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 są zarówno w strukturę porządkową, jak też w strukturę wyznaczoną przez *działania arytmetyczne* na liczbach.
- 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.

- Strukturą relacyjną nazywamy dowolny układ $\mathbf{A} = (A, R_1, \ldots, R_n, f_1, \ldots, f_m, a_1, \ldots, a_k)$, gdzie:
  - A jest zbiorem, nazywanym *uniwersum* (lub *dziedziną*) struktury $\mathbf{A}$,
  - $R_1, \ldots, R_n$ są relacjami na zbiorze A (każda z tych relacji ma określoną liczbę argumentów);
  - $f_1, \ldots, f_m$ są funkcjami o wartościach w zbiorze A (każda z tych funkcji ma określoną liczbę argumentów);
  - $a_1, \ldots, a_k$ są elementami wyróżnionymi w zbiorze A.
- Struktury postaci $\mathbf{A} = (A, f_1, \ldots, f_m, a_1, \ldots, a_k)$ nazywamy *algebrami*.

- Najczęściej rozważamy funkcje (operacje, działania) jedno- lub dwuargumentowe. Jeśli np. $\oplus : A \times A \to A$ jest operacją dwuargumentową, to wartość $\oplus(x, y)$ będziemy często zapisywali w postaci *infiksowej* $x \oplus y$. Podobnie, np. dla operacji jednoargumentowej $\ominus : A \to A$ w miejsce $\ominus(x)$ będziemy często pisali $\ominus x$.

- Jeśli A ma n elementów, to na zbiorze A można określić n^{n^2} operacji dwuargumentowych. Można zatem określić $2^{2^2} = 16$ operacji dwuargumentowych na zbiorze dwuelementowym oraz $3^{3^2} = 19683$ operacji dwuargumentowych na zbiorze trójelementowym.

- Niech np. $A = \{0, 1, 2\}$, $\oplus_3 : A \times A \to A$, $\otimes_3 : A \times A \to A$, gdzie:
  - $x \oplus_3 y =$ reszta z dzielenia $x + y$ przez 3
  - $x \otimes_3 =$ reszta z dzielenia $x \cdot y$ przez 3

$\oplus_3$	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

Ćwiczenie: rozszerz powyższe operacje na cały zbiór $\mathbb{N}$.

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 *łączne*, 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 $x \circ y = y \circ x = e$, gdzie e jest elementem neutralnym działania $\circ$.

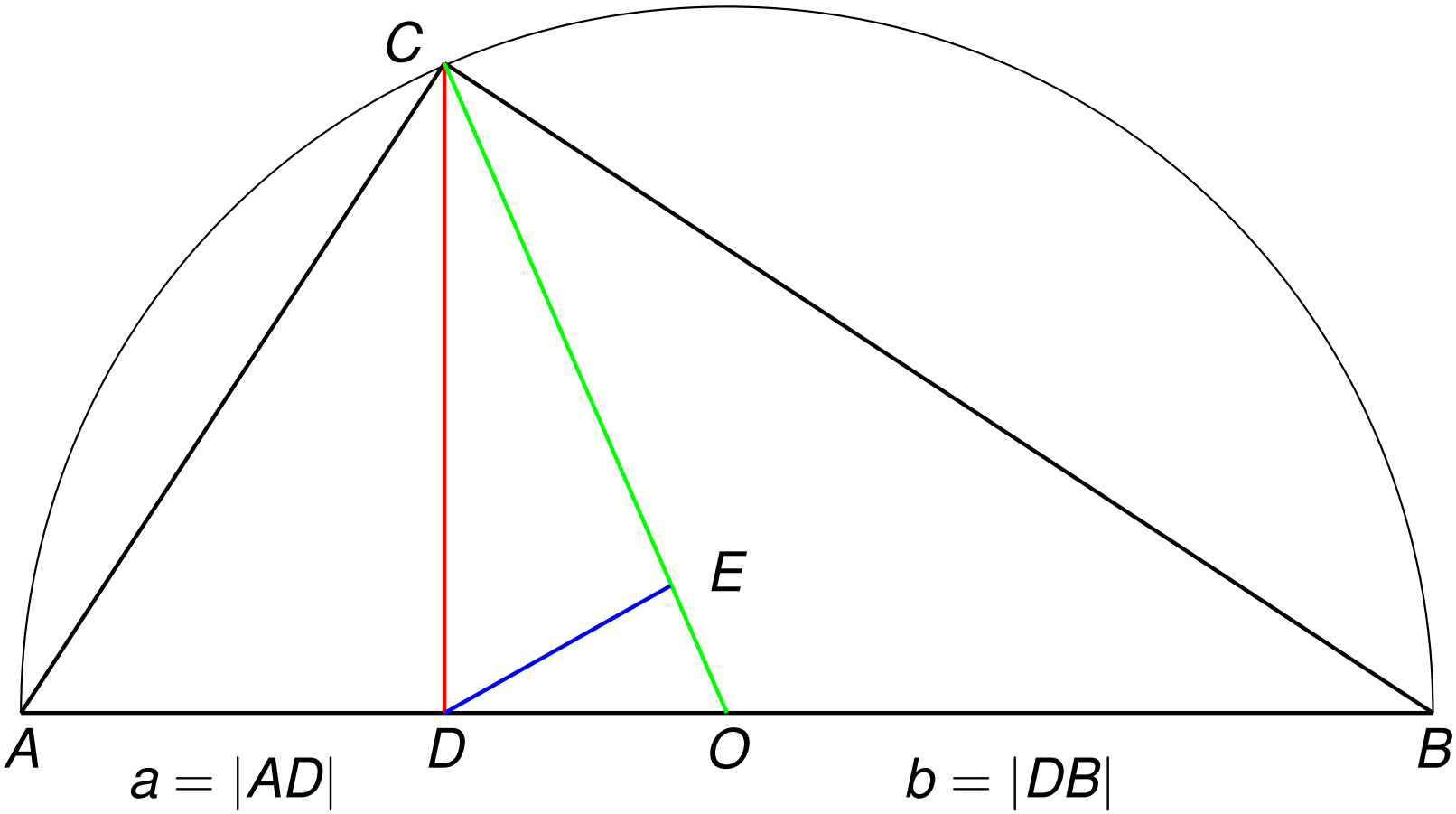
Niech $(A, \oplus, \otimes)$ będzie algebrą z dwiema operacjami dwuargumentowymi. Powiemy, że operacja $\otimes$ jest względem operacji $\oplus$: *lewostronnie rozdzielna*, gdy $x \otimes (y \oplus z) = (x \otimes y) \oplus (y \otimes z)$, dla wszystkich $x, y, z \in A$; *prawostronnie rozdzielna*, gdy $(y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x)$, 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 0, elementem neutralnym mnożenia liczb rzeczywistych jest 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 dwóch liczb rzeczywistych jest przemienna, ale nie jest łączna.
- Operacja dzielenia liczb rzeczywistych jest prawostronnie rozdzielna względem dodawania, ale nie jest lewostronnie rozdzielna względem dodawania.

Dla dowolnych $a > 0$, $b > 0$ mamy $\frac{2ab}{a+b} \leqslant \frac{a+b}{2}$.

