak{p} \neq 0$.

Wniosek 9.7

1) $\aleph_0 \cdot \mathfrak{C} = \mathfrak{C} \cdot \mathfrak{C} = \mathfrak{C}$.

2) $\aleph_0^{\aleph_0} = \mathfrak{C}^{\aleph_0} = \mathfrak{C}$;

3) $2^{\mathfrak{C}} = \aleph_0^{\mathfrak{C}} = \mathfrak{C}^{\mathfrak{C}}$.

Dowód:

1) Bo $\mathfrak{C} \leq \aleph_0 \cdot \mathfrak{C} \leq \mathfrak{C} \cdot \mathfrak{C} = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0} = \mathfrak{C}$.

2) Bo $\mathfrak{C} = 2^{\aleph_0} \leq \aleph_0^{\aleph_0} \leq \mathfrak{C}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = \mathfrak{C}$.

3) Bo $2^{\mathfrak{C}} \leq \aleph_0^{\mathfrak{C}} \leq \mathfrak{C}^{\mathfrak{C}} = (2^{\aleph_0})^{\mathfrak{C}} = 2^{\aleph_0 \cdot \mathfrak{C}} = 2^{\mathfrak{C}}$. ∎

Uwaga 1: Jak już stwierdziliśmy, działania na liczbach kardynalnych są monotoniczne ze względu na nieostrą nierówność $\leq$. Nie jest to jednak prawdą dla nierówności ostrej $<$. Istotnie: mamy wprawdzie $5 < \aleph_0$, ale:

- $5 + \aleph_0 = \aleph_0 + \aleph_0 = \aleph_0$;
- $5 \cdot \aleph_0 = \aleph_0 \cdot \aleph_0 = \aleph_0$;
- $2^{\aleph_0} = \aleph_0^{\aleph_0} = \mathfrak{C}$;
- $\mathfrak{C}^5 = \mathfrak{C}^{\aleph_0} = \mathfrak{C}$.

Uwaga 2: Nie można w sensowny sposób określić odejmowania liczb kardynalnych. Odejmowanie jest działaniem odwrotnym do dodawania. Aby można było je zdefiniować, z warunku $\mathfrak{m} + \mathfrak{p} = \mathfrak{m} + \mathfrak{q} = \mathfrak{n}$ musiałoby wynikać $\mathfrak{p} = \mathfrak{q}$. Wtedy przyjęlibyśmy, że $\mathfrak{n} - \mathfrak{m} = \mathfrak{p}$. Ale skoro na przykład $\aleph_0 + 5 = \aleph_0 + \aleph_0 = \aleph_0$, to różnica $\aleph_0 - \aleph_0$ nie ma sensu. Podobnie nie można zdefiniować dzielenia, pierwiastkowania ani logarytmowania liczb kardynalnych.

Hipoteza continuum *

Nie znamy żadnej liczby $\mathfrak{m}$ spełniającej nierówności $\aleph_0 < \mathfrak{m} < \mathfrak{C}$. Przypuszczenie, że takiej liczby nie ma nazywane jest *hipotezą continuum*. Hipoteza continuum okazała się zdaniem niezależnym od aksjomatów teorii mnogości. Oznacza to, że nie można jej z tych aksjomatów wyprowadzić (P.J. Cohen, 1964), ale też, że nie można udowodnić jej zaprzeczenia (K. Gödel, 1939).

10 Relacje porządkujące

Definicja 10.1 Relację r w zbiorze A nazywamy relacją *częściowego porządku*, gdy jest

$$\begin{array}{rll} \textit{zwrotna} & \text{czyli} & \forall x{\in}A\,(x\,r\,x) \\ \textit{przechodnia} & \text{czyli} & \forall x{\in}A\,\forall y{\in}A\,\forall z{\in}A(x\,r\,y \wedge y\,r\,z \to x\,r\,z) \\ \textit{antysymetryczna} & \text{czyli} & \forall x{\in}A\,\forall y{\in}A\,(x\,r\,y \wedge y\,r\,x \to x = y) \end{array}$$

Parę $\langle A, r\rangle$, a czasami sam zbiór A, nazywamy *zbiorem częściowo uporządkowanym*, lub po prostu *częściowym porządkiem.* Określenie „częściowy porządek" jest też używane w stosunku do samej relacji.

Jeśli dodatkowo relacja r jest spójna, tj.

$$\forall x{\in}A\,\forall y{\in}A\,(x\,r\,y \vee y\,r\,x)$$

to mówimy, że jest to relacja *liniowego porządku.* Określenia *liniowy porządek*, *zbiór liniowo uporządkowany*, stosuje się odpowiednio.

Przykład 10.2

- Relacja $\leq$ w zbiorze liczb naturalnych jest liniowym porządkiem.
- Zbiór $\mathbb{N} - \{0\}$ jest częściowo uporządkowany przez relację podzielności:
  $$m|n \text{ wtedy i tylko wtedy, gdy } \exists k \in \mathbb{N} - \{0\}\,(k \cdot m = n).$$
- Każda rodzina zbiorów jest częściowo uporządkowana przez inkluzję. Dokładniej, dla dowolnego A, para $\langle A, r\rangle$, gdzie dla $a, b \in A$
  $$a\,r\,b \text{ wtedy i tylko wtedy, gdy } a \subseteq b,$$
  jest zawsze częściowym porządkiem. Zamiast $\langle A, r\rangle$ piszemy zwykle po prostu $\langle A, \subseteq\rangle$.

Relacje częściowo porządkujące najczęściej oznaczamy symbolami $\leq$, $\preceq$, $\sqsubseteq$ i podobnymi. Jeśli $\leq$ jest częściowym porządkiem w A , to relacja $<$ jest określona tak:

$$x < y \quad \text{wtedy i tylko wtedy, gdy} \quad x \leq y \text{ i } x \neq y.$$

Dla $A \neq \emptyset$, ta relacja *nie jest* częściowym porządkiem, bo nie jest zwrotna. Notację $\prec$, $\sqsubset$ itp. stosujemy odpowiednio.

Jeśli $\langle A, r\rangle$ jest częściowym (liniowym) porządkiem, oraz $B \subseteq A$, to łatwo zauważyć, że $\langle B, r \cap (B \times B)\rangle$ jest też częściowym (liniowym) porządkiem. Dla prostoty oznaczamy go przez $\langle B, r\rangle$.

Definicja 10.3 Niech $\langle A, \leq \rangle$ będzie częściowym porządkiem.

1. Elementy $a, b \in A$ są *porównywalne*, gdy $a \leq b$ lub $b \leq a$. W przeciwnym razie a, b są *nieporównywalne*.
2. Jeśli $B \subseteq A$ i każde dwa elementy zbioru B są porównywalne (tj. $\langle B, \leq \rangle$ jest liniowo uporządkowany) to mówimy, że B jest *łańcuchem* w A.
3. Jeśli $B \subseteq A$ i każde dwa różne elementy zbioru B są nieporównywalne, to mówimy, że B jest *antyłańcuchem* w A.

Ostrzeżenie: W zbiorze częściowo uporządkowanym z warunku $x \not\leq y$ nie wynika $x > y$! Elementy x, y mogą być nieporównywalne.

Porządkowanie słów

Niech A będzie ustalonym alfabetem. Przypomnijmy, że *słowo* nad A, długości n, to funkcja $w : n \to A$, i że słowo puste oznaczamy przez ε. *Konkatenacją* (złożeniem) słów $w : n \to A$ i $v : m \to A$ nazywamy słowo $w \cdot v$ powstałe przez dopisanie słowa v na końcu słowa w. A zatem $w \cdot v : n + m \to A$, a dla $i < n + m$ mamy:

$$(w \cdot v)(i) = \begin{cases} w(i), & \text{jeśli } i < n; \\ v(i - n), & \text{w przeciwnym przypadku.} \end{cases}$$

Operacja konkatenacji jest łączna, na przykład:

$$ein \cdot (und \cdot zwanzig) = (ein \cdot und) \cdot zwanzig = einundzwanzig$$

Słowo puste jest elementem neutralnym konkatenacji, tj. $\varepsilon \cdot w = w \cdot \varepsilon = w$ dla dowolnego słowa w.

Lemat 10.4 *Dla dowolnych słów $w, v \in A^*$,*

$$w \subseteq v \quad \Leftrightarrow \quad \exists u \in A^*(v = w \cdot u).$$

Dowód: $(\Rightarrow)$ Przypuśćmy, że $w \subseteq v$. Wtedy $\mathrm{Dom}(w) \subseteq \mathrm{Dom}(v)$, a zatem $|w| \leq |v|$. Niech $k = |v| - |w|$. Dla $i < k$, niech $u(i) = v(|w| + i)$. Wtedy $v = w \cdot u$.

$(\Leftarrow)$ Jeśli $v = w \cdot u$ to oczywiście $w = v|_{|w|}$, więc $w \subseteq v$. ∎

A zatem $w \subseteq v$ oznacza dokładnie tyle, że słowo w jest przedrostkiem (prefiksem) słowa v. Relację inkluzji w zbiorze A^* nazywamy więc porządkiem *prefiksowym*.

Często przyjmujemy, że alfabet A jest uporządkowany przez jakąś relację $\leq$. Wtedy w zbiorze A^* możemy określić porządek *leksykograficzny* $\preceq$. Przyjmujemy, że $w \preceq v$, gdy zachodzi jedna z możliwości

- $w \subseteq v$;
- Istnieje takie słowo u, że $ua \subseteq w$ i $ub \subseteq v$, dla pewnych $a, b \in A$ takich, że $a < b$.

Na przykład, jeśli $a < b$, to $\varepsilon \preceq ab \preceq aba \preceq baba \preceq bba$.

Lemat 10.5 *Jeśli $wu = vu'$ to $w \subseteq v$ lub $v \subseteq w$.*

Dowód: Niech $x = wu = vu'$. Wówczas $w = x|_{|w|}$ i $v = x|_{|v|}$. Zatem nierówność $|w| \leq |v|$ implikuje $w \subseteq v$ a nierównośc przeciwna $v \subseteq w$. ∎

Fakt 10.6 *Porządek leksykograficzny jest relacją częściowego porządku w zbiorze A^*. Jeśli alfabet jest liniowo uporządkowany, to porządek leksykograficzny też jest liniowy.*

Dowód: Zwrotność relacji $\preceq$ wynika ze zwrotności relacji $\subseteq$. Aby udowodnić przechodniość załóżmy, że $w \preceq v$ i $v \preceq x$. Mamy do rozpatrzenia 4 przypadki.

Przypadek 1: $w \subseteq v$ i $v \subseteq x$. Wtedy oczywiście $w \subseteq x$.

