Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Społeczny

Elementarna teoria mnogości

Halszka Tutaj-Gasińska

Kraków, 2021

Spis treści

Wstęp **2**

1 Podstawowe pojęcia logiczne **3**

2 Zbiory i działania na zbiorach **9**

3 Działania uogólnione, rodziny indeksowane **13**

4 Iloczyn kartezjański zbiorów. Relacje i ich własności **17**

5 Funkcje, przykłady. Injekcja, surjekcja, bijekcja, funkcja odwrotna **21**

6 Obrazy, przeciwobrazy i pewne operacje na funkcjach **26**

7 Relacje równoważności, klasy abstrakcji, zbiór ilorazowy **29**

8 Relacje porządku i elementy wyróżnione. **32**

9 Teoria mocy, zbiory przeliczalne **37**

10 Zbiory nieprzeliczalne. Twierdzenie Cantora. Hipoteza continuum **43**

11 Twierdzenie Cantora–Bernsteina **47**

12 Lemat Kuratowskiego–Zorna **49**

13 Pewne zastosowania lematu Kuratowskiego–Zorna. **52**

14 Twierdzenie Zermelo o dobrym uporządkowaniu (i szkic dowodu) **55**

15 Aksjomatyczna konstrukcja liczb naturalnych (dodatek) **59**

Bibliografia **64**

Indeks **65**

Wstęp

Wykład ten opiera się w dużej mierze na ogólnie dostępnych podręcznikach, w szczególności [7] i [4] i zbiorze [8]. Nie ma w nim oryginalnych ujęć pewnych tematów albo dowodów. Jest pomyślany jako pomoc dla studenta, który spotyka się z teorią mnogości w zasadzie po raz pierwszy, stąd dużo dowodów nawet prostych faktów. Całość składa się z piętnastu części – o objętości odpowiadającej mniej więcej dwugodzinnym wykładom. Część pierwsza poświęcona jest pewnym fragmentom logiki matematycznej, niezbędnym w dalszych matematycznych rozważaniach. W kolejnych wykładach omawiane są podstawy teorii zbiorów, relacje (w tym relacje równoważności i klasy abstrakcji), funkcje, relacje porządku i teoria mocy – zbiory skończone, przeliczalne i nieprzeliczalne. Następnie omawiamy lemat Kuratowskiego–Zorna, jego zastosowania oraz twierdzenie Zermelo. Ostatnia część poświęcona jest podstawom aksjomatycznej konstrukcji liczb naturalnych.

Rozdział 1

Podstawowe pojęcia logiczne

Na tym wykładzie omówimy zdania logiczne, tautologie, tabelki wartości logicznych, formy zdaniowe, kwantyfikatory oraz wspomnimy o dowodach formalnych.

Zanim przejdziemy do wykładu, parę słów wstępnych. Każda dyscyplina naukowa posługuje się charakterystycznym dla niej językiem. Język ten jest specyficzny przede wszystkim dlatego, że słowa zaczerpnięte z języka mówionego w słowniku danej dyscypliny mają często znaczenie bardzo zawężone, a czasem całkiem odmienne od znaczenia pierwotnego. Przykładem takiej zmiany znaczenia może być słowo „ciało", które ma inne znaczenie w medycynie, inne w fizyce, i jeszcze inne w matematyce. Takie zawężenie znaczenia, czy nadanie znaczenia całkiem nowego jakiemuś pojęciu nazywamy definiowaniem. Jest rzeczą zrozumiałą, że należy ustalić reguły posługiwania się językiem mówionym w nauce, by nie dochodziło do nieporozumień. Konieczność rozpoczynania wszelkiej nauki od ustalenia takich reguł została dostrzeżona już przez Arystotelesa[1], dając początek dyscyplinie naukowej zwanej dziś logiką (logos oznacza po grecku słowo). Głównym zadaniem logiki jest ustalenie (stworzenie) reguł wnioskowania dla danej dziedziny nauki – na przykład matematyki, prawa, bądź filozofii. Na tym wykładzie zajmiemy się pewnymi fragmentami logiki matematycznej. Na początku wprowadzimy pewne podstawowe pojęcia logiczne, którymi będziemy posługiwać się w dalszych częściach wykładu.

Zacznijmy od pojęcia zdania logicznego.

W języku mówionym zdaniami nazywamy wypowiedzi typu: *dziś jest piątek, czy już wróciłaś do domu?, nie lubię szarlotki, wchodzisz czy wychodzisz? dwa dzieli siedem, Kraków jest miastem.*

Zauważmy, że nie o każdym z tych zdań można powiedzieć, że jest prawdziwe lub fałszywe.

Takie zdanie oznajmujące, któremu (przynajmniej potencjalnie) możemy przyporządkować ocenę - prawda lub fałsz, czyli możemy powiedzieć, czy zdanie jest prawdziwe czy fałszywe, nazywamy zdaniem logicznym.

A zatem, zdanie *czy wróciłaś już do domu?* nie jest zdaniem logicznym, zdanie *dwa dzieli siedem* jest zdaniem logicznym (fałszywym), *Kraków jest miastem* jest zdaniem logicznym prawdziwym, a prawdziwość zdania logicznego *dziś jest piątek* zależy od dnia tygodnia, w którym je wypowiadamy. Ciekawym przykładem jest zdanie *podczas bitwy pod Grunwaldem jednego z rycerzy bolało prawe ucho.* Nikt obecnie nie jest w stanie powiedzieć, czy było tak rzeczywiście, niemniej, potencjalnie, gdybyśmy mogli cofnąć się w czasie i zapytać rycerzy o stan uszu, zdanie uzyskałoby status prawdziwego bądź fałszywego. To zdanie jest zatem zdaniem logicznym.

Zdania logiczne oznaczamy najczęściej małymi literami $p, q, r \ldots$. Mając dane zdanie logiczne p, możemy przyporządkować mu *wartość logiczną*, $w(p)$, gdzie $w(p) = 1$, jeśli p jest zdaniem prawdziwym, $w(p) = 0$, gdy p jest zdaniem fałszywym.

Jeśli za litery $p, q, r, \ldots$ podstawiamy dowolne zdanie logiczne, to mówimy, że $p, q, r, \ldots$ są *zmiennymi zdaniowymi*.

Jeśli mamy dane zdania logiczne, możemy tworzyć nowe zdania logiczne (zwane też *formułami zdaniowymi*), za pomocą *spójników logicznych*, zwanych *spójnikami zdaniotwórczymi*. W języku mówionym też tak, oczywiście, postępujemy, mówiąc na przykład: *dziś jest niedziela i dziś na obiad będą kotlety schabowe* (spójnik „i"), czy też: *sprzedajemy auta na benzynę lub sprzedajemy auta na olej napędowy* (spójnik „lub").

Przy tworzeniu zdań logicznych używamy najczęściej następujących spójników: jednoargumentowego spójnika *zaprzeczenia*, spójników dwuargumentowych: *i*, *lub*, *albo*, *wynika* (*implikuje*), *jest równoważne.* Oznaczamy (i nazywamy) je następująco:

- $\neg$ *zaprzeczenie*, czyli *negacja*
- $\wedge$ *i*, czyli *koniunkcja*

[1] Arystoteles (384–322 p.n.e.), filozof grecki.

- $\vee$ *lub*, czyli *alternatywa*
- $\dot{\vee}$ *albo*, czyli *alternatywa rozłączna*
- $\Longrightarrow$ *wynikanie*, czyli *implikacja*
- $\Longleftrightarrow$ *równoważność.*

Jeśli ze zdań logicznych utworzymy za pomocą spójników nowe zdanie logiczne, to musimy tym nowym zdaniom przypisać wartość logiczną.

Mówiąc bardziej formalnie, spójniki logiczne n-argumentowe możemy traktować jako funkcje, które układowi $(e_1, \dots e_n)$, gdzie $e_j \in \{0, 1\}$ przypisują wartość 0 lub 1.

Trzeba zatem określić jakie wartości przyjmują zdania z wypisanymi wyżej spójnikami. Najwygodniej będzie to zrobić za pomocą tabelek wartości logicznych. Zdanie p może mieć wartość logiczną 0 lub 1, zapisujemy to następująco

p
0
1

Jeśli p ma wartość logiczną 1 (względnie 0), to jego zaprzeczenie, $\neg p$ ma wartość logiczną 0 (względnie 1). Zapisujemy to w tabelce następująco:

p	$\neg p$
0	1
1	0

Przykład 1.1. Zdanie $\neg p$ czytamy jako *nieprawda, że p.* Zdanie *Kraków jest miastem* jest prawdziwe, zdanie *nieprawda, że Kraków jest miastem* jest fałszywe.

Koniunkcja $p \wedge q$ dwóch zdań p i q, jest prawdziwa, tylko jeśli oba są prawdziwe:

p	q	$p \wedge q$
0	0	0
1	0	0
0	1	0
1	1	1

Przykład 1.2. Zdania *dwa dzieli sześć* oraz *trzy dzieli sześć* są oba prawdziwe, zatem prawdziwe też jest zdanie *dwa dzieli sześć i trzy dzieli sześć.*

Alternatywa $p \vee q$ dwóch zdań p i q, jest prawdziwa, jeśli chociaż jedno ze zdań jest prawdziwe:

p	q	$p \vee q$
0	0	0
1	0	1
0	1	1
1	1	1

Przykład 1.3. Zdania *dwa dzieli sześć* oraz *trzy dzieli sześć* są oba prawdziwe, zdanie *cztery dzieli sześć* jest nieprawdziwe. Alternatywy *dwa dzieli sześć lub trzy dzieli sześć* oraz *dwa dzieli sześć lub cztery dzieli sześć* są obie prawdziwe.

Alternatywa rozłączna $p \dot{\vee} q$ dwóch zdań p i q, jest prawdziwa, jeśli dokładnie jedno ze zdań jest prawdziwe:

p	q	$p \dot{\vee} q$
0	0	0
1	0	1
0	1	1
1	1	0

Przykład 1.4. Zdanie $p \dot{\vee} q$ czytamy jako *p albo q*. Tak jak w poprzednim przykładzie, zdania *dwa dzieli sześć* oraz *trzy dzieli sześć* są prawdziwe, a zdanie *cztery dzieli sześć* jest nieprawdziwe, zatem zdanie *dwa dzieli sześć albo trzy dzieli sześć* jest nieprawdziwe, natomiast *dwa dzieli sześć albo cztery dzieli sześć* jest prawdziwe.

Zdanie $p \Longrightarrow q$ nazywamy implikacją. Czytamy *z p wynika q* lub *p implikuje q*. Zdanie p nazywamy *poprzednikiem*, a zdanie q *następnikiem* implikacji. Implikacja jest *fałszywa*, tylko jeśli zdanie p jest prawdziwe, a zdanie q fałszywe (co odzwierciedla rozsądną zasadę, że z prawdziwych przesłanek nie powinny wynikać fałszywe wnioski).

p	q	$p \Longrightarrow q$
0	0	1
1	0	0
0	1	1
1	1	1

Przykład 1.5. Zdanie *Moskwa leży na zachód od Warszawy* jest nieprawdziwe, ale oba zdania: *jeśli Moskwa leży na zachód od Warszawy, to Berlin leży na wschód od Warszawy* oraz *jeśli Moskwa leży na zachód od Warszawy, to Berlin leży na zachód od Warszawy* są prawdziwe. Fałszywe natomiast będzie zdanie *jeśli Moskwa leży na wschód od Warszawy, to Berlin leży na wschód od Warszawy* (poprzednik implikacji jest prawdziwy a następnik fałszywy, implikacja jest wtedy zdaniem fałszywym).

Zdanie $p \iff q$ nazywamy *równoważnością*, czytamy je *p jest równoważne q* lub *p wtedy i tylko wtedy, gdy q*. Równoważność jest prawdziwa, gdy oba zdania mają tę samą wartość logiczną.

p	q	$p \iff q$
0	0	1
1	0	0
0	1	0
1	1	1

Przykład 1.6. Zdanie *dwa dzieli sześć wtedy i tylko wtedy gdy trzy dzieli sześć* jest prawdziwe, zarówno jak zdanie *nieprawda, że dwa dzieli sześć wtedy i tylko wtedy, gdy nieprawda, że trzy dzieli sześć.*

Definicja 1.7. Formuła zdaniowa to wyrażenie utworzone z symboli oznaczających zdania (liter p, q, r najczęściej) i spójników logicznych.

Przykładowo, wyrażenia $p \vee q$, $p \Longrightarrow p$, $p \wedge q \wedge r$ to formuły zdaniowe. Formuły zdaniowe stają się zdaniami gdy za symbole podstawimy konkretne zdania.

Definicja 1.8. Formułę zdaniową nazywamy

- *spełnioną*, jeśli dla danego wartościowania logicznego zmiennych (zdań w tej formule) jest ona prawdziwa (ma wartość logiczną 1);
- *spełnialną*, jeśli dla pewnego wartościowania logicznego zmiennych (zdań w tej formule) jest ona prawdziwa;
- *tautologią*, jeśli dla każdego wartościowania logicznego zmiennych (zdań w tej formule) jest ona prawdziwa;
- *fałszywą*, jeśli dla każdego wartościowania logicznego zmiennych (zdań w tej formule) jest ona fałszywa.

Przykład 1.9. Formuła $p \wedge q$ jest spełnialna (bo jest spełniona gdy $w(p) = w(q) = 1$), ale nie jest tautologią (bo jest fałszywa na przykład gdy $w(p) = 1, w(q) = 0$).

W następnym stwierdzeniu zobaczymy wybrane tautologie rachunku zdań, niektóre z nich mają specjalne nazwy:

Stwierdzenie 1.10.

1. $(\neg(\neg p)) \iff p$ *zasada podwójnej negacji*
2. $(p \wedge q) \iff (q \wedge p)$ *przemienność koniunkcji*
3. $(p \vee q) \iff (q \vee p)$ *przemienność alternatywy*
4. $(p \iff q) \iff (q \iff p)$

5. $((p \vee q) \vee r) \iff (q \vee (p \vee r))$ *łączność alternatywy*

6. $((p \wedge q) \wedge r) \iff (q \wedge (p \wedge r))$ *łączność koniunkcji*

7. $(p \vee (q \wedge r)) \iff ((p \vee q) \wedge (p \vee r))$ *rozdzielność alternatywy względem koniunkcji*

8. $(p \wedge (q \vee r)) \iff ((p \wedge q) \vee (p \wedge r))$ *rozdzielność koniunkcji względem alternatywy*

9. $\neg(p \wedge \neg p)$ *prawo wyłączonej sprzeczności*

10. $p \vee \neg p$ *prawo wyłączonego środka*

11. $(p \Longrightarrow q) \iff (\neg q \Longrightarrow \neg p)$ *prawo kontrapozycji*

12. $(\neg(p \Longrightarrow q)) \iff (p \wedge \neg q)$ *zaprzeczenie implikacji.*

Czytelnik może samodzielnie sprawdzić (na przykład za pomocą tabelek), że wszystkie powyższe zdania są tautologiami. My sprawdzimy tylko wybrane przykłady. Warto może w tym miejscu zwrócić uwagę, że nasze wartościowanie logiczne jest dwuwartościowe (przyjmuje tylko wartości 0 i 1), czyli zdania mogą być tylko albo fałszywe, albo prawdziwe. W życiu oczywiście tak nie jest, zainteresowani mogą poczytać o teorii zbiorów rozmytych i logice wielowartościowej na przykład w książce [1]. W stosowanej do naszych potrzeb logice dwuwartościowej tautologia 9. mówi, że nie może być równocześnie prawdziwe zdanie i jego zaprzeczenie, a 10., że zawsze zachodzi zdanie lub jego zaprzeczenie. Sprawdźmy, że rzeczywiście mamy do czynienia z tautologiami:

p	$\neg p$	$(p \wedge \neg p)$	$\neg(p \wedge \neg p)$
0	1	0	1
1	0	0	1

p	$\neg p$	$(p \vee \neg p)$
0	1	1
1	0	1

Tautologia 11. służy do dowodzenia nie wprost (zakładamy, że zdanie p jest prawdziwe; zamiast dowodzić, że ze zdania p wynika zdanie q, możemy założyć, że zachodzi zdanie $\neg q$ i wykazać, że wtedy zachodzi zdanie $\neg p$; niektórzy być może spotkali się z podobnym rozumowaniem przy dowodzie, że pierwiastek z 2 jest liczbą niewymierną.)

p	q	$\neg p$	$\neg q$	$p \Longrightarrow q$	$\neg q \Longrightarrow \neg p$	$(p \Longrightarrow q) \iff (\neg q \Longrightarrow \neg p)$
0	0	1	1	1	1	1
1	0	0	1	0	0	1
0	1	1	0	1	1	1
1	1	0	0	1	1	1

Sprawdźmy jeszcze, że zaprzeczenie implikacji równoważne jest koniunkcji poprzednika i zaprzeczenia następnika tej implikacji:

p	q	$\neg q$	$p \Longrightarrow q$	$\neg(p \Longrightarrow q)$	$p \wedge \neg q$	$(\neg(p \Longrightarrow q)) \iff (p \wedge \neg q)$
0	0	1	1	0	0	1
1	0	1	0	1	1	1
0	1	0	1	0	0	1
1	1	0	1	0	0	1

Osobno wypiszemy dwie ważne tautologie, zwane prawami de Morgana[2].

Stwierdzenie 1.11 (Prawa de Morgana)**.** *Dla dowolnych zdań p, q następujące formuły są zawsze prawdziwe*

1. $(\neg(p \vee q)) \iff (\neg p \wedge \neg q)$
(zaprzeczenie alternatywy jest równoważne koniunkcji zaprzeczeń)

2. $(\neg(p \wedge q)) \iff (\neg p \vee \neg q)$
(zaprzeczenie koniunkcji jest równoważne alternatywie zaprzeczeń)

[2] Augustus de Morgan (1806–1871), angielski matematyk i logik.

Dowód. Faktycznie,

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$	$(\neg(p \vee q)) \iff (\neg p \wedge \neg q)$
0	0	1	1	0	1	1	1
1	0	0	1	1	0	0	1
0	1	1	0	1	0	0	1
1	1	0	0	1	0	0	1

p	q	$\neg p$	$\neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$	$(\neg(p \wedge q)) \iff (\neg p \vee \neg q)$
0	0	1	1	0	1	1	1
1	0	0	1	0	1	1	1
0	1	1	0	0	1	1	1
1	1	0	0	1	0	0	1

□

Wprowadzimy teraz pojęcie funkcji zdaniowej. Aby je wprowadzić formalnie potrzebujemy pojęcia zbioru, które pojawi się na następnym wykładzie. Ponieważ jednak pojęcie zbioru jest pojęciem pierwotnym – czyli nie definiuje się go – zakładając, że każdy „intuicyjnie wie co to jest", możemy już teraz powiedzieć, że bierzemy dowolny niepusty zbiór X.

Definicja 1.12. *Funkcją zdaniową jednej zmiennej x* nazywamy wyrażenie $\varphi(x)$, które staje się zdaniem logicznym jeśli za zmienną x podstawimy element zbioru X. Zbiór X nazywamy *zakresem zmienności* funkcji φ.

Mówimy, że x *spełnia* $\varphi(x)$, jeśli $w(\varphi(x)) = 1$. Sbiór x spełniających $\varphi(x)$ zapisujemy jako $\{x \in X : \varphi(x)\}$.

W życiu dość często spotykamy funkcje zdaniowe. Na przykład w teście z historii możemy zobaczyć wyrażenie: „W roku 1656 królem Polski był .....", i w zależności od tego, czy wpiszemy zamiast kropek Jana Kazimierza czy Jana III Sobieskiego, dostajemy zdanie prawdziwe albo fałszywe. Naturalnym zakresem zmienności tej funkcji zdaniowej jest oczywiście zbiór królów Polski.

Oto bardziej matematyczny przykład:

Przykład 1.13. Niech $X = \mathbb{R}$. Jeśli napiszemy $x^2 > 1$, to mamy funkcję zdaniową (o zakresie zmienności $\mathbb{R}$), o wyrażeniu $x^2 > 1$ nie możemy powiedzieć, czy jest prawdziwe, czy fałszywe, póki nie podstawimy za x konkretnej liczby rzeczywistej. Zbiór x spełniających $x^2 > 1$, czyli $\{x \in \mathbb{R} : x^2 > 1\}$, to $\mathbb{R} \setminus [-1, 1]$ i faktycznie, podstawiając x z tego zbioru do wyrażenia $x^2 > 1$, dostajemy zdanie prawdziwe.

Funkcje zdaniowe (o tym samym zakresie zmienności) możemy łączyć omówionymi wyżej spójnikami logicznymi. Innym rodzajem operacji logicznych, które możemy zastosować do funkcji zdaniowych, są *kwantyfikatory*. Kwantyfikatory możemy traktować jako operacje, które z funkcji zdaniowej tworzą zdanie, czyli tak zwane *funktory zdaniotwórcze*. Kwantyfikatory, których będziemy używać, są następujące.

Definicja 1.14. Niech $\varphi(x)$ będzie funkcją zdaniową o zakresie zmienności X.

- $\forall_{x \in X}\ \varphi(x)$ oznacza: *dla każdego $x \in X$ zachodzi $\varphi(x)$*; kwantyfikator $\forall$ nazywa się czasem *dużym kwantyfikatorem* albo *kwantyfikatorem ogólnym, uniwersalnym*.
- $\exists_{x \in X}\ \varphi(x)$ oznacza: *istnieje $x \in X$, takie, że zachodzi $\varphi(x)$*; kwantyfikator $\exists$ nazywamy *małym kwantyfikatorem* albo *kwantyfikatorem szczegółowym, egzystencjalnym*.

Przykład 1.15. Wyrażenie $x^2 > 1$ nie jest zdaniem, ale wyrażenie $\forall_{x \in \mathbb{R}}\ x^2 > 1$ jest już zdaniem logicznym (fałszywym). Podobnie, $x^2 \geqslant 0$ nie jest zdaniem logicznym, ale $\forall_{x \in \mathbb{R}}\ x^2 \geqslant 0$ jest zdaniem prawdziwym.

Uwaga 1.16. 1. Nieformalnie mówiąc, możemy patrzeć na kwantyfikatory jako na pewnego rodzaju skrócony zapis: $\forall_{x \in X}\ \varphi(x)$ zastępuje $\varphi(x_1) \wedge \varphi(x_2) \wedge \ldots$, gdzie x_i przebiega wszystkie x w X, a $\exists_{x \in X}\ \varphi(x)$ zastępuje $\varphi(x_1) \vee \varphi(x_2) \vee \ldots$, gdzie znów x_i przebiega wszystkie x w X. Dlatego też spotyka się zapis $\bigwedge$ jako $\forall$ oraz $\bigvee$ jako $\exists$.

2. Wiele kwantyfikatorów tego samego rodzaju często łączy się w jeden. Tak więc zapis $\forall_{x,y \in \mathbb{R}}$ znaczy to samo, co $\forall_{x \in \mathbb{R}} \forall_{y \in \mathbb{R}}$.

3. Jeśli zbiór $A \subset X$ i chcemy powiedzieć, że dla każdego elementu z A zachodzi $\varphi(x)$, to zamiast zapisu $\forall_{x \in X}\ x \in A \implies \varphi(x)$ stosujemy skrócony zapis $\forall_{x \in A}\ \varphi(x)$. Podobnie postępujemy dla pozostałych kwantyfikatorów. Niekiedy brak kwantyfikatora rozumiemy jako duży kwantyfikator, na przykład w wyrażeniu $x^2 = y^2 \implies (x = y \vee x = -y)$ opuszczone jest $\forall_{x,y \in \mathbb{R}}$.

4. Oczywiście, zdania możemy tworzyć przy pomocy więcej niż jednego kwantyfikatora, na przykład: $\forall_{x\in\mathbb{N}}\,\exists_{y\in\mathbb{N}}\,x<y$ to zdanie logiczne (prawdziwe).

5. Tworząc zdania z kwantyfikatorami, należy zwracać uwagę na kolejność kwantyfikatorów. Zdanie *dla każdego studenta istnieją spodnie, które nosi* znaczy zupełnie coś innego, niż zdanie *istnieją spodnie, które nosi każdy student.*

6. Używa się również zapisu $\forall!_{x\in X}$ i $\exists!_{x\in X}$. Ten pierwszy czytamy „dla prawie wszystkich $x\in X$" (czyli dla wszystkich poza skończoną liczbą), $\forall!_{x\in X}\varphi(x)$ jest skróconą formą zapisu „istnieje zbiór S taki, że S ma skończenie wiele elementów i dla każdego $x\in X\setminus S$ zachodzi $\varphi(x)$. Natomiast zapis $\exists!_{x\in X}\varphi(x)$ oznacza, że istnieje dokładnie jeden $x\in X$ taki, że zachodzi $\varphi(x)$. Jest to skrócony zapis zdania „istnieje $x\in X$ taki, że zachodzi $\varphi(x)$ i dla dowolnego $y\in X$ jeśli zachodzi $\varphi(y)$ to $y=x$. Piszemy też $\exists_{x\in X}:\varphi(x)$ i czytamy: istnieje x należący do X, taki, że zachodzi $\varphi(x)$.

Zaprzeczeniami zdań z kwantyfikatorami rządzą prawa zwane *prawami de Morgana dla kwantyfikatorów*:

Stwierdzenie 1.17 (Prawa de Morgana dla kwantyfikatorów)**.** *Niech $\varphi(x)$ będzie formą zdaniową o zakresie zmienności X.*

- $\neg(\forall_{x\in X}\ \varphi(x)) \iff (\exists_{x\in X}\ \neg\varphi(x))$
- $\neg(\exists_{x\in X}\ \varphi(x)) \iff (\forall_{x\in X}\ \neg\varphi(x))$

Przykład 1.18. Zaprzeczając zdaniu $\forall_{x\in\mathbb{R}}\ x^2>0$, dostajemy zdanie $\exists_{x\in\mathbb{R}}\ x^2\leqslant 0$.

Poniższe stwierdzenie podaje pewne prawa dla zdań z kwantyfikatorami.

Stwierdzenie 1.19. *Niech $\varphi(x)$ i $\psi(x)$ będą formami zdaniowymi o zakresie zmienności X.*

1. $\exists_{x\in X}\ (\varphi(x)\vee\psi(x)) \iff \exists_{x\in X}\ \varphi(x)\vee\exists_{x\in X}\ \psi(x)$
2. $\forall_{x\in X}\ (\varphi(x)\wedge\psi(x)) \iff \forall_{x\in X}\ \varphi(x)\wedge\forall_{x\in X}\psi(x)$
3. $\exists_{x\in X}\ (\varphi(x)\wedge\psi(x)) \implies \exists_{x\in X}\ \varphi(x)\wedge\exists_{x\in X}\ \psi(x)$
4. $\forall_{x\in X}\ \varphi(x)\vee\forall_{x\in X}\psi(x) \implies \forall_{x\in X}\ (\varphi(x)\vee\psi(x))$

Uwaga 1.20. Zwróćmy uwagę, że w punktach 3. i 4. mamy wynikanie tylko w jedną stronę. Wynikanie w drugą stronę nie musi zachodzić. Weźmy zdanie *istnieje człowiek, który jest mężem Małgosi i istnieje człowiek, który jest mężem Kasi* (to prawa strona 3.). Nie wynika z tego jednak, że *istnieje człowiek, który jest mężem Małgosi i mężem Kasi* (lewa strona 3.). Podobnie dla 4., weźmy zdanie *każda liczba rzeczywista jest większa od* 2 *lub mniejsza lub równa od* 2*,* z tego nie wynika, że *każda liczba rzeczywista jest większa od* 2 *lub każda liczba rzeczywista jest mniejsza lub równa* 2*.*

Na zakończenie tego wykładu powiedzmy kilka słów o dowodach formalnych. Niech dane będą zdania $p_1,\dots,p_n$, które nazwiemy *założeniami*, i zdanie q, które nazwiemy *tezą*. Postać twierdzeń matematycznych to najczęściej implikacja postaci $(p_1\wedge p_2\wedge\dots\wedge p_n)\implies q$. Chcemy udowodnić prawdziwość tej implikacji. Oczywiście dowód jest interesujący tylko w przypadku, gdy każde ze zdań p_i jest prawdziwe. Dowód formalny tej implikacji to ciąg składający się ze zdań, z których każde jest założeniem lub tautologią lub wnioskiem z poprzednich wyrażeń powstałym przy pomocy *reguł wnioskowania*. Reguły wnioskowania to pewne tautologie, przykładowo:

- reguła zwana *modus ponendo ponens*, czyli *sposób potwierdzający przez potwierdzenie*, to $(p\wedge(p\implies q))\implies q$
- reguła zwana *modus tollendo tollens*, czyli *sposób zaprzeczający przez zaprzeczenie*, to $((p\implies q)\wedge\neg q)\implies(\neg p)$
- sylogizm hipotetyczny to $((p\implies q)\wedge(q\implies r))\implies(p\implies r)$
- sylogizm alternatywny $((p\vee q)\wedge(\neg p))\implies q$
- dowód nie wprost $((p\wedge\neg q)\implies(r\wedge\neg r))$

Warto, jako ćwiczenie, sprawdzić, że powyższe reguły są tautologiami. Trzecia z tautologii to inaczej *prawo przechodniości implikacji.*

Uwaga 1.21. Warto też przyjrzeć się ostatniej z tych reguł. Opisuje ona sposób rozumowania przy dowodzeniu nie wprost. W dowodzie prowadzonym nie wprost przypuszczamy, że implikacja $p\implies q$ nie zachodzi. Zachodzi zatem jej zaprzeczenie, $p\wedge\neg q$. Jeśli z tego zaprzeczenia wyniknie sprzeczność $(r\wedge\neg r)$, to znaczy, że przypuszczenie nie mogło być prawdziwe.

Rozdział 2

Zbiory i działania na zbiorach

Na tym wykładzie omówimy pojęcia zbioru i elementu zbioru, operacje na zbiorach, dowody równości zbiorów, uzupełnienie, prawa de Morgana, zbiór pusty; wspomnimy o aksjomatach teorii mnogości.

Pojęcie *zbioru* i pojęcie *należenia do zbioru* to pojęcia pierwotne, nie definiujemy ich, przyjmując, że każdy intuicyjnie je rozumie. (Z wyrażeniem *pojęcie pierwotne* czytelnik prawdopodobnie już się spotkał na szkolnych lekcjach geometrii – pojęciami pierwotnymi były prosta lub punkt). Zbiory najczęściej oznaczamy dużymi literami $A, B, C, \ldots X, Y, Z$. Pojawią się też w dalszych wykładach szczególne zbiory – zbiór liczb naturalnych, całkowitych, wymiernych i rzeczywistych, oznaczane odpowiednio $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. Fakt, że *element a należy do zbioru A*, zapisujemy $a \in A$. Jeśli *a nie należy do A*, piszemy $\neg(a \in A)$ albo (częściej) $a \notin A$. Jeśli z jakiś powodów chcemy napisać najpierw zbiór, a potem element do niego należący, piszemy $A \ni a$.

Symbolem $\varnothing$ oznaczamy *zbiór pusty*, czyli taki, do którego nie należy żaden element. Dla działań na zbiorach (zobacz poniżej) zbiór pusty odgrywa rolę podobną jak zero w arytmetyce.

Zbiory zwane były dawniej *mnogościami*, stąd *teoria mnogości* to inaczej nazwana teoria zbiorów.

Zacznijmy od definicji pewnych operacji na zbiorach i zależności między zbiorami:

Definicja 2.1. Niech A, B będą zbiorami.

- *Suma zbiorów* A i B to zbiór $A \cup B$, do którego należą wszystkie elementy zbioru A, wszystkie elementy zbioru B i żadne inne.
- *Iloczyn* (*przecięcie*, *część wspólna*) zbiorów A i B to zbiór $A \cap B$ złożony z tych elementów zbiorów A i B, które należą i do A i do B.
- *Różnica zbiorów* A i B to zbiór $A \setminus B$, złożony z tych i tylko tych elementów zbioru A, które nie należą do B.
- Mówimy, że *zbiór A zawiera się w zbiorze B*, co zapisujemy $A \subset B$ jeśli każdy element zbioru A jest też elementem zbioru B.
- Zbiory A i B są *równe* (co zapisujemy $A = B$), jeśli $A \subset B$ i $B \subset A$.

Możemy powyższą definicję zapisać także następująco:

$$\begin{aligned} x \in A \cup B &\iff x \in A \vee x \in B \\ x \in A \cap B &\iff x \in A \wedge x \in B \\ x \in A \setminus B &\iff x \in A \wedge \neg(x \in B) \\ A \subset B &\iff (x \in A \Longrightarrow x \in B) \\ A = B &\iff ((x \in A \Longrightarrow x \in B) \wedge (x \in B \Longrightarrow x \in A) \end{aligned}$$

Ostatnia formuła dla równości nie jest ściśle formalna (patrz aksjomat ekstensjonalności na końcu rozdziału), ale użyteczna.

