

Matematyka 2

Elementy logiki i teorii mnogości

Informatyka Stosowana, I rok*

Tomasz Połacik

Spis treści

1	Pierwsze zajęcia	2
2	Drugie zajęcia	3
3	Trzecie zajęcia	6
4	Czwarte zajęcia	9
5	Piąte zajęcia	12
6	Szóste zajęcia	16
7	Siódme zajęcia	18

*Semestr letni 2021

1 Pierwsze zajęcia

Równoliczność

1.1. Przypomnienie. Funkcja różnowartościowa, na, bijekcja, złożenie funkcji, funkcja odwrotna.

1.2 Definicja (Równoliczność). Mówimy, że zbiory A i B są *równoliczne* (lub że *mają tę samą moc*), gdy istnieje bijekcja ze zbioru A na zbiór B . Piszemy wówczas $A \sim B$ lub $|A| = |B|$.

1.3 Twierdzenie ([GZ1], Twierdzenie 5.1). Dla dowolnych zbiorów A i B :

1. $A \sim A$,
2. $A \sim B \rightarrow B \sim A$,
3. $A \sim B \wedge B \sim C \rightarrow A \sim C$.

Dowód. 1. Funkcja identycznościowa jest bijekcją. 2. Funkcja odwrotna do bijekcji jest bijekcją. 3. Złożenie bijekcji jest bijekcją. \dashv

1.4 Przykład ([GZ1, Wykład 5, Przykłady]).

1. $A \sim \emptyset \iff A = \emptyset$.
2. $\mathbb{N} \sim \mathbb{N} \setminus \{0\}$.
3. $\mathbb{N} \sim 2\mathbb{N}$, $\mathbb{N} \sim \mathbb{N} \setminus 2\mathbb{N}$.
4. $\mathbb{N} \sim \mathbb{Z}$.

$$f(n) = \begin{cases} \frac{n}{2}, & \text{dla } n \in 2\mathbb{N}, \\ -\frac{n+1}{2}, & \text{dla } n \in \mathbb{N} \setminus 2\mathbb{N}, \end{cases}$$

5. $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

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

Dowód, że f jest bijekcją, [GZ1, Tw. 7.27, str. 129–130].

6. Dla dowolnych $a, b, c, d \in \mathbb{R}$ takich, że $a < b$ i $c < d$, mamy $[a, b] \sim [c, d]$.

$$f(x) = \frac{(d-c)x + bc - ad}{b-a}.$$

7. $(-1, 1) \sim \mathbb{R}$.

$$f(x) = \frac{x}{1 - |x|}.$$

8. $(0, 1] \sim (0, 1)$.

$$f(x) = \begin{cases} \frac{1}{n+1}, & \text{dla } x = \frac{1}{n}, n \in \mathbb{N} \setminus \{0\}, \\ x, & \text{else.} \end{cases}$$

9. $[-1, 1] \sim (-1, 1)$

$$[-1, 0] \sim (-1, 0] \quad \& \quad (0, 1] \sim (0, 1)$$

Skąd $[-1, 1] \sim (-1, 1)$.

10. $[0, 1] \sim \mathbb{R}$.

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

Ćwiczenia

[GZ2, Wykład 5] Wybór zadań spośród 5.1—5.6.

2 Drugie zajęcia

$|\mathbb{N}|$ vs $|\mathbb{R}|$

2.1 Lemat ([GZ1, Lemat 6.2]). $[0, 1] \not\sim \mathbb{N}$.

Idea dowodu. Niech dana będzie dowolna funkcja $f : \mathbb{N} \rightarrow [0, 1]$. Pokażemy, że f nie może być „na”. *Krok 0.* Dzielimy odcinek $[0, 1]$ na trzy części:

- (a) $[0, \frac{1}{3}]$,
- (b) $[\frac{1}{3}, \frac{2}{3}]$,
- (c) $[\frac{2}{3}, 1]$

i wybieramy przedział

- (a) gdy $f(0) > \frac{1}{3}$,
- (b) gdy $f(0) < \frac{1}{3}$,
- (c) gdy $f(0) = \frac{1}{3}$.

Procedurę tę powtarzamy biorąc w roli przedziału $[0, 1]$ wybrany przez nas przedział. Iterując tę procedurę otrzymujemy zstępującą rodzinę przedziałów domkniętych. Rodzina taka ma przekrój P będący zbiorem niepustym. Można udowodnić, że P jest jednopunktowy. Zauważmy, że dla każdego $n \in \mathbb{N}$, wartość $f(n)$ nie należy do P . A więc P nie jest zawarty w $\text{rng}(f)$, czyli f nie jest na $[0, 1]$. \dashv

2.2 Twierdzenie ([GZ1, Twierdzenie 6.3]). $\mathbb{R} \not\sim \mathbb{N}$.

Dowód. Jeżeli istniałaby funkcja f z \mathbb{N} na \mathbb{R} , to funkcja

$$g(x) = \begin{cases} f(x), & \text{gdy } f(x) \in [0, 1] \\ 0, & \text{else} \end{cases}$$

byłaby funkcją z \mathbb{N} na $[0, 1]$, co przeczy Lematowi 2.1. \dashv

Metoda przekątniowa

2.3 Twierdzenie ([GZ1, Przykład 6.4]). $\mathbb{N}^{\mathbb{N}} \not\sim \mathbb{N}$.

Dowód. Metoda przekątniowa. \dashv

Analogicznie dowodzimy, że

2.4 Twierdzenie ([GZ1, Przykład 6.5]). $\{0, 1\}^{\mathbb{N}} \not\sim \mathbb{N}$.

Dowód. Metoda przekątniowa. \dashv

Twierdzenie Cantora

2.5. Twierdzenie Cantora. [GZ1, Twierdzenie 6.6] $A \not\sim \mathcal{P}(A)$, dla dowolnego zbioru A .

Dowód. Niech f będzie dowolną iniekcją

$$f : A \xrightarrow{1-1} \mathcal{P}(A).$$

Pokażemy, że f nie może być suriekcją. Definiujemy:

$$Z := \{x \in A : x \notin f(x)\} \in \mathcal{P}(A).$$

Wówczas, dla dowolnego $x \in A$ mamy

$$x \in Z \iff x \notin f(x)$$

czyli

$$x \in [Z \setminus f(x)] \cup [f(x) \setminus Z].$$

Zatem, dla każdego $x \in A$,

$$Z \neq f(x).$$

⊥

2.6 Wniosek ([GZ1, Wniosek 6.8]). $A \not\sim \mathcal{P}(\mathcal{P}(A))$.

Dowód. Przypuśćmy, że $A \sim \mathcal{P}(\mathcal{P}(A))$. Rozważmy zbiór $B \subseteq \mathcal{P}(A)$:

$$B = \{\{a\} : a \in A\}.$$

Mamy

$$B \sim A$$

wtedy

$$\mathcal{P}(A) \supseteq B \sim A \sim \mathcal{P}(\mathcal{P}(A)).$$

Oznaczałoby to, że zbiór $\mathcal{P}(\mathcal{P}(A))$ jest równoliczny z (pewnym podzbiorem zbioru) $\mathcal{P}(A)$. Sprzeczność z Twierdzeniem Cantora. ⊥

Twierdzenie Cantora-Bersteina

2.7 Definicja (Porównywanie mocy). Mówimy, że *moc zbioru A jest niewiększa od mocy zbioru B* i piszemy $|A| \leq |B|$, gdy istnieje zbiór $C \subseteq B$ taki, że $A \sim C$. Ponadto, $|A| < |B|$ wtedy i tylko wtedy, gdy $|A| \leq |B|$ oraz $|A| \neq |B|$.