Przypadek 2: $w \subseteq v = uav'$, oraz $x = ubx'$, gdzie $a < b$. Mamy tu dwie możliwości (Lemat 10.5): albo $w \subseteq u$ albo $u \subsetneq w$. Wtedy odpowiednio, albo $w \subseteq x$, albo $ua \subseteq w$, czyli $w = uaw'$, a wtedy $w \preceq x$ na mocy drugiej części definicji.

Przypadek 3: $w = uaw'$ oraz $v = ubv' \subseteq x$ i $a < b$. Wtedy $x = ubv'x'$ i mamy $w \preceq x$ na mocy drugiej części definicji.

Przypadek 4: $w = uaw'$ i $v = ubv'$ oraz jednocześnie $v = u'a'v''$ i $x = u'b'x'$ gdzie $a < b$ i $a' < b'$. Skoro $v = ubv' = u'a'v''$, to $u \subseteq u'$ lub $u' \subseteq u$ Jeśli $u \subsetneq u'$ to $x = ubx''$, więc $w \preceq x$. Podobnie, jeśli $u' \subsetneq u$, to $w = u'a'w''$ i też $w \preceq x$. Natomiast $u = u'$ implikuje $x = ub'x''$, oraz $a < b = a' < b'$. Zatem znowu $w \preceq x$.

Pozostaje wykazać antysymetrię. Niech więc $w \preceq v$ i $v \preceq w$. Tu też mamy cztery przypadki, analogiczne do rozpatrzonych powyżej. Zauważmy jednak, że powtarzając poprzednie rozumowanie dla $x = w$, w przypadkach 2,3 i 4 otrzymamy sprzeczność. Okaże się bowiem, że $w = uaw' = ubw''$, gdzie $a < b$. Zostaje więc tylko przypadek 1, czyli $w \subseteq v$ i $v \subseteq w$. A więc $w = v$.

Przypuśćmy teraz, że alfabet jest liniowo uporządkowany. Weźmy dowolne $w, v \in A^*$ i przypuśćmy na przykład, że $|w| \leq |v|$. Jeśli $w \not\subseteq v$, to istnieje takie i, że $i < |w|$ oraz $w(i) \neq v(i)$. Wybierzmy najmniejsze takie i. Oznaczmy słowo $w|_i = v|_i$ przez u. Jeśli teraz $w(i) < v(i)$ to $w = uw(i)w' \preceq uv(i)v' = v$. Podobnie, jeśli $v(i) < w(i)$ to $v \preceq w$. ∎

Elementy wyróżnione

Definicja 10.7 *Niech $\langle A, \leq \rangle$ będzie częściowym porządkiem i niech $a \in A$. Mówimy, że element a jest w zbiorze A:*

$$
\begin{array}{lll}
\textit{największy,} & \textit{gdy} & \forall x \in A\,(x \leq a); \\
\textit{maksymalny,} & \textit{gdy} & \forall x \in A\,(a \leq x \to a = x); \\
\textit{najmniejszy,} & \textit{gdy} & \forall x \in A\,(a \leq x); \\
\textit{minimalny,} & \textit{gdy} & \forall x \in A\,(x \leq a \to a = x).
\end{array}
$$

Fakt 10.8 *Jeśli a jest elementem największym (najmniejszym) w $\langle A, \leq \rangle$, to jest też elementem maksymalnym (minimalnym) i innych elementów maksymalnych (minimalnych) nie ma.*

Dowód: Załóżmy, że a jest największy w A. Aby pokazać, że jest maksymalny, przypuśćmy, że $a \leq x$. Ale skoro a jest największy, to $x \leq a$ więc $a = x$. Niech teraz $b \in A$ będzie też elementem maksymalnym. Skoro a jest największy, to $b \leq a$ więc $b = a$ bo b jest maksymalny. A więc a jest jedynym elementem maksymalnym w A. ∎

Przykład 10.9

- W zbiorze uporządkowanym $\langle\, \mathbb{N} - \{0, 1\},\ |\ \rangle$, gdzie $|$ oznacza relację podzielności, nie ma elementu najmniejszego ani żadnych elementów maksymalnych. Natomiast liczby pierwsze są elementami minimalnymi.
- W zbiorze $\mathbb{Z}$ liczb całkowitych, uporządkowanym przez zwykłą relację $\leq$, nie ma żadnych elementów minimalnych ani maksymalnych.
- Rozpatrzmy częściowy porządek $\langle \mathbb{Z} \cup \{\omega\}, \preceq \rangle$ gdzie $\omega \notin \mathbb{Z}$, oraz
$$x \preceq y \quad \Leftrightarrow [(x, y \in \mathbb{Z}) \land (x \leq y)] \lor [x = y = \omega]$$
Ten porządek ma tylko jeden element minimalny ω, ale nie ma elementu najmniejszego.

Uwaga: Relacja odwrotna do relacji częściowo porządkującej r też jest relacją częściowo porządkującą. Elementy minimalne ze względu na r są elementami maksymalnymi ze względu na r^{-1} i na odwrót. Podobny dualizm dotyczy elementów najwiekszych i najmniejszych. Dlatego wszystkie fakty dotyczące elementów maksymalnych i największych stosują się też odpowiednio do elementów minimalnych i najmniejszych.

Fakt 10.10

1) *Każdy skończony i niepusty częściowy porządek ma element maksymalny.*

2) *Jeśli $\langle A, \leq \rangle$ jest porządkiem liniowym i $a \in A$ jest jego elementem maksymalnym to a jest elementem najwiekszym.*

3) *A zatem każdy skończony i niepusty liniowy porządek ma element najwiekszy.*

4) *Analogiczne fakty mają miejsce w odniesieniu do elementów najmniejszych i minimalnych.*

Dowód: (1) Przez indukcję ze względu na $n \geq 0$ pokażemy, że każdy częściowy porządek mocy n ma element maksymalny. Jeśli zbiór ma tylko jeden element to ten element jest oczywiście maksymalny. Załóżmy więc, że teza zachodzi dla zbiorów n-elementowych i niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym o $n+1$ elementach. Wtedy możemy przedstawić zbiór A jako sumę $A = B \cup \{a\}$, gdzie B jest zbiorem n-elementowym, a zatem z założenia indukcyjnego ma element maksymalny b. Jeśli teraz $b \not\leq a$ to b jest elementem maksymalnym w A. W przeciwnym razie elementem maksymalnym jest a. Istotnie, przypuśćmy, że $a \leq c$. Wtedy $c = a$ (i dobrze) lub $c \in B$. W tym drugim przypadku łatwo zauważyć, że $a = b = c$, bo b jest maksymalny w B.

(2) Załóżmy, że $\langle A, \leq \rangle$ jest porządkiem liniowym i $a \in A$ jest maksymalny. Niech $b \in A$. Gdyby $b \not\leq a$ to $a \leq b$, więc $a = b$ z maksymalności.

(3) Oczywista konsekwencja (1) i (2).

(4) Należy zastosować (1), (2) i (3) do porządku odwrotnego. ∎

Definicja 10.11 Niech $\langle A, \leq \rangle$ będzie porządkiem częściowym i niech $B \subseteq A$ i $a \in A$. Mówimy, że a jest *ograniczeniem górnym* zbioru B (oznaczenie $a \geq B$), gdy $b \leq a$ dla wszystkich $b \in B$.

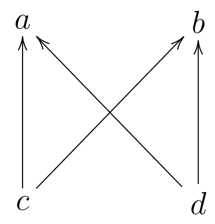
Element a jest *kresem górnym* zbioru B (oznaczenie $a = \sup B$), gdy jest najmniejszym ograniczeniem górnym B, czyli:

- $a \geq B$;
- jeśli $c \geq B$ to $c \geq a$, dla dowolnego $c \in A$.

Analogicznie definiujemy ograniczenia dolne (oznaczenie $a \leq B$) i kresy dolne (oznaczenie $a = \inf B$).

Przykład 10.12

- W rodzinie wszystkich podzbiorów zbioru A (uporządkowanej przez inkluzję) kresem górnym dowolnej podrodziny $X \subseteq \mathbf{P}(A)$ jest suma $\bigcup X$.
- W rodzinie wszystkich wypukłych[10] podzbiorów płaszczyzny, każdy podzbiór X ma kres górny. Kresem tym jest iloczyn wszystkich zbiorów wypukłych zawierających wszystkie zbiory z X. Zwykle nie jest to $\bigcup X$, bo suma nie musi być wypukła.
- W zbiorze liczb wymiernych $\mathbb{Q}$ ze zwykłym uporządkowaniem zbiór $\{q \in \mathbb{Q} \mid q^2 < 2\}$ ma ograniczenia górne ale nie ma kresu górnego.
- W zbiorze $\{a, b, c, d\}$ uporzadkowanym jak na rysunku, podzbiór $\{c, d\}$ ma dwa ograniczenia górne, ale nie ma kresu górnego.



Następujący fakt podamy na razie bez dowodu (zob. Wniosek 13.12).

Twierdzenie 10.13 (Lemat Kuratowskiego-Zorna) *Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym, spełniającym następujący warunek:*

(*) Każdy łańcuch ma w A ograniczenie górne

Wtedy w A istnieje element maksymalny.

Następujące twierdzenie stanowi ważny przykład zastosowania Lematu Kuratowskiego-Zorna. Przypomnijmy, że podzbiór A przestrzeni liniowej V jest *niezależny liniowo*, jeśli z warunku $k_1 v_1 + \cdots + k_n v_n = 0$, gdzie $v_1, \ldots, v_n \in A$, wynika $k_1 = \cdots = k_n = 0$. Zbiór A jest *bazą* przestrzeni V, wtedy i tylko wtedy, gdy jest liniowo niezależny, oraz każdy element przestrzeni jest kombinacją liniową elementów zbioru A.

Twierdzenie 10.14 *Każda przestrzeń liniowa ma bazę.*

Dowód: Nietrudno zauważyć, że zbiór A jest bazą przestrzeni V wtedy i tylko wtedy, gdy dodanie do zbioru A dowolnego nowego elementu powoduje utratę liniowej niezależności. A zatem baza to element maksymalny rodziny

[10] Zbiór jest *wypukły* wtedy i tylko wtedy, gdy wraz z dowolnymi dwoma punktami zawiera odcinek łączący te punkty.

$$Z = \{A \subseteq V \mid A \text{ jest liniowo niezależny}\},$$

uporządkowanej przez inkluzję. Użyjemy więc Lematu Kuratowskiego-Zorna, aby wykazać istnienie elementu maksymalnego zbioru Z. W tym celu wystarczy stwierdzić, że każdy łańcuch jest w Z ograniczony z góry. Niech więc $Ł$ będzie łańcuchem w Z i niech $B = \bigcup Ł$. Pokażemy, że zbiór B jest liniowo niezależny.

