WSTĘP DO LOGIKI I TEORII MNOGOŚCI

Marek Bienias Szymon Głąb

Instytut Matematyki, Politechnika Łódzka

Łódź 2022

Marek Bienias

Szymon Głąb

Wstęp do logiki i teorii mnogości

Instytut Matematyki, Politechnika Łódzka

Łódź, 2022

Recenzenci:

Dr hab. Szymon Żeberski, prof. Politechniki Wrocławskiej

Dr hab. Jacek Hejduk, prof. Uniwersytetu Łódzkiego

2022 ISBN 978-83-66741-02-7

DOI: 10.34658/9788366741027

Wydawnictwo Politechniki Łódzkiej
93-005 Łódź, ul. Wólczańska 223
Tel. 42-631-20-87, 42-631-29-52
E-mail: zamowienia@info.p.lodz.pl
www.wydawnictwo.p.lodz.pl

Podręczniki i Skrypty Politechniki Łódzkiej, Nr 2359

Publikacja elektroniczna

Spis treści

ROZDZIAŁ 1

Formalizm matematyczny i metoda indukcji

Celem głównym wykładu *Wstęp do logiki i teorii mnogości* jest zapoznanie słuchaczy z **formalizmem matematycznym** i uświadomienie im konieczności jego stosowania.

1. Podstawowe oznaczenia

Stosujemy konwencję definiowania zbiorów przez wypisywanie elementów zbioru pomiędzy dwoma nawiasami klamrowymi „{" i „}". Dla przykładu: $\{3, 5, 12\}$ to zbiór zawierający elementy 3, 5 oraz 12 i żadnych innych. Gdy nie chcemy lub nie możemy wypisać wszystkich elementów zbioru, to użyteczna jest konwencja wielokropka, np. $\{2, 4, 8, ..., 2^{20}\}$ lub $\{2, 4, 6, 8, ...\}$ czy nawet $\{..., -4, -2, 0, 2, 4, ...\}$. Konwencja wielokropka działa, o ile wzorzec wypisywania kolejnych elementów jest jasny. Dla przykładu rozważmy zbiór $\{3, 5, 33, 35, 53, 55, ...\}$. Nie jest zupełnie jasne, jaki element powinien nastąpić po 55. Być może domyślacie się, że chodziło nam o wszystkie liczby naturalne, które w zapisie dziesiętnym mają tylko cyfry 3 i 5. Lepszy jest następujący zapis niepozostawiający miejsca na domysły:

$$\{x : x \text{ jest liczbą naturalną, która w zapisie dziesiętnym ma tylko cyfry 3 i 5}\}.$$

Stosujemy więc kolejną konwencję definiowania zbiorów: zbiór $\{x : W(x)\}$ składa się ze wszystkich elementów x, które mają własność W. Dla przykładu $\{x \in \mathbb{N} : x \text{ jest podzielna przez } 2\}$ czytamy: zbiór liczb $x \in \mathbb{N}$ takich, że x jest podzielna przez 2. Czasami wygodnie jest stosować inną konwencję: zbiór $\{f(x) : x \in X\}$ to zbiór wszystkich elementów postaci $f(x)$ dla $x \in X$, gdzie f to odwzorowanie określone na X. Zapis $\{3n + 1 : n \in \mathbb{Z}\}$ czytamy: zbiór liczb postaci $3n + 1$ takich, że $n \in \mathbb{Z}$.

W trakcie wykładu będziemy posługiwali się następującymi, często dobrze znanymi czytelnikom, symbolami:

- $\mathbb{N} = \{1, 2, 3, ...\}$ – zbiór liczb naturalnych
- $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ – zbiór liczb całkowitych
- $\mathbb{Q}$ – zbiór liczb wymiernych, tj. wszystkich ułamków postaci $\frac{p}{q}$, gdzie p jest liczbą całkowitą, zaś q liczbą naturalną
- $\mathbb{R}$ – zbiór liczb rzeczywistych.

2. Elementy formalnej teorii matematycznej

W języku matematycznym, podobnie jak w każdym innym języku, mamy do czynienia ze zdaniami, które zawierają pewną treść.

Przykłady zdań matematycznych:

1. **Definicje** – sformułowania, które nadają nazwy pewnym obiektom.

- ***Powiemy, że*** *liczba naturalna n jest podzielna przez liczbę naturalną $k \leq n$, gdy istnieje liczba naturalna l taka, że $n = k \cdot l$.*
- *Liczbę naturalną podzielną przez 2* ***nazywamy*** *liczbą parzystą.*
- *Czworokąt o co najmniej jednej parze boków równoległych* ***nazywamy*** *trapezem.*
- ***Mówimy, że*** *liczba naturalna jest liczbą pierwszą, jeśli ma dokładnie dwa różne dzielniki.*

Słowa kluczowe: *„nazywamy", „mówimy, że", „powiemy, że".*

2. **Aksjomaty** – zdania, których prawdziwość przyjmujemy na zasadzie umowy.

- *Każda liczba naturalna n ma swój następnik $n + 1$, który jest też liczbą naturalną;*
- *Dwa zbiory są równe jedynie wtedy, kiedy mają te same elementy.*

3. **Twierdzenia** – zdania, których prawdziwość należy udowodnić przeprowadzając odpowiednie rozumowanie/wnioskowanie (tzw. dowód). Dowody rozpoczynamy słowem „Dowód", a kończymy znakiem □.

- *Jeśli liczba naturalna jest podzielna przez 4, to jest podzielna przez 2;* (twierdzenie prawdziwe)
- *Każda liczba naturalna jest parzysta.* (twierdzenie fałszywe)

Z reguły konstrukcja: *jeśli ... to ...*

Twierdzenie to zdanie, które ma zawsze **jednoznacznie** określoną wartość logiczną, jest albo **prawdziwe** (symbolicznie nadajemy mu wartość logiczną 1) albo **fałszywe** (wartość logiczną 0).

3. Aksjomatyka Peana liczb naturalnych

Konstrukcje liczb mają charakter hierarchiczny – od prostszych do coraz bardziej złożonych. Mając liczby naturalne $\mathbb{N}$, konstruuje się liczby całkowite $\mathbb{Z}$, dodając dla każdej liczby naturalnej $n \in \mathbb{N}$ liczbę do niej przeciwną $-n$ oraz 0. Dalej konstruujemy liczby wymierne $\mathbb{Q}$ jako ułamki $\frac{n}{m}$, gdzie $n \in \mathbb{Z}$, $m \in \mathbb{N}$. Liczby rzeczywiste $\mathbb{R}$ definiujemy jako ciągi przybliżeń liczbami wymiernymi, np. liczbę $\sqrt{2} = 1{,}414213562373095...$ można przybliżać ciągiem liczb wymiernych $(1; 1{,}4; 1{,}41; 1{,}414; 1{,}1412; ...)$ [1].

[1] Przedstawiamy tu tylko idee konstrukcji liczb $\mathbb{Z}, \mathbb{Q}$ i $\mathbb{R}$, które można precyzyjnie sformalizować.

A co z liczbami naturalnymi? Czy one także mogą być skonstruowane z bardziej elementarnych składników? Czy potrafilibyśmy powiedzieć, czym są liczby naturalne i jakie mają własności bez używania pojęcia liczby?

Przedstawimy taką konstrukcję, opracowaną przez Giuseppe Peana[2]. Co to znaczy być liczbą, zostaje uchwycone za pomocą pięciu aksjomatów – pięciu podstawowych prawd o liczbach naturalnych. Uchwycone w tych prawdach zostały własności, które powodują, że $\mathbb{N} = \{1, 2, 3, ...\}$ jest zbiorem liczb naturalnych.

Aksjomat 1. $\blacksquare \in N$

Obiekt $\blacksquare$ symbolizuje pierwszą najmniejszą liczbę. Piszemy $\blacksquare$ zamiast 1, bo nie chcemy używać liczb do definiowania liczb. Poza tym interesują nas własności obiektów, a nie to, czym one są.

Aksjomat 2. Jeśli $x \in N$, to $S(x) \in N$; innymi słowy S jest funkcją działającą z N w N.

Drugi aksjomat wprowadza pojęcie następnika – $S(x)$ to kolejny obiekt po x. Zauważmy jednak, że stwierdzenie $S(\blacksquare) = \blacksquare$ nie przeczy aksjomatom 1 i 2. Następnikiem $\blacksquare$ nie powinno być $\blacksquare$. Potrzebujemy, więc kolejny aksjomat.

Aksjomat 3. $\blacksquare$ nie jest następnikiem żadnego obiektu z N.

Używając aksjomatów 1, 2 i 3 wiemy, że $\blacksquare$ i $S(\blacksquare)$ to dwa różne obiekty. Jednak zdanie $S(S(\blacksquare)) = S(\blacksquare)$ nie przeczy żadnemu z dotychczasowych aksjomatów.

Aksjomat 4. Jeśli $S(x) = S(y)$, to $x = y$; innymi słowy S jest funkcją różnowartościową.

Aksjomaty 1–4 implikują istnienie nieskończonego ciągu $\blacksquare, S(\blacksquare), S(S(\blacksquare)), S(S(S(\blacksquare))), ...$ parami różnych obiektów. Dla skrócenia zapisu oznaczmy te obiekty następująco: $\blacksquare$ to 1, $S(\blacksquare)$ to 2, $S(S(\blacksquare))$ to 3, $S(S(S(\blacksquare)))$ to 4, itd. Zauważmy, że jeśli do zbioru $\{1, 2, 3, 4, ...\}$ dołożymy dwa elementy $\heartsuit$ and $\spadesuit$ i zdefiniujemy $S(\heartsuit) = \spadesuit$ oraz $S(\spadesuit) = \heartsuit$, to dla zbioru $\{1, 2, 3, 4, ...\} \cup \{\heartsuit, \spadesuit\}$ będą spełnione aksjomaty 1–4. Aby uniknąć takiej sytuacji, potrzebny jest kolejny aksjomat.

Aksjomat 5. Jeśli X jest podzbiorem zbioru N takim, że:

- $\blacksquare \in X$,
- dla każdego $x \in N$: jeśli $x \in X$ to $S(x) \in X$,

to $X = N$.

Zauważmy, że $N = \{1, 2, 3, 4, ...\} \cup \{\heartsuit, \spadesuit\}$ nie spełnia aksjomatu 5. Jeśli weźmiemy $X = \{1, 2, 3, 4, ...\}$, to $\blacksquare \in X$ oraz dla każdego $x \in N$ zachodzi implikacja: jeśli $x \in X$ to $S(x) \in X$. Ale $X \neq N$. Aksjomat 5, zwany zasadą indukcji, mówi o tym, że N musi być minimalnym zbiorem spełniającym aksjomaty 1–4, to znaczy poza łańcuchem $\blacksquare, S(\blacksquare), S(S(\blacksquare)), S(S(S(\blacksquare))), ...$ nie zawiera już nic innego.

---

[2] Giuseppe Peano, 1858–1932.

Trójkę $(N, S, \blacksquare)$ spełniającą aksjomaty Peana nazywamy zbiorem liczb naturalnych i oznaczamy symbolem $\mathbb{N}$.

Bazując na powyższej aksjomatyce, możemy również zdefiniować naturalne działania: dodawania i mnożenia oraz naturalny porządek w zbiorze $\mathbb{N}$.

Definicja 1.1. *Dla dowolnych $n, m \in \mathbb{N}$ definiujemy:*

- $n + 1 = S(n)$ *oraz* $n + S(m) = S(n + m)$
- $n \cdot 1 = n$ *oraz* $n \cdot S(m) = n \cdot m + n$
- $n \leq m$, *jeśli* $n = m$ *lub istnieje* $k \in \mathbb{N}$ *takie, że* $m = n + k$.

Stwierdzenie 1.2. $4 + 3 = 7$.

Dowód. Wykorzystujemy pierwszą część definicji dodawania dla $n = 4$:

$$4 + 1 = S(4) = 5.$$

Następnie z części drugiej definicji dodawania, mamy:

$$4 + 2 = 4 + S(1) = S(4 + 1) = S(5) = 6.$$

W końcu:

$$4 + 3 = 4 + S(2) = S(4 + 2) = S(6) = 7.$$

□

Stwierdzenie 1.3. *Dla $n \in \mathbb{N}$ mamy $n + 1 = 1 + n$.*

Dowód. Niech $X = \{n \in \mathbb{N} \colon n + 1 = 1 + n\}$. Wykorzystując $(A5)$ pokażemy, że $X = \mathbb{N}$.
Krok 1.: Zauważmy, że dla $n = 1$ mamy:

$$1 + 1 = 1 + 1.$$

Stąd $1 \in X$.
Krok 2.: Niech $n_0 \in \mathbb{N}$ i załóżmy, że $n_0 \in X$. Pokażemy, że $S(n_0) \in X$. Mamy:

$$1 + S(n_0) \overset{def+}{=} S(1 + n_0) \overset{n_0 \in X}{=} S(n_0 + 1) = S(S(n_0)) = S(n_0) + 1.$$

Stąd $S(n_0) \in X$.
Podsumowanie: Wobec $(A5)$ $X = \mathbb{N}$, co należało pokazać. □

W podobny sposób można udowodnić następujące twierdzenia:

TWIERDZENIE 1.4 (przemienność dodawania liczb naturalnych). *Dla $n, m \in \mathbb{N}$ mamy $n+m = m+n$.*

TWIERDZENIE 1.5 (przemienność mnożenia liczb naturalnych). *Dla $n, m \in \mathbb{N}$ mamy $n \cdot m = m \cdot n$.*

czy też twierdzenia o łączności dodawania/mnożenia, rozdzielności mnożenia względem dodawania itd.

4. Indukcja matematyczna

Zanim przejdziemy do Zasady indukcji matematycznej[3], potrzebujemy następującej definicji. Funkcją zdaniową nazwiemy formułę $W(n)$, która po wstawieniu konkretnego $n \in \mathbb{N}$ staje się zdaniem prawdziwym albo fałszywym.

W aksjomatyce Peana liczb naturalnych pojawia się aksjomat (zdanie, którego prawdziwość przyjmujemy) $(A5)$ – tzw. *zasada indukcji matematycznej.*

AKSJOMAT (zasada indukcji). *Jeśli $W(n)$ jest funkcją zdaniową zmiennej $n \in \mathbb{N}$ taką, że:*

- *$W(1)$ zachodzi, tj. jest zdaniem prawdziwym*
- *dla dowolnej liczby $n_0 \in \mathbb{N}$, jeśli $W(n_0)$ zachodzi, to $W(n_0+1)$ zachodzi,*

to $W(n)$ jest prawdziwe dla wszystkich liczb naturalnych n.

Zasada indukcji matematycznej ma następującą interpretację: *wyobraźmy sobie nieskończony rząd kostek domina – każda ponumerowana kolejną liczbą naturalną. Przyjmijmy, że zachodzenie $W(n)$, dla $n \in \mathbb{N}$, oznacza, że n-ta kostka przewraca się. Niniejszym założenie:*

- *„$W(1)$ zachodzi", oznacza, że pierwsza kostka przewraca się*
- *„dla dowolnej liczby $n_0 \in \mathbb{N}$, jeśli $W(n_0)$ zachodzi, to $W(n_0+1)$ zachodzi", oznacza, że każda kostka, jeśli się przewraca, to przewraca też następną.*

W powyższej sytuacji każda kostka się przewraca, gdyż przewraca się pierwsza i pociąga za sobą drugą itd. Ostatecznie tezą zasady indukcji matematycznej jest, że wszystkie kostki się przewracają, tj. własność $W(n)$ mają wszystkie liczby naturalne n.

Zasadę indukcji stosuje się przede wszystkim w dowodach twierdzeń o własnościach, równościach, nierównościach przysługujących kolejnym liczbom naturalnym. Poniżej podamy dwa przykłady zastosowania Zasady indukcji matematycznej.

---

[3] W logice indukcja to wnioskowanie „od szczegółu do ogółu". Przykładem rozumowania indukcyjnego jest: *Wszystkie odkryte dotąd formy życia nie mogą istnieć bez wody w stanie ciekłym. Dlatego prawdopodobnie żadna forma życia nie może istnieć bez wody w stanie ciekłym.* Jak widać, w naukach przyrodniczych, rozumowanie indukcyjne nie musi być niezawodne. Dedukcja natomiast to dochodzenie do wniosku z założonego zbioru przesłanek. Termin *indukcja matematyczna* wziął się od indukcji zupełnej, czyli rozumowania, które bierze pod uwagę wszystkie możliwe wystąpienia. W praktyce nie jest możliwe przebadanie wszystkich obiektów, np. wszystkich form życia. Aby przeprowadzić rozumowanie oparte na indukcji zupełnej, należy początkowo przyjąć pewne założenia dotyczące wszystkich badanych obiektów, a potem dopiero wyciągnąć wnioski. Jak zatem widać indukcja zupełna to ukryte rozumowanie dedukcyjne. W szczególności indukcja matematyczna, to rodzaj rozumowania dedukcyjnego. Co więcej, matematyka w całości jest nauką dedukcyjną.

TWIERDZENIE 1.6. *Dla dowolnej liczby naturalnej $n \in \mathbb{N}$ zachodzi równość:*

$$(\star) \qquad 1 + 2 + ... + n = \frac{n(n+1)}{2}.$$

DOWÓD. Dla liczby naturalnej $n \in \mathbb{N}$ niech $W(n)$ oznacza równość opisaną $(\star)$. Wykażemy, że założenia zasady indukcji matematycznej są spełnione.
Krok 1.: Zauważmy, że dla $n = 1$ w $(\star)$ mamy: $L = 1$ oraz $P = \frac{1\cdot 2}{2} = 1$ zatem $(\star)$ dla $n = 1$ zachodzi, tj. $W(1)$ zachodzi.
Krok 2.: Niech $n_0 \in \mathbb{N}$ i załóżmy, że $W(n_0)$ zachodzi. Pokażemy, że zachodzi $W(n_0 + 1)$. Zachodzenie $W(n_0)$ oznacza, że zdanie $(\star)$ jest prawdziwe dla $n = n_0$. Należy wykazać, że $(\star)$ zachodzi także dla $n = n_0 + 1$. Mamy:

$$L = 1 + 2 + ... + (n_0 + 1) = 1 + 2 + ... + n_0 + (n_0 + 1) \overset{W(n_0)}{=} \frac{n_0(n_0+1)}{2} + (n_0 + 1) =$$

$$= \frac{n_0(n_0+1) + 2(n_0+1)}{2} = \frac{(n_0+1)(n_0+2)}{2} = P$$

co oznacza, że zachodzi $W(n_0 + 1)$.
Podsumowanie: Na mocy zasady indukcji matematycznej, równość $(\star)$ jest prawdziwa dla każdego $n \in \mathbb{N}$. □

TWIERDZENIE 1.7. *Dla dowolnej liczby naturalnej $n \in \mathbb{N}$, liczba $n^3 + 5n$ jest podzielna przez* 6.

DOWÓD. Dla liczby naturalnej $n \in \mathbb{N}$ przyjmijmy, że $W(n)$ oznacza, że liczba n^3+5n jest podzielna przez 6. Wykażemy, że założenia zasady indukcji matematycznej są spełnione.
Krok 1.: Zauważmy, że dla $n = 1$ liczba $n^3 + 5n = 6$ jest podzielna przez 6, tj. $W(1)$ zachodzi.
Krok 2.: Niech $n_0 \in \mathbb{N}$ i załóżmy, że $W(n_0)$ zachodzi. Pokażemy, że zachodzi $W(n_0 + 1)$. Zachodzenie $W(n_0)$ oznacza, że liczba $n_0^3 + 5n_0$ jest podzielna przez 6, tj. $n_0^3 + 5n_0 = 6k$ dla pewnego $k \in \mathbb{Z}$. Należy wykazać, że liczba $(n_0 + 1)^3 + 5(n_0 + 1)$ jest podzielna przez 6. Mamy:

$$(n_0 + 1)^3 + 5(n_0 + 1) = n_0^3 + 3n_0^2 + 3n_0 + 1 + 5n_0 + 5 =$$

$$= (n_0^3 + 5n_0) + 3n_0(n_0 + 1) + 6 \overset{W(n_0)}{=} 6k + 3n_0(n_0 + 1) + 6.$$

Zauważmy, że liczba $n_0(n_0 + 1)$ jest parzysta jako iloczyn dwóch kolejnych liczb naturalnych. Zatem liczba $3n_0(n_0 + 1)$ jest podzielna przez 6. Stąd $(n_0 + 1)^3 + 5(n_0 + 1)$ jest też podzielna przez 6 jako suma liczba podzielnych przez 6. To oznacza, że zachodzi $W(n_0 + 1)$.
Podsumowanie: Na mocy zasady indukcji matematycznej, dla każdego $n \in \mathbb{N}$ liczba $n^3 + 5n$ jest podzielna przez 6. □

Czasami zasada indukcji w przedstawionej formie nie jest wystarczająca. Aby to zilustrować rozważmy następujący przykład.

PRZYKŁAD 1.8. Każda liczba naturalna $n > 1$ jest iloczynem skończenie wielu liczb pierwszych.

Aby wykazać to twierdzenie, wprowadźmy oznaczenie: $W(n)$ oznacza, że $n = 1$ lub n jest liczbą pierwszą, lub n jest iloczynem skończenie wielu liczb pierwszych. Wówczas $W(1)$ zachodzi.

Zastanówmy się jak z faktu, że $W(n)$ zachodzi wywnioskować, że zachodzi $W(n+1)$. Rozważmy przykład: $W(663)$ zachodzi, bo $663 = 3 \cdot 13 \cdot 17$, a $W(664)$ zachodzi, bo $664 = 2 \cdot 2 \cdot 2 \cdot 83$. Jak z faktu, że zachodzi $W(663)$, wywnioskować, że zachodzi $W(664)$? Trudna sprawa. Zauważmy jednak, że 664 to iloczyn $2 \cdot 332$. Gdybyśmy wiedzieli, że $W(2)$ i $W(332)$ zachodzą, to mielibyśmy, że $W(2 \cdot 332)$ też zachodzi.

Nie da się tego zrobić, używając jedynie Aksjomatu indukcji. Potrzebujemy silniejszego narzędzia.

TWIERDZENIE 1.9 (zasada indukcji zupełnej). *Jeśli $W(n)$ jest funkcją zdaniową zmiennej $n \in \mathbb{N}$ taką, że:*

- *$W(1)$ zachodzi*
- *dla dowolnej liczby $n_0 \in \mathbb{N}$, jeśli $W(k)$ zachodzi dla $k \leq n_0$, to $W(n_0 + 1)$ zachodzi,*

to $W(n)$ jest prawdziwe dla wszystkich liczb naturalnych n.

Wróćmy do Przykładu 1.8. $W(1)$ zachodzi wprost z definicji funkcji zdaniowej $W(n)$. Niech n_0 oraz załóżmy, że $W(k)$, zachodzi dla wszystkich $k \leq n_0$. Mamy dwie możliwości. Liczba $n_0 + 1$ może być liczbą pierwszą. Wówczas $W(n_0 + 1)$ zachodzi wprost z definicji funkcji zdaniowej $W(n)$. Liczba $n_0 + 1$ może być liczbą złożoną. Wówczas istnieją liczby naturalne $m, l > 1$ takie, że $n_0 + 1 = m \cdot l$. Wtedy $m, l < n_0 + 1$, a w konsekwencji $m, l \leq n_0$. Zatem z założenia $W(m)$ i $W(l)$ zachodzą. To oznacza, że zarówno m jak i l jest albo liczbą pierwszą, albo iloczynem skończenie wielu liczb pierwszych. Stąd $m \cdot l$ jest iloczynem skończenie wielu liczb pierwszych. Zatem $W(n_0 + 1)$ zachodzi. Wykażemy teraz twierdzenie 1.9.

DOWÓD. Niech $W(n)$ będzie funkcją zdaniową zmiennej $n \in \mathbb{N}$ spełniającą założenia Twierdzenia 1.9. Niech $\varphi(n)$ będzie funkcją zdaniową taką, że zdanie $\varphi(n)$ zachodzi, gdy zachodzą jednocześnie zdania $W(1), W(2), ..., W(n)$. Symbolicznie $\varphi(n)$ to $W(1) \wedge W(2) \wedge ... \wedge W(n)$. Wówczas to, że $W(1)$ zachodzi, oznacza, że $\varphi(1)$ zachodzi. Ponadto fakt, że $W(k)$ zachodzi dla $k \leq n_0$, oznacza, że $\varphi(n_0)$ zachodzi. Zatem:

- $W(1)$ zachodzi
- dla dowolnej liczby $n_0 \in \mathbb{N}$, jeśli $W(k)$ zachodzi dla $k \leq n_0$, to $W(n_0 + 1)$ zachodzi.

oznacza, że:

- $\varphi(1)$ zachodzi
- dla dowolnej liczby $n_0 \in \mathbb{N}$, jeśli $\varphi(n_0)$, to $W(n_0+1)$ zachodzi.

Zauważmy, że jeśli $\varphi(n_0)$ i $W(n_0+1)$ zachodzą, to $\varphi(n_0+1)$ zachodzi. Stąd otrzymujemy:

- $\varphi(1)$ zachodzi
- dla dowolnej liczby $n_0 \in \mathbb{N}$, jeśli $\varphi(n_0)$, to $\varphi(n_0+1)$ zachodzi.

Teraz na mocy Zasady indukcji otrzymujemy, że $\varphi(n)$ zachodzi dla każdego $n \in \mathbb{N}$. Stąd $W(n)$ zachodzi dla każdego $n \in \mathbb{N}$. □

5. Przykłady błędnych rozumowań indukcyjnych

Przeprowadzimy teraz dwa niepoprawne rozumowania indukcyjne. Pokaże to, jakich błędów należy unikać. W dowodach indukcyjnych nie można pomijać ani kroku pierwszego, ani drugiego.

Przykład 1.10. Każda liczba postaci $2n+1$ jest parzysta.

Niech $W(n)$ oznacza, że liczba postaci $2n+1$ jest parzysta. Niech n_0 będzie liczbą naturalną taką, że zachodzi $W(n_0)$, czyli, że liczba $2n_0+1 = 2k$ dla pewnego $k \in \mathbb{N}$. Wtedy:

$$2(n_0+1)+1 = 2n_0+2+1 = 2k+2 = 2(k+1),$$

co oznacza, że $W(n_0+1)$ zachodzi. Zatem $W(n)$ zachodzi dla dowolnego $n \in \mathbb{N}$.

Błąd rozumowania polega na tym, że nie został sprawdzony warunek $W(1)$.

Przykład 1.11. Rozważmy następujące, ewidentnie fałszywe, zdanie: *Wszystkie koty na świecie są tego samego koloru.* Aby to wykazać, wystarczy pokazać, że dla dowolnego $n \in \mathbb{N}$ prawdziwe jest zdanie $W(n)$: *każdy n-elementowy zbiór kotów składa się z kotów tego samego koloru.*

Przeprowadzimy indukcyjny dowód tego stwierdzenia. Oczywiście $W(1)$ jest prawdą. Załóżmy, że $W(n)$ zachodzi. Aby wykazać $W(n+1)$, ustalmy dowolny zbiór $n+1$-elementowy kotów $\{K_1, K_2, ..., K_n, K_{n+1}\}$. Podzielmy ten zbiór na dwa podzbiory $\{K_1, K_2, ..., K_n\}$ i $\{K_2, ..., K_n, K_{n+1}\}$. Oba te zbiory mają n-elementów. Zatem na mocy założenia indukcyjnego oba zbiory składają się z kotów o tym samym kolorze. Koty w pierwszym zbiorze mają kolor A, a w drugim kolor B. Zauważmy, że zbiory $\{K_1, K_2, ..., K_n\}$ i $\{K_2, ..., K_n, K_{n+1}\}$ mają wspólny element K_2. Ten kot ma kolor A i kolor B. Ponieważ kot może mieć tylko jeden kolor, to $A = B$. W konsekwencji wszystkie koty ze zbioru $\{K_1, K_2, ..., K_n, K_{n+1}\}$ mają ten sam kolor A.

Na czym polega problem? Krok indukcyjny nie działa dla $W(2)$, bo podzbiory 1-elementowe zbioru 2-elementowego nie muszą mieć części wspólnej.

Uwaga 1.12 (bardzo ważne wiadomości z pierwszego wykładu). Podczas pierwszego wykładu dowiedzieliśmy się m.in.:

- że formalizm matematyczny jest **ważny**
- jak mogą wyglądać zdania matematyczne i że ZAWSZE są albo prawdziwe, albo fałszywe
- czym są aksjomaty
- co to jest aksjomatyka Peana liczb naturalnych
- co to jest zasada indukcji
- jak redagować dowody indukcyjne
- jakich błędów unikać w dowodach indukcyjnych.

ROZDZIAŁ 2

Spójniki logiczne i metoda zero-jedynkowa

1. Spójniki logiczne

Zdanie logiczne może mieć wartość logiczną 1, gdy jest prawdziwe, albo wartość logiczną 0, gdy jest fałszywe. Zdania logiczne będziemy oznaczać małymi literami: $p, q, r, s, \ldots$. Zaczniemy od najprostszej definicji.

Definicja 2.1 (Negacja). *Negacją zdania p nazywamy zdanie oznaczone przez $\neg p$ o wartości logicznej określonej następująco:*

p	$\neg p$
0	1
1	0

Zdanie $\neg p$ czytamy: ***nieprawda, że*** *p, albo po prostu:* ***nie*** *p.*

W matematyce dla dowolnego zdania p dokładnie jedno spośród zdań $p, \neg p$ jest prawdziwe i dokładnie jedno fałszywe. Zaprzeczenie w języku naturalnym nie zawsze pokrywa się z negacją, np. negacja zdania *Lubię Jolę* brzmi *Nieprawda, że lubię Jolę*. Zdanie *Nie lubię Joli* nie jest tym samym co *Nieprawda, że lubię Jolę* – Jola może być mi osobą obojętną: ani ją lubię, ani nie. Negacja to nie jest przeciwieństwo, np. *kocham* i *nienawidzę*.

Przejdziemy teraz do dwuargumentowych spójników logicznych.

Definicja 2.2 (alternatywa). *Alternatywą zdań p, q nazywamy zdanie oznaczone przez $p \vee q$ o wartości logicznej określonej następująco:*

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

Zdanie $p \vee q$ czytamy: p ***lub*** *q.*

Dla dowolnych zdań p, q alternatywa $p \vee q$ jest prawdziwa, gdy **co najmniej** jedno ze zdań p, q jest prawdziwe. Innymi słowy, alternatywa $p \vee q$ jest fałszywa jedynie, gdy oba zdania p, q są fałszywe.

Definicja 2.3 (koniunkcja). *Koniunkcją zdań p, q nazywamy zdanie oznaczone przez $p \wedge q$ o wartości logicznej określonej następująco:*

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

*Zdanie $p \wedge q$ czytamy: p **i** q.*

Dla dowolnych zdań p, q koniunkcja $p \wedge q$ jest prawdziwa jedynie, gdy **oba** zdania p, q są prawdziwe.

Zanim przejdziemy do definicji kolejnego spójnika logicznego – implikacji, rozważmy dwa przykłady. Niech $\varphi(n)$ będzie zdaniem:

jeśli liczba n jest podzielna przez 4, to jest podzielna przez 2.

Widzimy, że to zdanie jest prawdziwe dla każdej liczby naturalnej n. Teraz przez $p(n)$ oznaczmy *liczba n jest podzielna przez 4*, a przez $q(n)$ oznaczmy *liczba n jest podzielna przez 2*. Wtedy $\varphi(n)$, to zdanie *jeśli $p(n)$, to $q(n)$*. Zdanie to jest prawdziwe także dla liczb, które nie są podzielne przez 4. Wtedy po prostu nie ma czego sprawdzać. Zauważmy, że:

- zdanie $p(6)$ jest fałszywe, a $q(6)$ jest prawdziwe
- zdanie $p(3)$ jest fałszywe i $q(3)$ jest fałszywe
- zdanie $p(4)$ jest prawdziwe i $q(4)$ jest prawdziwe.

Rozważmy teraz zdanie postaci *jeżeli..., to...*, które jest fałszywe. Niech $\psi(n)$ będzie zdaniem:

jeśli liczba jest podzielna przez 3, to jest parzysta.

Dlaczego jest fałszywe? Na przykład dlatego, że *9 dzieli się przez 3, ale 9 nie jest liczbą parzystą*. To pokazuje, że zdanie postaci *jeśli p, to q* jest fałszywe, gdy z prawdziwej przesłanki p wynika fałszywy wniosek q. Podsumujmy te rozważania w następnej definicji.

Definicja 2.4 (implikacja). *Implikacją o poprzedniku p i następniku q nazywamy zdanie oznaczone przez $p \Rightarrow q$ o wartości logicznej określonej następująco:*

p	q	$p \Rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

Zdanie $p \Rightarrow q$ czytamy: ***jeśli*** p ***to*** q *albo* ***z*** p ***wynika*** q.

Dla dowolnych zdań p, q implikacja $p \Rightarrow q$ jest fałszywa jedynie, gdy **poprzednik** p jest prawdziwy. zaś **następnik** q jest fałszywy.

Uwaga 2.5. Znaczna większość twierdzeń w matematyce ma postać implikacji $p \Rightarrow q$. W takim przypadku p nazywamy założeniem, zaś q tezą twierdzenia. Ponadto (gdy twierdzenie jest prawdziwe), mówimy też, że p jest warunkiem **wystarczającym** dla q, zaś q jest warunkiem **koniecznym** dla p.

Istotne w przypadku implikacji jest, że implikacja to rozumowanie – poprawna implikacja to poprawne rozumowanie.

Widać, że prawdziwość implikacji zależy od kolejności ułożenia i prawdziwości zdań p, q. Prowadzi to do poniższej definicji.

Definicja 2.6. *Implikację $q \Rightarrow p$ nazywamy implikacją odwrotną do implikacji $p \Rightarrow q$.*

Implikacje $p \Rightarrow q$ oraz $q \Rightarrow p$ mogą mieć różne wartości logiczne. Aby to dostrzec, wystarczy przeanalizować zdania p, q z poprzednich przykładów.

Definicja 2.7 (równoważność). *Równoważnością między zdaniami p, q nazywamy zdanie oznaczone przez $p \iff q$ o wartości logicznej określonej następująco:*

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

Zdanie $p \iff q$ czytamy: p ***wtedy i tylko wtedy, gdy*** q *albo p* ***jest równoważne*** q.

Przykład 2.8. Niech p będzie oznaczało zdanie *Liczba naturalna n jest podzielna przez* 4, zaś q będzie oznaczało zdanie *Liczba naturalna n jest podzielna przez* 2. Wówczas zdanie $p \iff q$ oznacza *Liczba naturalna n jest podzielna przez* 4 *wtedy i tylko wtedy, gdy jest jest podzielna przez* 2. To zdanie nie jest prawdziwe.

Dla dowolnych zdań p, q równoważność $p \iff q$ jest prawdziwa dokładnie wtedy, gdy oba zdania p, q mają taką samą wartość logiczną. Mówimy wówczas, że zdania p i q są *logicznie równoważne*, lub – krótko – *równoważne*.

Ostatnim spójnikiem, wartym uwagi w ramach spójnego wykładu jest spójnik **albo**.

Definicja 2.9 (alternatywa wykluczająca). *Alternatywą wykluczającą między zdaniami p, q nazywamy zdanie oznaczone przez $p \underline{\vee} q$ o wartości logicznej określonej następująco:*

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

Zdanie $p \underline{\vee} q$ czytamy: p ***albo*** *q.*

W matematyce często posługujemy się konwencjami, inaczej – umowami. Dla przykładu wartość wyrażenia $a+b\cdot c$ liczmy: najpierw mnożąc b i c, a następnie do otrzymanego wyniku dodając a. Wynika to z konwencji wykonywania w pierwszej kolejności mnożenia. W rachunku zdań przyjmujemy konwencję, że negacja ma pierwszeństwo przed każdym innym spójnikiem. Ważnym elementem rachunku zdań są nawiasy, które określają kolejność rozpatrywania spójników. Dla przykładu – zdania $(p \vee q) \wedge r$ i $p \vee (q \wedge r)$ nie są równoważne. Zatem zdanie $p \vee q \wedge r$ rodzi wątpliwości, jak je rozumieć. Aby tego uniknąć, należy wstawiać nawiasy w sposób niebudzący wątpliwości co do kolejności wykonywanych działań. Każdy zapis zawierający zmienne logiczne $p_1, p_2, ..., p_n$, spójniki logiczne oraz nawiasy pozwalające wyliczyć jego wartość logiczną w kolejności niepozostawiającej wątpliwości nazywamy *schematem zdania logicznego zmiennych $p_1, ..., p_n$.*

2. Tautologie i metoda zero-jedynkowa

Rozważmy następujący przykład:

Przykład 2.10. Przeanalizujmy wartość logiczną schematu zdania $p \vee \neg p$. Zauważmy, że mamy możliwości:

p	$\neg p$	$p \vee \neg p$
1	0	1
0	1	1

Powyższa tabela oznacza, że niezależnie od wartości logicznej zdania p (zmiennej zdaniowej) zdanie $p \vee \neg p$ jest zdaniem prawdziwym.

Zdanie logiczne, którego wartość logiczna niezależnie od wartości logicznych zmiennych pojawiających się w tym zdaniu jest zawsze równa 1, jest na pewno interesujące – można nazwać je prawem logicznym albo **tautologią**. Formalizując powyższe:

DEFINICJA 2.11. *Zdanie logiczne nazywamy* ***tautologią*** *lub* ***prawem logicznym****, jeśli niezależnie od wartości logicznych zmiennych zdaniowych wchodzących w jego skład, ma ono wartość logiczną równą* 1. *Innymi słowy: jest zdaniem zawsze prawdziwym.*

Przykład 2.10 pokazuje, że zdanie $p \vee \neg p$ jest tautologią. Co więcej, wstawiając w miejsce p dowolny schemat φ zmiennych $p_1, ..., p_n$, otrzymamy zdanie $\phi \vee \neg\varphi$, które jest prawdziwe niezależnie od wartości logicznych zdań $p_1, ..., p_n$, czyli także jest tautologią. Np. $(p_1 \vee p_2) \vee \neg(p_1 \vee p_2)$ jest tautologią. Obserwację tę można uogólnić następująco:

TWIERDZENIE 2.12. *Załóżmy, że $\psi(p_1, ..., p_n)$ jest tautologią oraz że $\varphi_1, ..., \varphi_n$ są zdaniami logicznymi. Przez $\psi(\varphi_1, ..., \varphi_n)$ oznaczmy zdanie, które powstaje przez zastąpienie każdego występowania p_i przez φ_i dla $i \leq n$. Wówczas $\psi(\varphi_1, ..., \varphi_n)$ jest tautologią.*

Przykład 2.10 zawiera również bardzo użyteczne narzędzie służące sprawdzaniu, czy dane zdanie jest, czy nie jest tautologią: tzw. metodę zero-jedynkową.

