

# Matematyczne podstawy kognitywistyki

Jerzy Pogonowski

Zakład Logiki i Kognitywistyki UAM

pogon@amu.edu.pl

Struktury algebraiczne

# Matematyka jako nauka o strukturach

- Zarówno w samej matematyce, jak i w jej zastosowaniach w innych naukach bada się różnego rodzaju *struktury*. Składają się one z pewnego *uniwersum* (zbioru obiektów) oraz relacji i funkcji określonych na tym uniwersum.
- Uniwersa liczb (naturalnych, całkowitych, wymiernych, rzeczywistych) wyposażone były zarówno w strukturę porządkową, jak też w strukturę wyznaczoną przez *działania arytmetyczne* na liczbach: dodawanie, odejmowanie, mnożenie, dzielenie, potęgowanie, itd.
- Także w rozważaniach geometrycznych mowa jest o pewnych strukturach: obiektami są np. punkty, proste, płaszczyzny, odcinki, okręgi i wiele innych figur geometrycznych, między którymi zachodzą różne zależności (podobieństwo, przystawanie, leżenie między, itp.) i dla których określone są funkcje, wyznaczające np. ich własności miarowe (długość, pole, objętość, odległość, itp.).

# Opisy aksjomatyczne

- Obecnie obowiązującym standardem jest charakteryzowanie struktur na sposób *aksjomatyczny*. Polega on na przyjęciu pewnych założeń o badanych obiektach, relacjach, funkcjach, przy czym owe założenia spełniać muszą określone warunki, np.: nie mogą być wzajem *sprzeczne*, powinny być od siebie *niezależne*, powinny być – w jakimś sensie – oczywiste, naturalne.
  - Cała reszta roboty dedukcyjnej matematyka polega na dowodzeniu *twierdzeń* o strukturach scharakteryzowanych wyjściowymi aksjomatami.
- 
- Matematyka interesują liczby wraz z operacjami na nich, „gołe” liczby interesują być może filozofów.
  - Matematyk pytany o to, *czym* są liczby danego rodzaju odpowie: są obiektami, które spełniają założone o nich aksjomaty.

- Przez *strukturę relacyjną* rozumiemy układ złożony ze zbioru (*uniwersum struktury*) oraz określonych na tym zbiorze relacji i funkcji.
- Dla dowolnego zbioru  $A$  niech  $A^*$  oznacza zbiór wszystkich skończonych potęg kartezyjskich zbioru  $A$ , czyli  $A^* = \{A, A^2, A^3, \dots\}$ .

*Strukturę relacyjną* nazywamy dowolny układ:

$\mathbf{A} = (A, \{r_i : i \in I\}, \{f_j : j \in J\}, \{a_k : k \in K\})$ , gdzie:

- 1  $A$  jest zbiorem (uniwersum struktury, oznaczanym  $dom(\mathbf{A})$ );
- 2  $\{r_i : i \in I\}$  jest zbiorem relacji, z których każda jest określona na jakimś elemencie zbioru  $A^*$ ;
- 3  $\{f_j : j \in J\}$  jest zbiorem funkcji, z których każda działa z jakiegoś elementu zbioru  $A^*$  w zbiór  $A$ ;
- 4  $\{a_k : k \in K\}$  jest zbiorem elementów (wyróżnionych) zbioru  $A$ .

Struktury o postaci  $(A, \{f_j : j \in J\}, \{a_k : k \in K\})$  nazywamy *algebrami*.

# Przykłady

- Zbiór  $\mathbb{N}$  liczb naturalnych wraz z operacjami dodawania i mnożenia, uporządkowany przez relację mniejszości.
  - Zbiór  $\mathbb{Z}$  liczb całkowitych wraz z operacjami dodawania, odejmowania oraz mnożenia, uporządkowany przez relację mniejszości.
  - Zbiór  $\mathbb{Q}$  liczb wymiernych wraz z operacjami dodawania, odejmowania, mnożenia oraz dzielenia, uporządkowany przez relację mniejszości.
  - Zbiór  $\mathbb{R}$  liczb rzeczywistych wraz z operacjami dodawania, odejmowania, mnożenia oraz dzielenia, uporządkowany przez relację mniejszości.
- 
- Zbiór wszystkich wielomianów o współczynnikach rzeczywistych wraz z operacjami dodawania i mnożenia wielomianów.
  - Zbiór wszystkich permutacji skończonego zbioru  $X$  wraz z operacją składania permutacji (rozumianą jako złożenie funkcji).

## Przykłady

Niech  $A = \{0, 1, 2\}$ , a operacja  $\oplus_3 : A \times A \rightarrow A$  niech dla argumentów  $x$  oraz  $y$  daje wartość równą reszcie z dzielenia  $x + y$  przez 3, natomiast operacja  $\otimes_3 : A \times A \rightarrow A$  dla argumentów  $x$  oraz  $y$  daje wartość równą reszcie z dzielenia  $x \cdot y$  przez 3. Wtedy tabelki tych operacji wyglądają następująco:

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- Dla dowolnego zbioru  $X$ , układ  $(\wp(X), \subseteq, \cup, \cap, X, \emptyset)$  jest strukturą relacyjną.
- Zbiór wartości logicznych wraz z określonymi na nich funkcjami prawdziwościami jest strukturą relacyjną.