2.8. Powtórzenie. Obraz i przeciwobraz.

2.9 Twierdzenie ([GZ1, Twierdzenie 6.10, Twierdzenie 6.11]). Dla dowolnych zbiorów A i B ,

$$(i) \quad |A| \leq |B| \iff \text{istnieje iniekcja } f : A \rightarrow B.$$

Ponadto, gdy zbiory A i B są niepuste,

$$(ii) \quad |A| \leq |B| \iff \text{istnieje suriekcja } g : B \rightarrow A.$$

Dowód. (i) Z definicji. (ii) \Rightarrow Załóżmy, że $|A| \leq |B|$. Wtedy z (i) istnieje $f : A \xrightarrow{1-1} B$. Dla ustalonego $a \in A$ definiujemy

$$g(x) = \begin{cases} f^{-1}(x), & \text{gdy } x \in \text{rng}(f); \\ a, & \text{gdy } x \notin \text{rng}(f). \end{cases}$$

Wówczas $g : B \xrightarrow{\text{na}} A$. \Leftarrow Niech $g : B \xrightarrow{\text{na}} A$, wtedy $g^{-1}[\{a\}] \neq \emptyset$ dla wszystkich $a \in A$. Stosujemy AC do $\{g^{-1}[\{a\}] : a \in A\}$ otrzymując selektor S . Oczywiście, $S \subseteq B$ oraz $g \upharpoonright S : S \xrightarrow{\text{na}, 1-1} A$. Zatem $|A| \leq |B|$. \dashv

2.10 Uwaga. Jeżeli $A \subseteq B$, to $|A| \leq |B|$, ponieważ $\text{id}_A : A \xrightarrow{1-1} \text{rng}(A) \subseteq B$.

2.11 Twierdzenie ([GZ1, Twierdzenie 6.12]). Dla dowolnych zbiorów A, B, C :

1. $|A| \leq |A|$,
2. $|A| \leq |B| \wedge |B| \leq |C| \rightarrow |A| \leq |C|$,
3. $|A| = |B| \rightarrow |A| \leq |B| \wedge |B| \leq |A|$.

Dowód. Korzystamy z faktów mówiących, że: identyczność jest injekcją, złożenie injekcji jest injekcją i każda bijekcja jest injekcją. \dashv

2.12. Twierdzenie Cantora-Bernsteina. Dla dowolnych zbiorów A i B :

$$\text{jeżeli } |A| \leq |B| \text{ oraz } |B| \leq |A| \text{ to } |A| = |B|.$$

Bez dowodu. \dashv

2.13 Przykład ([GZ1, Przykład 16]). Wiadomo z Przykładu 1.4¹, że $(a, b) \sim (c, d)$ dla dowolnych $a, b, c, d \in \mathbb{R}$ takich, że $a < b$ oraz $c < d$ oraz, że $(-1, 1) \sim \mathbb{R}$. Stosując Twierdzenie Cantora-Bernsteina, pokazujemy, że dla dowolnego zbioru A takiego, że

$$(0, 1) \subseteq A \text{ oraz } A \subseteq (0, 2),$$

mamy $|A| = |\mathbb{R}|$.

2.14 Przykład (Hotel Hilberta, [GZ1, Przykład 18]). $\mathbb{N} \cup \{-1\} \sim \mathbb{N}$.

2.15 Przykład (Hotel Hilberta, [GZ1, Przykład 19]). $(0, 1) \cup \{-1\} \sim (0, 1)$.

2.16 Przykład ([GZ1, Przykład 25]). Dla każdego zbioru A ,

$$|A| < |\mathcal{P}(A)|.$$

Dowód. Z Twierdzenie Cantora, $A \not\sim \mathcal{P}(A)$. Ponadto $|A| \leq |\mathcal{P}(A)|$, bo $f : A \xrightarrow{1-1} \mathcal{P}(A)$, dla funkcji f takiej, że $f(x) = \{x\}$. \dashv

Ćwiczenia

[GZ2, Wykład 6]. Wybór zadań spośród 6.1—6.7.

¹ [GZ1, Przykład 5.17, Przykład 5.20]

3 Trzecie zajęcia

Zbiory co najwyżej przeliczalne

3.1 Definicja (Zbiory skończone, co najwyżej przeliczalne i przeliczalne). Zbiór A nazywamy

1. *skończonym*, gdy $A = \emptyset$ lub istnieje liczba $0 < n \in \mathbb{N}$ taka, że $A \sim \{1, \dots, n\}$;
2. *przeliczalnym*, gdy $A \sim \mathbb{N}$;
3. *co najwyżej przeliczalnym*, gdy A jest zbiorem skończonym lub przeliczalnym;
4. *nieskończonym*, gdy A nie jest zbiorem skończonym;
5. *nieprzeliczalnym*, gdy A nie jest zbiorem co najwyżej przeliczalnym.

3.2 Twierdzenie ([GZ1, Twierdzenie 7.16, Dowód 3]). Każdy nieskończony podzbiór zbioru \mathbb{N} jest zbiorem przeliczalnym.