Istotnie, przypuśćmy, że $k_1v_1+\cdots+k_nv_n = 0$, gdzie $v_1, \dots, v_n \in B$. Skoro wektory $v_1, \dots, v_n$ należą do sumy łańcucha $Ł$, to każdy z nich należy do pewnego składnika. Stąd wynika, że $v_1 \in A_1, \dots, v_n \in A_n$ dla pewnych $A_1, \dots, A_n \in Ł$. Rodzina zbiorów $\{A_1, \dots, A_n\}$ jest skończona i liniowo uporządkowana przez inkluzję, ma więc element największy na mocy Faktu 10.10(3). To znaczy, że dla pewnego i mamy $v_1, \dots, v_n \in A_i$, a przecież zbiór A_i jest liniowo niezależny. Stąd kombinacja liniowa $k_1v_1 + \cdots + k_nv_n = 0$ musi byc trywialna: $k_1 = \cdots = k_n = 0$.

Ponieważ B jest liniowo niezależny, więc $B \in Z$, a przy tym oczywiście B zawiera wszystkie elementy $Ł$, jest więc ograniczeniem górnym naszego łańcucha w zbiorze Z. Spełnione jest więc założenie Twierdzenia 10.13 i musi istnieć element maksymalny. ∎

11 Punkty stałe

Definicja 11.1 Niech $\langle A, \leq \rangle$ będzie porządkiem częściowym.

- Podzbiór B zbioru A jest *skierowany* wtedy i tylko wtedy, gdy dla dowolnych $a, b \in B$ istnieje takie $c \in B$, że $a, b \leq c$.
- Zbiór A jest *zupełnym* porządkiem częściowym (cpo) wtedy i tylko wtedy, gdy każdy jego skierowany podzbiór ma kres górny.
- Zbiór A jest *kratą zupełną* wtedy i tylko wtedy, gdy każdy podzbiór A ma kres górny.

Oczywiście każdy łańcuch jest zbiorem skierowanym. W szczególności elementy dowolnego ciągu wstępującego $a_0 \leq a_1 \leq a_2 \leq \dots$ tworzą zbiór skierowany. Także zbiór pusty jest zbiorem skierowanym. Z definicji porządku zupełnego wynika więc istnienie elementu najmniejszego $\sup \emptyset$, tradycyjnie oznaczanego przez $\perp$.

Fakt 11.2 *W kracie zupełnej każdy podzbiór ma kres dolny.*

Dowód: Niech $\langle A, \leq \rangle$ będzie kratą zupełną i niech $B \subseteq A$. Przez C oznaczmy zbiór wszystkich ograniczeń dolnych zbioru B:

$$C = \{x \in A \mid x \leq B\}.$$

Teraz jeśli $b \in B$ to $b \geq C$, więc dla $c = \sup C$ mamy $b \geq c$. To znaczy, że c jest ograniczeniem dolnym zbioru B. Co więcej, c jest kresem dolnym, bo $x \leq B$ oczywiście implikuje $x \leq c$. ∎

Definicja 11.3 Niech $\langle A, \leq \rangle$ i $\langle B, \leq \rangle$ będą porządkami częściowymi.

- Funkcja $f : A \to B$ jest *monotoniczna* wtedy i tylko wtedy, gdy dla dowolnych $x, y \in A$ nierówność $x \leq y$ implikuje $f(x) \leq f(y)$.
- Jeśli $\langle A, \leq \rangle$ i $\langle B, \leq \rangle$ są zupełnymi porządkami częściowymi to funkcja $f : A \to B$ jest *ciągła* wtedy i tylko wtedy, gdy f zachowuje kresy górne niepustych zbiorów skierowanych, tj. dla dowolnego skierowanego i niepustego podzbioru $X \subseteq A$ istnieje $\sup \vec{f}(X)$ i zachodzi równość $f(\sup X) = \sup \vec{f}(X)$.
- Jeśli $f : A \to A$ oraz $f(a) = a$, to mówimy, że a jest *punktem stałym* funkcji f. *Najmniejszy* punkt stały danej funkcji to najmniejszy element zbioru wszystkich jej punktów stałych (o ile taki istnieje).

Fakt 11.4 *Każda funkcja ciągła jest monotoniczna.*

Dowód: Niech $x \leq y$. Wtedy zbiór $\{x, y\}$ jest skierowany, a jego kresem górnym jest y. Zatem $f(y)$ jest kresem górnym zbioru $\{f(x), f(y)\}$, czyli $f(x) \leq f(y)$. ∎

Uwaga*: Zbiór częściowo uporządkowany nazywamy *kratą*, gdy każdy jego dwuelementowy podzbiór ma kres górny i kres dolny. Ćwiczenie: pokazać, że krata zupełna to to samo co krata, która jest cpo.

Twierdzenie 11.5 *Jeśli zbiór częściowo uporządkowany $\langle A, \leq \rangle$ jest kratą zupełną, to każda funkcja monotoniczna $f : A \to A$ ma najmniejszy punkt stały.*

Dowód: Rozpatrzmy zbiór $B = \{x \in A \mid f(x) \leq x\}$. Niech $a = \inf B$. Pokażemy, że a jest najmniejszym punktem stałym funkcji f.

Dla dowolnego $x \in B$ mamy $a \leq x$, więc $f(a) \leq f(x) \leq x$. Zatem $f(a)$ jest ograniczeniem dolnym zbioru B, skąd $f(a) \leq a$, bo a jest kresem dolnym.

Ale skoro $f(a) \leq a$, to także $f(f(a)) \leq f(a)$, więc $f(a) \in B$. Zatem $a \leq f(a)$ i mamy równość.

Ponieważ wszystkie punkty stałe funkcji f muszą należeć do B, więc a jest najmniejszym punktem stałym. ∎

Nie zawsze mamy do czynienia z kratami zupełnymi. Ale jeśli funkcja jest ciągła, to można to założenie osłabić. Przypomnijmy, że dla dowolnej funkcji $f : A \to A$ notacja f^n oznacza n-krotne złożenie funkcji f, tj. $f^0 = \mathrm{id}_A$ oraz $f^{n+1} = f \circ f^n$.

Twierdzenie 11.6 *Jeśli* $\langle A, \leq \rangle$ *jest zupełnym porządkiem częściowym to każda funkcja ciągła* $f : A \to A$ *ma najmniejszy punkt stały, którym jest* $\sup\{f^n(\bot) \mid n \in \mathbb{N}\}$.

Dowód: Oczywiście $\bot \leq f(\bot)$. Ponieważ f jest monotoniczna (Fakt 11.4), więc przez łatwą indukcję wnioskujemy, że ciąg $f^n(\bot)$ jest wstępujący: $f^n(\bot) \leq f^m(\bot)$ dla $n \leq m$. A zatem zbiór $\{f^n(\bot) \mid n \in \mathbb{N}\}$ jest skierowany i faktycznie ma kres górny. Z ciągłości funkcji dostajemy

$$f(\sup\{f^n(\bot) \mid n \in \mathbb{N}\}) = \sup\{f^{n+1}(\bot) \mid n \in \mathbb{N}\} = \sup\{f^n(\bot) \mid n \in \mathbb{N}\},$$

czyli $a = \sup\{f^n(\bot) \mid n \in \mathbb{N}\}$ jest punktem stałym. Pozostaje sprawdzić, że jest najmniejszy.

Jeśli b jest innym punktem stałym, to przez indukcję wnioskujemy, że $f^n(\bot) \leq b$ dla dowolnego $n \in \mathbb{N}$. (Zaczynamy od oczywistej nierówności $\bot \leq b$, a krok indukcyjny wynika z monotonicznosci: $f^{n+1}(\bot) \leq f(b) = b$.) A zatem $b \geq \{f^n(\bot) \mid n \in \mathbb{N}\}$ skąd $b \geq a$. ∎

Omówimy teraz kilka przykładów, w których występują punkty stałe przekształceń monotonicznych. Pierwszy przykład dotyczy dosyć typowej sytuacji gdy pewien zbiór rozszerzamy o nowe elementy, tak aby otrzymać nowy zbiór zamknięty ze względu na pewne operacje.

Przykład 11.7 Niech r będzie relacją w zbiorze A. Przypomnijmy, że $(s; s')$ oznacza złożenie relacyj s i s'. Rozpatrzmy zbiór $\mathbf{P}(A \times A)$ uporządkowany przez inkluzję, oraz funkcję $f : \mathbf{P}(A \times A) \to \mathbf{P}(A \times A)$ określoną tak:

$$f(s) = r \cup s \cup (s; s).$$

Funkcja f jest ciągła, więc ma najmniejszy punkt stały. Jest to relacja r^+, która jest najmniejszą relacją przechodnią zawierającą r. Żeby się o tym przekonać, należy zauważyć, że warunek $f(s) = s$ zachodzi wtedy i tylko wtedy, gdy s jest przechodnie (tj. $(s; s) \subseteq s$) oraz $r \subseteq s$. Relację r^+ nazywamy *domknięciem przechodnim* relacji r.

Następny przykład jest raczej nieformalny, ale bardziej „informatyczny". Typy rekurencyjne (indukcyjne) też mogą być uważane za punkty stałe.

Przykład 11.8 Przyjmijmy, że $\mathbf{1}$ oznacza typ jednostkowy, którego jedynym elementem jest **nil**. Niech $\tau \times \sigma$ i $\tau + \sigma$ oznaczają odpowiednio produkt i sumę prostą (rozłączną) typów τ i σ. Wówczas typ listy liczb całkowitych (oznaczmy go przez **list**) można utożsamiać z typem $\mathbf{1} + (\mathbf{int} \times \mathbf{list})$. Inaczej mówiąc, typ **list** można uważać za najmniejszy punkt stały operatora F, który dowolnemu typowi α przypisuje typ $F(\alpha) = \mathbf{1} + (\mathbf{int} \times \alpha)$. Typ **list** jest sumą ciągu przybliżeń $\bot, F(\bot), F^2(\bot), \ldots$ gdzie $\bot$ to typ pusty, a każde z $F^n(\bot)$ składa się z list długości co najwyżej $n - 1$.

Przedsmak semantyki denotacyjnej

Kolej na nieco bardziej rozbudowany przykład. Rozpoczniemy od definicji.

Definicja 11.9 *Funkcja częściowa* ze zbioru A do zbioru B to dowolna funkcja $f : A' \to B$, gdzie $A' \subseteq A$. Piszemy $f : A \multimap\!\!\rightarrow B$. Jeśli $f : A \multimap\!\!\rightarrow B$ oraz $\mathrm{Dom}(f) = A$ to mówimy, że f jest funkcją *całkowitą*.