- Dowód algebraiczny:
  - $(a-b)^2 \geqslant 0$ dla wszystkich a, b (w szczególności dla $a > 0$, $b > 0$)
  - $a^2 - 2ab + b^2 \geqslant 0$
  - $a^2 - 2ab + b^2 + 4ab \geqslant 4ab$
  - $a^2 + 2ab + b^2 \geqslant 4ab$
  - $(a+b)^2 \geqslant 4ab$
  - $\frac{1}{2}(a+b)^2 \geqslant 2ab$
  - $\frac{a+b}{2} \geqslant \frac{2ab}{a+b}$
- Zauważmy jeszcze, że $\frac{2ab}{a+b} = \frac{2}{\frac{1}{a}+\frac{1}{b}}$.

- Pokażemy jeszcze interpretację geometryczną średnich: arytmetycznej, geometrycznej i harmonicznej.



- Rozważmy wielkości a, b, dla których $a = |AD|$, $b = |DB|$, a więc $a + b = |AB|$.
- Kreślimy półokrąg, którego środek O znajduje się w połowie odcinka AB.

- Punkt C wyznaczamy, kreśląc prostopadłą do odcinka AB, przechodzącą przez punkt D.
- Łączymy odcinkiem punkty C i O.
- Punkt E znajdujemy, kreśląc prostopadłą do odcinka OC, przechodzącą przez punkt D.
- Kąty proste: ACB, ADC, DEO.
- Wyznaczymy teraz długości odcinków, które odpowiadają:
  - średniej arytmetycznej a i b, czyli $\frac{a+b}{2}$
  - średniej geometrycznej a i b, czyli $\sqrt{ab}$
  - średniej harmonicznej a i b, czyli $\frac{2ab}{a+b}$, co jest tym samym co $\frac{2}{\frac{1}{a}+\frac{1}{b}}$.

- Jest oczywiste, że średnia arytmetyczna $\frac{a+b}{2}$ równa jest długości promienia rozważanego półokręgu.
- Wynika z tego, że $\frac{a+b}{2} = |OC|$.

- Na podstawie podobieństwa trójkątów prostokątnych ADC i CDB mamy: $\frac{|AD|}{|DC|} = \frac{|DC|}{|DB|}$. Tak więc, $|DC|^2 = |AD| \cdot |DB| = a \cdot b$. Stąd $|DC| = \sqrt{ab}$.
- Z faktu, że DOC jest trójkątem prostokątnym, OC jego przeciwprostokątną, a CD jedną z przyprostokątnych wynika, że $\sqrt{ab} \leqslant \frac{a+b}{2}$.
- Na podstawie podobieństwa trójkątów prostokątnych DEC i CDO mamy: $\frac{|CE|}{|CD|} = \frac{|CD|}{|CO|}$, a zatem $|CD|^2 = |CE| \cdot |CO|$. Tak więc $ab = |CE| \cdot \frac{a+b}{2}$. Mamy zatem $|CE| = \frac{2ab}{a+b}$.
- Z faktu, że CDE jest trójkątem prostokątnym, CD jego przeciwprostokątną, a CE jedną z przyprostokątnych wynika, że $|CE| \leqslant |CD|$, czyli $\frac{2ab}{a+b} \leqslant \sqrt{ab}$.

- Pokazaliśmy zatem, że zachodzą następujące nierówności między rozważanymi trzema rodzajami średnich (harmoniczną, geometryczną, arytmetyczną) liczb a i b:
  $\frac{2}{\frac{1}{a}+\frac{1}{b}} = \frac{2ab}{a+b} \leqslant \sqrt{ab} \leqslant \frac{a+b}{2}$
- Równość zachodzi tylko wtedy, gdy $a = b$.
- Operacja brania każdej z tych średnich jest przemienna.
- Operacja średniej arytmetycznej dwóch liczb nie jest łączna.
- Ćwiczenie: sprawdzić, czy operacje średniej geometrycznej i średniej harmonicznej są łączne.

- Niech $\mathbf{A} = (A, R)$ i $\mathbf{B} = (B, S)$ będą strukturami relacyjnymi, gdzie $R \subseteq A^2$ i $S \subseteq B^2$. Mówimy, że $\mathbf{A}$ jest podstrukturą $\mathbf{B}$, gdy:
  - $A \subseteq B$
  - $R = S \cap A^2$.
- Np. $(\mathbb{N}, \leqslant)$ jest podstrukturą $(\mathbb{R}, \leqslant)$.

- Niech $\mathbf{A} = (A, f)$ i $\mathbf{B} = (B, g)$ będą algebrami z jedną operacją dwuargumentową. Mówimy, że $\mathbf{A}$ jest podalgebrą $\mathbf{B}$, gdy:
  - $A \subseteq B$
  - $g = f|(A \times A)$ (czyli g jest obcięciem f do $A \times A$)
  - A jest zamknięty ze względu na f (jeśli $x, y \in A$, to $f(x, y) \in A$).
- Np. $(\mathbb{N}, +)$ jest podalgebrą $(\mathbb{R}, +)$.

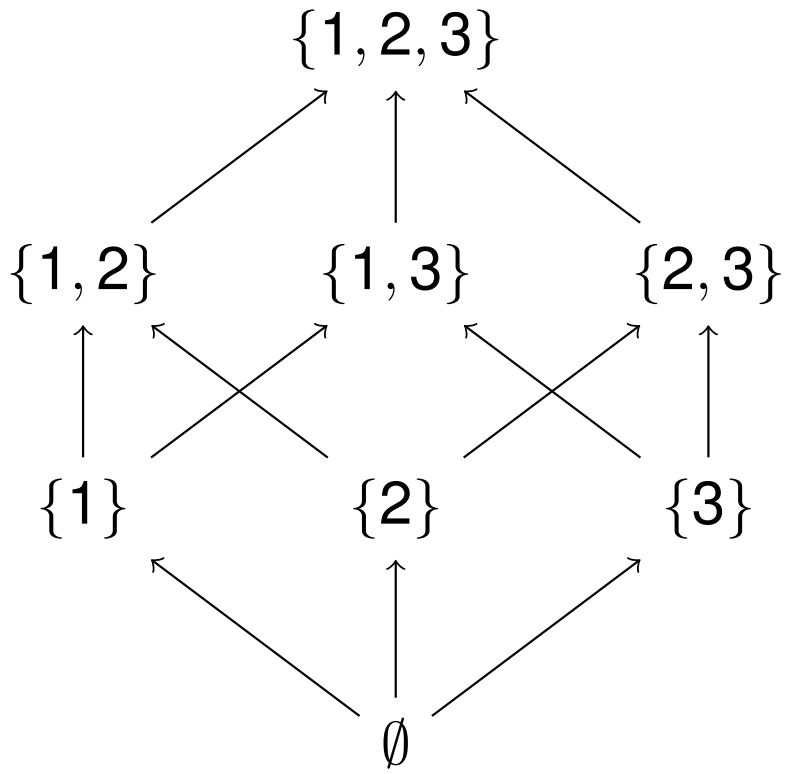
Ćwiczenie: pomyśl, jak zdefiniować te pojęcia w przypadku struktur relacyjnych i algebr o dowolnych zestawach relacji i operacji.