Niech  $(A, \circ)$  będzie algebrą z jednym działaniem dwuargumentowym. Powiemy, że:

- 1  $\circ$  jest *przemienne*, gdy  $x \circ y = y \circ x$  dla wszystkich  $x, y \in A$
- 2  $\circ$  jest *łącznie*, gdy  $x \circ (y \circ z) = (x \circ y) \circ z$  dla wszystkich  $x, y, z \in A$
- 3 element  $e \in A$  jest *neutralny* dla działania  $\circ$ , gdy  $x \circ e = e \circ x = x$  dla wszystkich  $x \in A$ . Element neutralny działania nazywamy też *modułem* działania.
- 4 Powiemy, że  $y$  jest elementem *odwrotnym* dla  $x$  (względem  $\circ$ ), gdy  $x \circ y = y \circ x = e$ .

Niech  $(A, \oplus, \otimes)$  będzie algebrą z dwiema operacjami dwuargumentowymi. Powiemy, że operacja  $\otimes$  jest względem operacji  $\oplus$ : *lewostronnie rozdzielna*, gdy  $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$ , dla wszystkich  $x, y, z \in A$ ; *prawostronnie rozdzielna*, gdy  $(y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x)$ , dla wszystkich  $x, y, z \in A$ ; *rozdzielna*, gdy jest ona lewo- i prawostronnie rozdzielna.

- Dodawanie i mnożenie liczb rzeczywistych są działaniami łącznymi i przemiennymi. Mnożenie jest rozdzielne względem dodawania, ale dodawanie nie jest rozdzielne względem mnożenia.
- Elementem neutralnym dodawania liczb rzeczywistych jest liczba 0, elementem neutralnym mnożenia liczb rzeczywistych jest liczba 1.
- Elementem odwrotnym dla liczby  $x$  względem dodawania liczb rzeczywistych jest liczba  $-x$ , elementem odwrotnym dla liczby  $x$  różnej od 0 względem mnożenia liczb rzeczywistych jest liczba  $\frac{1}{x}$ .
- Operacje sumy oraz iloczynu zbiorów są działaniami łącznymi i przemiennymi. Suma jest rozdzielna względem iloczynu, iloczyn jest rozdzielny względem sumy.
- Operacja brania średniej arytmetycznej (powiedzmy dwóch liczb rzeczywistych) jest przemienna, ale nie jest łączna.
- Operacja dzielenia (powiedzmy, liczb rzeczywistych) jest prawostronnie rozdzielna względem dodawania, ale nie jest lewostronnie rozdzielna względem dodawania.



- Niech  $\mathbf{A}_1 = (A_1, \{r_i^1 : i \in I\})$  oraz  $\mathbf{A}_2 = (A_2, \{r_i^2 : i \in I\})$  będą strukturami relacyjnymi (czystymi) tego samego typu.
- Mówimy, że  $\mathbf{A}_1 = (A_1, \{r_i^1 : i \in I\})$  jest *podstrukturą*  $\mathbf{A}_2 = (A_2, \{r_i^2 : i \in I\})$ , gdy  $A_1 \subseteq A_2$  oraz dla każdego  $i \in I$  zachodzi:  $r_i^1 = r_i^2 \cap A_1^{n_i}$ , gdzie  $n_i$  jest liczbą argumentów relacji  $r_i^1$  (a także, oczywiście, relacji  $r_i^2$ ).
- Jeśli  $\mathbf{A}_1$  jest podstrukturą  $\mathbf{A}_2$ , to piszemy  $\mathbf{A}_1 \subseteq \mathbf{A}_2$ .

- Niech  $\mathbf{A}_1 = (A_1, \{f_j^1 : j \in J\})$  oraz  $\mathbf{A}_2 = (A_2, \{f_j^2 : j \in J\})$  będą algebraami tego samego typu.
- Mówimy, że  $\mathbf{A}_1$  jest *podalgebrą*  $\mathbf{A}_2$ , gdy  $A_1 \subseteq A_2$  oraz  $A_1$  jest *domknięty na wszystkie operacje*  $f_j$ , czyli gdy dla wszystkich  $x_1, \dots, x_n \in A_1$  oraz wszystkich  $n$ -argumentowych operacji  $f_j$ , mamy:  $f_j(x_1, \dots, x_n) \in A_1$ .

# Przykłady

- Dodawanie i mnożenie liczb naturalnych daje w wyniku liczby naturalne. Tak więc, strukturę  $(\mathbb{N}, +, \cdot)$  uważać możemy za podstrukturę (podalgebrę) struktury  $(\mathbb{R}, +, \cdot)$  liczb rzeczywistych z ich dodawaniem oraz mnożeniem.
- Podobnie, strukturę uporządkowaną  $(\mathbb{N}, \leq)$  traktować możemy jako podstrukturę struktury  $(\mathbb{R}, \leq)$ .
- Rozważmy zbiór wszystkich *symetrii* trójkąta równobocznego. Ma on sześć elementów: przekształcenie identyfikacyjne (obrót o  $0^\circ$ ), obrót o  $120^\circ$ , obrót o  $240^\circ$  (oba względem środka trójkąta) oraz trzy symetrie względem prostych zawierających wysokości tego trójkąta. Operacją na tym zbiorze jest składanie przekształceń. Podstrukturą tej struktury jest zbiór złożony z przekształcenia identyfikacyjnego oraz obu wspomnianych obrotów, z operacją składania przekształceń.

Niech  $\mathbf{A}_1 = (A_1, \{r_i^1 : i \in I\}, \{f_j^1 : j \in J\})$  oraz  $\mathbf{A}_2 = (A_2, \{r_i^2 : i \in I\}, \{f_j^2 : j \in J\})$  będą strukturami tego samego typu. Mówimy, że odwzorowanie  $f : A_1 \rightarrow A_2$  jest *homomorfizmem*  $\mathbf{A}_1$  w  $\mathbf{A}_2$ , gdy dla wszystkich  $x_1, \dots, x_n \in A_1$  oraz wszystkich  $n$  argumentowych relacji  $r_i^1$  oraz  $r_i^2$  i wszystkich  $n$ -argumentowych funkcji  $f_j^1$  oraz  $f_j^2$ :

- 1  $f(f_j^1(x_1, \dots, x_n)) = f_j^2(f(x_1), \dots, f(x_n))$
- 2 jeśli zachodzi  $r_i^1(x_1, \dots, x_n)$ , to zachodzi  $r_i^2(f(x_1), \dots, f(x_n))$ .