PRZYKŁAD 2.13 (metoda zero-jedynkowa). Rozważmy schemat zdania Z skończenie wielu zmiennych zdaniowych $p_1, p_2, ..., p_n$, np. schemat utworzony z trzech zmiennych p, q, r postaci: $(p \wedge (q \Rightarrow r)) \Rightarrow q$. Sprawdzimy, czy Z jest tautologią:

p	q	r	$q \Rightarrow r$	$p \wedge (q \Rightarrow r)$	Z
1	1	1	1	1	1
1	1	0	0	0	1
1	0	1	1	1	0
0	1	1	1	0	1
1	0	0	1	1	0
0	1	0	0	0	1
0	0	1	1	0	1
0	0	0	1	0	1

Jeśli w ostatnim kroku okaże się, że zdanie Z ma wartość logiczną równą 1 (jest prawdziwe) w każdym przypadku (przy każdej możliwej kombinacji wartości logicznych zmiennych zdaniowych), to Z jest tautologią. W przeciwnym wypadku Z nie jest tautologią. Zatem powyższy schemat nie jest tautologią.

Przedstawimy teraz najważniejsze tautologie. Dowód, że poszczególne zdania są tautologiami pozostawiamy jako ćwiczenie. Wielość prezentowanych poniżej schematów (i ich nazw) ma charakter raczej informacyjny. Warto wiedzieć, jakie przekształcenia są logicznie dozwolone. Ich poprawność można uzasadnić na bieżąco wraz z potrzebą użycia.

TWIERDZENIE 2.14 (własności negacji i prawa De Morgana). *Następujące zdania są tautologiami:*

1. *(prawo podwójnej negacji):* $\neg(\neg p) \iff p$
2. *(prawo wyłączonego środka – patrz Przykład 2.10):* $p \vee \neg p$
3. *(prawo sprzeczności):* $\neg(p \wedge \neg p)$

4a. *(prawa De Morgana):* $\neg(p \wedge q) \iff (\neg p \vee \neg q)$

4b. *(prawa De Morgana)* $\neg(p \vee q) \iff (\neg p \wedge \neg q)$

5. *(zaprzeczenie implikacji):* $\neg(p \Rightarrow q) \iff (p \wedge \neg q)$.

Tautologie mogą i powinny być wykorzystywane i rozumiane jako dozwolone prawa przekształcania zdań. Dla przykładu – w ciągu równoważności:

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

użyliśmy najpierw prawa de Morgana, a następnie prawa podwójnej negacji, by wykazać równoważność zdania $\neg(\neg p \vee \neg q)$ i zdania $(p \wedge q)$.

Sformułowanie *zdanie p jest równoważne zdaniu q* zostało już w logice zapisane przy użyciu symbolu $\iff$. Dlatego też sformułowania w powyższym twierdzeniu można znacząco uprościć. W następnym pojawią się już, z pewnością zrozumiałe, symbole równoważności.

TWIERDZENIE 2.15 (własności alternatywy i koniunkcji). *Dla dowolnych zdań p, q i r następujące zdania są tautologiami:*

1. *(idempotentność koniunkcji i alternatywy):* $(p \wedge p) \iff p, (p \vee p) \iff p$
2. *(łączność koniunkcji i alternatywy):* $((p \wedge q) \wedge r) \iff (p \wedge (q \wedge r)), ((p \vee q) \vee r) \iff (p \vee (q \vee r))$
3. *(przemienność koniunkcji i alternatywy):* $(p \wedge q) \iff (q \wedge p), (p \vee q) \iff (q \vee p)$
4. *(rozdzielność koniunkcji względem alternatywy):* $(p \wedge (q \vee r)) \iff ((p \wedge q) \vee (p \wedge r))$
5. *(rozdzielność alternatywy względem koniunkcji):* $(p \vee (q \wedge r)) \iff ((p \vee q) \wedge (p \vee r))$.

PRZYKŁAD 2.16. Rozważmy tzw. prawo idempotentności koniunkcji. Niech p oznacza zdanie: *liczba 4 jest podzielna przez 2*. Oczywiście jest to zdanie prawdziwe. Łatwo zauważyć, że zdanie $p \wedge p$ oznacza *liczba 4 jest podzielna przez 2 i liczba 4 jest podzielna przez 2*, co oczywiście jest niepotrzebnym powtórzeniem i powinno brzmieć tak samo, jak p.

Łączność koniunkcji oznacza, że niezależnie w jakiej kolejności wyliczymy wartość logiczną $p \wedge q \wedge r$, to otrzymamy to samo. Możemy zatem w zapisie zaoszczędzić nawiasy i pisać $p \wedge q \wedge r$ zamiast $(p \wedge q) \wedge r$ czy $p \wedge (q \wedge r)$. Podobnie dla alternatywy.

TWIERDZENIE 2.17 (własności implikacji i równoważności). *Następujące zdania są tautologiami:*

1. *(prawo odrywania):* $(p \wedge (p \Rightarrow q)) \Rightarrow q$
2. *(przechodniość implikacji):* $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
3. *(prawo kontrapozycji):* $(p \Rightarrow q) \iff (\neg q \Rightarrow \neg p)$
4. *(prawo eliminacji równoważności):* $(p \iff q) \iff ((p \Rightarrow q) \wedge (q \Rightarrow p))$
5. $(p \iff q) \iff (\neg p \iff \neg q)$.

Twierdzenia w matematyce są budowane w postaci implikacji $p \Rightarrow q$. Jeśli p jest zdaniem fałszywym, to implikacja $p \Rightarrow q$ jest prawdziwa. Jednak implikacja o poprzedniku fałszywym nie ma wartości poznawczej – tzn. nic z niej nie wynika. Gdy jednak implikacja (twierdzenie) $p \Rightarrow q$ jest prawdziwa oraz p jest zdaniem prawdziwym, to prawo odrywania mówi, że prawdziwe jest także zdanie q. Odkryte zostało w ten sposób nowe prawdziwe zdanie q, co poszerzyło naszą wiedzę.

Prawo eliminacji równoważności pokazuje, że aby udowodnić:

$$(n \text{ jest podzielna przez } 4) \iff (\text{istnieją liczby parzyste } m, k > 1 \text{ takie, że } n = mk),$$

trzeba pokazać dwie implikacje:

$$(n \text{ jest podzielna przez } 4) \Rightarrow (\text{istnieją liczby parzyste } m, k > 1 \text{ takie, że } n = mk)$$

oraz

$$(\text{istnieją liczby parzyste } m, k > 1 \text{ takie, że } n = mk) \Rightarrow (n \text{ jest podzielna przez } 4).$$

Obie te implikacje są jasne, co pokazuje prawdziwość równoważności.

Uwaga 2.18 (bardzo ważne wiadomości z drugiego wykładu). Podczas drugiego wykładu dowiedzieliśmy się m.in.:

- jak formalnie definiuje się spójniki logiczne
- jaka jest różnica między **lub** a **albo**!
- co to jest tautologia
- co to jest metoda zero-jedynkowa i czemu służy.

ROZDZIAŁ 3

Aksjomaty teorii mnogości i działania na zbiorach

Dla uproszczenia dalszych zapisów wprowadźmy następujące oznaczenia:

Oznaczenie 3.1.

- *Zapis* ***dla każdego*** x *oznaczamy skrótowo:* $\forall x$.
- *Zapis* ***istnieje*** x *oznaczamy skrótowo:* $\exists x$.
- *Symbole* $\forall, \exists$ *nazywamy odpowiednio* ***kwantyfikatorem ogólnym i szczególnym****, zaś* x *zmienną, na której oparty jest ten kwantyfikator.*
- *Zapis* $x \in A$ *czytamy: x należy do A lub x jest elementem zbioru A. Dla skrótowego zapisu* $\neg(x \in A)$ *używamy symbolu* $x \notin A$.

Uwaga 3.2. Warto odnotować, że każdy zapis postaci $x \in A$ jest **zdaniem**, które jest prawdziwe lub fałszywe. W matematyce nie ma możliwości, by obiekt x należał do zbioru A *częściowo* - albo *należy*, albo *nie należy*.

Przykład 3.3. Zdanie $0 \in \mathbb{N}$ jest fałszywe, zaś zdanie $127 \in \mathbb{N}$ jest prawdziwe.

Przykład 3.4. Niech $A = (0, 1)$ będzie przedziałem, wówczas zdanie $0 \in A$ jest fałszywe, zaś zdanie $\frac{1}{2} \in A$ jest prawdziwe.

1. Aksjomaty teorii ZFC

Pojęciem pierwotnym aksjomatycznej teorii ZFC[1] jest zbiór. Oznacza to, że nie definiujemy, czym jest zbiór[2]. W skład języka teorii mnogości wchodzą: dwie relacje dwuargumentowe „$\in$" – należenie do zbioru oraz „$=$" – równość dwóch zbiorów, spójniki logiczne oraz kwantyfikatory. Pozostałe symbole

[1] Litery Z i F pochodzą od nazwisk Zermelo (niemiecki matematyk Ernst Zermelo, 1871–1953) i Fraenkel (niemiecko- -izraelski matematyk Abraham Fraenkel, 1891–1965). Litera C jest związana z aksjomatem wyboru (Axiom of Choice).

[2] W aksjomatycznej teorii mnogości ZFC wszystkie obiekty to zbiory. Odbiega to od typowego myślenia o zbiorach. Zazwyczaj, gdy piszemy $n \in \mathbb{N}$, myślimy, że n to liczba, a $\mathbb{N}$ to zbiór; że oba te obiekty n i $\mathbb{N}$, to różne typy bytów. O n nie myślimy, że to zbiór, bo to jest liczba. Mogą istnieć rodziny zbiorów, np. $\mathcal{A} = \{[0, 1], [2, 3], [4, 5]\}$ to rodzina, w skład której wchodzą trzy przedziały $[0, 1], [2, 3], [4, 5]$. Przedziały też są zbiorami, np. $[2, 3] = \{x \in \mathbb{R} : 2 \leq x \leq 3\}$. Często można się spotkać w matematyce z konwencją, że małe litery $a, b, ..., x, y, z$ oznaczają obiekty, $A, B, ..., Z$ zbiory, a $\mathcal{A}, \mathcal{B}, ..., \mathcal{Z}$ oznaczają rodziny zbiorów. Taka trzypoziomowa hierarchia jest często wystarczająca.
Tymczasem w teorii mnogości ZFC wszystkie obiekty są zbiorami z tego samego poziomu. Często zapisujemy zbiory małymi literami i np. formuła $x \in y \vee x = y \vee y \in x$ jest skonstruowana poprawnie; nie ma tu pomieszania poziomów czy hierarchii.

pojawiające się w teorii mnogości są definiowane za ich pomocą, np. $X \subseteq Y$ to skrótowy zapis formuły $\forall v(v \in X \implies v \in Y)$. Każde zdanie teorii mnogości można zapisać symbolicznie, jednak dla jasności aksjomaty ZFC będą zapisane w języku naturalnym.

Zacznijmy od następującego postulatu:

Aksjomat 1 (aksjomat równości zbiorów). *Dwa zbiory są równe wtedy i tylko wtedy, gdy mają dokładnie te same elementy.*

Ten aksjomat mówi, że po pierwsze: kolejność elementów w zbiorze nie ma znaczenia, np. $\{1, 2, 3\} = \{2, 3, 1\}$; po drugie: w zbiorze każdy element występuje tylko raz, np. $\{1, 2, 3\} = \{3, 2, 1, 3, 1\}$.

Aksjomat 2 (aksjomat zbioru pustego). *Istnieje zbiór taki, że żaden element do niego nie należy*[3].

Wobec faktu, że w aksjomatyce ZFC wszystko jest zbiorem – aksjomat zbioru pustego postuluje: *istnieje zbiór X, który nie ma żadnego elementu*. Wobec aksjomatu równości zbiorów istnieje dokładnie jeden taki zbiór X. Nazywamy go **zbiorem pustym** i oznaczamy $\emptyset$.

Pozostałe aksjomaty ZFC dotyczą tego, jak z istniejących zbiorów tworzy się nowe zbiory.

Aksjomat 3 (aksjomat pary). *Dla każdych zbiorów X, Y istnieje zbiór, który zawiera jako elementy zbiory X i Y, i tylko te. Zbiór ten oznaczamy symbolem $\{X, Y\}$*[4].

Aksjomat 4 (aksjomat sumy). *Dla każdych zbiorów X, Y istnieje zbiór, który zawiera wszystkie elementy zbioru X i wszystkie elementy zbioru Y, i tylko te. Zbiór ten oznaczamy symbolem $X \cup Y$*[5].

Funkcja zdaniowa to wyrażenie zawierające zmienną (lub zmienne), po podstawieniu za którą odpowiedniej wartości staje się zdaniem, na przykład: $x > 2$ jest funkcją zdaniową dla $x \in \mathbb{R}$.

Kolejny aksjomat ZFC pozwalający z istniejących zbiorów tworzyć nowe to aksjomat wycinania.

Aksjomat 5 (aksjomat wycinania[6]). *Dla dowolnego zbioru X i dowolnej funkcji zdaniowej $W(x)$ istnieje zbiór $\{x \in X \colon W(x)\}$ składający się ze wszystkich elementów x zbioru X mających własność W.*

---

3 aksjomat zbioru pustego można zapisać symbolicznie: $\exists x\, \forall y\, (y \notin x)$.

4 aksjomat pary zapisujemy symbolicznie: $\forall x \forall y \exists z \big(x \in z \wedge y \in z \wedge \forall v \big(v \in z \implies (v = x \vee v = y)\big)\big)$.

5 aksjomat sumy zapisujemy symbolicznie:
$\forall x \forall y \exists z \big(\forall v (v \in x \implies v \in z) \wedge \forall v (v \in y \implies v \in z) \wedge \forall v \big(v \in z \implies (v \in x \vee v \in y)\big)\big)$.

6 Jest to uproszczona wersja aksjomatu wycinania. Pełna wersja brzmi: *Dla dowolnej formuły $\varphi(s, t)$, dowolnego zbioru x i parametru p istnieje zbiór $y = \{u \in x : \varphi(u, p)\}$, który zawiera wszystkie elementy $u \in x$ mające własność φ.*

2. Relacje między zbiorami i działania na zbiorach

W języku teorii mnogości jest zadana jedna relacja między definiowanymi obiektami: relacja należenia $\in$. Wykorzystując wprowadzone dotychczas definicje możemy określić tzw. relację inkluzji $\subseteq$:

DEFINICJA 3.5. *Niech A, B będą zbiorami. Powiemy, że zbiór A zawiera się w zbiorze B albo zbiór A jest podzbiorem zbioru B (oznaczamy $A \subseteq B$) gdy: $\forall x\ (x \in A \Rightarrow x \in B)$, innymi słowy, gdy: każdy **element** zbioru A jest też **elementem** zbioru B. Dla skrócenia zapisu $\neg(A \subseteq B)$ stosujemy zapis $A \nsubseteq B$.*

PRZYKŁAD 3.6. Rozważmy zbiory $A = \{1, 2, 3\}, B = \{n \in \mathbb{N}\colon n \leq 7\}$. Wówczas $A \subseteq B$, bo elementami zbioru A są: $1, 2, 3$ i **każdy** z nich jest też elementem zbioru B. Zarazem $B \nsubseteq A$, bo np. $5 \in B$, ale $5 \notin A$.

UWAGA 3.7. Zbiór pusty $\emptyset$ jest podzbiorem dowolnego zbioru. Istotnie, implikacja $x \in \emptyset \Rightarrow x \in A$ jest ZAWSZE prawdziwa, jako implikacja o fałszywym poprzedniku (zobacz: Definicja 2.4). Zarazem, gdyby $A \subseteq \emptyset$ i zbiór A zawierał jakiś element, to zbiór pusty też by go zawierał, a to jest niemożliwe. Zatem zbiór A nie ma elementów i **jedynym** podzbiorem zbioru pustego jest zbiór pusty.

Zauważmy, że zapis $A \subseteq B$ oznacza, że każdy element zbioru A jest też elementem zbioru B. Podobnie zapis $B \subseteq A$ oznacza, że każdy element zbioru B jest też elementem zbioru A. Stąd zdanie $(A \subseteq B) \wedge (B \subseteq A)$ oznacza, że zbiory A i B mają **dokładnie** te same elementy. Udowodniliśmy zatem następujące:

TWIERDZENIE 3.8 (równość zbiorów a inkluzje). *Niech A, B będą zbiorami. Wówczas: $A = B \iff (A \subseteq B \wedge B \subseteq A)$.*

UWAGA 3.9. Jest to bardzo prosta, ale bardzo ważna, podstawowa metoda wykazywania, że jakieś dwa zbiory są równe.

TWIERDZENIE 3.10 (przechodniość inkluzji). *Niech $A \subseteq B$ oraz $B \subseteq C$. Wówczas $A \subseteq C$.*

DOWÓD. Załóżmy, że $A \subseteq B$ i $B \subseteq C$. Niech $x \in A$. Skoro $A \subseteq B$, to $x \in B$. Następnie z faktu, że $B \subseteq C$ otrzymujemy, że $x \in C$.

Pokazaliśmy, że dowolnie wybrany element zbioru A należy do zbioru C. Zatem $A \subseteq C$. □

Wiedząc już co to jest inkluzja między zbiorami, możemy określić pewne działania na zbiorach. Do końca wykładu niech X będzie zbiorem oraz A, B, C, D będą jego podzbiorami (tj. $A, B, C, D \subseteq X$).

Definicja 3.11.

1. *Iloczynem (częścią wspólną/przekrojem) zbiorów A i B nazywamy zbiór:* $A \cap B = \{x \in X \colon x \in A \wedge x \in B\}$.
2. *Różnicą zbiorów A i B nazywamy zbiór:* $A \setminus B = \{x \in X \colon x \in A \wedge x \notin B\}$.
3. *Dopełnieniem zbioru A do zbioru X nazywamy zbiór:* $X \setminus A$.
4. *Sumą zbiorów A i B nazywamy zbiór:* $A \cup B = \{x \in X \colon x \in A \vee x \in B\}$.
5. *Różnicą symetryczną zbiorów A i B nazywamy zbiór:* $A \triangle B = A \setminus B \cup B \setminus A = (A \cup B) \setminus (A \cap B)$.

Twierdzenie 3.12. *Niech $A, B \subseteq X$. Zbiory $A \cap B$ oraz $A \setminus B$ można równoważnie zapisać jako:*

1. $A \cap B = \{x \in A \colon x \in B\} = \{x \in B \colon x \in A\}$.
2. $A \setminus B = \{x \in A \colon x \notin B\}$.

Przykład 3.13. Niech $A = \{1, 2, 3\}$ oraz $B = \{n \in \mathbb{N} \colon n \leq 7\}$. Wówczas:

$$A \cup B = \{1, 2, 3, ..., 7\}, \;\; A \cap B = \{1, 2, 3\}, \;\; A \setminus B = \emptyset \;\text{ oraz }\; B \setminus A = \{4, 5, 6, 7\}.$$

Przykład 3.14. Niech $A = [0, 2)$ oraz $B = [1, 3]$ będą przedziałami. Wówczas:

$$A \cup B = [0, 3], \;\; A \cap B = [1, 2), \;\; , A \setminus B = [0, 1) \;\text{ oraz }\; B \setminus A = [2, 3].$$

3. Własności działań na zbiorach i relacji inkluzji

Opisane w Definicji 3.11 działania na zbiorach mają następujące własności:

Twierdzenie 3.15 (własności sumy i iloczynu). *Dla dowolnych zbiorów A, B, C, D zachodzą następujące własności:*

1. *(idempotentność sumy i iloczynu):* $A \cup A = A, A \cap A = A$
2. *(przemienność sumy i iloczynu):* $A \cup B = B \cup A, A \cap B = B \cap A$
3. *(łączność sumy i iloczynu):* $A \cup (B \cup C) = (A \cup B) \cup C, A \cap (B \cap C) = (A \cap B) \cap C$
4. *(rozdzielność):* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C); A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
5. *(minimalność zbioru pustego):* $A \cup \emptyset = A, A \cap \emptyset = \emptyset$
6. $A \subseteq A \cup B, A \cap B \subseteq A$
7. $(A \subseteq B \wedge C \subseteq D) \Rightarrow A \cup C \subseteq B \cup D$
8. $(A \subseteq B \wedge C \subseteq D) \Rightarrow A \cap C \subseteq B \cap D$.

Dowody powyższych równości i zawierań wynikają z tautologii rachunku zdań. Pokażemy to na dwóch przykładach. Aby wykazać, że $A \subseteq A \cup B$, weźmy dowolny element x zbioru A. Wobec definicji zawierania trzeba pokazać, że:

$$x \in A \implies x \in A \cup B.$$

Z definicji sumy zbiorów mamy:

$$x \in A \cup B \iff (x \in A \vee x \in B).$$

Zatem trzeba pokazać, że:

$$x \in A \implies (x \in A \vee x \in B).$$

Implikacja ta wynika z tautologii $p \implies (p \vee q)$, w której w miejsce zmiennej zdaniowej p wstawiamy $x \in A$, a w miejsce q wstawiamy $x \in B$. To dowodzi, że $A \subseteq A \cup B$.

Zapiszmy teraz dowód równości $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Trzeba pokazać, że dla dowolnego elementu x,

$$x \in A \cap (B \cup C) \iff x \in (A \cap B) \cup (A \cap C).$$

Rozpiszmy obie strony tej równoważności – lewa strona:

$$x \in A \cap (B \cup C) \iff (x \in A \wedge x \in B \cup C) \iff (x \in A \wedge (x \in B \vee x \in C))$$

i prawa strona:

$$x \in (A \cap B) \cup (A \cap C) \iff (x \in A \cap B \vee x \in A \cap C) \iff ((x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)).$$

Musimy pokazać zatem, że:

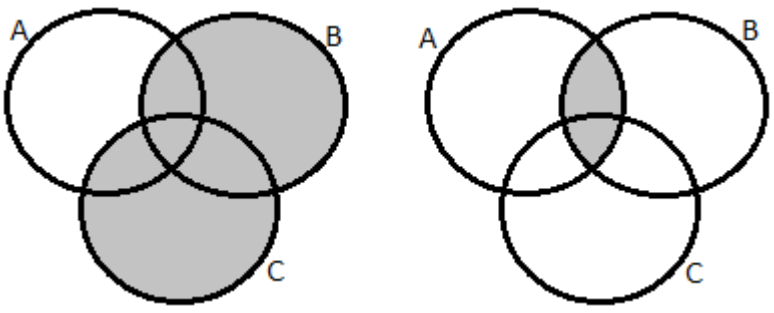
$$(x \in A \wedge (x \in B \vee x \in C)) \iff ((x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)).$$

Zastępując $x \in A$ przez p, $x \in B$ przez q i $x \in C$ przez r, otrzymujemy zdanie logiczne

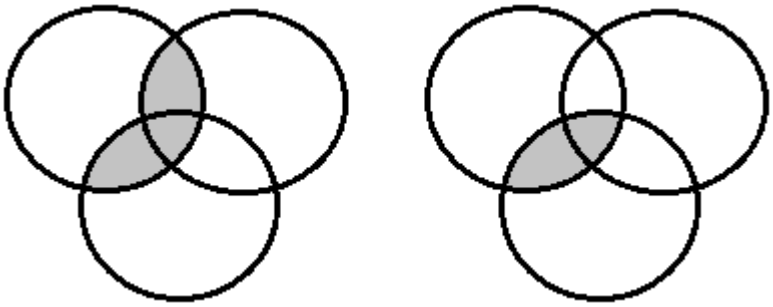
$$p \wedge (q \vee r) \iff ((p \wedge q) \vee (p \wedge r)),$$

które jest tautologią. To dowodzi, że $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

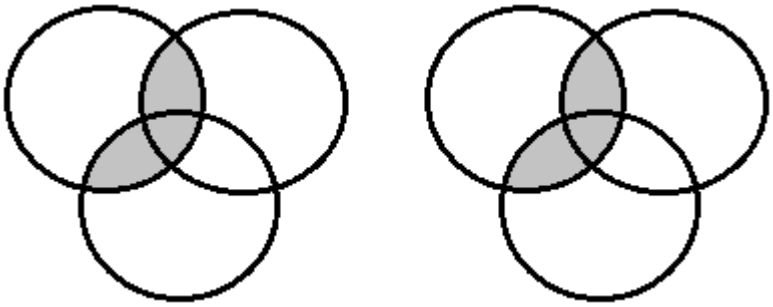
W praktyce matematycy sprawdzają dowodami rysunkowymi, czy dana własność zachodzi. Aby pokazać, że zachodzi równość $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, zaznaczmy na lewym obrazku zbiór $B \cup C$, a na prawym $A \cap B$:



Następnie na lewym obrazku zaznaczmy $A \cap (B \cup C)$, a na prawym $A \cap C$:



W końcu na lewym obrazku zaznaczmy $A \cap (B \cup C)$, a na prawym $(A \cap B) \cup (A \cap C)$, czyli sumę z poprzednich dwóch obrazków na nim:



Oba obrazki są takie same, co pokazuje równość $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

TWIERDZENIE 3.16 (własności dopełnienia i prawa De Morgana). *Niech X będzie zbiorem oraz $A, B \subseteq X$. Zachodzą następujące własności:*

1. $(X \setminus (X \setminus A)) = A$
2. $A \setminus B = A \cap (X \setminus B)$
3. *(prawa De Morgana):* $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B), X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$
4. $X \setminus \emptyset = X, X \setminus X = \emptyset$
5. $A \subseteq B \iff X \setminus B \subseteq X \setminus A$.

Dowód powyższego twierdzenia pozostawiamy na ćwiczenia.

Przypomnijmy, że zbiory opisane w Definicji 3.11 są określone poprzez odpowiednią funkcję zdaniową. Na przykład zbiór $A \cap B = \{x \in X : W(x)\}$, gdzie $W(x)$ oznacza formułę $x \in A \wedge x \in B$. Związek operacji na zbiorach z operacjami logicznymi jest bardzo istotny, co potwierdza poniższe:

TWIERDZENIE 3.17 (związek działań mnogościowych z operacjami logicznymi). *Załóżmy, że $A = \{x \in X : W(x)\}$ oraz $B = \{x \in X : G(x)\}$, wówczas zachodzą następujące własności:*

1. $X \setminus A = \{x \in X : \neg W(x)\}$
2. $A \cap B = \{x \in X : W(x) \wedge G(x)\}$

3. $A \cup B = \{x \in X \colon W(x) \vee G(x)\}$.

Dowód powyższego twierdzenia również pozostawiamy na ćwiczenia.
Warto na koniec zauważyć jeszcze dwie własności używanych dotychczas relacji między zbiorami:

TWIERDZENIE 3.18. *Dla każdego zbioru A mamy $A \subseteq A$.*

AKSJOMAT 6. *Dla każdego zbioru A mamy $A \notin A$.*

O ile dowód Twierdzenia 3.18 jest łatwy, o tyle tę drugą własność potraktujmy jako aksjomat.

4. Nie istnieje zbiór wszystkich zbiorów

Niech X będzie dowolnym zbiorem oraz $W(x)$ będzie funkcją zdaniową. Na mocy aksjomatu wycinania obiekt postaci $\{x \in X \colon W(x)\}$ również jest zbiorem. Zapis $\{x \in X \colon W(x)\}$ czytamy: *zbiór wszystkich x ze zbioru X mających własność W*. Można zapytać, czy istnieje *zbiór wszystkich takich x, że x ma własność W*, czyli $\{x \colon W(x)\}$? Nie musi tak być, o czym mówi następujące twierdzenie.

TWIERDZENIE 3.19. *Nie istnieje zbiór wszystkich zbiorów.*

DOWÓD. Przypuśćmy, że istnieje zbiór X wszystkich zbiorów. Niech $W(u)$ będzie własnością postaci $u \notin u$. Na mocy aksjomatu wycinania istnieje zbiór

$$\{u \in X : W(u)\} = \{u \in X : u \notin u\}.$$

Nazwijmy ten zbiór Y. Ponieważ X jest zbiorem wszystkich zbiorów, to $Y \in X$. Każdy element zbioru X albo należy do Y, albo nie należy do Y, bo Y jest podzbiorem X. Zarazem Y jest elementem X, więc zachodzi jedna z dwóch możliwości:

- $Y \in Y$, ale wtedy $Y \notin \{u \in X : u \notin u\} = Y$, co daje sprzeczność, więc ta możliwość nie zachodzi;
- $Y \notin Y$, ale wtedy $Y \in \{u \in X : u \notin u\} = Y$, co znowu daje sprzeczność, więc ta możliwość też nie zachodzi.

Otrzymana sprzeczność wynika z przypuszczenia, że istnieje zbiór wszystkich zbiorów. Zatem nie istnieje zbiór wszystkich zbiorów. □

W dowodzie powyższego twierdzenia podkreślone jest jedno zdanie. W tym miejscu w dowodzie wykorzystaliśmy fakt, że X jest zbiorem wszystkich zbiorów. Gdyby w dowodzie zamiast X użyć dowolnego zbioru, a podkreślone zdanie zastąpić zdaniem: *Przypuśćmy, że $Y \in X$*, to również doszlibyśmy do sprzeczności. Sprzeczność wynikłaby z założenia, że $Y \in X$. W ten sposób otrzymamy następujący ogólniejszy fakt, z którego wynika nieistnienie zbioru wszystkich zbiorów.

TWIERDZENIE 3.20. *Niech X będzie dowolnym zbiorem. Wówczas $\{u \in X : u \notin u\} \notin X$.*

UWAGA 3.21 (bardzo ważne wiadomości z trzeciego wykładu). Podczas trzeciego wykładu dowiedzieliśmy się m.in.:

- co to są kwantyfikatory: **ogólny** i **szczególny**
- co to jest zbiór pusty $\emptyset$
- jak opisuje się zbiory i definiuje działania między nimi
- jak definiuje się relację inkluzji
- jakie podstawowe własności mają działania i relacje między zbiorami
- nie istnieje zbiór wszystkich zbiorów.

ROZDZIAŁ 4

Kwantyfikatory ograniczone, zbiór potęgowy i iloczyn kartezjański

1. Kwantyfikatory ograniczone

Na Wykładzie 3. poznaliśmy symbole kwantyfikatorów: ogólnego i szczególnego. Podamy teraz definicję kwantyfikatora ogólnego i szczególnego ograniczonego do pewnego zbioru X.

Definicja 4.1. *Niech X będzie dowolnym zbiorem. Niech $W(x)$ będzie funkcją zdaniową zmiennej $x \in X$. Zdanie $(\forall x \in X)\, W(x)$ oznacza zdanie $\forall x(x \in X \implies W(x))$, a czytamy je: dla każdego $x \in X$ zachodzi $W(x)$. Zdanie $(\exists x \in X)\, W(x)$ oznacza zdanie $\exists x(x \in X \wedge W(x))$, a czytamy je: istnieje taki $x \in X$, że zachodzi $W(x)$.*

Twierdzenie 4.2. *Zdanie $(\forall x \in X)\, W(x)$ jest równoważne równości $\{x \in X \colon W(x)\} = X$. Zdanie $(\exists x \in X)\, W(x)$ jest równoważne równości $\{x \in X \colon W(x)\} \neq \emptyset$.*

Dowód. Załóżmy, że prawdziwe jest zdanie:
(1) $(\forall x \in X)W(x)$.
Musimy pokazać, że zachodzą zawierania:
(2) $\{x \in X : W(x)\} \subseteq X$
(3) $X \subseteq \{x \in X : W(x)\}$.
Zbiór $\{x \in X : W(x)\}$ jest podzbiorem X dla dowolnej funkcji zdaniowej $W(x)$, więc inkluzja (2) jest prawdziwa. Aby pokazać drugą inkluzję, ustalmy $x_0 \in X$. Skoro zachodzi (1), to prawdziwe jest zdanie:
(4) $x_0 \in X \implies W(x_0)$.
Skoro $x_0 \in X$ jest zdaniem prawdziwym, to z definicji implikacji zdaniem prawdziwym jest $W(x_0)$. Pokazaliśmy, że dla $x_0 \in X$ zachodzi $W(x_0)$, a zatem:
(5) $x_0 \in \{x \in X : W(x)\}$.
Z faktu, że $x_0 \in X$ wywnioskowaliśmy, że zachodzi (5). To oznacza następującą implikację:
(6) $x_0 \in X \implies x_0 \in \{x \in X : W(x)\}$.
Wybór punktu x_0 ze zbioru X był zupełnie dowolny. Zatem z dowolności wyboru x_0 otrzymujemy (3). Zawierania (2) i (3) dają równość zbiorów:
(7) $\{x \in X : W(x)\} = X$.

Załóżmy teraz, że zachodzi (7). Niech $x_0 \in X$. Z (7) otrzymujemy, że:
(8) $x_0 \in \{x \in X : W(x)\}$,
czyli zachodzi $W(x_0)$. Pokazaliśmy, że jeśli $x_0 \in X$, to $W(x_0)$, czyli implikację:
(9) $x_0 \in X \implies W(x_0)$.
Wobec dowolności wyboru $x_0 \in X$ implikacja (9) zachodzi dla każdego elementu zbioru X:
(10) $\forall x(x \in X \implies W(x))$,
co daje (1) i kończy dowód.

Wykażemy teraz drugą część tezy dowodzonego twierdzenia. Załóżmy najpierw, że:
(11) $(\exists x \in X)W(x)$,
co oznacza, że:
(12) $\exists x(x \in X \wedge W(x))$.
Zatem istnieje $x_0 \in X$ taki, że zachodzi $W(x_0)$. To oznacza, że $x_0 \in \{x \in X : W(x)\}$, a w konsekwencji:
(13) $\{x \in X : W(x)\} \neq \emptyset$.
Teraz załóżmy, że zachodzi (13). Skoro zbiór $\{x \in X : W(x)\}$ jest niepusty, to istnieje $x_0 \in \{x \in X : W(x)\}$, czyli zachodzi (12). To oznacza, że zachodzi także (11). Ostatecznie wynika stąd, że zdania (11) oraz (13) są logicznie równoważne. □

Zobaczymy teraz, jak zdania $(\forall x \in X)\ W(x)$ oraz $(\exists x \in X)\ W(x)$ i ich zaprzeczenia mają się do siebie.

Twierdzenie 4.3 (zależność między kwantyfikatorami). *Niech $X \neq \emptyset$ będzie dowolnym zbiorem i niech $W(x)$ będzie funkcją zdaniową zmiennej $x \in X$. Jeśli $(\forall x \in X)\ W(x)$, to $(\exists x \in X)\ W(x)$.*

Dowód. Załóżmy, że $(\forall x \in X)\ W(x)$. Oznacza to, że $\{x \in X\colon W(x)\} = X$. Skoro $X \neq \emptyset$, to $\{x \in X\colon W(x)\} \neq \emptyset$, czyli $(\exists x \in X)\ W(x)$. □

Twierdzenie 4.4 (prawa De Morgana rachunku kwantyfikatorów). *Niech X będzie dowolnym zbiorem oraz $W(x), G(x)$ będą funkcjami zdaniowymi zmiennej $x \in X$. Wówczas:*

1. $\neg((\forall x \in X)\ W(x)) \iff (\exists x \in X)\ \neg W(x)$
2. $\neg((\exists x \in X)\ W(x)) \iff (\forall x \in X)\ \neg W(x)$.

Dowód. Udowodnimy jedną z implikacji pierwszej równoważności. Załóżmy, że:
(1) $\neg((\forall x \in X)\ W(x))$.
Z Twierdzenia 4.2 mamy:
(2) $\neg(\{x \in X\colon W(x)\} = X)$,
czyli:

(3) $X \setminus \{x \in X \colon W(x)\} \neq \emptyset$.

Wobec Twierdzenia 3.17 mamy:

(4) $X \setminus \{x \in X \colon W(x)\} = \{x \in X \colon \neg W(x)\}$, więc:

(5) $\{x \in X \colon \neg W(x)\} \neq \emptyset$.

Ponownie korzystając z Twierdzenia 4.2, otrzymujemy:

(6) $(\exists x \in X)\ \neg W(x)$.

Założyliśmy (1) i wywnioskowaliśmy z tego (6), a zatem: (7) $\neg((\forall x \in X)\ W(x)) \implies (\exists x \in X)\ \neg W(x)$.

□

Przykład 4.5. Niech $W(n)$ będzie funkcją zdaniową zmiennej $n \in \mathbb{N}$ oznaczającą: $2|n(n+1)$. Wówczas zdanie $(\forall n \in \mathbb{N})\ 2|n(n+1)$ oznacza, że *dla każdej liczby naturalnej n mamy* $2|n(n+1)$, co jest zdaniem prawdziwym.

Przykład 4.6. Niech $W(n)$ będzie funkcją zdaniową zmiennej $n \in \mathbb{N}$ oznaczającą: $(n+2)^2 - n^2$ *jest kwadratem liczby naturalnej.* Wówczas zdanie $(\exists n \in \mathbb{N})\ W(n)$ oznacza, że *istnieje liczba naturalna n taka, że $(n+2)^2 - n^2 = k^2$ dla pewnej liczby $k \in \mathbb{N}$*, co jest zdaniem prawdziwym, bo $n = 3$ jest przykładem takiej liczby. Zarazem zdanie $(\forall n \in \mathbb{N})\ W(n)$ jest zdaniem fałszywym, bo nie zachodzi dla $n = 1$.

Uwaga 4.7. Niech $X \neq \emptyset$ będzie dowolnym zbiorem i niech $W(x)$ będzie funkcją zdaniową zmiennej $x \in X$. Może zdarzyć się tak, że oba zdania $(\forall x \in X)\ W(x)$ oraz $(\exists x \in X)\ W(x)$ są fałszywe. Rozważ np. $X = \mathbb{N}$ i $W(n)$ oznaczające $n < 0$.

Notacja z kwantyfikatorami ograniczonymi jest bardzo użyteczna i pozwala zapisywać twierdzenia w znacznie prostszej postaci. Np. Zasadę indukcji można zapisać w postaci:

Twierdzenie. *Jeśli $W(n)$ jest funkcją zdaniową zmiennej $n \in \mathbb{N}$ taką, że:*

- $W(1)$ *zachodzi*
- $(\forall n_0 \in \mathbb{N})\ (W(n_0) \Rightarrow W(n_0+1))$,

to $(\forall n \in \mathbb{N})\ W(n)$.