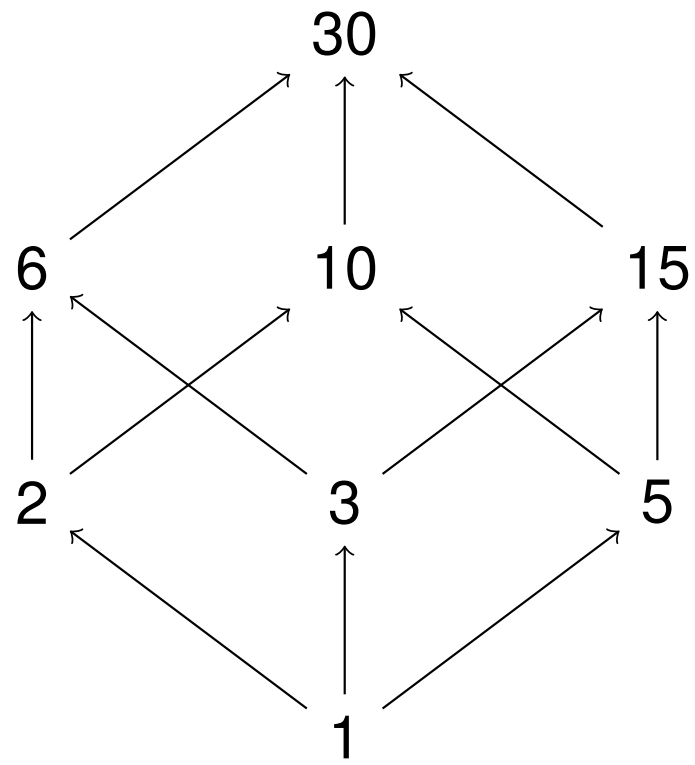
- Niech $\mathbf{A} = (A, R, f)$ i $\mathbf{B} = (B, S, g)$ będą strukturami, gdzie R i S są relacjami dwuargumentowymi, a f i g funkcjami dwuargumentowymi. Mówimy, że funkcja $h : A \to B$ jest *homomorfizmem* **A** w **B**, gdy dla wszystkich $x, y \in A$:
  - xRy wtedy i tylko wtedy, gdy $h(x)Sh(y)$.
  - $h(f(x, y)) = g(h(x), h(y))$.
- Np. funkcja logarytmiczna $\log : \mathbb{R}_+ \to \mathbb{R}$ jest homomorfizmem struktury $(\mathbb{R}_+, \leqslant, \cdot)$ w strukturę $(\mathbb{R}, \leqslant, +)$. Słuchacze pamiętają ze szkoły, że logarytm z iloczynu równy jest sumie logarytmów: $\log(x \cdot y) = \log(x) + \log(y)$.
- Jeśli h jest bijekcją i homomorfizmem **A** w **B**, to h nazywamy *izomorfizmem* między **A** i **B**. Mówimy, że **A** i **B** są *izomorficzne*, gdy istnieje izomorfizm **A** na **B**.

Ćwiczenie: pomyśl, jak zdefiniować te pojęcia w przypadku struktur relacyjnych i algebr o dowolnych zestawach relacji i operacji.

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 $f : \wp(\{1, 2, 3\}) \to \{1, 2, 3, 5, 6, 10, 15, 30\}$ 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 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?



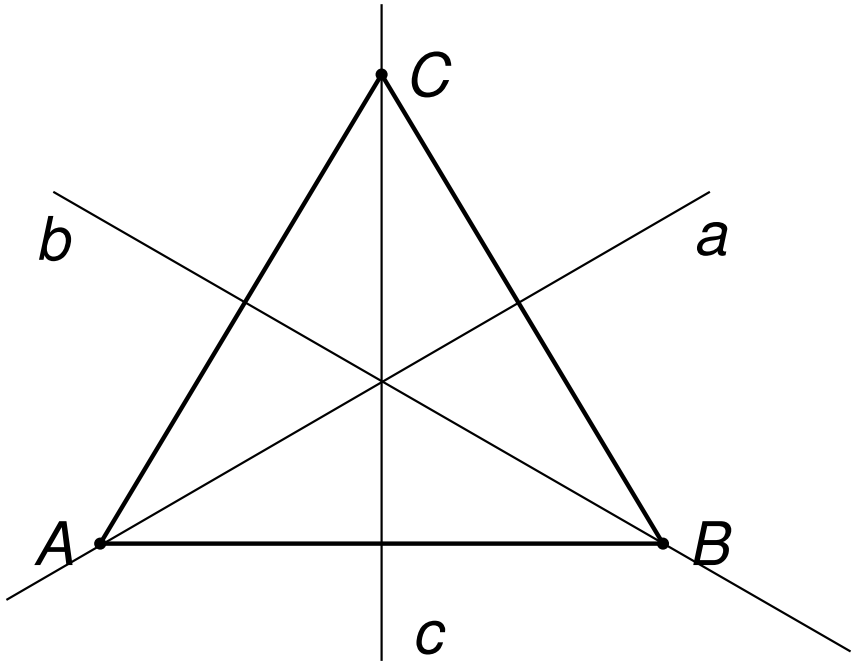


Strzałki w lewym diagramie reprezentują inkluzję, a w prawym relację podzielności. Ponieważ obie te relacje są przechodnie, więc dla uproszczenia pominięto pewne strzałki.

- Algebrą Peana jest każda algebra $\mathbf{A} = (A, f, a)$ taka, że:
  1. $a \in A$ (element początkowy algebry)
  2. $f : A \to A$ (funkcja następnika)
  3. $a \notin rng(f)$
  4. f jest funkcją różnowartościową
  5. Dla dowolnego zbioru $X \subseteq A$, jeśli $a \in X$ oraz $f(x) \in X$, o ile $x \in X$, dla wszystkich $x \in X$, to $X = A$.
- Każda algebra Peana jest izomorficzna z algebrą $(\mathbb{N}, s, 0)$, gdzie s jest funkcją następnika. Jak pamiętamy, dodawanie i mnożenie w $\mathbb{N}$ można zdefiniować, używając 0 i s.
- Definiujemy: $x \leqslant y$ wtedy i tylko wtedy, gdy istnieje $z \in \mathbb{N}$ taka, że $x + z = y$.

- Zbiór wszystkich permutacji skończonego zbioru X wraz z operacją składania permutacji (rozumianą jako złożenie funkcji) jest algebrą.

Algebrą jest zbiór wszystkich (sześciu) *symetrii* (tj. izometrii własnych, czyli przekształceń, w których obrazem figury jest ona sama) trójkąta równobocznego:



1. o_1: obrót o 0 stopni, o_2: obrót o 120 stopni, o_3: obrót o 240 stopni,
2. s_a: symetria względem prostej a, s_b: symetria względem prostej b, s_c: symetria względem prostej c.

Na przecięciu wiersza i kolumny tej tabeli znajduje się wynik złożenia operacji z tego wiersza i tej kolumny:

$\circ$	o_1	o_2	o_3	s_a	s_b	s_c
o_1	o_1	o_2	o_3	s_a	s_b	s_c
o_2	o_2	o_3	o_1	s_c	s_a	s_b
o_3	o_3	o_1	o_2	s_b	s_c	s_a
s_a	s_a	s_b	s_c	o_1	o_2	o_3
s_b	s_b	s_c	s_a	o_3	o_1	o_2
s_c	s_c	s_a	s_b	o_2	o_3	o_1

Podstrukturą powyższej struktury jest:

$\circ$	o_1	o_2	o_3
o_1	o_1	o_2	o_3
o_2	o_2	o_3	o_1
o_3	o_3	o_1	o_2

Rozważmy strukturę $\mathbb{K}_4 = (\{e, a, b, c\}, \circ)$, gdzie dwuargumentowe (łączne i przemienne) działanie $\circ$ jest określone tabelą:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

- $\mathbb{K}_4$ (*grupa czwórkowa Kleina*) jest izomorficzna np. ze strukturą $(\wp(\{x, y\}), \div)$, gdzie $\div$ operacją różnicy symetrycznej zbiorów. Elementem neutralnym w $(\wp(\{x, y\}), \div)$ jest $\emptyset$.
- W $\mathbb{K}_4$ każdy element jest elementem do siebie odwrotnym. Złożenie dowolnych dwóch elementów różnych od elementu neutralnego jest równe trzeciemu elementowi różnemu od neutralnego.