Dowód. Niech $X \subseteq \mathbb{N}$ będzie zbiorem nieskończonym (w szczególności X jest niepusty). Zasada Indukcji pociąga następującą Zasadę Minimum

*Każdy niepusty podzbiór zbioru \mathbb{N} ma element najmniejszy.*²

Definiujemy $g : \mathbb{N} \rightarrow X$

$$\begin{aligned} g(0) &= \min X \\ g(n) &= \min(X \setminus \{g(0), \dots, g(n-1)\}), \quad \text{dla } n > 0. \end{aligned}$$

Funkcja g jest iniekcją — wprost z definicji. Żeby wykazać, że g jest suriekcją wystarczy pokazać, że dla każdego $n \in \mathbb{N}$

$$n \in X \rightarrow \exists k (k \leq n \wedge g(k) = n).$$

Indukcja względem n . Baza jest oczywista, bo 0 jest najmniejszym elementem, więc $0 = g(0)$. Krok indukcyjny. Założenie dla $m \leq n$. *Przypadek 1:* $m+1 \notin X$ jest pusto spełniony. *Przypadek 2:* $m \in X$. *Podprzypadek 2a:* $n+1 \in \{g(0), \dots, g(n)\}$ jest oczywiste. *Podprzypadek 2b:* $n+1 \notin \{g(0), \dots, g(n)\}$. Wtedy $n+1 = \min((X \setminus \{g(0), \dots, g(n)\}))$, zatem $n+1 = g(n+1)$. \dashv

3.3 Twierdzenie ([GZ1, Twierdzenie 7.21, Dowód 1]). Niech $X \neq \emptyset$. Zbiór X jest zbiorem co najwyżej przeliczalnym wtedy i tylko wtedy, gdy elementy zbioru X można ustawić w ciąg.

Dowód. Zbiór X jest co najwyżej przeliczalny wtedy i tylko wtedy, gdy $|X| \leq |\mathbb{N}|$. Oraz $|X| \leq |\mathbb{N}|$ wtedy i tylko wtedy, gdy istnieje $f : \mathbb{N} \xrightarrow{\text{na}} X$. \dashv

3.4 Twierdzenie ([GZ1, Twierdzenie 7.23]). Suma dwóch zbiorów przeliczalnych jest zbiorem przeliczalnym.

² Ćwiczenie.

Dowód. Jeżeli $A = \emptyset$ lub $B = \emptyset$, to twierdzenie jest oczywiste. Załóżmy, że A i B są niepuste oraz co najwyżej przeliczalne, wtedy elementy zbiorów A i B można ustawić w ciągi

$$(x_n)_{n \in \mathbb{N}}, \quad (y_n)_{n \in \mathbb{N}}.$$

Wówczas elementy zbioru $A \cup B$ tworzą ciąg

$$x_0, y_0, x_1, y_1, \dots$$

Zatem $X \cup Y$ jest zbiorem co najwyżej przeliczalnym. \dashv

3.5 Wniosek ([GZ1, Wniosek 7.25]). Suma skończenie wielu zbiorów co najwyżej przeliczalnych jest zbiorem co najwyżej przeliczalnym.

3.6 Wniosek ([GZ1, Wniosek 7.26]). \mathbb{Z} jest zbiorem przeliczalnym.

Dowód. $\mathbb{Z} = \mathbb{N} \cup \{-n : n \in \mathbb{N}\}$. \dashv

3.7 Twierdzenie ([GZ1, Twierdzenie 7.27, Twierdzenie 7.28]). Produkt kartezjański dwóch zbiorów przeliczalnych jest zbiorem przeliczalnym.

Dowód. Niech $p : \mathbb{N} \times \mathbb{N} \xrightarrow{\text{na}, 1-1} \mathbb{N}$ będzie dowolną funkcją pary, np.

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

lub

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

Niech X i Y będą zbiorami przeliczalnymi oraz niech

$$g : \mathbb{N} \xrightarrow{\text{na}, 1-1} X \text{ oraz } h : \mathbb{N} \xrightarrow{\text{na}, 1-1} Y.$$

Wówczas funkcja $f : X \times Y \rightarrow \mathbb{N}$ określona jako

$$f(x, y) = p(g(x), h(y)) \quad \text{dla } x \in X, y \in Y$$

jest bijekcją. \dashv

3.8 Wniosek. \mathbb{Q} jest zbiorem przeliczalnym.

Dowód. Z faktu, że $\mathbb{N} \subseteq \mathbb{Q} \subseteq \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ i Twierdzenia Cantora-Bernsteina. \dashv

3.9 Wniosek. $\mathbb{R} \setminus \mathbb{Q}$ jest zbiorem nieprzeliczalnym.

Dowód. W przeciwnym przypadku zbiór \mathbb{R} byłby przeliczalny, gdyż $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$. Sprzeczność z Twierdzeniem 2.2. \dashv

3.10 Twierdzenie ([GZ1, Twierdzenie 7.32]). Suma przeliczalnej rodziny zbiorów przeliczalnych jest zbiorem przeliczalnym.

Dowód. Niech $\mathcal{R} = \{X_n : n \in \mathbb{N}\}$ i załóżmy, że $X_n \neq \emptyset$ dla $n \in \mathbb{N}$, oraz niech $f_n : \mathbb{N} \xrightarrow{\text{na}} X_n$. Definiujemy:

$$f : \mathbb{N} \times \mathbb{N} \xrightarrow{\text{na}} \bigcup_{n \in \mathbb{N}} X_n, \quad f(n, k) = f_n(k).$$

Pokazujemy, że f jest surjekcją. \dashv

3.11 Twierdzenie ([GZ1, Twierdzenie 7.33]). Zbiór X^* wszystkich skończonych ciągów o wartościach w niepustym co najwyżej przeliczalnym zbiorze X jest zbiorem przeliczalnym.

Dowód. Dla $n \in \mathbb{N}$ niech $X^{[n]}$ oznacza zbiór wszystkich ciągów o długości n o elementach z X . Indukcyjnie dowodzimy, że

$$X^{[n]} \text{ jest zbiorem cnp.}$$

Baza. Dla $n = 0$: $X^{[0]} = X^\emptyset = \emptyset$. Dla $n = 1$: $X^{[1]} \sim X$.

Krok indukcyjny. Zauważyć, że

$$X^{[n+1]} \sim X^{[n]} \times X.$$

Oczywiście,

$$X^* = \bigcup_{n \in \mathbb{N}} X^{[n]},$$

więc X^* jest przeliczalną sumą zbiorów co najwyżej przeliczalnych. \dashv

3.12 Wniosek ([GZ1, Wniosek 7.35]). Zbiór wszystkich skończonych podzbiorów zbioru przeliczalnego jest przeliczalny.

Dowód. Funkcja $f : X^* \xrightarrow{\text{na}} \mathcal{P}_{\text{fin}}(X)$ taka, że

$$f((x_n)_{n \in \mathbb{N}}) = \{x_n : n \in \mathbb{N}\}$$

jest suriekcją. Ponadto $\mathcal{P}_{\text{fin}}(X)$ jest nieskończony bo zawiera rodzinę $\{\{x\} : x \in X\}$. \dashv

3.13 Wniosek. Zbiór wszystkich wielomianów o współczynnikach z \mathbb{Z} jest przeliczalny. Zbiór liczb algebraicznych jest przeliczalny. Zbiór liczb przestępnych jest nieprzeliczalny.

Zbiory mocy kontinuum

3.14 Twierdzenie ([GZ1, Twierdzenia 8.16]). $|\mathbb{R}| = |\{0, 1\}^{\mathbb{N}}| = |\mathbb{N}^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|$.