Podobnie inne znane twierdzenia można dużo bardziej przejrzyście zapisać przy użyciu kwantyfikatorów. Np. zdanie: *Dla każdej liczby naturalnej n istnieje liczba naturalna $m > n$ będąca kwadratem liczby naturalnej* zapisujemy:

$$(\forall n \in \mathbb{N})\ (\exists m \in \mathbb{N})\ (m > n \wedge (\exists k \in \mathbb{N})\ m = k^2).$$

W praktyce zapisujemy to w krótszej formie:

$$(\forall n \in \mathbb{N})\ (\exists m > n)\ (\exists k \in \mathbb{N})\ m = k^2.$$

2. Prawa rachunku kwantyfikatorów

Zachodzą następujące prawa rachunku kwantyfikatorów.

TWIERDZENIE 4.8 (prawa rachunku kwantyfikatorów 1). *Niech X będzie dowolnym zbiorem oraz $W(x), G(x)$ będą funkcjami zdaniowymi zmiennej $x \in X$. Wówczas:*

1. $(\forall x \in X)\ (W(x) \wedge G(x)) \iff ((\forall x \in X)\ W(x) \wedge (\forall x \in X)\ G(x))$
2. $(\exists x \in X)\ (W(x) \vee G(x)) \iff ((\exists x \in X)\ W(x) \vee (\exists x \in X)\ G(x))$.

DOWÓD. Wykażemy następującą implikację:

(1) $(\forall x \in X)\ (W(x) \wedge G(x)) \implies ((\forall x \in X)\ W(x) \wedge (\forall x \in X)\ G(x))$

W tym celu załóżmy, że zachodzi poprzednik w implikacji (1):

(2) $(\forall x \in X)\ (W(x) \wedge G(x))$.

Musimy pokazać, że zachodzą jednocześnie następujące dwa zdania:

(3) $(\forall x \in X)\ W(x)$,

(4) $(\forall x \in X)\ G(x)$.

Ustalmy $x_0 \in X$. Skoro zachodzi (2), w szczególności zachodzi:

(5) $W(x_0) \wedge G(x_0)$.

Zatem zachodzi zdanie $W(x_0)$. Doszliśmy do tego zakładając, że $x_0 \in X$, a zatem wykazaliśmy implikację:

(6) $x_0 \in X \implies W(x_0)$.

Wobec dowolności wyboru $x_0 \in X$ mamy (3). W ten sam sposób wykazujemy (4). Z faktu, że zachodzi (3) i (4) wynika, że zachodzi ich koniunkcja:

(7) $(\forall x \in X)\ W(x) \wedge (\forall x \in X)\ G(x)$.

Zauważmy, że zdanie (7) to następnik implikacji (1). Z założenia (2) wywnioskowaliśmy (7), czyli wykazaliśmy implikację (1). □

TWIERDZENIE 4.9 (prawa rachunku kwantyfikatorów 2). *Niech X będzie dowolnym zbiorem oraz $W(x)$ będzie funkcją zdaniową zmiennej $x \in X$ i niech φ będzie formułą bez zmiennej wolnej x. Wówczas:*

1. $(\forall x \in X)\ (\varphi \wedge W(x)) \iff (\varphi \wedge (\forall x \in X)\ W(x))$
2. $(\forall x \in X)\ (\varphi \vee W(x)) \iff (\varphi \vee (\forall x \in X)\ W(x))$
3. $(\exists x \in X)\ (\varphi \wedge W(x)) \iff (\varphi \wedge (\exists x \in X)\ W(x))$

4. $(\exists x \in X)\ (\varphi \vee W(x)) \iff (\varphi \vee (\exists x \in X)\ W(x))$.

Dowód. Wykażemy implikację:

(1) $(\forall x \in X)\ (\varphi \wedge W(x)) \implies (\varphi \wedge (\forall x \in X)\ W(x))$.

W tym celu załóżmy, że zachodzi poprzednik implikacji (1):

(2) $(\forall x \in X)\ (\varphi \wedge W(x))$.

Z Twierdzenia 4.2 otrzymujemy:

(3) $X = \{x \in X : \varphi \wedge W(x)\}$.

Z definicji sumy zbiorów mamy:

(4) $\{x \in X : \varphi\} \cap \{x \in X : W(x)\}$.

Na mocy (3) i (4) zbiór X zawiera się w części wspólnej zbiorów $\{x \in X : \varphi\}$ i $\{x \in X : W(x)\}$, a w konsekwencji zawiera się w każdym z nich:

(5) $X \subseteq \{x \in X : \varphi\}$ i $X \subseteq \{x \in X : W(x)\}$.

Zarazem $\{x \in X : \varphi\}$ i $\{x \in X : W(x)\}$ są podzbiorami X, co wobec (5) daje

(6) $X = \{x \in X : \varphi\}$

oraz

(7) $X = \{x \in X : W(x)\}$.

Formuła nie zależy od zmiennej x, więc równość (6) oznacza, że zachodzi φ. Równość (7) na mocy Twierdzenia 4.2 oznacza, że $(\forall x \in X)W(x)$. W konsekwencji:

(8) $\varphi \wedge (\forall x \in X)W(x)$.

Z założenia (2) i jego konsekwencji (8) otrzymujemy implikację (1). □

Twierdzenie 4.10 (prawa przestawiania kwantyfikatorów). *Niech X, Y będą dowolnymi zbiorami oraz $W(x, y)$ będzie funkcją zdaniową dwu zmiennych $x \in X, y \in Y$. Wówczas:*

1. $(\forall x \in X)\ (\forall y \in Y)\ W(x, y) \iff (\forall y \in Y)\ (\forall x \in X)\ W(x, y)$

2. $(\exists x \in X)\ (\exists y \in Y)\ W(x, y) \iff (\exists y \in Y)\ (\exists x \in X)\ W(x, y)$

3. $(\exists x \in X)\ (\forall y \in Y)\ W(x, y) \Rightarrow (\forall y \in Y)\ (\exists x \in X)\ W(x, y)$.

Dowód. Wykażemy implikację:

(1) $(\forall x \in X)\ (\forall y \in Y)\ W(x, y) \implies (\forall y \in Y)\ (\forall x \in X)\ W(x, y)$.

W tym celu zakładamy poprzednik implikacji:

(2) $(\forall x \in X)\ (\forall y \in Y)\ W(x, y)$.

Na mocy Twierdzenia 4.2 otrzymujemy:

(3) $\{x \in X : (\forall y \in Y)W(x, y)\} = X$.

Przypuśćmy, że następnik implikacji (1) nie zachodzi, czyli:

(4) $\neg\Big((\forall y \in Y)\ (\forall x \in X)\ W(x,y)\Big)$.

Na mocy praw De Morgana rachunku kwantyfikatorów otrzymujemy kolejno:

(5) $(\exists y \in Y)\ \neg\Big((\forall x \in X)\ W(x,y)\Big)$

(6) $(\exists y \in Y)\ (\exists x \in X)\ \neg W(x,y)$.

Zatem istnieją elementy $y_0 \in Y$ i $x_0 \in X$ takie, że $W(x_0, y_0)$ nie zachodzi. Dlatego:

(7) $y_0 \notin \{y \in Y : W(x_0, y)\}$,

czyli:

(8) $\{y \in Y : W(x_0, y)\} \neq Y$,

stąd:

(9) $x_0 \in \{x \in X : \{y \in Y : W(x_0, y)\} \neq Y\}$,

co daje:

(10) $x_0 \notin \{x \in X : \{y \in Y : W(x_0, y)\} = Y\}$.

W konsekwencji:

(11) $\{x \in X : \{y \in Y : W(x_0, y)\} = Y\} \neq X$,

co przeczy (3). Uzyskana sprzeczność wynika z przypuszczenia (4). Zatem (4) nie jest prawdziwe, czyli:

(12) $(\forall y \in Y)\ (\forall x \in X)\ W(x,y)$.

Zakładając (2), wykazaliśmy (12), co daje implikację (1). □

3. Zbiory potęgowe

W czasie poprzedniego wykładu poznaliśmy pojęcie *podzbioru*. Naturalne wydaje się pytanie, czy mając ustalony zbiór A, możemy zgromadzić wszystkie jego podzbiory, tj. czy możemy zdefiniować zbiór składający się z wszystkich podzbiorów zbioru A i tylko z nich.

Aksjomat 7 (aksjomat zbioru potęgowego). *Niech A będzie zbiorem. Istnieje zbiór składający się ze wszystkich podzbiorów zbioru A i tylko z nich, który nazywamy zbiorem potęgowym zbioru A i oznaczamy $\mathcal{P}(A)$.*

Przykład 4.11. Rozważmy zbiór $\emptyset$. Z wcześniejszych wykładów wynika m.in., że $\emptyset \subseteq \emptyset$. Zatem $\emptyset \in \mathcal{P}(\emptyset)$. Co więcej, zbiór $\mathcal{P}(\emptyset)$ nie ma innych elementów, bo $\emptyset$ nie ma innych podzbiorów. Stąd $\mathcal{P}(\emptyset) = \{\emptyset\}$.

Przykład 4.12. Dla zbioru $A = \{1, 2, 3\}$ mamy, że:

$$\mathcal{P}(A) = \big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\big\}.$$

Jak widać $\mathcal{P}(A)$ ma $8 = 2^3$ elementów. Nie jest przypadkiem, że zbiór potęgowy zbioru trzyelementowego ma 2^3 elementów. Wynika to z ogólniejszej prawidłowości, którą opisuje kolejne twierdzenie.

TWIERDZENIE 4.13. *Niech A będzie zbiorem n-elementowym dla pewnego $n \in \mathbb{N}$. Wówczas zbiór $\mathcal{P}(A)$ ma dokładnie 2^n elementów.*

Dowód tego twierdzenia zostawimy na kolejne wykłady.

4. Para uporządkowana

DEFINICJA 4.14 (para uporządkowana). *Parą uporządkowaną o poprzedniku a i następniku b nazywamy zbiór $\{\{a\}, \{a, b\}\}$ i oznaczamy (a, b).*

Następujące twierdzenie oddaje istotę pojęcia pary uporządkowanej:

TWIERDZENIE 4.15 (równość par uporządkowanych). $(a, b) = (c, d) \iff a = c \wedge b = d$.

Dowód powyższego twierdzenia zostawiamy jako ćwiczenie.
Pojęcie pary uporządkowanej pozwala zdefiniować produkt kartezjański dwóch zbiorów.

DEFINICJA 4.16 (iloczyn kartezjański). *Niech A, B będą dowolnymi zbiorami. Produktem kartezjańskim (iloczynem kartezjańskim) zbiorów A i B nazywamy zbiór*

$$A \times B = \{(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B)) \colon a \in A \wedge b \in B\}.$$

PRZYKŁAD 4.17. Niech $A = \{1, 2, 3\}, B = \{2, 3\}$ wówczas

$$A \times B = \big\{(1, 2), (1, 3), (2, 2), (2, 3), (3, 2), (3, 3)\big\},$$

zaś $B \times A = \big\{(2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\big\}$. Zauważmy przy tym, że $(A \times B) \cap (B \times A) = \big\{(2, 2), (2, 3), (3, 2), (3, 3)\big\}$.

Nim przejdziemy do sekcji z ogólnymi własnościami iloczynu kartezjańskiego, zaobserwujmy, że:

OBSERWACJA 4.18. Dla każdego zbioru A mamy $A \times \emptyset = \emptyset \times A = \emptyset$.

5. Własności iloczynu kartezjańskiego

TWIERDZENIE 4.19 (własności iloczynu kartezjańskiego). *Niech A, B, C, D będą dowolnymi zbiorami. Zachodzą następujące własności:*

1. *Jeśli $A \subseteq C$ i $B \subseteq D$, to $A \times B \subseteq C \times D$*

2a. $A \times (B \cup C) = (A \times B) \cup (A \times C)$

2b. $(B \cup C) \times A = (B \times A) \cup (C \times A)$

3a. $A \times (B \cap C) = (A \times B) \cap (A \times C)$

3b. $(B \cap C) \times A = (B \times A) \cap (C \times A)$

4a. $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$

4b. $(B \setminus C) \times A = (B \times A) \setminus (C \times A)$

5. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.

Dowód Twierdzenia 4.19 zostawiamy jako ćwiczenie. Podamy jedynie przykład prostego dowodu z iloczynem kartezjańskim.

Aby wykazać równość dwóch zbiorów, np. $A \times (B \cup C) = (A \times B) \cup (A \times C)$, należy wykazać dwa zawierania $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$ oraz $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$. Wykażemy dla przykładu zawieranie: $A \times (B \cap C) \subseteq A \times B$. W tym celu weźmy dowolną parę (x, y). Załóżmy, że:
(1) $(x, y) \in A \times (B \cap C)$;
z definicji iloczynu kartezjańskiego otrzymujemy:
(2) $x \in A \wedge y \in B \cap C$;
z definicji iloczynu zbiorów mamy:
(3) $x \in A \wedge (y \in B \wedge y \in C)$;
na mocy tautologii $[p \wedge (q \wedge r)] \iff [(p \wedge q) \wedge r]$, gdzie w podstawiamy w miejsce zmiennej zdaniowej p wartość $x \in A$, w miejsce q wartość $x \in B$, a w miejsce r wartość $x \in C$, otrzymujemy:
(4) $(x \in A \wedge y \in B) \wedge y \in C$;
na mocy tautologii $p \wedge q \implies q$, gdzie podstawiamy w miejsce zmiennej zdaniowej p wartość $x \in A \wedge y \in B$, a w miejsce zmiennej q wartość $y \in C$ otrzymujemy:
(5) $x \in A \wedge y \in B$;
ponownie z definicji iloczynu kartezjańskiego :
(6) $(x, y) \in A \times B$.

Pokazaliśmy, że $(x, y) \in A \times (B \cap C) \implies (x, y) \in A \times B$. To oznacza, że każdy element zbioru $A \times (B \cap C)$ jest także elementem zbioru $A \times B$, czyli $A \times (B \cap C) \subseteq A \times B$.

Uwaga 4.20 (bardzo ważne wiadomości z czwartego wykładu). Podczas czwartego wykładu dowiedzieliśmy się m.in.:

- co to jest zbiór potęgowy danego zbioru
- co to jest para nieuporządkowana, para uporządkowana i iloczyn kartezjański zbiorów
- jak definiuje się kwantyfikatory ograniczone
- jakie są prawa rachunku kwantyfikatorów.

ROZDZIAŁ 5

Ciągi skończone i relacje porządku

1. Ciągi skończone

W czasie wykładu 4. poznaliśmy definicję pary uporządkowanej (patrz: Definicja 4.14) oraz iloczynu kartezjańskiego dwóch zbiorów (patrz: Definicja 4.16). Rozszerzymy te definicje na n-kę uporządkowaną $(a_1, a_2, ..., a_n)$ i iloczyn kartezjański $X_1 \times X_2 \times ... \times X_n$. Rekurencyjnie definiujemy $X_1 \times ... \times X_n \times X_{n+1}$ jako $(X_1 \times ... \times X_n) \times X_{n+1}$. Dla przykładu $X \times Y \times Z$ oznacza $(X \times Y) \times Z$. Zatem elementy $X \times Y \times Z$ są postaci $((a, b), c)$. Zarazem elementy $X \times (Y \times Z)$ są postaci $(a, (b, c))$. Skorzystamy teraz z Twierdzenia 4.15, by wykazać ciąg równoważności:

$$((a,b),c) = ((x,y),z) \iff \Big((a,b) = (x,y) \wedge c = z\Big) \iff \Big(a = x \wedge b = y \wedge c = z\Big) \iff$$

$$\iff \Big(a = x \wedge (b,c) = (y,z)\Big) \iff (a,(b,c)) = (x,(y,z))).$$

Wykazaliśmy kluczową własność trójki uporządkowanej: trójka $((a, b), c)$ równa się $((x, y), z)$ wtedy i tylko wtedy, gdy odpowiednie współrzędne są równe. Dzieje się tak niezależnie od tego, czy trójki zapisujemy tak $((a, b), c)$, czy też tak $(a, (b, c))$. W celu redukcji liczby nawiasów wygodny jest zapis (a, b, c) zamiast $((a, b), c)$. Podobnie elementy iloczynu kartezjańskiego $X_1 \times X_2 \times ... \times X_n$ zapisujemy $(a_1, a_2, ..., a_n)$. Gdy $X_1 = X_2 = ... = X_n = X$, to iloczyn kartezjański $X_1 \times X_2 \times ... \times X_n$ zapisujemy skrótowo X^n.

Definicja 5.1 (ciąg n-wyrazowy elementów zbioru X). *Niech $n \in \mathbb{N}$. Ciągiem n-wyrazowym elementów zbioru X nazywamy dowolny element produktu X^n.*

2. Relacje

Dla uproszczenia zapisów do końca wykładu X, Y, Z będą dowolnymi niepustymi zbiorami.

Definicja 5.2 (relacja). *Relacją między elementami zbioru X, a elementami zbioru Y nazywamy dowolny podzbiór $\rho \subseteq X \times Y$.*

Jak widzimy, *relacja* to dowolny zbiór par uporządkowanych o poprzednikach ze zbioru X i następnikach ze zbioru Y. Na przykład zbiór pusty jest relacją. Dla uproszczenia notacji, dla $x \in X$, $y \in Y$ i relacji $\rho \subseteq X \times Y$, zamiast pisać $(x, y) \in \rho$ będziemy także używać notacji $x \rho y$.

Przykład 5.3.

- Niech $X = \{7, 8, 9\}, Y = \{1, 2, 3\}$. Relacją między elementami zbioru X a elementami zbioru Y jest na przykład $\rho = \{(7, 1), (7, 2), (7, 3)\}$.
- Niech $X = Y = \mathbb{N}$. Wówczas $\rho = \{(n, n) : n \in \mathbb{N}\}$ jest relacją.

W dalszej części będą bardziej interesujące dla nas relacje zawarte w produkcie tego samego zbioru, tzn. gdy $X = Y$. Dlatego wprowadźmy następującą definicję:

Definicja 5.4 (relacja w zbiorze X). *Relacją w zbiorze X nazywamy dowolny podzbiór $\rho \subseteq X \times X$.*

Przeanalizujmy bardziej szczegółowo następujące trzy relacje: relacja mniejszy lub równy dla liczb naturalnych, relacja podzielności liczb całkowitych oraz relacja zawierania zbiorów.

Przykład 5.5 (relacja mniejszy lub równy dla liczb naturalnych). Rozważmy relację ρ w zbiorze $\mathbb{N}$ określoną następująco: dla $x, y \in \mathbb{N}$

$$x \rho y \iff x \leq y$$

Innymi słowy: dwie liczby naturalne są ze sobą w relacji ρ, gdy pierwsza jest mniejsza od drugiej lub jej równa.

Zauważmy, że:

- dla każdej liczby $x \in \mathbb{N}$ mamy $x \leq x$
- dla dowolnych liczb $x, y, z \in \mathbb{N}$ mamy $(x \leq y \wedge y \leq z) \Rightarrow x \leq z$
- dla dowolnej liczby $x \in \mathbb{N}$ mamy $1 \leq x$
- dla dowolnych liczb $x, y \in \mathbb{N}$ mamy $x \leq y \vee y \leq x$
- dla dowolnych liczb $x, y \in \mathbb{N}$ mamy $(x \leq y \wedge y \leq x) \Rightarrow x = y$.

Przykład 5.6 (relacja podzielności liczb całkowitych). Rozważmy relację ρ w zbiorze $\mathbb{Z} \setminus \{0\}$ określoną następująco: dla $x, y \in \mathbb{Z} \setminus \{0\}$

$$x \rho y \iff x | y.$$

Innymi słowy: dwie całkowite liczby niezerowe są ze sobą w relacji ρ, gdy pierwsza jest dzielnikiem drugiej.

Zauważmy, że:

- dla każdej liczby $x \in \mathbb{Z} \setminus \{0\}$ mamy $x | x$
- dla dowolnych liczb $x, y, z \in \mathbb{Z} \setminus \{0\}$ mamy $(x | y \wedge y | z) \Rightarrow x | z$
- mamy $1 | -1$ oraz $-1 | 1$, ale $1 \neq -1$

- mamy $\neg(3|4)$ oraz $\neg(4|3)$
- dla każdej liczby $x \in \mathbb{Z} \setminus \{0\}$ mamy $1|x$ oraz $-1|x$.

PRZYKŁAD 5.7 (relacja inkluzji w zbiorze $\mathcal{P}(\mathbb{R})$). Spójrzmy na inkluzję z perspektywy podzbiorów zbioru $\mathbb{R}$, czyli dla $A, B \subseteq \mathbb{R}$ mamy, że $A \subseteq B$, gdy $(\forall x \in A)\ x \in B$. Inkluzja „$\subseteq$" jest podzbiorem produktu $\mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R})$, czyli jest relacją w zbiorze $\mathcal{P}(\mathbb{R})$. Zauważmy, że:

- dla każdego $A \in \mathcal{P}(\mathbb{R})$ mamy $A \subseteq A$
- dla każdych $A, B \in \mathcal{P}(\mathbb{R})$ mamy $(A \subseteq B \wedge B \subseteq A) \Rightarrow A = B$
- dla każdego $A \in \mathcal{P}(\mathbb{R})$ mamy $\emptyset \subseteq A$
- dla każdego $A \in \mathcal{P}(\mathbb{R})$ mamy $A \subseteq \mathbb{R}$
- dla zbiorów $A = \{1, 2, 3\}, B = \{2, 3, 4\}$ mamy $\neg(A \subseteq B)$ oraz $\neg(B \subseteq A)$
- dla każdych $A, B, C \in \mathcal{P}(\mathbb{R})$ mamy $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$.

Wobec powyższych przykładów warto więc wyodrębnić pewne własności relacji, gdyż jak widać, różne relacje mogą mieć podobne lub różne właściwości.

DEFINICJA 5.8 (rodzaje relacji). *Niech $\rho \subseteq X \times X$ będzie relacją w zbiorze X. Powiemy, że relacja ρ jest:*

(1) ***zwrotna****, jeśli* $(\forall x \in X)\ x\rho x$

(2) ***przechodnia****, jeśli* $(\forall x, y, z \in X)\ ((x\rho y \wedge y\rho z) \Rightarrow x\rho z)$

(3) ***symetryczna****, jeśli* $(\forall x, y \in X)\ x\rho y \Rightarrow y\rho x$

(4) ***słabo antysymetryczna****, jeśli* $(\forall x, y \in X)\ ((x\rho y \wedge y\rho x) \Rightarrow x = y)$

(5) ***spójna****, jeśli* $(\forall x, y \in X)\ (x\rho y \vee y\rho x)$

(6) ***przeciwzwrotna****, jeśli* $(\forall x \in X)\neg(x\rho x)$.

OBSERWACJA 5.9. Wobec powyższego:

- relacja $\leq$ dla liczb naturalnych jest: zwrotna, przechodnia, spójna i słabo antysymetryczna;
- relacja $|$ dla niezerowych liczb całkowitych jest: zwrotna, przechodnia, ale nie jest spójna ani słabo antysymetryczna;
- relacja $\subseteq$ w $\mathcal{P}(\mathbb{R})$ jest: zwrotna, przechodnia i słabo antysymetryczna, ale nie jest spójna.

OBSERWACJA 5.10. W matematyce na relacje patrzy się przeważnie zgodnie ze słownikowym znaczeniem tego słowa – jako na związek (relację, własność) dwóch obiektów, np.:

$$x \leq y, \quad 7|15, \quad A \subseteq B, \quad x \in \mathbb{R}.$$

Przy takim intuicyjnym podejściu nie sposób zdefiniować, czym w ogólności jest pojęcie relacji. Można definiować różne przykłady relacji, np. mniejsze lub równe, ale próba podania ogólnej definicji relacji sprowadza się do użycia innego słowa, np. związek czy własność. Gdybyśmy jednak drążyli dalej i pytali czym jest związek czy własność, to po pewnym czasie zabrnęlibyśmy w ślepy zaułek. Teoria mnogości ma rozwiązanie tego problemu. Definiuje się relację ρ jako zbiór wszystkich par (x, y) takich, że x jest w relacji z y, symbolicznie $x\rho y$. Dzięki temu pojęcie relacji zostaje zredukowane do pojęcia zbioru. Wówczas:

- relacja mniejsze bądź równe na $\mathbb{N}$, to zbiór $\{(x, y) \in \mathbb{N} \times \mathbb{N} : x \leq y\}$
- relacja podzielności na $\mathbb{Z} \setminus \{0\}$, to zbiór $\{(x, y) \in (\mathbb{Z} \setminus \{0\}) \times (\mathbb{Z} \setminus \{0\}) : x|y\}$
- relacja zawierania podzbiorów liczb rzeczywistych, to zbiór $\{(A, B) \in \mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R}) : A \subseteq B\}$.

3. Relacje porządkujące

Definicja 5.11 (częściowy porządek). *Relację $\leq$ w zbiorze X nazywamy częściowym porządkiem, jeśli jest relacją zwrotną, przechodnią i słabo antysymetryczną. Parę $(X, \leq)$ nazywamy zbiorem częściowo uporządkowanym albo krótko* – posetem.[1]

Uwaga 5.12. Użycie znanego symbolu $\leq$ nie jest tu przypadkowe, gdyż bardzo często myśląc o częściowym porządku wyobrażamy go sobie często właśnie jako klasyczną relację mniejsze lub równe.

Przykład 5.13. Dla dowolnego niepustego zbioru X relacja $\subseteq$ w zbiorze $\mathcal{P}(X)$ jest częściowym porządkiem. Zarazem relacja podzielności w liczbach całkowitych niezerowych nie jest częściowym porządkiem, bo nie jest relacją słabo antysymetryczną. Jednak ograniczona tylko do liczb naturalnych już jest relacją częściowego porządku.

W bardzo wielu sytuacjach dla częściowego porządku $\leq$ w zbiorze X rozważa się tzw. silny porządek $<$, określony następująco: $x < y \iff x \leq y \wedge x \neq y$ dla $x, y \in X$. Silny porządek jest przechodni i przeciwzwrotny. Odwrotnie, mając silny porządek $<$ w zbiorze X relacja $\leq$ określona formułą: $x \leq y \iff x < y \vee x = y$ jest częściowym porządkiem.

Uwaga 5.14. Intuicyjnie oczekuje się od częściowego porządku, że dwa dowolne elementy zbioru X winny być porównywalne (wynika to z naturalnego, acz mylnego patrzenia na częściowy porządek jak na znaną relację mniejszy/równy). Tak oczywiście nie jest – patrz przykład z relacją inkluzji.

Definicja 5.15 (liniowy porządek). *Relację $\leq$ w zbiorze X nazywamy liniowym porządkiem, jeśli jest spójnym częściowym porządkiem.*

[1] Po angielsku zbiór częściowo uporządkowany to *partially ordered set* – w skrócie *poset*.

PRZYKŁAD 5.16. Niech $X = \mathbb{R}^2$ i rozważmy relację $\preceq_L$ w zbiorze X określoną następująco: dla $(x_1, y_1), (x_2, y_2) \in X$:

$$(x_1, y_1) \preceq_L (x_2, y_2) \iff (x_1 < x_2 \vee (x_1 = x_2 \wedge y_1 \leq y_2))$$

(po prawej stronie równoważności występuje klasyczna relacja $\leq$). Można sprawdzić, że relacja $\preceq_L$ jest liniowym porządkiem.

4. Elementy wyróżnione

Analiza przykładów dotyczących relacji inkluzji, relacji podzielności w liczbach naturalnych czy też relacji $\leq$ w liczbach naturalnych prowadzi do kolejnej definicji.

DEFINICJA 5.17 (elementy wyróżnione). *Niech $(X, \leq)$ będzie zbiorem częściowo uporządkowanym. Niech $A \subseteq X$ i niech $a \in A$. Element a nazywamy:*

- *najmniejszym w zbiorze A, jeśli $(\forall x \in A)\ a \leq x$*
- *minimalnym w zbiorze A, jeśli $\neg((\exists x \in A) x < a)$*
- *największym w zbiorze A, jeśli $(\forall x \in A)\ x \leq a$*
- *maksymalnym w zbiorze A, jeśli $\neg((\exists x \in A)\ a < x)$.*

W szczególności, gdy $A = X$ to mówimy odpowiednio o elementach: najmniejszym, minimalnym, największym i maksymalnym.

Mimo że definicje elementu maksymalnego i największego oraz minimalnego i najmniejszego wydają się łudząco podobne – to niekoniecznie definiują ten sam obiekt! Istotne jest tu, że częściowy porządek nie musi być liniowy.

PRZYKŁAD 5.18. Rozważmy zbiór $\mathbb{N}$ z klasyczną relacją $\leq$. Oczywiście w $\mathbb{N}$ jest dokładnie jeden element najmniejszy: 1, dokładnie jeden element minimalny: 1 oraz nie ma elementów maksymalnych ani elementów największych.

Sformułujemy teraz kilka użytecznych faktów dotyczących elementów wyróżnionych.

STWIERDZENIE 5.19 (własności elementów wyróżnionych 1). *Niech $(X, \leq)$ będzie zbiorem częściowo uporządkowanym oraz $a \in X$. Wówczas:*

1. *Jeśli a jest elementem największym, to jest elementem maksymalnym.*
2. *Jeśli a jest elementem najmniejszym, to jest elementem minimalnym.*
3. *Jeśli relacja $\leq$ jest spójna, to każdy element maksymalny jest największy i każdy element minimalny jest najmniejszy.*

Dowód. Ad 1. Załóżmy, że a jest elementem największym, tj. $(\forall x \in X)\ x \leq a$. Przypuśćmy, że a nie jest elementem maksymalnym, oznacza to, że istnieje $x_0 \in X$ taki, że $a < x_0$. W szczególności skoro a jest największy, to $x_0 \leq a < x_0$, co daje sprzeczność (z przechodniością i przeciwzwrotnością relacji $<$).

Ad 2. Dowód analogiczny do dowodu w pkt. 1.

Ad 3. Załóżmy, że $\leq$ jest relacją spójną. Pokażemy, że każdy element maksymalny jest największy. Niech $a \in X$ będzie elementem maksymalnym, tj. $\neg((\exists x \in X)\ a < x)$. Z praw rachunku kwantyfikatorów mamy więc $(\forall x \in X)\ \neg(a < x)$, ale skoro $\leq$ jest spójna, to $\neg(a < x) \iff x \leq a$ czyli uzyskujemy:

$$(\forall x \in X)\ x \leq a$$

co oznacza, że a jest największy. Dowód w drugim przypadku jest analogiczny. □

Stwierdzenie 5.20 (własności elementów wyróżnionych 2). *Niech $(X, \leq)$ będzie zbiorem częściowo uporządkowanym. Jeśli element najmniejszy/największy istnieje to istnieje dokładnie jeden.*

Dowód. Niech $a, b \in X$ będą elementami największymi. Oznacza to, że $(\forall x \in X)\ x \leq a$ oraz $(\forall x \in X)\ x \leq b$. W szczególności stosując pierwszą własność dla $x = b$ i drugą własność dla $x = a$ mamy $b \leq a$ oraz $a \leq b$, co wobec słabej antysymetrii relacji $\leq$ daje, że $a = b$. Dla elementu najmniejszego dowód przebiega analogicznie. □

W czasie ćwiczeń, słuchacze poznają wiele przykładów zbiorów częściowo uporządkowanych (skończonych i nieskończonych) oraz nauczą się przedstawiać posety w bardziej czytelnej postaci: diagramu Hessego.

Uwaga 5.21 (bardzo ważne wiadomości z piątego wykładu). Podczas piątego wykładu dowiedzieliśmy się m.in.:

- co to są ciągi skończone elementów zbioru X
- co to jest relacja i jakie może mieć własności
- co to jest relacja częściowego porządku
- co to jest relacja liniowego porządku
- jakie elementy wyróżniamy w zbiorach częściowo uporządkowanych.

ROZDZIAŁ 6

Funkcje, operacje na funkcjach, obraz i przeciwobraz

1. Funkcja jako szczególny przykład relacji

Kolejnym, po relacjach porządkujących, szczególnie ważnym w matematyce rodzajem relacji jest funkcja.

DEFINICJA 6.1 (funkcja). *Niech X, Y będą dowolnymi zbiorami niepustymi. Relację $f \subseteq X \times Y$ nazywamy funkcją ze zbioru X w zbiór Y, gdy spełnia następujące warunki:*

$$(\forall x \in X)(\forall y, z \in Y)\ ((xfy \wedge xfz) \Rightarrow z = y)$$

oraz

$$\{x \in X \colon (\exists y \in Y)\ xfy\} = X,$$

innymi słowy – jeśli dla każdego $x \in X$ istnieje dokładnie jeden $y \in Y$ taki, że xfy.

OZNACZENIE 6.2. *Zdanie: f **jest funkcją ze zbioru X w zbiór Y** oznaczamy symbolicznie $f \colon X \to Y$. Zbiór X nazywamy dziedziną funkcji $f \colon X \to Y$ i często oznaczamy też symbolem* $\mathrm{dom}(f)$. *Jeśli $f \colon X \to Y$, to dla dowolnego $x \in X$ ten jedyny $y \in Y$, dla którego xfy, nazywamy wartością funkcji f w punkcie x i oznaczamy $f(x)$. Zbiór wszystkich funkcji ze zbioru X w zbiór Y oznaczamy symbolem Y^X.*

DEFINICJA 6.3 (zbiór wartości funkcji). *Niech $f \colon X \to Y$. Zbiorem wartości funkcji f nazywamy zbiór $f[X] = \{y \in Y \colon (\exists x \in X)\ y = f(x)\}$, który bywa również oznaczany symbolem* $\mathrm{rng}(f)$.

UWAGA 6.4. Dodatkowo dla dwu funkcji $f_1 \colon X_1 \to Y_1$ oraz $f_2 \colon X_2 \to Y_2$ równość $f_1 = f_2$ oznacza, że $X_1 = X_2$ oraz dla wszystkich $x \in X_1 = X_2$ mamy $f_1(x) = f_2(x)$.

PRZYKŁAD 6.5. Relacja ρ z Przykładu 5.3 nie jest funkcją, bo $(7,1), (7,2) \in \rho$ ale $1 \neq 2$.

PRZYKŁAD 6.6. Niech $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \colon xy = 1\}$. Wówczas f jest relacją. Przy tym f jest funkcją ze zbioru $\mathbb{R} \setminus \{0\}$ w $\mathbb{R}$, tj. $f \colon \mathbb{R} \setminus \{0\} \to \mathbb{R}$. Zauważmy przy okazji, że f jest również funkcją ze zbioru $\mathbb{R} \setminus \{0\}$ w zbiór $\mathbb{R} \setminus \{0\}$, tj. $f \colon \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$.

Uwaga 6.7. Zbiór Y „w który" działa funkcja $f\colon X \to Y$, nie musi być określony jednoznacznie! Istotne jest jedynie, by wszystkie wartości funkcji f były elementami zbioru Y.

Przykład 6.8. Niech $X' = Y = \mathbb{R}$ i niech $f = \{(x, y) \in \mathbb{R} \times \mathbb{R}\colon |x| = |y|\}$. Wówczas f nie jest funkcją, bo $(1, 1), (1, -1) \in f$.

Przypomnijmy jeszcze dwie definicje, z pewnością znane słuchaczom, ale sformułowane w powyższym języku będą dla nich prawdopodobnie nowe:

Definicja 6.9 (suriekcja). *Funkcję $f\colon X \to Y$ nazywamy suriekcją na Y, gdy $f[X] = Y$, innymi słowy: $(\forall y \in Y)(\exists x \in X)\ y = f(x)$. (W czasach szkolnych suriekcja była znana pod nazwą funkcja „na" i często tej nazwy będziemy używać.)*

Przykład 6.10. Niech $X = Y = \mathbb{R}$ i rozważmy funkcję $f\colon X \to Y$ określoną wzorem $f(x) = x^2$, dla $x \in \mathbb{R}$. Wówczas (łatwo sprawdzić) $f[X] = [0, \infty)$, zatem $f[X] \neq Y$, czyli f nie jest suriekcją na Y.

Przykład 6.11. Niech $X = \mathbb{R}, Y = [0, \infty)$ i rozważmy funkcję $f\colon X \to Y$ określoną wzorem $f(x) = x^2$, dla $x \in \mathbb{R}$. Wówczas $f[X] = [0, \infty) = Y$, zatem f jest suriekcją na Y.

Uwaga 6.12. Funkcje w powyższych przykładach są tym samym obiektem!

Definicja 6.13 (funkcja różnowartościowa). *Funkcję $f\colon X \to Y$ nazywamy różnowartościową (iniekcją lub $1-1$), gdy:*

$$(\forall x_1, x_2 \in X)\ x_1 \neq x_2 \Rightarrow (f(x_1) \neq f(x_2)).$$

Warunek definicyjny dla funkcji różnowartościowej, choć wydaje się naturalny, to nie jest wygodny w sprawdzaniu. Dlatego też sformułujmy następujące:

Stwierdzenie 6.14 (warunek równoważny różnowartościowości). *Funkcja $f\colon X \to Y$ jest różnowartościowa wtedy i tylko wtedy, gdy spełnia następujący warunek:*

$$(\forall x_1, x_2 \in X)\ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$

Dowód. Prostą konsekwencją zasady kontrapozycji (patrz: Twierdzenie 2.17) jest następująca równoważność: $(x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)) \iff (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$, skąd wynika podana w twierdzeniu charakteryzacja. □

Przykład 6.15. Niech $X = \mathbb{N}, Y = \mathbb{R}$ i rozważmy funkcję $f\colon X \to Y$ określoną wzorem $f(n) = \frac{3}{n}$, dla $n \in \mathbb{N}$. Pokażemy, że f jest różnowartościowa. Niech $n_1, n_2 \in \mathbb{N}$ i załóżmy, że $f(n_1) = f(n_2)$. Oznacza to, że $\frac{3}{n_1} = \frac{3}{n_2}$, skąd $n_1 = n_2$. Wobec Stwierdzenia 6.14, pokazaliśmy, że f jest różnowartościowa.

W powyższym przykładzie pojawiła się pewna szczególna klasa funkcji – tych określonych na zbiorze $\mathbb{N}$ liczb naturalnych. Zwyczajowo funkcje o dziedzinie będącej zbiorem $\mathbb{N}$ nazywamy *ciągami nieskończonymi*, najczęściej zamiast litery f używamy litery a oraz dla $n \in \mathbb{N}$ wartość tej funkcji w punkcie $n \in \mathbb{N}$ oznaczamy a_n. Sam zaś ciąg nieskończony oznaczamy $(a_1, a_2, ...)$ lub $(a_n)_{n\in\mathbb{N}}$. W szczególności, gdy $Y = \mathbb{R}$, to ciąg $a = (a_n)_{n\in\mathbb{N}}$ nazywamy nieskończonym ciągiem liczbowym. Na koniec tej sekcji przypomnimy jeszcze jedną znaną słuchaczom definicję związaną z pojęciami suriekcji i funkcji różnowartościowej.