Na potrzeby tego wykładu oznaczymy zbiór wszystkich funkcji częściowych z A do B przez $[A \multimap\!\!\rightarrow B]$. Zbiór $[A \multimap\!\!\rightarrow B]$ jest częściowo uporządkowany przez inkluzję. Co więcej, jest to porządek zupełny (chociaż nie krata zupełna).

Funkcje częściowe z A do B wygodnie jest utożsamiać z funkcjami całkowitymi z A do $B_\perp = B \cup \{\perp\}$, gdzie $\perp \notin B$ reprezentuje „wartość nieokreśloną”. Jeśli umówimy się, że zbiór $B_\perp$ jest uporządkowany tak:

$$b \leq b' \quad \text{wtedy i tylko wtedy, gdy} \quad b = \perp \text{ lub } b = b',$$

to możemy zauważyć, że zbiór $[A \multimap\!\!\rightarrow B]$ ma uporządkowanie „po współrzędnych”:

$$f \subseteq g \quad \text{wtedy i tylko wtedy, gdy} \quad \forall a \in A\,(f(a) \leq g(a)).$$

Rozpatrzmy teraz następującą rekurencyjną definicję funkcji częściowej $f : \mathbb{Z} \times \mathbb{Z} \multimap\!\!\rightarrow \mathbb{Z}$.

$$f(m,n) = \textbf{if } m = n \textbf{ then } 0 \textbf{ else } f(m+3,n)+3 \textbf{ fi} \qquad (*)$$

Ta definicja, rozumiana jako równanie na funkcjach częściowych, nie wyznacza jednoznacznie funkcji f. Równanie ma więcej niż jedno rozwiązanie. Inaczej mówiąc, operator na funkcjach częściowych

$$\Phi : [\mathbb{Z} \times \mathbb{Z} \multimap\!\!\rightarrow \mathbb{Z}] \to [\mathbb{Z} \times \mathbb{Z} \multimap\!\!\rightarrow \mathbb{Z}],$$

określony warunkiem

$$\Phi(f)(m,n) = \textbf{if } m = n \textbf{ then } 0 \textbf{ else } f(m+3,n)+3 \textbf{ fi},$$

ma więcej niż jeden punkt stały. Ale tylko jeden z tych punktów stałych odpowiada obliczeniowemu rozumieniu definicji rekurencyjnej (*). Jest to najmniejszy punkt stały. Funkcja f obliczana przez *program* zadany równaniem (*) jest sumą ciągu funkcyj częściowych $f_k = \Phi^k(\perp)$ gdzie $\perp$ to funkcja nigdzie nie określona. Łatwo widzieć, że f_k określone jest dla tych par $\langle m,n\rangle$ dla których obliczenie wymaga nie więcej niż $k-1$ odwołań rekurencyjnych.

Ćwiczenie: Wyznaczyć kilka początkowych wartości ciągu $\Phi^k(\perp)$, gdzie Φ jest zadane definicją rekurencyjną

$$f(m) = \textbf{if } m \leq 1 \textbf{ then } 1 \textbf{ else } f(\,\textbf{if } \mathit{parzyste}(m) \textbf{ then } m/2 \textbf{ else } 3m+1 \textbf{ fi}\,) \textbf{ fi}$$

Bisymulacje

Najmniejsze punkty stałe występują wszędzie tam, gdzie mamy do czynienia z indukcją, rekursją itp. Ale czasami przydatne jest też pojęcie największego punktu stałego. Mówimy wtedy o *ko-indukcji*. Na przykład najmniejszym rozwiązaniem równania $\alpha = \mathbf{int} \times \alpha$ jest oczywiście typ pusty. A największym? Typ **stream**, którego elementy to nieskończone ciągi liczb całkowitych. Nazywamy je *strumieniami* liczb całkowitych. Typ **stream** jest kresem dolnym zstępującego ciągu typów $\top, G(\top), G^2(\top), \ldots$ gdzie $\top$ to typ „pełny" (typ dowolnego obiektu), oraz $G(\alpha) = \mathbf{int} \times \alpha$.

Zajmiemy się teraz obszerniejszym przykładem najwiekszego punktu stałego. Przypuśćmy, że dany jest pewien zbiór A, w którym określona jest rodzina P relacji dwuargumentowych. O elementach A myślimy jako o możliwych stanach pewnego procesu, a relacje ze zbioru P reprezentują różne rodzaje możliwych przejść pomiędzy stanami. Aby to podkreślić, zamiast $\langle a, b\rangle \in \alpha$ (dla $\alpha \in P$) piszemy $a \rightsquigarrow_\alpha b$.

Powiemy, że relacja $\sim$ w zbiorze A jest *(częściową) bisymulacją*[11], gdy dla dowolnych $a_1, a_2 \in A$ takich, że $a_1 \sim a_2$, i dowolnego $\alpha \in P$, zachodzą następujące warunki:

- Jeśli $a_1 \rightsquigarrow_\alpha b_1$ dla pewnego b_1, to istnieje takie b_2, że $a_2 \rightsquigarrow_\alpha b_2$ i $b_1 \sim b_2$.
- Jeśli $a_2 \rightsquigarrow_\alpha b_2$ dla pewnego b_2, to istnieje takie b_1, że $a_1 \rightsquigarrow_\alpha b_1$ i $b_1 \sim b_2$.

Sens tej definicji jest taki: warunek $a_1 \sim a_2$ gwarantuje, że każde możliwe zachowanie procesu uruchomionego w stanie a_1 jest też możliwe, gdy proces uruchomimy w stanie a_2, i na odwrót.

Zauważmy teraz, że suma wszystkich bisymulacji częściowych jest bisymulacją. Jest to największa możliwa bisymulacja. Oznaczymy ją przez $\approx$ i nazwiemy *pełną bisymulacją*[12]. A więc warunek $a_1 \approx a_2$ to najsłabszy warunek gwarantujący takie samo zachowanie procesu w obu stanach.

Rozpatrzmy teraz następujący operator $\mathcal{F} : \mathbf{P}(A \times A) \to \mathbf{P}(A \times A)$:

$$\begin{aligned}\mathcal{F}(r) = \{&\langle a_1, a_2\rangle \mid \forall\alpha\forall b_1\,(a_1 \rightsquigarrow_\alpha b_1 \to \exists b_2\,(b_1\ r\ b_2 \wedge a_2 \rightsquigarrow_\alpha b_2))\}\\ &\cap \{\langle a_1, a_2\rangle \mid \forall\alpha\forall b_2\,(a_2 \rightsquigarrow_\alpha b_2 \to \exists b_1\,(b_1\ r\ b_2 \wedge a_1 \rightsquigarrow_\alpha b_1))\}.\end{aligned}$$

Nietrudno zauważyć, że $\mathcal{F}$ jest operatorem monotonicznym, i że częściowe bisymulacje to dokładnie te relacje, które spełniają warunek $r \subseteq \mathcal{F}(r)$. częściowe bisymulacje. Pełna bisymulacja jest największym punktem stałym operatora $\mathcal{F}$ (porównajmy to z konstrukcją w dowodzie twierdzenia 11.5). Co więcej, relacja $\approx$ jest iloczynem (kresem dolnym) zstępującego ciągu relacyj $\top, \mathcal{F}(\top), \mathcal{F}^2(\top), \ldots$ Symbol $\top$ oznacza oczywiście relację pełną $A \times A$,

[11] Ang.: bisimulation.
[12] Ang.: bisimilarity.

czyli największy element kraty zupełnej $\mathbf{P}(A \times A)$. Zauważmy jeszcze, że k-te przybliżenie $\mathcal{F}^k(\top)$ relacji $\approx$ można interpretować jako najsłabszą relację gwarantującą takie same zachowanie procesu przez pierwsze k kroków. Jako ćwiczenie warto udowodnić, że:

Fakt 11.10 *Pełna bisymulacja jest relacją równoważności.*

12 Izomorfizmy porządków

Często mamy do czynienia z dwoma zbiorami, które są różne, ale „tak samo" uporządkowane. Takie porządki nazywamy izomorficznymi.

Definicja 12.1 Mówimy, że zbiory częściowo uporządkowane $\langle A, \leq \rangle$ i $\langle B, \leq \rangle$ są *izomorficzne*, gdy istnieje bijekcja $f : A \xrightarrow[\text{na}]{1-1} B$ spełniająca warunek

$$a \leq a' \quad \Leftrightarrow \quad f(a) \leq f(a'),$$

dla dowolnych $a, a' \in A$. Piszemy wtedy $\langle A, \leq \rangle \approx \langle B, \leq \rangle$ (albo po prostu $A \approx B$), a funkcję f nazywamy *izomorfizmem*.

Jeśli dwa zbiory częściowo uporządkowane są izomorficzne i jeden z nich

- ma element najmniejszy, największy, maksymalny, minimalny;[13]
- jest liniowo uporządkowany;
- jest cpo, jest kratą zupełną;
- i tak dalej,

to ten drugi też ma odpowiednią własność. Zamiast „i tak dalej" można wstawić dowolny warunek dotyczący tylko relacji porządkującej.

Przykład 12.2

- Zbiór wszystkich liczb naturalnych $\mathbb{N}$ jest izomorficzny[14] z podzbiorem
  $$A = \{1 - \tfrac{1}{n} \mid n \in \mathbb{N} - \{0\}\}$$
  zbioru liczb rzeczywistych.

[13] Niepotrzebne skreślić.

[14] Jeśli mowa o $\mathbb{N}$, $\mathbb{R}$ itp., to domyślnie zakładamy, że chodzi o „zwykły" porządek, chyba że wyraźnie przyjęto inaczej.

- Żadne dwa spośród zbiorów: A, $A \cup \{1\}$, $A \cup \{1, 2\}$, $B = \{m - \frac{1}{n} \mid m, n \in \mathbb{N} - \{0\}\}$, nie są izomorficzne. Na przykład $A \not\approx A \cup \{1\}$, bo A nie ma elementu największego.

Mniej oczywisty jest nastepny fakt. Mówimy, że zbiór liniowo uporządkowany A jest *gęsty*, gdy dla dowolnych $a, b \in A$, jeśli $a < b$ to $a < c < b$ dla pewnego c.

Twierdzenie 12.3

- *Każdy przeliczalny zbiór liniowo uporządkowany jest izomorficzny z pewnym podzbiorem zbioru $\mathbb{Q}$ wszystkich liczb wymiernych.*
- *Każdy przeliczalny zbiór gęsty bez końców (tj. bez elementu największego i najmniejszego) jest izomorficzny z $\mathbb{Q}$.*

Dowód: Załóżmy, że $\langle A, \leq \rangle$ jest przeliczalnym zbiorem liniowo uporządkowanym. Bez straty ogólności zakładamy, że A jest nieskończony, tj. $A = \{a_n \mid n \in \mathbb{N}\}$, gdzie wszystkie a_n są różne. Podobnie, zbiór liczb wymiernych przedstawimy w postaci $\mathbb{Q} = \{q_n \mid n \in \mathbb{N}\}$, gdzie wszystkie q_n są różne.