- Jeśli  $f$  jest bijekcją,  $f$  jest homomorfizmem z  $\mathbf{A}_1$  w  $\mathbf{A}_2$  oraz  $f^{-1}$  jest homomorfizmem z  $\mathbf{A}_2$  w  $\mathbf{A}_1$ , to  $f$  nazywamy *izomorfizmem*  $\mathbf{A}_1$  oraz  $\mathbf{A}_2$ .
- Mówimy, że struktury  $\mathbf{A}$  oraz  $\mathbf{B}$  są *izomorficzne*, gdy istnieje izomorfizm z  $\mathbf{A}$  na  $\mathbf{B}$ . Jeśli  $\mathbf{A}$  oraz  $\mathbf{B}$  są izomorficzne, to piszemy  $\mathbf{A} \cong \mathbf{B}$ .

# Przykłady

- Na poprzednim wykładzie pokazaliśmy, że rodzina wszystkich podzbiorów zbioru  $\{1, 2, 3\}$  uporządkowana częściowo przez inkluzję jest izomorficzna ze zbiorem liczb  $\{1, 2, 3, 5, 6, 10, 15, 30\}$  uporządkowanym częściowo przez relację podzielności. Izomorfizm ten to bijekcja  $f : \wp(\{1, 2, 3\}) \rightarrow \{1, 2, 3, 5, 6, 10, 15, 30\}$  określona warunkami:  $f(\emptyset) = 1$ ,  $f(\{1\}) = 2$ ,  $f(\{2\}) = 3$ ,  $f(\{3\}) = 5$ ,  $f(\{1, 2\}) = 6$ ,  $f(\{1, 3\}) = 10$ ,  $f(\{2, 3\}) = 15$ ,  $f(\{1, 2, 3\}) = 30$ .
- Funkcja logarytmiczna  $\log : \mathbb{R}_+ \rightarrow \mathbb{R}$  jest homomorfizmem struktury  $(\mathbb{R}_+, \cdot)$  w strukturę  $(\mathbb{R}, +)$ . Słuchacze pamiętają ze szkoły, że logarytm z iloczynu równy jest sumie logarytmów:  
$$\log(x \cdot y) = \log x + \log y.$$
- Funkcja identycznościowa  $f(x) = x$  jest homomorfizmem  $(\mathbb{N}, <, +, \cdot)$  w  $(\mathbb{R}, <, +, \cdot)$ . Struktury  $(\mathbb{N}, <, +, \cdot)$  oraz  $(\mathbb{R}, <, +, \cdot)$  nie są jednak izomorficzne. Dlaczego?

Niech  $\mathbf{A} = (A, \{r_i : i \in I\}, \{f_j : j \in J\})$  będzie strukturą, a  $E$  relacją równoważności na zbiorze  $A$ . Mówimy, że  $E$  jest *kongruencją* w strukturze  $\mathbf{A}$ , gdy dla wszystkich  $x_1, \dots, x_n$ , wszystkich  $y_1, \dots, y_n$ , wszystkich  $n$ -argumentowych relacji  $r_i$  oraz wszystkich  $n$ -argumentowych funkcji  $f_j$ :

- 1 jeśli  $x_1 E y_1, \dots, x_n E y_n$ , to  $r_i(x_1, \dots, x_n)$  zachodzi wtedy i tylko wtedy, gdy zachodzi  $r_i(y_1, \dots, y_n)$
- 2 jeśli  $x_1 E y_1, \dots, x_n E y_n$ , to  $f_j(x_1, \dots, x_n) E f_j(y_1, \dots, y_n)$ .

- Najmniejszą (względem inkluzji) kongruencją w strukturze  $\mathbf{A}$  jest relacja identyczności na zbiorze  $dom(\mathbf{A})$ , a największą taką kongruencją jest relacja pełna w zbiorze  $dom(\mathbf{A})$ .

# Przykłady

- Na drugim wykładzie wspomnieliśmy o relacji równoważności  $\equiv_n$  określonej dla liczb całkowitych w sposób następujący:  $x \equiv_n y$  wtedy i tylko wtedy, gdy  $x$  oraz  $y$  mają takie same reszty z dzielenia przez  $n$ . Często używa się notacji:  $x \equiv y \pmod{n}$  i mówi, że liczba  $x$  *przystaje do liczby  $y$  modulo  $n$* . Ta relacja jest kongruencją w strukturze  $(\mathbb{Z}, +, \cdot)$  wszystkich liczb całkowitych z działaniami dodawania i mnożenia. Łatwo sprawdzić, że  $x \equiv_n y$  wtedy i tylko wtedy, gdy  $x - y$  jest podzielna bez reszty przez  $n$ . Szczególnie ważne są te relacje o postaci  $\equiv_p$ , gdzie  $p$  jest liczbą pierwszą.
- Relacja równoliczności zbiorów, określona w rodzinie wszystkich podzbiorów dowolnego zbioru  $X$  jest kongruencją struktury  $(\wp(X), \cup, \cap)$ .