Wypiszemy teraz pewne własności operacji $\cap, \cup, \setminus$:

Stwierdzenie 2.2. *Niech A, B, C będą zbiorami.*

1. $A \cap B = B \cap A$ *(przemienność iloczynu zbiorów)*
2. $A \cup B = B \cup A$ *(przemienność sumy zbiorów)*
3. $A \cup (B \cup C) = (A \cup B) \cup C$ *(łączność sumy zbiorów)*
4. $A \cap (B \cap C) = (A \cap B) \cap C$ *(łączność iloczynu zbiorów)*
5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *(rozdzielność iloczynu względem sumy zbiorów)*
6. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *(rozdzielność sumy względem iloczynu zbiorów)*
7. $A \cap B = A \setminus (A \setminus B)$
8. $A \cup B = A \cup (B \setminus A)$
9. $A \setminus (A \cap B) = A \setminus B$
10. $A \cap (B \setminus C) = (A \cap B) \setminus C$

Dowód. W każdej z równości będziemy wykazywać, że x należy do prawej strony wtedy i tylko wtedy, gdy należy do lewej. Bez dodatkowych wyjaśnień korzystamy z definicji sumy, przecięcia, różnicy zbiorów. Warto zwrócić uwagę, że dowody powyższych własności są analogiczne do dowodów własności ze stwierdzenia 1.10.

ad 1. $x \in A \cap B \iff (x \in A) \wedge (x \in B) \overset{1,10,2.}{\iff} (x \in B) \wedge (x \in A) \iff x \in B \cap A$

ad 2. $x \in A \cup B \iff (x \in A) \vee (x \in B) \overset{1,10,3.}{\iff} (x \in B) \vee (x \in A) \iff x \in B \cup A$

ad 3. $x \in A \cup (B \cup C) \iff x \in A \vee (x \in B \cup C) \iff x \in A \vee (x \in B \vee x \in C) \overset{1,10,5.}{\iff} (x \in A \vee x \in B) \vee x \in C \iff (x \in A \cup B) \vee x \in C \iff x \in (A \cup B) \cup C$

ad 4. $x \in A \cap (B \cap C) \iff x \in A \wedge (x \in B \cap C) \iff x \in A \wedge (x \in B \wedge x \in C) \overset{1,10,6.}{\iff} (x \in A \wedge x \in B) \wedge x \in C \iff (x \in A \cap B) \wedge x \in C \iff x \in (A \cap B) \cap C$

ad 5. $x \in A \cap (B \cup C) \iff x \in A \wedge (x \in B \cup C) \iff x \in A \wedge (x \in B \vee x \in C) \overset{1,10,8.}{\iff} (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \iff x \in (A \cap B) \cup (A \cap C)$

ad 6. $x \in A \cup (B \cap C) \iff x \in A \vee (x \in B \cap C) \iff x \in A \vee (x \in B \wedge x \in C) \overset{1,10,7.}{\iff} (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \iff x \in (A \cup B) \cap (A \cup C)$

ad 7. $x \in A \cap B \iff x \in A \wedge x \in B \iff (x \in A \wedge \neg(x \in A)) \vee (x \in A \wedge \neg(\neg(x \in B)) \iff x \in A \wedge \neg(x \in A \wedge \neg(x \in B)) \iff x \in A \wedge \neg(x \in (A \setminus B)) \iff x \in A \setminus (A \setminus B)$, gdzie druga równoważność wynika z faktu, że zdanie $(x \in A \wedge \neg(x \in A))$ jest zawsze fałszywe (prawo wyłączonej sprzeczności 1.10.9.), zatem prawdziwość alternatywy zależy od drugiego ze zdań alternatywy, a zdanie $\neg(\neg(x \in B))$ jest równoważne zdaniu $x \in B$.

ad 8. $x \in A \cup (B \setminus A) \iff x \in A \vee x \in (B \setminus A) \iff x \in A \vee (x \in B \wedge \neg(x \in A)) \overset{1,10,7.}{\iff} (x \in A \vee x \in B) \wedge (x \in A \vee (\neg(x \in A))) \iff (x \in A \vee x \in B) \iff x \in A \cup B$, gdzie przedostatnia równoważność wynika z faktu, że zdanie $x \in A \vee (\neg(x \in A))$ jest zawsze prawdziwe (por. zasada wyłączonego środka 1.10.10.).

ad 9. $x \in A \wedge \neg(x \in A \cap B) \iff x \in A \wedge (x \notin A \vee x \notin B) \iff (x \in A \wedge x \notin A) \vee (x \in A \wedge x \notin B) \iff x \in A \wedge x \notin B \iff x \in A \setminus B$, gdzie przedostatnią równoważność uzasadniamy tak jak w punkcie 8.

ad 10. $x \in A \cap (B \setminus C) \iff x \in A \wedge (x \in B \setminus C) \iff x \in A \wedge (x \in B \wedge x \notin C) \overset{1,10,6.}{\iff} (x \in A \wedge x \in B) \wedge x \notin C \iff x \in A \cap B \wedge x \notin C \iff x \in (A \cap B) \setminus C.$ □

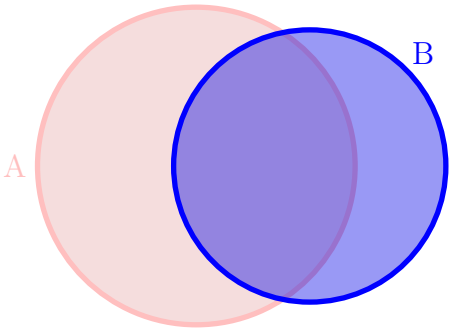
Uwaga 2.3. Do obrazowania pewnych zależności między zbiorami można używać *diagramów Venna*[1]. Przykład takiego diagramu dla dwóch zbiorów A, B widzimy na rysunku 2.1. Na rysunku zbiory są w położeniu ogólnym ogólne, mogą więc na przykład posłużyć do graficznego dowodu, że $A \setminus B = A \setminus (A \cap B)$ oraz do zobrazowania przykładu, że $A \cup (A \setminus B) \neq A \setminus (A \cap B)$. Więcej o ogólnym położeniu i dowodzeniu przy pomocy diagramów Venna Czytelnik może znaleźć w [4] albo na stronie

`http://www.deltami.edu.pl/temat/matematyka/teoria_mnogosci/2011/02/12/Diagramy_Venna/`

Wykażemy teraz, że zbiór pusty jest tylko jeden. Przypomnijmy, że zbiór pusty to taki zbiór, w którym nie ma żadnego elementu. Równoważnie, możemy postawić definicję

[1] John Venn (1834–1923), angielski matematyk, logik i filozof.

Rysunek 2.1:



Definicja 2.4. *Zbiór pusty* to zbiór, który zawiera się w każdym zbiorze.

Te dwa sposoby zdefiniowania zbioru pustego są równoważne. Faktycznie, jeśli w $\varnothing$ nie ma żadnego elementu, to spełniona jest implikacja $x \in \varnothing \implies x \in A$ (poprzednik jest fałszywy). Niech teraz zbiór $\varnothing$ zawiera się w każdym zbiorze. Gdyby istniał $x \in \varnothing$, to biorąc zbiór $A = \{y\}$, gdzie $y \neq x$, dostajemy $x \in A$, czyli $x = y$, sprzeczność.

Stwierdzenie 2.5. *Jest tylko jeden zbiór pusty.*

Dowód. Przypuśćmy, że są dwa zbiory puste $\varnothing_1$ i $\varnothing_2$. Wykażemy, że są równe. Ponieważ $\varnothing_1$ jest zbiorem pustym, $\varnothing_1 \subset \varnothing_2$ (bo zbiór pusty zawiera się w każdym zbiorze). Analogicznie, skoro $\varnothing_2$ jest zbiorem pustym, to $\varnothing_2 \subset \varnothing_1$. Stąd dostajemy, że $\varnothing_1 = \varnothing_2$. □

Sformułujemy teraz i wykażemy *prawa de Morgana dla zbiorów.*

Stwierdzenie 2.6 (Prawa de Morgana dla zbiorów)**.** *Niech dane będą zbiory A, B, X. Wówczas*

1. $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$
2. $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$

Dowód. Dla każdej z równości wykażemy, że x należy do lewej strony wtedy i tylko wtedy, gdy x należy do prawej.
ad 1. $x \in X \setminus (A \cup B) \iff x \in X \wedge \neg(x \in A \cup B) \overset{1.11.1}{\iff} x \in X \wedge \neg(x \in A) \wedge \neg(x \in B) \iff x \in X \setminus A \wedge x \in X \setminus B \iff x \in (X \setminus A) \cap (X \setminus B)$.
ad 2. $x \in X \setminus (A \cap B) \iff x \in X \wedge \neg(x \in A \cap B) \overset{1.11.2}{\iff} x \in X \wedge (\neg(x \in A) \vee \neg(x \in B)) \iff x \in (X \setminus A) \vee x \in (X \setminus B) \iff x \in (X \setminus A) \cup (X \setminus B)$. □

Rozważmy teraz następującą sytuację. Mamy dany, ustalony zbiór X (zwany czasem *przestrzenią*). Zbiory A, B są podzbiorami zbioru X.

Definicja 2.7. *Uzupełnieniem zbioru A* nazywamy zbiór $A^c := X \setminus A = \{x \in X : x \notin A\}$.

Uwaga 2.8.

$$\varnothing^c = X, \quad X^c = \varnothing$$

Prawa de Morgana możemy teraz zapisać następująco:

Stwierdzenie 2.9. *Niech dane będą zbiory A, B, X. Wówczas*

1. $(A \cup B)^c = A^c \cap B^c$
2. $(A \cap B)^c = A^c \cup B^c$

Powiemy teraz kilka słów o aksjomatach teorii mnogości. Początkowo teorię mnogości rozwijano intuicyjnie (tak, jak my w tym wykładzie). Pod koniec XIX wieku zaczęło się stawać oczywiste, że takie intuicyjne podejście do tej teorii nie wystarczy. Intuicyjnie chcielibyśmy na przykład definiować zbiory przez podanie jaką własność spełniają jego elementy, przykładowo $\{x \in \mathbb{R} : x > 1\}$ to zbiór liczb rzeczywistych większych od 1. Ogólnie $\{x : \varphi(x)\}$ to zbiór

x spełniających własność φ. Wygląda to na pozór w porządku, ale weźmy teraz zbiór Z zdefiniowany jako zbiór tych zbiorów, które nie są swoimi elementami:

$$Z = \{A : A \notin A\}.$$

Czy sam zbiór Z jest elementem zbioru Z? Jeśli zbiór Z należy do Z, to z określenia zbioru Z mamy $Z \notin Z$. Jeśli natomiast $Z \notin Z$, to znowu z określenia zbioru Z mamy $Z \in Z$. Zatem dostajemy:

$$Z \in Z \iff Z \notin Z,$$

sprzeczność. Powyższy problem zwany jest *antynomią Russela*[2]. Być może niektórym czytelnikom ta antynomia znana jest w wersji:
Fryzjer z pewnego miasta strzyże tych jego mieszkańców, którzy sami się nie strzygą. Czy fryzjer strzyże się sam?
Ta antynomia (jak i inne, o których wspomnimy w dalszych wykładach) dała impuls do stworzenia teorii mnogości opartej na aksjomatach. Obecnie jako *aksjomaty teorii mnogości* przyjmuje się zestaw aksjomatów zaproponowanych w I połowie XX wieku przez Zermelo[3] i Fraenkla[4]. Podamy tylko niektóre z nich, zaznaczając, że nie jest to też zestaw minimalny (to znaczy możemy niektóre aksjomaty wywnioskować z innych).

- *Aksjomat istnienia*: Istnieje co najmniej jeden zbiór.
- *Aksjomat ekstensjonalności* (jednoznaczności): Jeśli A i B mają te same elementy, to są identyczne.
- *Aksjomat zbioru pustego*: Istnieje zbiór, który nie ma żadnego elementu.
- *Aksjomat sumy*: Dla dowolnych zbiorów A i B istnieje zbiór, którego elementami są wszystkie elementy zbioru A, wszystkie elementy zbioru B i żadne inne.
- *Aksjomat różnicy*: Dla dowolnych zbiorów A i B istnieje zbiór, którego elementami są te i tylko te elementy zbioru A, które nie są elementami zbioru B.
- *Aksjomat zbioru potęgowego*: Dla każdego zbioru X istnieje zbiór, oznaczany $\mathcal{P}(X)$ (albo 2^X), którego elementami są podzbiory zbioru X, czyli $\mathcal{P}(X) = \{Z : Z \subset X\}$.
- *Aksjomat wyróżniania*: Dla każdej formuły $\varphi(x)$ i dla każdego zbioru A istnieje zbiór złożony dokładnie z tych elementów zbioru A, które spełniają $\varphi(x)$. (Zauważmy, że stąd wynika istnienie zbioru jednoelementowego $\{a\}$, bo $\{a\} = \{x : x \in A \wedge x = a\}$.)

Później poznamy jeszcze aksjomat zwany *aksjomatem nieskończoności*. Poniżej, osobno wypiszemy jeszcze jeden aksjomat, z którego będziemy korzystać wielokrotnie. Jest *aksjomat wyboru*, zwany także *pewnikiem wyboru*.

• **Pewnik wyboru:** Dla każdej rodziny $\mathcal{R}$ zbiorów niepustych i parami rozłącznych istnieje zbiór, który ma z każdym ze zbiorów z rodziny $\mathcal{R}$ dokładnie jeden element wspólny (czyli z każdego z tych zbiorów możemy wybrać po jednym elemencie).

Wybiegając naprzód powiedzmy, że aksjomatu tego będziemy używać w następującej wersji:
Dla każdej rodziny $\mathcal{R}$ zbiorów niepustych istnieje funkcja $g : \mathcal{R} \to \bigcup \mathcal{R}$, taka, że dla każdego $R \in \mathcal{R}$ mamy $g(R) \in R$.

Pojęcia funkcji i sumy rodziny zbiorów $\bigcup \mathcal{R}$ pojawią się wkrótce.

[2] Bertrand Russell (1872–1970), brytyjski filozof, logik, matematyk
[3] Ernst Zermelo (1871–1953), niemiecki matematyk.
[4] Abraham Fraenkel (1891–1965), niemiecko-izraelski matematyk.

Rozdział 3

Działania uogólnione, rodziny indeksowane

Na tym wykładzie wprowadzimy pojęcie rodziny zbiorów i indeksowanej rodziny zbiorów. Zdefiniujemy sumę i przecięcie rodzin zbiorów oraz przedstawimy pewne własności tych operacji. Powiemy też parę słów o iloczynie kartezjańskim dwóch zbiorów.

W zasadzie ten wykład powinien zostać przedstawiony po formalnym wprowadzeniu pojęcia funkcji. Czytelnik, który nie zna tego pojęcia, może pominąć ten wykład i wrócić do niego po definicji 5.1.

Niech dany będzie niepusty zbiór T (zwany *zbiorem wskaźników*). Niech Y będzie dowolnym zbiorem. Przypomnijmy, że przez $\mathcal{P}(Y)$ oznaczamy zbiór podzbiorów zbioru Y.

Niech dana będzie funkcja $F : T \to \mathcal{P}(Y)$. Zwyczajowo $F(t)$ zapisujemy jako F_t, gdzie $t \in T$.

Definicja 3.1. Zbiór $\{F_t : t \in T\}$ nazywamy *indeksowaną rodziną zbiorów*.

Przykład 3.2. Niech $T = \{2, 3, 4\}$. Zbiór F_t zdefiniujmy jako przedział $[1, t) \subset \mathbb{R}$, gdzie $t \in T$, czyli

$$F_t = [1, t) = \{x \in \mathbb{R} : 1 \leqslant x < t\}.$$

Rodzina składa się z trzech zbiorów: $[1, 2), [1, 3), [1, 4)$.

Zdefiniujmy teraz sumę i przecięcie (iloczyn) takiej rodziny.

Definicja 3.3. $\bigcup_{t\in T} F_t$ to *suma zbiorów* F_t gdzie $t \in T$ zdefiniowana następująco:

$$x \in \bigcup_{t\in T} F_t \iff \exists_{t\in T}\ x \in F_t.$$

Ta definicja mówi, że x należy do sumy zbiorów F_t jeśli należy do przynajmniej jednego z nich.

Definicja 3.4. $\bigcap_{t\in T} F_t$ to *przecięcie zbiorów* F_t, gdzie $t \in T$ zdefiniowane następująco:

$$x \in \bigcap_{t\in T} F_t \iff \forall_{t\in T}\ x \in F_t.$$

Ta definicja mówi, że x należy do przecięcia zbiorów F_t, $t \in T$, jeśli należy do każdego z nich.

W przykładzie 3.2 mamy $\bigcup_{t\in T} F_t = \bigcup_{t\in\{2,3,4,\dots\}}[1, t) = [1, +\infty)$ oraz $\bigcap_{t\in T} F_t = \bigcap_{t\in\{2,3,4,\dots\}}[1, t) = [1, 2)$.

Uwaga 3.5. 1. Czytelnik może spotkać się też z pojęciem *rodziny zbiorów* – czyli zbioru, którego elementami są zbiory z $\mathcal{P}(Y)$. Ze względów, które wyjaśnimy później, matematycy unikają określenia „zbiór zbiorów". Warto zdawać sobie sprawę z różnicy pomiędzy rodziną zbiorów a indeksowaną rodziną zbiorów. Niech przykładowo rodzina zbiorów $\mathcal{R}$ składa się z jednego zbioru A, czyli $\mathcal{R} = \{A\}$. Na indeksowaną rodzinę zbiorów natomiast patrzymy jak na funkcję $F : T \ni t \to \{A\}$ taką, że $F_t = A$ dla wszystkich $t \in T$, a T jest naszym zbiorem indeksów, na przykład $T = \{2, 3, 4\}$ albo $T = \mathbb{N}$ albo $T = \mathbb{R}$.

2. Dla (niepustej) rodziny zbiorów również możemy zdefiniować *sumę* i przecięcie, które zapisujemy $\bigcup \mathcal{R}$ lub $\bigcup_{A\in\mathcal{R}} A$ oraz $\bigcap \mathcal{R}$ lub $\bigcap_{A\in\mathcal{R}} A$:

$$x \in \bigcup \mathcal{R} \iff \exists_{A\in\mathcal{R}}\ x \in A.$$

$$x \in \bigcap \mathcal{R} \iff \forall_{A\in\mathcal{R}}\ x \in A.$$

Zdanie po prawej możemy zapisać też tak: $\forall_A\ A \in \mathcal{R} \implies x \in A$. Gdyby rodzina $\mathcal{R}$ była pusta, wynikanie byłoby zawsze spełnione. Tu zatem przydaje się warunek niepustości rodziny.

3. Jeśli zbiór indeksów $T = \mathbb{N}$, to stosujemy zapis: $\bigcup_{n=1}^{\infty} F_n$ oraz $\bigcap_{n=1}^{\infty} F_n$

Wypiszemy teraz i udowodnimy pewne własności działań uogólnionych. We wszystkich poniższych punktach stwierdzenia mamy rodzinę indeksowaną zbiorów F_t, gdzie $t \in T$.

Stwierdzenie 3.6.

1. *Dla dowolnego $t_0 \in T$ mamy:*
$$\bigcap_{t\in T} F_t \subset F_{t_0} \subset \bigcup_{t\in T} F_t.$$

2. *Prawa de Morgana*
$$(\bigcup_{t\in T} F_t)^c = \bigcap_{t\in T} F_t^c,$$
$$(\bigcap_{t\in T} F_t)^c = \bigcup_{t\in T} F_t^c.$$

3. *Załóżmy, że mamy rodzinę indeksowaną G_t taką, że dla każdego $t \in T$ zachodzi $F_t \subset G_t$. Wtedy*
$$\bigcup_{t\in T} F_t \subset \bigcup_{t\in T} G_t,$$
$$\bigcap_{t\in T} F_t \subset \bigcap_{t\in T} G_t.$$

4. *Jeśli dla każdego $t \in T$ mamy $F_t \subset A$, dla pewnego zbioru A, to*
$$\bigcup_{t\in T} F_t \subset A.$$

5. *Jeśli dla każdego $t \in T$ mamy $A \subset F_t$, dla pewnego zbioru A, to*
$$A \subset \bigcap_{t\in T} F_t.$$

Dowód. 1. Niech $x \in \bigcap_{t\in T} F_t$, czyli $\forall_{t\in T}\ x \in F_t$. Z tego wynika, że $x \in F_{t_0}$ dla wybranego t_0. Stąd, z definicji sumy $x \in \bigcup_{t\in T} F_t$.

2. Najpierw wykażemy, że $(\bigcup_{t\in T} F_t)^c = \bigcap_{t\in T} F_t^c$, pokazując, że x jest elementem lewej strony równości wtedy i tylko wtedy, gdy jest elementem prawej strony. Zaprzeczając zdaniom z kwantyfikatorami, korzystamy z 1.17.
Zatem $x \in (\bigcup_{t\in T} F_t)^c \iff \neg(x \in \bigcup_{t\in T} F_t) \iff \neg(\exists_{t\in T}\ x \in F_t) \iff \forall_{t\in T}\ \neg(x \in F_t) \iff \forall_{t\in T}\ x \in F_t^c \iff x \in \bigcap_{t\in T} F_t^c$.
Teraz analogicznie wykażemy, że $(\bigcap_{t\in T} F_t)^c = \bigcup_{t\in T} F_t^c$. Mamy $x \in (\bigcap_{t\in T} F_t)^c \iff \neg(x \in \bigcap_{t\in T} F_t) \iff \neg(\forall_{t\in T}\ x \in F_t) \iff \exists_{t\in T}\ \neg(x \in F_t) \iff \exists_{t\in T}\ x \in F_t^c \iff x \in \bigcup_{t\in T} F_t^c$.

3. Mamy $x \in \bigcup_{t\in T} F_t \iff \exists_{t\in T}\ x \in F_t \overset{F_t\subset G_t}{\Longrightarrow} \exists_{t\in T}\ x \in G_t \iff x \in \bigcup_{t\in T} G_t$.
Podobnie, $x \in \bigcap_{t\in T} F_t \iff \forall_{t\in T}\ x \in F_t \overset{F_t\subset G_t}{\Longrightarrow} \forall_{t\in T}\ x \in G_t \iff x \in \bigcap_{t\in T} G_t$.

4. Mamy $x \in \bigcup_{t\in T} F_t \iff \exists_{t\in T}\ x \in F_t \overset{F_t\subset A}{\Longrightarrow} x \in A$.

5. Mamy $x \in A \overset{A\subset F_t}{\Longrightarrow} \forall_{t\in T}\ x \in F_t \iff x \in \bigcap_{t\in T} F_t$. □

Zdefiniujemy teraz iloczyn kartezjański dwóch zbiorów i wykażemy niektóre jego własności. Do tego pojęcia wrócimy na następnym wykładzie.

Przypomnijmy, że zbiór złożony z jednego elementu a, oznaczamy przez $\{a\}$. Zbiór mający dwa elementy a i b oznaczamy $\{a, b\}$. Pamiętamy, że element a to nie to samo co zbiór jednoelementowy (singleton) $\{a\}$.

Definicja 3.7 (Para uporządkowana)**.** *Para*, nazywana też *parą uporządkowaną*, to zbiór $\{\{a\}, \{a, b\}\}$. Parę uporządkowaną oznaczamy (a, b), pierwszym elementem pary jest a, drugim b.

W definicji pary mamy zbiór $\{a, b\}$ (z tych elementów składa się para) oraz wskazujemy, przez zbiór jednoelementowy $\{a\}$, który element jest pierwszy w parze. Zauważmy, że para (a, a) to zbiór $\{\{a\}\}$.

Uwaga 3.8. Zauważmy, że dwie pary są równe, gdy ich pierwsze i drugie elementy są odpowiednio równe, czyli $(a,b) = (c,d) \iff a = c \wedge b = d$.

Dowód. Faktycznie, jeśli $\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}$, to albo $\{a\} = \{c\}$, i wtedy $\{a,b\} = \{c,d\} = \{a,d\}$, czyli $b = d$, albo $\{a\} = \{c,d\}$, czyli $c \in \{a\} \wedge d \in \{a\}$, skąd $c = d = a$, skąd $\{\{a\},\{a,b\}\} = \{\{a\}\}$, czyli $b = a$, co kończy dowód. □

Weźmy teraz dwa dowolne zbiory X i Y.

Definicja 3.9. *Iloczyn kartezjański zbiorów X i Y* to zbiór

$$X \times Y := \{(x,y) : x \in X, y \in Y\}.$$

Uwaga 3.10. Oznaczenie $:=$ czytamy jako *z definicji*. Stosuje się również oznaczenie $\stackrel{def}{=}$.

Przykład 3.11.
- Płaszczyznę możemy traktować jako iloczyn kartezjański $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.
- Walec możemy traktować jako iloczyn kartezjański koła i odcinka.
- Torus (torusem jest np. dętka rowerowa) to iloczyn kartezjański dwóch okręgów.
- Prostokąt możemy traktować jako iloczyn kartezjański dwóch odcinków.
- Warto zauważyć, że najczęściej zbiór $X \times Y$ nie jest równy zbiorowi $Y \times X$ (ćwiczenie: kiedy zachodzi równość?)

Do definicji iloczynu kartezjańskiego wrócimy na następnym wykładzie, omówimy tam szerzej jego własności.

Niech teraz dana będzie indeksowana rodzina zbiorów dana przez funkcję $F : T \to \mathcal{P}(Y)$. Jeśli $T = S \times Q$ to rodzinę $\{F_t\}_{t\in T}$ możemy zapisać jako $\{F_{s,q}\}_{s\in S, q\in Q}$. Taką rodzinę nazywamy *podwójnie indeksowaną rodziną zbiorów*. Analogicznie jak poprzednio (definicja 3.3 i 3.4) możemy zdefiniować sumę i przecięcie takiej rodziny:

$$\bigcup_{(s,q)\in S\times Q} F_{s,q} = \{x : \exists_{(s,q)\in S\times Q}\ x \in F_{s,q}\}$$

$$\bigcap_{(s,q)\in S\times Q} F_{s,q} = \{x : \forall_{(s,q)\in S\times Q}\ x \in F_{s,q}\}$$

Możemy też rozważać *sumy iterowane*:

$$\bigcup_{q\in Q}\left(\bigcup_{s\in S} F_{s,q}\right),$$

$$\bigcup_{s\in S}\left(\bigcup_{q\in Q} F_{s,q}\right)$$

i analogicznie *przecięcia iterowane*

$$\bigcap_{q\in Q}\left(\bigcap_{s\in S} F_{s,q}\right),$$

$$\bigcap_{s\in S}\left(\bigcap_{q\in Q} F_{s,q}\right)$$

a także sumy przecięć i przecięcia sum:

$$\bigcup_{q\in Q}\left(\bigcap_{s\in S} F_{s,q}\right),$$

$$\bigcap_{s\in S}\left(\bigcup_{q\in Q} F_{s,q}\right).$$

Zachodzi następujące stwierdzenie:

Stwierdzenie 3.12. *Dla dowolnej podwójnie indeksowanej rodziny zbiorów $\{F_{s,q}\}_{s\in S,q\in Q}$ zachodzą równości:*

1.

$$\bigcup_{(s,q)\in S\times Q} F_{s,q} = \bigcup_{q\in Q}\left(\bigcup_{s\in S} F_{s,q}\right) = \bigcup_{s\in S}\left(\bigcup_{q\in Q} F_{s,q}\right)$$

2.

$$\bigcap_{(s,q)\in S\times Q} F_{s,q} = \bigcap_{q\in Q}\left(\bigcap_{s\in S} F_{s,q}\right) = \bigcap_{s\in S}\left(\bigcap_{q\in Q} F_{s,q}\right).$$

Dowód. Dla potrzeb dowodu oznaczmy $B_s := \bigcup_{q\in Q} F_{s,q}$ oraz $C_s := \bigcap_{q\in Q} F_{s,q}$
ad 1. Mamy $x \in \bigcup_{(s,q)\in S\times Q} F_{s,q} \iff \exists_{(s_0,q_0)\in S\times Q}\ x \in F_{s_0,q_0} \iff \exists_{s_0\in S}\exists_{q_0\in Q}\ x \in F_{s_0,q_0} \iff \exists_{s_0\in S}\ x \in \bigcup_{q\in Q} F_{s_0,q} \iff \exists_{s_0\in S}\ x \in B_{s_0} \iff x \in \bigcup_{s\in S} B_s \iff x \in \bigcup_{s\in S}\left(\bigcup_{q\in Q} F_{s,q}\right)$.
ad 2. $x \in \bigcap_{(s,q)\in S\times Q} F_{s,q} \iff \forall_{(s,q)\in S\times Q}\ x \in F_{s,q} \iff \forall_{s\in S}\forall_{q\in Q}\ x \in F_{s,q} \iff \forall_{s\in S}\ x \in \bigcap_{q\in Q} F_{s,q} \iff \forall_{s\in S}\ x \in C_s \iff x \in \bigcap_{s\in S} C_s \iff x \in \bigcap_{s\in S}\left(\bigcap_{q\in Q} F_{s,q}\right)$. □

Ze stwierdzenia 3.12 wynika, że możemy dowolnie przestawiać sumowanie po q z sumowaniem po s, jak też przecięcia po q z przecięciami po s. Nie możemy jednak „bezkarnie" wymieniać sumowania i przecięcia ze sobą. Zobaczmy następujący przykład:

Przykład 3.13. Niech $F_{s,q} = \{x \in \mathbb{R} : x < s + q\}$, gdzie $S = Q = \mathbb{R}$. Wówczas $\bigcap_{s\in S} F_{s,q} = \varnothing$, bo dla dowolnego $x \in \mathbb{R}$ zachodzi $x \notin F_{x-q,q}$. Zatem $\bigcup_{q\in Q}\bigcap_{s\in S} F_{s,q} = \varnothing$. Zarazem, dla dowolnego s mamy $\bigcup_{q\in Q} F_{s,q} = \mathbb{R}$, bo dla danego s mamy $x \in F_{s,x+1-s}$. A zatem $\bigcup_{q\in Q}\bigcap_{s\in S} F_{s,q} \neq \bigcap_{s\in S}\bigcup_{q\in Q} F_{s,q}$

Jak widać z powyższego przykładu nie musi być równości pomiędzy $\bigcup_{q\in Q}\bigcap_{s\in S} F_{s,q}$ a $\bigcap_{s\in S}\bigcup_{q\in Q} F_{s,q}$. Zachodzi natomiast zawieranie:

Stwierdzenie 3.14. *Dla dowolnej rodziny podwójnie indeksowanej $F_{s,q}$ mamy*

$$\bigcup_{q\in Q}\bigcap_{s\in S} F_{s,q} \subset \bigcap_{s\in S}\bigcup_{q\in Q} F_{s,q}.$$

Dowód. Oznaczmy $C_q := \bigcap_{s\in S} F_{s,q}$. Mamy $x \in \bigcup_{q\in Q}\bigcap_{s\in S} F_{s,q} \iff \exists_{q_0\in Q}\ x \in C_{q_0} \iff \exists_{q_0\in Q}\forall_{s\in S}\ x \in F_{s,q_0} \overset{\text{zob.1.19}}{\Longrightarrow} \forall_{s\in S}\exists_{q_0\in Q}\ x \in F_{s,q_0} \iff x \in \bigcap_{s\in S}\bigcup_{q\in Q} F_{s,q}$. □

Ćwiczenie 3.15. Dla $S = Q = \{1, 2\}$ niech $F_{1,1} = \{1, 2, 3\}, F_{1,2} = \{2\}, F_{2,1} = \{1\}, F_{2,2} = \{3\}$. Sprawdzić dla tej rodziny $F_{s,q}$ stwierdzenie 3.14.

Rozdział 4

Iloczyn kartezjański zbiorów. Relacje i ich własności

Na tym wykładzie omówimy raz jeszcze iloczyn kartezjański zbiorów, relacje, dziedzinę, przeciwdziedzinę i składanie relacji, relację odwrotną, pewne własności relacji (zwrotność, przechodniość etc).

Przypomnijmy z poprzedniego wykładu, że parą uporządkowaną (a, b) nazywamy zbiór $\{\{a\}, \{a, b\}\}$. Jednym z pierwszych matematyków, którzy podali formalną definicję pary, był Kazimierz Kuratowski.

Przypomnijmy, że iloczynem kartezjańskim zbiorów X i Y nazywamy zbiór

$$X \times Y := \{(x, y) : x \in X, y \in Y\}.$$

Nazwa „iloczyn kartezjański" pochodzi od nazwiska francuskiego matematyka, René Descartesa, którego spolszczone nazwisko to Kartezjusz[1].

Poniższe stwierdzenie podaje pewne własności iloczynu kartezjańskiego.

Stwierdzenie 4.1. *Niech X, Y, X_1, X_2, Y_1, Y_2 będą zbiorami.*

1. $(X_1 \cup X_2) \times Y = (X_1 \times Y) \cup (X_2 \times Y)$.
2. $X \times (Y_1 \cup Y_2) = (X \times Y_1) \cup (X \times Y_2)$.
3. $(X_1 \setminus X_2) \times Y = (X_1 \times Y) \setminus (X_2 \times Y)$.
4. $(X_1 \cap X_2) \times (Y_1 \cap Y_2) = (X_1 \times Y_1) \cap (X_2 \times Y_2)$.
5. *Jeśli X_1, X_2, Y_1, Y_2 są niepuste, to* $(X_1 \times Y_1 = X_2 \times Y_2) \iff (X_1 = X_2 \wedge Y_1 = Y_2)$.

Dowód. Dla każdego z przypadków 1–4 wykażemy, że para (a, b) należy do lewej strony równości wtedy i tylko wtedy, gdy należy do prawej. Podczas dowodu korzystamy z odpowiednich praw dla działań logicznych oraz z definicji sumy, różnicy, iloczynu zbiorów.

ad 1. $(a, b) \in (X_1 \cup X_2) \times Y \iff a \in (X_1 \cup X_2) \wedge (b \in Y) \iff (a \in X_1 \vee a \in X_2) \wedge (b \in Y) \overset{1.10.9}{\iff} (a \in X_1 \wedge b \in Y) \vee (a \in X_2 \wedge b \in Y) \iff (a, b) \in X_1 \times Y \vee (a, b) \in X_2 \times Y \iff (a, b) \in (X_1 \times Y) \cup (X_2 \times Y)$.

ad 2. $(a, b) \in X \times (Y_1 \cup Y_2) \iff (a \in X) \wedge (b \in Y_1 \cup Y_2) \iff (a \in X) \wedge (b \in Y_1 \vee b \in Y_2) \overset{1.10.9}{\iff} (a \in X \wedge b \in Y_1) \vee (a \in X \wedge b \in Y_2) \iff (a, b) \in (X \times Y_1) \cup (X \times Y_2)$.

ad 3. $(a, b) \in (X_1 \setminus X_2) \times Y \iff (a \in X_1 \setminus X_2) \wedge b \in Y \iff (a \in X_1 \wedge \neg(a \in X_2)) \wedge b \in Y \iff (a \in X_1 \wedge b \in Y) \wedge (\neg(a \in X_2)) \overset{*}{\iff} ((a \in X_1 \wedge b \in Y) \wedge (\neg(a \in X_2))) \vee (a \in X_1 \wedge b \in Y \wedge \neg(b \in Y)) \overset{1.10.9}{\iff} a \in X_1 \wedge b \in Y \wedge (\neg(a \in X_2) \vee \neg(b \in Y)) \iff (a, b) \in X_1 \times Y \wedge \neg((a, b) \in X_2 \times Y) \iff (a, b) \in (X_1 \times Y) \setminus (X_2 \times Y)$, gdzie równoważność $*$ wynika z faktu, że zdanie $(a \in X_1 \wedge b \in Y \wedge \neg(b \in Y))$ jest zawsze fałszywe.

ad 4. $(a, b) \in (X_1 \cap X_2) \times (Y_1 \cap Y_2) \iff (a \in X_1 \cap X_2) \wedge (b \in Y_1 \cap Y_2) \iff (a \in X_1 \wedge a \in X_2) \wedge (b \in Y_1 \wedge b \in Y_2) \iff (a \in X_1 \wedge b \in Y_1) \wedge (a \in X_2 \wedge b \in Y_2) \iff (a, b) \in X_1 \times Y_1 \wedge (a, b) \in X_2 \times Y_2 \iff (a, b) \in (X_1 \times Y_1) \cap (X_2 \times Y_2)$.

ad 5. Wynikanie ($\Longleftarrow$) jest oczywiste. Wynikanie ($\Longrightarrow$): Skoro oba iloczyny kartezjańskie są równe (i niepuste), to $(a, b) \in X_1 \times Y_1 \iff (a, b) \in X_2 \times Y_2$ czyli $a \in X_1 \wedge b \in Y_1 \iff a \in X_2 \wedge b \in Y_2$ czyli $a \in X_1 \iff a \in X_2$ oraz $b \in Y_1 \iff b \in Y_2$, a stąd mamy żądaną równość zbiorów.