Określamy funkcję $f : A \xrightarrow{1-1} \mathbb{Q}$, definiując $f(a_n)$ przez indukcję ze względu na n, w ten sposób, aby dla dowolnych $i, j \leq n$ zachodziła równoważność:

$$a_i < a_j \qquad \text{wtedy i tylko wtedy, gdy} \qquad f(a_i) < f(a_j). \qquad (*)$$

Przypuśćmy więc, że $f(a_i)$ są już określone dla $i < n$, i że założenie indukcyjne $(*)$ zachodzi dla $i, j < n$. Ustawmy w ciąg rosnący $a_{i_1} < a_{i_1} < \cdots < a_{i_n}$ elementy $a_0, \ldots, a_{n-1}$. Wtedy liczby $f(a_{i_1}) < f(a_{i_1}) < \cdots < f(a_{i_n})$ także tworzą ciąg rosnący.

Jeśli $n = 0$, to przyjmijmy $X_0 = A$ i $Y_0 = \mathbb{Q}$. Jeśli zaś $n > 0$, to niech

- $X_0 = \{a \in A \mid a < a_{i_1}\}$ oraz $Y_0 = (-\infty, f(a_{i_1})) \cap \mathbb{Q}$;
- $X_j = \{a \in A \mid a_{i_j} < a < a_{i_{j+1}}\}$ oraz $Y_j = (f(a_{i_j}), f(a_{i_{j+1}})) \cap \mathbb{Q}$, dla $j \in \{1, \ldots, n-1\}$;
- $X_n = \{a \in A \mid a_{i_n} < a\}$ oraz $Y_n = (f(a_{i_n}), \infty) \cap \mathbb{Q}$.

Element a_n, dla którego chcemy określić wartość $f(a_n)$, należy do jednego ze zbiorów $X_0, X_1, \ldots, X_n$, powiedzmy do X_ℓ. Nazwijmy go *przedziałem krytycznym dla n*. Elementy zbioru Y_ℓ nazwiemy zaś liczbami *dozwolonymi dla n*. Aby zachodził warunek $(*)$, wystarczy, aby $f(a_n)$ było dozwolone dla n. Niech więc $f(a_n) = q_m$, gdzie $m = \min\{k \in \mathbb{N} \mid q_k \in Y_\ell\}$.

Załóżmy teraz, że A jest gęsty i nie ma końców. Wtedy określona wyżej funkcja f jest izomorfizmem porządków. Wystarczy w tym celu sprawdzić, że f jest surjekcją.

Przypuśćmy więc, że tak nie jest i niech $m = \min\{k \mid q_k \notin \mathrm{Rg}(f)\}$. Liczby q_j dla $j < m$, dzielą zbiór $\mathbb{Q}$ na $m+1$ przedziałów, a do jednego z nich należy q_m. Przypuśćmy, że jest to przedział (q_l, q_r). (W przypadku, gdy jest to przedział niewłaściwy, dowód jest podobny.) Mamy więc $l, r < m$ oraz $q_j \notin (q_l, q_r)$ dla $j < m$. Ponadto $q_l, q_r \in \mathrm{Rg}(f)$, czyli $q_l = f(a_p)$ i $q_r = f(a_s)$ dla pewnych p, s. Niech $d = \min\{k \mid a_p < a_k < a_s\}$ i niech $f(a_d) = q_x$. Ponieważ funkcja f zachowuje porządek i jest injekcją, więc na pewno $q_x \in (q_l, q_r)$, skąd mamy $x > m$.

Przedział krytyczny dla d jest wyznaczony przez jedną lub dwie spośród liczb $a_0, a_1, \ldots, a_{d-1}$, z których żadna nie należy do zbioru $C = \{a \in A \mid a_p < a < a_s\}$. Zatem zbiór C jest zawarty w przedziale krytycznym, a wszystkie liczby z przedziału (q_l, q_r), w tym q_m, są dozwolone dla d. Tu otrzymujemy sprzeczność, bo liczbą dozwoloną dla d o najmniejszym numerze jest q_x, a przecież $x > m$. ∎

Definicja 12.4 Niech $\langle A, \leq \rangle$ będzie zbiorem częściowo uporządkowanym. Jeśli każdy niepusty podzbiór zbioru A ma element minimalny, to mówimy, że $\langle A, \leq \rangle$ jest *częściowym dobrym porządkiem*, lub, że jest *dobrze ufundowany*. Jeśli ponadto porządek $\langle A, \leq \rangle$ jest liniowy, to mówimy, że jest to *dobry porządek*. (Wtedy każdy niepusty podzbiór A ma element najmniejszy.)

Przykład 12.5

- Wszystkie zbiory z Przykładu 12.2 są dobrze uporządkowane.
- Zbiory $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nie są dobrze uporządkowane.
- Relacja $\subseteq$ jest dobrym ufundowaniem zbioru A^*.
- Jeśli w A są dwa elementy a, b, takie że $a < b$ to porządek leksykograficzny $\preceq$, wyznaczony przez $\leq$, nie jest dobrym ufundowaniem zbioru A^*. (Zbiór $\{a^n b \mid n \in \mathbb{N}\}$ nie ma elementu minimalnego.)

Fakt 12.6 *Zbiór $\langle A, \leq \rangle$ jest dobrze ufundowany wtedy i tylko wtedy, gdy nie istnieje w nim ciąg malejący, tj. taki podzbiór $\{a_i \mid i \in \mathbb{N}\}$, że $a_{i+1} < a_i$ dla dowolnego i.*

Dowód: $(\Rightarrow)$ Gdyby taki istniał, to by nie miał elementu minimalnego.

$(\Leftarrow)$ Weźmy niepusty podzbiór $B \subseteq A$ i przypuśćmy, że B nie ma elementu minimalnego. Skoro B jest niepusty to ma jakiś element b_0. On oczywiście nie jest minimalny, więc jest takie $b_1 \in B$, że $b_1 < b_0$. I tak dalej: przez indukcję[15] określamy ciąg malejący $b_0 > b_1 > b_2 > \cdots$ ∎

[15]Owszem, ta konstrukcja wymaga pewnika wyboru. I co z tego?

Drzewa

Definicja 12.7 Podzbiór B zbioru częściowo uporządkowanego A nazywamy *odcinkiem początkowym* w A, gdy

$$\forall x, y \in A\, (x \in B \wedge y \leq x \rightarrow y \in B).$$

Szczególny przypadek odcinka początkowego to odcinek wyznaczony przez element $x \in A$:

$$\mathcal{O}_A(x) = \{y \in A \mid y < x\}.$$

Uwaga: nierówność w definicji $\mathcal{O}_A(x)$ jest ostra, tj. $x \notin \mathcal{O}_A(x)$. Jeśli wiadomo o jaki zbiór chodzi, to zamiast $\mathcal{O}_A(x)$ piszemy po prostu $\mathcal{O}(x)$.

Definicja 12.8 Jeśli w zbiorze częściowo uporządkowanym mamy $a < b$, ale dla żadnego c nie zachodzi $a < c < b$, to mówimy, że a jest *bezpośrednim poprzednikiem* b, i że b jest *bezpośrednim nastepnikiem* a.

Definicja 12.9 Zbiór częściowo uporządkowany $\langle T, \leq \rangle$ nazywamy *drzewem*, gdy spełnia on następujące warunki:

1) Istnieje element najmniejszy.

2) Każdy odcinek postaci $\mathcal{O}_T(x)$ jest skończonym[16] łańcuchem.

Niech A będzie dowolnym alfabetem (niekoniecznie skończonym). Niepusty podzbiór T zbioru A^* nazywamy *drzewem słów* (nad A), gdy jest on odcinkiem początkowym w $\langle A^*, \subseteq \rangle$, czyli gdy spełniony jest warunek

$$\forall w, u \in A^*\, (w \cdot u \in T \rightarrow w \in T).$$

Na przykład następujący zbiór jest drzewem słów nad alfabetem $\{a, b\}$:

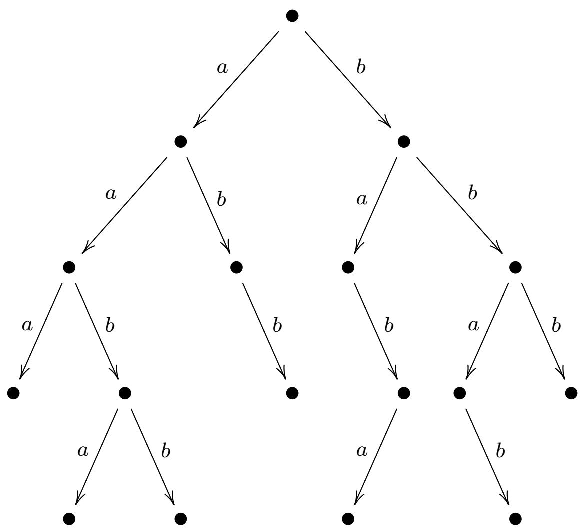
$$\{\varepsilon, a, b, aa, ab, ba, bb, aaa, aab, abb, bab, bba, bbb, aaba, aabb, baba, bbab\}.$$

Przedstawiamy go tak jak na Rysunku 3.[17]

Twierdzenie 12.10 *Każde drzewo jest izomorficzne z pewnym drzewem słów.*

[16] Czasami drzewem nazywa się każdy porządek, który ma element najmniejszy i w którym wszystkie zbiory $\mathcal{O}(x)$ są dobrze uporządkowane (ale niekoniecznie skończone).

[17] Jak wiadomo, drzewa rosną zwykle z góry na dół.



Rysunek 3: Drzewo

Dowód: Niech $\langle T, \leq \rangle$ będzie drzewem. Dla $a \in T$, przez S_a oznaczymy zbiór wszystkich bezpośrednich nastepników a. Weźmy dowolny zbiór A spełniający warunek $\overline{\overline{A}} \geq \overline{\overline{S_a}}$, dla dowolnego $a \in T$. Istnieją wtedy funkcje $\xi_a : S_a \xrightarrow{1-1} A$.

Ponieważ T spełnia warunki (1) i (2), więc $T = \bigcup\{T_n \mid n \in \mathbb{N}\}$, gdzie

$$T_n = \{a \in T \mid \overline{\overline{\mathcal{O}(a)}} \leq n\}.$$

Przy tym $T_0 = \{\bot\}$, gdzie a_0 jest najmniejszym elementem T. Określimy przez indukcję wstępujący ciąg funkcji $f_n : T_n \xrightarrow{1-1} A^*$, w ten sposób aby dla dowolnych $a, b \in T_n$ zachowany był warunek

$$a \leq b \quad \Leftrightarrow \quad f_n(a) \leq f_n(b),$$

oraz by obraz $\mathrm{Rg}(f_n)$ był drzewem słów. Szukanym izomorfizmem będzie wtedy oczywiście $f = \bigcup\{f_n \mid n \in \mathbb{N}\}$.