DEFINICJA 6.16. *Funkcję $f\colon X \to Y$, która jest równocześnie suriekcją na Y i funkcją różnowartościową, nazywamy bijekcją na Y.*

2. Operacje na funkcjach

DEFINICJA 6.17 (obcięcie funkcji). *Niech $f\colon X \to Y$ oraz $A \subseteq X$. Obcięciem funkcji f do zbioru A nazywamy relację $f|A = \{(x, y) \in f\colon x \in A\} \subseteq A \times Y$.*

UWAGA 6.18. Obcięcie $f|A$ funkcji $f\colon X \to Y$ do zbioru $A \subseteq X$ też jest funkcją (tj. $f|A\colon A \to Y$). Istotnie, jeśli $(x, y), (x, z) \in f|A$, to w szczególności $(x, y), (x, z) \in f$, zatem skoro f jest funkcją, to $y = z$. Ponadto $\mathrm{dom}(f|A) = A$.

Drugą operacją jest złożenie dwu funkcji.

DEFINICJA 6.19 (złożenie funkcji). *Niech $f\colon X \to Y$ oraz $g\colon Y \to Z$ będą funkcjami. Złożeniem (superpozycją) funkcji g i f nazywamy funkcję: $g \circ f\colon X \to Z$ określoną następująco: dla dowolnego $x \in X$*

$$(g \circ f)(x) = g(f(x)).$$

STWIERDZENIE 6.20 (złożenie bijekcji). *Niech $f\colon X \to Y$ oraz $g\colon Y \to Z$ będą bijekcjami odpowiednio na Y i na Z. Wówczas funkcja $g \circ f\colon X \to Z$ jest bijekcją na Z.*

DOWÓD. Niech $f\colon X \to Y$ oraz $g\colon Y \to Z$ będą bijekcjami odpowiednio na Y i na Z i rozważmy funkcję $g \circ f\colon X \to Z$.

Niech $x_1, x_2 \in X$ i załóżmy, że $g(f(x_1)) = g(f(x_2))$. Ponieważ g jest różnowartościowa, to $f(x_1) = f(x_2)$ oraz skoro f jest różnowartościowa, to $x_1 = x_2$.

Niech $z \in Z$. Ponieważ g jest bijekcją na Z, to istnieje $y \in Y$ taki, że $g(y) = z$. Ponadto skoro f jest bijekcją na Y, to istnieje $x \in X$ taki, że $f(x) = y$. Zatem mamy też, że $g(f(x)) = g(y) = z$. □

Bezpośrednio z dowodu części $1 - 1$ powyżej wynika następujący:

Wniosek 6.21. *Niech $f\colon X \to Y$ oraz $g\colon Y \to Z$ będą funkcjami różnowartościowymi. Wówczas funkcja $g \circ f\colon X \to Z$ jest różnowartościowa, tj. złożenie funkcji różnowartościowych jest funkcją różnowartościową.*

Dla uproszczenia dalszych rozważań warto wyodrębnić pewną specjalną funkcję i nadać jej szczególną nazwę.

Definicja 6.22 (funkcja identyczność). *Niech X będzie dowolnym zbiorem. Funkcję $id_X\colon X \to X$ określoną następująco:*

$$id_X(x) = x, \text{ dla } x \in X$$

nazywamy funkcją identycznościową (tożsamościową) na zbiorze X.

Uwaga 6.23. Funkcja identycznościowa na zbiorze X jest bijekcją na X.

Każda funkcja $f\colon X \to Y$ jest w pewnym sensie parowaniem elementów zbioru X z elementami zbioru Y. Naturalne jest pytanie: czy to parowanie można odwrócić, tj. czy można parować elementy zbioru Y z elementami zbioru X mając jako narzędzie funkcję $f\colon X \to Y$. Okazuje się, że **nie zawsze funkcję można odwrócić**.

Definicja 6.24 (funkcja odwrotna). *Niech $f\colon X \to Y$ będzie funkcją **różnowartościową**. Funkcję $f^{-1}\colon f[X] \to X$ odwrotną do f określamy następująco: $f^{-1}(y) = x$, gdzie $y = f(x)$ dla $y \in f[X]$.*

Uwaga 6.25. Dzięki założeniu, że f jest funkcją różnowartościową, f^{-1} jest funkcją.

Stwierdzenie 6.26 (własności funkcji odwrotnej). *Załóżmy, że $f\colon X \to Y$ jest funkcją różnowartościową oraz $f^{-1}\colon f[X] \to X$ jest funkcją odwrotną do f. Wówczas $f \circ f^{-1}\colon f[X] \to Y$, $f^{-1} \circ f\colon X \to X$ są takie, że $(f \circ f^{-1})(y) = y$, $(f^{-1} \circ f)(x) = x$ dla $y \in f[X], x \in X$. Przy tym $f^{-1}(y) = x \iff y = f(x)$.*

Dowód. Niech $y \in f[X]$. Wówczas istnieje $x \in X$ taki, że $y = f(x)$ (taki x istnieje dokładnie jeden, bo funkcja f jest różnowartościowa). Mamy, że $(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y$. Dowód drugiej części przebiega podobnie i zostawiamy go jako ćwiczenie dla słuchaczy. □

Obserwacja 6.27. Dodatkowo możemy napisać, że dla funkcji różnowartościowej $f\colon X \to Y$ i funkcji do niej odwrotnej $f^{-1}\colon f[X] \to X$ mamy $f \circ f^{-1} = id_{f[X]}$, $f^{-1} \circ f = id_X$.

Dla lepszego zobrazowania powyższych pojęć rozważmy następujący przykład.

Przykład 6.28. Niech $f\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ będzie określona wzorem: dla $(n, m) \in \mathbb{Z} \times \mathbb{Z}$

$$f((n, m)) = n + m$$

(w tym przypadku dziedziną funkcji f jest zbiór $\mathbb{Z}\times\mathbb{Z}$ wszystkich par uporządkowanych o poprzedniku i następniku będącym liczbą całkowitą). Zauważmy, że:

- f nie jest różnowartościowa, bo $f((-1,1)) = 0 = f((-2,2))$
- f jest na $\mathbb{Z}$, bo dla każdego $w \in \mathbb{Z}$ mamy $w = f((0,w))$
- funkcja $f|\mathbb{N}\times\mathbb{N}$ nie jest różnowartościowa
- funkcja $f|\mathbb{N}\times\mathbb{N}$ nie jest funkcją na $\mathbb{Z}$ ale też nie jest funkcją na $\mathbb{N}$.

Przy tym, skoro $f\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ nie jest różnowartościowa, to f nie jest bijekcją i nie istnieje funkcja odwrotna do f.

STWIERDZENIE 6.29. *Niech $f : X \to Y$ będzie funkcją. Wówczas f jest bijekcją wtedy i tylko wtedy, gdy istnieje funkcja $g : Y \to X$ taka, że $f \circ g = id_Y$ i $g \circ f = id_X$.*

DOWÓD. Załóżmy, że f jest bijekcją. Skoro f jest różnowartościowa, to istnieje do niej funkcja odwrotna $f^{-1} : f[X] \to Y$. Ponieważ f jest na Y, to $f[X] = Y$, czyli f^{-1} działa z Y w X. Na mocy Stwierdzenia 6.26 mamy $f \circ f^{-1} = id_Y$, $f^{-1} \circ f = id_X$, czyli teza zachodzi dla $g = f^{-1}$.

Załóżmy, że istnieje funkcja $g : Y \to X$ taka, że $f \circ g = id_Y$ i $g \circ f = id_X$. Pokażemy, że f jest $1-1$ i na Y. Załóżmy, że $f(x_1) = f(x_2)$. Wtedy $g(f(x_1)) = g(f(x_2))$. Ale $g(f(x)) = x$ dla każdego $x \in X$. Zatem $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. To dowodzi, że f jest $1-1$. Niech $y \in Y$. Wtedy $f(g(y)) = id_Y(y) = y$. Niech $x_0 = g(y)$. Wówczas $f(x_0) = y$. Czyli f jest na Y. □

Okazuje się, że jedyną funkcją g spełniającą warunki $f \circ g = id_Y$ i $g \circ f = id_X$ jest funkcja f^{-1}.

3. Obraz i przeciwobraz zbioru

Poznaliśmy już pojęcie funkcji i kilku operacji z nim związanych. Dodatkowymi dwoma pojęciami są obraz i przeciwobraz zbioru. Do końca tej sekcji niech X, Y, Z będą niepustymi zbiorami.

DEFINICJA 6.30 (obraz zbioru wyznaczony przez funkcję). *Niech $f\colon X \to Y$ oraz $A \subseteq X$. Obrazem zbioru A wyznaczonym przez funkcję f nazywamy zbiór $f[A] = \{y \in Y\colon (\exists x \in A)\ y = f(x)\} \subseteq Y$.*

UWAGA 6.31. Zauważmy, że notacja $f[X]$ jest zgodna z definicją obrazu zbioru wyznaczonego przez funkcję f dla $A = X$.

PRZYKŁAD 6.32. Rozważmy funkcję $f\colon \mathbb{Z} \to \mathbb{R}$ określoną wzorem $f(x) = \frac{x}{2}$ dla $x \in \mathbb{Z}$. Niech $A = \{2, 4, 6, ...\}$, wówczas obrazem zbioru A wyznaczonym przez funkcję f jest zbiór $f[A] = \mathbb{N}$.

Definicja 6.33 (przeciwobraz zbioru wyznaczony przez funkcję). *Niech $f\colon X \to Y$ oraz $B \subseteq Y$. Przeciwobrazem zbioru B wyznaczonym przez funkcję f nazywamy zbiór*

$$f^{-1}[B] = \{x \in X\colon f(x) \in B\} \subseteq X.$$

Uwaga 6.34. Symbol f^{-1} pojawił się już jako oznaczenie funkcji odwrotnej (o ile ona istnieje!). W definicji 6.33 zapis $f^{-1}[B]$ nie ma nic wspólnego z funkcją odwrotną, gdyż ta dla funkcji f może nie istnieć. Jednak, kiedy dla funkcji f będzie istniała funkcja odwrotna, to symbol ten okaże się uzasadniony. Wrócimy do tego problemu na przyszłym wykładzie.

Analizowanie własności przeciwobrazu zaczniemy od oczywistej obserwacji.

Obserwacja 6.35. Niech $f\colon X \to Y$. Wówczas $f^{-1}[Y] = X$.

Dowód. Inkluzja $f^{-1}[Y] \subseteq X$ wynika bezpośrednio z definicji przeciwobrazu zbioru. Dla dowodu przeciwnej inkluzji, niech $x \in X$, wówczas $f(x) \in Y$, zatem z definicji przeciwobrazu $x \in f^{-1}[Y]$. □

Przykład 6.36. Niech $f\colon \mathbb{R} \to \mathbb{R}$ będzie określona wzorem $f(x) = x^2$ dla $x \in \mathbb{R}$. Niech $B_1 = (-1, 0), B_2 = [1, 4]$, będą przedziałami. Wówczas $f^{-1}[B_1] = \emptyset, f^{-1}[B_2] = [-2, -1] \cup [1, 2]$.

Uwaga 6.37 (bardzo ważne wiadomości z szóstego wykładu). Podczas szóstego wykładu dowiedzieliśmy się m.in.:

- co to jest funkcja
- co to jest funkcja różnowartościowa i na oraz bijekcja
- co to jest obcięcie funkcji, złożenie funkcji, funkcja odwrotna
- co to jest obraz i przeciwobraz zbioru przez funkcję.

ROZDZIAŁ 7

Własności obrazu i przeciwobrazu

1. Własności obrazu zbioru

Przedstawimy teraz kilka podstawowych własności obrazów zbiorów przez funkcję.

TWIERDZENIE 7.1 (własności obrazów). *Niech $f\colon X \to Y$ oraz $A_1, A_2 \subseteq X$. Zachodzą następujące własności:*

1. *Jeśli $A_1 \subseteq A_2$, to $f[A_1] \subseteq f[A_2]$*
2. *$f[A_1 \cup A_2] = f[A_1] \cup f[A_2]$*
3. *$f[A_1 \cap A_2] \subseteq f[A_1] \cap f[A_2]$.*

DOWÓD. Ad. 1. Załóżmy, że $A_1 \subseteq A_2$ i niech $y \in f[A_1]$. Oznacza to, że istnieje $x \in A_1$ taki, że $y = f(x)$. Skoro $x \in A_1 \subseteq A_2$, to $x \in A_2$. Zatem $y \in f[A_2]$.

Ad 2. Niech $y \in f[A_1 \cup A_2]$, oznacza to, że istnieje $x \in A_1 \cup A_2$ taki, że $y = f(x)$. Jeśli $x \in A_1$, to wtedy $y = f(x) \in f[A_1]$, zaś gdy $x \in A_2$, to $y = f(x) \in f[A_2]$. Niniejszym $y \in f[A_1] \cup f[A_2]$. Zauważmy, że oczywiście $A_1 \subseteq A_1 \cup A_2$ oraz $A_2 \subseteq A_1 \cup A_2$. Stąd wobec udowodnionej już własności 1. mamy, że $f[A_1] \subseteq f[A_1 \cup A_2]$ oraz $f[A_2] \subseteq f[A_1 \cup A_2]$. Stąd $f[A_1] \cup f[A_2] \subseteq f[A_1 \cup A_2]$.

Ad 3. Niech $y \in f[A_1 \cap A_2]$, oznacza to, że istnieje $x \in A_1 \cap A_2$ taki, że $y = f(x)$. W szczególności skoro $x \in A_1$, to $y = f(x) \in f[A_1]$ oraz skoro $x \in A_2$, to $y = f(x) \in f[A_2]$. Ostatecznie $y \in f[A_1] \cap f[A_2]$. □

UWAGA 7.2. Zauważmy, że w ogólności inkluzja w przeciwną stronę niż ta w Twierdzeniu 7.1 punkt 3. nie musi zachodzić. Wystarczy rozważyć następującą funkcję oraz zbiory: $f\colon \mathbb{R} \to \mathbb{R}$ określoną wzorem $f(x) = 1$ dla $x \in \mathbb{R}$ oraz przedziały $A_1 = (0, 1), A_2 = (2, 3)$.

Kolejne twierdzenie opisuje obraz zbioru przez funkcję będącą złożeniem dwu innych.

TWIERDZENIE 7.3 (obraz zbioru przez superpozycję). *Niech $f\colon X \to Y$, $g\colon Y \to Z$ oraz $A \subseteq X$. Zachodzi następująca równość:*

$$(g \circ f)[A] = g[f[A]].$$

DOWÓD. Dla wykazania równości dwu zbiorów $(g \circ f)[A]$ oraz $g[f[A]]$ pokażemy inkluzję w dwie strony.

„$\subseteq$” Niech $z \in (g \circ f)[A]$, oznacza to, że istnieje $x \in A$ taki, że $z = (g \circ f)(x) = g(f(x))$. W szczególności skoro $x \in A$, to $f(x) \in f[A]$. W konsekwencji $z = g(f(x)) \in g[f[A]]$.
„$\supseteq$” Niech $z \in g[f[A]]$, oznacza to, że istnieje $y \in f[A]$ taki, że $z = g(y)$. Ale skoro $y \in f[A]$, to istnieje $x \in A$ taki, że $y = f(x)$. Ostatecznie $z = g(y) = (g(f(x)) = (g \circ f)(x) \in (g \circ f)[A]$. □

Na koniec warto zauważyć jeszcze pewną zależność między operacją obrazu zbioru wyznaczonego przez funkcję a jej obcięciem, mianowicie:

Stwierdzenie 7.4. *Niech $f\colon X \to Y$ oraz $A \subseteq X$. Wówczas $f[A] = (f|A)[A]$.*

Uwaga 7.5. Z wcześniejszych wyników wiadomo, że obcięcie funkcji jest też funkcją, zatem zapis $(f|A)[A]$ jest uprawniony.

Dowód. Pamiętajmy, że jeśli $f\colon X \to Y$ oraz $A \subseteq X$, to $f|A\colon A \to Y$. Mamy:

$$(f|A)[A] = \{y \in Y\colon (\exists x \in A)\ y = (f|A)(x)\}.$$

W szczególności dla $x \in A$ mamy $(f|A)(x) = f(x)$. Zatem

$$\Big\{y \in Y\colon (\exists x \in A)\ y = (f|A)(x)\Big\} = \Big\{y \in Y\colon (\exists x \in A)\ y = f(x)\Big\} = f[A].$$

□

2. Własności przeciwobrazów

Przedstawimy teraz kilka własności przeciwobrazów.

Twierdzenie 7.6 (własności przeciwobrazów). *Niech $f\colon X \to Y$ oraz $B_1, B_2 \subseteq Y$. Zachodzą następujące własności:*

1. *Jeśli $B_1 \subseteq B_2$, to $f^{-1}[B_1] \subseteq f^{-1}[B_2]$*
2. *$f^{-1}[B_1 \cup B_2] = f^{-1}[B_1] \cup f^{-1}[B_2]$*
3. *$f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$.*

Dowód. Ad 1. Załóżmy, że $B_1 \subseteq B_2$ i niech $x \in f^{-1}[B_1]$. Oznacza to, że $f(x) \in B_1$. Skoro $f(x) \in B_1 \subseteq B_2$, to $f(x) \in B_2$. Zatem $x \in f^{-1}[B_2]$.

Ad 2. Niech $x \in f^{-1}[B_1 \cup B_2]$, oznacza to, że $f(x) \in B_1 \cup B_2$. Jeśli $f(x) \in B_1$ to wtedy $x \in f^{-1}[B_1]$, zaś gdy $f(x) \in B_2$, to $x \in f^{-1}[B_2]$. Niniejszym $x \in f^{-1}[B_1] \cup f^{-1}[B_2]$. Zauważmy, że $B_1 \subseteq B_1 \cup B_2$ oraz $B_2 \subseteq B_1 \cup B_2$. Stąd wobec udowodnionej już własności 1. mamy, że $f^{-1}[B_1] \subseteq f^{-1}[B_1 \cup B_2]$ oraz $f^{-1}[B_2] \subseteq f^{-1}[B_1 \cup B_2]$. Stąd $f^{-1}[B_1] \cup f^{-1}[B_2] \subseteq f^{-1}[B_1 \cup B_2]$.

Ad 3. Inkluzja „⊆” wynika znów z udowodnionej 1. (zostawiamy to jako ćwiczenie). Niech więc $x \in f^{-1}[B_1] \cap f^{-1}[B_2]$. Oznacza to, że $x \in f^{-1}[B_1]$ i $x \in f^{-1}[B_2]$ tj. $f(x) \in B_1$ i $f(x) \in B_2$. Ostatecznie $f(x) \in B_1 \cap B_2$ więc $x \in f^{-1}[B_1 \cap B_2]$. □

Następne twierdzenie opisuje przeciwobraz zbioru przez funkcję będącą złożeniem dwóch innych.

Twierdzenie 7.7 (przeciwobraz zbioru przez superpozycję). *Niech $f\colon X \to Y$, $g\colon Y \to Z$. Dla każdego $B \subseteq Z$ zachodzi następująca równość:*

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

Dowód. Dla wykazania równości dwu zbiorów $(g \circ f)^{-1}[B]$ oraz $f^{-1}[g^{-1}[B]]$ pokażemy inkluzję w dwie strony.
„⊆” Niech $x \in (g \circ f)^{-1}[B]$, oznacza to, że $(g \circ f)(x) = g(f(x)) \in B$. Stąd $f(x) \in g^{-1}[B]$ zatem $x \in f^{-1}[g^{-1}[B]]$.
„⊇” Niech $x \in f^{-1}[g^{-1}[B]]$, oznacza to, że $f(x) \in g^{-1}[B]$ czyli $g(f(x)) \in B$ tj. $x \in (g \circ f)^{-1}[B]$. □

Mając już wprowadzone dwa podobne pojęcia: obrazu i przeciwobrazu, możemy sformułować pewne zależności między nimi.

Twierdzenie 7.8 (zależność między obrazem a przeciwobrazem). *Niech $f\colon X \to Y$ oraz $A \subseteq X$ i $B \subseteq Y$. Zachodzą następujące własności:*
1. $A \subseteq f^{-1}[f[A]]$. Dodatkowo, jeśli f jest różnowartościowa, to inkluzja staje się równością.
2. $f[f^{-1}[B]] \subseteq B$. Dodatkowo, jeśli $B \subseteq f[X]$ (lub też, gdy f jest suriekcją na Y), to inkluzja staje się równością.

Dowód. Ad 1. Wykażemy najpierw pierwszą część tezy. Niech $x \in A$, wówczas $f(x) \in f[A]$, więc z definicji przeciwobrazu $x \in f^{-1}[f[A]]$. Dla dowodu drugiej części tezy wystarczy pokazać, że inkluzja $f^{-1}[f[A]] \subseteq A$ wynika z różnowartościowości funkcji f. Istotnie, załóżmy, że f jest różnowartościowa i niech $x \in f^{-1}[f[A]]$. Oznacza to, że $f(x) \in f[A]$, czyli istnieje $x' \in A$ taki, że $f(x) = f(x')$. Ale skoro funkcja f jest różnowartościowa, to jest to jedynie możliwe, gdy $x = x'$, zatem $x \in A$.

Ad 2. Wykażemy najpierw pierwszą część tezy. Niech $y \in f[f^{-1}[B]]$, wówczas istnieje $x \in f^{-1}[B]$ taki, że $y = f(x)$. W szczególności skoro $x \in f^{-1}[B]$, to $f(x) \in B$, zatem $y = f(x) \in B$. Dla dowodu drugiej części tezy wystarczy pokazać, że inkluzja $B \subseteq f[f^{-1}[B]]$ wynika z inkluzji $B \subseteq f[X]$ (lub suriektywności na Y funkcji f). Istotnie, załóżmy, że $B \subseteq f[X]$ i niech $y \in B$. Skoro $B \subseteq f[X]$ (analogicznie gdy f jest suriekcją na Y), to wartość y jest *realizowana*, tj. istnieje $x \in X$ taki, że $y = f(x)$. Stąd w szczególności $x \in f^{-1}[B]$, zatem ostatecznie $y \in f[f^{-1}[B]]$. □

Na koniec tej sekcji wrócimy do Uwagi 6.34. Dla funkcji różnowartościowej $f\colon X \to Y$, relacja odwrotna f^{-1} jest funkcją oraz $f \circ f^{-1} = id_{f[X]}, f^{-1} \circ f = id_X$ (patrz: Stwierdzenie 6.26). Symbol $f^{-1}[B]$ dla $B \subseteq Y$ może się więc kojarzyć z obrazem zbioru B przez funkcję f^{-1}. Okazuje się, że intuicja ta jest zgodna z prawdą.

STWIERDZENIE 7.9 (związek przeciwobrazu z funkcją odwrotną). *Niech $f\colon X \to Y$ będzie funkcją różnowartościową oraz niech $B \subseteq f[X]$. Wówczas przeciwobraz zbioru B przez funkcję f jest równy obrazowi zbioru B przez funkcję f^{-1}:*

$$f^{-1}[B] = (f^{-1})[B].$$

DOWÓD. Załóżmy, że $f\colon X \to Y$ jest funkcją różnowartościową oraz $B \subseteq f[X]$. Dla dowodu równości wykażemy inkluzję w dwie strony:
„$\subseteq$" niech $x \in f^{-1}[B]$, oznacza, że $y = f(x) \in B$. W szczególności z postaci funkcji odwrotnej do f mamy, że $x = f^{-1}(y)$. Skoro $y \in B$, to $x \in (f^{-1})[B]$.
„$\supseteq$" niech $x \in (f^{-1})[B]$, oznacza, że istnieje $y \in B$ taki, że $x = f^{-1}(y)$. W szczególności skoro $f(x) = y$ oraz $y \in B$ to $x \in f^{-1}[B]$. □

UWAGA 7.10 (bardzo ważne wiadomości z siódmego wykładu). Podczas siódmego wykładu dowiedzieliśmy się m.in.:

- jakie są własności operacji brania obrazu i przeciwobrazu
- jaki jest związek między funkcją odwrotną a braniem przeciwobrazu.

ROZDZIAŁ 8

Relacje równoważności i ich zastosowanie

Przedstawiliśmy dotąd przykłady pewnych szczególnych rodzajów relacji: relacje porządku i funkcje. Skupimy się teraz na innym bardzo ważnym rodzaju – relacjach równoważności. Wprowadzenie odpowiednich pojęć poprzedzimy dwoma przykładami.

PRZYKŁAD 8.1. Niech $X = \mathbb{N}$ i rozważmy relację ρ w zbiorze X określoną następująco: dla $n, m \in \mathbb{N}$

$$n\rho m \iff 3|n-m.$$

Innymi słowy, dwie liczby naturalne są ze sobą w relacji ρ kiedy dają tę samą resztę z dzielenia przez 3. Zauważmy, że relacja ρ definiuje pewnego rodzaju podobieństwo: *dwie liczby naturalne są* ***podobne****, gdy dają tę samą resztę z dzielenia przez* 3. „Podobieństwo" jest zwrotne (obiekt jest podobny sam do siebie), symetryczne (jeśli pierwszy obiekt jest podobny do drugiego, to drugi do pierwszego też) i przechodnie (jeśli pierwszy obiekt jest podobny do drugiego i drugi do trzeciego, to pierwszy i trzeci też są podobne).

PRZYKŁAD 8.2. Niech $X = \mathbb{R}^2$ i rozważmy relację ρ w zbiorze X określoną następująco: dla $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$

$$(x_1, y_1)\rho(x_2, y_2) \iff x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

Innymi słowy, dwa punkty na płaszczyźnie $\mathbb{R}^2$ są ze sobą w relacji ρ (są **podobne**), gdy są tak samo odległe od punktu $(0, 0)$.

1. Relacja równoważności

Niech X będzie niepustym zbiorem.

DEFINICJA 8.3 (relacja równoważności). *Relację ρ w zbiorze X nazywamy relacją równoważności, jeśli jest zwrotna, symetryczna i przechodnia, tzn.:*

(1) zwrotna, jeśli $(\forall x \in X)\ x\rho x$

(2) przechodnia, jeśli $(\forall x, y, z \in X)\ ((x\rho y \wedge y\rho z) \Rightarrow x\rho z)$

(3) symetryczna, jeśli $(\forall x, y \in X)\ (x\rho y \Rightarrow y\rho x)$.

Przykład 8.4. Najprostszym przykładem relacji równoważności jest relacja równości. Ponadto, łatwo sprawdzić, że relacje z Przykładów 8.1, 8.2 są relacjami równoważności.

Przykład 8.5. Relacja $\leq$ w zbiorze $\mathbb{N}$ nie jest relacją równoważności, bo nie jest symetryczna.

Przykład 8.6. Niech $X = \mathbb{R} \setminus \{0\}$. Rozważmy relację ρ w zbiorze X określoną następująco: dla $x, y \in X$

$$x \rho y \iff xy \geq 0.$$

Pokażemy, że ρ jest relacją równoważności.

Zwrotność: Niech $x \in X$, oczywiście $x^2 \geq 0$, zatem $x \rho x$.

Symetria: Niech $x, y \in X$ i załóżmy, że $x \rho y$. Oznacza to, że $xy \geq 0$. Oczywiście oznacza to też, że $yx \geq 0$, czyli $y \rho x$.

Przechodniość: Niech $x, y, z \in X$ i załóżmy, że $x \rho y$ oraz $y \rho z$. Oznacza to, że $xy \geq 0$ oraz $yz \geq 0$. W szczególności (mnożąc stronami) $xy^2z \geq 0$, co wobec dodatniości y^2 oznacza, że $xz \geq 0$. Ostatecznie mamy $x \rho z$.

Wobec powyższego ρ jest relacją równoważności. Warto przy tym zauważyć, że dwie niezerowe liczby rzeczywiste są ze sobą w relacji ρ, jeśli są tego samego znaku. Oznacza to: w relacji ρ *bycie podobnym* oznacza *bycie tego samego znaku*; innymi słowy – są dwa różne typy liczb rzeczywistych niezerowych przy relacji ρ. Wrócimy do tej obserwacji później.

Dla ustalonej relacji równoważności ρ w zbiorze X i ustalonego $x \in X$, zgrupujemy obiekty podobne do x w sensie relacji ρ; wprowadzimy pojęcie klasy abstrakcji.

Definicja 8.7 (klasa abstrakcji). *Niech ρ będzie relacją równoważności w zbiorze X. Dla każdego $x \in X$ klasą abstrakcji elementu x w relacji równoważności ρ nazywamy zbiór wszystkich elementów zbioru X, które są z x w relacji, tj. zbiór*

$$[x]_\rho = \{y \in X : x \rho y\}.$$

Uwaga 8.8. Skoro ρ jest relacją równoważności, to w szczególności jest symetryczna, zatem klasę abstrakcji elementu x można równoważnie opisać formułą

$$[x]_\rho = \{y \in X : y \rho x\}.$$

Przy tym ρ jest zwrotna, więc dla każdego $x \in X$ mamy $x \rho x$. Zatem też $x \in [x]_\rho$ dla każdego $x \in X$.

Przykład 8.9. Rozważmy relację ρ z Przykładu 8.6. Wówczas mamy:

$$[1]_\rho = (0, \infty)$$

$$[2]_\rho = (0, \infty)$$

$$[-1]_\rho = (-\infty, 0).$$

Oznaczenie 8.10. *Dla relacji równoważności ρ w zbiorze X zbiór wszystkich klas abstrakcji tej relacji oznaczamy X/ρ, tj.*

$$X/\rho = \{[x]_\rho \colon x \in X\}.$$

Przykład 8.11. Łatwo zauważyć, że $X/\rho = \{(0, \infty), (-\infty, 0)\}$ dla relacji ρ z Przykładu 8.6.

Sformułujemy teraz kilka istotnych własności klas abstrakcji relacji równoważności, które w przyszłości okażą się też być własnościami je charakteryzującymi.

Twierdzenie 8.12 (równość klas abstrakcji). *Niech ρ będzie relacją równoważności w zbiorze X. Wówczas*:

$$(\forall x, y \in X)\ ([x]_\rho = [y]_\rho \iff x \rho y).$$

Dowód. Niech $x, y \in X$.
„$\Rightarrow$” Załóżmy, że $[x]_\rho = [y]_\rho$. Wobec udowodnionej już własności mamy $x \in [x]_\rho = [y]_\rho$, czyli $x \in [y]_\rho$. Zatem $x \rho y$.
„$\Leftarrow$” Załóżmy, że $x \rho y$. Załóżmy, że $z \in [x]_\rho$, wówczas $x \rho z$. Skoro też $x \rho y$, to z przechodniości i symetrii relacji ρ mamy $z \rho y$, czyli $z \in [y]_\rho$. Z dowolności z mamy więc $[x]_\rho \subseteq [y]_\rho$. Analogicznie wykazujemy przeciwną inkluzję. □

Twierdzenie 8.12 mówi też, że dla każdego $x \in X$ klasa abstrakcji $[x]_\rho$ jest też wyznaczana przez dowolny $y \in X$ taki, że $x \rho y$. Wprowadźmy następujące pojęcie:

Definicja 8.13. *Niech $x \in X$. Reprezentantem klasy abstrakcji $[x]_\rho$ nazywamy dowolny element $y \in X$ taki, że $[y]_\rho = [x]_\rho$.*

Wnioskiem z Twierdzenia 8.12 jest też:

Wniosek 8.14. *Niech ρ będzie relacją równoważności w zbiorze X. Wówczas*:

$$(\forall x, y \in X)\ ([x]_\rho = [y]_\rho \vee [x]_\rho \cap [y]_\rho = \emptyset).$$

Dowód. Niech $x, y \in X$. Jeśli $[x]_\rho \cap [y]_\rho = \emptyset$ to teza wniosku zachodzi. Załóżmy więc, że $[x]_\rho \cap [y]_\rho \neq \emptyset$, oznacza to, że istnieje $z \in [x]_\rho \cap [y]_\rho$. W szczególności $z \rho x$ i $z \rho y$, skąd wobec Twierdzenia 8.12 $[x]_\rho = [z]_\rho = [y]_\rho$. □

Powyższe obserwacje pozwalają stwierdzić, że rodzina zbiorów X/ρ ma następujące własności:

- każdy element zbioru X należy do pewnego elementu rodziny X/ρ, zatem rodzina X/ρ sumuje się do X
- elementy rodziny X/ρ są niepuste, parami rozłączne (powtarzające się elementy można pominąć).

WNIOSEK 8.15. *Każda relacja równoważności w zbiorze X generuje rodzinę X/ρ podzbiorów zbioru X (tzw. **rozbicie zbioru** X), której elementy są niepuste, parami rozłączne i sumują się do X.*

Okazuje się, że powyższą obserwację można odwrócić – zachodzi mianowicie następujące:

TWIERDZENIE 8.16. *Niech $\mathcal{P}$ będzie rozbiciem zbioru X, tj. rodziną podzbiorów zbioru X, której elementy są niepuste, parami rozłączne i sumują się do X. Wówczas istnieje dokładnie jedna relacja równoważności ρ w zbiorze X taka, że $X/\rho = \mathcal{P}$.*

DOWÓD. Określmy relację $\rho \subseteq X \times X$ następująco: dla $x, y \in X$

$$x \rho y \iff (\exists P \in \mathcal{P})\ x, y \in P.$$

Formalny dowód, że tak zdefiniowana relacja jest tą szukaną pozostawiamy czytelnikowi. □

Powyższe Twierdzenie i Wniosek połączone noszą nazwę **zasady abstrakcji**.

TWIERDZENIE 8.17 (zasada abstrakcji). *Każda relacja równoważności w zbiorze X generuje rozbicie zbioru X oraz każde rozbicie zbioru X definiuje relację równoważności w zbiorze X.*

Na koniec tej sekcji wrócimy na chwilę do Przykładu 8.2.

PRZYKŁAD 8.18. Rozważmy relację równoważności ρ w zbiorze $\mathbb{R}^2$ określoną następująco: dla $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$

$$(x_1, y_1) \rho (x_2, y_2) \iff x_1^2 + y_1^2 = x_2^2 + y_2^2.$$

Zauważmy, że $[(1,1)]_\rho = \{(x, y) \in \mathbb{R}^2 \colon x^2 + y^2 = 1^2 + 1^2\}$, co oznacza, że $[(1,1)]_\rho$ jest okręgiem o środku w punkcie $(0,0)$ i promieniu $\sqrt{2}$. Łatwo zauważyć, że każda klasa abstrakcji, poza $[(0,0)]_\rho = \{(0,0)\}$ jest okręgiem o pewnym promieniu i środku w punkcie $(0,0)$. Stąd $\mathbb{R}^2/\rho = \{S((0,0), r) \colon r > 0\} \cup \{(0,0)\}$, gdzie $S((0,0), r) = \{(x, y) \in \mathbb{R}^2 \colon x^2 + y^2 = r^2\}$.

2. Praktyczne wykorzystanie relacji równoważności

2.1. Konstrukcja liczb całkowitych. Teraz na gruncie teorii mnogości, mając już zbiór liczb naturalnych $\mathbb{N}$, skonstruujemy liczby całkowite. Mamy już liczby całkowite dodatnie. Potrzebujemy

zdefiniować liczbę zero i liczby $-n$ dla $n \in \mathbb{N}$. Musimy to zrobić, używając jedynie środków teorii mnogości.

W zbiorze $\mathbb{N} \times \mathbb{N}$ rozważmy relację określoną następująco: dla $(m,n),(k,l) \in X$

$$(m,n)\rho(k,l) \iff m+l = k+n.$$

Intuicyjnie para (m,n) jest podobna do pary (k,l), jeżeli równe są różnice[1]: $m-n$ i $k-l$. Okazuje się, że ρ jest relacją równoważności.

O parze (m,n) będziemy myśleć, jako o liczbie $m-n$. Dla przykładu:

- (32,8) to liczba $32-8=24$
- (1,5) to liczba $1-5=-4$
- (7,7) to liczba $7-7=0$.

Zauważmy pewien problem związny z takim myśleniem. Pary (32,8) i (25,1) generują tę samą liczbę 24. Aby liczba 24 miała tylko jednego reprezetanta – utożsamiamy z nią wszystkie pary (m,n) takie, że $m-n=24$. Zatem 24 to klasa abstrakcji $[(25,1)]_\rho = [(m,n)]_\rho$ dla $m-n=24$.

Zauważmy, że dla liczb całkowitych mamy $(k-l)+(m-n) = (k+m)-(l+n)$. Zatem dodawanie klas abstrakcji relacji ρ zdefiniujemy wzorem: $[(k,l)]_\rho + [(m,n)]_\rho = [(k+m,l+n)]_\rho$. Zauważmy dalej, że: $(k-l)(m-n) = km-kn-lm+ln = (km+ln)-(kn+lm)$. Zatem mnożenie klas abtrakcji relacji ρ zdefiniujemy wzorem: $[(k,l)]_\rho \cdot [(m,n)]_\rho = [(km+ln, kn+lm)]_\rho$.

Aby uzasadnić poprawność tych definicji należy. wykazać, że:

Stwierdzenie 8.19. *Załóżmy, że* $(k,l)\rho(k',l')$ *oraz* $(m,n)\rho(m',n')$. *Wówczas*:

- $(k+m,l+n)\rho(k'+m',l'+n')$
- $(km+ln,kn+lm) = (k'm'+l'n',k'n'+l'm')$.

Zauważmy, że $k-l \leq m-n \iff k+n \leq m+l$. Zatem relację $\leq$ wśród liczb całkowitych definiujemy wzorem:

$$[(k,l)]_\rho \leq [(m,n)]_\rho \iff k+n \leq m+l.$$

Stwierdzenie 8.20. *Załóżmy, że* $(k,l)\rho(k',l')$ *oraz* $(m,n)\rho(m',n')$. *Wówczas*:

- $k+n \leq m+l \iff k'+n' \leq m'+l'$;

Liczby całkowite $\mathbb{Z}$ definiujemy jako $\mathbb{N} \times \mathbb{N}/\rho$.

---

[1] Czytelnik może się zastanawiać, co oznacza $m-n$, gdy $n > m$. Przecież nie zdefiniowaliśmy jeszcze liczb ujemnych. To prawda. Na tym etapie posługiwanie się symbolem różnicy $m-n$ nie jest formalnie poprawne. Służy tylko odwołaniu się do intuicji.

UWAGA 8.21. Liczby całkowite można zdefiniować na różne sposoby. Inny sposób niż przedstawiony, to:

$$\{n, (n,1) : n \in \mathbb{N}\} \cup \{(2,2)\}.$$

Liczby postaci n uważamy za liczby całkowite dodatnie, liczby $(n,1)$ za liczby ujemne $-n$, a liczbę $(2,2)$ za zero. Trzeba jeszcze zdefiniować odpowiednio dodawanie, mnożenie i relację $\leq$ na tak zdefiniowanych liczbach całkowitych. Definicję za pomocą relacji ρ cechuje jednak pewna elegancja. Matematycy dość powszechnie stosują kryteria estetyczne w ocenie różnych teorii, twierdzeń czy dowodów, używając słów typu *elegancka teoria*, *ładne twierdzenie*, *piękny dowód*. Piękno i prostota teorii uważane są często za wartości same w sobie.