[1] René Descartes (1596–1650), francuski filozof, matematyk i fizyk.

Zauważmy, że pisząc powyżej „czyli", korzystamy z wynikania (w dwie strony) $((p \wedge q) \implies (r \wedge s)) \implies ((p \implies s) \wedge (q \implies r))$, które zachodzi, gdy wszystkie zdania są prawdziwe. Tu właśnie wykorzystujemy fakt, że zbiory są niepuste, zatem np. $a \in X_1$ jest zdaniem prawdziwym. □

Zdefiniujemy teraz pojęcie ogólniejsze niż pojęcie pary – pojęcie s-ki uporządkowanej. Podamy definicję rekurencyjną (choć formalnie ten sposób definiowania pojawi się później na wykładzie).

Definicja 4.2 (s-ka uporządkowana)**.** Niech $s \in \mathbb{N}, s \geqslant 2$ i niech dane będą elementy $a_1, \ldots, a_s$ (niekoniecznie różne) pewnego zbioru A. Dla $s = 2$ s-ka uporządkowana jest parą uporządkowaną (a_1, a_2). Załóżmy, że mamy zdefiniowaną $(s-1)$-tkę uporządkowaną $(a_1, \ldots, a_{s-1})$ dla pewnego $s > 2$. Wtedy s-kę uporządkowaną definiujemy jako $(a_1, \ldots, a_s) := ((a_1, \ldots, a_{s-1}), a_s)$.

Niech teraz $X_1, \ldots, X_s$ będą zbiorami.

Definicja 4.3. *Iloczyn kartezjański zbiorów* $X_1, \ldots, X_s$ to zbiór

$$X_1 \times \cdots \times X_s := \{(a_1, \ldots, a_s) : a_1 \in X_1, \ldots, a_s \in X_s\}.$$

Uwaga 4.4. Jeśli wszystkie zbiory $X_1, \ldots, X_s$ są równe pewnemu zbiorowi X, to stosujemy zapis $\underbrace{X \times \cdots \times X}_{s \text{ razy}} = X^s$.

Zapis ten jest zapewne wszystkim znany w przypadku $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ albo $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$.

Gdy mamy indeksowaną rodzinę zbiorów, możemy wprowadzić pojęcie uogólnionego iloczynu kartezjańskiego.

Definicja 4.5. Niech $\{F_t, t \in T\}$ będzie indeksowaną rodziną zbiorów, niech $Y = \bigcup_{t \in T} F_t$. *Uogólniony iloczyn kartezjański* definiujemy następująco:

$$\prod_{t \in T} F_t := \{f : T \to Y : f(t) \in F_t\}.$$

Uwaga 4.6. Łatwo zauważyć, że gdy zbiór T jest zbiorem $\{1, \ldots, s\}$, powyższa definicja jest równoważna z definicją 4.3.
Weźmy w szczególności $T = \{1, 2\}$ i niech $F_1, F_2 \subset Y$ i weźmy funkcje $f : \{1, 2\} \to Y$ spełniające warunek $f(1) \in F_1, f(2) \in F_2$. Elementy iloczynu kartezjańskiego $(a_1, a_2) \in F_1 \times F_2$ możemy traktować jako pary (a_1, a_2), gdzie $a_1 \in F_1, a_2 \in F_2$ lub też jako funkcje $f : T \to Y$ spełniające warunek $a_1 := f(1) \in F_1, a_2 := f(2) \in F_2$.

Przejdziemy teraz do definicji relacji. Niech dane będą zbiory X_1, $X_2, \ldots, X_m$.

Definicja 4.7. *Relacją (dwuargumentową)* nazywamy dowolny podzbiór R iloczynu kartezjańskiego $X_1 \times X_2$.
Podzbiór iloczynu kartezjańskiego m zbiorów $X_1 \times \cdots \times X_m$ nazywamy *relacją m-argumentową*.

Dla relacji dwuargumentowej R i pary $(x_1, x_2) \in R$ stosujemy też zapis $x_1 \, R \, x_2$. Mówimy wtedy, że x_1 *jest w relacji* R z x_2. Relacje oznaczamy też literami S, T albo jako $R_1, R_2, \ldots$.

Przykład 4.8. • Niech $X_1 = X_2 = \mathbb{R}$. Określamy podzbiór $S \subset \mathbb{R}^2$ następująco: $S = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 2\}$. Jak widać, x jest w relacji S z y wtedy i tylko wtedy, gdy punkt (x, y) leży na okręgu o promieniu $\sqrt{2}$, zobacz rysunek 4.1.

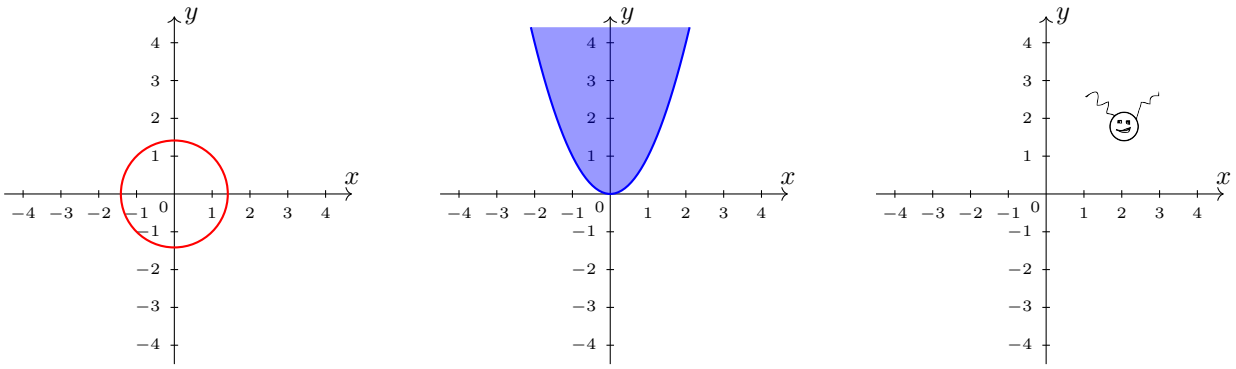
• Niech $X_1 = X_2 = \mathbb{N}$. Określamy podzbiór $R \subset \mathbb{N}^2$ następująco: $R = \{(x, y) \in \mathbb{N}^2 : x|y\}$, gdzie zapis $x|y$ oznacza, że x *dzieli* y. Mamy wówczas $2 \, R \, 4$, ale $(4, 2) \notin R$, podobnie $(5, 12) \notin R$.

• Niech $X_1 = X_2 = \mathbb{R}$. Określamy podzbiór $S \subset \mathbb{R}^2$ następująco: $S = \{(x, y) \in \mathbb{R}^2 : y - x^2 \geqslant 0\}$. Para (x, y) jest w relacji R, gdy punkt (x, y) leży na wykresie albo nad wykresem paraboli $y = x^2$ (środkowy rysunek).

• Zbiór z prawej na rysunku 4.1 także przedstawia relację w $\mathbb{R}^2$.

• Czytelnikowi znane są też zapewne relacje równoległości prostych albo podobieństwa trójkątów, omówimy je dokładniej na dalszych wykładach.

Rysunek 4.1:



Definicja 4.9 (Dziedzina i przeciwdziedzina relacji)**.** *Dziedziną relacji* $R \subset X_1 \times X_2$ nazywamy zbiór

$$\mathrm{Dom}_R := \{x_1 \in X_1 : \exists_{x_2 \in X_2}\ x_1\, R\, x_2\}.$$

Przeciwdziedziną relacji $R \subset X_1 \times X_2$ nazywamy zbiór

$$\mathrm{Dom}^*_R := \{x_2 \in X_2 : \exists_{x_1 \in X_1}\ x_1\, R\, x_2\}.$$

Przykład 4.10. Niech $X_1 = \{2,3,5\}, X_2 = \{4,6,7\}$. Niech $x\, R\, y \iff x|y$. Wówczas $R = \{(2,4),(2,6),(3,6)\}$, $\mathrm{Dom}_R = \{2,3\}$, $\mathrm{Dom}^*_R = \{4,6\}$.

Uwaga 4.11. Dwie relacje są równe, jeśli są równe jako podzbiory iloczynu kartezjańskiego.

Zdefiniujemy teraz złożenie relacji, i wykażemy, że składanie relacji jest działaniem łącznym. Niech zatem X_1, X_2, X_3 będą zbiorami, niech $R_1 \subset X_1 \times X_2$ i $R_2 \subset X_2 \times X_3$.

Definicja 4.12. *Złożeniem relacji* R_1 *z relacją* R_2 nazywamy relację $R_2 \circ R_1 \subset X_1 \times X_3$, zdefiniowaną jako zbiór

$$R_2 \circ R_1 := \{(x_1, x_3) \in X_1 \times X_3 : \exists_{x_2 \in X_2}\ (x_1, x_2) \in R_1 \wedge (x_2, x_3) \in R_2\}.$$

Warto zwrócić uwagę na kolejność zapisu składanych relacji i fakt, że niektórych podręcznikach $R_2 \circ R_1$ nazywa się złożeniem R_2 z R_1.

Przykład 4.13. Rozpatrzmy następującą, dość szczególną, sytuację. Niech $X_1 = X_2 = X_3 = \mathbb{R}$, niech $R_1 = R_2 = R$, gdzie $R = \{(x,y) \in \mathbb{R}^2 : y = x^2\}$. Wtedy $R \circ R = \{(x,z) \in \mathbb{R}^2 : \exists_y : x\, R\, y \wedge y\, R\, z\}$, co oznacza, że $(x,z) \in R \circ R$ jeśli istnieje y takie, że $y = x^2$ oraz $z = y^2$, a stąd mamy, że $(x,z) \in R \circ R$ wtedy i tylko wtedy, gdy $z = x^4$.

Więcej o składaniu relacji powiemy przy okazji składania funkcji.

Teraz wykażemy następujące stwierdzenie, mówiące, że składanie relacji jest łączne. Warto to twierdzenie zapamiętać, bo mówi w szczególności, że składanie funkcji jest działaniem łącznym. Przydaje się także na algebrze liniowej, jako jedna z możliwości wykazania łączności mnożenia macierzy.

Stwierdzenie 4.14. *Niech* X_1, X_2, X_3, X_4 *będą zbiorami, niech* $R_1 \subset X_1 \times X_2$, $R_2 \subset X_2 \times X_3$ *oraz* $R_3 \subset X_3 \times X_4$. *Wówczas*

$$(R_3 \circ R_2) \circ R_1 = R_3 \circ (R_2 \circ R_1).$$

Dowód. Niech $(x_1, x_4) \in (R_3 \circ R_2) \circ R_1$. Wykorzystując definicję złożenia następujący ciąg równoważności, mamy: $(x_1,x_4) \in (R_3 \circ R_2) \circ R_1 \iff \exists_{x_2 \in X_2} : (x_1,x_2) \in R_1 \wedge (x_2,x_4) \in R_3 \circ R_2 \iff \exists_{x_2 \in X_2} : (x_1,x_2) \in R_1 \wedge \exists_{x_3 \in X_3} (x_2,x_3) \in R_2 \wedge (x_3,x_4) \in R_3 \iff \exists_{x_3 \in X_3} (x_3,x_4) \in R_3 \wedge \exists_{x_2 \in X_2} (x_1,x_2) \in R_1 \wedge (x_2,x_3) \in R_2 \iff \exists_{x_3 \in X_3} (x_3,x_4) \in R_3 \wedge (x_1,x_3) \in R_2 \circ R_1 \iff (x_1,x_4) \in R_3 \circ (R_2 \circ R_1)$.

□

Dla danej relacji $R \subset X_1 \times X_2$ wprowadzimy pojęcie relacji odwrotnej.

Definicja 4.15. Niech $R \subset X_1 \times X_2$. *Relacja odwrotna*, zapisywana jako R^{-1} to zbiór zawarty w $X_2 \times X_1$, zdefiniowany jako

$$R^{-1} := \{(x_2, x_1) \in X_2 \times X_1 : (x_1, x_2) \in R\}.$$

Przykład 4.16. Niech $X_1 = X_2 = \mathbb{R}$.
1. Niech $x\,R\,y \iff y = x + 2$. Wówczas $R^{-1} = \{(y, x) : y = x + 2\} = \{(x + 2, x), x \in \mathbb{R}\} = \{(x, x - 2) \in \mathbb{R}^2\}$.
2. Niech $x\,R\,y \iff y = x^2$. Wówczas $R^{-1} = \{(y, x) : y = x^2\} = \{(x^2, x), x \in \mathbb{R}\} = \{(x, \sqrt{x}) : x \geqslant 0\} \cup \{(x, -\sqrt{x}) : x \geqslant 0\}$.

Skupimy się teraz na sytuacji, gdy relacja R jest podzbiorem $X \times X$.

Definicja 4.17 (Relacja zwrotna)**.** Mówimy, że relacja $R \subset X^2$ jest *zwrotna*, gdy

$$\forall_{x \in X} \quad x\,R\,x.$$

Przykład 4.18. Relacja podzielności w liczbach naturalnych ($X = \mathbb{N}, x\,R\,y \iff x|y$) jest relacją zwrotną, bo każda liczba naturalna dzieli samą siebie (liczby naturalne rozważamy bez zera).
Relacja równoległości prostych na płaszczyźnie (dwie proste są w relacji, jeśli są do siebie równoległe, czyli albo nie mają punktów wspólnych, albo mają wszystkie punkty wspólne) jest relacją zwrotną (bo każda prosta jest równoległa do siebie).
Relacja „$<$" dla liczb rzeczywistych nie jest relacją zwrotną.

Definicja 4.19 (Relacja przeciwzwrotna)**.** Mówimy, że relacja $R \subset X^2$ jest *przeciwzwrotna*, gdy

$$\forall_{x \in X} \quad \neg(x\,R\,x).$$

Przykład 4.20. Relacja „$<$" dla liczb rzeczywistych ($x\,R\,y \iff x < y$) jest relacją przeciwzwrotną.

Definicja 4.21 (Relacja symetryczna)**.** Mówimy, że relacja $R \subset X^2$ jest *symetryczna*, gdy

$$\forall_{x,y \in X} \quad x\,R\,y \Longrightarrow y\,R\,x.$$

Przykład 4.22. Relacja równoległości prostych na płaszczyźnie jest relacją symetryczną.

Definicja 4.23 (Relacja antysymetryczna)**.** Mówimy, że relacja $R \subset X^2$ jest *antysymetryczna*, gdy

$$\forall_{x,y \in X} \quad x\,R\,y \Longrightarrow \neg(y\,R\,x).$$

Przykład 4.24. Relacja „$<$" dla liczb rzeczywistych jest relacją antysymetryczną.

Definicja 4.25 (Relacja słabo antysymetryczna)**.** Mówimy, że relacja $R \subset X^2$ jest *słabo antysymetryczna*, gdy

$$\forall_{x,y \in X} \quad (x\,R\,y \wedge y\,R\,x) \Longrightarrow x = y.$$

Przykład 4.26. Relacja podzielności w liczbach naturalnych jest relacją słabo antysymetryczną, bo jeśli $x|y \wedge y|x$, to mamy $x = y$ (ćwiczenie).
Relacja „$\leqslant$" dla liczb rzeczywistych ($x\,R\,y \iff x \leqslant y$) jest relacją słabo antysymetryczną (bo $x \leqslant y \wedge y \leqslant x \Longrightarrow x = y$).
Warto zauważyć, że relacja „$<$" dla liczb rzeczywistych jest też relacją słabo antysymetryczną, bo warunek $xRy \wedge yRx$ jest zawsze fałszywy, zatem implikacja $(x\,R\,y \wedge y\,R\,x) \Longrightarrow x = y$ jest prawdziwa. Analogiczne rozumowanie pozwala ogólnie wykazać, że relacja antysymetryczna jest też słabo antysymetryczna.

Definicja 4.27 (Relacja przechodnia)**.** Mówimy, że relacja $R \subset X^2$ jest *przechodnia*, gdy

$$\forall_{x,y,z \in X} \quad (x\,R\,y \wedge yRz) \Longrightarrow xRz.$$

Przykład 4.28. Relacja podzielności w liczbach naturalnych jest relacją przechodnią (bo łatwo sprawdzić (ćwiczenie), że jeśli $x|y \wedge y|z$ to $x|z$.)
Relacja równoległości prostych na płaszczyźnie jest relacją przechodnią

Definicja 4.29 (Relacja spójna)**.** Mówimy, że relacja $R \subset X^2$ jest *spójna*, gdy

$$\forall_{x,y \in X} \quad x\,R\,y \vee y\,R\,x \vee x = y.$$

Przykład 4.30. Spójność relacji oznacza, że każde dwa elementy zbioru X są ze sobą w relacji, ewentualnie są sobie równe.
Relacja podzielności w liczbach naturalnych nie jest relacją spójną (wystarczy np. rozważyć elementy 5 i 7.)
Relacja $<$ w $\mathbb{R}$ jest relacją spójną (dla każdych dwóch liczb rzeczywistych x, y: $x < y$ lub $y < x$ lub $y = x$).

Rozdział 5

Funkcje, przykłady. Injekcja, surjekcja, bijekcja, funkcja odwrotna

Na tym wykładzie zajmiemy się pewnymi szczególnymi relacjami, zwanymi funkcjami. Zdefiniujemy injekcje, surjekcje i bijekcje, zdefiniujemy funkcję odwrotną i wykażemy twierdzenie o istnieniu funkcji odwrotnej.

Niech X, Y będą zbiorami. Weźmy relację (czyli podzbiór $X \times Y$) tym razem oznaczoną przez f.

Definicja 5.1. Relację $f \subset X \times Y$ nazywamy *funkcją* wtedy i tylko wtedy, gdy spełniony jest warunek

$$\forall_{x \in X} \exists!_{y \in Y} \ (x, y) \in f.$$

Równoważnie ten warunek możemy zapisać jako koniunkcję dwóch warunków:
1. $\forall_{x \in X} \exists_{y \in Y} \ (x, y) \in f$
2. $\forall_{x \in X, y_1, y_2 \in Y} \ ((x, y_1) \in f \wedge (x, y_2) \in f) \Longrightarrow y_1 = y_2$.

Uwaga 5.2. 1. Dla funkcji (jak już zapewne wszyscy wiedzą) nie stosujemy zwyczajowo zapisu $(x, y) \in f$ ani xfy, tylko piszemy $f(x) = y$. Niemniej, na tym wykładzie będzie pojawiał się niekiedy zapis $(x, y) \in f$. Nie piszemy też $f \subset X \times Y$, ale $f : X \to Y$, ewentualnie $X \xrightarrow{f} Y$.

2. Zbiór wszystkich funkcji $f : X \to Y$ oznaczamy Y^X, czyli $Y^X = \{f : X \to Y\}$.

3. Zauważmy, że w powyższej definicji dziedziną relacji (funkcji) f jest cały zbiór X. Często spotykamy się jednak z sytuacją, gdy dziedziną funkcji jest zbiór A istotnie zawarty w X (co zapisujemy $A \subsetneq X$). Przykładowo, gdy mamy zadanie „wyznacz dziedzinę funkcji $f : \mathbb{R} \to \mathbb{R}$, danej wzorem $f(x) = \frac{\sqrt{x}}{x-3}$", formalnie powinniśmy najpierw tę dziedzinę wyznaczyć, bo $f : \mathbb{R} \to \mathbb{R}$ zadane tym wzorem, nie jest funkcją w sensie definicji 5.1. Dlatego albo wprowadzamy pojęcie funkcji częściowej, czyli prowadzącej z pewnego podzbioru X, co zapisujemy tak: $f : X \nrightarrow Y$, albo pomijamy ten problem, przyjmując, że zapis $f : X \to Y$ oznacza również funkcję częściową.

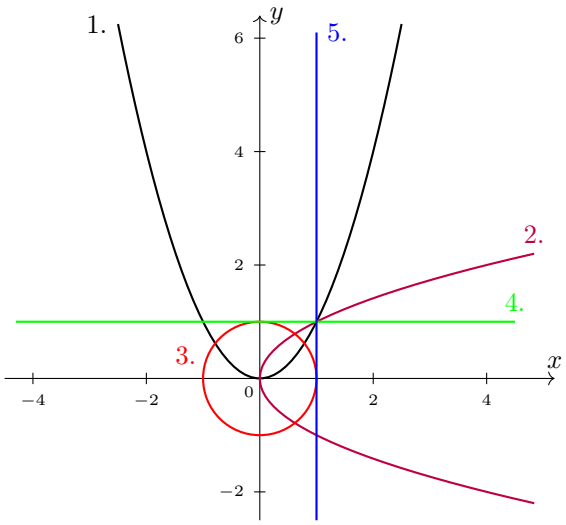
4. O dwóch funkcjach $f \subset X \times Y$ i $g \subset X \times Y$ powiemy, że są *równe*, jeśli są równe jako relacje (czyli są takimi samymi podzbiorami $X \times Y$). W szczególności oznacza to, że dziedziny funkcji są takie same, ale też, że zbiór Y do którego funkcje prowadzą ma być ten sam. Na przykład, funkcja $f(x) = x^2$ będzie inną funkcją, jeśli rozważamy ją jako funkcję z $X = \mathbb{R}$ do $Y = \mathbb{R}$, a inną, jeśli rozważamy ją jako funkcję z $X = \mathbb{R}$ do $Y = [0, +\infty)$.

Przypomnijmy, że przeciwdziedziną relacji (a zatem i funkcji f) jest zbiór $\mathrm{Dom}_f^* = \{y \in Y : \exists_{x \in X}(x, y) \in f\} = \{y \in Y : \exists_{x \in X} y = f(x)\}$.

Przykład 5.3. Niech f będzie relacją w $\mathbb{R} \times \mathbb{R}$. Łatwo sprawdzić, że:
1. Relacja zadana warunkiem $(x, y) \in f \iff y = x^2$ jest funkcją.
2. Relacja zadana warunkiem $(x, y) \in f \iff y^2 = x$ nie jest funkcją.
3. Relacja zadana warunkiem $(x, y) \in f \iff x^2 + y^2 = 1$ nie jest funkcją.
4. Relacja zadana warunkiem $(x, y) \in f \iff y = 1$ jest funkcją.
5. Relacja zadana warunkiem $(x, y) \in f \iff x = 1$ nie jest funkcją.

Rysunek 5.1 ilustruje te relacje.

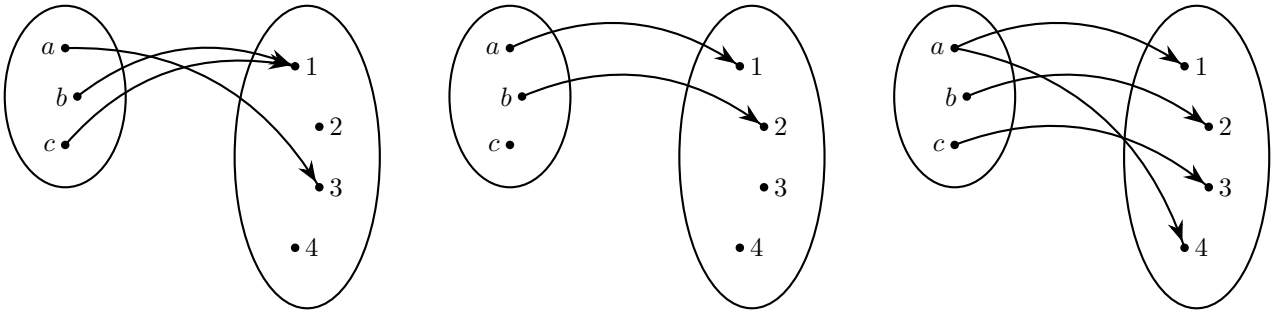
Rysunek 5.1:



Przykład 5.4. Niech teraz $X = \mathbb{N}$ a Y niech będzie dowolnym zbiorem. Funkcję $f : \mathbb{N} \to Y$ nazywamy *ciągiem* o wartościach w Y. Większości znane są już zapewne ciągi o wyrazach rzeczywistych, czyli funkcje $f : \mathbb{N} \to \mathbb{R}$. Dla ciągów stosuje się specjalne oznaczenia, zapisując te funkcje małymi literami $a, b, \ldots$ i pisząc a_n zamiast $a(n)$.

Funkcje możemy też zadać graficznie, tak jak na rysunku 5.2. Strzałka od elementu zbioru X do elementu zbioru Y pokazuje, że te elementy są w relacji. Relacja na rysunku po lewej jest funkcją, a na rysunkach w środku i po prawej nie jest funkcją. Relacja na rysunku w środku nie spełnia warunku 1. z definicji 5.1, jest natomiast funkcją częściową, relacja na rysunku po prawej nie spełnia warunku 2. tej definicji.

Rysunek 5.2:



Jeszcze jeden sposób definiowania funkcji (ogólniej, relacji) to tabelka relacji. Stosuje się go, jeśli elementów zbiorów X i Y jest niezbyt dużo. Wówczas pionowo wypisujemy elementy zbioru X, poziomo elementy zbioru Y a kropka w tabelce oznacza, że dane dwa elementy są w relacji.

Zobaczmy następujący przykład.

Przykład 5.5. Niech $X = \{a, b, c\}$, $Y = \{1, 2, 3, 4\}$.

	1	2	3	4
a			•	
b	•			
c	•			

Która z relacji z rysunku 5.2 jest zadana przez tę tabelkę?

W szczególnym przypadku, gdy mamy funkcję $f : X \to Y$ i zbiór X jest iloczynem kartezjańskim s zbiorów $X = X_1 \times \cdots \times X_s$, to piszemy

$$f : X_1 \times \cdots \times X_s \to Y$$

i f nazywamy *funkcją s zmiennych.*

Najczęściej zapisujemy $f(x_1, \ldots, x_s)$ zamiast (jak formalnie powinniśmy) $f((x_1, \ldots, x_s))$.

Przykład 5.6. Weźmy $f : \mathbb{R}^2 \to \mathbb{R}$. Przykładowa funkcja dwóch zmiennych (o wartościach w $Y = \mathbb{R}$) to $f(x_1, x_2) = x_1 x_2$.
Inny, dość ważny przykład, to projekcja: funkcję z $\mathbb{R}^n$ w $\mathbb{R}$, która jest dana wzorem

$$f(x_1, x_2, \ldots, x_n) = x_i$$

nazywamy *projekcją* (*rzutowaniem*) na i-tą zmienną, $i = 1, \ldots, n$.
Weźmy teraz $f : \mathbb{R}^2 \to \mathbb{R}^3$. Przykładowa funkcja dwóch zmiennych o wartościach w $Y = \mathbb{R}^3$ to $f(x_1, x_2) = (x_1^2, x_1 + x_2, \cos x_2)$.

Zajmiemy się teraz *złożeniem funkcji*, zwanym inaczej *superpozycją funkcji.*

Definicja 5.7. Niech X, Y, Z, V będą zbiorami, i niech $Y \subset V$. Niech dane będą dwie funkcje $f : X \to Y$ i $g : V \to Z$. Te dwie funkcje są relacjami, zatem *złożenie funkcji* f i g to złożenie relacji oznaczane przez $g \circ f$. Przypomnijmy, że $g \circ f \subset X \times Z$, oraz $(x, z) \in g \circ f \iff \exists_{y \in Y} : (x, y) \in f \wedge (y, z) \in g$.

Pozostaje pytanie, czy złożenie funkcji jest także funkcją. Twierdzącą odpowiedź na to pytanie podaje poniższe stwierdzenie.

Stwierdzenie 5.8. *Załóżmy, że mamy taką sytuację jak w definicji 5.7. Wówczas złożenie funkcji f i g, czyli $g \circ f$ jest funkcją.*

Dowód. Sprawdźmy pierwszy warunek definicji 5.1. Pytamy, czy dla każdego $x \in X$ istnieje $z \in Z$ takie, że para $(x, z) \in g \circ f$. Weźmy zatem dowolne $x \in X$. Ponieważ f jest funkcją, istnieje $y \in Y$ takie, że $(x, y) \in f$. Weźmy teraz właśnie to y. Ponieważ g jest funkcją, istnieje $z \in Z$ takie, że $(y, z) \in g$. Skoro $(x, y) \in f$ i $(y, z) \in g$, to $(x, z) \in g \circ f$, a zatem pierwszy warunek jest spełniony.
Sprawdźmy drugi warunek definicji 5.1. Niech z_1 i z_2 będą takie, że $(x, z_1) \in g \circ f$ i $(x, z_2) \in g \circ f$. Z definicji złożenia mamy

$$\exists_{y_1 \in Y} : (x, y_1) \in f \wedge (y_1, z_1) \in g$$

oraz

$$\exists_{y_2 \in Y} : (x, y_2) \in f \wedge (y_2, z_2) \in g.$$

Skoro f jest funkcją, i z powyższego $(x, y_1) \in f$ i $(x, y_2) \in f$, to $y_1 = y_2$. W takim razie mamy $(y_1, z_1) \in g$ i $(y_1, z_2) \in g$. Ponieważ g jest funkcją, dostajemy $z_1 = z_2$. Zatem drugi warunek definicji funkcji też jest spełniony. □

Skoro $g \circ f$ jest funkcją, to możemy napisać, że $(g \circ f)(x) = z \iff \exists_{y \in Y} : f(x) = y \wedge g(y) = z$.

Zdefiniujemy teraz pewne szczególne rodzaje funkcji. Niech dane będą dwa zbiory X, Y i funkcja $f : X \to Y$.

Definicja 5.9 (Injekcja)**.** Funkcja $f : X \to Y$ jest *injekcją* wtedy i tylko wtedy, gdy zachodzi następujący warunek:

$$\forall_{x_1, x_2 \in X} : f(x_1) = f(x_2) \Longrightarrow x_1 = x_2.$$

Równoważnie (prawo kontrapozycji) możemy warunek sformułować jako:

$$\forall_{x_1, x_2 \in X} : x_1 \neq x_2 \Longrightarrow f(x_1) \neq f(x_2).$$

Definicja 5.10 (Surjekcja)**.** Funkcja $f : X \to Y$ jest *surjekcją* wtedy i tylko wtedy, gdy zachodzi następujący warunek:

$$\forall_{y \in Y} \exists_{x \in X} : y = f(x).$$

Injekcje znane są też pod nazwą *funkcje różnowartościowe* a surjekcje nazywa się czasami *funkcjami na.* Stosowana jest też pisownia *iniekcja.*

Przykład 5.11. 1. Weźmy $f : \mathbb{N} \to \mathbb{N}$ daną wzorem $f(n) = 3n$. Łatwo sprawdzić, że ta funkcja jest injekcją (faktycznie, $f(n_1) = f(n_2) \iff 3n_1 = 3n_2 \Longrightarrow n_1 = n_2$), natomiast nie jest surjekcją (bo, biorąc na przykład $y = 1$, widzimy, że nie istnieje $n \in \mathbb{N}$, dla którego $3n = 1$).

2. Niech funkcja $f : \mathbb{Q} \to \mathbb{Q}$ będzie dana wzorem $f(x) = x^3$. Funkcja ta jest injekcją, bo $x_1^3 = x_2^3 \iff x_1^3 - x_2^3 = 0 \iff (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^3) = 0$. Wyrażenie w drugim nawiasie (niepełny kwadrat dwumianu) jest zerem tylko wtedy, gdy $x_1 = x_2 = 0$. Jeśli x_1 lub x_2 są różne od zera, to zerem musi być wyrażenie w pierwszym nawiasie, zatem $x_1 = x_2$.
Funkcja ta nie jest surjekcją, bo, przykładowo, dla $y = 2$ nie istnieje $x \in \mathbb{Q}$, takie, że $x^3 = 2$.

3. Niech $f : \mathbb{Q} \to \mathbb{Q}$ będzie dana wzorem $f(x) = x^2$. Funkcja ta nie jest ani injekcją, ani surjekcją. Sprawdzenie tego faktu zostawiamy jako proste ćwiczenie.

4. Niech $f : \mathbb{R} \to \mathbb{R}$ będzie dana jako $f(x) = x^3$. Funkcja ta jest zarówno injekcją jak i surjekcją. Sprawdzenie tego faktu zostawiamy jako proste ćwiczenie (dowód injektywności przebiega tak, jak w punkcie 2.)

Definicja 5.12. Funkcję $f : X \to Y$ nazywamy *bijekcją* jeśli f jest injekcją i f jest surjekcją.

Funkcja z punktu 4. przykładu 5.11 jest bijekcją.

Uwaga 5.13. Chcąc zaznaczyć, że funkcja f między zbiorami X i Y jest bijekcją, będziemy używać oznaczenia $X \hookrightarrow\!\!\!\!\rightarrow Y$. Stosuje się też oznaczenia $X \twoheadrightarrow Y$ dla surjekcji i $X \hookrightarrow Y$ dla injekcji.

Przypomnijmy teraz, że relację odwrotną do relacji R oznaczamy R^{-1} i definiujemy poprzez warunek $(y, x) \in R^{-1} \iff (x, y) \in R$. W przypadku gdy f jest funkcją, relację odwrotną oznaczamy przez f^{-1}.

Uwaga 5.14. Relacja odwrotna do funkcji nie musi być funkcją. Weźmy przykładowo $f : \mathbb{R} \to \mathbb{R}$ daną jako $f(x) = x^2$. Zatem $f^{-1} = \{(y, x) : (x, y) \in f\} = \{(x^2, x), x \in \mathbb{R}\}$, por. przykład 4.16. Skoro tak, to w szczególności $(1, 1) \in f^{-1}$ oraz $(1, -1) \in f^{-1}$, co oznacza, że f^{-1} nie jest funkcją.

Następujące twierdzenie odpowiada na pytanie kiedy relacja odwrotna do funkcji jest funkcją.