Zaczynamy od $f_0(\bot) = \varepsilon$. Jeśli funkcja f_n jest już określona, to przyjmujemy

$$f_{n+1}(b) = \begin{cases} f_n(b), & \text{jeśli } b \in T_n; \\ f_n(a) \cdot \xi_a(b), & \text{jeśli } b \in T_{n+1} - T_n \text{ i } a \text{ jest bezpośrednim poprzednikiem } b. \end{cases}$$

Uwaga: Konstrukcję powyżej można uważać za definicję indukcyjną

$$f(\bot) = \varepsilon, \qquad f(b) = f(a) \cdot \xi_a(b), \text{ gdy } b \text{ ma bezpośredni poprzednik } a. \quad \blacksquare$$

Definicja 12.11

1. *Gałęzią* w drzewie T nazywamy dowolny ciąg postaci $\varepsilon = a_0, a_1, a_2, \ldots$ (skończony lub nieskończony) gdzie każde a_{i+1} jest bezpośrednim nastepnikiem a_i.
2. Mówimy, że T jest drzewem o skończonym rozgałęzieniu, jeśli każdy element T ma skończenie wiele bezpośrednich nastepników.

Twierdzenie 12.12 (Lemat Königa) *Jeśli T jest nieskończonym drzewem o skończonym rozgałęzieniu to w T jest gałąź nieskończona.*

Dowód: Dla $a \in T$ niech $T_a = \{b \in T \mid a \leq b\}$. Przez indukcję konstruujemy nieskończoną gałąź $\varepsilon = a_0, a_1, a_2, \ldots$ w ten sposób, aby dla każdego i zbiór T_{a_i} był nieskończony. Krok bazowy jest poprawny, bo $T_\varepsilon = T$. Jeśli teraz T_{a_n} jest zbiorem nieskończonym, oraz a_n ma tylko skończenie wiele bezpośrednich nastepników $b_1, \ldots, b_k$, to zauważmy, że $T_{a_n} = \{a_n\} \cup T_{b_1} \cup \cdots \cup T_{b_k}$, więc któryś ze zbiorów $T_{b_j}, \ldots, T_{b_k}$ musi być nieskończony, powiedzmy T_{b_j}. Jako a_{n+1} możemy więc przyjąć b_j. ∎

Lemat Königa ma rozmaite zastosowania. Często używamy go, aby pokazać, że pewne obliczenia muszą się zakończyć w ograniczonym czasie. Spójrzmy na dwa przykłady.

Definicja 12.13 Relacja $\to$ w zbiorze A ma własność *silnej normalizacji* (SN) wtedy i tylko wtedy, gdy nie istnieje nieskończony ciąg postaci $a_0 \to a_1 \to a_2 \to \cdots$

Fakt 12.14 *Załóżmy, że relacja $\to$ w zbiorze A ma własność* SN *oraz dla dowolnego $a \in A$, zbiór $S_a = \{b \in A \mid a \to b\}$ jest skończony. Wówczas dla dowolnego $a \in A$ istnieje taka liczba n, że każdy ciąg postaci $a = a_0 \to a_1 \to a_2 \to \cdots \to a_k$ spełnia warunek $k \leq n$.*

Dowód: Ustalmy $a \in A$ i niech $T \subseteq A^*$ będzie zbiorem wszystkich słów postaci $a_0 a_1 \ldots a_k$, gdzie $a_0 = a$ oraz $a_i \to a_{i+1}$ dla $i < k$. Zbiór T z porządkiem prefiksowym jest drzewem o skończonym rozgałęzieniu, a zatem teza wynika z lematu Königa. ∎

Nastepny przykład dotyczy problemu znanego stąd, że jego algorytmiczne rozwiązanie jest w ogólnym przypadku niemożliwe. Przypuśćmy, że dany jest skończony zbiór K (dozwolonych rodzajów kafelków). Na zbiorze K mamy określone relacje zgodności poziomej r i pionowej s. Jeśli $M \subseteq \mathbb{Z} \times \mathbb{Z}$, to mówimy, że funkcja $f : M \to K$ jest *pokryciem* zbioru M, gdy zachodzą warunki

$$\langle f(x,y), f(x+1,y) \rangle \in r \qquad \langle f(x,y), f(x,y+1) \rangle \in s$$

dla wszystkich x, y dla których odpowiednie punkty leżą w zbiorze M. Mówiąc o pokryciu zbioru $M \subseteq \mathbb{R} \times \mathbb{R}$ mamy na myśli pokrycie dla $M \cap (\mathbb{Z} \times \mathbb{Z})$.

Fakt 12.15 *Jeśli istnieje pokrycie dowolnie wielkiego kwadratu to istnieje pokrycie całej płaszczyzny.*

Dowód: Niech $W_n = \{p \in \mathbb{Z} \mid -n < p < n\}$, gdzie $n \in \mathbb{N}$ i niech

$$T = \{f \mid f \text{ jest pokryciem } W_n^2 \text{ dla pewnego } n \in \mathbb{N}\}.$$

Zbiór T uporządkowany przez inkluzję jest drzewem o skończonym rozgałęzieniu. Istotnie, każde pokrycie kwadratu W_n o boku $2n-1$ ma co najwyżej $(\overline{\overline{K}})^{8n}$ rozszerzeń do pokrycia kwadratu W_{n+1}. Drzewo T jest nieskończone, bo istnieją pokrycia dowolnie wielkich kwadratów, a zatem ma nieskończoną gałąź $\emptyset \subseteq f_1 \subseteq f_2 \subseteq f_3 \subseteq \ldots$, gdzie każde f_n jest pokryciem W_n^2. Suma wszystkich funkcji f_n stanowi pokrycie całej płaszczyzny. ∎

Indukcja

Zasada indukcji, którą znamy dla liczb naturalnych, uogólnia się łatwo na dowolne zbiory dobrze ufundowane. Tę uogólnioną zasadę indukcji nazywamy czasem *indukcją strukturalną* lub *noetherowską*.

Fakt 12.16 (Zasada indukcji) *Niech $\langle A, \leq \rangle$ będzie dobrze ufundowany i niech $P \subseteq A$. Załóżmy, że dla dowolnego $a \in A$ zachodzi implikacja:*

$$\mathcal{O}_A(a) \subseteq P \;\Rightarrow\; a \in P.$$

Wtedy $P = A$.

Dowód: Przypuśćmy, że $P \neq A$. Zbiór $A - P$ jest wtedy niepusty i ma element minimalny a. Z minimalności mamy jednak $\mathcal{O}_A(a) \subseteq P$, więc $a \in P$. ∎

Nastepująca definicja jest nam potrzebna do podania przykładu zastosowania indukcji noetherowskiej.

Definicja 12.17 Niech $\to$ będzie relacją binarną w zbiorze A. Wtedy przez $\twoheadrightarrow$ oznaczamy najmniejszą relację zwrotną i przechodnią zawierającą $\to$ (domknięcie przechodnie sumy relacji $\to$ i relacji identycznościowej). Symbol $\leftarrow$ (odp. $\twoheadleftarrow$) oznacza oczywiście relację odwrotną do $\to$ (odp. $\twoheadrightarrow$). Piszemy $a \downarrow b$ gdy istnieje takie c, że $a \twoheadrightarrow c \twoheadleftarrow b$. Mówimy, że $\to$ ma *własność Churcha-Rossera* (CR), gdy dla dowolnych $a, b, c \in A$

$$\textit{jeśli} \quad b \twoheadleftarrow a \twoheadrightarrow c \quad \textit{to} \quad b \downarrow c.$$

Relacja $\to$ ma *słabą własność Churcha-Rossera* (WCR), gdy dla dowolnych $a, b, c \in A$:

$$\textit{jeśli}\quad b \leftarrow a \rightarrow c \quad \textit{to} \quad b \downarrow c.$$

Zauważmy, że własność CR nie wynika z WCR. Najprostszy przykład jest chyba taki:

$$\bullet \longleftarrow \bullet \longleftrightarrow \bullet \longrightarrow \bullet$$

Fakt 12.18 (Lemat Newmana) *Relacja o własnościach* WCR *i* SN *ma też własność* CR.

Dowód: Załóżmy, że relacja $\rightarrow$ w zbiorze A ma własności WCR i SN. Na początek zauważmy, że relacja $\twoheadleftarrow$ jest dobrze ufundowanym częściowym porządkiem. Istotnie, zwrotność i przechodniość wynikają z samej definicji, a antysymetria z silnej normalizacji. A zatem zbiór $\langle A, \twoheadleftarrow \rangle$ jest dobrze ufundowany i możemy zastosować indukcję ze względu na porządek $\twoheadleftarrow$. Udowodnimy, że każdy element a ma własność:

„Dla dowolnych b, c, jeśli $b \twoheadleftarrow a \twoheadrightarrow c$, to $b \downarrow c$."

Jeśli $a = b$ lub $a = c$ to teza jest oczywista. Załóżmy więc (zob. Rysunek 4), że

$$b \twoheadleftarrow b_1 \leftarrow a \rightarrow c_1 \twoheadrightarrow c.$$

Na mocy WCR jest takie d, że $b_1 \twoheadrightarrow d \twoheadleftarrow c_1$. Z założenia indukcyjnego, zastosowanego do b_1 i c_1 mamy więc $b \twoheadrightarrow e \twoheadleftarrow d \twoheadrightarrow f \twoheadleftarrow c_1$, dla pewnych e, f. Teraz możemy zastosować założenie indukcyjne dla d. Dostaniemy takie g, że $e \twoheadrightarrow g \twoheadleftarrow f$. Ale wtedy także $b \twoheadrightarrow g \twoheadleftarrow c$. ∎

$$\begin{tikzcd}
 & & a \arrow[dl] \arrow[dr] & & \\
 & b_1 \arrow[dl, two heads] \arrow[dr, dashed, two heads] & & c_1 \arrow[dl, dashed, two heads] \arrow[dr, two heads] & \\
b \arrow[dr, dashed, two heads] & & d \arrow[dl, dashed, two heads] \arrow[dr, dashed, two heads] & & c \arrow[dl, dashed, two heads] \\
 & e \arrow[dr, dashed, two heads] & & f \arrow[dl, dashed, two heads] & \\
 & & g & &
\end{tikzcd}$$

Rysunek 4: Dowód lematu Newmana

13 Porządki dobre

Zaczynamy od dwóch nietrywialnych przykładów dobrych porządków.