Przypominamy, że jeśli  $E$  jest relacją równoważności na zbiorze  $A$ , to:

- ①  $[x]_E = \{y \in A : xEy\}$  (klasa abstrakcji elementu  $x$  względem relacji  $E$ )
- ②  $A/E = \{[x]_E : x \in A\}$  (zbiór ilorazowy zbioru  $A$  względem relacji  $E$ ).

Niech  $\mathbf{A} = (A, \{r_i : i \in I\}, \{f_j : j \in J\})$  będzie strukturą, a  $E$  kongruencją na zbiorze  $A$ . *Strukturę ilorazową*  $\mathbf{A}/E$  definiujemy w sposób następujący:

- ①  $\mathbf{A}/E = (A/E, \{r_i^E : i \in I\}, \{f_j^E : j \in J\})$
- ② dla każdej  $n$ -argumentowej relacji  $r_i$  definiujemy relację  $r_i^E$ :  
 $r_i^E([x_1]_E, \dots, [x_n]_E)$  wtedy i tylko wtedy, gdy  $r_i(x_1, \dots, x_n)$
- ③ dla każdej  $n$ -argumentowej funkcji  $f_j$  definiujemy funkcję  $f_j^E$ :  
 $f_j^E([x_1]_E, \dots, [x_n]_E) = [f_j(x_1, \dots, x_n)]_E$

Ponieważ  $E$  jest kongruencją na  $A$ , więc powyższa definicja jest poprawna (nie zależy od wyboru elementów z klas abstrakcji), co łatwo sprawdzić rachunkiem.

# Przykład

- W zbiorze  $\mathbb{Z}/\equiv_p$  wszystkich klas abstrakcji omówionej przed chwilą relacji równoważności  $\equiv_p$ , gdzie  $p$  jest liczbą pierwszą, wprowadzić możemy działania arytmetyczne, wykorzystując działania arytmetyczne w zbiorze  $\mathbb{Z}$ .
- Zauważmy, że  $\mathbb{Z}/\equiv_p$  liczy dokładnie  $p$  elementów. Jak już wspomniano, relacja  $\equiv_p$  jest kongruencją w strukturze  $(\mathbb{Z}, +, \cdot)$ .

Definiujemy:

$$[x]_{\equiv_p} \oplus_p [y]_{\equiv_p} = [x + y]_{\equiv_p}$$

$$[x]_{\equiv_p} \otimes_p [y]_{\equiv_p} = [x \cdot y]_{\equiv_p}$$

- Na początku tej prezentacji podaliśmy tabelki działań dla operacji  $\oplus_3$  oraz  $\otimes_3$  (czyli operacji dodawania i mnożenia modulo 3).



- Dotąd zakładaliśmy, że słuchacze dysponują intuicyjną wiedzą na temat liczb: naturalnych, całkowitych, wymiernych, rzeczywistych.
  - W matematyce wprowadza się te rodzaje liczb (oraz wiele innych) bądź na drodze aksjomatycznej bądź poprzez konstrukcję pewnych rodzajów liczb, gdy inne są już określone.
- 
- Systemy liczbowe są strukturami: składają się z uniwersum obiektów, na których wykonujemy pewne operacje.
  - We współczesnej algebrze bada się nie tylko systemy liczbowe, ale także bardzo ogólne struktury różnych rodzajów, np.: grupy, pierścienie, ciała, przestrzenie wektorowe, itd.
  - Studentów kognitywistyki UAM interesować mogą różne problemy dotyczące np. przyswajania pojęcia liczby naturalnej przez umysł w jego rozwoju, uzyskiwanie w tym rozwoju zdolności numerycznych, itp. Problematyka ta wykracza jednak poza nasz usługowy kurs matematyki.

Przez *algebrę Peana* rozumiemy każdą algebrę  $\mathbf{A} = (A, f, a)$  taką, że:

- 1  $a \in A$  (element początkowy algebry)
- 2  $f : A \rightarrow A$  (funkcja następnika)
- 3  $a \notin \text{rng}(f)$
- 4  $f$  jest funkcją różnowartościową
- 5 Dla dowolnego zbioru  $X \subset A$ , jeśli  $a \in X$  oraz  $f(x) \in X$ , o ile  $x \in X$ , dla wszystkich  $x \in X$ , to  $X = A$ .

- Istnieje dokładnie jedna algebra Peana (z dokładnością do izomorfizmu). Jej uniwersum  $\mathbb{N}$  to zbiór wszystkich liczb *naturalnych*.
- Istnieje dokładnie jedna funkcja dwuargumentowa  $+$  :  $\mathbb{N}^2 \rightarrow \mathbb{N}$ , która spełnia warunki:  $x + 0 = x$ ,  $x + (y + 1) = (x + y) + 1$ .
- Istnieje też dokładnie jedna funkcja dwuargumentowa  $\cdot$  :  $\mathbb{N}^2 \rightarrow \mathbb{N}$ , która spełnia warunki:  $x \cdot 0 = 0$ ,  $x \cdot (y + 1) = (x \cdot y) + x$ .

- Określamy relację  $\approx_1 \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$ :  $(x, y) \approx_1 (u, v)$  wtedy i tylko wtedy, gdy  $x + v = u + y$ .
- Jest to relacja równoważności na zbiorze  $\mathbb{N} \times \mathbb{N}$ , co nietrudno sprawdzić, wykonując proste rachunki.
- *Definiujemy* zbiór wszystkich liczb *całkowitych*:  $\mathbb{Z} = \mathbb{N}^2 / \approx_1$ .
- Odwzorowanie  $\varphi_1 : \mathbb{N} \rightarrow \mathbb{Z}$  określone wzorem  $\varphi_1(k) = [(k, 0)]_{\approx_1}$  jest iniekcją.