Twierdzenie 5.15. *Niech $f : X \to Y$ będzie funkcją. Relacja odwrotna f^{-1} jest funkcją wtedy i tylko wtedy, gdy f jest bijekcją.*

Dowód. ($\Longrightarrow$). Zakładamy, że f^{-1} jest funkcją. Chcemy sprawdzić, czy f jest bijekcją.
1. Najpierw sprawdzamy, czy f jest injekcją. Dla dowodu nie wprost, przypuśćmy, że f nie jest injekcją. Wtedy istnieją $x_1, x_2 \in X$, $x_1 \neq x_2$, takie, że $(x_1, y) \in f$ i $(x_2, y) \in f$. Stąd i z definicji f^{-1} mamy $(y, x_1) \in f^{-1}$ i $(y, x_2) \in f^{-1}$, czyli f^{-1} nie jest funkcją. Zatem f musi być injekcją.

2. Przypuśćmy teraz, że f nie jest surjekcją. Wówczas istnieje $y \in Y$ taki, że dla każdego $x \in X$ para $(x, y) \notin f$. To oznacza, że dla każdego $x \in X$ para $(y, x) \notin f^{-1}$. To oznacza, że f^{-1} nie spełnia warunku 1. z definicji funkcji, czyli otrzymaliśmy sprzeczność.

($\Longleftarrow$) Wykażemy, że jeśli f jest bijekcją, to f^{-1} jest funkcją.
1. Jeśli f jest surjekcją to dla każdego $y \in Y$ istnieje $x \in X$ takie, że $(x, y) \in f$. Stąd dla każdego $y \in Y$ istnieje $x \in X$ takie, że $(y, x) \in f^{-1}$, zatem f^{-1} spełnia warunek 1. definicji 5.1.

2. Jeśli f jest injekcją, to mamy następującą implikację $((x_1, y) \in f \wedge (x_2, y) \in f) \Longrightarrow x_1 = x_2$, co jest równoważne implikacji $((y, x_1) \in f^{-1} \wedge (y, x_2) \in f^{-1}) \Longrightarrow x_1 = x_2$ a to oznacza, że f spełnia 2. z definicji 5.1. □

Kolejne stwierdzenie mówi, że jeśli f jest bijekcją (wtedy f^{-1} jest funkcją), to funkcja f^{-1} jest też bijekcją.

Stwierdzenie 5.16. *Niech $f : X \hookrightarrow\!\!\!\!\rightarrow Y$ będzie bijekcją. Wówczas funkcja f^{-1} jest także bijekcją.*

Dowód. 1. Sprawdzamy, czy f^{-1} jest injekcją. Niech $(y_1, x) \in f^{-1}$ i $(y_2, x) \in f^{-1}$. Wówczas $(x, y_1) \in f$ i $(x, y_2) \in f$. Skoro f jest funkcją, to musi być $y_1 = y_2$, zatem f^{-1} jest injekcją.

2. Sprawdzamy, czy funkcja f^{-1} jest surjekcją, to znaczy chcemy wiedzieć, czy dla dowolnego $x \in X$ istnieje $y \in Y$ takie, że $(y, x) \in f^{-1}$. Weźmy zatem dowolne $x \in X$. Skoro f jest funkcją, to istnieje $y \in Y$ takie, że $(x, y) \in f$ (warunek 1. definicji 5.1), skąd $(y, x) \in f^{-1}$. □

Niech teraz Z będzie zbiorem. Zdefiniujemy funkcję identycznościową na zbiorze Z.

Definicja 5.17. Niech $\mathrm{Id}_Z : Z \to Z$ będzie funkcją taką, że $\mathrm{Id}_Z(z) = z$ dla każdego $z \in Z$. Id_Z nazywamy *funkcją identycznościową* (albo *identycznością*) na zbiorze Z.

Zachodzi następujące stwierdzenie,

Stwierdzenie 5.18. *Niech $f : X \hookrightarrow\!\!\!\!\rightarrow Y$ będzie bijekcją. Wówczas:*

$$f^{-1} \circ f = Id_X \text{ oraz } f \circ f^{-1} = Id_Y.$$

Dowód. 1. Złożenie $f^{-1} \circ f$ przeprowadza zbiór X w zbiór X, zatem dla dowolnego $x_1 \in X$ istnieje $x_2 \in X$ spełniające $(f^{-1} \circ f)(x_1) = x_2$. Jeśli wykażemy teraz, że $x_1 = x_2$, to wykażemy $f^{-1} \circ f = \mathrm{Id}_X$. Z definicji złożenia, $(x_1, x_2) \in f^{-1} \circ f \iff \exists_{y \in Y} : (x_1, y) \in f \wedge (y, x_2) \in f^{-1}$. Skoro $(x_1, y) \in f$ i $(y, x_2) \in f^{-1}$ zatem $(y, x_1) \in f^{-1}$. f^{-1} jest bijekcją, zatem $x_1 = x_2$, czyli dla dowolnego $x_1 \in X$ zachodzi $(f^{-1} \circ f)(x_1) = x_1$.

2. Rozumowanie jest analogicznie jak to w punkcie 1. Złożenie $f \circ f^{-1}$ przeprowadza zbiór Y w zbiór Y, zatem dla dowolnego $y_1 \in Y$ mamy $(f \circ f^{-1})(y_1) = y_2$, dla pewnego $y_2 \in Y$. Jeśli wykażemy, że $y_1 = y_2$, to wykażemy $f \circ f^{-1} = \mathrm{Id}_Y$. Z definicji złożenia, $(y_1, y_2) \in f \circ f^{-1} \iff \exists_{x \in X} : (y_1, x) \in f^{-1} \wedge (x, y_2) \in f \iff (y_1, x) \in f^{-1} \wedge (y_2, x) \in f^{-1}$. Skoro f^{-1} jest bijekcją (twierdzenie 5.16), to $y_1 = y_2$. Zatem $(f \circ f^{-1})(y_1) = y_1$ dla dowolnego y_1, czyli $f \circ f^{-1} = \mathrm{Id}_Y$. □

Na zakończenie tego wykładu wypiszemy dwa ćwiczenia, które warto zrobić samodzielnie.

Ćwiczenie 5.19. Weźmy dwie funkcje $f : X \to Y$ i $g : Y \to Z$ oraz ich złożenie $g \circ f : X \to Z$.

1. Wykazać, że jeśli f i g są surjekcjami, to $g \circ f$ też.
2. Wykazać, że jeśli f i g są injekcjami, to $g \circ f$ też.
3. Jeśli $g \circ f$ jest injekcją i f jest injekcją, to co można powiedzieć o injektywności g?
4. Jeśli f jest injekcją a g surjekcją (lub na odwrót), to co można powiedzieć o $g \circ f$?

Ćwiczenie 5.20. Weźmy dwie bijekcje $f : X \to Y$ i $g : Y \to Z$ oraz ich złożenie $g \circ f : X \to Z$. Wiemy, że $g \circ f$ też jest bijekcją. Wykazać, że zachodzi następujący wzór na odwrotność złożenia funkcji:

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

Rozdział 6

Obrazy, przeciwobrazy i pewne operacje na funkcjach

Na tym wykładzie omówimy definicje i własności obrazu i przeciwobrazu zbioru przez funkcję oraz operacje restrykcji, sklejenia, zestawienia i iloczynu kartezjańskiego funkcji.

Definicja 6.1. Niech X, X_1, Y będą zbiorami, takimi, że $X \subset X_1$. Weźmy funkcje $f_1 : X_1 \to Y$ oraz $f : X \to Y$. Jeśli dla każdego $x \in X$ zachodzi $f(x) = f_1(x)$ to

1. f_1 nazywamy *przedłużeniem funkcji* f (do zbioru X_1),
2. natomiast f nazywamy *restrykcją* (albo *zacieśnieniem*) f_1 do zbioru X. Zapisujemy wtedy $f = f_1|_X$

Przykład 6.2. Często rozważa się zacieśnienie funkcji okresowej do jednego okresu, np. $(\sin x)|_{[0,2\pi]}$.

Definicja 6.3. Niech X_1, X_2, Y będą zbiorami a $f_1 : X_1 \to Y$, $f_2 : X_2 \to Y$ funkcjami. Zdefiniujmy relację sklejenia określoną na $(X_1 \cup X_2) \times Y$ jako $f_1 \cup f_2$.

Stwierdzenie 6.4. *Przy oznaczeniach jak w powyższej definicji, relacja $f = f_1 \cup f_2$ jest funkcją (zwaną sklejeniem funkcji f_1 i f_2) wtedy i tylko wtedy, gdy dla każdego $x \in X_1 \cap X_2$ zachodzi $f_1(x) = f_2(x)$.*

Dowód. Warunek pierwszy z definicji 5.1 jest oczywiście spełniony. Sprawdźmy warunek drugi. Niech $(x, y_1) \in f$ i $(x, y_2) \in f$. Jeśli $x \in X_1 \setminus X_2$ to $(x, y_1) \in f_1$ i $(x, y_2) \in f_1$, a stąd (skoro f_1 jest funkcją) $y_1 = y_2$. Analogicznie rozumujemy w przypadku, gdy $x \in X_2 \setminus X_1$. Pozostaje do sprawdzenia przypadek, gdy $x \in X_1 \cap X_2$. Wtedy $y_1 = f(x) = f_1(x)$ (bo $x \in X_1$) i $y_2 = f(x) = f_2(x)$ (bo $x \in X_2$) ale dla $x \in X_1 \cap X_2$ mamy $f_1(x) = f_2(x)$, to $y_1 = y_2$. □

Przykład 6.5. Funkcja

$$f(x) = \begin{cases} -x^2, & x \leqslant 0 \\ x^2, & x \geqslant 0 \end{cases}$$

jest zadana na $\mathbb{R}$ jako sklejenie funkcji $f_1(x) = -x^2, x \in (-\infty, 0]$ i $f_2(x) = x^2, x \in [0, \infty)$. Obie te funkcje są równe na części wspólnej swoich dziedzin, czyli na zbiorze $\{0\}$.

Definicja 6.6. Niech X, Y_1, Y_2 będą zbiorami a $f_1 : X \to Y_1$, $f_2 : X \to Y_2$ funkcjami. Niech $Y := Y_1 \times Y_2$.
Zestawieniem funkcji f_1 i f_2 nazywamy funkcję $f : X \to Y$ zdefiniowaną następująco: $f(x) = (f_1(x), f_2(x))$.

Uwaga 6.7. Zestawienie funkcji jest funkcją. Faktycznie, warunek pierwszy definicji 5.1 jest spełniony. Niech zatem $(x, z) \in f$ oraz $(x, w) \in f$ dla pewnych $z, w \in Y$, zatem $z = (z_1, z_2)$, $w = (w_1, w_2)$. Z definicji f mamy $(x, z_1) \in f_1 \ni (x, w_1)$ oraz $(x, z_2) \in f_2 \ni (x, w_2)$, skąd $z_1 = w_1$ i $z_2 = w_2$, czyli $z = w$, czyli f jest funkcją.

Przykład 6.8. Jeśli $f_1(x) = \cos x$, $f_2(x) = \sin x$, $x \in [0, 2\pi]$, to zestawienie tych funkcji $(\cos x, \sin x)$ jest przykładem parametryzacji okręgu jednostkowego.

Definicja 6.9. Niech X_1, X_2, Y_1, Y_2 będą zbiorami. Weźmy funkcje $f_1 : X_1 \to Y_1$ oraz $f_2 : X_2 \to Y_2$. *Iloczyn kartezjański funkcji* f_1 i f_2 jest funkcją (to sprawdzimy poniżej), zdefiniowaną jako

$$f_1 \times f_2 : X_1 \times X_2 \to Y_1 \times Y_2,$$

$$(f_1 \times f_2)(x_1, x_2) = (f_1(x_1), f_2(x_2)), \quad (x_1, x_2) \in X_1 \times X_2.$$

Uwaga 6.10. Iloczyn kartezjański funkcji jest funkcją.

Dowód. Faktycznie, $f_1 \times f_2$ jest określony na całym iloczynie $X_1 \times X_2$. Niech zatem $((x_1, x_2), (z_1, z_2)) \in f_1 \times f_2 \ni ((x, x_2), (w_1, w_2))$. Z określenia $f_1 \times f_2$ mamy $z_1 = f_1(x_1) = w_1$ i $z_2 = f_2(x_2) = w_2$, czyli $(z_1, z_2) = (w_1, w_2)$, zatem $f_1 \times f_2$ jest funkcją. □

Przejdziemy teraz do zdefiniowania pojęć obrazu i przeciwobrazu zbioru przez funkcję oraz wykażemy pewne własności operacji brania obrazu i przeciwobrazu.

Niech X, Y, A, B będą zbiorami, niech ponadto $A \subset X$, $B \subset Y$ i niech $f : X \to Y$ będzie funkcją.

Definicja 6.11. *Obrazem zbioru $A \subset X$* przez funkcję f nazywamy zbiór

$$f(A) = \{y \in Y \mid \exists x \in A : y = f(x)\}.$$

Przykład 6.12.

- Niech $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. Niech $A = [-1, 1]$. Wówczas $f(A) = [0, 1]$.
- Niech $f : X \to \mathcal{P}(X)$, $f(x) = \{x\}$. Niech $A = X$. Wtedy $f(A) = \{\{x\} : x \in X\}$.
- Niech $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 5$. Niech $A = \mathbb{R}$. Wówczas $f(A) = \{5\}$.

Definicja 6.13. *Przeciwobrazem zbioru $B \subset Y$* nazywamy zbiór

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

Uwaga 6.14. Symbol f^{-1} nie jest jednoznaczny, może oznaczać przeciwobraz (jak powyżej), funkcję odwrotną (definicja 5.15), relację odwrotną, albo też $\frac{1}{f}$.

Przykład 6.15.

- Niech $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. Niech $B = [0, 1]$. Wówczas $f^{-1}(B) = [-1, 1]$. Jeśli $B = \{4\}$, to $f^{-1}(B) = \{-2, 2\}$.
- Niech $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 5$. Niech $B \subset \mathbb{R}$. Wówczas $f^{-1}(B) = \begin{cases} \mathbb{R}, & \text{jeśli } 5 \in B \\ \varnothing, & \text{jeśli } 5 \notin B. \end{cases}$.

Poniższe stwierdzenie zbiera własności operacji brania obrazów i przeciwobrazów.

Stwierdzenie 6.16. *Niech $X, Y, A_1, A_2, B_1, B_2, T$ będą zbiorami (T jest zbiorem wskaźników), niech $A_1, A_2 \subset X$, $B_1, B_2 \subset Y$, niech $\{A_t\}_{t \in T}$ i $\{B_t\}_{t \in T}$ będą rodzinami zbiorów indeksowanymi przez T, przy czym $A_t \subset X$, $B_t \subset Y$ dla każdego $t \in T$. Niech $f : X \to Y$ będzie funkcją. Wówczas*

1. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
2. $f(\bigcup_{t \in T} A_t) = \bigcup_{t \in T} f(A_t)$.
3. $f(A_1) \setminus f(A_2) \subset f(A_1 \setminus A_2)$.
4. $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.
5. $f(\bigcap_{t \in T} A_t) \subset \bigcap_{t \in T} f(A_t)$.
6. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
7. $f^{-1}(\bigcup_{t \in T} B_t) = \bigcup_{t \in T} f^{-1}(B_t)$.
8. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.
9. $f^{-1}(\bigcap_{t \in T} B_t) = \bigcap_{t \in T} f^{-1}(B_t)$.
10. $f^{-1}(B_1) \setminus f^{-1}(B_2) = f^{-1}(B_1 \setminus B_2)$.

Dowód. Dowód wymaga tylko konsekwentnego użycia definicji obrazu (bądź przeciwobrazu), będziemy korzystać też z własności formuł logicznych i kwantyfikatorów. Warto zwrócić uwagę na przykłady pokazujące, że w punktach $3, 4, 5$ zawieranie w drugą stronę nie musi zachodzić.

ad. 1. $y \in f(A_1 \cup A_2) \iff \exists x \in A_1 \cup A_2 : y = f(x) \iff \exists x \in A_1 \vee \exists x \in A_2 : y = f(x) \iff \exists x \in A_1 : y = f(x) \vee \exists x \in A_2 : y = f(x) \iff y \in f(A_1) \vee y \in f(A_2) \iff y \in f(A_1) \cup f(A_2)$.

ad. 2. $y \in f(\bigcup_{t\in T} A_t) \iff \exists x \in \bigcup_{t\in T} A_t : y = f(x) \iff \exists t_0 \in T\, \exists x : x \in A_{t_0} \wedge y = f(x) \iff \exists t_0 \in T y \in f(A_{t_0}) \iff y \in \bigcup_{t\in T} f(A_t)$.

ad. 3. $y \in f(A_1) \setminus f(A_2) \iff y \in f(A_1) \wedge \neg(y \in f(A_2)) \iff (\exists x \in X : x \in A_1 \wedge y = f(x)) \wedge \neg(\exists x \in X : x \in A_2 \wedge y = f(x)) \iff (\exists x \in X : x \in A_1 \wedge y = f(x)) \wedge (\forall x \in X\ y \neq f(x) \vee x \notin A_2) \implies (\exists x \in X : x \in A_1 \wedge y = f(x)) \wedge (y \neq f(x) \vee x \notin A_2) \iff (\exists x \in X : x \in A_1 \wedge y = f(x) \wedge y \neq f(x)) \vee (\exists x \in X : x \in A_1 \wedge y = f(x) \wedge x \notin A_2)$.

Pierwsze z dwóch ostatnich zdań jest zawsze fałszywe, zatem alternatywa jest równoważna drugiemu z nich:

$\exists x \in X : x \in A_1 \wedge y = f(x) \wedge x \notin A_2$, a to zdanie mówi, że $y \in f(A_1 \setminus A_2)$.

Zauważmy, że występującej w powyższym rozumowaniu implikacji nie można zastąpić przez równoważność (jeśli jakiś warunek nie jest spełniony dla pewnego x, to nie znaczy, że nie jest spełniony dla każdego x).

Aby zobaczyć przykład funkcji, dla której $f(A_1)\setminus f(A_2) \not\supset f(A_1\setminus A_2)$ wystarczy wziąć funkcję stałą, np. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 7$ oraz $A_1 = [1, 2], A_2 = [3, 4]$. Wtedy $f(A_1 \setminus A_2) = f(A_1) = \{7\}$, podczas gdy $f(A_1) \setminus f(A_2) = \{7\} \setminus \{7\} = \varnothing$.

ad. 4. $y \in f(A_1 \cap A_2) \iff \exists x \in X : x \in A_1 \cap A_2 \wedge y = f(x) \iff \exists x \in X : x \in A_1 \wedge x \in A_2 \wedge y = f(x) \implies (\exists x \in X : x \in A_1 \wedge y = f(x)) \wedge (\exists x \in X : x \in A_2 \wedge y = f(x)) \iff y \in f(A_1) \wedge y \in f(A_2) \iff y \in f(A_1) \cap f(A_2)$.

Zauważmy znowu, że wynikania w powyższym dowodzie nie można zastąpić przez równoważność (dla kwantyfikatora „*istnieje*" zachodzi wynikanie $\exists x : p(x) \wedge q(x) \implies \exists x : p(x) \wedge \exists x : q(x)$, ale nie musi zachodzić wynikanie w drugą stronę, por. 1.19).

Aby zobaczyć przykład funkcji, dla której $f(A_1 \cap A_2) \not\supset f(A_1) \cap f(A_2)$, znowu wystarczy wziąć funkcję stałą, np. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 7$ dla każdego $x \in \mathbb{R}$, oraz $A_1 = [1, 2]$, $A_2 = [3, 4]$. Wtedy $f(A_1 \cap A_2) = f(\varnothing) = \varnothing$, podczas gdy $f(A_1) \cap f(A_2) = \{7\} \cap \{7\} = \{7\}$.

ad. 5. $y \in f(\bigcap_{t\in T} A_t) \iff \exists x \in X : x \in \bigcap_{t\in T} A_t \wedge y = f(x) \iff \exists x \in X : \forall t \in T x \in A_t \wedge y = f(x) \implies \forall t \in T\ \exists x \in X : x \in A_t \wedge y = f(x) \iff \forall t \in T y \in f(A_t) \iff y \in \bigcap_{t\in T} f(A_t)$.

Zauważmy, że implikacji w tym dowodzie też nie możemy odwrócić, por. uwaga 1.16.

Przykład funkcji, dla której $f(\bigcap_{t\in T} A_t) \not\supset \bigcap_{t\in T} f(A_t)$, może być dokładnie taki sam jak powyżej, czyli $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 7$, zbiór $T = \{1, 2\}$ oraz $A_1 = [1, 2]$, $A_2 = [3, 4]$.

Można też wziąć nieskończoną rodzinę zbiorów, niech $T = \mathbb{N}$, $A_1 = (1, 2)$, $A_2 = (2, 3)$, $A_3 = (3, 4) \ldots$. Łatwo zobaczyć, że $\bigcap_{t\in T} f(A_t) = \{7\}$ a $f(\bigcap_{t\in T}(A_t)) = f(\varnothing) = \varnothing$.

ad. 6. $x \in f^{-1}(B_1 \cup B_2) \iff f(x) \in B_1 \cup B_2 \iff f(x) \in B_1 \vee\ f(x) \in B_2 \iff x \in f^{-1}(B_1) \vee x \in f^{-1}(B_2) \iff x \in f^{-1}(B_1) \cup f^{-1}(B_2)$.

ad. 7. $x \in f^{-1}(\bigcup_{t\in T} B_t) \iff f(x) \in \bigcup_{t\in T} B_t \iff \exists t_0 \in T : f(x) \in B_{t_0} \iff \exists t_0 \in T : x \in f^{-1}(B_{t_0}) \iff x \in \bigcup_{t\in T} f^{-1}(B_t)$.

ad. 8. $x \in f^{-1}(B_1 \cap B_2) \iff f(x) \in B_1 \cap B_2 \iff f(x) \in B_1 \wedge\ f(x) \in B_2 \iff x \in f^{-1}(B_1) \wedge x \in f^{-1}(B_2) \iff x \in f^{-1}(B_1) \cap f^{-1}(B_2)$.

ad. 9. $x \in f^{-1}(\bigcap_{t\in T} B_t) \iff f(x) \in \bigcap_{t\in T} B_t \iff \forall t \in T : f(x) \in B_t \iff \forall t \in T : x \in f^{-1}(B_t) \iff x \in \bigcap_{t\in T} f^{-1}(B_t)$.

ad. 10. $x \in f^{-1}(B_1 \setminus B_2) \iff f(x) \in B_1 \setminus B_2 \iff f(x) \in B_1 \wedge \neg(f(x) \in B_2) \iff x \in f^{-1}(B_1) \wedge \neg(x \in f^{-1}(B_2)) \iff x \in f^{-1}(B_1) \setminus f^{-1}(B_2)$. □

Uwaga 6.17. Warto zauważyć, że jeśli funkcja $f : X \to Y$ jest bijekcją, to obraz przez f^{-1} zbioru $B \subset Y$ jest równy przeciwobrazowi tego zbioru przez funkcję f. Dowód pozostawiamy czytelnikowi jako proste (ale ważne) ćwiczenie.

Rozdział 7

Relacje równoważności, klasy abstrakcji, zbiór ilorazowy

Na tym wykładzie zdefiniujemy pewien szczególny typ relacji – relację równoważności, podamy przykłady i własności tych relacji. Pojawi się pojęcie klasy abstrakcji i zbioru ilorazowego. Warto przypomnieć sobie własności relacji, zwłaszcza definicje 4.17, 4.21, 4.27.

Definicja 7.1. Niech dany będzie zbiór niepusty X i relacja $R \subset X \times X$. Relację R nazywamy *relacją równoważności*, gdy jest zwrotna, symetryczna i przechodnia.

Przykład 7.2.

- Niech $X = \mathbb{N} \cup \{0\}$. Zadajmy relację R warunkiem $x\,R\,y \iff 2|(x+y)$ (dwa dzieli $x+y$). Faktycznie, jest to relacja równoważności: jest zwrotna, bo $2|2x$; symetryczna, bo $2|(x+y) \implies 2|(y+x)$; oraz przechodnia – bo jeśli $2|(x+y) \wedge 2|(y+z)$, to $x+y=2s$, $y+z=2t$ dla pewnych s,t naturalnych, zatem $x+2y+z=2(s+t)$, czyli $x+z=2(s+t-y)$, zatem $2|(x+z)$.
- Relacja równoległości w zbiorze prostych na płaszczyźnie jest relacją równoważności (ćwiczenie).
- Relacja podobieństwa w zbiorze trójkątów na płaszczyźnie też jest relacją równoważności (ćwiczenie).
- Relacja podzielności w zbiorze $\mathbb{N}$ **nie** jest relacją równoważności (bo nie jest symetryczna).

Definicja 7.3. Niech $R \subset X \times X$ będzie relacją równoważności. *Klasą abstrakcji* $[x]_R$ *elementu* $x \in X$ *w relacji* R nazywamy zbiór wszystkich elementów $y \in X$, które są w relacji R z elementem x:

$$[x]_R = \{y \in X : x\,R\,y\}.$$

Uwaga 7.4. Zauważmy, że klasa abstrakcji elementu $x \in X$ jest zawsze zbiorem niepustym. Ponieważ relacja równoważności jest zwrotna, to zawsze $x\,R\,x$, a zatem $x \in [x]_R$.

Rozważmy teraz relacje równoważności z przykładu 7.2.

Przykład 7.5.

- Pierwsza relacja ma dwie klasy abstrakcji – jedną są wszystkie liczby parzyste, a drugą wszystkie nieparzyste (bo dwie liczby są ze sobą w relacji gdy mają tę samą resztę z dzielenia przez dwa).
- W relacji równoległości w zbiorze prostych na płaszczyźnie klasą abstrakcji danej prostej są wszystkie proste równoległe do danej prostej.
- Klasą abstrakcji danego trójkąta w relacji podobieństwa w zbiorze trójkątów na płaszczyźnie jest zbiór wszystkich trójkątów podobnych do danego.

Zdefiniujemy teraz pojęcie podziału zbioru.

Definicja 7.6.

- Mówimy, że *rodzina zbiorów* $\{A_j\}_{j\in J}$ *pokrywa zbiór* X jeśli $X = \bigcup_{j\in J} A_j$. Mówimy też, że rodzina $\{A_j\}_{j\in J}$ jest pokryciem zbioru X.

- Rodzina zbiorów $\{A_j\}_{j\in J}$ nazywa się *podziałem zbioru* X, jeśli
  (a) rodzina $\{A_j\}_{j\in J}$ jest pokryciem X,
  (b) zbiory A_j są parami rozłączne: $A_i \cap A_j = \varnothing$, $\forall_{i,j\in J} : i \neq j$,
  (c) zbiory A_j są niepuste: $A_j \neq \varnothing$ $\forall j \in J$.

Uwaga 7.7. Nietrudno sprawdzić że klasy abstrakcji z przykładu 7.5 tworzą podział zbioru, na którym dana relacja jest określona. Nie jest to przypadek, jak zobaczymy w poniższym twierdzeniu.

Twierdzenie 7.8. *Niech X będzie zbiorem niepustym, a R relacją równoważności na X. Wówczas klasy abstrakcji relacji R tworzą podział zbioru X.*

Dowód. 1. Zauważmy, że dla dowolnego $x \in X$ zachodzi (ze zwrotności relacji R) $x \in [x]_R$. Wynika stąd, że wszystkie klasy abstrakcji są zbiorami niepustymi, zatem warunek (c) definicji podziału jest spełniony.

2. Ponieważ $x \in [x]_R$, to $\{x\} \subset [x]_R$, a zatem, skoro mamy $\bigcup_{x\in X}[x]_R \subset X$ (bo klasy abstrakcji są wszystkie podzbiorami X) oraz mamy $X = \bigcup_{x\in X}\{x\} \subset \bigcup_{x\in X}[x]_R$, a więc $\{[x]_R\}_{x\in X}$ jest pokryciem X, warunek (a) jest zatem spełniony.

3. Pozostaje sprawdzić warunek (b). Wykażemy najpierw lemat.

Lemat 7.9. *Dla dowolnych $x_1, x_2 \in X$ zachodzi*

$$[x_1]_R = [x_2]_R \iff x_1 \, R \, x_2.$$

Dowód lematu 7.9. ($\Longrightarrow$): $[x_1]_R = [x_2]_R \Longrightarrow x_1 \in [x_2]_R \Longrightarrow x_1 R x_2$.
($\Longleftarrow$): Przypuśćmy, że $[x_1]_R \neq [x_2]_R$. Zatem, możemy bez zmniejszenia ogólności, przypuścić, że istnieje $y \in [x_1]_R$, takie, że $y \notin [x_2]_R$. Skoro $y \in [x_1]_R$, to $y \, R \, x_1$. Zarazem, z założenia, $x_1 \, R \, x_2$. Z przechodniości relacji R mamy, że $y \, R \, x_2$, czyli $y \in [x_2]_R$, sprzeczność. □

Kolejny fakt również sformułujemy jako lemat.

Lemat 7.10. *Klasy abstrakcji relacji równoważności są równe albo rozłączne, czyli:*

$$[x_1]_R \cap [x_2]_R \neq \varnothing \Longrightarrow [x_1]_R = [x_2]_R.$$

Dowód lematu 7.10. Jeśli $[x_1]_R \cap [x_2]_R \neq \varnothing$ to istnieje $y \in [x_1]_R \cap [x_2]_R$, skąd $x_1 R y$ i $y R x_2$, a zatem, z przechodniości relacji R, $x_1 \, R \, x_2$. Stąd, na podstawie lematu 7.9, mamy $[x_1]_R = [x_2]_R$. □

Ostatni lemat pokazuje, że warunek (b) z definicji 7.6 jest spełniony (dwie różne klasy abstrakcji są rozłączne), a zatem klasy abstrakcji dają podział zbioru X. □

Wykażemy teraz stwierdzenie w pewnym sensie odwrotne do twierdzenia 7.8, mianowicie mówiące, że jeśli mamy dany podział zbioru, to istnieje relacja równoważności, której klasy abstrakcji są dokładnie zbiorami z tego podziału.

Stwierdzenie 7.11. *Niech X będzie zbiorem niepustym, a $\{A_j\}_{j\in J}$ podziałem zbioru X. Wtedy istnieje relacja równoważności R_A, dla której klasy równoważności to zbiory z podziału.*

Dowód. Zdefiniujmy relację R_A w taki sposób:

$$\forall x_1, x_2 \in X, x_1 \, R_A \, x_2 \iff \exists j \in J : x_1 \in A_j \wedge x_2 \in A_j.$$

Aby zakończyć dowód wystarczy sprawdzić, że R_A jest relacją równoważności (wtedy zbiory A_j są jej klasami abstrakcji).

Relacja R_A jest zwrotna, bo dla dowolnego $x \in X$, skoro $X = \bigcup_{j\in J} A_j$, mamy istnienie j_0 takiego, że $x \in A_{j_0}$, a zatem $x \, R_A \, x$.

Relacja R_A jest oczywiście symetryczna, bo $x \, R_A \, y \iff \exists_{j\in J} : x, y \in A_j \iff \exists_{j\in J} : y, x \in A_j \iff y \, R_A \, x$.

Sprawdzimy teraz przechodniość relacji R_A. Niech $x \, R_A \, y$ i $y \, R_A \, z$, dla pewnych $x, y, z \in X$. Z definicji R_A mamy istnienie j_1 takiego, że $x, y \in A_{j_1}$ i istnienie j_2 takiego, że $y, z \in A_{j_2}$. Zatem $y \in A_{j_1} \cap A_{j_2}$, ale dla $j_1 \neq j_2$ z definicji podziału mamy $A_{j_1} \cap A_{j_2} = \varnothing$, zatem musi być $j_1 = j_2$. Stąd, $x, y, z \in A_{j_1}$, a zatem $x \, R_A \, z$. □

Zdefiniujemy teraz pojęcie zbioru ilorazowego.
Niech X będzie zbiorem niepustym a R relacją równoważności na tym zbiorze.

Definicja 7.12. Zbiorem ilorazowym relacji R (albo ilorazem zbioru X przez relację R) nazywamy zbiór wszystkich klas abstrakcji tej relacji.

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

Przykład 7.13.

- Niech $X = \mathbb{N} \times \mathbb{N}$. Zdefiniujmy relację R następująco. Dla dowolnych $(m_1, n_1), (m_2, n_2) \in X$

$$(m_1, n_1)\, R\, (m_2, n_2) \iff m_1 + n_2 = m_2 + n_1.$$

  Jako ćwiczenie zostawiamy sprawdzenie, że R jest faktycznie relacją równoważności, a zbiór klas abstrakcji tej relacji można utożsamiać ze zbiorem liczb całkowitych (Wskazówka: $z = m_1 - n_1$).

- Niech $X = \mathbb{Z} \times \mathbb{N}^*$. Zdefiniujmy relację R następująco. Dla dowolnych $(m_1, n_1), (m_2, n_2) \in X$

$$(m_1, n_1)\, R\, (m_2, n_2) \iff m_1 \cdot n_2 = m_2 \cdot n_1.$$

  Jako ćwiczenie zostawiamy tu też sprawdzenie, że R jest faktycznie relacją równoważności, a zbiór klas abstrakcji tej relacji można utożsamiać ze zbiorem liczb wymiernych (Wskazówka: $q = \frac{m_1}{n_1}$).

Na zakończenie tego wykładu powiemy kilka słów o zgodności funkcji z relacją równoważności.

Definicja 7.14.

- Jeśli mamy relację równoważności R na zbiorze X i funkcję $f : X \to X$, to mówimy, że ta funkcja f jest *zgodna z relacją* R, jeśli dla dowolnych $x, y \in X$ zachodzi $x\, R\, y \implies f(x)\, R\, f(y)$.

- Podobnie, jeśli mamy relację równoważności R na zbiorze X i funkcję $f : X \times X \to X$, to mówimy, że ta funkcja f jest *zgodna z relacją* R, jeśli dla dowolnych $x, y, x_1, y_1 \in X$ zachodzi $x\, R\, x_1 \wedge y\, R\, y_1 \implies f(x, y)\, R\, f(x_1, y_1)$.

Przykład 7.15. (Dodawanie liczb całkowitych). Niech $[(m, n)]_R$ będzie klasą abstrakcji w relacji R zdefiniowanej w pierwszym punkcie przykładu 7.13, zatem liczbą całkowitą. Zdefiniujmy funkcję dodawania $f : X \times X \to X$ następująco: $f((m, n), (a, b)) = (m + a, n + b)$. Sprawdzimy, że tak zdefiniowane dodawanie jest zgodne z relacją R. Jeśli $(m, n)\, R\, (m_1, n_1)$, to z definicji R mamy $m + n_1 = n + m_1$, tak samo $(a, b)\, R\, (a_1, b_1)$ gdy $a + b_1 = a_1 + b$. Zatem: $m + n_1 + a + b_1 = n + m_1 + a_1 + b$ czyli w relacji są pary $(m + a, n + b), (m_1 + a_1, n_1 + b_1)$, czyli tak określone dodawanie jest zgodne z relacją definiującą liczby całkowite.