2.2. Konstrukcja liczb wymiernych. Liczba wymierna to ułamek $\frac{k}{l}$, gdzie $k \in \mathbb{Z}$, $l \in \mathbb{N}$. Dwa ułamki $\frac{k}{l}$ i $\frac{m}{n}$ są równe, jeżeli $kn = ml$. Rozważmy relację ρ na $\mathbb{Z}\times\mathbb{N}$ daną wzorem: dla $(m,n),(k,l) \in X$

$$(m,n)\rho(k,l) \iff ml = kn.$$

Okazuje się, że ρ jest relacją równoważności.

O parach (k,l) myślimy jako o ułamkach $\frac{k}{l}$. Zauważmy, że $\frac{3}{6}$, $\frac{2}{4}$ i $\frac{1}{2}$ definiują tę samą liczbę wymierną. Ponadto pary $(1,2)$, $(2,4)$ i $(3,6)$ są ze sobą wzajemnie w relacji. Zauważmy, że w klasie abstrakcji $[(1,2)]_\rho$ są wszystkie ułamki, które po skróceniu dają liczbę $\frac{1}{2}$. Zatem $\frac{k}{l}$ to klasa abstrakcji $[(k,l)]_\rho$.

Zauważmy, że:

$$\frac{k}{l} + \frac{m}{n} = \frac{kn+ml}{ln}, \quad \frac{k}{l}\cdot\frac{m}{n} = \frac{km}{ln} \quad \text{i} \quad \frac{k}{l} \leq \frac{m}{n} \iff km \leq nl.$$

Na zbiorze $(\mathbb{Z}\times\mathbb{N})/\rho$ zdefiniujmy następujące działania i relację: dla $[(k,l)]_\rho, [(m,n)]_\rho \in X/\rho$

1. $[(k,l)]_\rho + [(m,n)]_\rho = [(kn+ml, nl)]_\rho$;
2. $[(k,l)]_\rho \cdot [(m,n)]_\rho = [(km, ln)]_\rho$;
3. $[(k,l)]_\rho \leq [(m,n)]_\rho \iff km \leq nl$

Aby uzasadnić poprawność tych definicji należy wykazać:

STWIERDZENIE 8.22. *Załóżmy, że $(k,l)\rho(k',l')$ oraz $(m,n)\rho(m',n')$. Wówczas*

1. $(kn+ml, nl)\rho(k'n'+m'l', n'l')$;
2. $(km, ln)\rho(k'm', l'n')$;
3. $km \leq nl \iff k'm' \leq n'l'$.

Liczby wymierne $\mathbb{Q}$ definiujemy jako $(\mathbb{Z}\times\mathbb{N})/\rho$ wraz z działaniami dodawania, mnożenia i relacją $\leq$.

2.3. Konstrukcja liczb rzeczywistych. Mając już skonstruowane liczby naturalne $\mathbb{N}$ i liczby wymierne $\mathbb{Q}$ możemy skonstruować w obrębie teorii mnogości liczby rzeczywiste. Zbiór wszystkich ciągów liczb wymiernych oznaczamy symbolem $\mathbb{Q}^{\mathbb{N}}$. Przez $\mathcal{X} \subset \mathbb{Q}^{\mathbb{N}}$ oznaczmy zbiór wszystkich ciągów (q_n) takich, że:

$$(\forall k \in \mathbb{N})(\exists m \in \mathbb{N})(\forall n, l \geq m)|q_n - q_l| < \frac{1}{k}.$$

Jak wiemy z analizy, zbiór $\mathcal{X}$ składa się z ciągów spełniających warunek Cauchy'ego. Na $\mathcal{X}$ wprowadzamy relację ρ daną następująco:

$$(q_n)\rho(p_n) \iff (\forall k \in \mathbb{N})(\exists m \in \mathbb{N})(\forall n \geq m)|q_n - p_n| < \frac{1}{k}.$$

Liczby rzeczywiste definiujemy jako granice zbieżnych ciągów liczb wymiernych. Relacja ρ pozwala na utożsamienie ze sobą ciągów zbieżnych do tej samej granicy, np. ciągi $(0, 0, 0, ...)$, $(1, \frac{1}{2}, \frac{1}{3}, ...)$ i $(-1, -\frac{1}{2}, -\frac{1}{3}, ...)$ należą do tej samej klasy abstrakcji. W tej definicji liczby rzeczywiste to ciąg kolejnych przybliżeń liczby rzeczywistej liczbami wymiernymi. Na przykład klasa abstrakcji ciągu $q_1 = 1$, $q_2 = \frac{14}{10}$, $q_3 = \frac{141}{100}$, $q_4 = \frac{1414}{1000}$, $q_5 = \frac{14142}{10000}$, ... jest liczba $\sqrt{2} = [(q_n)]_\rho$.

Na zbiorze liczb rzeczywistych $\mathbb{R} = \mathcal{X}/\rho$ definiujemy operacje i relację:

1. $[(q_n)]_\rho \pm [(p_n)]_\rho = [(q_n \pm p_n)]_\rho$
2. $[(q_n)]_\rho \cdot [(p_n)]_\rho = [(q_n \cdot p_n)]_\rho$
3. $[(0, 0, 0, ...)]_\rho < [(p_n)]_\rho \iff (\exists r \in \mathbb{Q})(\exists m \in \mathbb{N})(\forall n \geq m) 0 < r < p_n$
4. $[(q_n)]_\rho < [(p_n)]_\rho \iff [(0, 0, 0, ...)]_\rho < [(p_n - q_n)]_\rho$.

Aby uzasadnić poprawność tych definicji należy wykazać:

STWIERDZENIE 8.23. *Załóżmy, że* $(q_n)\rho(q'_n)$ *oraz* $(p_n)\rho(p'_n)$. *Wówczas*:

1. $(q_n \pm p_n)\rho(q'_n \pm p'_n)$
2. $(q_n \cdot p_n)\rho(q'_n \cdot p'_n)$
3. $[(q_n)]_\rho < [(p_n)]_\rho \iff [(q'_n)]_\rho < [(p'_n)]_\rho$.

UWAGA 8.24 (bardzo ważne wiadomości z ósmego wykładu). Podczas ósmego wykładu dowiedzieliśmy się m.in.:

- co to jest relacja równoważności
- co to są klasy abstrakcji i zasada abstrakcji
- jak wykorzystując relację równoważności można skonstruować zbiory $\mathbb{Z}$, $\mathbb{Q}$ oraz $\mathbb{R}$.

ROZDZIAŁ 9

Ciągi zbiorów i działania uogólnione

Wiemy już, czym jest suma i iloczyn zbiorów $A \cup B$ i $A \cap B$. Możemy te działania uogólnić na sumę i iloczyn n zbiorów:

$$x \in A_1 \cup A_2 \cup ... \cup A_n \iff x \in A_1 \vee x \in A_2 \vee ... \vee x \in A_n \iff (\exists i \in \{1, 2, ..., n\})x \in A_i.$$

Zatem:

$$A_1 \cup A_2 \cup ... \cup A_n = \bigcup_{i=1}^{n} A_i = \{x : (\exists i \leq n)x \in A_i\}.$$

Podobnie:

$$x \in A_1 \cap A_2 \cap ... \cap A_n \iff x \in A_1 \wedge x \in A_2 \wedge ... \wedge x \in A_n \iff (\forall i \in \{1, 2, ..., n\})x \in A_i$$

i w konsekwencji:

$$A_1 \cap A_2 \cap ... \cap A_n = \bigcap_{i=1}^{n} A_i = \{x : (\forall i \leq n)x \in A_i\}.$$

Teraz będziemy dalej uogólniać działania sumy i iloczynu na nieskończone ciągi i rodziny indeksowane zbiorów.

1. Ciągi zbiorów

Zaczniemy od definicji ciągu zbiorów. Niech X będzie dowolnym niepustym zbiorem.

Definicja 9.1 (ciąg podzbiorów zbioru X). *Dowolną funkcję $A\colon \mathbb{N} \to \mathcal{P}(X)$ nazywamy ciągiem podzbiorów zbioru X.*

Spróbujmy rozszyfrować tę definicję. Skoro funkcja A działa z $\mathbb{N}$ w $\mathcal{P}(X)$, to dla $n \in \mathbb{N}$, mamy $A(n) \in \mathcal{P}(X)$. To oznacza, że $A(n) \subseteq X$ dla $n \in \mathbb{N}$. Będziemy pisać A_n zamiast $A(n)$, a ciąg A będziemy oznaczali symbolem $(A_n)_{n\in\mathbb{N}}$.

Przykład 9.2. Niech $X = \mathbb{R}$ oraz niech A będzie ciągiem przedziałów takim, że $A_n = [0, n]$ dla $n \in \mathbb{N}$. Wówczas $A = (A_n)_{n\in\mathbb{N}}$ jest ciągiem podzbiorów zbioru $\mathbb{R}$.

Jesteśmy teraz gotowi na sformułowanie definicji iloczynu i sumy ciągu zbiorów.

Definicja 9.3 (iloczyn ciągu zbiorów). *Niech $(A_n)_{n\in\mathbb{N}}$ będzie ciągiem podzbiorów zbioru X. Iloczynem ciągu zbiorów $(A_n)_{n\in\mathbb{N}}$ nazywamy zbiór tych elementów X, które należą* ***do każdego*** *wyrazu ciągu A, tj. zbiór*:

$$\{x \in X \colon x \in A_n \text{ dla każdego } n \in \mathbb{N}\} = \{x \in X : (\forall n \in \mathbb{N}) x \in A_n\}.$$

Iloczyn ciągu zbiorów $(A_n)_{n\in\mathbb{N}}$ oznaczamy $\bigcap\limits_{n\in\mathbb{N}} A_n$ lub $\bigcap\limits_{n=1}^{\infty} A_n$.

Przykład 9.4. Rozważmy ciąg $(A_n)_{n\in\mathbb{N}}$ podzbiorów zbioru $\mathbb{R}$ określony następująco $A_n = [0, n]$ dla $n \in \mathbb{N}$. Wówczas $\bigcap\limits_{n\in\mathbb{N}} A_n = [0, 1]$. Istotnie:
„$\subseteq$” Niech $x \in \bigcap\limits_{n\in\mathbb{N}} A_n$. Oznacza to, że dla każdego $n \in \mathbb{N}$ mamy $x \in A_n$. Gdyby $x < 0$, to wtedy $x \notin A_1$, zatem $x \notin \bigcap\limits_{n\in\mathbb{N}} A_n$. Podobnie, gdyby $x > 1$, to $x \notin A_1$, zatem $x \notin \bigcap\limits_{n\in\mathbb{N}} A_n$. Ostatecznie $x \in [0, 1]$.
„$\supseteq$” Łatwo zauważyć, że $[0, 1] \subseteq [0, n]$ dla każdego $n \in \mathbb{N}$. Stąd $[0, 1] \subseteq \bigcap\limits_{n\in\mathbb{N}} A_n$.

Ciąg wybrany w powyższym przykładzie ma pewną szczególną własność – można łatwo sprawdzić, że $A_n \subseteq A_{n+1}$ dla $n \in \mathbb{N}$.

Definicja 9.5 (wstępujący i zstępujący ciąg zbiorów). *Niech $(A_n)_{n\in\mathbb{N}}$ będzie ciągiem podzbiorów zbioru X. Powiemy, że ciąg $(A_n)_{n\in\mathbb{N}}$ jest* ***wstępujący****, jeśli $(\forall n \in \mathbb{N})\ A_n \subseteq A_{n+1}$. Powiemy, że ciąg $(A_n)_{n\in\mathbb{N}}$ jest* ***zstępujący****, jeśli $(\forall n \in \mathbb{N})\ A_n \supseteq A_{n+1}$.*

Dla ciągów wstępujących opis iloczynu ciągu jest bardzo prosty.

Twierdzenie 9.6 (iloczyn wstępującego ciągu zbiorów). *Niech $(A_n)_{n\in\mathbb{N}}$ będzie wstępującym ciągiem podzbiorów zbioru X. Wówczas*:

$$\bigcap_{n\in\mathbb{N}} A_n = A_1.$$

Dowód. Dowód jest ćwiczeniem naśladującym analizę Przykładu 9.4. □

Przejdziemy teraz do dualnej definicji – sumy ciągu zbiorów.

Definicja 9.7 (suma ciągu zbiorów). *Niech $(A_n)_{n\in\mathbb{N}}$ będzie ciągiem podzbiorów zbioru X. Sumą ciągu zbiorów $(A_n)_{n\in\mathbb{N}}$ nazywamy zbiór tych elementów X, które* ***należą do co najmniej jednego*** *wyrazu ciągu A, tj. zbiór*:

$$\{x \in X \colon x \in A_n \text{ dla pewnego } n \in \mathbb{N}\} = \{x \in X \colon (\exists n \in \mathbb{N})\ x \in A_n\}.$$

Iloczyn ciągu zbiorów $(A_n)_{n\in\mathbb{N}}$ oznaczamy $\bigcup\limits_{n\in\mathbb{N}} A_n$ lub $\bigcup\limits_{n=1}^{\infty} A_n$.

PRZYKŁAD 9.8. Rozważmy ciąg $(A_n)_{n\in\mathbb{N}}$ podzbiorów zbioru $\mathbb{R}$ określony następująco: $A_n = [0, n]$ dla $n \in \mathbb{N}$. Wówczas $\bigcup_{n\in\mathbb{N}} A_n = [0, +\infty)$. Istotnie:
„$\subseteq$" Łatwo zauważyć, że $A_n \subseteq [0, +\infty)$ dla każdego $n \in \mathbb{N}$. Zatem $\bigcup_{n\in\mathbb{N}} A_n \subseteq [0, +\infty)$.
„$\supseteq$" Niech $x \in [0, +\infty)$. Wówczas istnieje $n_0 \in \mathbb{N}$ takie, że $x \leq n_0$ (wystarczy np. wziąć $n_0 = [x] + 1$). Wtedy też $x \in A_{n_0}$, zatem $x \in \bigcup_{n\in\mathbb{N}} A_n$.

Analogicznie, dla klasy ciągów zstępujących opis sumy ciągu jest bardzo prosty, mianowicie:

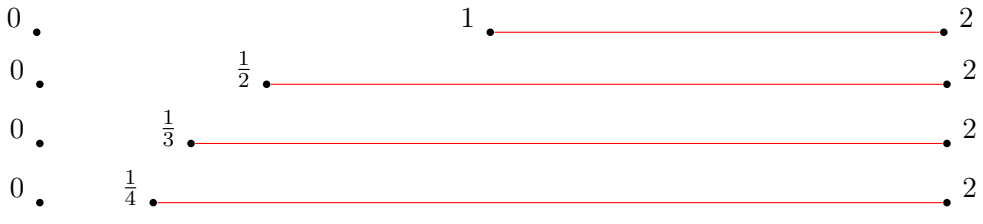
TWIERDZENIE 9.9 (suma zstępującego ciągu zbiorów). *Niech $(A_n)_{n\in\mathbb{N}}$ będzie zstępującym ciągiem podzbiorów zbioru X. Wówczas*:

$$\bigcup_{n\in\mathbb{N}} A_n = A_1.$$

DOWÓD. Dowód jest ćwiczeniem naśladującym analizę Przykładu 9.8. □

PRZYKŁAD 9.10. Niech $A_n = [\frac{1}{n}, 2]$. Wyznaczymy $\bigcup_{n=1}^{\infty} A_n$ oraz $\bigcap_{n=1}^{\infty} A_n$. W tym celu zobaczmy, jak wygląda kilka pierwszych elementów ciągu $(A_n)_{n=1}^{\infty}$.

- $A_1 = [1, 2]$
- $A_2 = [\frac{1}{2}, 2]$
- $A_3 = [\frac{1}{3}, 2]$
- $A_4 = [\frac{1}{4}, 2]$



Widzimy, że przedziały stają się coraz dłuższe i w końcu ich suma pokrywa przedział $(0, 2]$. Dlaczego nie $[0, 2]$? Zauważmy, że 2 jest elementem każdego zbioru A_n, podczas gdy 0 nie należy do żadnego ze zbiorów A_n. Z rysunku widać, że jedyne elementy, które należą do wszystkich zbiorów A_n jednocześnie, to liczby z przedziału $[1, 2] = A_1$. Zapiszmy to symbolicznie:

$$\bigcup_{n=1}^{\infty} A_n = (0, 2] \quad \text{i} \quad \bigcap_{n=1}^{\infty} A_n = [1, 2].$$

Czasami rysunki w matematyce są na tyle przekonujące, że mogą być uznane za dowód. Na tym wykładzie rysunki będą miały jednak jedynie charakter pomocniczy. Powyższe równości uznamy za hipotezy, które wymagają formalnego dowodu.

Niech $x \in \bigcup_{n=1}^{\infty} A_n$. Rozważmy następujący ciąg implikacji:

$$x \in \bigcup_{n=1}^{\infty} A_n \implies (\exists n \in \mathbb{N}) x \in A_n \implies (\exists n \in \mathbb{N}) x \in [\frac{1}{n}, 2] \implies x \in (0, 2].$$

Stąd otrzymujemy $x \in \bigcup_{n=1}^{\infty} A_n \implies x \in (0,2]$, co wobec dowolności wyboru punktu x oznacza, że

$$\bigcup_{n=1}^{\infty} A_n \subseteq (0,2]. \tag{1}$$

Aby wykazać przeciwną inkluzję, ustalmy $x \in (0,2]$. Ponieważ $x > 0$, to istnieje taka liczba $n \in \mathbb{N}$, że $x \geq \frac{1}{n} > 0$. Zatem $x \in [\frac{1}{n}, 2] = A_n$. Pokazaliśmy, że $x \in (0,2] \implies x \in \bigcup_{n=1}^{\infty} A_n$, czyli:

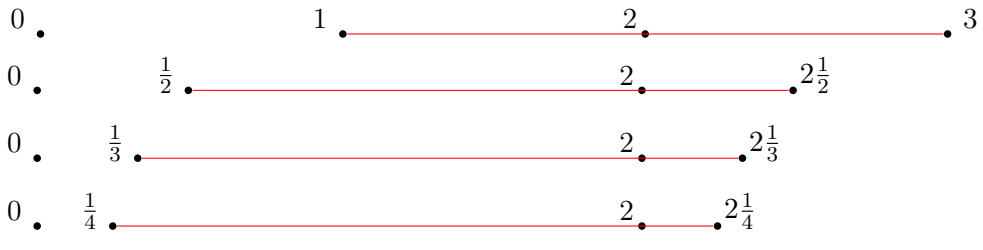
$$(0,2] \subseteq \bigcup_{n=1}^{\infty} A_n. \tag{2}$$

Zawierania (1) i (2) implikują równość $\bigcup_{n=1}^{\infty} A_n = (0,2]$.

Zauważmy, że $(A_n)_{n\in\mathbb{N}}$ jest wstępującym ciągiem zbiorów. Zatem na mocy Twierdzenia 9.6 mamy $\bigcap_{n=1}^{\infty} A_n = A_1 = [1,2]$.

Przykład 9.11. Niech $B_n = [\frac{1}{n}, 2 + \frac{1}{n})$. Wyznaczymy $\bigcup_{n=1}^{\infty} B_n$ oraz $\bigcap_{n=1}^{\infty} B_n$. W tym celu zobaczmy, jak wygląda kilka pierwszych elementów ciągu $(B_n)_{n=1}^{\infty}$.

- $B_1 = [1,3)$
- $B_2 = [\frac{1}{2}, 2\frac{1}{2})$
- $B_3 = [\frac{1}{3}, 2\frac{1}{3})$
- $B_4 = [\frac{1}{4}, 2\frac{1}{4})$



Widać, że jeśli zsumujemy wszystkie przedziały B_n, to powstały zbiór pokryje przedział $(0,3)$. Ponadto wszystkie punkty ze zbioru $[1,2]$ są zawarte w każdym ze zbiorów B_n; żaden punkt poza $[1,2]$ nie ma tej własności. Zapiszmy to symbolicznie:

$$\bigcup_{n=1}^{\infty} B_n = (0,3) \quad \text{i} \quad \bigcap_{n=1}^{\infty} B_n = [1,2].$$

Teraz udowodnimy powyższe równości. Niech $x \in \bigcup_{n=1}^{\infty} B_n$. Istnieje taka liczba $n \in \mathbb{N}$, że $x \in B_n$. Zauważmy, że $0 < \frac{1}{n}$ oraz $2 + \frac{1}{n} \leq 3$. Zatem $B_n = [\frac{1}{n}, 2 + \frac{1}{n}) \subseteq (0,3)$. Stąd $x \in (0,3)$, w konsekwencji:

$$\bigcup_{n=1}^{\infty} B_n \subseteq (0,3). \tag{3}$$

Niech $x \in (0,3)$. Mamy dwie możliwości:

(a) $x \in [1,3)$

(b) $x \in (0,1)$.

Ad (a): Jeżeli $x \in [1,3)$, to $x \in B_1$.

Ad (b): Jeżeli $x \in (0,1)$, to istnieje taka liczba $n \in \mathbb{N}$, że $\frac{1}{n} \leq x < 1$. Zatem $x \in [\frac{1}{n}, 2+\frac{1}{n}) = B_n$.

Pokazaliśmy, że:

$$x \in (0,3) \implies (\exists n \in \mathbb{N}) x \in B_n \implies x \in \bigcup_{n=1}^{\infty} B_n.$$

Stąd:

$$(0,3) \subseteq \bigcup_{n=1}^{\infty} B_n. \tag{4}$$

Zawierania (3) i (4) implikują równość $\bigcup_{n=1}^{\infty} B_n = (0,3)$.

Zauważmy, że w przeciwieństwie do ciągu (A_n) ciąg (B_n) nie jest wstępujący i nie możemy użyć Twierdzenia 9.6. Niech $x \in \bigcap_{n=1}^{\infty} B_n$. Wtedy $x \in B_n$ dla każdego $n \in \mathbb{N}$. W szczególności $x \in B_1 = [1,3)$, czyli $x \geq 1$. Jednocześnie $x \in B_n = [\frac{1}{n}, 2+\frac{1}{n})$, czyli $x < 2 + \frac{1}{n}$ dla każdego $n \in \mathbb{N}$. Zatem $x \leq 2$. Skoro jednocześnie $x \geq 1$ oraz $x \leq 2$, to $x \in [1,2]$. Stąd:

$$\bigcap_{n=1}^{\infty} B_n \subseteq [1,2]. \tag{5}$$

Niech $x \in [1,2]$. Wtedy dla dowolnego $n \in \mathbb{N}$ zachodzą nierówności:

$$\frac{1}{n} \leq 1 \leq x \leq 2 < 2 + \frac{1}{n},$$

czyli $x \in [\frac{1}{n}, 2+\frac{1}{n}) = B_n$. Zatem:

$$[1,2] \subseteq \bigcap_{n=1}^{\infty} B_n. \tag{6}$$

Zawierania (5) i (6) implikują równość $\bigcap_{n=1}^{\infty} B_n = [1,2]$.

2. Rodziny indeksowane

Definicja 9.12. *Niech I będzie dowolnym niepustym zbiorem. Rodziną $\mathcal{G}$ podzbiorów zbioru X indeksowaną zbiorem I nazywamy zbiór wartości dowolnej funkcji ze zbioru I w zbiór $\mathcal{P}(X)$ i oznaczamy $\mathcal{G} = \{G_i \colon i \in I\}$.*

Definicja 9.13 (suma rodziny indeksowanej). *Niech $\{G_i \colon i \in I\}$ będzie rodziną podzbiorów zbioru X. Sumą $\{G_i \colon i \in I\}$ nazywamy zbiór*

$$\{x \in X \colon x \in G_i \text{ dla pewnego } i \in I\} = \{x \in X : (\exists i \in I) x \in G_i\}.$$

Sumę rodziny $\{G_i\colon i\in I\}$ *oznaczamy* $\bigcup\limits_{i\in I} G_i$.

Definicja 9.14 (iloczyn rodziny indeksowanej). *Niech* $\{G_i\colon i\in I\}$ *będzie rodziną podzbiorów zbioru* X. *Iloczynem* $\{G_i\colon i\in I\}$ *nazywamy zbiór*

$$\{x\in X\colon x\in G_i \text{ dla każdego } i\in I\}=\{x\in X:(\forall i\in I)x\in G_i\}.$$

Iloczyn rodziny $\{G_i\colon i\in I\}$ *oznaczamy* $\bigcap\limits_{i\in I} G_i$.

Uwaga 9.15. Gdy $\mathcal{G}=\{G_i\colon i\in I\}$, to używamy też symboli: $\bigcap\mathcal{G}$ zamiast $\bigcap\limits_{i\in I} G_i$ oraz $\bigcup\mathcal{G}$ zamiast $\bigcup\limits_{i\in I} G_i$. W literaturze często od zbioru I oczekuje się też pewnych własności (np. skierowanie) niemniej, na potrzeby tego skryptu, nie zakładamy dla zbioru I nic więcej niż niepustość. Ponadto, pewnym naturalnym indeksowaniem rodziny $\mathcal{G}\subseteq\mathcal{P}(X)$ jest sama rodzina $\mathcal{G}$, mianowicie: $\mathcal{G}=\{G\colon G\in\mathcal{G}\}$.

Przykład 9.16. Rozważmy rodzinę $\mathcal{G}=\{(x,x+1)\colon x\in\mathbb{R}\}$. Wówczas:

$$\bigcap\mathcal{G}=\bigcap_{x\in\mathbb{R}}(x,x+1)=\emptyset$$

oraz

$$\bigcup\mathcal{G}=\bigcup_{x\in\mathbb{R}}(x,x+1)=\mathbb{R}.$$

Na koniec sformułujemy jeszcze bardzo ważne twierdzenie będące analogonem praw De Morgana dla skończonych operacji mnogościowych oraz inne własności operacji uogólnionych na rodzinach zbiorów.

Twierdzenie 9.17 (prawa De Morgana dla działań uogólnionych). *Niech* $\{G_i : i\in I\}\subseteq\mathcal{P}(X)$ *będzie dowolną niepustą rodziną podzbiorów zbioru* X. *Wówczas zachodzą równości:*

1. $(\bigcap\limits_{i\in I} G_i)^c=\bigcup\limits_{i\in I} G_i^c$;
2. $(\bigcup\limits_{i\in I} G_i)^c=\bigcap\limits_{i\in I} G_i^c$.

Dowód. 1. Niech $x\in X$. Wówczas:

$$x\in(\bigcap_{i\in I}G_i)^c \iff \neg(x\in\bigcap_{i\in I}G_i) \iff \neg((\forall i\in I)x\in G_i),$$

co na mocy prawa De Morgana dla kwantyfikatorów jest równoważne:

$$\iff (\exists i\in I)x\notin G_i \iff (\exists i\in I)x\in G_i^c \iff x\in\bigcup_{i\in I}G_i^c.$$

Równoważność $x\in(\bigcap\limits_{i\in I} G_i)^c \iff x\in\bigcup_{i\in I}G_i^c$ wobec dowolności wyboru x oznacza równość $(\bigcap\limits_{i\in I} G_i)^c=\bigcup\limits_{i\in I} G_i^c$.

2. Niech $x \in X$. Wówczas:

$$x \in (\bigcup_{i\in I} G_i)^c \iff \neg(x \in \bigcup_{i\in I} G_i) \iff \neg((\exists i \in I)x \in G_i),$$

co na mocy prawa De Morgana dla kwantyfikatorów jest równoważne:

$$\iff (\forall i \in I)x \notin G_i \iff (\forall i \in I)x \in G_i^c \iff x \in \bigcap_{i\in I} G_i^c.$$

Stąd otrzymujemy równość $(\bigcup_{i\in I} G_i)^c = \bigcap_{i\in I} G_i^c$. □

TWIERDZENIE 9.18. *Niech $\{A_i \colon i \in I\}, \{B_i \colon i \in I\}$ będą rodzinami podzbiorów zbioru X indeksowanymi zbiorem I. Zachodzą następujące własności:*

1. $A_{i_0} \subseteq \bigcup_{i\in I} A_i$ *dla każdego* $i_0 \in I$
2. $\bigcap_{i\in I} A_i \subseteq A_{i_0}$ *dla każdego* $i_0 \in I$
3. $\bigcap_{i\in I} A_i \subseteq \bigcup_{i\in I} A_i$
4. *jeśli* $A_i \subseteq B_i$ *dla każdego* $i \in I$, *to* $\bigcup_{i\in I} A_i \subseteq \bigcup_{i\in I} B_i$ *oraz* $\bigcap_{i\in I} A_i \subseteq \bigcap_{i\in I} B_i$.

Poniższe twierdzenia są łatwymi wnioskami z praw rachunku kwantyfikatorów.

TWIERDZENIE 9.19 (własności działań uogólnionych 1). *Niech $\{A_i \colon i \in I\}, \{B_i \colon i \in I\}$ będą rodzinami podzbiorów zbioru X indeksowanymi zbiorem I. Zachodzą następujące własności:*

1. $\bigcap_{i\in I}(A_i \cap B_i) = \bigcap_{i\in I} A_i \cap \bigcap_{i\in I} B_i$
2. $\bigcup_{i\in I}(A_i \cup B_i) = \bigcup_{i\in I} A_i \cup \bigcup_{i\in I} B_i$
3. $\bigcup_{i\in I}(A_i \cap B_i) \subseteq \bigcup_{i\in I} A_i \cap \bigcup_{i\in I} B_i$
4. $\bigcap_{i\in I} A_i \cup \bigcap_{i\in I} B_i \subseteq \bigcap_{i\in I}(A_i \cup B_i)$.

TWIERDZENIE 9.20 (własności działań uogólnionych 2). *Niech $\{A_i \colon i \in I\}$ będzie rodziną podzbiorów zbioru X indeksowaną zbiorem I oraz $A \subseteq X$. Zachodzą następujące własności:*

1. $\bigcap_{i\in I}(A_i \cap A) = A \cap \bigcap_{i\in I} A_i$
2. $\bigcap_{i\in I}(A_i \cup A) = A \cup \bigcap_{i\in I} A_i$
3. $\bigcup_{i\in I}(A_i \cup A) = A \cup \bigcup_{i\in I} A_i$
4. $\bigcup_{i\in I}(A_i \cap A) = A \cap \bigcup_{i\in I} A_i$.

OZNACZENIE 9.21. *Rozważmy rodzinę indeksowaną produktem dwu zbiorów, mianowicie $\{A_{(i,j)} \colon i \in I, j \in J\}$. Zwyczajowo taką rodzinę zapisuje się w postaci $\{A_{i,j} \colon i \in I, j \in J\}$.*

TWIERDZENIE 9.22 (prawa przestawiania działań uogólnionych). *Niech* $\{A_{i,j} \colon i \in I, j \in J\}$ *będzie rodziną podzbiorów zbioru* X*. Zachodzą następujące własności:*

1. $\bigcup\limits_{i\in I}\bigcup\limits_{j\in J} A_{i,j} = \bigcup\limits_{j\in J}\bigcup\limits_{i\in I} A_{i,j}$
2. $\bigcap\limits_{i\in I}\bigcap\limits_{j\in J} A_{i,j} = \bigcap\limits_{j\in J}\bigcap\limits_{i\in I} A_{i,j}$
3. $\bigcup\limits_{i\in I}\bigcap\limits_{j\in J} A_{i,j} \subseteq \bigcap\limits_{j\in J}\bigcup\limits_{i\in I} A_{i,j}$.

UWAGA 9.23 (bardzo ważne wiadomości z dziewiątego wykładu). Podczas dziewiątego wykładu dowiedzieliśmy się m.in.:

- co to są ciągi podzbiorów zbioru X i ich sumy oraz iloczyny
- co to są rodziny podzbiorów i ich sumy oraz iloczyny
- co to są rodziny indeksowane zbiorów
- jakie są podstawowe własności iloczynów i sum rodzin zbiorów.

ROZDZIAŁ 10

Zbiory skończone i równoliczność

Na kilku kolejnych wykładach zajmiemy się analizą wielkości zbiorów pod względem ich liczności. Intuicja związana ze zbiorami skończonymi jest dość naturalna i nie wymaga wprowadzenia, a jedynie formalnego usystematyzowania. Główny ciężar położymy na analizę liczności i porównywania tej liczności dla zbiorów nieskończonych.

1. Zliczanie elementów zbiorów skończonych i równoliczność

Pierwszą, dość jasno wyodrębnioną, grupą zbiorów względem ich liczności jest ta, na którą składają się zbiory najmniej liczne. Intuicyjnie wiadomo, czym jest zbiór skończony – taki, który ma skończenie wiele elementów, którego elementy można policzyć i określić ich liczbę. Jako punkt wyjścia dla dalszych dociekań rozważmy następujący prosty problem:

PROBLEM 10.1. *W jaki sposób określić, czy w klasie jest więcej dziewczyn czy chłopców?*

Jednym z pierwszych pomysłów, które przychodzą do głowy, jest policzenie dziewczyn, policzenie chłopców i porównanie tych dwóch liczb. Zastanówmy się czym z formalnego punktu widzenia jest *liczenie ile jest dziewczyn* (analogicznie chłopców).

OZNACZENIE 10.2 (przedział w zbiorze $\mathbb{N}$). *Dla $n \in \mathbb{N}$ oznaczamy $\langle 1, n\rangle := \{1, ..., n\}$.*

Wróćmy do formalizacji, czym jest *liczenie, ile jest dziewczyn*; odliczając osoby przypisujemy im odpowiednie numery: $1, 2, 3, ...$ Oczywiście ponieważ zbiór dziewczyn jest skończony, to nasze odliczanie się kiedyś skończy, przyjmijmy, że na liczbie $n \in \mathbb{N}$. Procedura odliczania, to nic innego jak tworzenie funkcji $f\colon \langle 1, n\rangle \to \mathcal{D}$ o dziedzinie $\langle 1, n\rangle$ działającej w zbiór $\mathcal{D}$ dziewczyn w klasie. Nasze odliczanie f jest różnowartościowe (różne numery są przypisane różnym osobom) oraz jest suriekcją na zbiór $\mathcal{D}$ (ponieważ każda dziewczyna została odliczona). Niniejszym stwierdzenie: *w klasie jest dokładnie n dziewczyn*, jest równoważne zdefiniowaniu funkcji $f\colon \langle 1, n\rangle \to \mathcal{D}$, która jest bijekcją na $\mathcal{D}$.

Powyższe rozumowanie pozwala nam sformalizować pojęcie zbioru n-elementowego, dla $n \in \mathbb{N}$.

DEFINICJA 10.3 (zbiór n-elementowy). *Niech $n \in \mathbb{N}$. Mówimy, że zbiór X jest n-elementowy, gdy istnieje bijekcja $f\colon \langle 1, n\rangle \to X$ na X. Mówimy, że X jest 0-elementowy, jeśli $X = \emptyset$.*

Drugim sposobem porównania liczby dziewczyn i chłopców w klasie jest próba łączenia ich w pary. Jeśli na koniec łączenia zostaną chłopcy, to znaczy, że było ich więcej; jeśli zostaną dziewczyny, to znaczy, że ich było więcej. Jeśli zaś nikt nie zostanie, to dziewczyn i chłopców jest tyle samo – innymi słowy, dwa zbiory $\mathcal{D}, \mathcal{C}$ są tak samo liczne (mają tyle samo elementów) oraz parowanie $f\colon \mathcal{D} \to \mathcal{C}$ jest bijekcją na $\mathcal{C}$. Powyższe pozwala wprowadzić ogólne pojęcie równoliczności dwu zbiorów (w tym zbiorów nieskończonych!).

Definicja 10.4 (równoliczność). *Powiemy, że zbiór X jest równoliczny ze zbiorem Y, jeśli istnieje bijekcja $f\colon X \to Y$ na Y. Fakt, że X jest równoliczny z Y oznaczamy symbolem $|X| = |Y|$.*

Uwaga 10.5. Symbol $|A|$ oznacza moc zbioru (jego liczności). Jednak aby to pojęcie formalnie zdefiniować dla wszystkich zbiorów, potrzebna jest teoria liczb kardynalnych.

Uwaga 10.6. Wobec powyższych definicji, dla $n \in \mathbb{N}$, zbiór X jest n-elementowy wtedy i tylko wtedy, gdy jest równoliczny ze zbiorem $\langle 1, n\rangle$ (symbolicznie $|X| = |\langle 1, n\rangle|$).

Oznaczenie 10.7. *Dla $n \in \mathbb{N}$ oraz zbioru n-elementowego X, liczbę n nazywamy mocą zbioru X i oznaczamy $|X| = n$.*

Następujące własności pojęcia równoliczności są konsekwencjami znanych już własności funkcji.

Stwierdzenie 10.8 (własności równoliczności 1). *Dla zbiorów X, Y, Z mamy*:

1. $|X| = |X|$
2. *jeśli* $|X| = |Y|$, *to* $|Y| = |X|$
3. *jeśli* $|X| = |Y|$ *oraz* $|Y| = |Z|$, *to* $|X| = |Z|$.

Dowód. Ad 1. Oczywiście $id_X\colon X \to X$ jest bijekcją na X, zatem ustala równoliczność zbiorów X oraz X.

Ad 2. Załóżmy, że $f\colon X \to Y$ jest bijekcją na Y ustalającą równoliczność zbiorów X i Y. Wiadomo, że $f^{-1}\colon Y \to X$ jest bijekcją na X i ustala równoliczność zbiorów Y i X.

Ad 3. Załóżmy, że $f\colon X \to Y$ oraz $g\colon Y \to Z$ ustalają równoliczności zbiorów X i Y oraz Y i Z. Wiadomo, że $g \circ f\colon X \to Z$ jest bijekcją na Z, jako złożenie bijekcji (patrz: Wykład 5.). Ustala ona równoliczność między X i Z. □

Uwaga 10.9. Zauważmy, że „relacja” równoliczności spełnia formalne własności relacji równoważności, jednak nie jest to **relacja**, gdyż obiekt, w którym jest zdefiniowana (rodzina wszystkich zbiorów), **nie** jest zbiorem!

Zanotujmy także dalsze własności równoliczności:

STWIERDZENIE 10.10 (własności równoliczności 2). *Dla zbiorów X, Y, X', Y', Z mamy:*

1. *Jeśli $|X| = |Y|$ oraz $|X'| = |Y'|$, to $|X \times X'| = |Y \times Y'|$*
2. *Jeśli $|X| = |Y|$ i $|X'| = |Y'|$ oraz $X \cap X' = Y \cap Y' = \emptyset$, to $|X \cup X'| = |Y \cup Y'|$*
3. *Jeśli $|X| = |Y|$, to $|X^Z| = |Y^Z|$*
4. *Jeśli $|X| = |Y|$, to $|Z^X| = |Z^Y|$*
5. $|(X^Y)^Z| = |X^{Y \times Z}|$.