Trzeba jeszcze określić działania arytmetyczne na liczbach całkowitych, ich *dodawanie*  $\oplus_1$ , ich *odejmowanie*  $\ominus_1$  oraz *mnożenie*  $\odot_1$ ; określimy też ich uporządkowanie  $\leq_1$ :

- $[(x, y)]_{\approx_1} \oplus_1 [(u, v)]_{\approx_1} = [x + u, y + v]_{\approx_1}$
- $[(x, y)]_{\approx_1} \ominus_1 [(u, v)]_{\approx_1} = [x + v, y + u]_{\approx_1}$
- $[(x, y)]_{\approx_1} \odot_1 [(u, v)]_{\approx_1} = [x \cdot u + y \cdot v, u \cdot y + x \cdot v]_{\approx_1}$
- $[(x, y)]_{\approx_1} \leq_1 [(u, v)]_{\approx_1}$ , jeśli  $x + v \leq y + u$ .

Wreszcie, trzeba pokazać, że:

- 1 te definicje są *poprawne* (wynik działania nie zależy od wyboru elementu z klasy abstrakcji)
- 2  $\oplus_1$  i  $\odot_1$  „rozszerzają”  $+$  i  $\cdot$  ze zbioru  $\mathbb{N}$  na zbiór  $\mathbb{Z}$ :
  - 1  $\varphi_1(m) \oplus_1 \varphi_1(n) = \varphi_1(m + n)$
  - 2  $\varphi_1(m) \odot_1 \varphi_1(n) = \varphi_1(m \cdot n)$

- Struktura  $(\{[(x, 0)]_{\approx_1} : x \in \mathbb{N}\}, \leq_1, \oplus_1, \odot_1)$ , która sama jest podstrukturą struktury  $(\mathbb{Z}, \leq_1, \oplus_1, \odot_1)$  jest izomorficzna ze strukturą  $(\mathbb{N}, \leq, +, \cdot)$ . Są to *nieujemne* liczby całkowite.
- Fakt ten skłania do pewnych uproszczeń w notacji liczb całkowitych:
  - 1 zamiast  $[(x, 0)]_{\approx_1}$  piszemy po prostu  $x$
  - 2 zamiast  $[(0, x)]_{\approx_1}$  piszemy po prostu  $-x$
  - 3 przyjmując powyższe uproszczenia, możemy napisać:  
 $\mathbb{Z} = \mathbb{N} \cup \{-x : x \in \mathbb{N}\}$ , co jest bliskie praktyce szkolnej.

- Określamy relację równoważności  $\approx_2 \subseteq (\mathbb{Z} \times (\mathbb{Z} - \{0\})) \times (\mathbb{Z} \times (\mathbb{Z} - \{0\}))$  wzorem:  $(x, y) \approx_2 (u, v)$  wtedy i tylko wtedy, gdy  $x \odot_1 v = y \odot_1 u$ .
- Definiujemy zbiór wszystkich liczb wymiernych:  $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} - \{0\})) / \approx_2$  oraz działania arytmetyczne na liczbach wymiernych,  $\oplus_2$  (dodawanie),  $\ominus_2$  (odejmowanie),  $\odot_2$  (mnożenie),  $\oslash_2$  (dzielenie) a także porządek  $\leq_2$ :

- $[(x, y)]_{\approx_2} \oplus_2 [(u, v)]_{\approx_2} = [((x \odot_1 v) \oplus_1 (y \odot_1 u), (y \odot_1 v))]_{\approx_2}$
- $[(x, y)]_{\approx_2} \ominus_2 [(u, v)]_{\approx_2} = [((x \odot_1 v) \ominus_1 (y \odot_1 u), (y \odot_1 v))]_{\approx_2}$
- $[(x, y)]_{\approx_2} \odot_2 [(u, v)]_{\approx_2} = [(x \cdot_1 u, y \cdot_1 v)]_{\approx_2}$
- $[(x, y)]_{\approx_2} \oslash_2 [(u, v)]_{\approx_2} = [x \cdot_1 v, y \cdot_1 u]_{\approx_2}$ , o ile  $[(u, v)]_{\approx_2} \neq [(0, 1)]_{\approx_2}$
- $[(x, y)]_{\approx_2} \leq_2 [(u, v)]_{\approx_2}$ , jeśli  $x \cdot_1 v \leq_1 y \cdot_1 u$ , gdzie  $0 <_1 y, 0 <_1 v$ .

Trzeba pokazać, że te definicje są *poprawne* (wynik działania nie zależy od wyboru elementu z klasy abstrakcji).

Trzeba też pokazać, że odwzorowanie  $\varphi_2 : \mathbb{Z} \rightarrow \mathbb{Q}$  określone wzorem  $\varphi_2(x) = [(x, 1)]_{\approx_2}$  jest iniekcją, oraz zachowuje działania i porządek, czyli że zachodzą warunki:

- $\varphi_2(x) \oplus_2 \varphi_2(y) = \varphi_2(x \oplus_1 y)$
- $\varphi_2(x) \odot_2 \varphi_2(y) = \varphi_2(x \odot_1 y)$
- jeśli  $x \leq_1 y$ , to  $\varphi_2(x) \leq_2 \varphi_2(y)$ .