Rozdział 8

Relacje porządku i elementy wyróżnione.

Zdefiniujemy teraz kolejny rodzaj relacji – relacje porządku. Warto powtórzyć własności relacji z definicji 4.17, 4.27, 4.25. Podamy definicje i własności elementów wyróżnionych (np. elementu maksymalnego, największego). Omówimy pewne rodzaje porządków, w tym dobry porządek, i podamy twierdzenie Zermelo o dobrym uporządkowaniu (na razie bez dowodu).

Definicja 8.1. Niech X będzie niepustym zbiorem a $R \subset X \times X$ relacją na tym zbiorze. Relację tę nazywamy *relacją porządku* (*częściowego*), jeśli relacja R jest zwrotna, przechodnia i słabo antysymetryczna. Zbiór X z relacją (częściowego) porządku R zapisujemy (X, R) i mówimy, że X jest *zbiorem częściowo uporządkowanym*.

Relację porządku często oznaczmy symbolem $\leqslant$ albo $\preccurlyeq$, a zapis $x \leqslant y$ czytamy standardowo *x jest mniejsze lub równe od y* lub też *y jest większe lub równe od x*.

Mówiąc *x jest mniejsze od y*, mamy na myśli, że x jest mniejsze lub równe od y i x jest różne od y.

Słowo *częściowy* pojawia się w powyższej definicji jako podkreślenie faktu, że w danym porządku mogą się zdarzyć elementy, których nie możemy porównać – jak w poniższym przykładzie w punkcie 3.

Przykład 8.2. 1. Zbiorem uporządkowanym jest $(\mathbb{N}, \leqslant)$, gdzie $\leqslant$ oznacza standardową nierówność pomiędzy liczbami naturalnymi.

2. Podobnie, zbiorem uporządkowanym jest $(\mathbb{R}, \leqslant)$, ale nie $(\mathbb{R}, <)$ – relacja $<$ nie jest zwrotna.

3. Niech $X = \mathbb{N}^*$. Relację porządku oznaczoną jako $\preccurlyeq$ zdefiniujmy następująco: $n \preccurlyeq m \iff n|m$. Łatwo sprawdzić, że $\preccurlyeq$ jest faktycznie relacją porządku. Faktycznie, relacja jest zwrotna, bo dla każdego $n \in \mathbb{N}$ n dzieli n; jest przechodnia, bo jeśli $n|m$ i $m|p$ to $m = kn$ i $p = lm$ dla pewnych naturalnych k i l, skąd $p = lkn$, więc $n|p$ czyli $n \preccurlyeq p$. Relacja jest też słabo antysymetryczna, to znaczy $m \preccurlyeq n \wedge m \preccurlyeq n \implies m = n$. Rzeczywiście, mamy $m = kn \wedge n = lm$ dla pewnych naturalnych k, l, skąd $m = klm$ a zatem $k = l = 1$ a zatem $m = n$. W tej relacji mamy na przykład $3 \preccurlyeq 6$ i $3 \preccurlyeq 9$, ale elementy 6 i 9 są nieporównywalne, bo ani 6 nie dzieli 9, ani 9 nie dzieli 6.

4. Na zbiorze takim, jak „drzewko" na rysunku 8.1 definiujemy porządek tak, że większe są elementy leżące „wyżej na gałęzi". Elementy na różnych gałęziach są nieporównywalne.

Uwaga 8.3. Jeśli mamy dane zbiory częściowo uporządkowane $(X_1, \leqslant_1), \ldots, (X_k, \leqslant_k)$, to w iloczynie kartezjańskim $X_1 \times \cdots \times X_k$ możemy zdefiniować porządek przykładowo tak: $(x_1, \ldots, x_k) \preceq (y_1, \ldots, y_k) \iff (x_1 \leqslant_1 y_1 \wedge x_1 \neq y_1) \vee (x_1 = y_1 \wedge x_2 \leqslant_2 y_2 \wedge x_2 \neq y_2) \vee \cdots \vee (x_1 = y_1 \wedge \cdots \wedge x_{k-1} = y_{k-1} \wedge x_k \leqslant_k y_k)$. $\preceq$ nazywamy *porządkiem leksykograficznym* (na takiej zasadzie układa się wyrazy alfabetycznie).

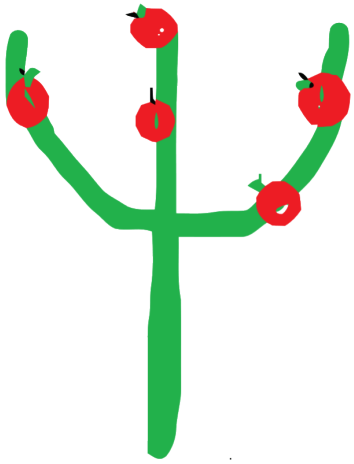
Uwaga 8.4. Jeśli mamy podzbiór A zawarty w zbiorze częściowo uporządkowanym $(X, \leqslant)$, to zbiór A z relacją porządku zacieśnioną do tego zbioru, zapisywany jako $(A, \leqslant_A)$, też jest zbiorem częściowo uporządkowanym. Zazwyczaj piszemy też $(A, \leqslant)$, pomijając oznaczenie zacieśnienia.

Niektóre elementy w zbiorze częściowo uporządkowanym mają, ze względu na porządek, pewne interesujące własności. Nazywamy je *elementami wyróżnionymi*. Poniżej zdefiniujemy i omówimy rodzaje elementów wyróżnionych – elementy maksymalne, minimalne, największe i najmniejsze.

Definicja 8.5. Niech $(X, \leqslant)$ będzie zbiorem częściowo uporządkowanym.

- Element $x_0 \in X$ nazywamy *elementem maksymalnym* zbioru X, jeśli dla dowolnego $x \in X$ zachodzi wynikanie $x_0 \leqslant x \implies x_0 = x$.

Rysunek 8.1:



- Element $x_0 \in X$ nazywamy *elementem minimalnym* zbioru X, jeśli dla dowolnego $x \in X$ zachodzi wynikanie $x \leqslant x_0 \implies x_0 = x$.

Mówiąc słowami, element x_0 jest elementem maksymalnym, jeśli z tego, że jakiś element x jest od niego większy lub równy wynika, że x musi być równe x_0, czyli, nie ma elementów, które są większe od x_0 – natomiast mogą być takie, które są z nim nieporównywalne.

Analogicznie, element x_0 jest elementem minimalnym, jeśli z tego, że jakiś element x jest od niego mniejszy lub równy wynika, że x musi być równe x_0, czyli, nie ma elementów, które są mniejsze od x_0 – natomiast mogą być takie, które są z nim nieporównywalne.

Przykład 8.6. 1. Niech A będzie zbiorem niepustym i niech $X = \mathcal{P}(A)$ będzie jego zbiorem podzbiorów uporządkowanym przez relację inkluzji. Wtedy A jest (jedynym) elementem maksymalnym w X a $\varnothing$ jedynym elementem minimalnym.

2. Weźmy $(\mathbb{N}^*, \preccurlyeq)$ jak w przykładzie 8.2.3. Weźmy podzbiór $A = \{4, 8, 12, 7, 3\} \subset \mathbb{N}$ z relacją $\preccurlyeq|_A$. Wówczas elementami maksymalnymi w A są $8, 12, 7$ a elementami minimalnymi $3, 4, 7$. (7 jest elementem, który jest równocześnie maksymalny jak i minimalny.)

3. Niech teraz $X = \{2, 3, 4, \dots\}$ z relacją porządku $\preceq$ zdefiniowaną następująco: $x \preceq y \iff y|x$. Jako proste ćwiczenie zostawiamy sprawdzenie, że tak określona relacja $\preceq$ jest faktycznie relacją porządku. Zbiór $(X, \preceq)$ ma nieskończenie wiele elementów maksymalnych, są to liczby pierwsze. Gdy p jest liczbą pierwszą a $n \in X$, to $n|p \implies n = p$.

Zdefiniujemy teraz element największy i najmniejszy.

Definicja 8.7. Niech $(X, \leqslant)$ będzie zbiorem częściowo uporządkowanym.

- Element $x_0 \in X$ jest *elementem największym* zbioru X, jeśli dla każdego $x \in X$ zachodzi $x \leqslant x_0$.
- Element $x_0 \in X$ jest *elementem najmniejszym* zbioru X, jeśli dla każdego $x \in X$ zachodzi $x_0 \leqslant x$.

Warto zwrócić uwagę, że każdy element zbioru X musi być porównywalny z elementem największym (lub najmniejszym) – o ile taki istnieje.

Przyjrzymy się teraz zbiorom uporządkowanym z przykładu 8.6.

Przykład 8.8. 1. Niech A będzie zbiorem niepustym i niech $X = \mathcal{P}(A)$ będzie jego zbiorem podzbiorów uporządkowanym przez relację inkluzji. Zbiór A jest (jedynym) elementem największym w X (zawiera każdy jego podzbiór), $\varnothing$ elementem najmniejszym w X (zawiera się w każdym podzbiorze).

2. Niech $(X, \leqslant) = (\mathbb{N}^*, \preccurlyeq)$. Ten zbiór ma element najmniejszy (1 dzieli każdą liczbę naturalną) i nie ma elementu największego (nie ma liczby naturalnej podzielnej przez wszystkie inne).

3. Niech $(X, \leqslant) = (\mathbb{N}_{\geqslant 2}, \preceq)$. Ten zbiór nie ma elementu najmniejszego (nie ma w nim liczby naturalnej, która dzieli wszystkie w tym zbiorze), nie ma też elementu największego.

Wykażemy teraz pewne własności poznanych elementów wyróżnionych.

Stwierdzenie 8.9. *Niech $(X, \leqslant)$ będzie zbiorem częściowo uporządkowanym. Wówczas w X istnieje co najwyżej jeden element największy. Jeśli istnieje, to jest też jedynym elementem maksymalnym.*

Dowód. Niech x_0 i x_1 będą największymi elementami w zbiorze X. Skoro x_0 jest elementem największym, to $x_1 \leqslant x_0$. Skoro x_1 jest elementem największym to $x_0 \leqslant x_1$. Ze słabej antysymetrii relacji porządku dostajemy, że $x_0 = x_1$, a zatem element największy jest jedyny.

Wykażemy teraz, że x_0 – element największy, jest też elementem maksymalnym. Musimy sprawdzić, że dla dowolnego $x_1 \in X$, $x_0 \leqslant x_1 \Longrightarrow x_0 = x_1$ Przypuśćmy zatem, że jest jakiś element $x_1 \in X$ taki, że $x_0 \leqslant x_1$. Zarazem x_0 jest elementem największym, czyli $x_1 \leqslant x_0$. Stąd (słaba antysymetria) mamy $x_0 = x_1$. Zatem sprawdziliśmy, że x_0 jest elementem maksymalnym. Gdyby istniał inny element maksymalny, powiedzmy x_2 to, ponieważ x_0 jest największym elementem, mamy $x_2 \leqslant x_0$ skąd, ponieważ x_2 miał być maksymalny, $x_2 = x_0$. □

Kolejne stwierdzenie dotyczy elementu najmniejszego:

Stwierdzenie 8.10. *Niech $(X, \leqslant)$ będzie zbiorem częściowo uporządkowanym. Wówczas w X istnieje co najwyżej jeden element najmniejszy. Jeśli istnieje, to jest też jedynym elementem minimalnym.*

Dowód tego stwierdzenia, analogiczny do dowodu stwierdzenia 8.9, zostawiamy czytelnikowi jako ćwiczenie.

Przejdziemy teraz do zdefiniowania majoranty (ograniczenia górnego) i minoranty (ograniczenia dolnego) zbioru uporządkowanego.

Definicja 8.11. Niech $(X, \leqslant)$ będzie zbiorem częściowo uporządkowanym. Niech A będzie podzbiorem zbioru X.

- Element $M \in X$ nazywamy *majorantą* zbioru A, jeśli dla każdego $a \in A$ zachodzi $a \leqslant M$.
- Element $m \in X$ nazywamy *minorantą* zbioru A, jeśli dla każdego $a \in A$ zachodzi $m \leqslant a$.

Przykład 8.12. • Niech $X = \mathbb{R}$ z naturalnym porządkiem $\leqslant$. Niech $A = \{1, \frac{1}{2}, \frac{1}{3}, \dots\}$. Majorantami tego zbioru są na przykład 2, $\sqrt{7}$, 158.5, 1 a minorantami $-\sqrt{2}$, -30, 0.

• Dla X jak poprzednio, niech $A = [-1, 1]$. Majorantami A są na przykład $2, \sqrt{17}, 1$ a minorantami -3, -2, $-\sqrt{17}$, -1. Zauważmy, że 1 jest specjalną majorantą A (nie ma mniejszej) a -1 specjalną minorantą A (nie ma większej).

Niech $(X, \leqslant)$ będzie zbiorem częściowo uporządkowanym. Niech A będzie podzbiorem zbioru X. Zdefiniujmy dwa zbiory:

$$A_M = \{M \in X : M \text{ jest majorantą } A\},$$

zbiór majorant zbioru A oraz

$$A_m = \{m \in X : M \text{ jest minorantą } A\},$$

zbiór minorant zbioru A.

Definicja 8.13. Dla $(X, \leqslant)$ jak powyżej i podzbioru $A \subset X$ definiujemy

- *kres górny zbioru A*, inaczej *supremum A*, jako najmniejszy element zbioru A_M (o ile istnieje). Supremum zbioru A oznaczamy $\sup A$.
- *kres dolny zbioru A*, inaczej *infimum A*, jako największy element zbioru A_m (o ile istnieje). Infimum zbioru A oznaczamy $\inf A$.

O jedyności supremum (infimum) mówi następujące stwierdzenie:

Stwierdzenie 8.14. *Niech $(X, \leqslant)$ będzie zbiorem częściowo uporządkowanym i niech A będzie podzbiorem zbioru X. Jeśli istnieje element X będący supremum (infimum) zbioru A, to jest on jedyny.*

Dowód. Dowód jest natychmiastowy ze stwierdzeń 8.9 i 8.10 o jedyności elementu największego bądź najmniejszego. □

Kolejne stwierdzenie mówi, że w niektórych przypadkach łatwo zidentyfikować supremum (infimum) zbioru A.

Stwierdzenie 8.15. *Niech $(X, \leqslant)$ będzie zbiorem częściowo uporządkowanym i niech A będzie podzbiorem zbioru X.*

1. *Jeśli x_0 jest elementem największym zbioru A, to $x_0 = \sup A$.*

2. *Jeśli x_0 jest elementem najmniejszym zbioru A, to $x_0 = \inf A$.*

Dowód. ad. 1. Po pierwsze, x_0 jest majorantą zbioru A, bo z definicji elementu największego mamy dla każdego $a \in A$: $a \leqslant x_0$. Po drugie, jeśli $x_1 \in X$ jest najmniejszą majorantą zbioru A to w szczególności $x_0 \leqslant x_1$ (bo $x_0 \in A$), ale też $x_1 \leqslant x_0$ bo x_0 jest majorantą a x_1 najmniejszą z majorant. Stąd $x_0 = x_1$.

ad. 2. Dowód jest analogiczny. Po pierwsze, x_0 jest minorantą zbioru A, bo z definicji elementu najmniejszego mamy dla każdego $a \in A$: $x_0 \leqslant a$. Po drugie, jeśli $x_1 \in X$ jest największą minorantą zbioru A, to w szczególności $x_1 \leqslant x_0$ (bo $x_0 \in A$), ale też $x_0 \leqslant x_1$, bo x_0 jest minorantą a x_1 największą z minorant. Stąd $x_0 = x_1$. □

Zajmiemy się teraz zdefiniowaniem i omówieniem pewnych specjalnych relacji porządku. Niech zbiór $(X, \leqslant)$ będzie zbiorem częściowo uporządkowanym.

Definicja 8.16. Zbiór $(X, \leqslant)$ jest *uporządkowany liniowo*, jeśli relacja porządku $\leqslant$ jest relacją spójną, czyli

$$\forall_{x,y \in X}\ x \leqslant y \vee y \leqslant x \vee x = y.$$

Przykład 8.17.

- Zbiór R z naturalnym porządkiem $\leqslant$ jest uporządkowany liniowo.
- Zbiór $\mathbb{N}^*$ z relacją porządku $\preccurlyeq$ jak z przykładu 8.2.3. nie jest liniowo uporządkowany (np. elementy 2 i 3 nie są porównywalne).
- Zbiór $\{2^n, n \in \mathbb{N}\}$ z relacją porządku $\preccurlyeq$ jak powyżej jest uporządkowany liniowo.

Uwaga 8.18. Jeśli zbiór $(X, \leqslant)$ jest liniowo uporządkowany, to każdy jego podzbiorów $A \subset X$ z relacją $\leqslant|_A$ też jest liniowo uporządkowany.

Definicja 8.19. Niech zbiór $(X, \leqslant)$ będzie częściowo uporządkowany. Podzbiór $A \subset X$ nazywamy *łańcuchem*, jeśli $(A, \leqslant_A)$ jest uporządkowany liniowo.

Przykład 8.20.

- Zbiór $\mathbb{N}^*$ z relacją porządku $\preccurlyeq$ jak w przykładzie 8.17 powyżej nie jest liniowo uporządkowany, ale jego podzbiór $A = \{2^n, n \in \mathbb{N}\}$ z relacją porządku $\preccurlyeq_A$ jest uporządkowany liniowo, czyli jest łańcuchem.
- Zbiór $\{3, 6, 12, 18\}$ z powyższą relacją $\preccurlyeq$ ma łańcuchy: $\{3, 6, 18\}, \{3, 6, 12\}$.

Kolejny rodzaj uporządkowania zbioru to uporządkowanie gęste.

Definicja 8.21. Niech zbiór $(X, \leqslant)$ będzie uporządkowany liniowo. Mówimy, że ten zbiór jest *uporządkowany gęsto*, jeśli

$$\forall_{x,y,z \in X} : x \leqslant y \wedge x \neq y\ \exists_{z \in X} : x \leqslant z \wedge z \leqslant y\ \ \wedge x \neq z \wedge y \neq z,$$

tzn. pomiędzy każde dwa różne elementy tego możemy wstawić trzeci element tego zbioru, różny od nich.

Przykład 8.22.

- Zbiór $\mathbb{Q}$ z relacją naturalnego porządku $\leqslant$ jest uporządkowany gęsto (wystarczy wziąć $z = \frac{x+y}{2}$).
- Zbiór $\mathbb{N}$ z relacją naturalnego porządku $\leqslant$ nie jest uporządkowany gęsto.

Przejdziemy teraz do pojęcia *dobrego porządku.* Załóżmy, że rozważany poniżej zbiór X jest niepusty. Zdefiniujmy dobry porządek:

Definicja 8.23. Niech $(X, \leqslant)$ będzie zbiorem uporządkowanym liniowo. Mówimy, że $(X, \leqslant)$ jest *uporządkowany dobrze* (albo, że $\leqslant$ jest *dobrym porządkiem*), gdy każdy niepusty podzbiór zbioru X ma element najmniejszy (w sensie porządku $\leqslant$), czyli

$$\forall_{A \subset X}\ A \neq \varnothing \Longrightarrow \exists_{a \in A}\ \forall_{x \in A}\ a \leqslant x.$$

Przykład 8.24. Zbiór liczb naturalnych $(\mathbb{N}, \leqslant)$ jest dobrze uporządkowany (formalny dowód Czytelnik znajdzie, czytając wykład 15), zbiór $(\mathbb{Z}, \leqslant)$ nie jest dobrze uporządkowany. Zbiór $(\{1 - \frac{1}{n} | n \in \mathbb{N}\} \cup \{1\}, \leqslant)$ jest dobrze uporządkowany.

Na wykładzie 14 udowodnimy ważne twierdzenie, pochodzące od niemieckiego matematyka Ernesta Zermelo. Twierdzenie to mówi, że każdy zbiór można dobrze uporządkować. Poniżej podamy (na razie bez dowodu) pewną wersję tego twierdzenia. Zaczniemy od definicji odcinka początkowego zbioru.

Definicja 8.25. Niech X będzie zbiorem uporządkowanym liniowo. Podzbiór $\mathcal{O} \subset X$ nazywamy *odcinkiem początkowym*, jeśli spełniony jest warunek

$$y \in \mathcal{O} \wedge x \leqslant y \Longrightarrow x \in \mathcal{O}.$$

Odcinkiem początkowym wyznaczonym przez element $a \in X$ nazywamy

$$\mathcal{O}(a) = \{x \in X : x \leqslant a \wedge x \neq a\}.$$

Domkniętym odcinkiem początkowym wyznaczonym przez element $a \in X$ nazywamy

$$\mathcal{D}(a) = \mathcal{O}(a) \cup \{a\}.$$

Przykład 8.26. Jeśli $(X, \leqslant)$ jest zbiorem liczb rzeczywistych z naturalnym porządkiem, to dla $a \in \mathbb{R}$ odcinek początkowy $\mathcal{O}(a)$ jest równy $(-\infty, a)$.

Niech teraz $(X, \leqslant)$ będzie zbiorem dobrze uporządkowanym. Weźmy funkcję

$$f : \mathcal{P}(X) \setminus \{X\} \to X$$

taką, że

$$f(A) \in X \setminus A.$$

Definicja 8.27. Niech $(X, \leqslant)$ będzie zbiorem dobrze uporządkowanym a $f : \mathcal{P}(X) \setminus \{X\} \to X$ funkcją jak powyżej. Mówimy, że *porządek* $\leqslant$ *jest zgodny z* f, jeśli dla każdego $a \in X$ zachodzi

$$a = f(\mathcal{O}(a)).$$

Możemy teraz sformułować twierdzenie Zermelo.

Twierdzenie 8.28 (Zermelo)**.** *Niech X będzie dowolnym zbiorem (niepustym). Niech $f : \mathcal{P}(X) \setminus \{X\} \to X$ będzie funkcją taką, że $f(A) \in X \setminus A$. Wówczas istnieje dokładnie jeden porządek na X, dobry i zgodny z f.*

Jako proste ćwiczenie dla czytelnika proponujemy znaleźć dobre uporządkowanie zbioru $\mathbb{Z}$.

Powiemy teraz parę słów na temat podobieństwa zbiorów liniowo uporządkowanych (tę część materiału można traktować jako nieobowiązkową).

Niech $(X, \leqslant)$ i $(X^*, \leqslant^*)$ będą dwoma liniowo uporządkowanymi zbiorami.

Definicja 8.29. Mówimy, że $(X, \leqslant)$ i $(X^*, \leqslant^*)$ są *podobne*, jeśli istnieje bijekcja $f : X \hookrightarrow X^*$ taka, że dla wszystkich $x, y \in X$ zachodzi $x \leqslant y \iff f(x) \leqslant^* f(y)$.

Przykład 8.30. Niech $(X, \leqslant) = (\mathbb{Z}, \leqslant)$ i $(X^*, \leqslant^*) = (\mathbb{N}, \leqslant^*)$, gdzie dla $m, n \in \mathbb{N}$ mamy

$$m \leqslant^* n \iff \begin{cases} m \text{ parzyste, } n \text{ nieparzyste} \\ m \text{ parzyste, } n \text{ parzyste i } n \leqslant m \\ m \text{ nieparzyste, } n \text{ nieparzyste i } m \leqslant n. \end{cases}$$

Łatwo sprawdzić, że $\leqslant^*$ jest liniowym porządkiem na $\mathbb{N}$. Jeśli zdefiniujemy bijekcję $f : \mathbb{Z} \hookrightarrow \mathbb{N}$ wzorem

$$f(k) = \begin{cases} 2k + 1, & k \geqslant 0 \\ -2k, & k < 0, \end{cases}$$

to nietrudno sprawdzić, że $m \leqslant n \iff f(m) \leqslant^* f(n)$, a zatem $(\mathbb{Z}, \leqslant)$ i $(\mathbb{N}, \leqslant^*)$ są podobne.

Przykład 8.31. 1. Wspomniany wyżej zbiór $(\{1 - \frac{1}{n} | n \in \mathbb{N}\} \cup \{1\}, \leqslant)$ jest dobrze uporządkowany, jest równoliczny z $\mathbb{N}$ (zobacz wykład 9), ale nie jest podobny do $\mathbb{N}$, bo 1 jest największym elementem tego zbioru, a w $\mathbb{N}$ nie ma największego elementu.

2. Zbiory $\mathbb{Z}$ i $\mathbb{Q}$ z naturalnym porządkiem nie są podobne – porządek na $\mathbb{Q}$ jest gęsty, a na $\mathbb{Z}$ nie.

Uwaga 8.32. Nietrudno sprawdzić, że relacja podobieństwa zbiorów liniowo uporządkowanych jest relacją równoważności.

Zbiorom liniowo uporządkowanym przypisujemy ten sam *typ porządkowy*, jeśli są podobne.

Zainteresowany czytelnik o typach porządkowych zbiorów może poczytać na przykład w [9, 3].

Rozdział 9

Teoria mocy, zbiory przeliczalne

Na tym wykładzie przechodzimy do podstaw teorii mocy. Zdefiniujemy relację równoliczności zbiorów, moc zbiorów, następnie powiemy co to znaczy, że zbiór jest skończony, przeliczalny, oraz wykażemy pewne twierdzenia o zbiorach przeliczalnych.

Definicja 9.1. Niech dane będą dwa zbiory A i B. Mówimy, że zbiory A i B są *równoliczne*, jeśli istnieje między nimi bijekcja

$$f : A \hookrightarrow\!\!\!\!\rightarrow B.$$

Piszemy $A \sim B$.

Definicja 9.2. Mówimy, że zbiór A jest skończony i ma n elementów (gdzie n jest liczbą $0, 1, 2, \ldots$), jeśli

- A jest zbiorem pustym, i wtedy $n = 0$ albo
- $A \sim \{1, 2, \ldots, n\}$.

Uwaga 9.3. W powyższej sytuacji piszemy $\#A = n$ albo $\mathrm{card}A = n$, albo $|A| = n$, albo $\overline{\overline{A}} = n$ oraz mówimy, że moc zbioru A jest równa n.

Uwaga 9.4. Zauważmy, że powyższa definicja wymaga znajomości zbioru liczb naturalnych. Formalna konstrukcja tego zbioru będzie przedstawiona na ostatnim wykładzie. Można jednak zdefiniować pojęcie zbioru skończonego bez używania liczb naturalnych. Otóż mówimy, że zbiór jest *skończony*, gdy nie jest równoliczny z żadnym swoim podzbiorem właściwym (ta definicja pochodzi od Richarda Dedekinda[1]). Jeśli wśród aksjomatów teorii mnogości mamy pewnik wyboru, to te definicje są równoważne. Więcej na temat różnych definicji zbiorów skończonych można przeczytać w [4].

Przykład 9.5. $\{1, 2, 3, 4\} \sim \{a, b, c, d\} \sim \{5, 7, -11, 3\}$, wszystkie te zbiory są skończone i mają cztery elementy, piszemy np. $\#\{5, 7, -11, 3\} = 4$.

Wykażemy teraz kilka, intuicyjnie dość oczywistych, faktów o zbiorach skończonych. W dowodach posłużymy się zasadą indukcji w wersji znanej ze szkoły. Więcej o zasadzie indukcji w wykładzie 15.

Stwierdzenie 9.6. *Niech A, B będą zbiorami skończonymi. Niech $A \subset B$ i niech $\#B = n$. Wtedy*

- $\#A \leqslant n$,
- $A \subsetneq B \Longrightarrow \#A < n$.

Dowód. Dowód prowadzimy indukcją ze względu na $n = \#B$.

1. Jeśli $n = 0$, to $\#B = 0$ czyli $B = \varnothing$, skąd, skoro $A \subset B$, to $A = \varnothing$, czyli $\#A = 0 = n$.

2. Niech $n > 0$ i załóżmy, że nasze twierdzenie zachodzi dla zbiorów B takich, że $\#B \leqslant n$. Weźmy teraz zbiór B taki, że $\#B = n + 1$.
Jeśli $A = B$, to wtedy $\#A = n + 1$.
Jeśli $A \neq B$ (ale z założenia $A \subset B$), to mamy $A \subsetneq B$, zatem istnieje $b \in B : b \notin A$. Stąd $A \subset B \setminus \{b\}$. Wystarczy teraz wykazać poniższy lemat.

[1] Richarda Dedekind (1831–1916), niemiecki matematyk.

Lemat 9.7.

$$\#(B \setminus \{b\}) = \#B - 1.$$

Faktycznie, jeśli wykażemy lemat, to skoro $A \subset B \setminus \{b\}$, to z założenia indukcyjnego mamy $\#A \leqslant n$ (i przy okazji $\#A < \#B$).

Dowód lematu 9.7. Mamy wykazać, że jeśli $f : B \hookrightarrow \{1, 2, \ldots, n+1\}$, to dla dowolnego $b \in B$ istnieje bijekcja $g : B \setminus \{b\} \hookrightarrow \{1, 2, \ldots, n\}$.
1. Niech b będzie takie, że $f(b) = n+1$. Wówczas g definiujemy jako $f|_{B\setminus\{b\}}$.

2. Niech dla $b \in \{1, 2, \ldots, n\}$ będzie $f(b) = a \in \{1, 2, \ldots, n\}$. Niech $f^{-1}(n+1) = c$ (zauważmy, że $c \neq b$). Definiujemy g następująco:

$$g(x) = \begin{cases} f(x), & x \neq c \\ a, & x = c. \end{cases}$$

Łatwo sprawdzić, że tak zdefiniowana funkcja g jest bijekcją. □

Stwierdzenie 9.8. *Niech A i B będą zbiorami i niech $\#A = n$ i $\#B = m$. Wówczas*

$$A \sim B \iff m = n.$$

Dowód. ($\Longleftarrow$). Jeśli $m = n$ to istnieją bijekcje f i g takie, że

$$F : A \hookrightarrow \{1, 2, \ldots, n\} \text{ i } g : B \hookrightarrow \{1, 2, \ldots, n\},$$

a zatem $g^{-1} \circ f$ jest bijekcją A na B, zatem $A \sim B$.
($\Longrightarrow$). Mamy następujące bijekcje: $f : A \hookrightarrow \{1, 2, \ldots, n\}, g : A \hookrightarrow B, h : B \hookrightarrow \{1, 2, \ldots, m\}$, a zatem mamy bijekcję

$$h \circ g \circ f^{-1} : \{1, 2, \ldots, n\} \hookrightarrow \{1, 2, \ldots, m\},$$

zatem $\{1, 2, \ldots, n\} \subset \{1, 2, \ldots, m\}$ i $\{1, 2, \ldots, m\} \subset \{1, 2, \ldots, n\}$. Stąd, na podstawie stwierdzenia 9.6 mamy $n \leqslant m$ i $m \leqslant n$, czyli $m = n$. □

Jako wniosek z poprzednich stwierdzeń dostajemy:

Stwierdzenie 9.9. *Jeśli zbiór A zawiera się w zbiorze B i zbiór B jest skończony, to zbiór A też jest skończony.*

Dowód. Faktycznie, skoro $A \subset B$ i $B \hookrightarrow \{1, \ldots, n\}$ to $\#A = k \leqslant n$. □

Kolejnym wnioskiem jest następująca uwaga.

Uwaga 9.10. Zbiór liczb naturalnych nie jest zbiorem skończonym.

Dowód. Gdyby zbiór liczb naturalnych był zbiorem skończonym, to dla pewnego $n \in \mathbb{N}$ mielibyśmy

$$\mathbb{N} \sim \{1, \ldots, n\}.$$

Zarazem jednak

$$\{1, \ldots, n, n+1\} \subset \mathbb{N},$$

a zatem, ze stwierdzenia 9.6 mielibyśmy $n + 1 \leqslant n$, sprzeczność. □

Zbiór nazwiemy przeliczalnym, jeśli jest równoliczny ze zbiorem liczb naturalnych.

Definicja 9.11. Zbiór A nazywamy zbiorem *przeliczalnym*, jeśli

$$A \sim \mathbb{N}.$$

Uwaga 9.12. O zbiorach przeliczalnych mówimy, że mają moc $\aleph_0$ (czytamy *alef-zero*).

Uwaga 9.13. W niektórych podręcznikach zbiorami przeliczalnymi nazywa się zbiory, które są równoliczne ze zbiorem skończonym lub równoliczne z $\mathbb{N}$, warto się upewnić jaką definicję stosuje autor. W tych wykładach przyjmujemy, że zbiór przeliczalny jest zbiorem nieskończonym, równolicznym z $\mathbb{N}$. Zbiór, który jest skończony lub przeliczalny nazywamy *zbiorem co najwyżej przeliczalnym*.

Przykład 9.14. • Zbiór liczb parzystych $2\mathbb{N}$ jest przeliczalny. Faktycznie, $f : \mathbb{N} \to 2\mathbb{N}$, dana wzorem $f(k) = 2k$ jest bijekcją pomiędzy zbiorem liczb naturalnych a zbiorem liczb parzystych.

• Zbiór liczb całkowitych $\mathbb{Z}$ jest zbiorem przeliczalnym. Nietrudno sprawdzić, że funkcja dana wzorem $f(k) = (-1)^k\lceil\frac{k}{2}\rceil$ jest bijekcją $\mathbb{N}$ na $\mathbb{Z}$.

Przy dowodzeniu przeliczalności zbiorów będziemy posługiwać się często następującym faktem.

Uwaga 9.15. Można powiedzieć, że zbiór nieskończony A jest przeliczalny wtedy i tylko wtedy, gdy jego wyrazy można ustawić w ciąg. Faktycznie, jeśli zbiór A jest przeliczalny, to istnieje bijekcja $f : \mathbb{N} \twoheadrightarrow A$. Ustawiamy wtedy wyrazy zbioru A w ciąg następująco:

$$a_1 = f(1), a_2 = f(2), \dots$$

I na odwrót, jeśli wyrazy zbioru A są ustawione w ciąg (nieskończony i różnowartościowy) $a_1, a_2, a_3, \dots$, to bijekcję $f : \mathbb{N} \twoheadrightarrow A$ definiujemy przez $f(k) = a_k,\ k \in \mathbb{N}$.

Poniższe stwierdzenie charakteryzuje podzbiory zbioru przeliczalnego.