$\mathbb{K}_4$ nie jest jednak izomorficzna np. ze strukturą $C_4 = (\{e, a, b, c\}, \bullet)$ (*grupą cykliczną rzędu cztery*), gdzie (łączne i przemienne) działanie $\bullet$ jest zdefiniowane tabelą:

$\bullet$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

- $a \bullet a = b$, $a \bullet (a \bullet a) = a \bullet b = c$, $a \bullet (a \bullet (a \bullet a)) = e$, czyli wszystkie elementy struktury można otrzymać (wygenerować) z elementu a.
- Czterokrotna iteracja operacji $\bullet$ na każdym z elementów tej struktury równa jest elementowi neutralnemu e (mamy też $e \bullet e = e$ oraz $b \bullet b = e$).
- $C_4 = (\{e, a, b, c\}, \bullet)$ ma dokładnie trzy podstruktury: $(\{e\}, \bullet)$, $(\{e, a, b, c\}, \bullet)$ oraz $(\{e, b\}, \bullet)$.

- Niech $\mathbf{A} = (A, f)$ będzie algebrą, gdzie $f : A \times A \to A$ i niech E będzie relacją równoważności na A. Mówimy, że E jest *kongruencją* algebry $\mathbf{A}$, gdy dla wszystkich $x_1, x_2, y_1, y_2 \in A$:
- Jeśli $x_1 E y_1$ i $x_2 E y_2$, to $f(x_1, x_2) E f(y_1, y_2)$.
- Najmniejszą (względem inkluzji) kongruencją w strukturze $\mathbf{A}$ jest relacja identyczności na zbiorze A, a największą taką kongruencją jest relacja pełna w zbiorze A.

- Jeśli E jest kongruencją algebry $\mathbf{A} = (A, f)$, to przez *algebrę ilorazową* rozumiemy algebrę $\mathbf{A}/E = (A/E, f_E)$ taką, że:
- Dla dowolnych $x, y \in A$: $f_E([x]_E, [y]_E) = [f(x, y)]_E$.
- Z faktu, że E jest kongruencją algebry $\mathbf{A}$ wynika, iż powyższa definicja jest poprawna (nie zależy od wyboru reprezentantów z klas abstrakcji).

Ćwiczenie: pomyśl, jak zdefiniować te pojęcia dla algebr z dowolną liczbą operacji.

- Relacja równoliczności zbiorów, określona w rodzinie wszystkich podzbiorów dowolnego zbioru X jest kongruencją struktury $(\wp(X), \cup, \cap)$.
- 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: $x \equiv y (\mathrm{mod}\ n)$ 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.

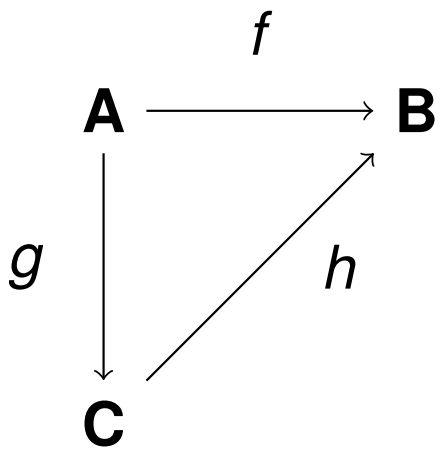
- W zbiorze $\mathbb{Z}/_{\equiv_p}$ wszystkich klas abstrakcji omówionej przed chwilą relacji równoważności $\equiv_p$, gdzie p jest liczbą pierwszą, wprowadzić możemy działania arytmetyczne, wykorzystując działania arytmetyczne w zbiorze $\mathbb{Z}$ i fakt, że relacja $\equiv_p$ jest kongruencją w strukturze $(\mathbb{Z}, +, \cdot)$:
- Zauważmy, że $\mathbb{Z}/_{\equiv_p}$ liczy dokładnie p elementów.
  - $[x]_{\equiv_p} \oplus_p [y]_{\equiv_p} = [x + y]_{\equiv_p}$
  - $[x]_{\equiv_p} \otimes_p [y]_{\equiv_p} = [x \cdot y]_{\equiv_p}$

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

Mając daną algebrę $(\mathbb{N}, +, \cdot, 0)$ można skonstruować algebry: $(\mathbb{Z}, +, \cdot, 0)$ (liczby całkowite) oraz $(\mathbb{Q}, +, \cdot, 0, 1)$ (liczby wymierne).
Relacja $\approx \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$: $(a, b) \approx (c, d)$ wtedy i tylko wtedy, gdy $a + d = c + b$ jest relacją równoważności.
Relacja $\sim \subseteq (\mathbb{Z} \times (\mathbb{Z} - \{0\})) \times (\mathbb{Z} \times (\mathbb{Z} - \{0\}))$: $(a, b) \sim (c, d)$ wtedy i tylko wtedy, gdy $a \cdot d = b \cdot c$ jest relacją równoważności.

- Kongruencje algebr związane są z homomorfizmami algebr. Każda funkcja $f : A \to B$ wyznacza pewną relację równoważności na A. Definiujemy mianowicie: $x \ker_f y$ wtedy i tylko wtedy, gdy $f(x) = f(y)$. Relację $\ker_f$ nazywamy *jądrem odwzorowania* f.
- Jeśli $f : \mathbf{A} \to \mathbf{B}$ jest homomorfizmem algebry $\mathbf{A}$ na algebrę $\mathbf{B}$, to relacja $\ker_f$ zdefiniowana wzorem: $x \ker_f y$ wtedy i tylko wtedy, gdy $f(x) = f(y)$ jest kongruencją algebry $\mathbf{A}$.
- Jeśli E jest kongruencją algebry $\mathbf{A}$, to *odwzorowanie kanoniczne* $k_E : \mathbf{A} \to \mathbf{A}/E$ dane wzorem $k_E(x) = [x]_E$ dla $x \in A$ jest homomorfizmem algebry $\mathbf{A}$ na algebrę ilorazową $\mathbf{A}/E$. Tak więc, dla dowolnej algebry $\mathbf{A}$:
  1. Każdy obraz homomorficzny algebry $\mathbf{A}$ jest izomorficzny z pewną algebrą ilorazową algebry $\mathbf{A}$.
  2. Każda algebra ilorazowa algebry $\mathbf{A}$ jest izomorficzna z pewnym homomorficznym obrazem algebry $\mathbf{A}$.

- **Twierdzenie** (o homomorfizmie). Niech **A**, **B** i **C** będą algebrami tego samego typu. Niech dalej $f : \mathbf{A} \to \mathbf{B}$ będzie homomorfizmem, a $g : \mathbf{A} \to \mathbf{C}$ będzie homomorfizmem surjektywnym, przy czym $ker_g \subseteq ker_f$. Wtedy istnieje dokładnie jeden homomorfizm $h : \mathbf{C} \to \mathbf{B}$ taki, że $h \circ g = f$.