Bez dowodu. \dashv

3.15 Definicja (Zbiory mocy kontinuum). Dowolny zbiór równoliczny z \mathbb{R} nazywamy *zbiorem mocy kontinuum*.

3.16 Twierdzenie. Zbiory *wszystkich skończonych* ciągów oraz wszystkich skończonych podzbiorów zbioru przeliczalnego są przeliczalne. Zbiory *wszystkich* ciągów oraz wszystkich podzbiorów zbioru przeliczalnego są zbiorami mocy kontinuum.

Bez dowodu. \dashv

3.17 Twierdzenie. Zbiory liczb naturalnych, całkowitych i wymiernych są przeliczalne. Zbiory liczb rzeczywistych i niewymiernych są mocy kontinuum.

Ćwiczenia

[GZ2, Wykład 7]. Wybór zadań spośród 7.1—7.9.

4 Czwarte zajęcia

Częściowe porządki

4.1 Definicja (Częściowy porządek, liniowy porządek, łańcuch). Relację \preceq na zbiorze A nazywamy *relacją częściowego porządku*, gdy

1. \preceq jest zwrotna: $\forall x \in X \ x \preceq x$,
2. \preceq jest słabo-symetryczna: $\forall x, y \in A \ (x \preceq y \wedge y \preceq x \rightarrow x = y)$,
3. \preceq jest przechodnia: $\forall x, y, z \in X \ (x \preceq y \wedge y \preceq z \rightarrow x \preceq z)$.

Jeżeli \preceq jest częściowym porządkiem na A , to parę $\langle A, \preceq \rangle$ nazywamy *zbiorem częściowo uporządkowanym*. Relację częściowego porządku \preceq nazywamy *relacją liniowego porządku*, gdy dodatkowo

4. \preceq jest spójna: $\forall x, y \in A \ (x \preceq y \vee y \preceq x)$.

Niech A będzie zbiorem częściowo uporządkowanym przez relację \preceq . Podzbiór B zbioru A taki, że $\preceq|_B$ jest relacją liniowego porządku nazywamy *łańcuchem*.

4.2 Przykład. Przykłady zbiorów częściowo uporządkowanych:

1. $\langle X, \subseteq \rangle$, dla dowolnego zbioru X ,
2. $\langle \mathbb{R}, \leq \rangle$,
3. $\langle \mathbb{R}, \geq \rangle$,
4. $\langle \mathbb{N} \setminus \{0\}, | \rangle$,
5. $\langle \mathbb{R}^{\mathbb{N}}, \preceq \rangle$, gdzie $f \preceq g \iff \forall n. f(n) \leq g(n)$,
6. $\langle X, \preceq \rangle$, gdzie X jest dowolnym zbiorem funkcji oraz $f \preceq g$ wtedy i tylko wtedy, gdy $f = g \upharpoonright \text{dom}(f)$,
7. *Porządek prefiksowy*. Ustalmy dowolny niepusty zbiór A . Zbiór ten będziemy nazywać *alfabetem*. Niech A^* będzie zbiorem wszystkich skończonych ciągów elementów ze zbioru A . Zbiór A^* nazywać będziemy zbiorem *słów nad alfabetem* A . Do zbioru A^* należy *słowo puste*, czyli słowo o długości 0, które będziemy oznaczać przez ϵ . Na zbiorze słów definiujemy binarną operację *konkatenacji* oznaczaną symbolem $*$: dla dowolnych $a, b \in A^*$, takich że $a = a_1, \dots, a_m$ oraz $b = b_1, \dots, b_n$, definiujemy

$$a * b = c,$$

gdzie

$$c_i = \begin{cases} a_i & \text{dla } 1 \leq i \leq m \\ b_j & \text{dla } i = m + j. \end{cases}$$

Na zbiorze słów A^* definiujemy relację \preceq *porządku prefiksowego* w następujący sposób:

$$a \preceq b \iff \exists c. (b = a * c).$$

Wówczas \preceq jest relacją częściowego porządku na A^* .

8. *Porządek leksykograficzny.* Ustalmy zbiór częściowo uporządkowany (A, \leq) . Rozważmy zbiór słów A^* oraz relację \preceq zwaną *porządkiem leksykograficznym nad* (A, \leq) zdefiniowaną następująco: dla $a, b \in A^*$,

$$a \preceq b \leftrightarrow a \leq b \vee \exists i (a_i < b_i \wedge \forall j < i (a_j < b_j)).$$

Porządek leksykograficzny \preceq nad (A, \leq) jest częściowym porządkiem. Ponadto, gdy (A, \leq) jest zbiorem liniowo uporządkowanym, to (A^*, \preceq) jest również zbiorem liniowo uporządkowanym.

4.3 Przykład. Przykłady łańcuchów w zbiorach częściowo uporządkowanych z Przykładu 4.2.

Diagramy Hassego

4.4 Przykład. Diagramy Hassego dla zbiorów częściowo uporządkowanych z Przykładu 4.2 oraz [GZ1, Przykład 10.8].

Elementy wyróżnione

4.5 Definicja (Elementy minimalny, maksymalny, największy, najmniejszy, kresy). Niech X będzie zbiorem częściowo uporządkowanym przez relację \preceq . Ponadto, niech $a \in X$ oraz $A \subseteq X$. Mówimy, że element a jest

1. *minimalnym* w A , gdy $a \in A$ oraz $x \preceq a \rightarrow x = a$ dla każdego $x \in A$;
2. *maksymalnym* w A , gdy $a \in A$ oraz $a \preceq x \rightarrow x = a$ dla każdego $x \in A$;
3. *najmniejszym* w A , gdy $a \in A$ oraz $a \preceq x$ dla każdego $x \in A$;
4. *największym* w A , gdy $a \in A$ oraz $x \preceq a$ dla każdego $x \in A$;
5. *ograniczeniem dolnym* zbioru A , gdy $a \preceq x$ dla każdego $x \in A$;
6. *ograniczeniem górnym* zbioru A , gdy $x \preceq a$ dla każdego $x \in A$;
7. *kresem dolnym* (*infimum*) zbioru A , gdy a jest największym ograniczeniem dolnym zbioru A , co zapisujemy $a = \inf A$;
8. *kresem górnym* (*supremum*) zbioru A , gdy a jest najmniejszym ograniczeniem górnym zbioru A , co zapisujemy $a = \sup A$.

4.6 Przykład. Przykłady elementów wyróżnionych na podstawie Przykładu 4.2 i Przykładu 4.2 oraz [GZ1, Przykład 10.8].

4.7 Twierdzenie ([GZ1, Twierdzenie 10.7]). Niech X będzie zbiorem częściowo uporządkowanym przez relację \preceq oraz niech $A \subseteq X$. Wtedy

1. W A istnieje co najwyżej jeden element największy i co najwyżej jeden element najmniejszy.
2. Zbiór A ma co najwyżej jeden kres górny i co najwyżej jeden kres dolny.
3. Jeżeli $a \in A$ jest elementem największym w A , to a jest
 - (i) jedynym elementem maksymalnym w A ,

(ii) kresem górnym zbioru A .