- Dla każdej liczby wymiernej  $[(x, y)]_{\approx_2}$  mamy:  
 $[(x, y)]_{\approx_2} = [(x, 1)]_{\approx_2} \odot_2 [(y, 1)]_{\approx_2}$ . Liczbę wymierną  $[(x, 1)]_{\approx_2}$ , na mocy Tradycji (oraz faktu, że  $\varphi_2$  jest izomorfizmem struktur  $(\mathbb{Z}, \leq_1, \oplus_1, \odot_1)$  oraz  $(\{[(x, 1)]_{\approx_2} : x \in \mathbb{Z}\}, \leq_2, \oplus_2, \odot_2)$ ) zwykle utożsamiamy z liczbą całkowitą  $x$ .
- Na mocy powyższych ustaleń, możemy zapisywać liczbę wymierną  $[(x, y)]_{\approx_2}$  w znany ze szkoły sposób, jako *ułamek*  $\frac{a}{b}$ . Przy takich oznaczeniach mamy zatem:  $\mathbb{Q} = \{\frac{a}{b} : a \in \mathbb{Z} \text{ oraz } b \in \mathbb{Z} - \{0\}\}$  do którego to zapisu przyzwyczajała nas szkoła.

Przekrojem Dedekinda nazywamy każdą parę  $(A, B)$  niepustych podzbiorów zbioru ostro liniowo uporządkowanego  $(X, <)$  taką, że:  $A \cup B = X$ ,  $a < b$  dla wszystkich  $a \in A$  oraz  $b \in B$ .  $A$  jest klasą *dolną*, a  $B$  klasą *górną* przekroju  $(A, B)$ . W przypadku dowolnego zbioru liniowo uporządkowanego przekrój Dedekinda  $(A, B)$  może być jednej z następujących postaci:

- W zbiorze  $A$  istnieje element największy i w zbiorze  $B$  istnieje element najmniejszy. Mówimy wtedy, że przekrój  $(A, B)$  wyznacza *skok* (w rozważanym porządku).
- W zbiorze  $A$  istnieje element największy i w zbiorze  $B$  nie istnieje element najmniejszy.
- W zbiorze  $A$  nie istnieje element największy i w zbiorze  $B$  istnieje element najmniejszy.
- W zbiorze  $A$  nie istnieje element największy i w zbiorze  $B$  nie istnieje element najmniejszy. Mówimy wtedy, że przekrój  $(A, B)$  wyznacza *lukę* (w rozważanym porządku).

# Definicja Dedekinda liczb rzeczywistych

Liczbą rzeczywistą (w sensie Dedekinda) nazywamy dowolny podzbiór  $A$  zbioru  $\mathbb{Q}$  wszystkich liczb wymiernihych taki, że:

- 1  $A \neq \emptyset$ ,  $A \neq \mathbb{Q}$
- 2 Dla wszystkich  $a, b \in \mathbb{Q}$ : jeśli  $a \in A$  oraz  $b < a$ , to  $b \in \mathbb{Q}$
- 3 W zbiorze  $A$  nie istnieje element największy (w sensie zwykłego porządku  $<$  liczb wymiernihych).

Niech  $\mathbb{R}$  będzie zbiorem tak zdefiniowanych liczb rzeczywistych.

Definiujemy dla  $A, B \in \mathbb{R}$ :  $A \leq_D B$  wtedy i tylko wtedy, gdy  $A \subseteq B$ .

Wtedy oczywiście  $A <_D B$  dokładnie wtedy, gdy  $A \subset B$ .

Każda liczba wymierna  $x$  wyznacza liczbę rzeczywistą

$O(x) = \{y \in \mathbb{Q} : y < x\}$ . Niech  $\mathbb{Q}^\circ = \{O(x) : x \in \mathbb{Q}\}$ . Wtedy  $\mathbb{Q}^\circ$  jest

izomorficzną (względem porządku) kopią  $\mathbb{Q}$ , co łatwo sprawdzić rachunkiem.



# Liczby niewymierne

- Istnieją jednak liczby rzeczywiste, które nie są wyznaczone przez liczby wymierne: odpowiadają one przekrojom Dedekinda wyznaczającym luki w rozważanym porządku liczb wymiernych. Taką liczbą rzeczywistą jest np.:

$$\{x \in \mathbb{Q} : x < 0 \text{ lub } (0 \leq x \text{ oraz } x^2 < 2)\}.$$

- Liczby rzeczywiste, które są elementami zbioru  $\mathbb{R} - \mathbb{Q}^o$  nazywamy *liczbami niewymiernymi*.
- Powyższe definicje bazują na własnościach porządkowych zbioru wszystkich liczb wymiernych.
- W jaki sposób uporządkowane są liczby rzeczywiste?

**Twierdzenie.** Zbiór  $\mathbb{R}$  jest uporządkowany w sposób ciągły przez relację  $\leq_D$ . Ponadto, zbiór  $\mathbb{Q}^\circ$  jest gęsty w  $\mathbb{R}$ , czyli dla każdych  $x, y \in \mathbb{R}$ , jeśli  $x <_D y$ , to istnieje  $z \in \mathbb{Q}^\circ$  taki, że  $x <_D z$  oraz  $z <_D y$ . **Szkic Dowodu:** Porządek  $\leq_D$  jest liniowy. Ten fakt wynika z tego, że każda liczba rzeczywista to odcinek początkowy liniowo uporządkowanego zbioru  $\mathbb{Q}$ . Zbiór  $\mathbb{Q}^\circ$  jest gęsty w  $\mathbb{R}$ . To wynika z nietrudnego rachunku, uwzględniającego fakt, że liczby rzeczywiste zdefiniowaliśmy jako odcinki początkowe nie mające elementu największego.

W  $\mathbb{R}$  nie ma elementu największego i elementu najmniejszego. To wynika z faktu, że dla dowolnej liczby rzeczywistej  $A$  mamy  $O(x) <_D A <_D O(y)$ , gdzie  $x \in A$  oraz  $y \in \mathbb{Q} - A$  (przy czym  $y$  nie jest elementem najmniejszym w  $\mathbb{Q} - A$ ).