DOWÓD. Ad 1. Załóżmy, że $f\colon X \to Y$ oraz $f'\colon X' \to Y'$ są bijekcjami na Y i Y' odpowiednio. Wówczas funkcja $f \times f'\colon X \times X' \to Y \times Y'$ określona wzorem $(f \times f')(x, x') = (f(x), f'(x'))$ dla $x \in X, x' \in X'$ jest bijekcją na $Y \times Y'$.

Ad 2. Załóżmy, że $f\colon X \to Y$ oraz $f'\colon X' \to Y'$ są bijekcjami na Y i Y' odpowiednio. Rozważmy sumę $f \cup f'$, która jest funkcją $X \cup X' \to Y \cup Y'$, bo $X \cap X' = \emptyset$. Pokażemy, że $f \cup f'$ jest bijekcją na $Y \cup Y'$.

Różnowartościowość: Niech $x_1, x_2 \in X \cup X'$ oraz $x_1 \neq x_2$. Jeśli $x_1, x_2 \in X$, to $(f \cup f')(x_1) = f(x_1)$ oraz $(f \cup f')(x_2) = f(x_2)$, więc z różnowartościowości f mamy $(f \cup f')(x_1) \neq (f \cup f')(x_2)$. Podobnie, gdy $x_1, x_2 \in X'$ (wtedy korzystamy z różnowartościowości f'). Jeśli zaś $x_1 \in X, x_2 \in X'$, to ponieważ $(f \cup f')(x_1) = f(x_1) \in Y, (f \cup f')(x_2) = f'(x_2) \in Y'$ oraz $Y \cap Y' = \emptyset$, to $(f \cup f')(x_1) \neq (f \cup f')(x_2)$.
Suriekcja na $Y \cup Y'$: Niech $y \in Y \cup Y'$. Jeśli $y \in Y$, to istnieje (z suriektywności f na Y) $x \in X$ taki, że $f(x) = y$, przy tym $(f \cup f')(x) = f(x) = y$ oraz $x \in X \cup X'$. Jeśli zaś $y \in Y'$, to istnieje (z suriektywności f' na Y') $x \in X'$ taki, że $f'(x) = y$, przy tym $(f \cup f')(x) = f'(x) = y$ oraz $x \in X \cup X'$.

Ad 3. Ustalmy funkcję różnowartościową $\varphi\colon X \to Y$ taką, że $\varphi[X] = Y$. Zdefiniujmy funkcję $F\colon X^Z \to Y^Z$ określoną wzorem: dla $f \in X^Z$

$$F(f) = \varphi \circ f.$$

Zauważmy, że F jest poprawnie określona, bo dla $f \in X^Z$ mamy $F(f) \in Y^Z$. Ponadto F jest różnowartościowa: istotnie, dla $f, g \in X^Z$, jeśli $F(f) = F(g)$, to $\varphi \circ f = \varphi \circ g$, więc $f = g$, bo φ jest bijekcją. Przy tym widać, że $F[X^Z] = Y^Z$, bo dla $h \in Y^Z$ funkcja $\varphi^{-1} \circ h \in X^Z$ oraz $F(\varphi^{-1} \circ h) = h$.

Ad 4. Analogicznie jak wyżej, dla ustalonej jak wcześniej funkcji $\varphi\colon X \to Y$, wystarczy zdefiniować $F\colon Z^X \to Z^Y$ wzorem $F(f) = f \circ \varphi$. Dalej dowód przebiega podobnie.

Ad 5. Rozważmy funkcję $H\colon (X^Y)^Z \to X^{Y \times Z}$ zdefiniowaną następująco: jeśli $f \in (X^Y)^Z$ jest funkcją postaci $f\colon Z \to X^Y$, to $H(f)\colon Y \times Z \to X$ jest funkcją określoną w punkcie f następująco: dla

dowolnych $(y, z) \in Y \times Z$

$$H(f)(y, z) = f(z)(y)$$

tzn. jako wartość funkcji $H(f)(y, z)$ przyjmujemy wartość funkcji $f(z)$ w punkcie y. Pokażemy, że H jest szukaną funkcją. Dla sprawdzenia różnowartościowości, ustalmy funkcje $f, g \in (X^Y)^Z$. Jeśli $f \neq g$ to istnieje $z \in Z$ takie, że $f(z) \neq g(z)$. Ponieważ funkcje $f(z)$ i $g(z)$ są różne, to istnieje $y \in Y$ takie, że $f(z)(y) \neq g(z)(y)$. W szczególności $H(f)(y, z) \neq H(g)(y, z)$.

Ustalmy teraz $h \in X^{Y \times Z}$ i określmy funkcje $f \in (X^Y)^Z$ wzorem: $f(z)(y) = h(y, z)$ dla $y \in Y, z \in Z$. Wówczas $H(f) = h$. □

2. Zbiory skończone i ich własności

W poprzedniej sekcji poznaliśmy pojęcie zbioru n-elementowego dla $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Ogół takich zbiorów tworzy klasę – nie zbiór! – zbiorów skończonych:

Definicja 10.11 (zbiór skończony). *Powiemy, że zbiór X jest zbiorem skończonym, jeśli jest zbiorem n-elementowym dla pewnego $n \in \mathbb{N}_0$.*

Wniosek 10.12. *Zbiór X jest zbiorem skończonym, jeśli jest zbiorem pustym, albo jest równoliczny ze zbiorem $\langle 1, n\rangle$ dla pewnego $n \in \mathbb{N}$.*

Przykład 10.13. Jest oczywiste, że jeśli zbiory X i Y są równoliczne oraz jeden z nich jest skończony, to drugi także. Zbiór pusty jest skończony z definicji. Ponadto, oczywiście dla każdego $n \in \mathbb{N}$, przedział $\langle 1, n\rangle$ jest skończony. Również każdy zbiór jednoelementowy $\{a\}$ jest skończony, jako równoliczny z przedziałem $\langle 1, 1\rangle$. Podobnie każda para jest zbiorem skończonym jako równoliczny z przedziałem $\langle 1, 2\rangle$.

Skoro wyodrębniliśmy zbiory skończone, to istotne są też te pozostałe.

Definicja 10.14 (zbiór nieskończony). *Zbiór X nazywamy zbiorem nieskończonym, jeśli nie jest zbiorem skończonym.*

Przykład 10.15. Zbiory: liczb naturalnych $\mathbb{N}$, liczb całkowitych $\mathbb{Z}$, liczb wymiernych $\mathbb{Q}$, liczb pierwszych, liczb parzystych, liczb nieparzystych, liczb rzeczywistych $\mathbb{R}$ są zbiorami nieskończonymi.

Zajmiemy się na razie krótko intuicyjnymi własnościami zbiorów skończonych.

Lemat 10.16. *Jeśli zbiór X jest skończony, przy czym X jest równoliczny z przedziałem $\langle 1, n+1\rangle$, to zbiór $X \setminus \{x\}$ jest równoliczny z przedziałem $\langle 1, n\rangle$ dla każdego $x \in X$.*

Dowód. Ustalmy dowolną bijekcję $f\colon X \to \langle 1, n+1\rangle$ na $\langle 1, n+1\rangle$ i niech $x \in X$. Jeśli $f(x) = n+1$, to funkcja $f|X \setminus \{x\}$ jest bijekcją zbioru $X \setminus \{x\}$ na $\langle 1, n\rangle$. Jeśli zaś $f(x) = k < n+1$, to zdefiniujmy funkcję $g\colon X \setminus \{x\} \to \langle 1, n\rangle$ wzorem:

$$g(y) = \begin{cases} f(y), \text{ gdy } f(y) < k \\ f(y) - 1, \text{ gdy } k < f(y). \end{cases}$$

Definicja funkcji g jest poprawna, bo jeśli $k < f(y) \leq n+1$, to $f(y)-1 \leq n$. Nietrudno też zobaczyć, że g jest bijekcją na $\langle 1, n\rangle$. □

Twierdzenie 10.17 (dziedziczność skończoności zbioru). *Podzbiór zbioru skończonego jest skończony.*

Dowód. Przeprowadzimy go indukcyjnie ze względu na $n \in \mathbb{N}$. Niech dla liczby naturalnej $n \in \mathbb{N}$, $W(n)$ oznacza, że jeśli X jest równoliczny ze zbiorem $\langle 1, n\rangle$ oraz $Y \subseteq X$, to Y jest skończony.
Zauważmy, że dla $n = 1$ mamy, że X jest jednoelementowy, więc dla każdego $Y \subseteq X$ albo Y jest pusty albo $Y = X$ więc Y jest skończony.
Niech $n_0 \in \mathbb{N}$ i załóżmy, że $W(n_0)$ zachodzi. Pokażemy, że zachodzi $W(n_0+1)$. Niech X będzie zbiorem równolicznym z $\langle 1, n_0 + 1\rangle$ oraz niech $Y \subseteq X$. Mamy możliwości:

- jeśli $Y = X$, to oczywiście Y skończony
- istnieje $x \in X \setminus Y$ i wtedy Y jest podzbiorem zbioru $X \setminus \{x\}$. Wobec Lematu zbiór $X \setminus \{x\}$ jest równoliczny z $\langle 1, n_0\rangle$ więc stosując założenie indukcyjne do zbioru $X \setminus \{x\}$ mamy, że Y jest skończony.

Na mocy zasady indukcji matematycznej, dla każdego $n \in \mathbb{N}$ zdanie $W(n)$ jest prawdziwe. □

Twierdzenie 10.18. *Jeśli $n, m \in \mathbb{N}$ oraz $n < m$, to dla każdej funkcji $f\colon \langle 1, m\rangle \to \langle 1, n\rangle$ istnieją takie $k, l \in \langle 1, m\rangle$, że $f(k) = f(l)$.*

Dowód. Dowód przeprowadzimy indukcyjnie ze względu na $n \in \mathbb{N}$. Niech dla liczby naturalnej $n \in \mathbb{N}$, $W(n)$ oznacza, że dla każdego $m \in \mathbb{N}$ takiego, że $n < m$ i dowolnej funkcji $f\colon \langle 1, m\rangle \to \langle 1, n\rangle$ istnieją takie $k, l \in \langle 1, m\rangle$, że $f(k) = f(l)$.
Krok 1.: Zauważmy, że dla $n = 1$ mamy $\langle 1, n\rangle = \{1\}$, zatem biorąc $m > n$ i dowolną funkcję $f\colon \langle 1, m\rangle \to \langle 1, n\rangle$ oraz $k = 1, l = 2$ mamy $k, l \in \langle 1, m\rangle$ oraz $f(k) = f(l) = 1$. tj. $W(1)$ zachodzi.
Krok 2.: Niech $n_0 \in \mathbb{N}$ i załóżmy, że $W(n_0)$ zachodzi. Pokażemy, że zachodzi $W(n_0+1)$. Niech $m > n_0+1$ i rozważmy funkcję $f\colon \langle 1, m\rangle \to \langle 1, n_0 + 1\rangle$. Weźmy pod uwagę zbiór $f^{-1}[\{n_0 + 1\}]$. Rozważmy trzy przypadki:
1. jeśli w zbiorze $f^{-1}[\{n_0 + 1\}]$ istnieją dwa różne elementy, to mamy tezę.

2. Jeśli zbiór $f^{-1}[\{n_0+1\}]$ jest pusty, to $f\colon \langle 1,m\rangle \to \langle 1,n_0\rangle$ i z założenia indukcyjnego $W(n_0)$ wynika teza.
3. Jeśli zbiór $f^{-1}[\{n_0+1\}]$ jest jednoelementowy, to istnieje bijekcja:

$$g\colon \langle 1,m-1\rangle \to \langle 1,m\rangle \setminus f^{-1}[\{n_0+1\}]$$

na $\langle 1,m\rangle \setminus f^{-1}[\{n_0+1\}]$. Rozważmy funkcję $h = f\circ g\colon \langle 1,m-1\rangle \to \langle 1,n_0\rangle$. Wówczas wobec założenia indukcyjnego $W(n_0)$ (bo $m-1>n_0$) mamy, że istnieją $k,l \in \langle 1,m-1\rangle$ takie, że $h(k)=h(l)$. W szczególności $f(g(k))=f(g(l))$ oraz $g(k),g(l)\in\langle 1,m\rangle$, co kończy dowód.
Podsumowanie: Na mocy zasady indukcji matematycznej, dla każdego $n\in\mathbb{N}$ zdanie $W(n)$ jest prawdziwe. □

Natychmiastowym wnioskiem z powyższego jest:

Wniosek 10.19. *Dla dowolnych różnych $m,n\in\mathbb{N}$, nie istnieje bijekcja $f\colon\langle 1,n\rangle\to\langle 1,m\rangle$ na $\langle 1,m\rangle$. W konsekwencji dla każdego zbioru skończonego X istnieje dokładnie jedna liczba $n\in\mathbb{N}$ taka, że X jest równoliczny z przedziałem $\langle 1,n\rangle$.*

Stwierdzenie 10.20 (liczność sumy zbiorów skończonych). *Jeśli X i Y są skończone, rozłączne oraz $|X|=n, |Y|=m$ dla pewnych $n,m\in\mathbb{N}_0$, to $|X\cup Y|=n+m$.*

Dowód. Gdy $X=\emptyset$ lub $Y=\emptyset$, to teza jest oczywista. Załóżmy, że X i Y są skończone, rozłączne oraz $|X|=n, |Y|=m$ dla pewnych $n,m\in\mathbb{N}$. Ustalmy bijekcje $f\colon X\to\langle 1,n\rangle, g\colon Y\to\langle 1,m\rangle$ odpowiednio na $\langle 1,n\rangle$ i $\langle 1,m\rangle$. Wskażemy bijekcję $h\colon X\cup Y\to\langle 1,n+m\rangle$ na $\langle 1,n+m\rangle$. Niech $h\colon X\cup Y\to\langle 1,n+m\rangle$ będzie zdefiniowana wzorem: dla $x\in X\cup Y$

$$h(x)=\begin{cases} f(x), \text{ gdy } x\in X \\ g(x)+n, \text{ gdy } x\in Y. \end{cases}$$

Łatwo sprawdzić (ćw.), że h jest bijekcją na $\langle 1,n+m\rangle$. □

Wniosek 10.21. *Suma skończenie wielu zbiorów skończonych jest skończona.*

Dowód. Przeprowadzimy dowód indukcyjny ze względu na długość sumy, tj. liczbę zbiorów skończonych, które sumujemy. Mianowicie dla $n\in\mathbb{N}$ niech $W(n)$ oznacza zdanie: *suma n zbiorów skończonych jest zbiorem skończonym.*
Krok 1.: Zauważmy, że dla $n=1$ teza jest oczywista, bo suma jednego zbioru skończonego to ten zbiór, więc jest skończona.
Krok 2.: Niech $n_0\in\mathbb{N}$ i załóżmy, że $W(n_0)$ zachodzi, tj. suma dowolnych n_0 zbiorów skończonych jest

zbiorem skończonym.. Pokażemy, że zachodzi $W(n_0+1)$. Ustalmy zbiory skończone X_1, X_2,...,X_{n_0}, X_{n_0+1}. Wówczas $\bigcup_{n=1}^{n_0+1} X_n = (\bigcup_{n=1}^{n_0} X_n) \cup X_{n_0+1}$, przy tym z założenia $W(n_0)$ mamy, że $\bigcup_{n=1}^{n_0} X_n$ jest zbiorem skończonym. Stąd $\bigcup_{n=1}^{n_0+1} X_n$ jest zbiorem skończonym jako suma dwu zbiorów skończonych: $\bigcup_{n=1}^{n_0} X_n$ oraz X_{n_0+1} (patrz Stwierdzenie 10.20).

Podsumowanie: Na mocy zasady indukcji matematycznej, $W(n)$ jest prawdziwe dla każdego $n \in \mathbb{N}$. □

Innym, bardzo ważnym, wnioskiem z Twierdzenia 10.18 jest powszechnie znana tzw. zasada szufladkowa, która w wersji popularnej brzmi: jeśli włożymy do n szuflad więcej niż n przedmiotów, to w którejś szufladzie będą co najmniej dwa.

Wniosek 10.22 (zasada szufladkowa Dirichleta). *Jeśli zbiory X, Y są skończone i $|X| > |Y|$, to dla każdej funkcji $f\colon X \to Y$ istnieją $x, y \in X$ takie, że $f(x) = f(y)$.*

Powyższy wniosek ma swój analogon w przypadku zbiorów nieskończonych - zob. w dalszej części wykładu.

Stwierdzenie 10.23 (liczność produktu zbiorów skończonych). *Jeśli $|X| = n$ oraz $|Y| = m$, to $|X \times Y| = m \cdot n$.*

Dowód. Ustalmy bijekcje $f\colon X \to \langle 1, n\rangle, g\colon Y \to \langle 1, m\rangle$ odpowiednio na $\langle 1, n\rangle$ i $\langle 1, m\rangle$. Wskażemy bijekcję $h\colon X \times Y \to \langle 1, n \cdot m\rangle$ na $\langle 1, n \cdot m\rangle$. Niech $h\colon X \times Y \to \langle 1, n \cdot m\rangle$ będzie zdefiniowana wzorem: $h((x, y)) = g(y-1)n + f(x)$ dla $(x, y) \in X \times Y$. Łatwo sprawdzić (ćw.), że h jest bijekcją na $\langle 1, n \cdot m\rangle$. □

Stwierdzenie 10.24 (liczność zbioru funkcji między zbiorami skończonymi). *Jeśli $|X| = n$ oraz $|Y| = m$, to $|X^Y| = n^m$.*

Wniosek 10.25 (moc zbioru potęgowego). *Jeśli X jest zbiorem n-elementowym, to $|\mathcal{P}(X)| = 2^n$.*

Dowód. Wystarczy zastosować Stwierdzenie 10.24 i Stwierdzenie 12.5. □

Uwaga 10.26 (bardzo ważne wiadomości z dziesiątego wykładu). Podczas dziesiątego wykładu dowiedzieliśmy się m.in.:

- co to znaczy zliczać elementy zbioru skończonego
- jak porównywać liczności zbiorów skończonych
- jakie są podstawowe własności zbiorów skończonych
- jak formalnie definiujemy pojęcie równoliczności dwu zbiorów
- jakie własności ma pojęcie równoliczności.

ROZDZIAŁ 11

Zbiory nieskończone

W czasie poprzedniego wykładu poznaliśmy pojęcia zbioru skończonego, zbioru nieskończonego i równoliczności dwu zbiorów. Wyodrębnimy pewne istotne grupy zbiorów nieskończonych pod względem ich liczności. Zaznaczamy, że nie pojawiła się formalna definicja, czym jest *moc* zbioru nieskończonego.

1. Zbiory nieskończone i ich własności

Przypomnijmy, że zbiór X nazywaliśmy nieskończonym, jeśli nie był zbiorem skończonym. Zanim przejdziemy do głębszych obserwacji odnotujmy, prostą własność.

LEMAT 11.1. *Niech X będzie zbiorem nieskończonym. Wówczas dla każdego $x \in X$ mamy, że $X \setminus \{x\}$ jest nieskończony.*

DOWÓD. Załóżmy, że X jest zbiorem nieskończonym i niech $x \in X$. Przypuśćmy, że $X \setminus \{x\}$ jest zbiorem skończonym. Wówczas $X = (X \setminus \{x\}) \cup \{x\}$ jest zbiorem skończonym jako suma dwu zbiorów skończonych (patrz: Stwierdzenie 10.20), co daje sprzeczność. □

Zauważmy, że powyższy Lemat stoi za następującą konstrukcją: niech X będzie zbiorem nieskończonym. Ustalmy dowolnie $x_1 \in X$. Na mocy Lematu 11.1 zbiór $X \setminus \{x_1\}$ jest nieskończony, więc ustalmy $x_2 \in X \setminus \{x_1\}$. W szczególności wtedy $x_1 \neq x_2$ oraz znów wobec Lematu 11.1 zbiór $X \setminus \{x_1, x_2\} = (X \setminus \{x_1\}) \setminus \{x_2\}$ jest nieskończony. Postępując tak dalej, możemy zdefiniować dla $n \in \mathbb{N}$ element $x_n \in X \setminus \{x_1, ..., x_{n-1}\}$. Indukcyjnie definiujemy więc różnowartościowy ciąg elementów zbioru X zawarty w zbiorze X[1].

Powyższa konstrukcja jest dowodem następującego, ważnego twierdzenia:

TWIERDZENIE 11.2 (minimalność zbioru $\mathbb{N}$). *Jeśli zbiór X jest nieskończony, to istnieje funkcja różnowartościowa $h\colon \mathbb{N} \to X$.*

OZNACZENIE 11.3. *Dla zbiorów X, Y, analogicznie do oznaczenia w definicji równoliczności zbioru, istnienie funkcji różnowartościowej $h\colon X \to Y$ oznaczamy $|X| \leq |Y|$. Oznaczenie to jest zgodne z intuicją, gdyż funkcja różnowartościowa $h\colon X \to Y$ zanurza w zbiór X w zbiór Y.*

[1] Konstrukcja ta wykorzystuje *aksjomat wyboru*, który omówimy w ostatnim rozdziale. Wykorzystujemy prawidłowość, że $\mathcal{P} = \mathcal{P}(X) \setminus \{\emptyset\}$ istnieje funkcja $f : \mathcal{P} \to X$ taka, że $f(P) \in \mathcal{P}$ dla $P \in \mathcal{P}$.

Udowodnimy teraz pewną użyteczną charakterystykę zbiorów nieskończonych.

TWIERDZENIE 11.4. *Jeśli zbiór X jest nieskończony, to $|X| = |X \setminus \{x_0\}|$ dla dowolnego $x_0 \in X$. Innymi słowy, zbiór nieskończony jest równoliczny z pewnym swoim podzbiorem właściwym.*

DOWÓD. Załóżmy, że X jest nieskończony, i ustalmy dowolnie $x_0 \in X$. Wówczas wobec Lematu 11.1 zbiór $X \setminus \{x_0\}$ jest nieskończony. Stąd wobec Twierdzenia 11.2 istnieje funkcja różnowartościowa $h\colon \mathbb{N} \to X \setminus \{x_0\}$. Pokażemy, że zbiory X oraz $X \setminus \{x_0\}$ są równoliczne. Niech $f\colon X \to X \setminus \{x_0\}$ będzie określona wzorem: dla $x \in X$

$$f(x) = \begin{cases} h(1), \text{ gdy } x = x_0 \\ h(n+1), \text{ gdy } x = h(n) \text{ dla pewnego } n \in \mathbb{N} \\ x, \text{ w przeciwnym przypadku.} \end{cases}$$

Funkcja f jest bijekcją na $X \setminus \{x_0\}$. □

OZNACZENIE 11.5. *Skrótowo fakt, że Y jest podzbiorem właściwym zbioru X oznaczamy $Y \subsetneq X$.*

Pokażemy teraz, że powyższe rozumowanie można odwrócić.

TWIERDZENIE 11.6. *Niech X będzie takim zbiorem, że istnieje $Y \subsetneq X$ taki, że $|X| = |Y|$. Wówczas X jest nieskończony.*

DOWÓD. Załóżmy, że X jest takim zbiorem, że istnieje $Y \subsetneq X$ taki, że $|X| = |Y|$. Przypuśćmy, że X jest skończony, wówczas Y jest skończony jako podzbiór X. Skoro $Y \neq X$, to $|X| \neq |Y|$, co prowadzi do sprzeczności. □

Powyższe dwa Twierdzenia dają następujące wnioski:

WNIOSEK 11.7 (charakterystyka zbiorów nieskończonych). *Zbiór X jest nieskończony wtedy i tylko wtedy, gdy jest równoliczny z pewnym swoim podzbiorem właściwym.*

WNIOSEK 11.8 (charakterystyka zbiorów skończonych). *Zbiór X jest skończony wtedy i tylko wtedy, gdy każda funkcja różnowartościowa $f\colon X \to X$ jest bijekcją na X.*

DOWÓD. Wystarczy pokazać, że brak równoliczności X z każdym swoim podzbiorem właściwym oznacza dokładnie, że każda funkcja różnowartościowa $f\colon X \to X$ jest bijekcją na X.
„⇒” Załóżmy, że X nie jest równoliczny z żadnym swoim podzbiorem właściwym i niech $f\colon X \to X$ będzie funkcją różnowartościową. Jeśli f nie jest bijekcją na X, to $Y = f[X] \neq X$ oraz f jest bijekcją na Y. W szczególności $Y \subsetneq X$ oraz $X| = |Y|$. To daje sprzeczność.

„⇐” Załóżmy, że każda funkcja różnowartościowa $f\colon X \to X$ jest bijekcją na X. Przypuśćmy, że istnieje $Y \subsetneq X$ taki, że $|X| = |Y|$, tj. istnieje bijekcja $g\colon X \to Y$ na Y. W szczególności $g\colon X \to X$ jest różnowartościowa i nie jest bijekcją na X. Otrzymujemy sprzeczność. □

Warto jeszcze na koniec odnotować oczywistą obserwację:

STWIERDZENIE 11.9. *Nadzbiór zbioru nieskończonego jest zbiorem nieskończonym.*

2. Nieskończone zbiory równoliczne

Przeanalizujemy teraz kilka przykładów zbiorów nieskończonych pod względem ich równoliczności. Będziemy znacząco korzystać ze Stwierdzenia 10.8.

STWIERDZENIE 11.10. *Zbiory liczb parzystych oraz nieparzystych są równoliczne. Przy tym oba są równoliczne ze zbiorem* $\mathbb{N}$.

DOWÓD. Przyjmijmy oznaczenia: $2\mathbb{N} = \{2n \in \mathbb{N}\colon n \in \mathbb{N}\}$ i $2\mathbb{N} - 1 = \{2n - 1 \in \mathbb{N}\colon n \in \mathbb{N}\}$. Rozważmy funkcję $f\colon 2\mathbb{N} \to 2\mathbb{N} - 1$ określoną wzorem $f(n) = n - 1$ dla $n \in 2\mathbb{N}$. Wówczas f jest bijekcją na $2\mathbb{N} - 1$. Stąd $|2\mathbb{N}| = |2\mathbb{N} - 1|$. Ponadto funkcja $g\colon 2\mathbb{N} \to \mathbb{N}$ określona wzorem $g(n) = n/2$ dla $n \in 2\mathbb{N}$ jest bijekcją na $\mathbb{N}$. Stąd $|2\mathbb{N}| = |\mathbb{N}|$. Wobec Stwierdzenia 10.8 mamy więc $|\mathbb{N}| = |2\mathbb{N}| = |2\mathbb{N} - 1|$. □

STWIERDZENIE 11.11. *Zbiór liczb całkowitych* $\mathbb{Z}$ *jest równoliczny ze zbiorem liczb naturalnych.*

DOWÓD. Rozważmy funkcję $f\colon \mathbb{Z} \to \mathbb{N}$ określoną wzorem:

$$f(p) = \begin{cases} 0, \text{ jeśli } p = 0 \\ 2p, \text{ jeśli } p \in \mathbb{N} \\ -2p - 1, \text{ jeśli } -p \in \mathbb{N}. \end{cases}$$

Wówczas f jest bijekcją na $\mathbb{N}$. Zatem $|\mathbb{Z}| = |\mathbb{N}|$. □

STWIERDZENIE 11.12. *Niech* $a, b, c, d \in \mathbb{R}$ *będą takie, że* $a < b$ *oraz* $c < d$. *Przedziały* $[a, b]$ *i* $[c, d]$ *są równoliczne.*

DOWÓD. Niech $a, b, c, d \in \mathbb{R}$ będą takie, że $a < b$ oraz $c < d$. Funkcja $f\colon [a, b] \to [c, d]$ określona wzorem

$$f(x) = \frac{(x - a)(d - c)}{b - a} + c \text{ dla } x \in [a, b]$$

jest bijekcją na $[c, d]$. □

Powyższe wraz ze Stwierdzeniem 10.8 daje następujący wniosek:

Wniosek 11.13. *Dowolny przedział domknięty ograniczony jest równoliczny z przedziałem* $[0,1]$.

Stwierdzenie 11.14. *Niech* $a,b\in\mathbb{R}$ *będą takie, że* $a<b$. *Przedziały* $[a,b]$ *oraz* (a,b) *są równoliczne.*

Dowód. Niech $a,b\in\mathbb{R}$ będą takie, że $a<b$. Oczywiście każdy przedział jest zbiorem nieskończonym, więc wobec Twierdzenia 11.2 ustalmy funkcję różnowartościową $h\colon\mathbb{N}\to(a,b)$. Zdefiniujmy funkcję $f\colon[a,b]\to(a,b)$ wzorem: dla $x\in[a,b]$

$$f(x)=\begin{cases}h(1),\text{ gdy } x=a\\ h(2),\text{ gdy } x=b\\ h(n+2),\text{ gdy } x=h(n)\text{ dla pewnego } n\in\mathbb{N}\\ x,\text{ w przeciwnym przypadku.}\end{cases}$$

Wówczas f jest bijekcją na (a,b). □

Postępując analogicznie jak w dowodzie Stwierdzenia 11.14 można pokazać też, że:

Stwierdzenie 11.15. *Niech* $a,b\in\mathbb{R}$ *będą takie, że* $a<b$. *Przedziały* $(a,b],[a,b]$ *oraz* $[a,b)$ *są równoliczne.*

Stwierdzenie 11.16. *Przedział* $(-\frac{\pi}{2},\frac{\pi}{2})$ *jest równoliczny z* $\mathbb{R}$.

Dowód. Funkcja $\operatorname{tg}\colon(-\frac{\pi}{2},\frac{\pi}{2})\to\mathbb{R}$ jest bijekcją na $\mathbb{R}$. □

Czytelnik bez trudu sam zdefiniuje funkcje ustalające równoliczność między pozostałymi rodzajami przedziałów i uzyska następujący wniosek:

Wniosek 11.17. *Wszystkie przedziały: domknięte/otwarte/ograniczone/nieograniczone/jednostronnie otwarte/jednostronnie domknięte są równoliczne. Przy tym są też równoliczne z* $\mathbb{R}$.

Okazuje się, że nie wszystkie zbiory nieskończone są równoliczne.

Stwierdzenie 11.18. *Przedział* $[0,1]$ ***nie*** *jest równoliczny z* $\mathbb{N}$.

Dowód. Przypuśćmy, że $|\mathbb{N}|=|[0,1]|$, tj. że istnieje bijekcja $f\colon\mathbb{N}\to[0,1]$ na $[0,1]$. Oznacza to, że $[0,1]=\{f(n)\in[0,1]\colon n\in\mathbb{N}\}$. Rozważmy rozwinięcia dziesiętne – nieskończone! – wszystkich liczb $f(n)$ dla $n\in\mathbb{N}$:

$$f(1)=0,\ a_1^1\,a_1^2\,a_1^3\,a_1^4\ldots$$

$$f(2)=0,\ a_2^1\,a_2^2\,a_2^3\,a_2^4\ldots$$

$$f(3) = 0,\ a_3^1\ a_3^2\ a_3^3\ a_3^4\ ...$$

...

Rozważmy liczbę $x \in \mathbb{R}$, której rozwinięcie dziesiętne jest następujące:

$$x = 0,\ x^1\ x^2\ x^3\ x^4\ ...,$$

gdzie cyfra x^1 jest różna od a_1^1 i 9, cyfra x^2 jest różna od a_2^2 i 9, itd., tj. cyfra x^n jest różna a_n^n i 9. Z konstrukcji widać, że $x \in [0,1]$. Zarazem $x \neq f(n)$ dla każdego $n \in \mathbb{N}$, bo x różni się od $f(n)$ na n-tym miejscu po przecinku, zaś na pozostałych $(n+1, n+2, ...)$ nie występują same 9. Ostatecznie x jest liczbą z przedziału $[0,1]$, taką, że $x \notin \{f(n) \in [0,1] \colon n \in \mathbb{N}\}$. Otrzymujemy sprzeczność. □

Uwaga 11.19 (bardzo ważne wiadomości z jedenastego wykładu). Podczas jedenastego wykładu dowiedzieliśmy się m.in.:

- co to są zbiory nieskończone i jakie mają własności
- jak można scharakteryzować zbiory nieskończone
- jakie pary zbiorów nieskończonych są równoliczne.

ROZDZIAŁ 12

Twierdzenia Cantora, Cantora-Bernsteina i o dychotomii

Na poprzednim wykładzie pojawił się szereg przykładów par zbiorów nieskończonych, które są albo które nie są równoliczne. Prezentowane zbiory można połączyć w dwie grupy: równolicznych z $\mathbb{N}$ oraz równolicznych z $\mathbb{R}$. Natychmiastowym zaś wnioskiem jest, że nie wszystkie zbiory nieskończone są równoliczne, na co mogłaby wskazywać ogólność definicji. Do tego podziału wrócimy w dalszej części wykładu. Teraz zaś skupimy się na pewnych ogólnych i dość głębokich twierdzeniach dotyczących porównywania dwu zbiorów względem ich liczności. Niech X, Y, Z będą dowolnymi zbiorami.

1. Twierdzenie Cantora

Wątpliwości dotyczące wrażenia, że wszystkie nieskończone zbiory są równoliczne, zostały potwierdzone Stwierdzeniem 11.18. Przykład ten nie jest odosobniony, można bowiem pokazać, że konstrukcja zbiorów coraz to bardziej licznych jest prosta, i dysponujemy już odpowiednimi do tego narzędziami. Przypomnijmy jeszcze dwa oznaczenia, które pojawiły się w czasie poprzedniego wykładu: dla zbiorów X, Y:

- $|X| = |Y|$ oznacza, że zbiory X i Y są równoliczne, czyli istnieje bijekcja $f\colon X \to Y$ na Y
- $|X| \leq |Y|$ oznacza, że istnieje funkcja różnowartościowa $f\colon X \to Y$.

W dalszej części, z powodów technicznych, będziemy rozważali tylko niepuste zbiory (choć wszystkie twierdzenia i własności dla zbioru pustego pozostają prawdziwe).

Twierdzenie 12.1 (twierdzenie Cantora). *Dla dowolnego zbioru X mamy $|X| \neq |\mathcal{P}(X)|$, tj. żaden zbiór X nie jest równoliczny ze zbiorem $\mathcal{P}(X)$ wszystkich swoich podzbiorów.*

Dowód. Przypuśćmy, że istnieje taka funkcja $f\colon X \to \mathcal{P}(X)$, która jest bijekcją na $\mathcal{P}(X)$. Oznacza to, że dla każdego $A \subseteq X$ istnieje $x \in X$ taki, że $f(x) = A$. W szczególności istnieje $x_0 \in X$ taki, że $f(x_0) = \emptyset$. Mamy przy tym, że $x_0 \notin f(x_0)$. Rozważmy zbiór wszystkich takich elementów, tzn.:

$$Y = \{x \in X\colon x \notin f(x)\}.$$

Skoro $Y \subseteq X$, to $Y \in \mathcal{P}(X)$, zatem istnieje $y \in X$ taki, że $f(y) = Y$. Mamy możliwości:

- jeśli $y \in Y$, to $y \notin f(y) = Y$, co prowadzi do sprzeczności

• jeśli $y \notin Y$, to $y \in f(y) = Y$, co także prowadzi do sprzeczności.

Uzyskana sprzeczność wynika z przypuszczenia, że f jest bijekcją na $\mathcal{P}(X)$. Zatem nie istnieje bijekcja X na $\mathcal{P}(X)$. □

STWIERDZENIE 12.2. *Dla dowolnego zbioru X istnieje funkcja różnowartościowa $f\colon X \to \mathcal{P}(X)$.*

DOWÓD. Funkcja $f\colon X \to \mathcal{P}(X)$ określona wzorem $f(x) = \{x\}$ dla $x \in X$ jest różnowartościowa. □

Wobec powyższego stwierdzenia $|X| \leq |\mathcal{P}(X)|$ dla dowolnego zbioru X. W szczególności, wobec Twierdzenia Cantora, $|X| \neq |\mathcal{P}(X)|$. Przyjmijmy następujące oznaczenie:

OZNACZENIE 12.3. *Dla dowolnych zbiorów X, Y zależność, że $|X| \leq |Y|$ oraz $|X| \neq |Y|$ oznaczamy $|X| < |Y|$.*

PRZYKŁAD 12.4. Twierdzenie 11.2 oraz Stwierdzenie 11.18 implikują, że $|\mathbb{N}| < |[0,1]|$.

STWIERDZENIE 12.5 (moc zbioru potęgowego dowolnego zbioru). *Dla dowolnego zbioru X zachodzi*

$$|\mathcal{P}(X)| = |\{0,1\}^X|.$$

DOWÓD. Dla dowolnego $A \in \mathcal{P}(X)$ rozważmy jego funkcję charakterystyczną:

$$\chi_A(x) = \begin{cases} 0, \text{ gdy } x \notin A \\ 1, \text{ gdy } x \in A. \end{cases}$$

Wówczas $\chi_A \in \{0,1\}^X$. Funkcja $f\colon \mathcal{P}(X) \to \{0,1\}^X$ zadana wzorem $f(A) = \chi_A$ jest różnowartościowa. Istotnie, jeśli $A \neq B$ oraz $x \in A \setminus B$, to $\chi_A(x) = 1 \neq 0 = \chi_B(x)$. Podobnie, jeśli $x \in B \setminus A$, to $\chi_A(x) = 0 \neq 1 = \chi_B(x)$. Zatem $\chi_A \neq \chi_B$.

Jeśli $h \in \{0,1\}^X$, to definiując $A = h^{-1}[\{1\}]$, mamy dla dowolnego $x \in X$:

$$\chi_A(x) = 1 \iff x \in A \iff x \in h^{-1}[\{1\}] \iff h(x) = 1,$$

$$\chi_A(x) = 0 \iff \chi_A(x) \neq 1 \iff h(x) \neq 1 \iff h(x) = 0.$$

Stąd $f(A) = h$. To oznacza, że f jest suriekcją na $\{0,1\}^X$. W konsekwencji f jest bijekcją na $\{0,1\}^X$. □

Wnioskiem z powyższego i ze Stwierdzenia 10.10 jest następujący:

WNIOSEK 12.6. *Jeśli $|X| = |Y|$, to $|\mathcal{P}(X)| = |\mathcal{P}(Y)|$.*

DOWÓD. Skoro $|X| = |Y|$, to $|\{0,1\}^X| = |\{0,1\}^Y|$ na mocy Stwierdzenia 10.10. Wobec Stwierdzenia 12.5 otrzymujemy:

$$|\mathcal{P}(X)| = |\{0,1\}^X| = |\{0,1\}^Y| = |\mathcal{P}(Y)|.$$

□

2. Twierdzenie Cantora-Bernsteina

Wiemy już, że dla zbiorów X, Y symbol $|X| \leq |Y|$ oznacza istnienie funkcji różnowartościowej $f\colon X \to Y$. W szczególności f jest bijekcją na $f[X]$, więc X jest równoliczny z pewnym podzbiorem zbioru Y. Zachodzi też bardzo użyteczna charakteryzacja.