Fakt 13.1 *Dla dowolnego k, zbiór $\mathbb{N}^k$, złożony z k-elementowych ciągów liczb naturalnych (słów długości k) jest dobrze uporządkowany przez porządek leksykograficzny (wyznaczony przez zwykłe uporządkowanie zbioru $\mathbb{N}$).*

Dowód: Indukcja ze względu na k. Dla $k = 0, 1$, teza jest oczywista. Załóżmy więc, że zbiór $\mathbb{N}^k$ jest dobrze uporządkowany i niech $B \subseteq \mathbb{N}^{k+1}$ będzie niepusty. Przyjmijmy:

- $b = \min\{n \mid \exists w \in B\,(w(0) = n)\}$;
- $B' = \{w \in \mathbb{N}^k \mid bw \in B\}$.

Zbiór B' jest niepustym podzbiorem $\mathbb{N}^k$, ma więc element najmniejszy w. Słowo bw jest wtedy najmniejszym elementem B. ∎

Czasami wygodne jest pojęcie „zbioru z powtórzeniami”, czyli *multizbioru*. Formalnie multizbiory definiujemy jako funkcje. Na przykład multizbiór $\{1, 2, 2, 3, 4, 4, 4\}$ to taka funkcja M, że $M(1) = M(3) = 1$, $M(2) = 2$ i $M(4) = 3$. Dla $x \neq 1, 2, 3, 4$ przyjmujemy $M(x) = 0$.

Definicja 13.2 *Multizbiorem* nad A nazywamy dowolna funkcję $M : A \to \mathbb{N}$.

W stosunku do multizbiorów używamy notacji teoriomnogościowej, pamiętając, że nie należy jej w tym przypadku rozumieć dosłownie. Na przykład piszemy $a \in M$ gdy $M(a) > 0$ oraz $M \subseteq N$ gdy $M(a) \leq N(a)$ dla wszystkich $a \in A$. Możemy też określić działania na multizbiorach, przyjmując

$$(M \cup N)(a) = M(a) + N(a), \text{ oraz } (M - N)(a) = \max\{0, M(a) - N(a)\},$$

dla dowolnego $a \in A$. Powiemy, że multizbiór jest *skończony*, gdy skończony jest zbiór $\{a \in A \mid a \in M\}$.

Niech teraz M, N będą skończonymi multizbiorami nad $\mathbb{N}$. Piszemy $M \to N$, gdy dla pewnych a, N' zachodzi równość $N = (M - \{a\}) \cup N'$, i przy tym $a > b$ dla wszystkich $b \in N'$.

Fakt 13.3 *Relacja $\to$ w zbiorze $\mathcal{M}$ wszystkich skończonych multizbiorów nad $\mathbb{N}$ ma własność silnej normalizacji.*

Dowód: Przypuśćmy, że mamy nieskończony ciąg skończonych multizbiorów

$$M_0 \to M_1 \to M_2 \to \cdots$$

i niech $k = 1 + \max\{n \mid n \in M_0\}$. Nietrudno zauważyć, że we wszystkich multizbiorach M_i występują tylko liczby mniejsze od k. Dla każdego i określimy teraz słowo $w_i \in \mathbb{N}^k$, przyjmując $w_i(j) = M_i(k-j-1)$, dla $j = 0, \ldots, k-1$. Inaczej mówiąc, ciąg w_i składa się z wypisanych od końca wartości wszystkich $M_i(l)$ dla $l = 0, \ldots, k-1$. Na przykład, jesli $k = 4$, oraz $M_i = \{0, 0, 2, 3, 3, 3\}$, to $w_i = \langle 3, 1, 0, 2 \rangle$. Nietrudno zauważyć, że wtedy

$$w_0 > w_1 > w_2 > \cdots$$

w porządku leksykograficznym, więc z Faktu 13.1 otrzymujemy sprzeczność. ∎

Wniosek 13.4 *Zbiór $\mathcal{M}$ wszystkich skończonych multizbiorów nad $\mathbb{N}$ jest dobrze uporządkowany przez relację $\twoheadleftarrow$.*

Dowód: Z Faktu 13.3 łatwo wynika dobre ufundowanie. Sprawdzenie, że porządek jest liniowy, pozostawiamy jako ćwiczenie. ∎

Własności dobrych porządków

Lemat 13.5 *Jeśli A jest zbiorem dobrze uporządkowanym, to każdy właściwy odcinek początkowy w A jest postaci $\mathcal{O}_A(x)$.*

Dowód: Niech B będzie właściwym odcinkiem początkowym w A i niech x będzie najmniejszym elementem zbioru $A - B$. Wówczas $B = \mathcal{O}_A(x)$. Rzeczywiście:

- Jeżeli $b \in B$ to $b < x$, bo inaczej $x \leq b$ i byłoby $x \in B$. Zatem $b \in \mathcal{O}_A(x)$.
- Jeżeli $b \in \mathcal{O}_A(x)$, to $b < x$, więc $b \notin A - B$, czyli $b \in B$. ∎

Lemat 13.6 *Jeśli A jest zbiorem dobrze uporządkowanym, to A nie jest izomorficzny z żadnym swoim właściwym odcinkiem początkowym.*

Dowód: Przypuśćmy, że to nieprawda i niech $x = \min\{y \in A \mid A \approx \mathcal{O}_A(y)\}$. Niech $f : A \to \mathcal{O}_A(x)$ będzie izomorfizmem. Wtedy f obcięte do odcinka $\mathcal{O}_A(x)$ też jest izomorfizmem, a mianowicie izomorfizmem odcinków $\mathcal{O}_A(x)$ i $\mathcal{O}_A(f(x))$. Stąd $A \approx \mathcal{O}_A(f(x))$, a przy tym $f(x) < x$, co jest sprzeczne z minimalnością x. ∎

Morał: Żadne dwa różne odcinki początkowe zbioru dobrze uporządkowanego nie są izomorficzne.

Lemat 13.7 *Niech A i B będą dobrymi porządkami i niech*

$$\forall x{\in}A\,\exists y{\in}B\,(\mathcal{O}_A(x) \approx \mathcal{O}_B(y)).$$

Wtedy A jest izomorficzny z pewnym odcinkiem początkowym zbioru B (być może niewłaściwym).

Dowód: Niech $\Phi = \{\langle x, y\rangle \in A \times B \mid \mathcal{O}_A(x) \approx \mathcal{O}_B(y)\}$. Udowodnimy, że dla dowolnych $\langle x, y\rangle, \langle x', y'\rangle \in \Phi$ zachodzi równoważność:

$$x < x' \quad \Leftrightarrow \quad y < y' \tag{*}$$

($\Rightarrow$) Przypuśćmy, że $x < x'$ ale $y \geq y'$. Niech $f : \mathcal{O}_A(x) \to \mathcal{O}_B(y)$ będzie izomorfizmem. Ponieważ $\mathcal{O}_B(y') \subseteq \mathcal{O}_B(y)$ więc odcinek $\mathcal{O}_B(y')$ jest izomorficzny z odcinkiem $\mathcal{O}_A(f^{-1}(y'))$. Oznacza to jednak, że $\mathcal{O}_A(x) \approx \mathcal{O}_A(f^{-1}(y'))$. Ale $f^{-1}(y') < x$, bo $f^{-1}(y') \in \mathcal{O}_A(x)$, więc mamy sprzeczność z Lematem 13.6: zbiór $\mathcal{O}_A(x)$ jest izomorficzny ze swoim właściwym odcinkiem początkowym.

Część ($\Leftarrow$) warunku (*) można udowodnić podobnie.

Z warunku (*) wynika, że $\Phi : A \xrightarrow{1-1} B$, i że $A \approx \vec{\Phi}(A)$. Pozostaje zauważyć, że $\vec{\Phi}(A)$ jest odcinkiem początkowym w B. Ale jeśli $y \in \vec{\Phi}(A)$ oraz $y' \leq y$, to odcinek $\mathcal{O}_B(y')$ jest izomorficzny z przeciwobrazem $\vec{\Phi}^{-1}(\mathcal{O}_B(y'))$, który jest odcinkiem początkowym w A. A więc $y' \in \vec{\Phi}(A)$ (por. Lemat 13.5). ∎

Twierdzenie 13.8 *Jeśli A i B są dobrze uporządkowane, to jeden z nich jest izomorficzny z odcinkiem początkowym drugiego.*

Dowód: Przypuśćmy, że B nie jest izomorficzny z żadnym właściwym odcinkiem początkowym zbioru A. Przez indukcję ze względu na uporzadkowanie zbioru A pokażemy:

$$\forall x{\in}A\,\exists y{\in}B\,(\mathcal{O}_A(x) \approx \mathcal{O}_B(y)) \tag{**}$$

Niech $x \in A$ i przypuśćmy, że każdy odcinek $\mathcal{O}_A(x')$, gdzie $x' < x$ jest izomorficzny z pewnym $\mathcal{O}_B(y')$. Z lematu 13.7 wnioskujemy, że $\mathcal{O}_A(x)$ jest izomorficzne z pewnym odcinkiem początkowym zbioru B. Nie może to być cały zbiór B, bo założyliśmy, że B nie jest izomorficzny z odcinkami właściwymi w A. A zatem $\mathcal{O}_A(x) \approx \mathcal{O}_B(y)$ dla pewnego y.

Stosując jeszcze raz Lemat 13.7 otrzymujemy, że A jest izomorficzny z jakimś odcinkiem początkowym zbioru B (możliwe, że z całym B). ∎

A zatem uporządkowanie dobre jest pojęciem bardzo jednoznacznym. Dwa dobre porządki albo są izomorficzne, albo jeden z nich jest *dłuższy*. Innych różnic między dobrymi porządkami nie ma.

Teraz jeszcze definicja, która za chwilę będzie przydatna.

Definicja 13.9 Mówimy, że element a zbioru dobrze uporządkowanego jest *graniczny*, gdy nie jest bezpośrednim nastepnikiem innego elementu. W przeciwnym razie element a nazywamy *niegranicznym*.

Twierdzenie o dobrym uporzadkowaniu

Poniższe twierdzenie znacznie ułatwia dowody wielu faktów, pozwala bowiem na postępowanie przez indukcję. Trzeba jednak pamiętać o jego niekonstruktywnym charakterze. Wynika z niego np. że istnieje relacja dobrze porządkująca zbiór liczb rzeczywistych, ale nie wynika, jaka ta relacja naprawdę jest.