Porządek  $\leq_D$  jest ciągły. Dla dowodu tego faktu rozważyć trzeba dowolny niepusty podzbiór  $S \subseteq \mathbb{R}$ , który jest ograniczony z góry, powiedzmy przez  $A_0 \in \mathbb{R}$ , czyli taki, że  $A \subseteq A_0$  dla wszystkich  $A \in S$ . Niezbyt trudnym rachunkiem sprawdzić można, że wtedy  $\bigcup S$  jest kresem górnym zbioru  $S$ , czyli że  $\bigcup S = \sup S$ .

W zbiorze  $\mathbb{R}$  wprowadzamy działania arytmetyczne w następujący sposób:

*Suma.* Jeśli  $a, b \in \mathbb{R}$ , to niech:  $a \oplus_D b = \{x \oplus_2 y : x \in a \text{ oraz } y \in b\}$ .

*Liczba przeciwna.* Jeśli  $a \in \mathbb{R}$ , to niech:

- 1  $-_D a = O(-x)$ , o ile  $a = O(x)$
- 2  $-_D a = \{-x : x \notin a\}$ , o ile  $a \notin \mathbb{Q}^0$ .

*Iloczyn.* Dla  $a, b \in \mathbb{R}$  definiujemy ich iloczyn  $a \odot_D b$  następująco:

- 1 Jeśli  $a >_D O(0)$  oraz  $b >_D O(0)$ , to niech:  
 $a \odot_D b = \{x \odot_2 y : x > 0, y > 0, x \in a, y \in b\} \cup \{x \in \mathbb{Q} : x \leq 0\}$ .
- 2 Jeśli  $a = O(0)$  lub  $b = O(0)$ , to  $a \odot_D b = O(0)$ .
- 3 Jeśli  $a <_D O(0)$  oraz  $b <_D O(0)$ , to  $a \odot_D b = (-_D a) \odot_D (-_D b)$
- 4 Jeśli  $a <_D O(0)$  oraz  $b >_D O(0)$ , to  $a \odot_D b = -_D((-_D a) \odot_D b)$
- 5 Jeśli  $a >_D O(0)$  oraz  $b <_D O(0)$ , to  $a \odot_D b = -_D(a \odot_D (-_D b))$ .

Struktury:  $(\mathbb{Q}^o, \oplus_D, \odot_D, O(0), O(1))$  oraz  $(\mathbb{Q}, \oplus_2, \odot_2, 0, 1)$  są izomorficzne.

# Definicja Cantora

- Niech  $\text{SEQ}$  będzie zbiorem wszystkich *ciągów podstawowych liczb wymiernych*, tj. zbiorem:
 
$$\left\{ f : \mathbb{N} \rightarrow \mathbb{Q} \text{ oraz dla każdej } k \in \mathbb{N} \text{ istnieje } m_0 \in \mathbb{N} \text{ taka,} \right.$$

$$\left. \text{ że dla wszystkich } m, n > m_0 \text{ zachodzi } |f(n) - f(m)| < \frac{1}{k+1} \right\}.$$
- Na zbiorze  $\text{SEQ}$  określamy relację  $\approx_3$  wzorem:
 
$$f \approx_3 g \text{ wtedy i tylko wtedy, gdy dla każdej } k \in \mathbb{N} \text{ istnieje } m_0 \in \mathbb{N} \text{ taka,} \\ \text{ że dla wszystkich } n > m_0 \text{ zachodzi: } |f(n) - g(n)| < \frac{1}{k+1}.$$
- Wtedy  $\approx_3$  jest relacją równoważności na  $\text{SEQ}$ , co nietrudno sprawdzić rachunkiem. *Definiujemy* zbiór wszystkich liczb rzeczywistych (w sensie Cantora):  $\mathbb{R} = \text{SEQ} / \approx_3$ .
- Funkcja  $\varphi_3 : \mathbb{Q} \rightarrow \mathbb{R}$  zdefiniowana wzorem  $\varphi_3(q) = [c_q]_{\approx_3}$  (gdzie  $c_q$  jest ciągiem stale równym  $q$ ) jest iniekcją.

Definiujemy działania arytmetyczne w  $\mathbb{R}$ :

$$\textcircled{1} [f]_{\approx_3} \oplus_3 [g]_{\approx_3} = [f \uplus g]_{\approx_3} \quad (\text{dodawanie})$$

$$\textcircled{2} [f]_{\approx_3} \odot_3 [g]_{\approx_3} = [f \otimes g]_{\approx_3} \quad (\text{mnożenie})$$

gdzie dodawanie  $\uplus$  i mnożenie  $\otimes$  *funkcji* (ze zbioru  $\mathbb{N}$  w zbiór  $\mathbb{Q}$ ) rozumiane jest następująco:

$$\textcircled{1} (f \uplus g)(n) = f(n) \oplus_2 g(n), \text{ dla } n \in \mathbb{N}$$

$$\textcircled{2} (f \otimes g)(n) = f(n) \odot_2 g(n), \text{ dla } n \in \mathbb{N}.$$

Można udowodnić, że wszystkie te definicje są poprawne i że adekwatnie określają działania arytmetyczne w  $\mathbb{R}$ .

Określona wyżej relacja równoważności między ciągami podstawowymi każe utożsamiać ze sobą ciągi, których odpowiednie wyrazy, począwszy od pewnego miejsca, stają się *dowolnie bliskie* sobie.

W dalszych wykładach to właśnie pojęcie: *być dowolnie blisko* będzie odgrywało bardzo istotną rolę.