Stwierdzenie 9.16. *Podzbiór zbioru przeliczalnego jest skończony lub przeliczalny.*

Dowód. Niech A będzie zbiorem przeliczalnym a B jego podzbiorem. Jeśli B jest zbiorem skończonym, lub jeśli $B = A$, to B spełnia tezę stwierdzenia. Przypuśćmy zatem, że $B \neq A$ i B jest zbiorem nieskończonym. Niech f będzie bijekcją $f : \mathbb{N} \twoheadrightarrow A$, która istnieje, bo A jest przeliczalny. Definiujemy bijekcję $g : \mathbb{N} \twoheadrightarrow B$ następująco. Niech k_1 będzie najmniejszą z liczb k takich, że $f(k) \in B$. Bierzemy $g(1) := f(k_1)$. (Formalnie stosujemy tu tzw. *zasadę minimum*, zob. wykład 15). Następnie niech k_2 będzie najmniejszą z liczb k, różnych od k_1 takich, że $f(k) \in B$. Bierzemy $g(2) := f(k_2)$, ogólnie definiujemy

$$g(n) = f(k_n),$$

gdzie

$$k_n = \min\{k : k \notin \{k_1, \dots, k_{n-1}\} \wedge f(k) \in B\}.$$

Łatwo zobaczyć, że g jest bijekcją z $\mathbb{N}$ na B. Faktycznie, g jest injekcją bo f jest injekcją. Niech $b \in B$. Wtedy $b = f(k)$ dla pewnego k. Niech $n := \#\{\ell : \ell < k \wedge f(\ell) \in B\} + 1$. Wówczas $k = k_n$ i $b = g(n)$. □

Twierdzenie 9.17. *Niech A, B, będą zbiorami przeliczalnymi. Wówczas $A \cup B$ też jest zbiorem przeliczalnym.*

Dowód. Skoro zbiór A jest przeliczalny, to istnieje bijekcja

$$h : \mathbb{N} \twoheadrightarrow A.$$

Weźmy $B' = B \setminus A$. Jeśli B' jest pusty, twierdzenie jest oczywiście prawdziwe. Jeśli B' jest niepusty ale skończony, czyli $f : \{1, \dots, k\} \twoheadrightarrow B'$ dla pewnego $k \in \mathbb{N}$, to definiujemy bijekcję z $A \cup B = A \cup B'$ w $\mathbb{N}$ wzorem

$$g(m) = \begin{cases} f(m), & m \leqslant k \\ h(m-k), & m \geqslant k+1. \end{cases}$$

Z takiego określenia g od razu wynika, że g jest bijekcją.

Przypuśćmy teraz, że zbiór B' jest nieskończony. Zatem jest nieskończonym podzbiorem zbioru przeliczalnego, czyli, na podstawie stwierdzenia 9.16 jest zbiorem przeliczalnym. Istnieje zatem bijekcja

$$f : \mathbb{N} \twoheadrightarrow B'.$$

Definiujemy bijekcję $\mathbb{N} \twoheadrightarrow A \cup B' = A \cup B$ następująco:

$$g(m) = \begin{cases} h(k), & \text{dla } m = 2k-1 \\ f(k), & \text{dla } m = 2k, \end{cases}$$

gdzie $k = 1, 2, \dots$ □

Uwaga 9.18. Powyższy dowód możemy bardziej obrazowo zapisać tak. Zbiór $A \cup B$ ustawiamy w ciąg

$$b_1, \dots, b_k, a_1, a_2, \dots,$$

gdy zbiór B' jest skończony i ma k elementów, oraz w ciąg

$$a_1, b_1, a_2, b_2, \dots$$

$a_i \in A, b_i \in B'$, gdy zbiór B' jest nieskończony.

Jako prosty wniosek (ćwiczenie) z powyższego mamy następujące stwierdzenie.

Stwierdzenie 9.19. *Skończona suma zbiorów przeliczalnych jest zbiorem przeliczalnym.*

Kolejne stwierdzenie mówi o przeliczalności iloczynu kartezjańskiego zbiorów przeliczalnych.

Stwierdzenie 9.20. *Niech A, B będą zbiorami przeliczalnymi. Wtedy zbiór $A \times B$ jest zbiorem przeliczalnym.*

Dowód. Wykażemy najpierw, że zbiór $\mathbb{N} \times \mathbb{N}$ jest zbiorem przeliczalnym. Faktycznie, jeśli $(k, m) \in \mathbb{N} \times \mathbb{N}$, to funkcja $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ zdefiniowana wzorem

$$f(k, m) = \frac{(k + m + 1)(k + m)}{2} + m$$

jest bijekcją (proszę to sprawdzić jako proste ćwiczenie).

Jeśli teraz weźmiemy bijekcje $g_1 : A \hookrightarrow \mathbb{N}$ i $g_2 : B \hookrightarrow \mathbb{N}$, to zestawienie $f \circ (g_1, g_2)$ jest bijekcją $A \times B$ na $\mathbb{N} \times \mathbb{N}$. □

Kolejny lemat dotyczy sumowania zbiorów skończonych.

Lemat 9.21. *Suma przeliczalnej rodziny zbiorów skończonych jest zbiorem przeliczalnym lub skończonym.*

Dowód. 1. Zauważmy, że sumę $\bigcup_{n\in\mathbb{N}} A_n$ możemy zamienić na sumę zbiorów rozłącznych. Niech $A'_1 = A_1$, niech $A'_2 = A_2 \setminus A'_1, A'_3 = A_3 \setminus (A'_1 \cup A'_2) \dots$ itd. Zbiory A'_i są parami rozłączne i możemy założyć bez zmniejszenia ogólności, że są one są niepuste (puste pomijamy). Niepustych zbiorów A'_i może być skończenie lub przeliczalnie wiele.

2. Zakładamy zatem, że mamy zbiory A_i, rozłączne i niepuste, gdzie albo i należy do zbioru skończonego $\{1, 2, \dots, n\}$, albo $i \in \mathbb{N}$. Skoro zbiory A_i są skończone, to każdy z tych zbiorów jest równoliczny ze zbiorem $\{1, 2, \dots, k_i\}$, czyli $A_i = \{a_{i1}, \dots, a_{ik_i}\}$. Wtedy, jeśli $i \in \{1, 2, \dots, n\}$, to elementy sumy $\bigcup_i A_i$ są następujące

$$a_{11}, a_{12}, \dots, a_{1k_1}, a_{21}, \dots, a_{2k_2}, \dots a_{n1}, \dots, a_{nk_n}$$

i suma ta jest zbiorem skończonym. Jeśli $i \in \mathbb{N}$, to elementy sumy $\bigcup_{i\in\mathbb{N}} A_i$ ustawiamy w ciąg (nieskończony)

$$a_{11}, a_{12}, \dots, a_{1k_1}, a_{21}, \dots, a_{2k_2}, a_{31}, \dots, a_{3k_3}, \dots$$

co kończy dowód. □

Podobnie jak przeliczalności iloczynu kartezjańskiego zbiorów przeliczalnych dowodzimy przeliczalności przeliczalnej sumy zbiorów przeliczalnych.

Twierdzenie 9.22. *Niech $A_1, A_2, \dots$ będą zbiorami przeliczalnymi. Wówczas suma $\bigcup_{n\in N} A_n$ jest zbiorem przeliczalnym.*

Dowód. Postępując jak w dowodzie powyżej, możemy zmienić $\bigcup_{n\in N} A_n$ na sumę zbiorów rozłącznych A'_n. Każdy ze zbiorów A'_n jest podzbiorem zbioru A_n, zatem jest zbiorem skończonym lub przeliczalnym. Oznaczmy przeliczalne A'_i przez B_i a skończone przez C_i. Jeśli zbiorów B_i jest skończenie wiele, to korzystając ze stwierdzenia 9.19 mamy przeliczalność $\bigcup_i B_i$ a z lematu 9.21 wnioskujemy, że zbiór $\bigcup_j C_j$ jest skończony lub przeliczalny. Zatem $\bigcup_n A_n = \bigcup_i B_i \cup \bigcup_j C_j$ jest (ze stwierdzenia 9.19) zbiorem przeliczalnym.

Jeśli zbiorów B_i jest nieskończenie wiele, to znaczy, że możemy ustawić je w ciąg $B_1, B_2, \dots$. Elementy sumy tych zbiorów (rozłącznych) możemy zatem ustawić w taki ciąg:

$$b_{11}, b_{12}, b_{21}, b_{13}, b_{22}, b_{31}, b_{14}, b_{23}, b_{32}, b_{41} \dots,$$

gdzie $B_i = \{b_{i1}, \dots, b_{ij}, \dots\}$, a zatem suma ta jest zbiorem przeliczalnym.

Dodając do sumy $\bigcup_i B_i =: B$, która jest zbiorem przeliczalnym, sumę $\bigcup_j C_j =: C$, która jest zbiorem skończonym lub przeliczalnym, dostajemy, na podstawie poprzednich wyników, że $\bigcup_{n\in N} A_n = B \cup C$ jest zbiorem przeliczalnym. □

Uwaga 9.23. Powyższy dowód możemy zobrazować następująco. Przypuśćmy, że zbiory A_i są przeliczalne i rozłączne. Ustawmy elementy A_1 w ciąg $a_{11}, a_{12}, a_{13} \ldots$, elementy A_2 w ciąg $a_{21}, a_{22}, a_{23} \ldots$ itd., następnie elementy sumy zbiorów A_i ustawmy w taką tablicę jak poniżej.

$$\begin{array}{cccccc} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & \ldots \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & \ldots \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & \ldots \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & \ldots \\ \ldots & & & & & \end{array}$$

Wówczas elementy sumy możemy ustawić w ciąg idąc poniższą ścieżką

$$\begin{array}{cccccc} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & \ldots \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & \ldots \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & \ldots \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \end{array}$$

Zauważmy, że analogiczną „rysunkową" metodę możemy zastosować dla dowodu, że $\mathbb{N} \times \mathbb{N}$ jest zbiorem przeliczalnym.

Użyjemy teraz powyższych rezultatów, by wykazać przeliczalność pewnych zbiorów. Zacznijmy od $\mathbb{Q}$.

Stwierdzenie 9.24. *Zbiór liczb wymiernych jest zbiorem przeliczalnym.*

Dowód. Wiemy już, że $\mathbb{Z}$ i $\mathbb{Z} \times \mathbb{N}^*$ są zbiorami przeliczalnymi. (Stwierdzenie 9.20 i przykład 9.14.) Przypomnijmy, że zbiór liczb wymiernych możemy utożsamiać ze zbiorem ilorazów $\frac{p}{q}$, gdzie $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ oraz p i q są względnie pierwsze. $\mathbb{Q}$ możemy zatem bijektywnie utożsamiać ze zbiorem par $A = \{(p, q) \in \mathbb{Z} \times \mathbb{N}^* \mid \mathrm{NWD}(p, q) = 1\} \subset \mathbb{Z} \times \mathbb{N}^*$. Zbiór A jest oczywiście nieskończony (zawiera liczby całkowite, czyli pary $(p, 1)$, oraz jest podzbiorem zbioru przeliczalnego. Zatem $\mathbb{Q}$ jest zbiorem przeliczalnym. □

Przypomnijmy teraz oznaczenie: $\mathbb{Z}[x]$ to wielomiany jednej zmiennej x o współczynnikach ze zbioru $\mathbb{Z}$, czyli funkcje $f : \mathbb{R} \to \mathbb{R}$ postaci $a_0 + a_1 x + \ldots a_n x^n$, gdzie $a_i \in \mathbb{Z}$ a jeśli $a_n \neq 0$, to n nazywamy stopniem wielomianu f. (Stopień wielomianu zerowego przyjmuje się jako równy $-\infty$.) Przez $Z_n[x]$ będziemy oznaczać zbiór wielomianów stopnia co najwyżej n.

Analogicznie definiujemy $\mathbb{Q}[x]$, jako wielomiany jednej zmiennej x o współczynnikach ze zbioru $\mathbb{Q}$.

Stwierdzenie 9.25. *Zbiór $\mathbb{Z}[x]$ jest zbiorem przeliczalnym.*

Dowód. Wielomiany o współczynnikach całkowitych możemy zapisać jako sumę:

$$\mathbb{Z}[x] = \bigcup_{n=0}^{\infty} Z_n[x].$$

Każdy ze zbiorów $Z_n[x]$ możemy utożsamić ze zbiorem $\mathbb{Z} \times \mathbb{Z} \cdots \times \mathbb{Z} = \mathbb{Z}^{n+1}$, przyporządkowując wielomianowi ciąg współczynników $a_0 + a_1 x + \ldots a_n x^n \to (a_0, a_1 \ldots, a_n)$. Każdy ze zbiorów $Z_n[x]$ jest zatem przeliczalny, a więc $\mathbb{Z}[x]$ jest zbiorem przeliczalnym jako suma przeliczalnej ilości zbiorów przeliczalnych. □

Uwaga 9.26. Analogicznie dowodzimy, że $\mathbb{Q}[x]$ jest zbiorem przeliczalnym.

Definicja 9.27. Liczbę rzeczywistą $a \in \mathbb{R}$ nazywamy *algebraiczną*, jeśli istnieje wielomian $w \in \mathbb{Z}[x] \setminus \{0\}$ taki, że $w(a) = 0$.

Uwaga 9.28. Nie wszystkie liczby rzeczywiste są algebraiczne. Liczby, które nie są algebraiczne, nazywamy *nie-algebraicznymi* lub *przestępnymi*. Liczbą przestępną jest na przykład π, dowód tego faktu jest nietrywialny, zob. np. [2].

Okazuje się, że liczb algebraicznych jest przeliczalnie wiele.

Stwierdzenie 9.29. *Zbiór liczb algebraicznych jest zbiorem przeliczalnym.*

Dowód. Niech A oznacza zbiór liczb algebraicznych. A możemy zapisać jako sumę

$$A = \bigcup_{w \in \mathbb{Z}[x]^*} A_w,$$

gdzie A_w to zbiór pierwiastków danego wielomianu w. Skoro wielomian w jest niezerowy, to ma stopień równy n, zatem zbiór A_w ma co najwyżej n elementów. Zbiór $\mathbb{Z}[x]^*$ (czyli zbiór wielomianów o współczynnikach całkowitych bez wielomianu zerowego) jest zbiorem przeliczalnym, zatem A jest przeliczalną sumą zbiorów skończonych, czyli z lematu 9.21, jest zbiorem przeliczalnym. □

Rozdział 10

Zbiory nieprzeliczalne. Twierdzenie Cantora. Hipoteza continuum

Na tym wykładzie omówimy pojęcie nieprzeliczalności, pokażemy nieprzeliczalność funkcji z $\mathbb{N}$ w $\{0,1\}$ i nieprzeliczalność $\mathbb{R}$. Wykażemy twierdzenie Cantora[1] *o mocy zbioru podzbiorów, wspomnimy o hipotezie continuum i na końcu krótko powiemy o podobieństwie porządkowym.*

Zacznijmy od definicji:

Definicja 10.1. Zbiór X nazywamy *zbiorem nieprzeliczalnym* jeśli nie jest ani skończony ani przeliczalny.

Poniższe twierdzenie pokazuje pierwszy przykład zbioru nieprzeliczalnego, dając zarazem odpowiedź na pytanie czy takie zbiory w ogóle istnieją.

Twierdzenie 10.2. *Zbiór C ciągów o wyrazach ze zbioru $\{0,1\}$ jest zbiorem nieprzeliczalnym.*

Dowód. Przypuśćmy, dla dowodu nie wprost, że zbiór C jest przeliczalny. Możemy zatem wszystkie jego wyrazy ustawić w ciąg (tworząc ciąg ciągów): $(c_1), (c_2), (c_3), \ldots$. Rozważmy teraz ciąg (d) ze zbioru C utworzony w ten sposób, że

$$d_j = \begin{cases} 0 \text{ jeśli ciąg } (c_j) \text{ ma na pozycji } j \text{ jedynkę} \\ 1 \text{ jeśli ciąg } (c_j) \text{ ma na pozycji } j \text{ zero} \end{cases}$$

Przykładowo, jeśli nasz ciąg $(c_1), (c_2), (c_3), \ldots$ jest następujący

$$\begin{array}{lcccccc} (c_1) = & \underline{1} & 0 & 1 & 1 & 0 & \ldots \\ (c_3) = & 1 & \underline{1} & 1 & 0 & 0 & \ldots \\ (c_3) = & 0 & 0 & \underline{0} & 1 & 0 & \ldots \\ \ldots & & & & & & \end{array}$$

to

$$(d) = 0\ 0\ 1\ \ldots$$

Zauważmy teraz, że ciąg (d) nie może być na żadnej pozycji w naszym ciągu ciągów $(c_1), (c_2), (c_3), \ldots$, bo skonstruowany ciąg różni się od każdego ciągu (c_k) na k-tej pozycji.

□

Fakt, że zbiór ciągów zero-jedynkowych jest zbiorem nieprzeliczalnym pozwala nam wykazać kolejne twierdzenie.

Twierdzenie 10.3. *Zbiór $\mathbb{R}$ liczb rzeczywistych jest zbiorem nieprzeliczalnym.*

Dowód. Skonstruujemy injekcję ι z C w $\mathbb{R}$. Ciągowi $(c) = (a_1, a_2, a_3, \ldots)$, gdzie $a_i \in \{0,1\}$ przyporządkujemy liczbę rzeczywistą $0, a_1a_2a_3\ldots$ (w zapisie dziesiętnym). Jeśli $0, a_1a_2a_3\cdots = 0, b_1b_2b_3\ldots$, to znaczy, że

$$\sum_{i=1}^{\infty} a_i 10^{-i} = \sum_{i=1}^{\infty} b_i 10^{-i}.$$

[1] Georg Cantor (1845–1918), niemiecki matematyk.

Jeśli $a_i = b_i$ dla każdego i, to nasze przyporządkowanie jest injekcją. Przypuśćmy, że tak nie jest. Niech zatem k będzie najmniejszym wskaźnikiem i, dla którego $a_i \neq b_i$ Niech na przykład $a_k = 1$ i $b_k = 0$. Wtedy $\sum_{i=k}^{\infty} a_i 10^{-i} \geqslant \frac{1}{10^k}$ oraz $\sum_{i=k}^{\infty} b_i 10^{-i} = \sum_{i=k+1}^{\infty} b_i 10^{-i} < \frac{1}{10^k}$, a zatem $\sum_{i=1}^{\infty} a_i 10^{-i} - \sum_{i=1}^{\infty} b_i 10^{-i} > 0$, sprzeczność.

Mamy zatem injekcję $\iota : C \hookrightarrow \mathbb{R}$, czyli zbiór C jest równoliczny z podzbiorem $\iota(C)$ zbioru $\mathbb{R}$ (obraz zbioru przez injekcję jest równoliczny z tym zbiorem.) Skoro tak, to zbiór $\mathbb{R}$ nie jest ani skończony (oczywiście), ani przeliczalny – bo zawiera zbiór nieprzeliczalny $\iota(C)$. □

W poprzednim twierdzeniu skonstruowaliśmy injekcję z C w $\mathbb{R}$. Kolejne twierdzenie pokaże jak skonstruować injekcję z podzbioru $(0,1) \subset \mathbb{R}$ w zbiór C, a stwierdzenie 10.6 pokaże równoliczność $(0,1)$ i $\mathbb{R}$. Dostaniemy zatem, po złożeniu odwzorowań, injekcję z $\mathbb{R}$ w C. W takim razie dostaniemy dwie injekcje: z $\mathbb{R}$ w C i z C w $\mathbb{R}$. Na następnym wykładzie poznamy twierdzenie, zwane twierdzeniem Cantora–Bernsteina, które pozwoli nam stwierdzić, że istnieje bijekcja pomiędzy C i $\mathbb{R}$.

Twierdzenie 10.4. *Istnieje injekcja z przedziału $(0,1)$ w zbiór C.*

Dowód. Każdy punkt z przedziału $(0,1)$ zapiszmy w systemie dwójkowym, np

$$0{,}3_{10} = 0{,}01001100110\ldots_2 .$$

Ten zapis może być niejednoznaczny, w tym sensie, że np. $0{,}011111\ldots_2 = 0{,}1_2 = 0{,}5_{10}$. Przyjmujemy zatem umowę, że jeśli w zapisie od pewnego miejsca o numerze $k+1$ jest nieskończenie wiele jedynek (a na miejscu k zero), to zapisujemy je jako jedynkę na miejscu k. Zauważmy, że liczba $0{,}1111111111\ldots_2$ jest równa 1_{10}, a zatem nie należy do przedziału $(0,1)$. Mając teraz jednoznaczność zapisu, definiujemy nasze odwzorowanie następująco. Liczbie c z przedziału $(0,1)$, zapisanej w systemie dwójkowym jako $0{,}c_1c_2c_3\ldots$, przyporządkowujemy ciąg

$$c = c_1c_2c_3\cdots \in C.$$

To przyporządkowanie jest oczywiście injektywne, co kończy dowód. □

Wiemy już, że zbiór $\mathbb{R}$ jest nieprzeliczalny. Zbiór, który jest równoliczny ze zbiorem liczb rzeczywistych (czyli istnieje bijekcja z tego zbiory w $\mathbb{R}$), nazwiemy *zbiorem mocy continuum.*

Definicja 10.5. Mówimy, że zbiór A ma *moc continuum*, jeśli $A \sim \mathbb{R}$. Moc zbioru $\mathbb{R}$ oznaczamy przez $\mathfrak{c}$.

Wykażemy teraz zapowiedziane wyżej stwierdzenie:

Stwierdzenie 10.6.

$$(0,1) \sim \mathbb{R}.$$

Dowód. Dowód tego faktu jest elementarny. Konstruujemy najpierw bijekcję z przedziału $(0,1)$ w przedział $(-\frac{\pi}{2}, \frac{\pi}{2})$, na przykład jako

$$f_1(x) = \pi x - \frac{\pi}{2}.$$

Następnie bierzemy

$$f_2(x) = \operatorname{tg}(x),$$

f_2 jest bijekcją z $(-\frac{\pi}{2}, \frac{\pi}{2})$ w $\mathbb{R}$. Składając te funkcje, dostajemy bijekcję $f = f_2 \circ f_1$ z $(0,1)$ w $\mathbb{R}$. □

Uwaga 10.7. Dociekliwy czytelnik może zapytać o bijektywność funkcji $\operatorname{tg} : (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$. Sprawdzenie injektywności jest prostym ćwiczeniem z trygonometrii, sprawdzenie surjektywności zostawiamy czytelnikowi jako ćwiczenie z analizy (należy wykazać ciągłość funkcji tangens, policzyć granice na końcach przedziału $(-\frac{\pi}{2}, \frac{\pi}{2})$ i skorzystać z własności Darboux).

Uwaga 10.8. Na poprzednim wykładzie wykazaliśmy, że zbiór liczb algebraicznych jest przeliczalny. Skoro $\mathbb{R}$ jest zbiorem nieprzeliczalnym, to zbiór liczb przestępnych jest także nieprzeliczalny (inaczej $\mathbb{R}$ jako suma dwóch zbiorów przeliczalnych byłby przeliczalny).

Zauważyliśmy już wcześniej, że relacja równoliczności zbiorów jest zwrotna, symetryczna i przechodnia. Ma zatem sens następująca definicja:

Definicja 10.9. Każdemu zbiorowi X przyporządkowujemy pewien obiekt, zwany *mocą zbioru* (albo: *liczbą kardynalną*, oznaczany $\#X$, w ten sposób, że dla zbiorów X, Y mamy

$$\#X = \#Y \iff X \sim Y.$$

Mamy następujące własności i oznaczenia.

1 $\#\varnothing = 0$.

2 $\#X = n \iff X \sim \{1, 2, \dots n\}$.

3 $\#\mathbb{N} = \aleph_0$

4 $\#\mathbb{R} = \mathfrak{c}$.

Definicja 10.10. Niech teraz $\#A = \mathfrak{a}$, $\#B = \mathfrak{b}$. Mówimy, że $\mathfrak{a} \leqslant \mathfrak{b}$, jeśli istnieje zbiór $C \subset B$ taki, że $A \sim C$ (czyli A jest równoliczny z podzbiorem B).

Jeśli $\mathfrak{a} \leqslant \mathfrak{b}$, ale $\mathfrak{a} \neq \mathfrak{b}$ (czyli zbiory A i B nie są równoliczne), to piszemy $\mathfrak{a} < \mathfrak{b}$.

Zauważmy, że dla zbioru skończonego X, zbiór podzbiorów tego zbioru $\mathcal{P}(X)$ ma zawsze więcej elementów niż zbiór X,

$$\mathcal{P}(\varnothing) = \{\varnothing\},$$
$$\mathcal{P}(\{a\}) = \{\varnothing, \{a\}\},$$
$$\mathcal{P}(\{a, b\}) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}.$$

(Łatwo zauważyć, że jeśli zbiór X ma n elementów, to zbiór $\mathcal{P}(X)$ ma 2^n elementów, co wyjaśnia występujące czasem oznaczenie zbioru podzbiorów X jako 2^X).

Okazuje się, że dla wszystkich zbiorów moc zbioru jest silnie mniejsza niż moc zbioru jego podzbiorów. Twierdzenie to zostało odkryte i udowodnione przez Georga Cantora (1845–1918).

Twierdzenie 10.11 (Twierdzenie Cantora)**.** *Niech X będzie dowolnym zbiorem. Wówczas*

$$\#X < \#\mathcal{P}(X).$$

Dowód. Dla zbioru pustego twierdzenie jest prawdziwe, jak zauważyliśmy powyżej.

Weźmy zatem niepusty zbiór X. Zauważmy, że

$$\#X \leqslant \#\mathcal{P}(X).$$

Faktycznie, funkcja $g : X \ni x \to \{x\} \in \mathcal{P}(X)$ jest bijekcją z X na istotny, różny od całego $\mathcal{P}(X)$, podzbiór $\mathcal{P}(X)$,

$$g : X \hookrightarrow \{\{x\} | x \in X\}.$$

Pozostaje wykazać, że $\#X \neq \#\mathcal{P}(X)$.

Przypuśćmy zatem, że dla jakiegoś zbioru niepustego X mamy $X \sim \mathcal{P}(X)$, czyli istnieje bijekcja

$$f : X \hookrightarrow \mathcal{P}(X).$$

Dla $x \in X$: $f(x)$ jest pewnym podzbiorem $\mathcal{P}(X)$. Zdefiniujmy pewien podzbiór Z zbioru X.

$$Z = \{x \in X \mid x \notin f(x)\},$$

czyli Z jest podzbiorem złożonym z tych elementów zbioru x, które nie należą do podzbioru danego przez $f(x)$.

Skoro f jest bijekcją, to istnieje $z \in X$ takie, że

$$Z = f(z).$$

Są dwie możliwości, albo $z \in Z$ albo $z \notin Z$. Jeśli $z \in Z$, to $z \notin f(z) = Z$, z definicji Z, co jest niemożliwe. Zatem, $z \notin Z$, ale wtedy, znowu z definicji Z, mamy $z \in f(z) = Z$, znowu sprzeczność. Zatem, niemożliwe jest by była bijekcja między X a $\mathcal{P}(X)$. Zatem

$$\#X < \#\mathcal{P}(X).$$

□

Z tego twierdzenia wynikają od razu dwa wnioski.

Wniosek 10.12. *Można konstruować zbiory coraz większych (nieskończonych) mocy.*

Faktycznie, na przykład:

$$\#\mathbb{N} < \#\mathcal{P}(\mathbb{N}) < \#\mathcal{P}(\mathcal{P}(\mathbb{N})) < \dots$$

Mamy zatem nieskończenie wiele różnych liczb kardynalnych, większych od danej liczby kardynalnej.

Drugi z wniosków mówi, że nie istnieje zbiór wszystkich zbiorów. Odkrycie tego faktu było sporym zaskoczeniem dla matematyków zajmujących się teorią mnogości w drugiej połowie XIX wieku, zwłaszcza dla Georga Cantora.

Wniosek 10.13. *Nie istnieje zbiór wszystkich zbiorów.*

Dowód. Przypuśćmy, że istnieje zbiór wszystkich zbiorów, oznaczmy go przez Z. Wtedy, zbiór jego podzbiorów jest zawarty w Z. Jako podzbiór Z ma moc mniejszą lub równą mocy Z, czyli jest

$$\#\mathcal{P}(Z) \leqslant \#Z,$$

a twierdzenie 10.11 mówi, że jest to niemożliwe, bo zawsze

$$\#Z < \#\mathcal{P}(Z).$$

□

Zauważmy teraz, że zachodzi następujący fakt:

Stwierdzenie 10.14. *Zdefiniowany na początku tego wykładu zbiór C ciągów zero-jedynkowych jest równoliczny ze zbiorem $\mathcal{P}(\mathbb{N})$.*

Dowód. Faktycznie, odwzorowanie, które ciągowi $c \in C$ przyporządkowuje podzbiór $\mathbb{N}$ złożony z takich i tylko takich elementów $n \in \mathbb{N}$, że $c_n = 1$, jest w oczywisty sposób bijekcją. □

Uwaga 10.15. Wspomnieliśmy wyżej, że na przyszłym wykładzie wykażemy, że $\mathbb{R} \sim C$. Widzimy zatem, że $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$.

Przez dłuższy czas matematycy, przede wszystkim Georg Cantor, próbowali znaleźć odpowiedź na pytanie: czy jest jakiś zbiór H taki, że

$$\#\mathbb{N} < \#H < \#\mathbb{R} = \#\mathcal{P}(\mathbb{N}).$$

Cantor wysunął hipotezę (zwaną hipotezą continuum), która mówi, że takiego zbioru nie ma, nie potrafił jednak tego udowodnić. I nic dziwnego, w połowie XX wieku okazało się, że ta hipoteza jest niezależna od aksjomatów teorii mnogości, to znaczy można przyjąć zarówno istnienie, jak i nieistnienie zbioru H, nie dostając sprzeczności z aksjomatyką teorii mnogości. Zainteresowany czytelnik może poczytać np. w [11] o pracach Gödla[2] (1940), który wykazał niesprzeczność hipotezy continuum z aksjomatami teorii mnogości i Cohena[3] (1963), który wykazał niezależność hipotezy continuum od tych aksjomatów.

[2]Kurt Gödel (1906–1978), austriacki logik i matematyk.
[3]Paul Cohen (1934–2007), amerykański matematyk.

Rozdział 11

Twierdzenie Cantora–Bernsteina

Ten wykład poświęcimy dowodowi twierdzenia sformułowanego przez Cantora, którego dowód pochodzi od Feliksa Bernsteina[1] *i Ernsta Schrödera*[2] .

Zwyczajowo to twierdzenie zwane jest twierdzeniem Cantora–Bernsteina.

Twierdzenie 11.1. *Jeśli istnieje injekcja ze zbioru A w zbiór B i istnieje injekcja ze zbioru B w zbiór A, to istnieje bijekcja z A w B.*

Uwaga 11.2. Twierdzenie 11.1 można sformułować także następująco: dla dowolnych liczb kardynalnych $\mathfrak{m}$ i $\mathfrak{n}$, jeśli $\mathfrak{m} \leqslant \mathfrak{n}$ i $\mathfrak{n} \leqslant \mathfrak{m}$, to $\mathfrak{m} = \mathfrak{n}$.

Dowód. Zauważmy, że wystarczy wykazać następujący lemat.

Lemat 11.3. *Dla dowolnych zbiorów X, Y, Z, jeśli $X \subset Y \subset Z$ i $\#X = \#Z$, to $\#Y = \#Z$.*

Faktycznie, załóżmy, że mamy wykazany powyższy lemat. Weźmy teraz injekcje $f : A \hookrightarrow B$ i $h : B \hookrightarrow A$. Zauważmy, że $h(B) \sim B$ i $f(A) \sim A$ oraz $f(A) \sim h(f(A))$, bo f i h są injekcjami. Niech

$$Z := A,$$
$$Y := h(B),$$
$$X := h(f(A)).$$

Wtedy, jak łatwo zauważyć,

$$X \subset Y \subset Z$$

(bo $h(f(A)) \subset h(B) \subset A$). Zauważmy też, że

$$Z = A \sim f(A) \sim h(f(A)) = X.$$

Wówczas, z lematu wynika, że

$$Y \sim Z$$

czyli

$$h(B) \sim A$$

a więc też

$$B \sim A$$

a zatem istnieje bijekcja z A w B.

Pozostaje więc wykazać lemat 11.3. Ponieważ $\#Z = \#X$, to istnieje bijekcja $f : Z \hookrightarrow\!\!\!\!\rightarrow X$. Zdefiniujmy rekurencyjnie ciąg zbiorów:

$$W_0 = Y \setminus X,\ W_{n+1} = f(W_n).$$

Zauważmy, że dla dowolnego $n \in \mathbb{N}$ mamy $W_n \subset Y$, dla W_0 jest to oczywiste. Dla W_n, $n > 0$ wynika to z faktu, że f prowadzi do $X \subset Y$. Zdefiniujmy zbiór $W \subset Y$ jako

$$W := \bigcup_{n=0}^{\infty} W_n.$$

[1] Felix Bernstein (1878–1956), niemiecki matematyk.
[2] Ernst Schröder (1841–1902), niemiecki matematyk.