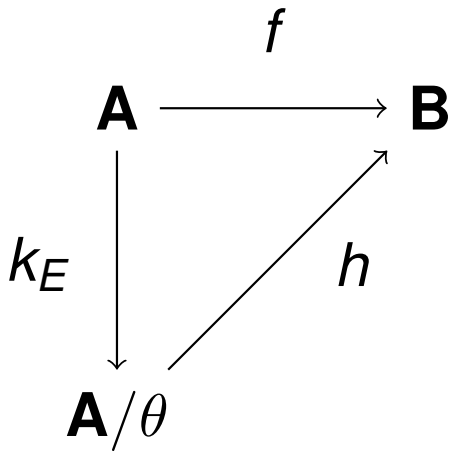
Dowód. Niech $h = \{(g(a), f(a)) : a \in A\}$. Pokażemy, że: h jest funkcją, nadto jedyną funkcją taką, że $h \circ g = f$, i wreszcie, że h jest homomorfizmem **C** w **B**.
Jeśli $g(a) = g(b)$, to $(a, b) \in ker_g$, a zatem także $(a, b) \in ker_f$, co oznacza, że $f(a) = f(b)$. Widać więc, że relacja h jest funkcją. Jej dziedziną jest C, ponieważ g jest surjekcją. Ponadto, $h(g(a)) = f(a)$ dla dowolnego $a \in A$, czyli $h \circ g = f$. Niech $h' \circ g = f$. Wtedy dla dowolnego $c \in C$ istnieje $a \in A$ takie, że $g(a) = c$. Ponadto:
$h'(c) = h'(g(a)) = (h' \circ g)(a) = f(a) = (h \circ g)(a) = h(g(a)) = h(c)$,
czyli $h = h'$, co oznacza, że funkcja h jest wyznaczona jednoznacznie.
Pokażemy, że h jest homomorfizmem **C** w **B**, zakładając, że w każdej z algebr **A**, **B** i **C** mamy jedną operację n-argumentową, czyli że $\mathbf{A} = (A, \omega^{\mathbf{A}})$, $\mathbf{B} = (B, \omega^{\mathbf{B}})$ i $\mathbf{C} = (C, \omega^{\mathbf{C}})$, gdzie $\omega^{\mathbf{A}} : A^n \to A$, $\omega^{\mathbf{B}} : B^n \to B$ i $\omega^{\mathbf{C}} : C^n \to C$. Dowód w przypadku ogólnym, czyli gdy każda z rozważanych algebr zawiera więcej niż jedną operację, przebiega analogicznie.

Aby pokazać, że h jest homomorfizmem $\mathbf{C}$ w $\mathbf{B}$, trzeba udowodnić, iż dla dowolnych $c_1, \ldots, c_m \in C$ zachodzi:
$h(\omega^{\mathbf{C}}(c_1, \ldots, c_m)) = \omega^{\mathbf{B}}(h(c_1), \ldots, h(c_m))$.
Niech $c_1, \ldots, c_m \in C$. Ponieważ g jest surjekcją, więc istnieją $a_1, \ldots, a_m \in A$ takie, że $g(a_i) = c_i$ dla wszystkich $1 \leqslant i \leqslant m$. Na mocy tego, że f i g są homomorfizmami, mamy:

$$
\begin{aligned}
&h(\omega^{\mathbf{C}}(c_1, \ldots, c_m)) = \\
&h(\omega^{\mathbf{C}}(g(a_1), \ldots, g(a_m))) = \\
&h(g(\omega^{\mathbf{A}}(a_1, \ldots, a_m))) = \\
&(h \circ g)(\omega^{\mathbf{A}}(a_1, \ldots, a_m)) = \\
&f(\omega^{\mathbf{A}}(a_1, \ldots, a_m)) = \\
&\omega^{\mathbf{B}}(f(a_1), \ldots, f(a_m)) = \\
&\omega^{\mathbf{B}}((h \circ g)(a_1), \ldots, (h \circ g)(a_m)) = \\
&\omega^{\mathbf{B}}(h(g(a_1)), \ldots, h(g(a_m))) = \\
&\omega^{\mathbf{B}}(h(c_1), \ldots, h(c_m)).
\end{aligned}
$$

A zatem h jest homomorfizmem $\mathbf{C}$ w $\mathbf{B}$. □

Twierdzenie (o izomorfizmie). Niech $f : \mathbf{A} \to \mathbf{B}$ będzie surjektywnym homomorfizmem. Jeśli $E = ker_f$, to istnieje dokładnie jeden izomorfizm $h : \mathbf{A}/E \to \mathbf{B}$ taki, że $h \circ k_E = f$.



Dowód. Ponieważ z założenia $E = ker_{k_E} = ker_f$, więc korzystając z poprzedniego twierdzenia wiemy, że istnieje dokładnie jeden homomorfizm $h : \mathbf{A}/E \to \mathbf{B}$ taki, że $h \circ k_E = f$. Trzeba pokazać, że h jest bijekcją.

- Ponieważ f jest surjekcją, więc dla każdego $b \in B$ istnieje $a \in A$ taki, że $f(a) = b$.
- Mamy zatem:

$$b = f(a) = (h \circ k_E)(a) = h(k_E(a)) = h([a]_E),$$

  czyli h jest surjekcją.
- Przypuśćmy, że $h([a]_E) = h([b]_E)$.
- Wtedy $f(a) = f(b)$, co oznacza, że $(a, b) \in ker_f = E$.
- A zatem $[a]_E = [b]_E$, czyli h jest injekcją.

□

- Świat struktur relacyjnych i algebr jest niezmiernie bogaty.
- Obejmuje różnego rodzaju struktury liczbowe (liczby naturalne, całkowite, wymierne, rzeczywiste, zespolone, kwaterniony, itd.), ale także struktury złożone z relacji, funkcji, wielomianów, macierzy, wektorów, a właściwie dowolnych obiektów matematycznych, na których wykonujemy pewne operacje.

- W dziejach matematyki rozważania algebraiczne dotyczyły początkowo przede wszystkim rozwiązywania równań.
- Rozwój algebry rozumianej jako badanie dowolnych struktur matematycznych ma miejsce nieprzerwanie od XIX wieku.
- Podajemy tu jedynie definicje kilku najważniejszych rodzajów struktur algebraicznych, wraz z prostymi przykładami.

Algebrę $(A, \circ)$ z działaniem dwuargumentowym $\circ$ nazywamy *grupą*, gdy:

1. $\circ$ jest łączne;
2. $\circ$ ma element neutralny;
3. dla każdego elementu $x \in A$ istnieje element odwrotny x^{-1} względem działania $\circ$.

Jeśli $\circ$ jest przemienne, to grupę $(A, \circ)$ nazywamy *przemienną* (*abelową*).

1. Wszystkie bijekcje zbioru A na A tworzą grupę, ze złożeniem odwzorowań jako działaniem grupowym. Wtedy elementem neutralnym jest bijekcja identycznościowa, a elementem odwrotnym do danego elementu jest bijekcja do niego odwrotna.
2. Wszystkie izometrie płaszczyzny tworzą grupę. Operacją grupową jest składanie przekształceń.
3. Grupami są np.: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$. Nie jest grupą np. $(\mathbb{N}, +)$.