4. Jeżeli $a \in A$ jest elementem najmniejszym w A , to a jest

(i) jedynym elementem minimalnym w A ,

(ii) kresem dolnym zbioru A .

Dowód. 1. Słaba antysymetria.

2. Definicja kresów.

3. Maksymalność oczywista. Element a jest ograniczeniem górnym zbioru A . Niech $x \in X$ będzie ograniczeniem górnym zbioru A , wtedy w szczególności $a \preceq x$; zatem a jest najmniejszym ograniczeniem górnym zbioru A .

4. j.w. \dashv

4.8 Twierdzenie. Niech X będzie zbiorem częściowo uporządkowanym przez relację \preceq oraz niech $A \subseteq X$ będzie łańcuchem. Wtedy

1. W A istnieje co najwyżej jeden element minimalny i jest on jednocześnie elementem najmniejszym w A .
2. W A istnieje co najwyżej jeden element maksymalny i jest on jednocześnie elementem największym w A .

Dowód. Łatwo. \dashv

4.9 Twierdzenie. Niech X będzie zbiorem częściowo uporządkowanym przez relację \preceq oraz niech $\emptyset \neq A \subseteq X$ będzie zbiorem skończonym. Wtedy

1. W A istnieje element maksymalny i element minimalny.
2. Jeżeli w A istnieje dokładnie jeden element maksymalny, to jest on jednocześnie elementem największym w A .
3. Jeżeli w A istnieje dokładnie jeden element minimalny, to jest on jednocześnie elementem najmniejszym w A .

Dowód. 1. Indukcja względem $|A|$.

2. Niech a będzie jedynym elementem maksymalnym w A i przypuśćmy, że a nie jest największym w A . Wówczas istnieje $b \in A$ taki, że $a \neq b$ oraz $b \not\prec a$. Niech

$$B = \{x \in A : b \preceq x\}.$$

Ponieważ $B \subseteq A$, to zbiór B jest skończony, a zatem na mocy pierwszego punktu twierdzenia, w B istnieje element maksymalny c .

Pokażemy, że c jest również elementem maksymalnym w A . Przypuśćmy dla dowodu nie wprost, że $c \prec x$ dla pewnego $x \in A$. Ponieważ $c \in B$, mamy wtedy $b \preceq c \prec x$, skąd $x \in B$. Ponieważ $c \prec x$, element c nie jest maksymalny w B , wbrew założeniu.

Z drugiej strony, $a \notin B$, bo w przeciwnym razie mielibyśmy $b \preceq a$ — sprzeczność z założeniem, że $b \not\prec a$. Zatem $a \neq c$. Sprzeczność z założeniem, że a jest jedynym elementem maksymalnym w A . \dashv

Lemat Kuratowskiego-Zorna

4.10. W skończonych zbiorach częściowo uporządkowanych zawsze istnieją elementy maksymalne i minimalne. Na ogół nieskończony zbiór częściowo uporządkowany nie musi zawierać elementów maksymalnych ani minimalnych. Warunek dostateczny na istnienie elementów maksymalnych podany jest w następującym twierdzeniu zwanym Lematem Kuratowskiego-Zorna. Twierdzenie to jest bardzo często stosowane w celu dowodzenia istnienia elementów o z góry określonych własnościach.

4.11. Lemat Kuratowskiego-Zorna. Niech X będzie zbiorem częściowo uporządkowanym przez relację \preceq . Wówczas, jeżeli każdy łańcuch ma ograniczenie górne w X , to w X istnieje element maksymalny.

Ćwiczenia

[GZ2, Wykład 10]. Wybór zadań spośród 10.1—10.4, 10.7, 10.8.

5 Piąte zajęcia

Izomorfizmy zbiorów częściowo uporządkowanych

5.1 Definicja. Niech (X, \leq_X) i (Y, \leq_Y) będą zbiorami częściowo uporządkowanymi. Funkcję $f : X \rightarrow Y$ nazywamy *izomorfizmem* zbiorów częściowo uporządkowanych (X, \leq_X) i (Y, \leq_Y) , gdy

1. f jest bijekcją,
2. f zachowuje porządek, czyli

$$\forall a, b \in X \ (a \leq_X b \leftrightarrow f(a) \leq_Y f(b))$$

5.2 Przykład. Przykłady z [GZ1, Przykład 10.16, Przykład 10.17].

Drzewa

5.3 Definicja. Niech A będzie zbiorem niepustym i niech \leq będzie prefikсовym porządkiem na A^* . *Drzewem nad A* nazywamy dowolny niepusty podzbiór T zbioru A^* spełniający warunek

$$u \in T \wedge v \leq u \rightarrow v \in T,$$

dla dowolnych $u, v \in T$.

5.4. Jeżeli nie prowadzi to do niejednoznaczności symbol konkatencji $*$ będziemy pomijać, dla słowa u i elementu a pisząc ua zamiast $u * a$.

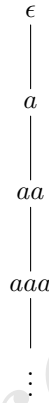
5.5. Ponieważ słowo puste ϵ jest elementem najmniejszym w (A^*, \leq) , z Definicji 5.3 wynika bezpośrednio, że ϵ należy do każdego drzewa. Element ten nazywamy *korzeniem* drzewa. Dowolny element drzewa nazywamy *wierzchołkiem*. Jeśli w drzewie T nad A , dla pewnych $u \in T$ oraz $a \in A$ mamy $ua \in T$, to wierzchołek ua nazywamy *a -następnikiem* wierzchołka u . Wierzchołki nie mające następników nazywamy *liśćmi* drzewa. *Rzędem wierzchołka u* nazywamy moc zbioru wszystkich następników tego wierzchołka. *Gałęzią* drzewa T nazywamy dowolny maksymalny łańcuch w T .

5.6 Przykład. Przykłady drzew:

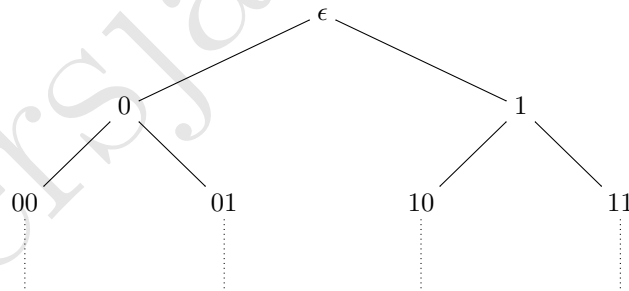
1. $\{\epsilon\}$
2. Niech $A = \{a\}$ oraz niech

$$a^n = \underbrace{a * \dots * a}_{n\text{-razy}}.$$

Wówczas $\{a^n : n \in \mathbb{N}\}$ jest drzewem. Poniżej przedstawiamy jego diagram.