Zdefiniujmy odwzorowanie $g : Z \to Y$ wzorem

$$g(x) = \begin{cases} f(x), & x \in Z \setminus W \\ x, & x \in W. \end{cases}$$

Sprawdzimy teraz, że:

1. g jest injekcją. Weźmy $x_1, x_2 \in Z, x_1 \neq x_2$. Mamy następujące możliwości:
   - $x_1, x_2 \in W$. Wtedy $g(x_1) = x_1 \neq x_2 = g(x_2)$.
   - $x_1, x_2 \notin W$. Wtedy $g(x_1) = f(x_1)$ i $g(x_2) = f(x_2)$, ale f jest injekcją, zatem dla $x_1 \neq x_2$ mamy $f(x_1) \neq f(x_2)$ czyli też $g(x_1) \neq g(x_2)$.
   - $x_1 \in W$, $x_2 \notin W$. Przypuśćmy, że w tym przypadku $g(x_1) = g(x_2)$, czyli, z definicji g, $x_1 = f(x_2)$. Skoro $x_1 \in W$ to $f(x_2) \in W$, zatem istnieje $n \in \mathbb{N}$ takie, że $f(x_2) \in W_n$. Jeśli $f(x_2) \in W_0$, to $f(x_2) \in Y \setminus X$, czyli $f(x_2) \notin X$, co daje sprzeczność, bo funkcja f prowadzi w X. Musi zatem być $f(x_2) \in W_n$ dla pewnego $n \geqslant 1$. Skoro $f(x_2) \in W_n$, to $f(x_2) \in f(W_{n-1})$, z definicji obrazu wynika zatem, że istnieje $w \in W_{n-1}$ takie, że $f(x_2) = f(w)$, a skoro f jest injekcją, to $x_2 = w \in W_{n-1}$, ale to oznacza, że $x_2 \in W$, co jest jest sprzeczne z naszym założeniem, że $x_1 \in W$, $x_2 \notin W$.
   - Przypadek $x_1 \notin W$, $x_2 \in W$ dowodzimy analogicznie jak powyżej.
2. g jest surjekcją. Chcemy sprawdzić, że $g(Z) = Y$. W serii równości poniżej będziemy korzystać:
   (a) z własności obrazu i przeciwobrazu wypisanych w stwierdzeniu 6.16 i Uwadze 6.17
   (b) z definicji W
   (c) z definicji g
   (d) z bijektywności f

   Zapiszmy
   $g(Z) = g(Z \setminus W \cup W) \overset{(a)}{=} g(Z \setminus W) \cup g(W) \overset{(c)}{=} f(Z \setminus W) \cup W \overset{(b)}{=} f(Z \setminus W) \cup W_0 \cup \bigcup_{n=0}^{\infty} W_{n+1} \overset{(b)}{=} f(Z \setminus W) \cup W_0 \cup \bigcup_{n=0}^{\infty} f(W_n) \overset{(b)}{=} f(Z \setminus W) \cup (Y \setminus X) \cup f(\bigcup_{n=0}^{\infty} W_n) = f(Z \setminus W) \cup (Y \setminus X) \cup f(W) = f(Z \setminus W) \cup f(W) \cup (Y \setminus X) \overset{(a)}{=} f(Z) \cup (Y \setminus X) \overset{(d)}{=} X \cup Y \setminus X = Y.$ □

Wniosek 11.4. *Na poprzednim wykładzie wykazaliśmy, że istnieje injekcja ze zbioru C ciągów zero-jedynkowych w $\mathbb{R}$ (twierdzenie 10.3) oraz injekcja z $\mathbb{R}$ w C (twierdzenie 10.4). Z twierdzenia Cantora–Bernsteina wnioskujemy zatem, że $\mathbb{R} \sim C$.*

Ćwiczenie 11.5. 1. Wykazać, że odwzorowanie $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dane wzorem $(k, l) \to 2^k 3^l$ jest injekcją.
2. Korzystając z powyższego faktu i z twierdzenia Cantora–Bernsteina, wykazać, że $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

Rozdział 12

Lemat Kuratowskiego–Zorna

Na tym wykładzie powrócimy do relacji częściowego porządku. Sformułujemy lemat Kuratowskiego[1]*–Zorna*[2]*. Wykażemy, że ten lemat wynika z twierdzenia Zermelo (o dobrym uporządkowaniu).*

Na kolejnym wykładzie zobaczymy, że zachodzi wynikanie: z lematu Kuratowskiego–Zorna wynika pewnik wyboru, a jeszcze później naszkicujemy dowód twierdzenia Zermelo przy założeniu pewnika wyboru. Zauważmy zatem, że lemat Kuratowskiego–Zorna jest równoważny pewnikowi wyboru, można go zatem przyjąć jako jeden z aksjomatów teorii mnogości.

Zacznijmy od przypomnienia.

Niech zbiór $(X, \preccurlyeq)$ będzie zbiorem częściowo uporządkowanym (to znaczy relacja $\preccurlyeq$ jest zwrotna, przechodnia, słabo antysymetryczna, zobacz definicja 8.1). Przypomnijmy, że podzbiór $L \subset X$ nazywamy łańcuchem, jeśli $(L, \preccurlyeq|_L)$ jest zbiorem uporządkowanym liniowo (definicja 8.19). Przypomnijmy, że element $M \in X$ nazywamy majorantą zbioru $A \subset X$, jeśli dla każdego $x \in A$ zachodzi $x \leqslant M$ (definicja 8.11), a element $a \in X$ nazywamy elementem maksymalnym zbioru X, jeśli dla dowolnego $x \in X$ zachodzi wynikanie $a \leqslant x \implies a = x$ (definicja 8.5).

Dla zbioru X uporządkowanego liniowo odcinkiem początkowym tego zbioru wyznaczonym przez punkt $a \in X$ nazywamy

$$\mathcal{O}(a) = \{x \in X : x \leqslant a \wedge x \neq a\},$$

zobacz definicja 8.25.

Mówimy, że $(X, \leqslant)$ jest uporządkowany dobrze, gdy każdy niepusty podzbiór zbioru X ma element najmniejszy (w sensie porządku $\leqslant$), zobacz definicja 8.23.

Niech teraz $(X, \leqslant)$ będzie zbiorem dobrze uporządkowanym. Weźmy funkcję $f : \mathcal{P}(X) \setminus \{X\} \to X$ taką, że $f(A) \in X \setminus A$ (jej istnienie wynika z pewnika wyboru). Mówimy, że porządek $\leqslant$ jest zgodny z f, jeśli dla każdego $a \in X$ zachodzi $a = f(\mathcal{O}(a))$. Przypomnijmy teraz twierdzenie Zermelo (twierdzenie 8.28):

Twierdzenie 12.1 (Zermelo)**.** *Niech X będzie zbiorem niepustym. Niech $f : \mathcal{P}(X) \setminus \{X\} \to X$ będzie funkcją taką, że $f(A) \in X \setminus A$. Wówczas istnieje dokładnie jeden porządek na X, dobry i zgodny z f.*

Zakładając to twierdzenie wykażemy teraz lemat Kuratowskiego–Zorna. Następnie, na kolejnym wykładzie, zobaczymy – bardzo istotne – zastosowania tego lematu. Dzięki niemu będziemy mogli wykazać, że każda przestrzeń wektorowa ma bazę, że moce dwóch dowolnych zbiorów można ze sobą porównać lub, na wykładzie ze wstępu do algebry, że w każdym pierścieniu istnieje ideał maksymalny.

Twierdzenie 12.2 (Lemat Kuratowskiego–Zorna)**.** *Niech X będzie zbiorem niepustym a $\preccurlyeq$ częściowym porządkiem na X. Załóżmy, że*

- *każdy łańcuch w X ma majorantę w X.*

Wówczas istnieje w X element maksymalny.

Dowód. Wprowadźmy oznaczenia. Niech L będzie łańcuchem w X, niech dla tego łańcucha $M(L)$ oznacza zbiór majorant L w X. Z założenia • wynika, że $M(L)$ jest zbiorem niepustym. Weźmy funkcję $f : \mathcal{P}(X) \setminus \{X\} \to X$ taką, że dla dowolnego $A \subsetneq X$ mamy $f(A) \in X \setminus A$ oraz dodatkowo $f(L) \in M(L) \setminus \{L\}$, o ile L jest łańcuchem i $M(L) \setminus L \neq \varnothing$.

Dla dowodu lematu Kuratowskiego–Zorna wykażemy trzy pomocnicze lematy.

[1] Kazimierz Kuratowski (1896–1980), polski matematyk.

[2] Max Zorn (1906–1993), amerykański matematyk pochodzenia niemieckiego.

Lemat 12.3. *Niech $(X, \preccurlyeq)$ będzie zbiorem częściowo uporządkowanym, niech L będzie niepustym łańcuchem w X, który ma w X majorantę. Wówczas, jeśli $M(L) \subset L$, to L ma element największy i jest to zarazem element maksymalny w X.*

Dowód lematu 12.3. Niech x będzie majorantą łańcucha, czyli $x \in M(L)$. Skoro $M(L) \subset L$, to $x \in L$. Z definicji majoranty mamy zatem, że dla każdego $y \in L$ zachodzi $y \preccurlyeq x$. To dokładnie oznacza, że x jest elementem największym w L. Pozostaje zobaczyć, że x jest też elementem maksymalnym w X. Weźmy zatem $z \in X$ i załóżmy, że $x \preccurlyeq z$. Skoro dla każdego $y \in L$ mamy $y \preccurlyeq x$, to także $y \preccurlyeq z, \forall_{y \in L}$, a zatem z jest majorantą L. Skoro z założenia $M(L) \subset L$, to $z \in L$, a zatem $z \preccurlyeq x$, bo x jest największym elementem L. W takim razie $x = z$ i wykazaliśmy, że x jest elementem maksymalnym w X. □

Mamy teraz dwie możliwości.

Możliwość I: Porządek $\preccurlyeq$ jest porządkiem liniowym na X. Wówczas X jest łańcuchem. Z założenia, ten łańcuch ma majorantę $x_0 \in X$, oraz wszystkie majoranty tego łańcucha są w X. Możemy zatem skorzystać z lematu 12.3, z którego dostajemy, że x_0 jest elementem największym w X, a więc i maksymalnym w X. To dowodzi tezy.

Możliwość II: Porządek $\preccurlyeq$ nie jest porządkiem liniowym na X. Ten przypadek jest bardziej skomplikowany. Wykorzystamy twierdzenie Zermelo, które mówi w szczególności, że w zbiorze X możemy wprowadzić dobry porządek. Oznaczmy go $\leqslant$. Zdefiniujmy podzbiór X:

$$Y := \{y \in X : D_{\leqslant}(y) \text{ nie jest } \preccurlyeq\text{-łańcuchem w } X\},$$

gdzie $D_{\leqslant}(y)$ oznacza domknięty odcinek początkowy wyznaczony przez punkt y względem dobrego porządku $\leqslant$, zob. definicja 8.25.

Wykażemy następujący lemat.

Lemat 12.4. *Jeśli $Z \subset X$ nie jest $\preccurlyeq$-łańcuchem, to $Z \cap Y \neq \varnothing$. W szczególności, $Y \neq \varnothing$.*

Dowód lematu 12.4. Weźmy zbiór Z, który nie jest $\preccurlyeq$-łańcuchem (taki zbiór istnieje, bo porządek $\preccurlyeq$ nie jest liniowy). Istnieją zatem $x, y \in Z$ nieporównywalne względem $\preccurlyeq$, natomiast x, y są porównywalne względem porządku $\leqslant$ (który jest w szczególności porządkiem liniowym). Bez zmniejszenia ogólności możemy przyjąć, że $x \leqslant y$. Wtedy $x \in D_{\leqslant}(y)$ oraz $D_{\leqslant}(y)$ nie jest $\preccurlyeq$-łańcuchem (bo x, y nie są porównywalne względem $\preccurlyeq$.) Z definicji Y mamy, że $y \in Y$, a zatem $y \in Z \cap Y$; w szczególności mamy także $Y \neq \varnothing$. □

Zbiór Y jest niepustym podzbiorem zbioru dobrze uporządkowanego $(X, \leqslant)$. Niech y_1 oznacza najmniejszy (w sensie porządku $\leqslant$) element zbioru Y. Zdefiniujmy pewien odcinek początkowy:

$$L_1 := \mathcal{O}_{\leqslant}(y_1).$$

Zauważmy, że $L_1 \neq \varnothing$. Faktycznie, skoro $y_1 \in Y$, to domknięty odcinek początkowy $D_{\leqslant}(y_1)$ nie jest $\preccurlyeq$-łańcuchem, zatem istnieje co najmniej jeden element $x \in D_{\leqslant}(y_1)$ nieporównywalny względem $\preccurlyeq$ z y_1, czyli $\#D_{\leqslant}(y_1) \geqslant 2$, skąd $\#\mathcal{O}_{\leqslant}(y_1) \geqslant 1$, czyli $\mathcal{O}_{\leqslant}(y_1) = L_1 \neq \varnothing$.

Co więcej, zauważmy też, że

$$L_1 \cap Y = \varnothing.$$

Faktycznie, $L_1 = \mathcal{O}_{\leqslant}(y_1) = \{x \in X : x < y_1\}$ ($<$ oznacza jak zwykle „mniejsze lub równe i różne"), zatem ponieważ y_1 jest najmniejszym elementem Y, to żaden z elementów L_1 nie może należeć do Y.

W takim razie L_1 jest $\preccurlyeq$-łańcuchem. Gdyby bowiem L_1 nie był $\preccurlyeq$-łańcuchem, to miałby – z lematu 12.4 – niepuste przecięcie z Y.

Udowodnimy teraz trzeci (i ostatni) lemat.

Lemat 12.5. *Majoranty L_1 względem porządku $\preccurlyeq$ zawierają się w L_1, czyli*

$$M_{\preccurlyeq}(L_1) \subset L_1.$$

Dowód lematu 12.5. Dla dowodu nie wprost przypuśćmy, że $M(L_1) \setminus L_1 \neq \varnothing$. Wówczas, z określenia funkcji f mamy

$$f(L_1) \in M(L_1) \setminus L_1.$$

Porządek $\leqslant$ jest zgodny z f, zatem

$$f(L_1) = f(\mathcal{O}_{\leqslant}(y_1)) = y_1$$

a zatem

$$y_1 \in M(L_1) \setminus L_1.$$

W takim razie y_1 jest majorantą (w porządku $\preccurlyeq$) L_1, zatem dla wszelkich $y \in L_1$ mamy $y \preccurlyeq y_1$. Stąd wynika następująca obserwacja:

Obserwacja. *$D_{\leqslant}(y_1)$ jest $\preccurlyeq$-łańcuchem.*

Faktycznie, z powyższego wynika, że y_1 jest porównywalny z każdym elementem $\mathcal{O}_{\leqslant}(y_1)$. Przypuśćmy, że w $D_{\leqslant}(y_1)$ istnieją y_2, y_3 (różne od y_1) nieporównywalne względem $\preccurlyeq$. Te elementy są porównywalne względem $\leqslant$, możemy przyjąć, że $y_3 \leqslant y_2$, zatem $D_{\leqslant}(y_2)$ zawiera element y_3 nieporównywalny względem $\preccurlyeq$ z y_2, czyli $D_{\leqslant}(y_2)$ nie jest $\preccurlyeq$-łańcuchem, czyli $y_2 \in Y$. Z drugiej strony $L_1 = \mathcal{O}_{\leqslant}(y_1) \supset D_{\leqslant}(y_2)$, czyli $y_2 \in L_1$, zarazem, jak zobaczyliśmy wyżej, $L_1 \cap Y = \varnothing$, co daje sprzeczność.

Skoro $D_{\leqslant}(y_1)$ jest $\preccurlyeq$-łańcuchem, to, z definicji Y, $y_1 \notin Y$, co daje sprzeczność z faktem, że y_1 jest (najmniejszym) elementem Y. Tym sposobem zakończyliśmy dowód lematu 12.5. □

Aby zakończyć dowód całego twierdzenia (lematu Kuratowskiego–Zorna) wystarczy zauważyć, że właśnie wykazaliśmy, że

$$M_{\preccurlyeq}(L_1) \subset L_1,$$

zatem na podstawie lematu 12.3 L_1 ma element największy, który jest maksymalny w X. Zatem w X istnieje element maksymalny. □

Uwaga 12.6. Zauważmy, że w założeniach twierdzenia 12.2 jest zdanie „każdy łańcuch w X ma majorantę w X". Istotne jest, żeby majoranta łańcucha z X należała do X, w przeciwnym razie twierdzenie nie musi zachodzić. Rozważmy na przykład $X = (0, 1)$ z naturalnym porządkiem. Każdy łańcuch z tego przedziału ma majorantę w $\mathbb{R}$, ale nie każdy ma majorantę w X, przykładowo $\{1 - \frac{1}{n} : n \in \mathbb{N}\}$ nie ma majoranty w $(0, 1)$; i oczywiście w X nie ma elementu maksymalnego.

Rozdział 13

Pewne zastosowania lematu Kuratowskiego–Zorna.

Na tym wykładzie pokażemy, że z lematu Kuratowskiego–Zorna wynika pewnik wyboru i przedstawimy zastosowania tego lematu do dowodu, że każda przestrzeń wektorowa ma bazę i do wykazania twierdzenia o porównywaniu liczb kardynalnych.

Twierdzenie 13.1. *Weźmy zbiór częściowo uporządkowany $(X, \leqslant)$. Załóżmy, że zachodzi lemat Kuratowskiego–Zorna.*

Wówczas dla dowolnej (niepustej) rodziny zbiorów niepustych $\{A_i\}_{i\in I}$ istnieje funkcja $f : I \to \bigcup_{i\in I} A_i$

$$f(i) \in A_i.$$

Dowód. Zakładamy, że z tego, że każdy łańcuch w X ma majorantę w X, wynika, że w X istnieje element maksymalny.

Zdefiniujmy zbiór P jako zbiór funkcji prowadzących z pewnego podzbioru zbioru wskaźników w $\bigcup_{i\in I} A_i$ oraz takich, że $f(i) \in A_i$, dokładniej:

$$P := \{(J_f, f) | J_f \subset I \wedge f : J_f \to \bigcup_{i\in I} A_i \wedge i \in J_f \Longrightarrow f(i) \in A_i\}.$$

Zauważmy, że P jest zbiorem niepustym, bo biorąc $i_0 \in I$ i $J = \{i_0\}$ dla dowolnego elementu $a \in A_{i_0}$, możemy zdefiniować $f(i_0) = a$. Zatem para $(\{i_0\}, f)$ dla tak zdefiniowanego f należy do P.

Na zbiorze P zdefiniujmy porządek $\leqslant$ następująco. Dla $f, g \in P$

$$f \leqslant g \iff J_f \subset J_g \wedge g|_{J_f} = f.$$

Sprawdzimy, że każdy łańcuch w zbiorze P ma majorantę. Weźmy łańcuch L i zdefiniujmy

$$J_0 = \bigcup_{(J_f,f)} J_f \subset I$$

jako dziedzinę funkcji

$$f_0 = \bigcup_{(J_f,f)} f.$$

Zauważmy, że f_0 jest funkcją, co wynika z faktu, że sumujemy funkcje z łańcucha i z definicji porządku na P. Zauważmy też, że (J_0, f_0) jest majorantą łańcucha L, bo jeśli $i \in J_0$ to $i \in J_f$ dla pewnego J_f a zatem $f_0(i) = f(i) \in A_i$, czyli $f_0(i) \in A_i$ dla każdego $i \in J_0$. W takim razie z lematu Kuratowskiego–Zorna wynika, że mamy w P element maksymalny, niech to będzie funkcja g z dziedziną J_g. Wystarczy wykazać, że $J_g = I$. Gdyby $I \neq J_g$, to istniałoby $j \notin J_g, j \in I$. Zdefiniujmy $J := J_g \cup \{j\}$ i funkcję $h : J \to \bigcup_i A_i$ taką, że $h(i) = g(i)$ jeśli $i \in J_g$ oraz $h(j) = a \in A_j$, dla dowolnego elementu $a \in A_j$. Wtedy (J_g, g) jest elementem P istotnie mniejszym niż (J, h), co jest sprzeczne z faktem, że (J_g, g) jest elementem maksymalnym. Zatem $J_g = I$. □

Kolejnym twierdzeniem, które wykażemy, jest twierdzenie o porównywaniu mocy zbiorów. W dowodzie tego twierdzenia wykorzystamy lemat Kuratowskiego–Zorna.

Twierdzenie 13.2. *Dla dowolnych dwóch zbiorów A, B zachodzi co najmniej jedna z nierówności:*

$$\#A \leqslant \#B, \quad \#B \leqslant \#A.$$

Dowód. Rozważmy zbiór X składający się z funkcji f takich, że

- $\mathrm{Dom}_f \subset A$
- $\mathrm{Dom}_f^* \subset B$
- f jest injekcją.

Elementy zbioru X traktujmy jako podzbiory $A \times B$ (funkcje są podzbiorami iloczynu kartezjańskiego). Zauważmy, że zbiór X jest niepusty, bo należy do niego przynajmniej funkcja pusta (czyli pusty podzbiór $A \times B$). Wprowadźmy w X porządek za pomocą relacji zawierania, określonej na podzbiorach $A \times B$.

Wykażemy teraz, że w zbiorze X istnieje element maksymalny. Niech L będzie łańcuchem w X, zatem jeśli $f_1, f_2 \in L$, to $f_1 \subset f_2$ lub $f_2 \subset f_1$.

Zdefiniujmy podzbiór

$$s = \bigcup_{f \in L} f.$$

Oczywiście $s \subset A \times B$. Chcemy sprawdzić, że s jest majorantą L w X. Musimy zatem sprawdzić, że s jest funkcją, większą lub równą od wszystkich funkcji L, oraz, że s jest injekcją.

Sprawdźmy, czy s jest funkcją. Niech $(x, y_1) \in s$ i $(x, y_2) \in s$ dla pewnych $x \in A$, $y_1, y_2 \in B$. Wówczas, z definicji sumy, istnieją $f_1, f_2 \in L$ takie, że $(x, y_1) \in f_1$ i $(x, y_2) \in f_2$. Ponieważ L jest łańcuchem, możemy, bez zmniejszenia ogólności, przyjąć, że $f_1 \subset f_2$. Zatem $(x, y_1) \in f_2$ i $(x, y_2) \in f_2$, a skoro f_2 jest funkcją, to $y_1 = y_2$.

Wprost z definicji s jako sumy funkcji łańcucha wynika, że funkcja s zawiera wszystkie funkcje f z łańcucha L, a więc jest majorantą L.

Sprawdźmy teraz, że s jest injekcją. Niech $(x_1, y) \in s$ i $(x_2, y) \in s$, dla pewnych $x_1, x_2 \in A$, $y \in B$. Podobnie jak wyżej, z definicji sumy, istnieją $f_1, f_2 \in L$ takie, że $(x_1, y) \in f_1$ i $(x_2, y) \in f_2$. Możemy znów, bez zmniejszenia ogólności, przyjąć, że $f_1 \subset f_2$. Zatem $(x_1, y) \in f_2$ i $(x_2, y) \in f_2$, a skoro f_2 jest injekcją, to $x_1 = x_2$, a więc s jest injekcją.

Wykazaliśmy więc, że każdy łańcuch w X ma majorantę w X. Z lematu Kuratowskiego–Zorna wynika zatem, że w X istnieje element maksymalny. Nazwijmy ten element maksymalny h.

Zauważmy, że jeśli h jest elementem maksymalnym w X, to $\mathrm{Dom}_h = A$ lub $\mathrm{Dom}_h^* = B$. Faktycznie, gdyby $\mathrm{Dom}_h \neq A$ i $\mathrm{Dom}_h^* \neq B$, to istniałyby dwa elementy a, b, takie, że $a \in A \setminus \mathrm{Dom}_f$ i $b \in B \setminus \mathrm{Dom}_f^*$. Mielibyśmy wtedy element $g := h \cup \{(a, b)\}$, istotnie większy od h i będący oczywiście funkcją injektywną (czyli $g \in X$ i $h \subsetneq g$). To daje sprzeczność z maksymalnością h.

W takim razie h jest elementem X spełniającym warunek

$$\mathrm{Dom}_h = A \text{ lub } \mathrm{Dom}_h^* = B.$$

Jeśli $\mathrm{Dom}_h = A$, to funkcja h jest, jako element X, injekcją z A w B, a zatem $\#A \leqslant \#B$.

Jeśli $\mathrm{Dom}_h^* = B$, to funkcja h^{-1} (która prowadzi z B do Dom_h, i jest dobrze zdefiniowana, bo funkcja h jest injekcją, a zatem jest bijekcją na $\mathrm{Im}(h) = B$) jest injekcją z B w A. Zatem, skoro mamy injekcję z B w A to $\#B \leqslant \#A$.

To kończy dowód twierdzenia. □

Kolejne twierdzenie wykracza nieco poza materiał wstępu do teorii mnogości. Mówi ono, że każda przestrzeń wektorowa ma bazę. Czytelnik, który jeszcze nie miał wykładu z algebry liniowej, może to twierdzenie pominąć.

Twierdzenie 13.3. *Każda niezerowa przestrzeń wektorowa ma bazę.*

Dowód. Przypomnijmy, że bazą przestrzeni wektorowej V nazywamy maksymalny (w sensie inkluzji) podzbiór wektorów liniowo niezależnych w tej przestrzeni. Niech v_1 będzie niezerowym wektorem. Łatwo zauważyć, że zbiór złożony tylko z wektora v_1 jest zbiorem wektorów liniowo niezależnych w V. Zdefiniujmy zbiór X następująco:

$$X = \{A \subset X : v_1 \in A \text{ i } A \text{ jest zbiorem wektorów liniowo niezależnych}\}.$$

Na zbiorze X wprowadzamy porządek częściowy za pomocą relacji inkluzji.

Jeśli uda nam się pokazać (wykorzystując lemat Kuratowskiego–Zorna), że w X istnieje element maksymalny, powiedzmy A_0, to ten element będzie bazą V.

Weźmy zatem łańcuch $L \subset X$. Weźmy $S = \bigcup_{A \in L} A$. Oczywiście, dla dowolnego $A \in L$ mamy $A \subset S$, zatem S jest majorantą L. Aby sprawdzić, czy S należy do X, trzeba sprawdzić, czy $v_1 \in S$ i czy S jest zbiorem wektorów liniowo niezależnych. Skoro $v_1 \in A$ dla każdego $A \in L$, to oczywiście $v_1 \in S = \bigcup_{A \in L} A$. Pozostaje sprawdzić, że S jest zbiorem wektorów liniowo niezależnych. Z definicji liniowej niezależności zbioru wektorów, oznacza to, że mamy sprawdzić, że dowolny skończony podzbiór $W = \{w_1, \dots w_k\} \subset S$ jest zbiorem wektorów liniowo niezależnych. Skoro $w_1, \dots w_k \in S$, to istnieją $A_1, \dots, A_k \in L$ takie, że $w_i \in A_i$, $i = 1, \dots, k$. Skoro L jest łańcuchem, to wszystkie te zbiory są porównywalne ze sobą, możemy więc, dokonując ewentualnie ich przenumerowania, założyć, że $A_1 \subset A_2 \subset \dots A_k$. Wtedy $w_1, \dots, w_k \in A_k$, ale A_k jest zbiorem wektorów liniowo niezależnych. Zatem $w_1, \dots, w_k$ są liniowo niezależne. W takim razie S jest zbiorem wektorów liniowo niezależnych, czyli majorantą łańcucha w X.

Wykazaliśmy zatem, że każdy łańcuch w X ma majorantę w X, w takim razie, z lematu Kuratowskiego–Zorna, wynika, że w X istnieje element maksymalny A_0. Ten element jest bazą V (jako maksymalny w sensie zawierania podzbiór wektorów liniowo niezależnych). □

Uwaga 13.4. Warto zastanowić się nad sytuacją, gdy rozważamy $\mathbb{R}$ jako przestrzeń wektorową nad $\mathbb{Q}$.

Rozdział 14

Twierdzenie Zermelo o dobrym uporządkowaniu (i szkic dowodu)

Na tym wykładzie naszkicujemy dowód tego, że z pewnika wyboru wynika twierdzenie Zermelo.

Dowód jest prowadzony według jednego z dowodów przedstawionych w podręczniku [4], do którego odsyłamy Czytelnika zainteresowanego też innymi dowodami.

Przypomnijmy:

Niech dany będzie zbiór $(X, \leqslant)$ dobrze uporządkowany i funkcja $f : \mathcal{P}(X) \setminus \{X\} \to X$ będzie taka, że $f(A) \notin A$. Mówimy, że porządek $\leqslant$ jest zgodny z f, jeśli dla każdego $a \in X$ zachodzi

$$a = f(\mathcal{O}(a)),$$

gdzie odcinkiem początkowym wyznaczonym przez element $a \in X$ nazywamy

$$\mathcal{O}(a) = \{x \in X : x \leqslant a \wedge x \neq a\}.$$

Zachodzi następujące stwierdzenie (będzie potrzebne do dowodu twierdzenia Zermelo):

Stwierdzenie 14.1. *Niech $(X, \leqslant)$ będzie zbiorem liniowo uporządkowanym. Wtedy następujące warunki są równoważne:*

(1) $\leqslant$ jest dobrym porządkiem;

(2) jeśli $\mathcal{O}$ jest odcinkiem początkowym (zob. definicja 8.25), to istnieje $a \in X$, taki, że $\mathcal{O} = \mathcal{O}(a)$;

(3) żaden ciąg w X nie jest ciągiem (silnie) malejącym.

Zanim zaczniemy dowód, zobaczmy „negatywny" przykład do stwierdzenia. Weźmy $\mathbb{R}$ z naturalnym porządkiem, $\leqslant$. Ten zbiór nie jest dobrze uporządkowany. Faktycznie, na przykład w zbiorze $(0, 1) \subset \mathbb{R}$ nie ma elementu najmniejszego. Zbiór $\{x \in \mathbb{R} : x < b, \forall_{b\in(0,1)}\}$ jest odcinkiem początkowym, ale nie jest odcinkiem początkowym wyznaczonym przez jakiś element $a \in \mathbb{R}$. Oczywiście mamy w $\mathbb{R}$ ciągi malejące (na przykład $a_n = -n$). Przejdźmy teraz do dowodu stwierdzenia.

Dowód. Możemy założyć, że X jest zbiorem niepustym.

(1) $\Longrightarrow$ (2). Weźmy $\mathcal{O}$, właściwy (zatem różny od X) odcinek początkowy w X. Skoro porządek jest dobry, to w $X \setminus \mathcal{O}$ (niepusty!) istnieje element najmniejszy, a. Wykażemy teraz, że $\mathcal{O} = \mathcal{O}a$. Jeśli $y \in \mathcal{O}(a)$, to $y \in \mathcal{O}$, bo a jest najmniejszym spośród elementów nienależących do $\mathcal{O}$. Jeśli $y \in \mathcal{O}$, to $y \leqslant a \wedge y \neq a$, zatem $y \in \mathcal{O}(a)$. Stąd $\mathcal{O} = \mathcal{O}(a)$.

(2) $\Longrightarrow$ (3). Weźmy ciąg $(x_n)_{n\in\mathbb{N}} \subset X$. Zdefiniujmy $\mathcal{O}$ jako zbiór punktów X mniejszych (lub równych) od wszystkich wyrazów ciągu, $y \in \mathcal{O} \iff y \leqslant x_n, \forall_{n\in\mathbb{N}}$. Zauważmy, że $\mathcal{O}$ jest odcinkiem początkowym zbioru X (bo wraz z każdym elementem zawiera wszystkie od niego mniejsze). Jeśli $\mathcal{O} = X$, to ciąg (x_n) musi być stały (równy największemu elementowi X). Jeśli $\mathcal{O}$ jest właściwym odcinkiem początkowym, to istnieje $a \in X$ taki, że $\mathcal{O} = \mathcal{O}(a)$, ale skoro $a \notin \mathcal{O}(a) = \mathcal{O}$, to istnieje element ciągu x_N taki, że $x_N < a$. Stąd $x_N \in \mathcal{O}$, a stąd $x_N \leqslant x_n$ dla wszystkich n, czyli w szczególności $x_N \leqslant x_{N+1}$, a zatem ciąg $(x_n)_{n\in\mathbb{N}}$ nie jest malejący.

(3) $\Longrightarrow$ (1). Całkiem formalny dowód tego wynikania wymaga twierdzenia o definiowaniu przez indukcję z wykładu 15, tu przedstawimy szkic rozumowania. Niech A będzie niepustym podzbiorem zbioru X. Weźmy dowolny element $x_0 \in A$. Jeśli ten element jest najmniejszy w A, to skończyliśmy dowód. Jeśli nie, to istnieje element x_1 od niego mniejszy. Jeśli x_1 to nie jest najmniejszy element A to kontynuujemy postępowanie, konstruując wyrazy $x_1 > x_2 > x_3 \dots$. Jeśli żaden z elementów x_n nie jest elementem najmniejszym w A, dostajemy nieskończony ciąg ściśle malejący, sprzeczność. □

Twierdzenie 14.2 (Zermelo)**.** *Niech dany będzie zbiór X i funkcja $f : \mathcal{P}(X) \setminus \{X\} \to X$ będzie taka, że $f(A) \notin A$. Wówczas istnieje dokładnie jeden porządek na X, dobry i zgodny z f.*

Dowód. Dowód twierdzenia opiera się na serii lematów.

Przypomnijmy, że podzbiór A zbioru X jest zgodny z f, jeśli istnieje na A dobry porządek $\leqslant_A$, zgodny z f.

Przykładowo, łatwo sprawdzić, że dla $a \in X$ z $f(\varnothing) = \{a\}$ zbiór $\{a\}$ jest dobrze uporządkowany i zgodny z f.

Lemat 14.3. *Każdy odcinek początkowy zbioru A zawartego w X i zgodnego z funkcją f jest też zgodny z funkcją f.*

Dowód lematu 14.3. Niech $C \subset A$ będzie jakimś odcinkiem początkowym zbioru A (z porządkiem z A zacieśnionym do C). Aby wykazać, że C jest zgodny z f, musimy wziąć jakiś odcinek początkowy zbioru C, powiedzmy $\mathcal{O}_{\leqslant_C}(c)$ dla pewnego $c \in C$ (przypomnijmy, że każdy odcinek początkowy jest wyznaczony przez jakiś element zbioru) i sprawdzić, że $f(\mathcal{O}_{\leqslant_C}(c)) = c$. Zauważmy, że

$$\mathcal{O}_{\leqslant_C}(c) = \mathcal{O}_{\leqslant_A}(c),$$

bo na C mamy zacieśnienie porządku z A. W takim razie

$$f(\mathcal{O}_{\leqslant_C}(c)) = f(\mathcal{O}_{\leqslant_A}(c)) = c,$$

gdzie druga nierówność wynika z założenia, że porządek na A jest zgodny z f. □

Lemat 14.4. *Niech dane będą dwa podzbiory A, B zbioru X, zgodne z f. Niech C będzie właściwym odcinkiem początkowym zbioru $(A \leqslant_A)$ i zbioru $(B, \leqslant_B)$ (właściwym, czyli $C \neq A, C \neq B$). Wówczas istnieje $c \in A \cap B$ takie, że $C = \mathcal{O}_{\leqslant_A}(c)$ i $C = \mathcal{O}_{\leqslant_B}(c)$.*

Dowód lematu 14.4. Skoro C jest odcinkiem początkowym A, to $C = \mathcal{O}_{\leqslant_A}(a)$ dla pewnego $a \in A$ i tak samo, skoro C jest odcinkiem początkowym B to $C = \mathcal{O}_{\leqslant_B}(b)$ dla pewnego $b \in B$. Ponieważ A jest zgodny z f, to $f(C) = f(\mathcal{O}_{\leqslant_A}(a)) = a$ i ponieważ B jest zgodny z f, to $f(C) = f(\mathcal{O}_{\leqslant_B}(b)) = b$; zatem $a = b$, więc biorąc $c := a = b$ wykazaliśmy lemat. □

Lemat 14.5. *Niech dane będą dwa podzbiory $(A, \leqslant_A), (B, \leqslant_B)$ zbioru X, zgodne z f. Wówczas jeden z tych zbiorów jest odcinkiem początkowym drugiego.*

Dowód lematu 14.5. Niech $\mathcal{R}$ będzie rodziną złożoną ze zbiorów $R \subset A \cap B$ takich, że R jest odcinkiem początkowym zarówno $(A, \leqslant_A)$, jak i $(B, \leqslant_B)$.