- Algebrę $(A, \oplus, \otimes)$ nazywamy *pierścieniem*, gdy $\oplus$ oraz $\otimes$ są działaniami dwuargumentowymi takimi, że:
  - $(A, \oplus)$ jest grupą abelową;
  - $\otimes$ jest łączne;
  - $\otimes$ jest lewo- oraz prawostronnie rozdzielne względem $\oplus$.
- Jeśli $\otimes$ ma element neutralny, to pierścień $(A, \oplus, \otimes)$ nazywamy *pierścieniem z jednością*.
- Mówimy, że element x pierścienia $(A, \oplus, \otimes)$ jest *dzielnikiem zera*, gdy istnieje $y \in A$ taki, że $x \otimes y = \mathbf{0}$, gdzie $\mathbf{0}$ jest elementem neutralnym względem $\oplus$.
- Pierścienie z przemiennym mnożeniem, z jednością oraz bez dzielników zera nazywamy *dziedzinami całkowitości*.

- $(\mathbb{Z}, +, \cdot)$ jest dziedziną całkowitości.
- Wszystkie wielomiany o współczynnikach rzeczywistych tworzą pierścień. Operacjami są tu: dodawanie i mnożenie wielomianów.
- Rozważmy zbiór $\mathbb{R} \times \mathbb{R}$ wraz z operacjami $\oplus$ i $\otimes$:
  1. $(a, b) \oplus (c, d) = (a + c, b + d)$
  2. $(a, b) \otimes (c, d) = (a \cdot c, a \cdot d + b \cdot c)$
- Wtedy $(\mathbb{R} \times \mathbb{R}, \oplus, \otimes)$ jest pierścieniem (liczby dualne), w którym mnożenie $\otimes$ jest przemienne, elementem neutralnym dodawania $\oplus$ jest para $(0, 0)$, jednością jest para $(1, 0)$. Istnieją w nim dzielniki zera $(0, b)$ (gdzie $b \neq 0$), ponieważ mamy: $(0, b) \otimes (b, 0) = (0, 0)$. Ta struktura nie jest zatem dziedziną całkowitości.

Algebrę $(A, \oplus, \otimes)$, gdzie A ma co najmniej 2 elementy, nazywamy *ciałem*, gdy $\oplus$ oraz $\otimes$ są działaniami dwuargumentowymi takimi, że:

1. $(A, \oplus)$ jest grupą abelową z elementem neutralnym $\mathbf{0}$
2. $\otimes$ jest łączne i przemienne
3. $\otimes$ ma element neutralny $\mathbf{1}$
4. dla każdego $x \neq \mathbf{0}$ istnieje y taki, że y jest elementem odwrotnym dla x względem działania $\otimes$
5. $\otimes$ jest rozdzielne względem $\oplus$.

Najmniejszą liczbę n taką, że $n \otimes \mathbf{1} = \mathbf{0}$ nazywamy *charakterystyką* ciała $(A, \oplus, \otimes)$. Jeżeli nie istnieje n taka, że $n \otimes \mathbf{1} = \mathbf{0}$, to mówimy, że ciało $(A, \oplus, \otimes)$ ma *charakterystykę* 0.

1. Liczby wymierne ze „zwykłym” dodawaniem i mnożeniem, liczby rzeczywiste ze „zwykłym” dodawaniem i mnożeniem tworzą ciała (charakterystyki 0). Są to ciała, w których porządek jest zgodny z działaniami arytmetycznymi.
2. Ciałem jest zbiór $\mathbb{A}$ wszystkich liczb algebraicznych z operacjami dodawania i mnożenia.
3. Zbiór $\mathbb{C}$ wszystkich liczb zespolonych z działaniami dodawania i mnożenia jest ciałem (charakterystyki 0). W ciele $\mathbb{C}$ nie można określić porządku, który byłby zgodny z działaniami arytmetycznymi.
4. Ciałem jest zbiór wszystkich liczb o postaci $a + b \cdot \sqrt{2}$, gdzie $a, b \in \mathbb{R}$.
5. Dla dowolnej liczby pierwszej p ciałem skończonym (charakterystyki p) jest zbiór wszystkich klas abstrakcji relacji przystawania liczb naturalnych modulo p.
6. $(\mathbb{Z}, +, \cdot)$ nie jest ciałem.

Przestrzenią liniową (*przestrzenią wektorową*) nad ciałem $\mathbb{S} = (S, \oplus, \otimes)$ (ciałem *skalarów*) nazywamy strukturę o niepustym uniwersum X oraz działaniami: dodawaniem $\boxplus$ elementów zbioru X (dodawaniem wektorów) oraz mnożeniem $\boxtimes$ elementów zbioru X przez elementy ciała $\mathbb{S}$ (czyli: mnożeniem wektora przez skalar), gdy:

1. dodawanie wektorów $\boxplus$ jest łączne i przemienne
2. istnieje element neutralny θ dodawania $\boxplus$ (wektor zerowy)
3. dla każdego $x \in X$ istnieje element odwrotny do x względem dodawania $\boxminus x$
4. zachodzą prawa rozdzielności – dla dowolnych wektorów $x, y \in X$ oraz skalara $a \in S$:
   $(x \boxplus y) \boxtimes a = (x \boxtimes a) \boxplus (y \boxtimes a)$
   $a \boxtimes (x \boxplus y) = (a \boxtimes x) \boxplus (a \boxtimes y)$
5. zachodzi prawo łączności – dla dowolnego wektora $x \in X$ oraz skalarów $a, b \in S$: $a \boxtimes (b \boxtimes x) = (a \otimes b) \boxtimes x$
6. dla dowolnego wektora $x \in X$ zachodzi $\mathbf{1} \boxtimes x = x$, gdzie $\mathbf{1}$ jest elementem neutralnym mnożenia w ciele $\mathbb{S}$.

W niektórych przestrzeniach liniowych określić można pojęcie *odległości*, opierając się na pojęciu *normy* wektora.
Niech $\mathbb{X} = (X, \boxplus, \boxtimes, \theta)$ będzie przestrzenią wektorową nad ciałem liczb rzeczywistych $\mathbb{R}$. *Normą* w przestrzeni $\mathbb{X}$ nazywamy odwzorowanie X w $\mathbb{R}$, które przyporządkowuje każdemu wektorowi $x \in X$ liczbę $\| x \| \in \mathbb{R}$, przy czym spełnione są następujące warunki:

1. $\| x \| \geqslant 0$ dla każdego $x \in X$
2. $\| x \| = 0$ wtedy i tylko wtedy, gdy $x = \theta$
3. $\| x \boxplus y \| \leqslant \| x \| + \| y \|$ dla $x, y \in X$
4. $a \cdot \| x \| = |a| \boxtimes \| x \|$ dla $x \in X$ oraz $a \in \mathbb{R}$.

Parę $(\mathbb{X}, \| \|)$ nazywamy *przestrzenią (liniową) unormowaną*. Odległość między wektorami x oraz y przestrzeni unormowanej można wtedy zdefiniować jako $\| x \boxminus y \|$.