W ujęciu algebraicznym, przez *kratę* rozumiemy strukturę  $(X, \sqcup, \sqcap)$  taką, że  $X \neq \emptyset$ , zaś  $\sqcup$  oraz  $\sqcap$  są dwuargumentowymi operacjami w  $X$ , spełniającymi następujące warunki dla dowolnych  $x, y, z \in X$ :

- 1 operacje  $\sqcup$  oraz  $\sqcap$  są łączne i przemienne;
- 2  $\sqcup(\sqcap(x, y), y) = y$
- 3  $\sqcap(\sqcup(x, y), y) = y$

Jeśli  $(X, \sqcup, \sqcap)$  jest kratą, to dla dowolnych  $x, y \in X$  zachodzi równoważność:  $\sqcap(x, y) = x$  wtedy i tylko wtedy, gdy  $\sqcup(x, y) = y$ . Wykorzystując ten fakt, można w kracie  $(X, \sqcup, \sqcap)$  zdefiniować relację porządku częściowego poprzez operacje algebraiczne:  $x \sqsubseteq y$  wtedy i tylko wtedy, gdy  $\sqcup(x, y) = y$ . Kresy w tym porządku wyznaczone są przez operacje w kracie:  $\inf\{x, y\} = \sqcap(x, y)$ ,  $\sup\{x, y\} = \sqcup(x, y)$ . Słuchacze domyślają się już, że także wychodząc od definicji kraty w terminach porządku częściowego (poprzedni wykład) możemy zdefiniować operacje algebraiczne  $\sqcup$  oraz  $\sqcap$ , otrzymując kratę w sensie algebraicznym.

Jeśli każda z operacji  $\sqcup$  oraz  $\sqcap$  jest rozdzielna względem pozostałej, to mówimy, że krata jest *dystrybutywna*.

Przez *algebrę Boole'a* rozumiemy strukturę  $(X, \sqcup, \sqcap, \ominus, \mathbf{0}, \mathbf{1})$  taką, że:

- ①  $(X, \sqcup, \sqcap)$  jest kratą dystrybutywną;
- ②  $\ominus$  jest operacją jednoargumentową w  $X$  (operacją uzupełnienia), zaś  $\mathbf{0}$  oraz  $\mathbf{1}$  są elementami zbioru  $X$  (odpowiednio: zero i jedynka algebry);
- ③ dla dowolnego elementu  $x \in X$  zachodzą równości:

$$\sqcup(x, \ominus(x)) = \mathbf{1} \quad \sqcap(x, \ominus(x)) = \mathbf{0}.$$

Ze względu na pewne nawyki, zwykle stosujemy notację *infiksową* (symbol funkcji między symbolami argumentów) dla operacji w kratkach, a więc piszemy:

- ①  $x \sqcup y$  zamiast  $\sqcup(x, y)$
- ②  $x \sqcap y$  zamiast  $\sqcap(x, y)$
- ③ w algebrach Boole'a dodatkowo:  $-x$  (albo np.  $x'$ ) zamiast  $\ominus(x)$ .

- W zbiorze  $\mathbb{N}_+$  możemy określić strukturę kratową, definiując dla dowolnych  $x, y \in \mathbb{N}_+$ :  
 $\sqcup(x, y) =$  najmniejsza wspólna wielokrotność  $x$  oraz  $y$   
 $\sqcap(x, y) =$  największy wspólny dzielnik  $x$  oraz  $y$ .
- Zbiór potęgowy  $\wp(X)$  dowolnego zbioru  $X$  jest algebrą Boole'a (a więc także kratą): zerem algebry jest zbiór pusty  $\emptyset$ , jej jedyneką jest zbiór  $X$ , a operacjami  $\sqcup$  oraz  $\sqcap$  są, odpowiednio, operacje sumy i iloczynu zbiorów. Uzupełnieniem elementu  $Y \subseteq X$  tej algebry jest dopełnienie  $Y' = X - Y$ .
- W dwuelementowym zbiorze  $\{0, 1\}$  wartości logicznych określamy strukturę algebry Boole'a, definiując:  
 $\sqcup(x, y) = 0$  wtedy i tylko wtedy, gdy  $x = y = 0$   
 $\sqcap(x, y) = 1$  wtedy i tylko wtedy, gdy  $x = y = 1$   
 $\ominus(0) = 1, \ominus(1) = 0$ .  
Te operacje to *funkcje prawdziwościowe*, odpowiadające, kolejno: alternatywie nierozłącznej, koniunkcji oraz negacji.



# Myśl przekornie!

- Wszyscy znamy różnego rodzaju *parkietaże*: pokrycia płaszczyzny wielokątami – np. trójkątami równobocznymi, kwadratami, sześciobokami foremnymi. Znamy też różnego rodzaju *mozaiki* pokrywające płaszczyznę. Można zastanawiać się, jakie w ogólności są możliwości pokrycia płaszczyzny wielokątami, być może różnych rodzajów. Czy możliwe jest nieokresowe pokrycie płaszczyzny za pomocą wielokątów np. dwóch rodzajów?
- Składanie obrotów na płaszczyźnie jest przemienne. Czy przemienne jest składanie obrotów w przestrzeni trójwymiarowej?
- Zakresy pojęć są zbiorami, a więc można na nich wykonywać operacje boolowskie. Jaką strukturę tworzy zestaw wszystkich zakresów pojęć *rzeczywiście* używanych w danym języku?

# Co musisz ZZZ

- Struktura relacyjna, algebra, podstruktura.
- Homomorfizm, izomorfizm.
- Kongruencja.
- Struktura ilorazowa.
- System liczb rzeczywistych: definicja Dedekinda i definicja Cantora.
- Kraty i algebry Boole'a.