3. Niech A będzie dowolnym alfabetem. Wówczas A^* nazywamy *pełnym drzewem nad A* . W szczególności, $\{0, 1\}^*$ nazywamy *pełnym drzewem binarnym*.



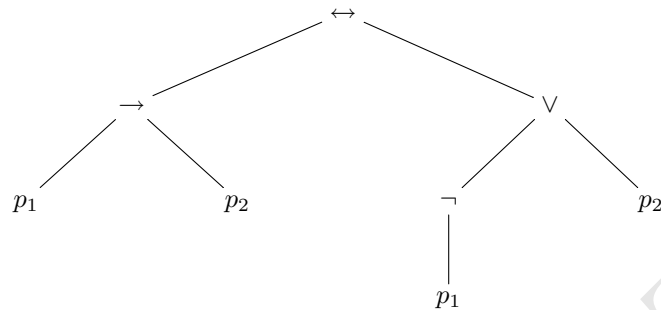
4. Niech $k > 0$. Dowolne drzewo T zawarte w zbiorze $\{0, 1, \dots, k-1\}$ nazywamy *drzewem k -argumentowym*, gdy każdy wierzchołek drzewa T niebędący liściem ma rząd równy k . Przykład drzewa 2-argumentowego:

$$T_1 = \{0^n : n \in \mathbb{N}\} \cup \{0^n 1 : n \in \mathbb{N}\} \cup \{0^{2n+1} 10 : n \in \mathbb{N}\} \cup \{0^{2n+1} 11 : n \in \mathbb{N}\}.$$

5.7. *Drzewem etykietowanym* nazywamy dowolne drzewo, w którym każdemu wierzchołkowi przyporządkowana jest dokładnie jeden element z ustalonego zbioru Σ , zwany *etykietą*.

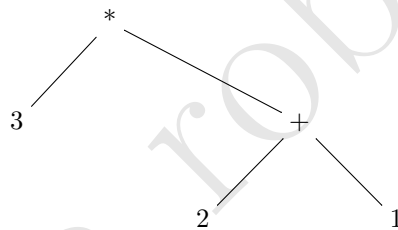
5.8 Przykład. Przykłady drzew etykietowanych:

1. Niech $\Sigma = \{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\} \cup \{p_i : i \in \mathbb{N}\}$. Drzewem struktury formuły $(p_1 \rightarrow p_2) \leftrightarrow (\neg p_1 \vee p_2)$ jest struktura postaci



Na diagramie przedstawiono etykiety przyporządkowane do odpowiednich wierzchołków drzewa.

2. *Drzewo wyrażeń arytmetycznych.* Wyrażenie arytmetyczne $3 * (2 + 1)$ jest reprezentowane przez następujące drzewo:



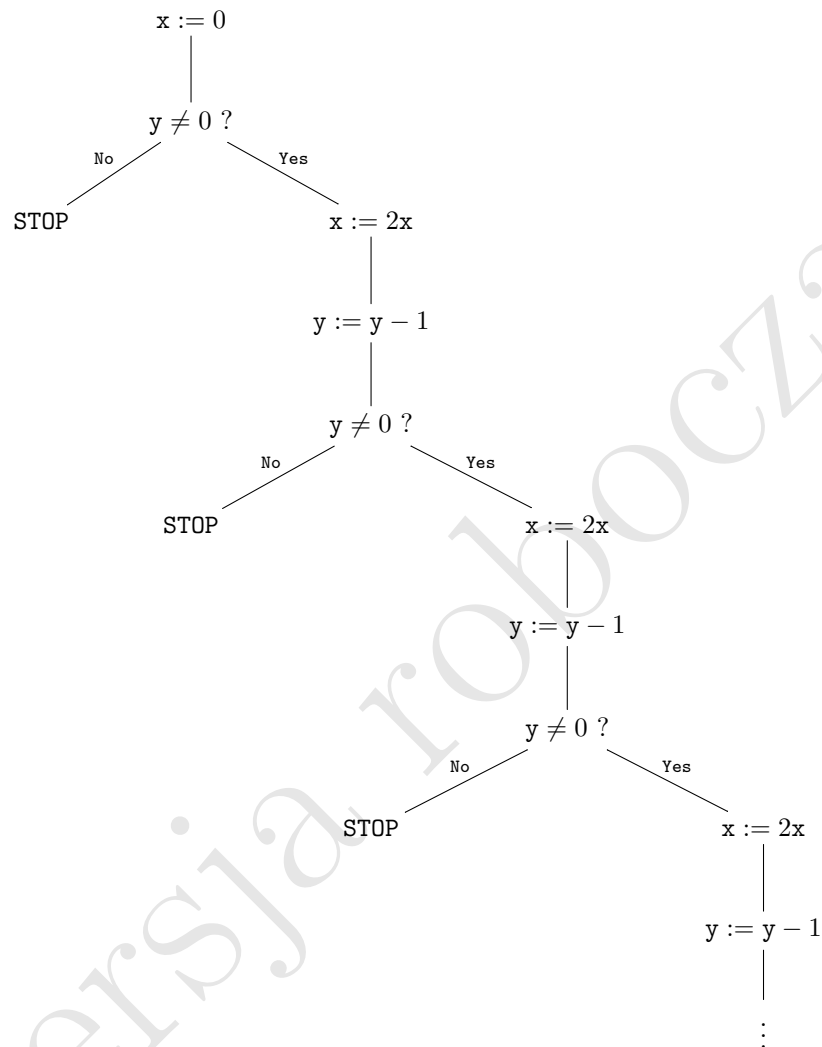
3. Rozważmy następujący program:

```

x:= 1;
while y ≠ 0 do
  x:= 2x ; y:=y-1 end
  
```

Program ten możemy reprezentować za pomocą nieskończonego drzewa

etykietowanego zwanego jego *drzewem formalnych obliczeń*.