- Każde ciało $\mathbb{K}$ można uważać za przestrzeń liniową nad ciałem $\mathbb{K}$ ujmowanym jako ciało skalarów.
- Każdy zbiór $\mathbb{R}^n$ ($n \geqslant 1$) tworzy przestrzeń liniową nad ciałem liczb rzeczywistych $\mathbb{R}$.
- Jeśli X jest dowolnym zbiorem, a $\mathbb{V}$ przestrzenią liniową nad ciałem liczb rzeczywistych $\mathbb{R}$, to przestrzenią liniową jest też zbiór wszystkich funkcji z X w $\mathbb{V}$, gdzie dodawanie $\boxplus$ funkcji oraz mnożenie $\boxtimes$ funkcji przez skalar określone są następująco:
  1. $(f \boxplus g)(x) = f(x) + g(x)$
  2. $a \boxtimes f(x) = a \cdot f(x)$.
- Zbiór wszystkich macierzy o m wierszach oraz n kolumnach tworzy przestrzeń liniową. Operacja dodawania jest tu dodawaniem macierzy: jeśli $A = [a_{ij}]$, $B = [b_{ij}]$, to $A \boxplus B = [a_{ij} + b_{ij}]$. Mnożenie $\boxtimes$ macierzy przez skalar polega na mnożeniu każdego elementu macierzy przez ten skalar: jeśli $A = [a_{ij}]$, to $x \boxtimes A = [x \cdot a_{ij}]$, dla $x \in \mathbb{R}$.

- *Definicja porządkowa*. Zbiór częściowo uporządkowany $(L, \leqslant)$ nazywamy *kratą*, gdy dla każdych $a, b \in L$ istnieją: kres dolny, oznaczany przez $\inf\{a, b\}$) oraz kres górny, oznaczany przez $\sup\{a, b\}$). Często używane oznaczenia dla $\inf\{a, b\}$: $a \wedge b$ (albo $a \cap b$); dla $\sup\{a, b\}$: $a \vee b$ (albo $a \cup b$).
- *Definicja algebraiczna*. Kratą nazywamy algebrę $(L, \wedge, \vee)$, spełniającą następujące warunki:

$(L1)$	$a \wedge b = b \wedge a$	$(L1')$	$a \vee b = b \vee a$
$(L2)$	$a \wedge a = a$	$(L2')$	$a \vee a = a$
$(L3)$	$a \wedge (b \wedge c) = (a \wedge b) \wedge c$	$(L3')$	$a \vee (b \vee c) = (a \vee b) \vee c$
$(L4)$	$a \wedge (a \vee b) = a$	$(L4')$	$a \vee (a \wedge b) = a$

Udowodnimy, że powyższe definicje są równoważne, czyli że:

- A. Jeśli $(L, \leqslant)$ jest zbiorem częściowo uporządkowanym, w którym istnieją kres dolny $x \wedge y$ oraz górny $x \vee y$, to $\wedge$ i $\vee$ spełniają warunki $(L1)$–$(L4')$.
- B. Jeśli $(L, \wedge, \vee)$ spełnia warunki $(L1)$–$(L4')$, to relacja $\leqslant$ określona waruniem $a \leqslant b$ wtedy i tylko wtedy, gdy $a \wedge b = a$ jest częściowym porządkiem w L, w którym $a \wedge b$ jest kresem dolnym a i b, a $a \vee b$ jest kresem górnym a i b, a ponadto $a \leqslant b$ wtedy i tylko wtedy, gdy $a \vee b = b$.

Dowód implikacji: jeśli A, to B. Niech $(L, \leqslant)$ będzie kratą w sensie definicji porządkowej. Pokażemy, że kresy $\wedge$ i $\vee$ spełniają warunki $(L1)$–$(L4')$.

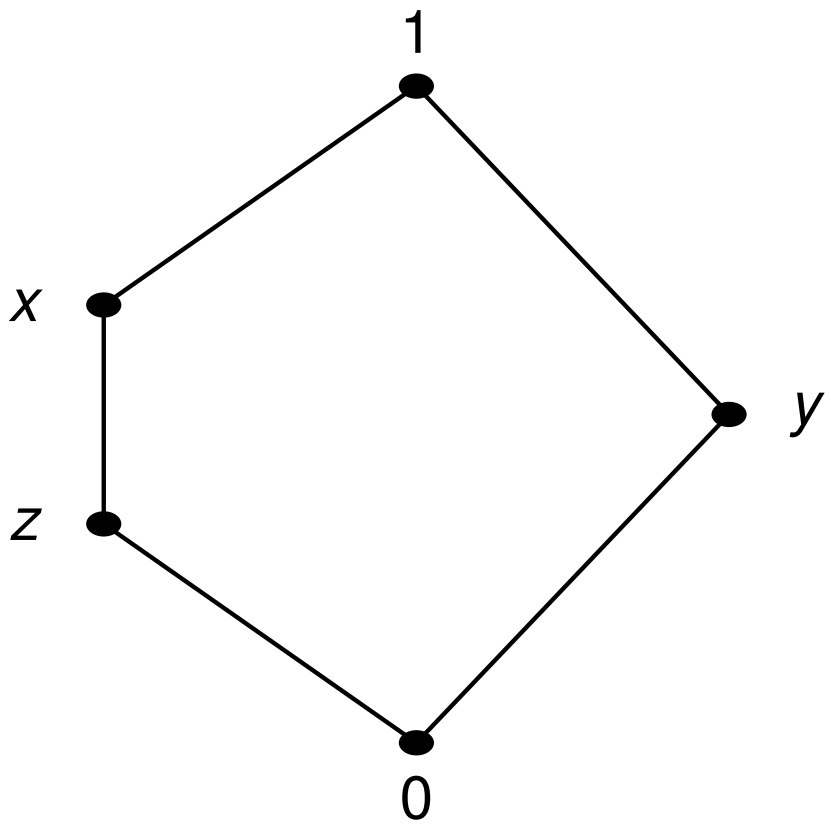
1. Warunki $(L1)$, $(L2)$, $(L1')$, $(L2')$ są oczywiste.
2. Łączność $\wedge$. Niech $d = a \wedge (b \wedge c)$. Wtedy $d \leqslant a$ i $d \leqslant b \wedge c$, a dalej $d \leqslant b$ i $d \leqslant c$. Skoro $d \leqslant a$ i $d \leqslant b$, to $d \leqslant a \wedge b$, a ponieważ $d \leqslant c$, więc $d \leqslant (a \wedge b) \wedge c$. Niech $e = (a \wedge b) \wedge c$. Wtedy kolejno: $e \leqslant c$, $e \leqslant a \wedge b$, $e \leqslant a$, $e \leqslant b$, $e \leqslant (b \wedge c)$, $e \leqslant a \wedge (b \wedge c)$.
3. Podobnie dowodzimy łączności $\vee$.
4. Na mocy definicji kresu dolnego: jeśli $a \leqslant b$, to $a \wedge b = a$, a jeśli $a \wedge b = a$, to $a \leqslant b$. Tak więc, $a \leqslant b$ wtedy i tylko wtedy, gdy $a \wedge b = a$. Podobnie, $a \leqslant b$ wtedy i tylko wtedy, gdy $a \vee b = b$, na mocy definicji kresu górnego.
5. Warunki $(L4)$ i $(L4')$ są zatem spełnione, ponieważ $a \wedge b \leqslant a \leqslant a \vee b$.

Dowód implikacji: jeśli B, to A. Niech $(L, \wedge, \vee)$ będzie kratą w sensie definicji algebraicznej. Pokażemy, że $(L, \leqslant)$ jest kratą w sensie definicji porządkowej, gdzie $a \leqslant b$ wtedy i tylko wtedy, gdy $a \wedge b = a$.