STWIERDZENIE 12.7. *Niech $X \neq \emptyset$. $|X| \leq |Y|$ wtedy i tylko wtedy, gdy istnieje suriekcja $g\colon Y \to X$ na X.*

DOWÓD. „⇒" Załóżmy, że $|X| \leq |Y|$, czyli, że istnieje funkcja różnowartościowa $f\colon X \to Y$. Mamy oczywiście, że f jest bijekcją na $f[X] \subseteq Y$. Ustalmy $x_0 \in X$ i zdefiniujmy funkcję $g\colon Y \to X$ wzorem: dla $y \in Y$

$$g(y) = \begin{cases} f^{-1}(y), \text{ gdy } y \in f[X] \\ x_0, \text{ w przeciwnym przypadku.} \end{cases}$$

Łatwo zauważyć, że g jest suriekcją na X.

„⇐" Załóżmy, że istnieje suriekcja $g\colon Y \to X$ na X. Wówczas $g^{-1}[\{x\}] \neq \emptyset$ dla każdego $x \in X$. Zdefiniujmy funkcję $f\colon X \to Y$ wzorem $f(x) = y_x$, gdzie $y_x \in g^{-1}[\{x\}]$ jest jakkolwiek wybrany. Wówczas f jest różnowartościowa – istotnie gdy $x_1, x_2 \in X$ są różne, to oczywiście $g^{-1}[\{x_1\}] \cap g^{-1}[\{x_2\}] = \emptyset$ więc $y_{x_1} \neq y_{x_2}$. □

Przejdziemy teraz do analizy własności pojęcia porównywania zbiorów względem ich liczności, czyli do „relacji" $\leq$. Warto w tym miejscu przypomnieć, że obiekt $|X|$ jest zdefiniowany dla klasy zbiorów równolicznych z X. Stąd też $\leq$, zdefiniowana wśród obiektów $|X|$, nie jest relacją, gdyż obiekty $|X|$ nie tworzą zbioru.

STWIERDZENIE 12.8. *Dla dowolnych zbiorów X, Y, Z mamy:*

1. *Jeśli $X \subseteq Y$, to $|X| \leq |Y|$; w szczególności $|X| \leq |X|$*
2. *Jeśli $|X| \leq |Y|$ i $|Y| \leq |Z|$, to $|X| \leq |Z|$.*

DOWÓD. Niech X, Y, Z będą dowolnymi zbiorami.

Ad 1. Załóżmy, że $X \subseteq Y$. Funkcja $id_X\colon X \to Y$ jest różnowartościowa, więc $|X| \leq |Y|$.

Ad 2. Załóżmy, że $|X| \leq |Y|$ i $|Y| \leq |Z|$, czyli istnieją funkcje różnowartościowe $f\colon X \to Y$ oraz $g\colon Y \to Z$. Z Wykładu 5. wiemy, że $g \circ f\colon X \to Z$ jest różnowartościowa, więc $|X| \leq |Z|$. □

Powyższe stwierdzenie pokazuje, że $\leq$ ma własności zwrotności i przechodniości. Nieco trudniej jest pokazać, że $\leq$ ma też własność słabej antysymetrii.

Twierdzenie 12.9 (twierdzenie Cantora-Bernsteina). *Dla dowolnych zbiorów A, B zachodzi implikacja*:

$$\textit{jeśli } |A| \leq |B| \textit{ oraz } |B| \leq |A|, \textit{ to } |A| = |B|.$$

Zanim przedstawimy dowód twierdzenia Cantora-Bernsteina, rozważmy następujący eksperyment myślowy zwany hotelem Hilberta. W **hotelu Hilberta** jest nieskończenie wiele pokoi ponumerowanych liczbami naturalnymi $1, 2, 3, ...$ Załóżmy, że w każdym pokoju jest dokładnie jeden gość. Tymczasem w drzwiach hotelu pojawia się nowy gość. Pracownicy hotelu znajdują dla niego miejsce, przesuwając gościa z pokoju nr n do pokoju nr $n + 1$, dla każdego $n \in \mathbb{N}$. W ten sposób pokój nr 1 staje się wolny i można w nim umieścić nowego gościa. Obsługa hotelu może dokonać czegoś więcej. Jeśli u drzwi hotelu pojawi się nieskończenie wielu gości: $g_1, g_2, g_3, ...$, to przemieszczając obecnych gości z pokoju nr n do pokoju nr $2n$ dla każdego $n \in \mathbb{N}$, można umieścić nowych gości w zwolnionych pokojach: gościa g_n w pokoju nr $2n - 1$, dla każdego $n \in \mathbb{N}$.

Dowód twierdzenia Cantora-Bernsteina. **Idea dowodu**[1] jest następująca. $|A| \leq |B|$ i $|B| \leq |A|$ oznacza, że istnieją funkcje różnowartościowe $f : A \to B$ oraz $g : B \to A$. O zbiorze A myślimy jako o gościach, a o zbiorze B myślimy jako o pokojach w hotelu. Na początku hotel jest zapełniony gośćmi. Funkcja $g : B \to A$ przyporządkowuje pokoje do gości hotelowych w sposób różnowartościowy. Jednak nie każdy gość ma przyporządkowany pokój, a jedynie ci ze zbioru $g[B]$. Funkcja f pokazuje, jak wszystkich gości można by umieścić w pokojach hotelowych (każdego w dokładnie jednym pokoju). Jeśli ich w ten sposób ulokować, zajmą oni tylko pokoje ze zbioru $f[A]$. Naszym celem jest umieszczenie każdego gościa w dokładnie jednym pokoju tak, by wszystkie pokoje były zajęte, czyli skonstruowanie bijekcji $h : A \to B$.

Przez $A_0 = A \setminus g[B]$ oznaczmy gości, którzy nie mają swojego pokoju w hotelu. Tych gości przeniesiemy do pokoi $f[A_0]$. Jednak te miejsca są już zajęte przez gości ze zbioru $A_1 = g[f[A_0]]$. Musimy tych gości gdzieś przenieść. Przenosimy ich do pokoi $f[A_1]$. Jednak te miejsca są zajęte przez gości ze zbioru $A_2 = g[f[A_1]]$. Postępując w ten sposób definiujemy zbiory $A_{n+1} = g[f[A_n]]$. Ich sumę $\bigcup_{n=0}^{\infty} A_n$ oznaczmy przez A_∞. Zbiór A_∞ składa się z gości A_0, którzy na początku nie mieli miejsc w hotelu,

[1] Jeżeli z tekstu dowodu usunąć wszystko, co mówi o hotelu, pokojach i gościach, to otrzymamy czysty matematyczny dowód.

oraz gości, którzy zostali przeniesieni. Zdefiniujmy odwzorowanie $h : A \to B$ wzorem:

$$h(x) = \begin{cases} f(x), \text{ gdy } x \in A_\infty \\ g^{-1}(x), \text{ w przeciwnym przypadku.} \end{cases}$$

Funkcja h działa w następujący sposób: jeśli x jest nowym gościem lub należał do A_n dla $n \geq 1$, to umieszczamy go w hotelu tak, jak mówi funkcja f. W przeciwnym razie pozostawiamy gościa hotelowego w pokoju, który zajmował.

Sprawdźmy, że h jest równowartościowa. Niech $x, y \in A$ i załóżmy, że $h(x) = h(y)$. Pokażemy, że $x = y$. Rozważmy przypadki:

- Jeżeli $x, y \in A_\infty$, to $h(x) = f(x)$ i $h(y) = f(y)$. Zatem $f(x) = f(y)$, więc równość $x = y$ wynika z różnowartościowości f.
- Jeżeli $x, y \in A \setminus A_\infty$, to $h(x) = g(x)$ i $h(y) = g(y)$. Teraz równość $x = y$ wynika z różnowartościowości g.
- Jeżeli $x \in A_\infty$ i $y \in A \setminus A_\infty$, to istnieje indeks $n \geq 0$ taki, że $x \in A_n$. Wtedy $f(x) = h(x) = h(y) = g^{-1}(y)$, a zatem $y = g(f(x)) \in g[f[A_n]] = A_{n+1}$. To jednak przeczy temu, że $y \notin A_\infty$. Zatem ten przypadek nie jest możliwy.
- Przypadek $y \in A_\infty$ i $x \in A \setminus A_\infty$ też nie jest możliwy.

Sprawdźmy teraz, że h jest suriekcją na B. W tym celu weźmy dowolny element $z \in B$. Niech $x = g(z)$. Możliwe są dwa przypadki:

- Jeżeli $x \notin A_\infty$, to $h(x) = g^{-1}(x) = z$.
- Jeżeli $x \in A_\infty$, to $x \in A_n$ dla pewnego $n \in \mathbb{N}$. Skoro $x = g(z) \in g[B]$ oraz $g[B] \cap A_0 = \emptyset$, to $n \neq 0$. A wtedy $x \in g[f[A_{n-1}]]$. Zatem istnieje taki $x' \in A_{n-1}$, że $x = g(f(x'))$. Wówczas $z = g^{-1}(x) = g^{-1}(g(f(x'))) = f(x') = h(x')$.

To pokazuje, że h jest suriekcją na B, a w konsekwencji bijekcją. To kończy dowód twierdzenia Cantora-Bernsteina. □

Twierdzenie Cantora-Bernsteina jest bardzo użyteczne przy sprawdzaniu równoliczności dwu zbiorów nieskończonych, gdyż określa, że wystarcza skonstruować jedynie dwie funkcje różnowartościowe (a nie bezpośrednio jedną bijekcję).

3. Twierdzenie o dychotomii

Ostatnią, ale najważniejszą własnością $\leq$ jest jej liniowość – czyli fakt, że dowolne dwa zbiory można porównać w sensie liczności. Dowód poniższego twierdzenia jest trudniejszy, więc przedstawimy jego szkic, który okaże się być wstępem do ostatniego Wykładu.

TWIERDZENIE 12.10 (twierdzenie o dychotomii). *Dla dowolnych zbiorów X i Y zachodzi alternatywa*

$$|X| \leq |Y| \text{ lub } |Y| \leq |X|.$$

SZKIC DOWODU TWIERDZENIA O DYCHOTOMII. Celem dowodu jest konstrukcja maksymalnego podzbioru $f \subseteq X \times Y$, który jest funkcją różnowartościową taką, że $\mathrm{dom}(f) \subseteq X$ oraz $\mathrm{rng}(f) \subseteq Y$. W przypadku, gdy dla tego maksymalnego obiektu będziemy mieli $\mathrm{dom}(f) = X$, to wtedy $|X| \leq |Y|$, zaś gdy będziemy mieli $\mathrm{rng}(f) = Y$, to wtedy $|Y| \leq |X|$ (patrz: Stwierdzenie 12.7).

Ustalmy $x_1 \in X$ oraz $y_1 \in Y$ i zdefiniujmy zbiór $f_1 = \{(x_1, y_1)\}$. Jeśli $\mathrm{dom}(f_1) = X$ lub $\mathrm{rng}(f_1) = Y$, to konstrukcja się kończy. Jeśli tak nie jest, to ustalmy $x_2 \in X \setminus \mathrm{dom}(f_1)$ oraz $y_2 \in Y \setminus \mathrm{rng}(f_1)$ i rozszerzmy funkcję f_1 do zbioru $f_2 = \{(x_1, y_1), (x_2, y_2)\}$. Znów, jeśli $\mathrm{dom}(f_2) = X$ lub $\mathrm{rng}(f_2) = Y$, to konstrukcja się kończy. Jeśli nie, to postępujemy tak dalej. W tym miejscu widać, że jeśli któryś ze zbiorów X, Y jest skończony, to po skończenie wielu krokach konstrukcja się zakończy. Jeśli któryś ze zbiorów X, Y jest równoliczny z $\mathbb{N}$, to zasada indukcji matematycznej pozwoli zakończyć konstrukcję. Co jednak, jeśli oba zbiory X, Y spełniają $|X| > |\mathbb{N}|$ i $|Y| > |\mathbb{N}|$?

Widać, że w takim przypadku konieczny jest inny aksjomat (inny niż zasada indukcji matematycznej), który taką konstrukcję zakończy „w którymś momencie". Zauważmy jeszcze przy tym, że każdy kolejny krok rozszerza nam dotychczas zdefiniowany zbiór (będący funkcją) – tworzymy tym samym wstępujący ciąg zbiorów i oczekujemy, że w którymś momencie uzyskamy element maksymalny (taki zbiór, którego już nie będziemy mogli rozszerzyć) kończący konstrukcję. Odpowiedzią na to zapotrzebowanie jest Lemat Kuratowskiego-Zorna, który opiszemy podczas ostatniego wykładu. □

UWAGA 12.11 (bardzo ważne wiadomości z dwunastego wykładu). Podczas dwunastego wykładu dowiedzieliśmy się m.in.:

- co to jest Twierdzenie Cantora
- jakie własności ma „relacja" $\leq$ między mocami zbiorów (m.in. twierdzenie Cantora-Bernsteina)
- że dowolne dwa zbiory można porównać w sensie liczności (twierdzenie o dychotomii).

ROZDZIAŁ 13

Zbiory przeliczalne i nieprzeliczalne

1. Zbiory przeliczalne

Twierdzenie 11.2 pokazuje, że wśród zbiorów nieskończonych, zbiór $\mathbb{N}$ jest w sensie mocy najmniejszy, bo każdy zbiór nieskończony zawiera podzbiór równoliczny z $\mathbb{N}$. Dodatkowo w czasie Wykładu 11. poznaliśmy wiele przykładów zbiorów równolicznych właśnie $\mathbb{N}$. Te obserwacje prowadzą do wyodrębnienia pewnej kolejnej (po zbiorach skończonych) grupy zbiorów pod względem ich liczności.

Definicja 13.1 (zbiór przeliczalny). *Zbiór X nazywamy przeliczalnym, jeśli $|X| \leq |\mathbb{N}|$, tj. jeśli X jest równoliczny z pewnym podzbiorem zbioru $\mathbb{N}$.*

Wniosek 13.2 (charakterystyka przeliczalności). *Niech X będzie dowolnym niepustym zbiorem. Następujące warunki są równoważne*

1. *Zbiór X jest przeliczalny*
2. *Zbiór X jest skończony lub zbiór X jest równoliczny ze zbiorem liczb naturalnych*
3. *Istnieje suriekcja $f\colon \mathbb{N} \to X$ na X*
4. *Zbiór X możemy zapisać jako $X = \{x_n \colon n \in \mathbb{N}\}$.*

Dowód. Równoważność warunków 1. i 2. wynika z Twierdzenia 11.2 (oraz Twierdzenia 12.9). Równoważność warunków 1. i 2. wynika ze Stwierdzenia 12.7. Jeśli zachodzi 3., to kładąc $x_n = f(n)$ otrzymujemy $X = f[\mathbb{N}] = \{f(n) : n \in \mathbb{N}\} = \{x_n \colon n \in \mathbb{N}\}$. Jeśli zachodzi 4., to definiujemy funkcję $f : \mathbb{N} \to X$ następująco: $f(n) = x_n$. Wtedy $X = \{x_n \colon n \in \mathbb{N}\} = \{f(n) \colon n \in \mathbb{N}\} = f[\mathbb{N}]$, co oznacza, że f jest funkcją na X. □

Ze Stwierdzenia 12.8 i definicji przeliczalności wynika następnie:

Stwierdzenie 13.3. *Podzbiór zbioru przeliczalnego jest przeliczalny.*

Dowód. Niech X będzie zbiorem przeliczalnym i niech $Y \subseteq X$. Przeliczalność X oznacza, że $|X| \leq |\mathbb{N}|$. Skoro $Y \subseteq X$, to na mocy Stwierdzenia 12.8 otrzymujemy $|Y| \leq |X|$. Fakt, że $|Y| \leq |X|$ i $|X| \leq |\mathbb{N}|$ implikuje $|Y| \leq |\mathbb{N}|$ (tu ponownie skorzystaliśmy ze Stwierdzenia 12.8). To oznacza, że Y jest zbiorem przeliczalnym. □

Może się zdarzyć, że właściwy podzbiór zbioru przeliczalnego jest z nim równoliczny (patrz: Stwierdzenie 11.10). Zarazem istnieją zbiory, które nie są równoliczne z $\mathbb{N}$ (patrz: Stwierdzenie 11.18). Jak widać z powyższego zbiór liczb naturalnych (a właściwie jego liczność) jest w pewnym sensie graniczna, dlatego warto wprowadzić pewne oznaczenie na $|\mathbb{N}|$. Z reguły moce zbiorów oznacza się literami hebrajskiego alfabetu (w teorii liczb kardynalnych), zaś dla zbioru $\mathbb{N}$ rezerwuje się pierwszą literę: alef, z indeksem 0. Oznaczmy więc $|\mathbb{N}| = \aleph_0$. W szczególności wobec przykładów z Wykładu 12. mamy:

$$|\mathbb{N}| = |2\mathbb{N}| = |2\mathbb{N} - 1| = |\mathbb{Z}| = \aleph_0.$$

W dalszej części sekcji zajmiemy się ogólnymi własnościami zbiorów przeliczalnych.

Stwierdzenie 13.4. *Zbiór $\mathbb{N} \times \mathbb{N}$ jest przeliczalny i nieskończony, tzn. $|\mathbb{N} \times \mathbb{N}| = \aleph_0$.*

Dowód. W dowodzie pokażemy, jak użytecznym narzędziem jest Twierdzenie Cantora-Bernsteina. Oczywiście $|\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$, bo funkcja $f\colon \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ określona wzorem $f(n) = (n, 1)$, jest różnowartościowa. Wskażemy teraz funkcję $g\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, która jest też różnowartościowa. Niech g będzie dana wzorem dla $n, m \in \mathbb{N}$:

$$g(n, m) = 2^n 3^n.$$

Można sprawdzić, że g jest różnowartościowa. Zatem $|\mathbb{N} \times \mathbb{N}| < |\mathbb{N}|$. Użycie Twierdzenia Cantora-Bernsteina kończy dowód. □

Uwaga 13.5. Przeliczalność $\mathbb{N}\times\mathbb{N}$ można wykazać też, bezpośrednio wskazując suriekcję $f\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ na $\mathbb{N} \times \mathbb{N}$, czyli innymi słowy, numerując liczbami naturalnymi wszystkie elementy zbioru $\mathbb{N} \times \mathbb{N}$.

Łatwym wnioskiem ze Stwierdzenia 13.4 jest następujący:

Wniosek 13.6 (przeliczalność produktu zbiorów przeliczalnych). *Jeśli X, Y są zbiorami przeliczalnymi, to ich iloczyn kartezjański $X \times Y$ jest przeliczalny.*

Dowód. Niech $f\colon \mathbb{N} \to X$ oraz $g\colon \mathbb{N} \to Y$ będą suriekcjami odpowiednio na X oraz Y. Rozważmy funkcję $h\colon \mathbb{N} \times \mathbb{N} \to X \times Y$ określoną wzorem: dla $(n, m) \in \mathbb{N} \times \mathbb{N}$

$$h((n, m)) = (f(n), g(m)).$$

Można sprawdzić, że h jest suriekcją na $X \times Y$. Stąd $|X \times Y| \leq |\mathbb{N} \times \mathbb{N}|$ i wobec Stwierdzenia 13.4 i Stwierdzenia 12.7 mamy $|X \times Y| \leq |\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$. □

Uwaga 13.7. Indukcyjnie łatwo uogólnić Wniosek 13.6, uzyskując: produkt skończenie wielu zbiorów przeliczalnych jest zbiorem przeliczalnym.

Kolejne własności będą dotyczyły sumy zbiorów przeliczalnych.

STWIERDZENIE 13.8. *Jeśli A, B są zbiorami przeliczalnymi, to $A \cup B$ jest zbiorem przeliczalnym.*

DOWÓD. Skoro A, B są zbiorami przeliczalnymi, to na mocy Wniosku 13.2 można je zapisać jako $A = \{a_n : n \in \mathbb{N}\}$ i $B = \{b_n : n \in \mathbb{N}\}$. Wówczas $A \cup B = \{c_n : n \in \mathbb{N}\}$, gdzie $c_1 := a_1$, $c_2 := b_1$, $c_3 := a_2$, $c_4 := b_2, \ldots$. To oznacza, że $A \cup B$ jest przeliczalny. □

TWIERDZENIE 13.9 (przeliczalność sumy zbiorów przeliczalnych). *Jeśli $\mathcal{P} = \{P_n\}$ jest rodziną przeliczalną zbiorów (ciągiem zbiorów) i każdy jej element jest zbiorem przeliczalnym, to $\bigcup_{n=1}^{\infty} P_n$ jest zbiorem przeliczalnym. Innymi słowy: przeliczalna suma zbiorów przeliczalnych jest zbiorem przeliczalnym.*

Oczywiście Stwierdzenie 13.8 jest łatwym wnioskiem z Twierdzenia 13.9.

DOWÓD TWIERDZENIA 13.9. Załóżmy, że $\mathcal{P}$ jest przeliczalną rodziną zbiorów przeliczalnych, tj. $\mathcal{P} = \{P_n : n \in \mathbb{N}\}$ oraz $|P_n| \leq |\mathbb{N}|$ dla $n \in \mathbb{N}$. Pokażemy, że $P = \bigcup_{n \in \mathbb{N}} P_n$ jest zbiorem przeliczalnym, wskazując suriekcję $f : \mathbb{N} \times \mathbb{N} \to P$ na P. Niech $n \in \mathbb{N}$. Skoro P_n jest przeliczalny, to istnieje suriekcja $f_n : \mathbb{N} \to P_n$ na P_n. Zdefiniujmy funkcję f dla $(n, m) \in \mathbb{N} \times \mathbb{N}$ wzorem:

$$f((n, m)) = f_n(m).$$

Wówczas f jest suriekcją na P. Istotnie, niech $p \in P$, wtedy istnieje $n_0 \in \mathbb{N}$ takie, że $p \in P_{n_0}$. Ponadto istnieje $m_0 \in \mathbb{N}$ takie, że $f_{n_0}(m_0) = p$. Ostatecznie $f((n_0, m_0)) = p$. Stąd $|P| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, stąd P jest przeliczalny. □

Rozważania o zbiorach przeliczalnych zakończymy kolejnym naturalnym przykładem nieskończonego zbioru równolicznego z $\mathbb{N}$.

TWIERDZENIE 13.10. *Zbiór liczb wymiernych $\mathbb{Q}$ jest przeliczalny i nieskończony, tzn. $|\mathbb{Q}| = \aleph_0$.*

DOWÓD. Wobec Stwierdzeń 13.6 i 11.11 mamy, że zbiór $\mathbb{Z} \times \mathbb{N}$ jest przeliczalny. Rozważmy funkcję $f : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$ określoną dla $(n, m) \in \mathbb{Z} \times \mathbb{N}$ wzorem:

$$f((n, m)) = \frac{n}{m}.$$

Łatwo zauważyć, że f jest suriekcją na $\mathbb{Q}$, zatem $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N}| = |\mathbb{N}|$. Zarazem $\mathbb{N} \subseteq \mathbb{Q}$, więc ze Stwierdzenia 12.7 $|\mathbb{N}| \leq |\mathbb{Q}|$. Wobec Twierdzenia Cantora-Bernsteina mamy więc $|\mathbb{Q}| = |\mathbb{N}|$. □

Poznaliśmy już szereg przykładów i własności zbiorów przeliczalnych. Jednocześnie jednak wiemy już też, że istnieją zbiory nieskończone, które nie są równoliczne z $\mathbb{N}$ – nie są zbiorami przeliczalnymi.

Podobny wniosek płynie też z Twierdzenia Cantora, mianowicie zbiór $\mathcal{P}(\mathbb{N})$ jest taki, że $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$. Prowadzi to do następującej definicji:

Definicja 13.11 (zbiór nieprzeliczalny). *Zbiór X nazywamy nieprzeliczalnym, jeśli nie jest zbiorem przeliczalnym. Równoważnie, gdy $|\mathbb{N}| < |X|$.*

2. Zbiory nieprzeliczalne i zbiory mocy continuum

W czasie Wykładu 12. poznaliśmy już kilka przykładów zbiorów nieprzeliczalnych.

Przykład 13.12. Wszystkie przedziały: domknięte/otwarte/ograniczone/nieograniczone/jednostronnie otwarte/jednostronnie domknięte oraz zbiory $\mathbb{R}, \mathcal{P}(\mathbb{N})$ nie są równoliczne z $\mathbb{N}$, więc są nieprzeliczalne.

Widzimy, że pozornie podobną rolę, jak dla zbiorów przeliczalnych grał zbiór $\mathbb{N}$, dla zbiorów nieprzeliczalnych gra zbiór $\mathbb{R}$. Warto więc jakoś wyodrębnić grupę zbiorów równolicznych z $\mathbb{R}$ i wprowadzić oznaczenie na $|\mathbb{R}|$. W literaturze przyjmuje się, że moc zbioru $\mathbb{R}$ oznacza się literą $\mathfrak{c}$ i mówi się, że $\mathbb{R}$ jest zbiorem mocy continuum.

Zaczniemy od bardzo istotnego twierdzenia.

Twierdzenie 13.13 (równoliczność $\mathbb{R}$ i $\mathcal{P}(\mathbb{N})$). *Zbiór liczb rzeczywistych $\mathbb{R}$ jest równoliczny ze zbiorem wszystkich podzbiorów zbioru liczb naturalnych, tzn. $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$. Innymi słowy $\mathcal{P}(\mathbb{N})$ jest mocy continuum.*

Dowód. Z kursu analizy matematycznej wiemy, że każda liczba rzeczywista $x \in \mathbb{R}$ jest kresem dolnym wszystkich liczb wymiernych większych od x, tj. $x = \inf\{q \in \mathbb{Q}\colon x < q\}$. Niech funkcja $g : \mathcal{P}(\mathbb{Q}) \setminus \{\emptyset\} \to \mathbb{R} \cup \{-\infty\}$ będzie dana wzorem $g(A) = \inf A$ dla $A \subset \mathbb{Q}$, $A \neq \emptyset$. Wówczas g jest suriekcją na $\mathbb{R} \cup \{-\infty\}$. Zatem $|\mathbb{R} \cup \{-\infty\}| \leq |\mathcal{P}(\mathbb{Q}) \setminus \{\emptyset\}|$. Na mocy Twierdzenia 11.4 otrzymujemy: $|\mathbb{R} \cup \{-\infty\}| = |\mathbb{R}|$ oraz $|\mathcal{P}(\mathbb{Q}) \setminus \{\emptyset\}| = |\mathcal{P}(\mathbb{Q})|$. Stąd $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})|$. Jednoczenie skoro $|\mathbb{Q}| = |\mathbb{N}|$, to $|\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})|$ (patrz: Wniosek 12.6). Zatem $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{N})|$.

Ponieważ $|\{0,1\}^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|$ (stwierdzenie 12.5), to pozostaje wykazać, że $|\{0,1\}^{\mathbb{N}}| \leq |\mathbb{R}|$ i zastosować Twierdzenie Cantora-Bernsteina. Rozważmy funkcję $f\colon \{0,1\}^{\mathbb{N}} \to \mathbb{R}$ określoną wzorem: dla $x \in \{0,1\}^{\mathbb{N}}$ niech $f(x)$ będzie liczbą rzeczywistą, której rozwinięcie dziesiętne, to $0,\ x(1)\ x(2)\ x(3)\ \ldots$. Niech $x, y \in \{0,1\}^{\mathbb{N}}$ będą takie, że $x \neq y$. Niech $m = \min\{n \in \mathbb{N}\colon x(n) \neq y(n)\}$. Wówczas $f(x) \neq f(y)$, bo liczby te różnią się na m-tym miejscu po przecinku. Zatem f jest różnowartościowa i w konsekwencji $|\{0,1\}^{\mathbb{N}}| \leq |\mathbb{R}|$. Twierdzenie Cantora-Bernsteina kończy dowód. □

W dalszej części skupimy się na innych przykładach zbiorów mocy continuum i na własnościach zbiorów nieprzeliczalnych. Pamiętamy, że każdy podzbiór zbioru przeliczalnego jest zbiorem przeliczalnym. W przypadku zbiorów nieprzeliczalnych ich nadzbiory są nieprzeliczalne.

STWIERDZENIE 13.14. *Załóżmy, że X jest zbiorem nieprzeliczalnym oraz $X \subseteq Y$. Wówczas Y jest nieprzeliczalny.*

DOWÓD. Gdyby Y był przeliczalny, to X jako jego podzbiór też byłby przeliczalny. Zatem Y nie jest przeliczalny. □

Kolejne własności sformułujemy w terminach zbiorów mocy continuum, gdyż te są bardziej dla nas interesujące (ogólna teoria tzw. arytmetyki liczb kardynalnych jest zbyt skomplikowana na ten moment, ale zainteresowanych słuchaczy odsyłamy do literatury uzupełniającej).

TWIERDZENIE 13.15 (produkt zbiorów mocy continuum). *Jeśli X, Y są zbiorami mocy continuum, to ich produkt $X \times Y$ również jest mocy continuum.*

DOWÓD. Załóżmy, że X, Y są zbiorami mocy continuum. Wobec Twierdzenia 13.13 (korzystając z równoliczności $|\mathbb{N}| = |2\mathbb{N}| = |2\mathbb{N} - 1|$), mamy $|X| = |\mathcal{P}(2\mathbb{N})| = |\{0,1\}^{2\mathbb{N}}|$ oraz $|Y| = |\mathcal{P}(2\mathbb{N} - 1)| = |\{0,1\}^{2\mathbb{N}-1}|$. Wobec Stwierdzenia 10.10 mamy więc:

$$|X \times Y| = |\{0,1\}^{2\mathbb{N}} \times \{0,1\}^{2\mathbb{N}-1}| = |\{0,1\}^{2\mathbb{N} \cup 2\mathbb{N}-1}| = |\{0,1\}^{\mathbb{N}}| = |\mathbb{R}| = \mathfrak{c}.$$

□

WNIOSEK 13.16. *Dla każdej liczby $n \in \mathbb{N}$ przestrzeń euklidesowa $\mathbb{R}^n$ jest zbiorem mocy continuum.*

Naturalne wydaje się pytanie, czy produkt większej liczby zbiorów mocy continuum nadal jest zbiorem mocy continuum.

TWIERDZENIE 13.17 (przeliczalny produkt zbiorów mocy continuum). *Jeśli X jest zbiorem takim, że $|X| = |\mathbb{N}|$, to dla każdego zbioru Y mocy continuum mamy, że zbiór Y^X wszystkich funkcji z X do Y jest mocy continuum.*

DOWÓD. Wobec Twierdzenia 13.13 mamy, że $|Y| = |\{0,1\}^{\mathbb{N}}|$, czyli wobec Stwierdzenia 10.10:

$$|Y^X| = |(\{0,1\}^{\mathbb{N}})^{\mathbb{N}}| = |\{0,1\}^{\mathbb{N}\times\mathbb{N}}| = |\{0,1\}^{\mathbb{N}}| = |\mathbb{R}| = \mathfrak{c}.$$

□

Pojawia się pytanie: *czy nieprzeliczalność X jest równoważna $|X| \leq |\mathbb{R}|$?* Oczywiście **nie**.

UWAGA 13.18. Wobec Twierdzenia Cantora (patrz: Twierdzenie 12.1) zbiór $\mathcal{P}(\mathbb{R})$ jest nieprzeliczalny oraz $|\mathbb{R}| < |\mathcal{P}(\mathbb{R})|$. Stosując Twierdzenie Cantora wielokrotnie, otrzymujemy:

$$|\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{R})))| < ...$$

Stąd otrzymujemy następujący wniosek:

WNIOSEK 13.19. *Zbiory nieprzeliczalne tworzą nieograniczony ciąg względem ich liczności.*

3. Hipoteza continuum

Rozróżniliśmy dwie ważne grupy zbiorów (ze względu na ich liczność): te które są przeliczalne (tj. takie zbiory X, że $|X| \leq |\mathbb{N}|$) oraz te które są mocy continuum (tj. takie zbiory X, że $|X| = |\mathbb{R}|$). Przeprowadźmy teraz krótkie podsumowanie tego kawałka materiału, ograniczając się tylko i wyłącznie do podzbiorów zbioru $\mathbb{R}$. Uważny czytelnik bez trudu zauważył, że dla dowolnie wymyślonego zbioru $A \subseteq \mathbb{R}$ mogliśmy pokazać, że albo $|A| \leq |\mathbb{N}|$, albo $|A| = |\mathbb{R}|$. Nasuwa się więc następującą hipoteza:

HIPOTEZA. *Dowolny zbiór $A \subseteq \mathbb{R}$ jest albo przeliczalny, albo mocy continuum. Innymi słowy, każdy nieprzeliczalny podzbiór $\mathbb{R}$ jest mocy continuum.*

Okazuje się – zaskakująco! – że hipoteza ta jest nierozstrzygalna w aksjomatyce ZFC, tzn. nie można ani udowodnić jej prawdziwości, ani fałszywości. Takie zdania mogą istnieć i wynika to z głębokich twierdzeń Gödla o niezupełności. Powyższa hipoteza nosi nazwę hipotezy continuum i oznaczana jest symbolem (CH). Wobec niezależności zdania (CH) od aksjomatów ZFC każde ze zdań (CH) albo $\neg(CH)$ można traktować jako dodatkowy aksjomat i tworzyć teorie na podstawie $ZFC + (CH)$ albo $ZFC + \neg(CH)$.

Warto zapamiętać, że tego typu zdania istnieją i konsekwencjami dodawania ich (albo ich zaprzeczeń) do zestawu aksjomatów zajmują się matematycy specjalizujący się w teorii mnogości.

UWAGA 13.20 (bardzo ważne wiadomości z trzynastego wykładu). Podczas trzynastego wykładu dowiedzieliśmy się m.in.:

- co to są zbiory przeliczalne i poznaliśmy przykłady takich zbiorów
- co to są zbiory nieprzeliczalne i poznaliśmy przykłady takich zbiorów
- co to są zbiory mocy continuum i poznaliśmy przykłady takich zbiorów
- co to jest hipoteza continuum.

ROZDZIAŁ 14

Ciało i σ-ciało

1. Ciało i σ-ciało

DEFINICJA 14.1 (ciało zbiorów). *Rodzinę zbiorów $\mathcal{S} \subseteq \mathcal{P}(X)$ nazywamy ciałem podzbiorów zbioru X, jeśli:*

1. $\emptyset \in \mathcal{S}$
2. *Jeśli* $A \in \mathcal{S}$ *to* $X \setminus A \in \mathcal{S}$
3. *Jeśli* $A, B \in \mathcal{S}$ *to* $A \cup B \in S$.

PRZYKŁAD 14.2. Niech $X = \{1, 2, 3\}$, rozważmy $\mathcal{S} = \{\emptyset, \{1\}, \{2, 3\}, \{1, 2, 3\}\}$. Wówczas $\mathcal{F}$ jest ciałem podzbiorów zbioru X.

Następujące twierdzenie pokazuje, że ciało zbiorów jest nie tylko zamknięte na branie dopełnienia i sumy dwu elementów, ale też na inne skończone operacje mnogościowe.

TWIERDZENIE 14.3 (własności ciała). *Niech $\mathcal{S} \subseteq \mathcal{P}(X)$ będzie ciałem. Wówczas:*

1. $X \in \mathcal{S}$
2. *Jeśli* $A, B \in \mathcal{S}$ *to* $A \cap B \in \mathcal{S}$
3. *Niech* $n \in \mathbb{N}$ *oraz* $A_1, A_2, ..., A_n \in S$ *wówczas* $A_1 \cap A_2 \cap ... \cap A_n \in \mathcal{S}$
4. *Niech* $n \in \mathbb{N}$ *oraz* $A_1, A_2, ..., A_n \in S$ *wówczas* $A_1 \cup A_2 \cup ... \cup A_n \in \mathcal{S}$
5. *Niech* $A, B \in \mathcal{S}$ *wówczas* $A \setminus B \in \mathcal{S}$.

Dowód powyższego twierdzenia pozostawiamy jako zadanie.

Patrząc na Twierdzenie 14.3(4.), można zastanawiać się, czy z definicji ciała wynika też jego zamkniętość na nieskończone sumy (skoro wynika zamkniętość na dowolnie długie skończone sumy). Okazuje się, że **nie**. Ilustruje to następujący przykład:

PRZYKŁAD 14.4. Niech $X = \mathbb{N}$ i rozważmy $\mathcal{S} = \{A \subseteq \mathbb{N}\colon A$ jest skończony lub $\mathbb{N} \setminus A$ jest skończony$\}$. Łatwo sprawdzić, że $\mathcal{S}$ jest ciałem podzbiorów zbioru $\mathbb{N}$. Zarazem $A_n = \{2n\} \in \mathcal{S}$ dla każdego $n \in \mathbb{N}$. Przy tym $A = \bigcup_{n \in \mathbb{N}} A_n = \{2n\colon n \in \mathbb{N}\}$ jest zbiorem liczb parzystych oraz $A \notin \mathcal{S}$, bo ani A, ani $\mathbb{N} \setminus A$ nie jest skończony.

Wprowadźmy więc następującą definicję:

DEFINICJA 14.5 (σ-ciało zbiorów). *Rodzinę zbiorów $\mathcal{S} \subseteq \mathcal{P}(X)$ nazywamy σ-ciałem podzbiorów zbioru X, jeśli:*

1. $\emptyset \in \mathcal{S}$
2. *Jeśli* $A \in \mathcal{S}$, *to* $X \setminus A \in \mathcal{S}$
3. *Jeśli* $A_1, A_2, ... \in \mathcal{S}$, *to* $\bigcup\limits_{n\in\mathbb{N}} A_n \in S$.

Następujące twierdzenie pokazuje, że σ-ciało zbiorów jest nie tylko zamknięte na branie dopełnienia i sumy ciągu elementów, ale też na inne operacje mnogościowe:

TWIERDZENIE 14.6 (własność σ-ciała). *Niech $\mathcal{S} \subseteq \mathcal{P}(X)$ będzie σ-ciałem oraz $A_1, A_2, ... \in \mathcal{S}$. Wówczas $\bigcap\limits_{n\in\mathbb{N}} A_n \in S$.*

Własności σ-ciała, analogiczne do własności ciała, są prawdziwe na mocy następującej obserwacji:

OBSERWACJA 14.7. Każde σ-ciało podzbiorów zbioru X jest ciałem podzbiorów zbioru X.

PRZYKŁAD 14.8. $\{\emptyset, X\}$ oraz $\mathcal{P}(X)$ są σ-ciałami.