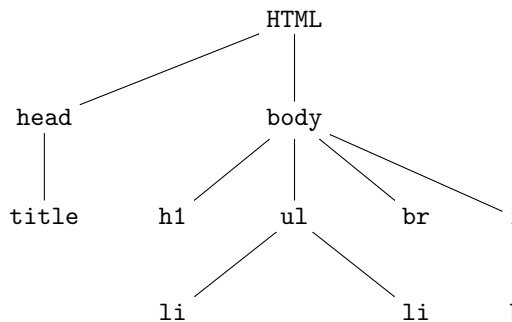
4. Rozważmy następujący dokument HTML:

```

<HTML>
  <HEAD>
    <TITLE>Matematyka 2</TITLE>
  </HEAD>
  <BODY>
    <H1>Relacje częściowego porządku</H1>
    <UL>
      <LI>Drzewa</LI>
      <LI>Kraty</LI>
    </UL>
    <BR>
    <I>Data ostatniej aktualizacji:
    <B>18 lutego 2015</B></I>
  
```

```
</BODY>
</HTML>
```

Kod w HTML ma strukturę drzewa:



5.9 Twierdzenie (Lemat Königa). Niech $T \subseteq A^*$ będzie drzewem nieskończonym, w którym każdy wierzchołek jest skończonego rzędu. Wówczas T zawiera ścieżkę nieskończoną.

Dowód. Nieskończoną gałąź x_0, x_1, x_2, \dots drzewa T definiujemy indukcyjnie:

- (i) Jako x_0 przyjmujemy korzeń drzewa T . Ponieważ drzewo T jest nieskończone, wierzchołek x_0 ma nieskończenie wiele następników.
- (ii) Załóżmy, że wierzchołki x_0, x_1, \dots, x_{n-1} wybrane zostały w ten sposób, że x_{i+1} jest bezpośrednim następnikiem x_i oraz tak, że x_{i+1} ma nieskończenie wiele następników. Z założenia, wierzchołek x_{n-1} jest skończonego rzędu, czyli ma tylko skończenie wiele *bezpośrednich* następników. Zatem, ponieważ x_{n-1} ma nieskończenie wiele następników, co najmniej jeden z bezpośrednich następników wierzchołka x_{n-1} ma nieskończenie wiele następników.

Ponieważ krok(ii) jest wykonalny dla każdego x_n , dla $n \in \mathbb{N}$, otrzymujemy nieskończoną gałąź x_0, x_1, \dots drzewa T . \dashv

Ćwiczenia

[GZ2, Wykład 10], 10.10, 10.15 (a), (b), (c).

5.10 Ćwiczenie. Niech T będzie drzewem skończonym. W tym przypadku mówimy, że T jest *pełnym drzewem binarnym* gdy każdy jego wierzchołek poza liśćmi jest stopnia 2. Pokazać, że każde skończone pełne drzewo binarne ma nieparzystą liczbę wierzchołków.

6 Szóste zajęcia

Kraty i algebry Boole'a

Kraty

6.1 Definicja. Zbiór częściowo uporządkowany (A, \leq) nazywamy *kratką*, gdy każdy dwuelementowy podzbiór zbioru A ma kresy. Kres dolny elementów x i

y oznaczać będziemy przez $x \cap y$, a kres górny przez $x \cup y$. Największy element kraty (o ile istnieje) oznaczać będziemy przez 1, a element najmniejszy (o ile istnieje) przez 0. Kratę nazywamy *zupełną* gdy każdy podzbiór zbioru A ma kresy.

Kratę (A, \leq) nazywamy *dystrybutywną*, gdy dla dowolnych $x, y, z \in A$ zachodzą równości:

$$\begin{aligned} ((x \cup y) \cap z) &= (x \cap z) \cup (y \cap z), \\ ((x \cap y) \cup z) &= (x \cup z) \cap (y \cup z). \end{aligned}$$

6.2 Przykład. Przykłady krat.

1. Dla dowolnego niepustego zbioru A zbiór częściowo uporządkowany $(\mathcal{P}(A), \subseteq)$ jest kratą zupełną. Krata ta jest dystrybutywna.
2. (\mathbb{N}, \leq) jest kratą. Nie jest to krata zupełna, ale każdy niepusty podzbiór ma kres dolny. Krata ta jest dystrybutywna.
3. $(\mathbb{N}, |)$ jest kratą. Nie jest to krata zupełna. Krata ta jest dystrybutywna.
4. Każdy zbiór liniowo uporządkowany jest kratą dystrybutywną.

6.3 Twierdzenie. W dowolnej kratce zachodzą równości:

$$x \cup y = y \cup x, \quad x \cap y = y \cap x \quad (1)$$

$$x \cup (y \cap z) = (x \cup y) \cap z, \quad x \cap (y \cup z) = (x \cap y) \cup z \quad (2)$$

$$(x \cap y) \cup y = y, \quad x \cap (x \cup y) = x. \quad (3)$$

6.4 Twierdzenie (Knaster-Tarski). Niech (K, \leq) będzie kratą zupełną oraz niech $f : K \rightarrow K$ będzie funkcją monotoniczną, czyli spełniającą warunek

$$\forall x, y \in K (x \leq y \rightarrow f(x) \leq f(y)).$$

Wtedy f ma najmniejszy punkt stały, to znaczy istnieje element $a \in K$ taki, że $f(a) = a$ oraz dla każdego $x \in K$, jeżeli $f(x) = x$, to $a \leq x$.

Dowód. Rozważmy zbiór $X = \{x \in K : f(x) \leq x\}$. Oczywiście $1 \in X$, zatem $X \neq \emptyset$. Niech

$$a := \inf(X).$$

Niech x będzie dowolnym elementem zbioru X . Wówczas $a \leq x$, skąd otrzymujemy $f(a) \leq f(x)$, gdyż f jest funkcją monotoniczną. Ponieważ $x \in X$, mamy również $f(x) \leq x$, skąd dostajemy

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

Zatem $f(a)$ jest ograniczeniem dolnym zbioru X , w szczególności,

$$f(a) \leq a. \quad (*)$$

Stąd, na mocy monotoniczności funkcji f ,

$$f(f(a)) \leq f(a),$$

czyli $f(a) \in X$. Zatem

$$a \leq f(a). \quad (**)$$

Z (*) oraz (**) dostajemy $f(a) = a$, czyli a jest punktem stałym funkcji f .

Pokażemy, że a jest najmniejszym punktem stałym. Załóżmy, że b jest dowolnym punktem stałym funkcji f . Wtedy, w szczególności, $f(b) \leq b$ czyli $b \in X$. Ponieważ $a = \inf(X)$, otrzymujemy $a \leq b$. \dashv

6.5 Przykład. Niech A będzie dowolnym alfabetem zawierającym 0 i 1. Definiujemy funkcję $f : \mathcal{P}(A^*) \rightarrow \mathcal{P}(A^*)$ w następujący sposób: dla dowolnego zbioru $X \subseteq A^*$,

$$f(X) = \{\epsilon\} \cup \{0w : w \in X\} \cup \{1w : w \in X\}.$$

Wówczas f jest funkcją monotoniczną i zbiór $\{0, 1\}^*$ jest najmniejszym punktem stałym funkcji f .