Twierdzenie 13.10 (Zermelo) *Każdy zbiór można dobrze uporządkować.*

Dowód: Niech A będzie dowolnym zbiorem i niech Φ będzie funkcją wyboru dla rodziny $\mathbf{P}(A) - \{\emptyset\}$. Powiemy, że zbiór uporządkowany $\langle D, \leq\rangle$ jest *fajny*, gdy $D \subseteq A$, oraz

$$\forall x \in D\,(x = \Phi(A - \mathcal{O}_D(x))).$$

Część 1: Pokażemy najpierw, że jeśli $\langle D_1, \leq_1\rangle$ i $\langle D_2, \leq_2\rangle$ są fajne, to jeden z nich jest (dosłownie) odcinkiem początkowym drugiego.

Dla ustalenia uwagi, załóżmy, że D_2 nie jest właściwym podzbiorem D_1. Przez indukcję ze względu na porządek $\leq_1$ dowodzimy, że dla dowolnego $x \in D_1$:

1) $x \in D_2$;

2) $\mathcal{O}_{D_1}(x) = \mathcal{O}_{D_2}(x)$.

Przypuśćmy, że wszystkie elementy odcinka $\mathcal{O}_{D_1}(x)$ spełniają powyższe warunki. Jeśli x jest graniczny, to mamy $\mathcal{O}_{D_1}(x) = \bigcup\{\mathcal{O}_{D_1}(y) \mid y < x\}$. Z założenia indukcyjnego jest to suma odcinków poczatkowych w D_2, a więc $\mathcal{O}_{D_1}(x)$ też jest odcinkiem początkowym w D_2. Jeśli x jest niegraniczny, to mamy natomiast $\mathcal{O}_{D_1}(x) = \mathcal{O}_{D_1}(x')\cup\{x'\} = \mathcal{O}_{D_2}(x')\cup\{x'\}$, dla odpowiedniego x'. (Skorzystalismy tu z założenia indukcyjnego o x'.) Zbiór $\mathcal{O}_{D_2}(x')\cup\{x'\}$ jest oczywiscie odcinkiem początkowym w D_2.

A więc $\mathcal{O}_{D_1}(x)$ w każdym przypadku jest odcinkiem początkowym w D_2. Jest to odcinek właściwy (bo inaczej $D_2 = \mathcal{O}_{D_1}(x) \subsetneq D_1$) czyli mamy $\mathcal{O}_{D_1}(x) = \mathcal{O}_{D_2}(y)$, dla pewnego y. Ale oba zbiory D_1 i D_2 są fajne, więc $x = \Phi(A - \mathcal{O}_{D_1}(x)) = \Phi(A - \mathcal{O}_{D_2}(y)) = y$, a stąd od razu wynika (1) i (2).

Ponieważ warunki (1) i (2) zachodzą dla wszystkich elementów zbioru D_1, więc $D_1 \subseteq D_2$. Musimy jeszcze sprawdzić, że D_1 jest odcinkiem początkowym w D_2. Niech więc $x \in D_1$

oraz $y < x$ i $y \in D_2$. Wtedy $y \in \mathcal{O}_{D_2}(x) = \mathcal{O}_{D_1}(x)$, w szczególności $y \in D_1$. To kończy część 1 naszego dowodu.

Morał: Jeśli $\langle D_1, \leq_{D_1}\rangle$ i $\langle D_2, \leq_{D_2}\rangle$ są fajne, to warunki $a \leq_{D_1} b$ i $b \leq_{D_2} a$ są równoważne, jesli tylko $a, b \in D_1 \cap D_2$.

Część 2: Następna obserwacja jest taka: suma wszystkich zbiorów fajnych jest fajna. Niech F oznacza tę sumę. Uporządkowanie $\leq_F$ zbioru F można okreslić jako (dosłownie) sumę uporządkowań wszystkich zbiorów fajnych. Sprawdźmy, czy to jest dobre uporządkowanie.

- Zwrotność: Jeśli $a \in F$ to $a \in D$ dla pewnego fajnego $\langle D, \leq_D\rangle$. Wtedy $a \leq_D a$, więc także $a \leq_F a$.
- Antysymetria: Niech $a \leq_F b$ i $b \leq_F a$. To znaczy, że $a \leq_{D_1} b$ i $b \leq_{D_2} a$, dla pewnych fajnych $\langle D_1, \leq_{D_1}\rangle$ i $\langle D_2, \leq_{D_2}\rangle$. Ale jeden z tych zbiorów jest odcinkiem początkowym drugiego, co oznacza, że tak naprawdę zachodzi też np. $a \leq_{D_2} b$. A więc $a = b$.
- Przechodniość: Niech $a \leq_F b$ i $b \leq_F c$. Są więc takie fajne porządki $\langle D_1, \leq_{D_1}\rangle$ i $\langle D_2, \leq_{D_2}\rangle$, że $a \leq_{D_1} b$ i $b \leq_{D_2} c$. Jeden z nich (niech będzie to np. D_1) jest odcinkiem początkowym drugiego, mamy więc $a \leq_{D_2} b$ i $b \leq_{D_2} a$, skąd wnioskujemy $a \leq_{D_2} c$ i wreszcie $a \leq_F c$.
- Spójność: Niech $a, b \in F$. Wtedy $a \in D_1$ i $b \in D_2$ dla pewnych fajnych D_1 i D_2. Jeśli na przykład $D_1 \subseteq D_2$ to elementy a i b są porównywalne w D_2, a więc i w F.
- Dobroć: Rozpatrzmy dowolny niepusty podzbiór $B \subseteq F$. Niech a będzie dowolnym jego elementem i niech D będzie takim fajnym zbiorem, że $a \in D$. Podzbiór $B \cap D$ zbioru D jest niepusty, ma więc element najmniejszy b. Jest to także najmniejszy element zbioru B ze wzgledu na porządek $\leq_F$. Istotnie, niech $c \in B$. Wtedy albo $c \geq_F a \geq_F b$, albo $c \leq_F a$. W tym drugim przypadku $c \in D$, więc także $c \geq_F b$.

Przyjemność sprawdzenia, że porządek $\langle F, \leq_F\rangle$ jest fajny, pozostawiamy czytelnikowi.

Część 3: Zbiór F jest identyczny ze zbiorem A. Rzeczywiscie, przypuśćmy, że $F \neq A$, i niech $a = \Phi(A - F)$. Uporządkowanie zbioru F można teraz rozszerzyć do uporządkowania zbioru $F_1 = F \cup \{a\}$, przyjmując, że a jest elementem najwiekszym. Tak uporządkowany zbiór F_1 jest fajny, ale nie jest zawarty w sumie wszystkich zbiorów fajnych i mamy sprzeczność.

Ostatecznie otrzymujemy, że $\langle A, \leq_F\rangle$ jest zbiorem fajnym, w szczególności jest to zbiór dobrze uporządkowany. ∎

Z twierdzenia 13.10 wynika istotna własność liczb kardynalnych:

Wniosek 13.11 *Dla dowolnych zbiorów A i B zachodzi $\overline{\overline{A}} \leq \overline{\overline{B}}$ lub $\overline{\overline{B}} \leq \overline{\overline{A}}$.*

Dowód: Zbiory A i B można dobrze uporządkować, a wtedy jeden z nich jest izomorficzny z odcinkiem początkowym drugiego. ∎

Możemy teraz udowodnić Twierdzenie 10.13.

Wniosek 13.12 (Lemat Kuratowskiego-Zorna) *Niech $\langle A, \leq \rangle$ będzie porządkiem częściowym, spełniającym następujący warunek:*

Każdy łańcuch ma w A ograniczenie górne

Wtedy w A istnieje element maksymalny.

Dowód: Niech $\preceq$ będzie relacją dobrze porządkującą zbiór A. Bez straty ogólności można założyć, że $\langle A, \preceq \rangle$ nie ma elementu ostatniego (ćwiczenie).

Dla dowolnego $a \in A$ określimy przez indukcję pewien zbiór $Ł_a$, w ten sposób, że:

a) $Ł_a \subseteq \{x \in A \mid x \prec a\}$;

b) $Ł_a$ jest łańcuchem ze względu na porządek $\leq$.

Zakładając, że $Ł_b$ jest już określone dla wszystkich $b \prec a$, definiujemy $Ł_a = \bigcup\{Ł_b \mid b \prec a\}$, gdy a jest elementem granicznym. Jeśli natomiast a jest bezpośrednim nastepnikiem pewnego b, to przyjmujemy:

$$Ł_a = \begin{cases} Ł_b \cup \{b\}, & \text{jeśli } Ł_b \cup \{b\} \text{ jest łańcuchem;} \\ Ł_b, & \text{w przeciwnym przypadku.} \end{cases}$$

Nietrudno sprawdzić, że warunki (a) i (b) są spełnione, i że suma $Ł = \bigcup\{Ł_a \mid a \in A\}$ jest też łańcuchem ze względu na $\leq$. Niech c będzie ograniczeniem górnym łańcucha $Ł$. Twierdzimy, że c jest elementem maksymalnym ze względu na $\leq$.

Istotnie, jeśli $c \leq a$, to a jest porównywalne z każdym elementem zbioru $Ł$, tym bardziej z każdym elementem zbioru $Ł_a$. Wtedy jednak $a \in Ł_b$, gdzie b jest bezpośrednim następnikiem a ze względu na $\preceq$. (Taki bezpośredni następnik istnieje, bo założyliśmy, że elementu ostatniego nie ma.) Ostatecznie wnioskujemy, że $a \in Ł$, czyli $a \leq c$. ∎

Uwaga*: Dowód lematu Kuratowskiego-Zorna ma charakter niekonstruktywny, tj. nie wskazuje elementu maksymalnego, a jedynie uzasadnia jego istnienie. Dowód ten opiera się istotnie na pewniku wyboru. Twierdzenie 10.13 jest w istocie równoważne pewnikowi wyboru.

Podziękowania

Za liczne uwagi, które pomogły usunąć z tych notatek rozmaite błędy, dziękuję Pani Karolinie Sołtys oraz Panom: Jarosławowi Apelskiemu, Łukaszowi Bieniaszowi-Krzywiec, Bartoszowi Dąbrowskiemu, WoJciechowi Dudkowi, Krzysztofowi Gerasowi, Maćkowi Fijałkowskiemu, Mateuszowi Greszcie, Danielowi Hansowi, Szczepanowi Hummelowi, Łukaszowi Kalbarczykowi, Szymonowi Kamińskiemu, Piotrowi Książkowi, Grzegorzowi Leszczyńskiemu, Aleksandrowi Lewandowskiemu, Karolowi Piotrowskiemu, Krzysztofowi Sachanowiczowi, Sławomirowi Sadziakowi, Michałowi Skrzypczakowi, Marcinowi Sulikowskiemu, Michałowi Świtakowskiemu, Szymonowi Toruńczykowi, Wojciechowi Wiśniewskiemu, Maciejowi Zdanowiczowi i dr. Sławomirowi Lasocie.

Ostatnia zmiana 2 stycznia 2008 o godzinie 15:47.