Niech

$$C = \bigcup_{R \in \mathcal{R}} R.$$

Zauważmy, że z definicji odcinka początkowego wynika, że suma odcinków początkowych jest odcinkiem początkowym. Zatem C jest odcinkiem początkowym zarówno A jak i B, czyli $C \in \mathcal{R}$. Zauważmy też, że C jest też największym w sensie zawierania elementem w $\mathcal{R}$. Tezę lematu dostaniemy, jeśli wykażemy, że $C = A$ lub $C = B$. Przypuśćmy zatem, że $C \neq A$ i $C \neq B$. Zatem C jest właściwym odcinkiem początkowym dla A i B, spełnia zatem założenia lematu 14.4. Istnieje więc element $c \in A \cap B$ taki, że

$$C = \mathcal{O}_{\leqslant_A}(c) \text{ i } C = \mathcal{O}_{\leqslant_B}(c).$$

Wtedy jednak $c \notin C$, zatem zbiór $C' = C \cup \{c\}$ jest odcinkiem początkowym i dla A i dla B, silnie większym od C. Uzyskaliśmy zatem sprzeczność z faktem, że C jest też największym w sensie zawierania elementem w $\mathcal{R}$, skąd wynika, że musi być $C = A$ lub $C = B$, a zatem jeden z tych zbiorów jest odcinkiem początkowym drugiego. □

Lemat 14.6. *Niech dane będą dwa podzbiory $(A, \leqslant_A), (B, \leqslant_B)$ zbioru X, zgodne z f oraz element $y \in A \cap B$. Wówczas*

$$\mathcal{O}_A(y) = \mathcal{O}_B(y),$$

czyli inaczej

$$\forall_{x \in X}\ x <_A y \iff x <_B y.$$

Dowód lematu 14.6. Zauważmy najpierw, że z tego lematu wynika, że jeśli zbiór $A \subset X$ jest zgodny z f to $\leqslant_A$ jest jedynym dobrym porządkiem na A zgodnym z f. Faktycznie, gdyby istniały dwa porządki, $\leqslant_1, \leqslant_2$, wystarczy zastosować lemat do $(A, \leqslant_1)$ i do $(B, \leqslant_B) = (A, \leqslant_2)$.

Aby udowodnić lemat 14.6 zauważmy, że z lematu 14.3 wynika, że $\mathcal{O}_A(y)$ jest zgodny z f. Skoro $y \notin \mathcal{O}_A(y)$, to $y \in B \setminus \mathcal{O}_A(y)$, zatem B nie jest odcinkiem początkowym $\mathcal{O}_A(y)$.

Natomiast, skoro $\mathcal{O}_A(y)$ i B są zgodne z f, to na podstawie lematu 14.5 jeden z nich jest odcinkiem początkowym drugiego; zatem $\mathcal{O}_A(y)$ jest odcinkiem początkowym B. W takim razie $\mathcal{O}_A(y)$ jest odcinkiem początkowym A i B. Lemat 14.4 mówi, że w takim razie ten odcinek jest w obu zbiorach wyznaczony przez ten sam element, a w zbiorze A jest to element y. Zatem

$$\mathcal{O}_A(y) = \mathcal{O}_B(y),$$

co kończy dowód lematu. □

Kolejny lemat jest ostatnim przed dowodem samego twierdzenia Zermelo.

Lemat 14.7. *Niech $\mathcal{R}$ będzie rodziną podzbiorów X zgodnych z f. Niech*

$$Y := \bigcup \mathcal{R}.$$

Określmy na Y relację porządku. Niech $x, y \in Y$

$$x \leqslant y \iff \exists_{A \in \mathcal{R}} : x \leqslant_A y.$$

Tak określony porządek jest dobrym porządkiem na Y, zgodnym z f.

Dowód lematu 14.7.
1. Z lematu 14.6 porządek na dowolnym zbiorze $A \in \mathcal{R}$ zgodny z f, czyli $\leqslant_A$ jest na A równy porządkowi na Y, zacieśnionemu do A czyli $\leqslant |_A$ (jako B bierzemy $(A, \leqslant |_A)$).

2. Mamy wykazać, że $\leqslant$ jest porządkiem liniowym na Y (czyli, że relacja $\leqslant$ jest zwrotna, słabo antysymetryczna, przechodnia i spójna). Niech $x, y, z \in Y$. Istnieją zatem $A_x, A_y, A_z \in \mathcal{R}$ takie, że $x \in A_x, y \in A_y, z \in A_z$. Ponieważ A_x, A_y, A_z są zgodne z f, to dla każdych dwóch z nich jeden jest odcinkiem początkowym drugiego. W takim razie, na przykład A_x i A_y są odcinkami początkowymi A_z. Stąd, $x, y, z \in A_z$ a relacja $\leqslant$ zacieśniona do A_z jest relacją porządku liniowego.

3. Chcemy teraz wykazać, że dla każdego zbioru A z rodziny $\mathcal{R}$ oraz dla $y \in A$ odcinek początkowy wyznaczony przez y w A jest taki sam jak odcinek początkowy wyznaczony przez y w Y, czyli

$$\mathcal{O}_Y(y) = \mathcal{O}_A(y).$$

Z definicji porządku na zbiorze Y mamy wynikanie: $x <_A y \Longrightarrow x <_Y y$ (dla $x \in Y$). Z drugiej strony, jeśli $x <_Y y$, to istnieje zbiór $B \in \mathcal{R}, y \in B$ taki, że $x <_B y$. Skoro $y \in A \cap B$, to z lematu 14.6 mamy $x <_B y \iff x <_A y$, co daje wynikanie w drugą stronę.

4. Pokażemy teraz, że porządek $\leqslant$ na Y jest dobry. Gdyby tak nie było, to ze stwierdzenia 14.1(3) istniałby w Y ciąg $(y_n)_{n \in \mathbb{N}}$ malejący w porządku $\leqslant$. Weźmy y_1 z tego ciągu. Istnieje zbiór A z rodziny $\mathcal{R}$ taki, że $y_1 \in A$. Skoro $y_n <_Y y_1$ to także $y_n <_A y_1$, czyli y_n tworzą malejący ciąg elementów z A, a zatem, znowu ze stwierdzenia 14.1, porządek na A nie jest dobry, sprzeczność.

5. Zauważmy, że porządek $\leqslant$ jest zgodny z funkcją f. Faktycznie, niech $y \in Y$. Wówczas $y \in A$, dla pewnego $A \in \mathcal{R}$. Z punktu 3. wiemy, że $\mathcal{O}_Y(y) = \mathcal{O}_A(y)$. Zatem $f(\mathcal{O}_Y(y)) = f(\mathcal{O}_A(y)) = y$. □

Możemy teraz przejść do dowodu twierdzenia Zermelo. Z lematu 14.7 wynika, że na zbiorze Y mamy porządek $\leqslant$ dobry i zgodny z f. Zatem $Y \in \mathcal{R}$, oczywiście Y jest największym w sensie zawierania elementem $\mathcal{R}$. Z lematu 14.6 wynika, że porządek $\leqslant$ jest jedynym dobrym porządkiem na Y zgodnym z f. Wystarczy teraz pokazać, że $Y = X$.

Przypuśćmy zatem, że $Y \neq X$. Wówczas istnieje $z \in X \setminus Y$ takie, że $f(Y) = z$. Zdefiniujmy $Z := Y \cup \{z\}$. Zdefiniujmy na Z porządek $\leqslant_Z$ tak, że $\leqslant_Z |_Y = \leqslant_Y = \leqslant$ oraz $\forall_{y \in Y}\ y <_Z z$. Łatwo zobaczyć, że $\leqslant_Z$ jest porządkiem liniowym i dobrym na Z. Porządek ten jest też zgodny z f, bo jeśli $x \in Y$, to $\mathcal{O}_Y(x) = \mathcal{O}_Z(x)$ z definicji porządku na Z, a zatem $f(\mathcal{O}_Z(x)) = f(\mathcal{O}_Y(x)) = x$, a jeśli $x = z$, to $\mathcal{O}_Z(x) = Y$, czyli $f(\mathcal{O}_Z(x)) = f(Y) = z = x$ z powyższego wyboru z. To daje nam dobry i zgodny z f porządek na zbiorze Z, ściśle większym od Y, co jest sprzeczne ze stwierdzonym wyżej faktem, że Y jest największym w sensie zawierania elementem $\mathcal{R}$. To kończy dowód twierdzenia Zermelo.

□

Rozdział 15

Aksjomatyczna konstrukcja liczb naturalnych (dodatek)

Na tym wykładzie zapoznamy się z podstawami aksjomatycznej konstrukcji liczb naturalnych

Aksjomatyczną konstrukcji liczb naturalnych zawdzięczamy między innymi Ernestowi Zermelo, Abrahamowi Fraenklowi, Albertowi Skolemowi, Johnowi von Neumannowi i Guiseppe Peano. Ernst Zermelo sformułował aksjomat wyboru i z jego pomocą udowodnił twierdzenie o dobrym uporządkowaniu. W 1908 przedstawił system aksjomatów teorii mnogości, następnie zmodyfikowany przez Fraenkla i Skolema[1]. John von Neuman[2] zaproponował konstrukcję liczb naturalnych a Giuseppe Peano[3] opracował aksjomatykę arytmetyki liczb naturalnych.

Zapoznamy się też z twierdzeniami o definiowaniu i dowodzeniu przez indukcję. Wykład ma częściowo charakter informacyjny, nie wszystkich faktów będziemy dowodzić.

Oprócz wspomnianych wcześniej aksjomatów potrzebny nam będzie aksjomat zwany aksjomatem nieskończoności.

- Aksjomat nieskończoności: istnieje rodzina zbiorów $\mathcal{A}$ o następujących własnościach:
  1. $\varnothing \in \mathcal{A}$
  2. $X \in \mathcal{A} \Longrightarrow \exists Y \in \mathcal{A} : Y = X \cup \{X\}$.

Definicja 15.1. Rodzinę zbiorów spełniających warunki aksjomatu nieskończoności nazywamy *rodziną induktywną*, albo też: *zbiorem induktywnym*.

Definicja 15.2. Jeśli X jest zbiorem, to zbiór $X \cup \{X\}$ nazywamy następnikiem zbioru X i oznaczamy przez X'.

Konstrukcja von Neumanna liczb naturalnych opiera się przede wszystkim na następującym twierdzeniu.

Twierdzenie 15.3. *Istnieje dokładnie jeden zbiór $\mathbb{N}$ o następujących własnościach:*
(1) $\varnothing \in \mathbb{N}$
(2) $X \in \mathbb{N} \Longrightarrow X' \in \mathbb{N}$
(3) Jeśli zbiór K spełnia (1) *i* (2)*, to $\mathbb{N} \subset K$.*

Dowód. Dowód zaczniemy od następującego lematu.

Lemat 15.4. *Niech $\mathcal{R}$ będzie rodziną zbiorów induktywnych. Wówczas $\bigcap_{R\in\mathcal{R}} R$ jest też zbiorem induktywnym.*

Dowód lematu 15.4. Musimy sprawdzić warunki 1. i 2. aksjomatu nieskończoności. Skoro każdy zbiór R jest zbiorem induktywnym, to dla każdego R mamy $\varnothing \in R$, a zatem $\varnothing \in \bigcap_{R\in\mathcal{R}} R$, zatem warunek 1. jest spełniony. Aby sprawdzić warunek 2. musimy sprawdzić, czy jeśli $X \in \bigcap_{R\in\mathcal{R}} R$, to $X' \in \bigcap_{R\in\mathcal{R}} R$. Jeśli $X \in \bigcap_{R\in\mathcal{R}} R$, to $X \in R\ \forall_{R\in\mathcal{R}}$, a zatem (skoro R są induktywne) $X' \in R\ \forall_{R\in\mathcal{R}}$, czyli $X' \in \bigcap_{R\in\mathcal{R}} R$, więc spełniony jest też warunek 2. □

Z aksjomatu nieskończoności wynika, że istnieje co najmniej jeden zbiór induktywny, nazwijmy go $\mathcal{A}$. Weźmy podzbiory tego zbioru, $\mathcal{P}(\mathcal{A})$ (istnienie zbioru podzbiorów też wynika z przyjętych aksjomatów). Z $\mathcal{P}(\mathcal{A})$ wybieramy podzbiory induktywne, tę rodzinę podzbiorów nazwiemy $\mathcal{R}$. Rodzina $\mathcal{R}$ jest niepusta, bo $\mathcal{A} \in \mathcal{R}$. Z lematu 15.4

[1] Albert Skolem (1887–1963), norweski matematyk.
[2] John von Neuman (1903–1957), węgierski matematyk pochodzenia żydowskiego.
[3] Giuseppe Peano (1858–1932), włoski matematyk i logik.

wynika, że $\mathbb{N} := \bigcap_{R\in\mathcal{R}} R$ jest zbiorem induktywnym. Jeśli K jest innym zbiorem induktywnym to dla dowolnego zbioru R z $\mathcal{R}$ zbiór $R \cap K$ jest (z powyższego lematu) zbiorem induktywnym, zatem także elementem $\mathcal{R}$. Stąd $\mathbb{N} = \bigcap_{R\in\mathcal{R}} R \subset R \cap K \subset K$. $\mathbb{N}$ jest więc najmniejszym zbiorem induktywnym. □

Definicja 15.5. Ten najmniejszy względem inkluzji zbiór induktywny nazwiemy *zbiorem liczb naturalnych*, $\mathbb{N}$.

Uwaga 15.6. Von Neumann zaproponował następującą konstrukcję zbioru liczb naturalnych:

0 to $\varnothing$

1 to $\{\varnothing\}$

2 to $\{\varnothing, \{\varnothing\}\}$

3 to $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$

...

Zauważmy, że tak skonstruowany zbiór liczb naturalnych ma elementy, które są zbiorami, zatem każdą liczbę naturalną możemy traktować jako zbiór, co więcej, poprzednia liczba, czyli poprzedni zbiór (o ile taki jest) jest elementem następnego zbioru. Szczegółowiej zajmiemy się tymi własnościami w dalszej części wykładu.

Przejdźmy teraz do zasady indukcji matematycznej. W „szkolnej wersji" ta zasada jest następująca: jeśli T_n jest stwierdzeniem zawierającym liczbę naturalną n i jeśli twierdzenie T_1 jest prawdziwe, oraz dla wszystkich $k \in \mathbb{N}$ spełnione jest wynikanie: jeśli T_k jest prawdziwe, to T_{k+1} jest prawdziwe, to wtedy stwierdzenie T_n jest prawdziwe dla wszystkich $n \in \mathbb{N}$. W ten sposób można wykazać na przykład, że $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. W szkole średniej nie dowodzi się zasady indukcji, przyjmując ją jako aksjomat. Teraz wykażemy formalnie ten fakt. Dla uproszczenia notacji elementy $\mathbb{N}$, choć traktujemy je jako zbiory, będziemy oznaczać małymi literami m, n, x, y.

Twierdzenie 15.7 (Zasada indukcji)**.** *Niech P będzie podzbiorem skonstruowanego wyżej zbioru liczb naturalnych $\mathbb{N}$ takim, że $\varnothing \in P$ oraz dla każdego $x \in P$ zachodzi $x' \in P$. Wówczas $P = \mathbb{N}$.*

Dowód. Jeśli zbiór P spełnia założenia twierdzenia, to jest zbiorem induktywnym. W takim razie $\mathbb{N} \subset P$, bo $\mathbb{N}$ jest najmniejszym zbiorem induktywnym. Z założenia jednak $P \subset \mathbb{N}$. W takim razie $P = \mathbb{N}$. □

Zajmiemy się teraz wykazaniem pewnych wybranych własności liczb naturalnych; głównym narzędziem będzie zasada indukcji.

Stwierdzenie 15.8. *Każdy element liczby naturalnej jest liczbą naturalną, czyli:*

$$\forall_x\ x \in \mathbb{N} \Longrightarrow (\forall_y\ y \in x \Longrightarrow y \in \mathbb{N}).$$

Dowód. Wykorzystamy zasadę indukcji. Niech

$$P = \{n \in \mathbb{N} : \forall_y\ y \in n \Longrightarrow y \in \mathbb{N}\},$$

czyli P jest zbiorem liczb naturalnych, spełniających tezę dowodzonego stwierdzenia. Wystarczy wykazać, że $P = \mathbb{N}$. Sprawdźmy:

0. Warunek $P \subset \mathbb{N}$ jest spełniony.

1. Zachodzi $\varnothing \in P$, bo $\varnothing$ nie ma żadnych elementów, zatem wynikanie z tezy jest dla niego spełnione.

2. Musimy sprawdzić, czy jeśli $n \in P$ to $n' \in P$. Zbiór $n' = n \cup \{n\}$, zatem jeśli $y \in n'$, to albo $y \in n$ albo $y = n$. Jeśli zachodzi $y = n \in P$, to oczywiście $y \in \mathbb{N}$. Jeśli $y \in n$ a $n \in P$, to z definicji P mamy $y \in \mathbb{N}$. Stąd każdy element n' należy do $\mathbb{N}$, zatem $n' \in P$.

Sprawdziliśmy, że P jest zawartym w $\mathbb{N}$ zbiorem induktywnym. W takim razie z zasady indukcji $P = \mathbb{N}$, co kończy dowód stwierdzenia. □

Stwierdzenie 15.9. *Każda liczba naturalna jest zbiorem pustym lub jest następnikiem liczby naturalnej, czyli:*

$$\forall_x\ x \in \mathbb{N} \Longrightarrow (x = \varnothing \vee (\exists_y\ y \in \mathbb{N} \wedge y' = x)).$$

Dowód. Znowu wykorzystamy zasadę indukcji. Niech

$$P = \{n \in \mathbb{N} : (n = \varnothing \vee (\exists_m\ m \in \mathbb{N} \wedge m' = n)\},$$

czyli P jest zbiorem liczb naturalnych spełniających tezę dowodzonego stwierdzenia. Wystarczy wykazać, że $P = \mathbb{N}$. Sprawdzamy podobnie jak poprzednio:

0. $P \subset \mathbb{N}$.

1. Warunek $\varnothing \in P$ zachodzi z definicji P.

2. Musimy sprawdzić, czy jeśli $n \in P$ to $n' \in P$. Żeby $n' \in P$ wystarczy, by n' był następnikiem jakiejś liczby naturalnej, co oczywiście zachodzi, bo n' jest następnikiem n.

Z zasady Indukcji $P = \mathbb{N}$, co kończy dowód stwierdzenia. □

Teraz sformułujemy i wykażemy nieco dziwnie brzmiące stwierdzenie, które będzie nam potrzebne w dalszej części wykładu, gdzie zajmiemy się porządkiem w zbiorze liczb naturalnych.

Stwierdzenie 15.10. *Niech $n \in \mathbb{N}$ i niech y będzie zbiorem. Wówczas $y \in n \Longrightarrow y \subset n$.*

Dowód. Niech P będzie zbiorem liczb naturalnych spełniających tezę stwierdzenia,

$$P = \{n \in \mathbb{N} : y \in n \Longrightarrow y \subset n\}.$$

Sprawdzamy:
0. $P \subset \mathbb{N}$.

1. Warunek $\varnothing \in P$ zachodzi, bo poprzednik implikacji ($y \in \varnothing$) jest fałszywy, skąd implikacja jest prawdziwa.

2. Sprawdzamy, czy jeśli $n \in P$ to $n' \in P$. Jeśli $y \in n'$ to $y \in n$ albo $y = n$. Jeśli $y \in n$, a $n \in P$, to $y \subset n \subset n'$. Jeśli $y = n$, to skoro $n \subset n'$, to także $y \subset n'$.

W takim razie P jest zbiorem induktywnym, a więc $P = \mathbb{N}$. □

Kolejne stwierdzenie, które zostawimy bez dowodu (można go zrobić jako ćwiczenie), także wykorzystamy przy omawianiu własności porządku w liczbach naturalnych.

Stwierdzenie 15.11. *Niech $m, n \in \mathbb{N}$. Wówczas,*

1. $m' = n' \Longrightarrow m = n$;
2. $m \subset n \wedge m \neq n \Longrightarrow m \in n$;
3. $m \subset n \vee n \subset m$;
4. *zachodzi dokładnie jedna z trzech możliwości: $m \in n$, $m = n$, $n \in m$.*

Powiemy teraz parę słów o porządku w liczbach naturalnych. Zdefiniujemy relację $\leqslant$ na zbiorze $\mathbb{N}$ i, wykorzystując poprzednie stwierdzenia, wykażemy własności tej relacji.

Definicja 15.12. Niech $m, n \in \mathbb{N}$. Wtedy

1. $m \leqslant n \iff m \subset n$
2. $m < n \iff m \in n$,

gdzie, jak zawsze, „$m < n$” oznacza $m \leqslant n \wedge m \neq n$.

Relacja $\leqslant$ ma następujące własności:

Stwierdzenie 15.13.

1. $m < n \Longrightarrow m \leqslant n$
2. $m \leqslant n \wedge m \neq n \Longrightarrow m < n$
3. $m \leqslant n$ *lub* $n \leqslant m$
4. *Zachodzi dokładnie jedna z trzech możliwości: $m < n$, $m = n$, $n < m$.*

Dowód. Dowód jest natychmiastowym wnioskiem ze stwierdzenia 15.11. □

Stwierdzenie 15.14. *Relacja $\leqslant$ jest relacją porządku na $\mathbb{N}$.*

Dowód. Zwrotność, słaba antysymetryczność i przechodniość wynika od razu z własności relacji $\subset$. Przykładowo $m \leqslant n$ i $n \leqslant m$ oznacza, że $m \subset n$ i $n \subset m$, skąd wynika $m = n$, zatem $\leqslant$ jest relacją słabo antysymetryczną.

□

Wniosek 15.15. *Każda liczba naturalna to zbiór liczb (naturalnych) istotnie od niej mniejszych.*

Dowód. Warto spojrzeć teraz na konstrukcję von Neumanna (uwaga 15.6).

Tezę wniosku możemy zapisać następująco:

$$\forall_{n\in\mathbb{N}}\ (\forall_m\ m \in n) \iff (m \in \mathbb{N} \wedge m < n).$$

Wykażmy wynikanie ($\Longrightarrow$). Jeśli $m \in n$, to $m \in \mathbb{N}$ ze stwierdzenia 15.8, oraz $m < n$ wprost z definicji $<$.
Wynikanie ($\Longleftarrow$) jest natychmiastowe z definicji $<$. □

Kolejne stwierdzenie mówi, że pomiędzy liczbą naturalną a jej następnikiem nie ma innych liczb naturalnych (co w zasadzie wiemy od dawna ☺)

Stwierdzenie 15.16. *Niech $m, n \in \mathbb{N}$. Jeśli $n \leqslant m \leqslant n'$, to $m = n$ lub $m = n'$,*

Dowód. Niech $n \leqslant m$, załóżmy, że $m \neq n$. Będziemy chcieli wykazać, że $m = n'$. Z założenia mamy, że $m \leqslant n'$, co oznacza, że $m \subset n \cup \{n\}$, co oznacza, że $m \in n \cup \{n\}$ lub $m = n \cup \{n\} = n'$. Gdyby ta ostatnia równość nie zachodziła, to mielibyśmy $m \in n \cup \{n\}$. Są zatem dwie możliwości: $m \in n$ lub $m \in \{n\}$. Jeśli $m \in \{n\}$, to $m = n$, co jest sprzeczne z naszym założeniem na początku dowodu. Zatem $m \in n$. Równocześnie, z założenia, $n \leqslant m$, co z definicji $\leqslant$ zachodzi gdy $n \in m \vee n = m$. Możliwość $n = m$ została wykluczona, zatem zostaje $n \in m$, ale jednocześnie ciągle $m \in n$, co daje sprzeczność (zbiór nie może być swoim elementem). Stąd $m = n'$. □

Kolejne twierdzenie, zwane *zasadą minimum*, pozwoli nam stwierdzić, że porządek na $\mathbb{N}$ jest dobry. Zauważmy, że ze stwierdzenia 15.13.(4) wynika, że porządek $\leqslant$ jest liniowy.

Twierdzenie 15.17 (Zasada minimum)**.** *Każdy niepusty podzbiór zbioru liczb naturalnych ma element najmniejszy.*

Dowód. W tym dowodzie zrezygnujemy trochę z formalności na korzyść przejrzystości. Weźmy niepusty zbiór $X \subset \mathbb{N}$. Zdefiniujmy

$$Z = \{n \in \mathbb{N} : \{0, 1, \ldots, n\} \cap X = \varnothing\}.$$

Wykorzystamy zasadę indukcji. Gdyby w X nie było elementu najmniejszego, to $0 \notin X$, zatem $0 \in Z$. Jeśli $n \in Z$, to $\{0, \ldots, n\} \cap X = \varnothing$. Gdyby zatem zachodziło $n' \in X$, to n' byłby najmniejszym elementem X (a miało takiego nie być). W takim razie $n' \in Z$, zatem oba warunki zasady indukcji są spełnione, a więc wynika z niej, że $Z = \mathbb{N}$, to jednak oznacza, że $X = \varnothing$, sprzeczność. W takim razie w X istnieje element najmniejszy. □

Ostatnie wykazane na tym wykładzie twierdzenie, to twierdzenie o definiowaniu przez indukcję.

Twierdzenie 15.18. *Niech A będzie niepustym zbiorem, $a \in A$, oraz niech $h : A \to A$ będzie funkcją. Wtedy istnieje dokładnie jedna funkcja*

$$f : \mathbb{N} \to A$$

taka, że

- $f(0) = a$
- $f(n') = h(f(n))$.

Dowód. Wykorzystamy zasadę indukcji. Niech

$$P = \{n \in \mathbb{N} : f(n) \text{ jest jednoznacznie zdefiniowane}\}.$$

Sprawdzamy warunki zasady indukcji. Oczywiście $P \subset \mathbb{N}$ i $0 \in P$. Jeśli $n \in P$, to znaczy, że $f(n)$ jest jednoznacznie zdefiniowane, ale w takim razie $f(n') = h(f(n))$ też jest zdefiniowane, czyli $n' \in P$. Zatem, z zasady indukcji, $P = \mathbb{N}$, czyli funkcja f jest jednoznacznie zdefiniowana dla wszystkich liczb naturalnych. □

Podobnie można wykazać następujące twierdzenie:

Twierdzenie 15.19. *Niech A będzie niepustym zbiorem, $a, b \in A$, oraz niech $h : A \times A \to A$ będzie funkcją. Wtedy istnieje dokładnie jedna funkcja*

$$f : \mathbb{N} \to A$$

taka, że

- $f(0) = a$
- $f(1) = b$

- $f((n')') = h(f(n'), f(n))$.

Przykład 15.20 (Ciąg Fibonacciego)**.** Niech $A = \mathbb{N}$, $a = b = 1$ i $h(m, n) = m + n$. Z powyższego twierdzenia wiemy, że istnieje dokładnie jedna funkcja $f : \mathbb{N} \to \mathbb{N}$ taka, że $f(0) = f(1) = 1$ oraz $f(n + 2) = h(f(n + 1), f(n)) = f(n + 1) + f(n)$. Ta funkcja, zwana *wzorem Bineta*, pozwala w sposób jawny zapisać rekurencyjnie zadany ciąg Fibonacciego. Czytelnik na ćwiczeniach z algebry liniowej wykaże być może, że

$$f(n) = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^{n+1} + \left(\frac{1 - \sqrt{5}}{2} \right)^{n+1} \right).$$

Uwaga 15.21. O rozszerzeniu zasady indukcji na zbiory dobrze uporządkowane, czyli o zasadzie indukcji pozaskończonej, zainteresowany czytelnik może poczytać na przykład w [4].

Bibliografia

[1] Dubois, D., Prade, H.: *Fundamentals of Fuzzy Sets*, Springer, New York 2000.

[2] Gelfond, A.: *Transcendental and Algebraic Numbers*, Courier Dover Publications, 2015.

[3] Grell B.: *Wstęp do matematyki*, `https://im.uj.edu.pl/studia/md/doskonaly-uniwersytet`, 2020.

[4] Guzicki W., Zakrzewski, P.: *Wykłady ze wstępu do matematyki*, PWN, Warszawa 2005

[5] Kozik, J., Kozik, M., Zaionc, M.: *Logika i teoria mnogości*, `http://wazniak.mimuw.edu.pl/index.php?title=Logika_i_teoria_mnogości`, dostęp 2020.05.03

[6] Kraszewski, J.: *Wstęp do matematyki*, WNT PWN 2020.

[7] Kuratowski, K.: *Wstęp do teorii mnogości i topologii*, PWN, Warszawa 1980.

[8] Marek, W., Onyszkiewicz, J.: *Elementy logiki i teorii mnogości w zadaniach*, PWN, Warszawa 1978.

[9] Sierpiński, W.: *Cardinal and ordinal numbers*, PWN, Warszawa 1965.

[10] Tarski, A.: *Sur les ensembles finis*, Fundamenta Mathematicae, **6** (1924), 45–95.

[11] Wójtowicz, K.: *O hipotezie continuum*, Zagadnienia Filozoficzne w Nauce, **12**, 1998, str. 35–52.

Indeks

A
aksjomat
  nieskończoności, 59
  wyboru, 12
aksjomaty teorii mnogości, 11, 12
alternatywa, 4
  rozłączna, 4
antynomia Russela, 12

B
bijekcja, 24

C
ciąg, 22
  Fibonacciego, 63
część wspólna zbiorów, 9

D
diagram Venna, 10
dziedzina relacji, 19

E
element
  maksymalny relacji, 32
  minimalny relacji, 33
  najmniejszy relacji, 33
  największy relacji, 33
  wyróżniony, 32

F
formuła zdaniowa, 3, 5
funkcja, 21
  identycznościowa, 24
  przedłużenie, 26
  restrykcja, zacieśnienie, 26
  zdaniowa jednej zmiennej, 7
  zestawienie, 26
  zgodna z relacją, 31
  złożenie, 23
funkcje
  iloczyn kartezjański, 26
funktor zdaniotwórczy, 7

H
hipoteza continuum, 46

I
iloczyn
  zbiorów, 9
iloczyn kartezjański, 15, 18
  funkcji, 26
  uogólniony, 18
implikacja, 4
infimum zbioru, 34
injekcja, 23

K
klasa abstrakcji, 29
koniunkcja, 3
konstrukcja liczb naturalnych, 59
kres zbioru
  dolny, 34
  górny, 34
kwantyfikator, 7
  duży, ogólny, uniwersalny, 7
  mały, szczegółowy, egzystencjalny, 7

L
lemat
  Kuratowskiego–Zorna, 49, 52
liczba
  algebraiczna, 41
  kardynalna, 45
  naturalna, 59
  niealgebraiczna, przestępna, 41
  wymierna, 41

Ł
łańcuch, 35

M
majoranta zbioru, 34
minoranta zbioru, 34
moc
  $\aleph_0$, 38
  continuum, 44
  zbioru, 45

N
negacja, 3

O
obraz zbioru przez funkcję, 27

odcinek początkowy, 36
    domknięty, 36

P
para uporządkowana, 14
pewnik wyboru, **12**, 49, 52, 55
podobieństwo zbiorów liniowo uporządkowanych, 36
podział zbioru, 30
pojęcie pierwotne, 9
pokrycie zbioru, 29
porządek
    dobry, 35
    gęsty, 35
    leksykograficzny, 32
    liniowy, 35
    zgodny z funkcją, 36
prawa de Morgana
    dla kwantyfikatorów, 8
    dla rodziny indeksowanej, 14
    dla zbiorów, 11
    dla zdań, 6
projekcja, 23
przecięcie
    rodziny zbiorów, 13
    zbiorów, 9
przeciwdziedzina relacji, 19
przeciwobraz zbioru przez funkcję, 27
przedłużenie funkcji, 26

R
reguły wnioskowania, 8
relacja, 18
    antysymetryczna, 20
    dobrego porządku, 35
    dziedzina, 19
    gęstego porządku, 35
    liniowego porządku, 35
    m-argumentowa, 18
    odwrotna, 19
    porządku (częściowego), 32
      element maksymalny, 32
      element minimalny, 33
      element najmniejszy, 33
      element największy, 33
    przechodnia, 20
    przeciwdziedzina, 19
    przeciwzwrotna, 20
    równoważności, 29
      klasa abstrakcji, 29
      zbiór ilorazowy, 31
    słabo antysymetryczna, 20
    spójna, 20
    symetryczna, 20
    złożenie, 19
    zwrotna, 20
restrykcja funkcji, 26
rodzina
    induktywna, 59
    zbiorów
      indeksowana, 13
rodzina zbiorów, 13
równoliczność, 37
równość zbiorów, 9
równoważność, 4
różnica zbiorów, 9
rzutowanie, 23

S
spójnik
    logiczny, 3
      n-argumentowy, 4
    zdaniotwórczy, 3
suma
    rodziny zbiorów, 13
    zbiorów, 9
supremum zbioru, 34
surjekcja, 23

T
tautologia, 5
teza twierdzenia, 8
twierdzenie
    Cantora, 45
    Cantora–Bernsteina, 47
    Zermelo, 36, 55, **56**
typ porządkowy, 36

U
uzupełnienie zbioru, 11

W
wartość logiczna, 3
wzór Bineta, 63

Z
zacieśnienie funkcji, 26
założenie twierdzenia, 8
zaprzeczenie, 3
zasada
    indukcji, 60
    minimum, 62
zawieranie zbiorów, 9
zbiory
    iloczyn kartezjański, 15
    iloczyn, przecięcie, część wspólna, 9
    równoliczne, 37
    równość, 9
    różnica, 9
    suma, 9
    zawieranie, 9
zbiór, 9, 37
    co najwyżej przeliczalny, 38
    częściowo uporządkowany, 32

ilorazowy relacji, 31
induktywny, 59
infimum, 34
kres
  dolny, 34
  górny, 34
liczb naturalnych, 59, 60
majoranta, 34
minoranta, 34
nieprzeliczalny, 43
podział, 30
pokrycie, 29
przeliczalny, 38
pusty, 9, 11
skończony, 37
  supremum, 34
  uporządkowany
    dobrze, 35
    gęsto, 35
    liniowo, 35
    liniowo, podobieństwo, 36
    liniowo, typ porządkowy, 36
  uzupełnienie, 11
zdanie logiczne, 3
zestawienie funkcji, 26
złożenie
  funkcji, 23
  relacji, 19
zmienna zdaniowa, 3