Algebry Boole'a

6.6 Definicja. Kratę dystrybutywną (A, \leq) nazywamy *algebrą Boole'a*, gdy ma element największy 1 i element najmniejszy 0 oraz dla każdego elementu $x \in A$ istnieje element $-x \in A$, zwany *dopełnieniem* elementu x , taki że

$$x \cap -x = 0 \quad \text{oraz} \quad x \cup -x = 1.$$

Algebrę Boole'a nazywamy *zupełną*, gdy jest kratą zupełną.

6.7 Przykład. Przykłady algebr Boole'a.

1. $(\{0, 1\}, \leq)$, gdzie $0 \leq 1$, jest algebrą Boole'a.
2. Dla dowolnego zbioru X , $(\mathcal{P}(X), \subseteq)$ jest zupełną algebrą Boole'a.
3. Skończone algebry Boole'a dwu-, cztero- i ośmioelementowe: diagramy Hassego.

6.8 Twierdzenie. Każda skończona algebra Boole'a jest izomorficzna z algebrą $(\mathcal{P}(X), \subseteq)$ dla pewnego skończonego zbioru X . W szczególności, każda skończona algebra Boole'a ma 2^n elementów, dla pewnego $n \in \mathbb{N}$.

Ćwiczenia

[LM]: 56, 57, 58.

7 Siódme zajęcia

7.1 Definicja (Relacja). *Relacją (binarną)* nazywamy dowolny podzbiór produktu kartezjańskiego dwóch zbiorów. *Dziedziną lewostronną* relacji R nazywamy zbiór $D_l(R) = \{x : \langle x, y \rangle \in R \text{ dla pewnego } y\}$, a *dziedziną prawostronną* relacji R nazywamy zbiór $D_r(R) = \{y : \langle x, y \rangle \in R \text{ dla pewnego } x\}$. Zbiór $D_l(R) \cup D_r(R)$ nazywamy *polem* relacji R .

7.2 Definicja (Złożenie relacji, relacja odwrotna). *Złożeniem relacji* R i S nazywamy relację

$$S \circ R = \{\langle x, z \rangle : \text{dla pewnego } y, \langle x, y \rangle \in R \text{ oraz } \langle y, z \rangle \in S\}.$$

Relacją odwrotną do R nazywamy relację

$$R^{-1} = \{\langle y, x \rangle : \langle x, y \rangle \in R\}.$$

7.3 Twierdzenie. Dla dowolnych relacji R i S mamy

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}.$$

Dowód. Mamy

$$\begin{aligned} \langle a, b \rangle \in (S \circ R)^{-1} &\iff \langle b, a \rangle \in (S \circ R) \\ &\iff \exists c . \langle b, c \rangle \in R \wedge \langle c, a \rangle \in S \\ &\iff \exists c . \langle c, b \rangle \in R^{-1} \wedge \langle a, c \rangle \in S^{-1} \\ &\iff \langle a, b \rangle \in R^{-1} \circ S^{-1}. \end{aligned}$$

A zatem $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$. +

7.4 Definicja (Relacja równoważności). Relację $R \subseteq X \times X$ nazywamy *relacją równoważności*, gdy

1. R jest zwrotna: $\forall x \in X \ xRx$,
2. R jest symetryczna: $\forall x, y \in X \ (xRy \rightarrow yRx)$,
3. R jest przechodnia: $\forall x, y, z \in X \ (xRy \wedge yRz \rightarrow xRz)$.

7.5 Przykład. Następujące relacje są relacjami równoważności:

1. $A = \mathcal{P}(\{1, \dots, n\})$ oraz $X R_A Y \iff X \sim Y$.
2. $B = \mathbb{Z}$ oraz $k R_B l \iff k \equiv l \pmod{3}$.
3. $C = \mathbb{N} \times \mathbb{N}$ oraz

$$\langle m_1, n_1 \rangle R_C \langle m_2, n_2 \rangle \iff m_1 + n_2 = m_2 + n_1.$$

4. $D = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ oraz

$$\langle k, l \rangle R_D \langle p, q \rangle \iff kq = lp.$$

7.6 Definicja (Klasa abstrakcji, zbiór ilorazowy). Niech R będzie relacją równoważności w zbiorze $X \neq \emptyset$. *Klasą abstrakcji* elementu $a \in X$ względem relacji R nazywamy zbiór

$$[a]_R = \{x \in X : xRa\}.$$

Zbiorem ilorazowym zbioru A względem relacji R nazywamy zbiór

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

7.7 Przykład. Zbiory ilorazowe:

1. $A/R_A =$.
2. $B/R_B =$.
3. $C/R_C =$.
4. $D/R_D =$.

7.8 Definicja (Podział zbioru). Rodzinę \mathcal{P} podzbiorów zbioru A nazywamy *podziałem* zbioru A gdy

1. $X \neq \emptyset$, dla każdego $X \in \mathcal{P}$;
2. $X \neq Y \rightarrow X \cap Y = \emptyset$, dla dowolnych $X, Y \in \mathcal{P}$;
3. $\bigcup \mathcal{P} = A$.

7.9 Przykład. Podziały:

1. $A/R_A =$.
2. $B/R_B =$.
3. $C/R_C =$.
4. $D/R_D =$.

7.10 Lemat. Niech R będzie relacją równoważności na zbiorze A . Wówczas, dla dowolnych $a, b \in A$ mamy $aRb \iff [a]_R = [b]_R$.

Dowód. Łatwo. ⊢

7.11 Twierdzenie (Zasada abstrakcji). Niech A będzie dowolnym niepustym zbiorem. Wówczas

1. Jeżeli R jest relacją równoważności na A , to A/R jest podziałem zbioru A .
2. Jeżeli rodzina \mathcal{P} jest podziałem zbioru A , to relacja R zdefiniowana jako

$$xRy \iff x, y \in Z, \text{ dla pewnego } Z \in \mathcal{P}$$

jest relacją równoważności na A .

3. Funkcja F określona na zbiorze wszystkich relacji równoważności R na A taka, że

$$F(R) = A/R$$

przekształca ten zbiór wzajemnie jednoznacznie na zbiór wszystkich podziałów zbioru A .

Dowód. [GZ1, Twierdzenie 9.6].

1. Mamy: $[a]_R \neq \emptyset$ (przechodność R); dla $a \neq b$, $[a]_R$ i $[b]_R$ są rozłączne (przechodność R); $\bigcup_{a \in A} [a]_R = A$ (zwrotność R).
2. Łatwo.
3. Opuszczam. ⊢

Literatura

- [GZ1] W. Guzicki, P. Zakrzewski. *Wykłady ze wstępu do matematyki*. PWN 2005.
- [GZ2] W. Guzicki, P. Zakrzewski. *Wstęp do matematyki. Zbiór zadań*. PWN 2005.
- [LM] I. Ławrow, L. Maksimowa. *Zadania z teorii mnogości, logiki matematycznej i teorii algorytmów*. PWN 2004.

tp. 18 lutego 2021