2. σ-ciało generowane przez rodzinę zbiorów

W tej sekcji skupimy się na ważnym zagadnieniu generowania σ-ciała. Naszym celem, dla ustalonej rodziny $\mathcal{F} \subseteq \mathcal{P}(X)$, będzie formalna konstrukcja najmniejszego w sensie inkluzji σ-ciała $\mathcal{S} \subseteq \mathcal{P}(X)$ takiego, że $\mathcal{F} \subseteq \mathcal{S}$. Konstrukcję taką można przeprowadzić *od środka* – startując z rodziny $\mathcal{F}$ dokładać do niej: dopełnienia, sumy wszystkich możliwych ciągów, dopełnienia, sumy wszystkich możliwych ciągów itd. Naturalne pytanie jest: czy ta droga prowadzi do czegoś sensownego?. Odpowiedź na to pytanie wymaga dużego aparatu matematycznego, sama zaś konstrukcja *od środka*, choć możliwa, ma dość skomplikowany formalny.

Opiszemy więc inną metodę – *z zewnątrz*. Mianowicie spojrzymy na wszystkie σ-ciała $\mathcal{S}$, które mają docelową własność, i z nich skonstruujemy to najmniejsze.

Rozważmy rodzinę $\mathcal{Z}$ wszystkich σ-ciał $\mathcal{S}$ zawierających rodzinę $\mathcal{F}$.

UWAGA 14.9. Formalnie $\mathcal{Z}$ jest rodziną σ-ciał podzbiorów zbioru X, zatem jest rodziną rodzin podzbiorów zbioru X. Skoro σ-ciało $\mathcal{S}$ jest rodziną podzbiorów zbioru X, to $\mathcal{S} \subseteq \mathcal{P}(X)$. W konsekwencji $\mathcal{S} \in \mathcal{P}(\mathcal{P}(X))$. Idąc dalej – $\mathcal{Z}$ jest rodziną σ-ciał, więc $\mathcal{Z} \subseteq \mathcal{P}(\mathcal{P}(X))$, czyli $\mathcal{Z} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(X)))$. Stąd

$$\mathcal{Z} = \{\mathcal{S} \in \mathcal{P}(\mathcal{P}(X)) \colon \mathcal{S} \text{ jest } \sigma\text{-ciałem} \wedge \mathcal{F} \subseteq \mathcal{S}\}.$$

Zatem na mocy aksjomatu wycinania $\mathcal{Z}$ jest zbiorem.

TWIERDZENIE 14.10 (istnienie najmniejszego σ-ciała). *Niech $\mathcal{F} \subseteq \mathcal{P}(X)$ będzie ustaloną rodziną podzbiorów zbioru X. Niech $\mathcal{Z}$ będzie rodziną wszystkich σ-ciał podzbiorów zbioru X zawierających $\mathcal{F}$. Wówczas $\mathcal{Z} \neq \emptyset$ oraz $\bigcap \mathcal{Z} = \{A \in \mathcal{P}(X) \colon (\forall \mathcal{S} \in \mathcal{Z})\ A \in \mathcal{S}\}$ jest σ-ciałem.*

UWAGA 14.11. Do zbioru $\bigcap \mathcal{Z}$ należą te podzbiory zbioru X, które są elementem każdego σ-ciała zawierającego $\mathcal{F}$.

DOWÓD. Zauważmy, że skoro $\mathcal{P}(X)$ jest σ-ciałem oraz $\mathcal{F} \subseteq \mathcal{P}(X)$, to $\mathcal{P}(X) \in \mathcal{Z}$, czyli $\mathcal{Z} \neq \emptyset$. Pokażemy, że $\bigcap \mathcal{Z}$ jest σ-ciałem:
Ad 1. Niech $\mathcal{S} \in \mathcal{Z}$. Skoro $\mathcal{S}$ jest σ-ciałem, to $\emptyset \in \mathcal{S}$. Stąd, z dowolności $\mathcal{S} \in \mathcal{Z}$, mamy $\emptyset \in \bigcap \mathcal{Z}$.
Ad 2. Niech $\mathcal{S} \in \mathcal{Z}$ i niech $A \in \bigcap \mathcal{Z}$, wówczas $A \in \mathcal{S}$. W szczególności, skoro $\mathcal{S} \in \mathcal{Z}$ jest σ-ciałem, to z definicji $X \setminus A \in \mathcal{S}$. Stąd, z dowolności $\mathcal{S} \in \mathcal{Z}$, mamy $X \setminus A \in \bigcap \mathcal{Z}$.
Ad 3. Niech $\mathcal{S} \in \mathcal{Z}$ i niech $A_1, A_2, ... \in \bigcap \mathcal{Z}$, wówczas $A_1, A_2, ... \in \mathcal{S}$. W szczególności, skoro $\mathcal{S} \in \mathcal{Z}$ jest σ-ciałem, to z definicji $\bigcup\limits_{n\in\mathbb{N}} A_n \in \mathcal{S}$. Stąd, z dowolności $\mathcal{S} \in \mathcal{Z}$, mamy $\bigcup\limits_{n\in\mathbb{N}} A_n \in \bigcap \mathcal{Z}$.
Wobec powyższego $\bigcap \mathcal{Z}$ jest σ-ciałem podzbiorów zbioru X. □

WNIOSEK 14.12. *Niech $\mathcal{F} \subseteq \mathcal{P}(X)$ będzie ustaloną rodziną podzbiorów zbioru X. Istnieje dokładnie jedno σ-ciało $\sigma(\mathcal{F})$ takie, że $\mathcal{F} \subseteq \sigma(\mathcal{F})$ oraz dla każdego σ-ciała $\mathcal{S}_0$ podzbiorów zbioru X zawierającego $\mathcal{F}$ mamy $\sigma(\mathcal{F}) \subseteq \mathcal{S}_0$, tj. $\sigma(\mathcal{F})$ jest najmniejszym w sensie inkluzji σ-ciałem zawierającym $\mathcal{F}$.*

DOWÓD. Niech $\mathcal{Z}$ będzie rodziną wszystkich σ-ciał podzbiorów zbioru X zawierających $\mathcal{F}$. Wobec Twierdzenia 14.10 zbiór $\bigcap \mathcal{Z}$ jest σ-ciałem. Niech $\sigma(\mathcal{F}) = \bigcap \mathcal{Z}$. Z definicji rodziny $\mathcal{Z}$ mamy, że $\mathcal{F} \subseteq \mathcal{S}$ dla każdego $\mathcal{S} \in \mathcal{Z}$, więc też $\mathcal{F} \subseteq \sigma(\mathcal{F})$. Ponadto niech $\mathcal{S}_0$ będzie σ-ciałem podzbiorów zbioru X zawierającym rodzinę $\mathcal{F}$. Wówczas $\mathcal{S}_0 \in \mathcal{Z}$, więc w szczególności $\sigma(\mathcal{F}) \subseteq \mathcal{S}_0$. Jedyność $\sigma(\mathcal{F})$ wynika z jedyności elementu najmniejszego w częściowym porządku $(\mathcal{Z}, \subseteq)$. □

DEFINICJA 14.13 (σ-ciało generowane). *Dla ustalonej rodziny $\mathcal{F} \subseteq \mathcal{P}(X)$ podzbiorów zbioru X, σ-ciało $\sigma(\mathcal{F})$ nazywamy σ-ciałem generowanym przez rodzinę $\mathcal{F}$.*

PRZYKŁAD 14.14. σ-ciało zbiorów borelowskich w $\mathbb{R}$ definiujemy jako najmniejsze σ-ciało podzbiorów zbioru $\mathbb{R}$ zawierające wszystkie przedziały otwarte. Wobec powyższej notacji $\mathcal{B}_\mathbb{R} = \sigma(\mathcal{G})$, gdzie $\mathcal{G} = \{(a, b) \subseteq \mathbb{R} \colon a < b,\ a, b \in \mathbb{R}\}$ jest rodziną wszystkich przedziałów otwartych w $\mathbb{R}$.

STWIERDZENIE 14.15 (własności σ-ciała generowanego). *Zachodzą następujące własności:*

1. *Jeśli $\mathcal{F} \subseteq \mathcal{P}(X)$ jest σ-ciałem, to $\sigma(\mathcal{F}) = \mathcal{F}$. W szczególności $\sigma(\sigma(\mathcal{F})) = \sigma(\mathcal{F})$.*
2. *Jeśli $\mathcal{F} \subseteq \mathcal{G}$, to $\sigma(\mathcal{F}) \subseteq \sigma(\mathcal{G})$.*
3. *Jeśli $\mathcal{F} \subseteq \sigma(\mathcal{G})$, to $\sigma(\mathcal{F}) \subseteq \sigma(\mathcal{G})$.*

Dowód. Ad 1. Załóżmy, że $\mathcal{F}$ jest σ-ciałem podzbiorów zbioru X. Wiemy, że $\sigma(\mathcal{F}) = \bigcap \mathcal{Z}$, gdzie $\mathcal{Z}$ jest rodziną wszystkich σ-ciał zawierających $\mathcal{F}$. W szczególności $\mathcal{F}$ jest też σ-ciałem i oczywiście $\mathcal{F} \subseteq \mathcal{F}$. Stąd $\mathcal{F} \in \mathcal{Z}$, więc $\sigma(\mathcal{F}) \subseteq \mathcal{F}$. Zarazem wiemy już, że $\mathcal{F} \subseteq \sigma(\mathcal{F})$ zatem $\sigma(\mathcal{F}) = \mathcal{F}$. Druga część tezy wynika z faktu, że $\sigma(\mathcal{F})$ jest w szczególności σ-ciałem.

Ad 2. Załóżmy, że $\mathcal{F} \subseteq \mathcal{G}$. Rozważmy rodziny $\mathcal{Z}_\mathcal{F}, \mathcal{Z}_\mathcal{G}$ wszystkich σ-ciał zawierających odpowiednio $\mathcal{F}$ oraz $\mathcal{G}$. Zauważmy, że jeśli $\mathcal{S} \in \mathcal{Z}_\mathcal{G}$, to $\mathcal{S} \in \mathcal{Z}_\mathcal{F}$, zatem $\mathcal{Z}_\mathcal{G} \subseteq \mathcal{Z}_\mathcal{F}$. Stąd $\bigcap \mathcal{Z}_\mathcal{F} \subseteq \bigcap \mathcal{Z}_\mathcal{G}$.

Ad 3. Załóżmy, że $\mathcal{F} \subseteq \sigma(\mathcal{G})$. Wówczas wobec udowodnionej 2. mamy $\sigma(\mathcal{F}) \subseteq \sigma(\sigma(\mathcal{G}))$, co wobec udowodnionej 1. oznacza $\sigma(\mathcal{F}) \subseteq \sigma(\mathcal{G})$. □

Wykorzystamy Stwierdzenie 14.15 w następującej obserwacji:

Obserwacja 14.16. σ-ciało $\mathcal{B}_\mathbb{R}$ jest generowane przez przedziały domknięte, tj. $\mathcal{B}_\mathbb{R} = \sigma(\mathcal{F})$, gdzie $\mathcal{F} = \{[a,b] \subseteq \mathbb{R} \colon a < b,\ a, b \in \mathbb{R}\}$.

Dowód. Niech $\mathcal{G} = \{(a,b) \subseteq \mathbb{R} \colon a < b,\ a, b \in \mathbb{R}\}$. Wiemy, że $\mathcal{B}_\mathbb{R} = \sigma(\mathcal{G})$. Zauważmy, że dla $a, b \in \mathbb{R}$ takich, że $a < b$ mamy:

1. $[a,b] = \bigcap\limits_{n\in\mathbb{N}} (a - \frac{1}{n}, b + \frac{1}{n})$, zatem $[a,b] \in \sigma(\mathcal{G})$
2. $(a,b) = \bigcup\limits_{n\in\mathbb{N}} [a + \frac{1}{n+N}, b - \frac{1}{n+N}]$, gdzie $N \in \mathbb{N}$ jest tak dobrane, by $a < a + \frac{1}{n+N} < b - \frac{1}{n+N} < b$. Zatem $(a,b) \in \sigma(\mathcal{F})$.

Wobec 1. mamy, że $\mathcal{F} \subseteq \sigma(\mathcal{G})$, zatem wobec Stwierdzenia 14.15 $\sigma(\mathcal{F}) \subseteq \sigma(\mathcal{G})$. Podobnie wobec 2. mamy, że $\mathcal{G} \subseteq \sigma(\mathcal{F})$, zatem wobec Stwierdzenia 14.15 $\sigma(\mathcal{G}) \subseteq \sigma(\mathcal{F})$. Ostatecznie $\sigma(\mathcal{F}) = \sigma(\mathcal{G}) = \mathcal{B}_\mathbb{R}$. □

Uwaga 14.17 (bardzo ważne wiadomości z piętnastego wykładu). Podczas piętnastego wykładu dowiedzieliśmy się m.in.:

- co to jest ciało i σ-ciało podzbiorów zbioru X
- co to jest σ-ciało generowane przez rodzinę zbiorów
- co to jest σ-ciało zbiorów borelowskich.

ROZDZIAŁ 15

Aksjomat wyboru i Lemat Kuratowskiego-Zorna

1. Wokół Aksjomatu wyboru

Wykład zaczniemy od przypomnienia niedokończonej konstrukcji z Wykładu 12. - dowodu Twierdzenia o dychotomii (patrz Twierdzenie 12.10):

TWIERDZENIE (twierdzenie o dychotomii). *Dla dowolnych zbiorów X i Y zachodzi alternatywa*

$$|X| \leq |Y| \text{ lub } |Y| \leq |X|.$$

SZKIC DOWODU TWIERDZENIA O DYCHOTOMII. Celem dowodu jest konstrukcja maksymalnego podzbioru $f \subseteq X \times Y$, który jest funkcją różnowartościową.

Ustalmy $x_1 \in X$ oraz $y_1 \in Y$ i zdefiniujmy zbiór $f_1 = \{(x_1, y_1)\}$. Jeśli $\mathrm{dom}(f_1) = X$ lub $\mathrm{rng}(f_1) = Y$, to konstrukcja się kończy. Jeśli tak nie jest, to ustalmy $x_2 \in X \setminus \mathrm{dom}(f_1)$ oraz $y_2 \in Y \setminus \mathrm{rng}(f_1)$ i rozszerzmy funkcję f_1 do zbioru $f_2 = \{(x_1, y_1), (x_2, y_2)\}$. Znów, jeśli $\mathrm{dom}(f_2) = X$ lub $\mathrm{rng}(f_2) = Y$, to konstrukcja się kończy. Jeśli nie, to postępujemy tak dalej. W tym miejscu widać, że jeśli któryś ze zbiorów X, Y jest skończony, to po skończenie wielu krokach konstrukcja się zakończy. Jeśli któryś ze zbiorów X, Y jest równoliczny z $\mathbb{N}$, to zasada indukcji matematycznej pozwoli zakończyć konstrukcję. Co jednak, jeśli oba zbiory X, Y są nieprzeliczalne? □

Zauważmy, że przyjmując w naszej szkicowej konstrukcji następujące oznaczenie:

$$\mathcal{R} = \{f \subseteq X \times Y \colon f \text{ jest funkcją różnowartościową}\},$$

stworzyliśmy obiekty f_1, $f_2 \in \mathcal{R}$ takie, że $f_1 \subseteq f_2$, zaś celem głównym dowodu jest wykazanie istnienia w zbiorze $\mathcal{R}$ elementu maksymalnego względem relacji inkluzji (maksymalnego podzbioru produktu $X \times Y$ będącego funkcją różnowartościową). Ten element maksymalny okaże się szukaną w dowodzie funkcją. Nim jednak dokończymy dowód twierdzenia o dychotomii, sformułujemy pewien dodatkowy (bardzo silny) aksjomat, który pozwala tego typu konstrukcje (dłuższe niż zasada indukcji matematycznej) prowadzić, i krótko przedstawimy jego znaczenie.

AKSJOMAT 8 (aksjomat wyboru, AC). *Jeśli $\mathcal{P}$ jest rodziną zbiorów niepustych, to istnieje taka funkcja $f \colon \mathcal{P} \to \bigcup \mathcal{P}$, że $f(P) \in P$ dla każdego $P \in \mathcal{P}$.*

Uwaga 15.1. Funkcję f, której istnienie postuluje AC, nazywamy funkcją wyboru rodziny $\mathcal{P}$.

Potraktowanie aksjomatu wyboru w wyjątkowy sposób jest uzasadnione tym, że postulat ten ma odmienny charakter niż inne aksjomaty ZFC. Stwierdza się w nim bowiem istnienie pewnego zbioru, ale nie daje wskazówek, jak go skonstruować. W innych natomiast postulatach takie wskazówki są, np. aksjomat sumy określa, w jaki sposób zbudować sumę zbiorów: aby otrzymać sumę, należy wziąć wszystkie elementy, które należą do przynajmniej jednego spośród zbiorów rozważanej sumy. W związku z tą różnicą dowody, w których używa się aksjomatu wyboru, nazywamy *nieefektywnymi*. Interesujące wydaje się, że aksjomat wyboru jest równoważny następującemu zdaniu: *produkt kartezjański niepustych zbiorów jest zbiorem niepustym*. Twierdzenie to jest prawdziwe (nie wymaga aksjomatu wyboru) w przypadku produktu skończenie wielu zbiorów, jednak przypadek nieskończonego produktu wymaga już wskazania odpowiedniej funkcji wyboru – wymaga użycia AC. Jak widzimy, nieraz intuicyjne fakty istotnie korzystają z mocy AC.

Niekiedy aksjomat wyboru formułuje się dla rodziny $\mathcal{P}$ zbiorów parami rozłącznych. Także taka wersja jest równoważna tej sformułowanej przez nas. Okazuje się – takich twierdzeń (tzw. równoważników aksjomatu wyboru) jest w matematyce dużo więcej i można by im poświęcić semestralny kurs.

W dalszej części przyjrzymy się dwóm równoważnikom AC, choć wspomnimy jedynie, że są to konsekwencje aksjomatu wyboru (dowód drugiej implikacji można znaleźć w literaturze uzupełniającej).

2. Lemat Kuratowskiego-Zorna

Pierwszą konsekwencją aksjomatu wyboru jest Lemat Kuratowskiego-Zorna. Twierdzenie to okaże się być brakującą cegiełką w naszym dowodzie twierdzenia o dychotomii.

Wprowadźmy następującą definicję:

Definicja 15.2 (łańcuch). *Niech $(X, \leq)$ będzie zbiorem częściowo uporządkowanym oraz $A \subseteq X$. Powiemy, że A jest łańcuchem, jeśli wszystkie elementy zbioru A są ze sobą porównywalne w sensie relacji $\leq$.*

Uwaga 15.3. Oczywiście jeśli częściowy porządek $\leq$ jest liniowy, to dowolny podzbiór zbioru X jest łańcuchem. Ponadto zawsze zbiór pusty jest łańcuchem.

Przykład 15.4. Rozważmy zbiór $\mathcal{P}(\mathbb{N})$ i częściowy porządek będący relacją inkluzji $\subseteq$. Wówczas zbiór $\{\langle 1, n\rangle \subseteq \mathbb{N} \colon n \in \mathbb{N}\}$ jest łańcuchem, bo dla $n, m \in \mathbb{N}$, jeśli $n \leq m$, to $\langle 1, n\rangle \subseteq \langle 1, m\rangle$.

Zarazem zbiór $\{\{1, 2, 3\}, \{2, 3, 4\}\}$ nie jest łańcuchem, bo $\{1, 2, 3\} \not\subseteq \{2, 3, 4\}$ oraz $\{2, 3, 4\} \not\subseteq \{1, 2, 3\}$.

W dalszej części skupimy się tylko na pewnym szczególnym częściowym porządku - mianowicie na inkluzji. W poniższej teorii istnieje przestrzeń na uogólnienia w kierunku dowolnego częściowego porządku, jednak pełna ogólność w tym momencie nie jest nam potrzebna.

TWIERDZENIE 15.5 (Lemat Kuratowskiego-Zorna). *Niech $X \neq \emptyset$ oraz $\mathcal{R} \subseteq \mathcal{P}(X)$ będzie niepustą rodziną taką, że suma dowolnego niepustego łańcucha w $(\mathcal{R}, \subseteq)$ jest w $\mathcal{R}$. Wówczas istnieje w $\mathcal{R}$ element maksymalny.*

UWAGA 15.6. Warunek narzucony na rodzinę $\mathcal{R}$ oznacza, że dla każdego $\mathcal{A} \subseteq \mathcal{R}$ będącego łańcuchem względem relacji $\subseteq$, mamy $\bigcup \mathcal{A} \in \mathcal{R}$.

DOWÓD LEMATU KURATOWSKIEGO-ZORNA. (w dowodzie mówiąc *łańcuch*, mamy na myśli łańcuch względem relacji $\subseteq$).

FAKT 15.7 (Ćwiczenie). *Niech $\mathcal{R} \subset \mathcal{P}(X)$. Zdefiniujmy rodzinę*

$$\bar{\mathcal{R}} = \{A \subseteq X : (\exists B \in \mathcal{R}) \ \ A \subseteq B\}.$$

Jeśli $\bar{\mathcal{R}}$ spełnia założenia Lematu Kuratowskiego-Zorna, to rodzina $\mathcal{R}$ również. Ponadto jeśli $Y \subseteq X$ jest elementem maksymalnym w $\bar{\mathcal{R}}$, to jest też elementem maksymalnym w $\mathcal{R}$.

Niech $X \neq \emptyset$ oraz $\mathcal{R} \subseteq \mathcal{P}(X)$ będzie niepustą rodziną taką, że dla dowolnego łańcucha $\mathcal{A} \subseteq \mathcal{R}$, mamy $\bigcup \mathcal{A} \in \mathcal{R}$. Bez zmniejszenia ogólności, możemy założyć, że $\mathcal{R}$ jest zamknięta na branie podzbiorów. W szczególności wtedy $\emptyset \in \mathcal{R}$.

Niech f będzie funkcją wyboru dla rodziny $\mathcal{P}(X) \setminus \{\emptyset\}$. Dla $A \in \mathcal{R}$ oznaczmy:

$$\hat{A} = \{x \in X \colon A \cup \{x\} \in \mathcal{R}\},$$

tj. zbiór tych elementów zbioru X, o które można rozszerzyć zbiór A, pozostając w rodzinie $\mathcal{R}$. Zauważmy, że w szczególności, dla $A \in \mathcal{R}$ oraz $x \in A$ mamy, że $A \cup \{x\} = A \in \mathcal{R}$, zatem $A \subseteq \hat{A}$.

Zauważmy, że $M \in \mathcal{R}$ będzie elementem maksymalnym w $\mathcal{R}$ wtedy i tylko wtedy, gdy $\hat{M} = M$, czyli gdy $\hat{M} \setminus M = \emptyset$. Rozważmy funkcję $g \colon \mathcal{R} \to \mathcal{R}$ określoną dla $A \in \mathcal{R}$ wzorem:

$$g(A) = \begin{cases} A \cup \{f(\hat{A} \setminus A)\}, \text{ gdy } \hat{A} \setminus A \neq \emptyset \\ A, \text{ gdy } A = \hat{A}. \end{cases}$$

Wystarczy więc pokazać, że g ma punkt stały w zbiorze $\mathcal{R}$, tzn. istnieje zbiór $A \in \mathcal{R}$ taki, że $g(A) = A$.

Zauważmy, że z definicji funkcji g mamy, że $A \subseteq g(A)$ dla każdego $A \in \mathcal{R}$. Dodatkowo $g(A)$ różni się od A o maksymalnie jeden element $f(\hat{A} \setminus A)$. Dla wygody redakcji wprowadźmy następujące oznaczenie – rodzinę $\mathcal{T} \subseteq \mathcal{R}$ nazywamy wieżą, jeśli:

1. $\emptyset \in \mathcal{T}$
2. $A \in \mathcal{T} \Rightarrow g(A) \in \mathcal{T}$
3. Jeśli $\mathcal{A} \subseteq \mathcal{T}$ jest łańcuchem, to $\bigcup \mathcal{A} \in \mathcal{T}$.

Oczywiście $\mathcal{T} = \mathcal{R}$ jest wieżą, wobec założenia.

Fakt 15.8 (ćwiczenie). *Niech $\mathcal{Z} = \{\mathcal{T} \subseteq \mathcal{R} : \mathcal{T}$ jest wieżą$\}$. Niech*

$$\mathcal{T}_0 = \{A \subset X : (\forall \mathcal{T} \in \mathcal{Z}) \;\; A \in \mathcal{T}\}$$

będzie rodziną tych podzbiorów X, które należą do wszystkich wież. Wówczas $\mathcal{T}_0$ jest wieżą oraz $\mathcal{T}_0 \subseteq \mathcal{T}$ dla dowolnej wieży $\mathcal{T}$.

Można zdefiniować najmniejszą wieżę $\mathcal{T}_0$ jako przecięcie wszystkich wież w $\mathcal{R}$. Pokażemy, że $\mathcal{T}_0$ jest łańcuchem. Nazwijmy element $C \in \mathcal{T}_0$ **porównywalnym**, jeśli dla każdego $A \in \mathcal{T}_0$ mamy $C \subseteq A$ lub $A \subseteq C$. Wystarczy więc pokazać, że każdy element $\mathcal{T}_0$ jest porównywalny (zauważmy, że oczywiście $\emptyset \in \mathcal{T}_0$ jest porównywalny).

Niech $C \in \mathcal{T}_0$ będzie porównywalny i niech $A \in \mathcal{T}_0$ będzie taki, że $A \subsetneq C$. Ponieważ C jest porównywalny oraz $g(A) \in \mathcal{T}_0$, to $C \subsetneq g(A)$ albo $g(A) \subseteq C$. W pierwszym przypadku A byłby właściwym podzbiorem właściwego podzbioru $g(A)$, co jest niemożliwe, bo A i $g(A)$ różnią się maksymalnie o jeden element. Stąd, o ile istnieje $A \in \mathcal{T}_0$ taki, że $A \subsetneq C$, to $g(A) \subseteq C$.

Niech teraz:

$$\mathcal{U} = \{A \in \mathcal{T}_0 \colon A \subseteq C \vee g(C) \subseteq A\},$$

$$\mathcal{U}' = \{A \in \mathcal{T}_0 \colon A \subseteq g(C) \vee g(C) \subseteq A\},$$

tj. $\mathcal{U}'$ jest zbiorem elementów porównywalnych z $g(C)$. Ponadto, skoro $C \subseteq g(C)$, to $\mathcal{U} \subseteq \mathcal{U}'$. Pokażemy, że $\mathcal{U}$ jest wieżą.

Ad 1. Oczywiście $\emptyset \in \mathcal{U}$, bo $\emptyset \subseteq C$.

Ad 2. Niech $A \in \mathcal{U}$. Mamy możliwości:

- $A \subsetneq C$, wtedy wobec wcześniejszego, $g(A) \subseteq C$, więc $g(A) \in \mathcal{U}$
- $A = C$, wtedy $g(A) = g(C)$, więc $g(C) \subseteq g(A)$, tj. $g(A) \in \mathcal{U}$
- $g(C) \subseteq A$, wtedy skoro $A \subseteq g(A)$, to $g(C) \subseteq g(A)$, czyli $g(A) \in \mathcal{U}$.

Ad 3. Niech $\mathcal{A} \subseteq \mathcal{U}$ będzie łańcuchem, wówczas mamy możliwości:

- jeśli dla każdego $A \in \mathcal{A}$ mamy, że $A \subseteq C$, to $\bigcup \mathcal{A} \subseteq C$, więc $\bigcup \mathcal{A} \in \mathcal{U}$
- jeśli istnieje $A \in \mathcal{A}$ takie, że $g(C) \subseteq A$, to $g(C) \subseteq \bigcup \mathcal{A}$, więc $\bigcup \mathcal{A} \in \mathcal{U}$.

Wobec powyższego $\mathcal{U}$ jest wieżą taką, że $\mathcal{U} \subseteq \mathcal{T}_0$. Ale jednocześnie $\mathcal{T}_0$ jest najmniejszą wieżą w sensie inkluzji, więc $\mathcal{U} = \mathcal{T}_0$.

Stąd, dla zbioru porównywalnego $C \in \mathcal{T}_0$, i dla $A \in \mathcal{T}_0 = \mathcal{U}$ mamy, że $A \subseteq C$ (i wtedy $A \subseteq g(C)$) lub $g(C) \subseteq A$. Oznacza to, że $g(C)$ jest też porównywalny.

Podsumowując wiemy, że:

- $\emptyset$ jest porównywalny
- odwzorowanie g przekształca zbiory porównywalne na zbiory porównywalne.

Przy tym, jeśli $\mathcal{A}$ jest łańcuchem zbiorów porównywalnych, to $\bigcup \mathcal{A}$ jest też porównywalny. Ostatecznie rodzina $\mathcal{T}_C$ zbiorów porównywalnych jest wieżą, więc $\mathcal{T}_0 \subseteq \mathcal{T}_C$, tj. każdy element $\mathcal{T}_0$ jest porównywalny. Niniejszym $\mathcal{T}_0$ jest łańcuchem, więc $M = \bigcup \mathcal{T}_0 \in \mathcal{T}_0$. Przy tym $g(M) \subseteq M$ oraz $M \subseteq g(M)$. Zatem $M = g(M)$, co kończy dowód. □

3. Konsekwencje Lematu Kuratowskiego-Zorna

Pierwszą konsekwencją Lematu Kuratowskiego-Zorna jest możliwość dokończenia dowodu twierdzenia o dychotomii.

Dowód twierdzenia o dychotomii. Rozważmy rodzinę:

$$\mathcal{R} = \{f \subseteq X \times Y \colon f \text{ jest funkcją różnowartościową}\}.$$

Oczywiście $\mathcal{R} \neq \emptyset$, bo np. $\emptyset \in \mathcal{R}$. Niech $\mathcal{A} \subseteq \mathcal{R}$ będzie łańcuchem, tj. dla dowolnych $f, g \in \mathcal{A}$ mamy $f \subseteq g$ lub $g \subseteq f$. Pokażemy, że $\bigcup \mathcal{A} \in \mathcal{R}$, tj. że $h = \bigcup \mathcal{A}$ jest funkcją różnowartościową. Że $\bigcup \mathcal{A}$ jest funkcją, wynika z tego, że $\mathcal{A}$ jest łańcuchem. Ponadto, jeśli $x, y \in \operatorname{dom}(\bigcup \mathcal{A})$, to istnieją $f, g \in \mathcal{A}$ takie, że $x \in \operatorname{dom}(f)$ oraz $y \in \operatorname{dom}(g)$. W szczególności, skoro $\mathcal{A}$ jest łańcuchem, to $f \subseteq g$ lub $g \subseteq f$. Załóżmy więc, że $f \subseteq g$, wtedy $x, y \in \operatorname{dom}(g)$ oraz z różnowartościowości g mamy $g(x) \neq g(y)$. Przy tym mamy: $h(x) = g(x) \neq g(y) = h(y)$.

Wobec powyższego $\mathcal{R}$ spełnia założenia Lematu Kuratowskiego-Zorna, więc w $\mathcal{R}$ istnieje element maksymalny $h \in \mathcal{R}$. Zauważmy, że gdyby $\operatorname{dom}(h) \subsetneq X$ oraz $\operatorname{rng}(h) \subsetneq Y$, to istniałyby $x \in X \setminus \operatorname{dom}(h)$ oraz $y \in Y \setminus \operatorname{rng}(h)$, oraz $h \cup \{(x, y)\}$ byłaby dalej funkcją różnowartościową rozszerzającą h, co przeczy maksymalności h. Ostatecznie $\operatorname{dom}(h) = X$ lub $\operatorname{rng}(h) = Y$. □

Lemat Kuratowskiego-Zorna niesie za sobą wiele konsekwencji w różnych działach matematyki. Wymienimy tylko kilka z nich (z częścią z pewnością się Państwo zetkną lub zetknęli).

Konsekwencje Lematu Kuratowskiego-Zorna:

1. Twierdzenie Hahna-Banacha w analizie funkcjonalnej (rozszerzanie funkcjonałów liniowych ciągłych)
2. Twierdzenie, że każda przestrzeń liniowa ma bazę
3. Twierdzenie Tichonowa w topologii (produkt przestrzeni zwartych jest przestrzenią zwartą)
4. Twierdzenie Zermelo (w każdym zbiorze istnieje relacja dobrego porządku).

4. Zbiory dobrze uporządkowane

W poprzedniej sekcji wspomniana została jedna z konsekwencji Lematu Kuratowskiego-Zorna w postaci twierdzenia Zermelo o dobrym uporządkowaniu. Przez chwilę skupimy się na tym ważnym typem relacji.

Definicja 15.9 (relacja dobrego porządku). *Relację częściowego porządku $\leq$ w zbiorze X nazywamy dobrym porządkiem, gdy w każdym niepustym podzbiorze zbioru X istnieje element najmniejszy względem relacji $\leq$. Parę $(X, \leq)$ nazywamy zbiorem dobrze uporządkowanym.*

Zauważmy, że w warunku definicyjnym w każdym niepustym zbiorze $A \subseteq X$ ma istnieć element najmniejszy (czyli w szczególności porównywalny z każdym innym elementem zbioru A). Pamiętamy, że w zbiorach częściowo uporządkowanych niekoniecznie wszystkie elementy musiały być porównywalne. Okazuje się jednak, że zachodzi następujące:

Stwierdzenie 15.10. *Niech $(X, \leq)$ będzie zbiorem dobrze uporządkowanym. Wówczas $\leq$ jest liniowym porządkiem.*

Dowód. Wystarczy pokazać, że każdy dobry porządek $\leq$ w zbiorze X jest spójny. Niech $x, y \in X$ i rozważmy (niepusty) zbiór $A = \{x, y\} \subseteq X$. Wobec założenia, że $\leq$ jest dobrym porządkiem, istnieje w zbiorze A element najmniejszy. Jeśli x jest tym elementem najmniejszym, to $x \leq y$. Zarazem, jeśli y jest tym elementem, to $y \leq x$. Ostatecznie x, y są porównywalne, zatem $\leq$ jest spójna. □

Przykład 15.11. Rozważmy klasyczną relację $\leq$ w zbiorze $\mathbb{N}$. Wówczas oczywiście w dowolnym niepustym podzbiorze zbioru $\mathbb{N}$ istnieje element najmniejszy. Istotnie, niech $A \subseteq \mathbb{N}$ będzie niepusty. Przypuśćmy, że w A nie ma elementu najmniejszego. Wówczas oczywiście $1 \notin A$. Kontynuując taki sposób rozumowania, można stwierdzić, że skoro $1 \notin A$ oraz w A nie ma elementu najmniejszego, to $2 \notin A$. Niech $n_0 \in \mathbb{N}$ i załóżmy, że $1, 2, ..., n_0 \notin A$. Wówczas skoro w A nie ma elementu najmniejszego, to $n_0 + 1 \notin A$. Na mocy zasady indukcji matematycznej pokazaliśmy więc, że $(\forall n \in \mathbb{N})\ n \notin A$ zatem $A = \emptyset$. To jest sprzeczność. Ostatecznie $(\mathbb{N}, \leq)$ jest zbiorem dobrze uporządkowanym.

Widzimy, że w zbiorze $\mathbb{N}$ łatwo wprowadzić relację dobrego porządku. Zauważmy, że poszukiwanie *pomysłu* na dobry porządek w $\mathbb{R}$ jest raczej kłopotliwe. Okazuje się jednak, że zachodzi następujące twierdzenie, będące konsekwencją aksjomatu wyboru:

TWIERDZENIE 15.12 (twierdzenie Zermelo). *Dla każdego zbioru X istnieje relacja, która jest relacją dobrego porządku w zbiorze X.*

5. Istnienie bazy w przestrzeni liniowej

W tej części udowodnimy ostatnie twierdzenie.

TWIERDZENIE 15.13. *Każda przestrzeń liniowa ma bazę.*

Zanim przystąpimy do dowodu, przypomnimy kilka faktów z algebry liniowej. Niech X będzie przestrzenią liniową nad ciałem $\mathbb{R}$. Układ wektorów $x_1, x_2, ..., x_n \in X$ jest liniowo niezależny, gdy dla dowolnych liczb $a_1, a_2, ..., a_n \in \mathbb{R}$: jeśli $a_1x_1 + a_2x_2 + ... + a_nx_n = \theta$, to $a_1 = a_2 = ... = a_n = 0$. Zbiór $L \subset X$ jest liniowo niezależny, jeśli każdy jego skończony podzbiór jest liniowo niezależny. Zbiór $B \subset X$ jest bazą, jeśli jest liniowo niezależny, oraz jest maksymalny, tzn. dla każdego $x \in X \setminus B$ zbiór $B \cup \{x\}$ nie jest liniowo niezależny.

DOWÓD TWIERDZENIA O ISTNIENIU BAZY. Niech $\mathcal{R} = \{L \subset X : L \text{ jest liniowo niezależny}\}$.

Niech $\mathcal{L}$ będzie łańcuchem w $\mathcal{R}$. Niech $S = \bigcup\{L : L \in \mathcal{L}\}$. Pokażemy, że S jest liniowo niezależny. W tym celu weźmy dowolny skończony podzbiór $\{x_1, x_2, ..., x_n\} \subseteq S$. Wówczas istnieją $L_1, L_2, ..., L_n \in \mathcal{L}$ takie, że $x_i \in L_i$. Skoro $\mathcal{L}$ jest łańcuchem, to $L_i \subseteq L_j$ lub $L_j \subseteq L_i$ dla $1 \leq i < j \leq n$. Zatem istnieje k takie, że $L_i \subseteq L_k$ dla $i \leq n$. Stąd $x_1, ..., x_n \in L_k$. Skoro L_k jest liniowo niezależny, to układ $x_1, ..., x_n$ jest także liniowo niezależny. Z dowolności wyboru zbioru skończonego $\{x_1, x_2, ..., x_n\} \subseteq S$, zbiór S jest liniowo niezależny. Zatem $S \in \mathcal{R}$, czyli suma S łańcucha $\mathcal{L}$ jest w $\mathcal{R}$.

Maksymalny element w $\mathcal{R}$, który istnieje na mocy Lematu Zorna, jest bazą przestrzeni X. □

Bibliografia

[1] Aleksander Błaszczyk, Sławomir Turek, *Teoria mnogości*, Wydawnictwo Naukowe PWN, Wydanie 1, Warszawa 2021

[2] Ryszard Engelking, *Topologia ogólna*, Wydawnictwo Naukowe PWN, Wydanie 3, Warszawa 2021

[3] Jan Kraszewski, *Wstęp do matematyki*, Wydawnictwo Naukowe PWN, WNT, Wydanie 2, Warszawa 2020

[4] Helena Rasiowa, *Wstęp do matematyki współczesnej*, Wydawnictwo Naukowe PWN, Wydanie 14, Warszawa 2021

Skorowidz