1. Relacja $\leqslant$ jest zwrotna na mocy $(L2)$. Jeśli $a \leqslant b$ i $b \leqslant c$, to $a \wedge b = a$ i $b \wedge c = b$. Mamy: $a = a \wedge b = a \wedge (b \wedge c) = (a \wedge b) \wedge c = a \wedge c$, czyli $a \leqslant c$, a więc $\leqslant$ jest przechodnia. Jeśli $a \leqslant b$ i $b \leqslant a$, to $a \wedge b = a$ i $b \wedge a = b$, a zatem $\leqslant$ jest antysymetryczna.
2. Pokażemy, że $a \wedge b = \inf\{a, b\}$. Mamy: $(a \wedge b) \wedge a = a \wedge (b \wedge a) = a \wedge (a \wedge b) = (a \wedge a) \wedge b = a \wedge b$, czyli $a \wedge b \leqslant a$. Podobnie, $a \wedge b \leqslant b$. Jeśli $x \leqslant a$ i $x \leqslant b$, to $x \wedge a = x$ i $x \wedge b = x$. A zatem $x = x \wedge b = (x \wedge a) \wedge b = x \wedge (a \wedge b)$, co oznacza, że $x \leqslant (a \wedge b)$.
3. Pokażemy, że $a \vee b = \sup\{a, b\}$. Ponieważ $a = a \wedge (a \vee b)$, więc $a \leqslant a \vee b$ (podobnie, $b \leqslant a \vee b$). Jeśli $a \leqslant y$ i $b \leqslant y$, to $a \wedge y = a$ i $b \wedge y = b$. Mamy wtedy: $a \vee y = (a \wedge y) \vee y = y \vee (y \wedge a) = y$ (podobnie, $b \vee y = y$). Dalej: $(a \vee b) \wedge y = (a \vee b) \wedge (a \vee y) =$ $(a \vee b) \wedge (a \vee (b \vee y)) = (a \vee b) \wedge ((a \vee b) \vee y) = a \vee b$, czyli $a \vee b \leqslant y$.

- Rodzina wszystkich podzbiorów dowolnego zbioru, częściowo uporządkowana przez relację inkluzji jest kratą. Kresem dolnym jest iloczyn, a kresem górnym suma zbiorów.
- Rodzina wszystkich skończonych podzbiorów zbioru $\mathbb{N}$, częściowo uporządkowana przez relację inkluzji jest kratą.
- Zbiór wszystkich dodatnich liczb naturalnych częściowo uporządkowany przez relację podzielności (bez reszty) jest kratą. Największy wspólny dzielnik jest tu kresem dolnym, a najmniejsza wspólna wielokrotność kresem górnym.
- Dowolny skończony zbiór liniowo uporządkowany jest kratą.
- Rodzina $Eq(X)$ wszystkich relacji równoważności na zbiorze X jest kratą. Kresem dolnym jest iloczyn relacji, kresem górnym relacji $\theta, \psi \in Eq(X)$ jest $\theta \cup (\theta \circ \psi) \cup (\theta \circ \psi \circ \theta) \cup (\theta \circ \psi \circ \theta \circ \psi) \cup \ldots$.
- Rodzina $Con(\mathbf{A})$ wszystkich kongruencji algebry $\mathbf{A}$ jest kratą.

Krata N_5. Tę kratę nazywamy też pentagonem:

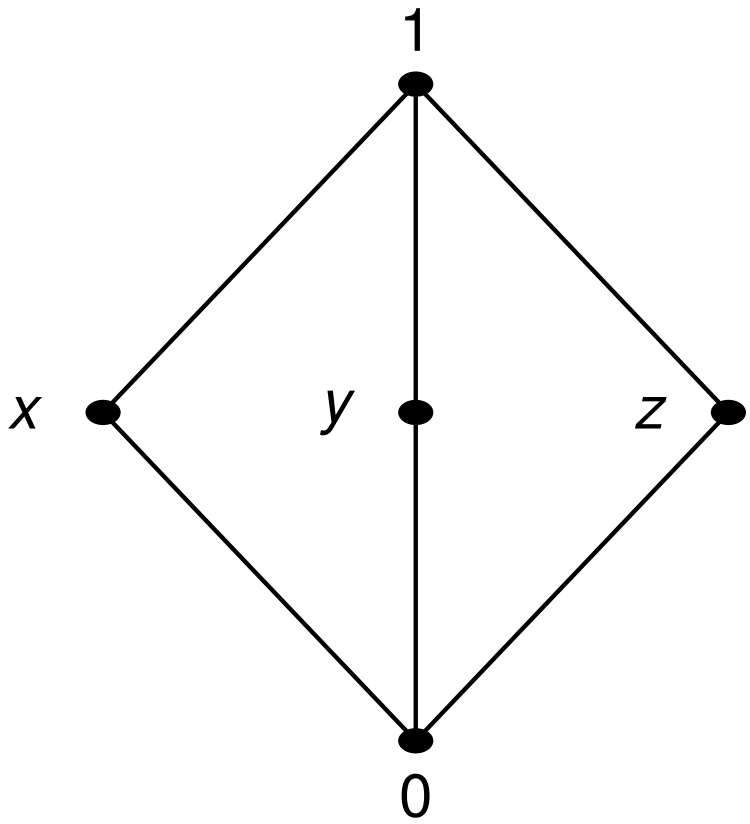


Mamy tutaj:

$x \wedge (y \vee z) = x \wedge 1 = x$

$(x \wedge y) \vee (x \wedge z) = 0 \vee z = z$

Krata M_3. Tę kratę nazywamy też diamentem:

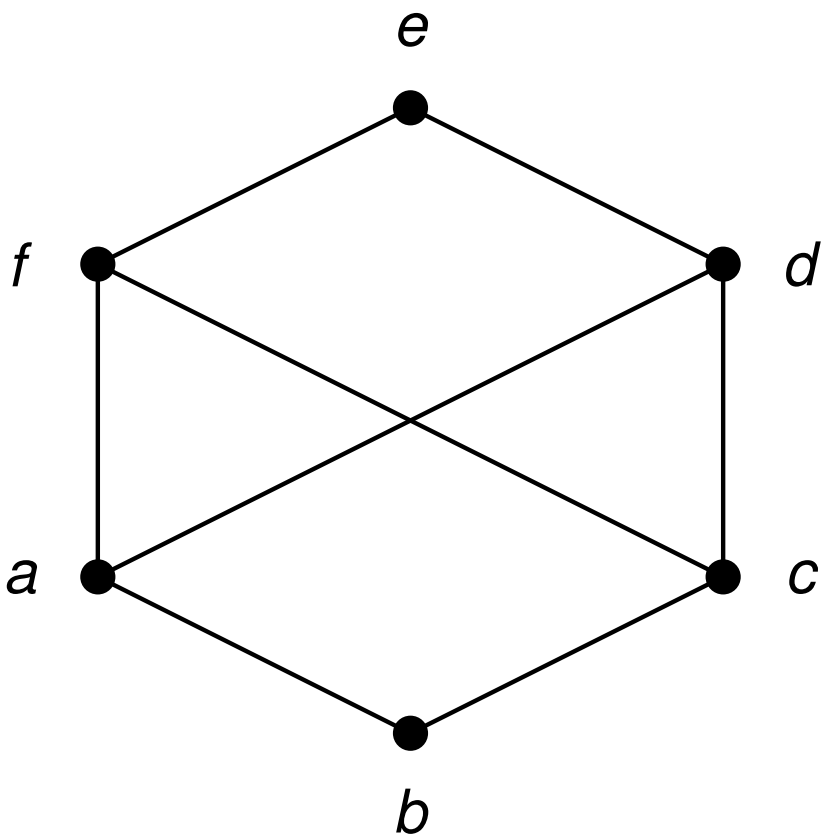


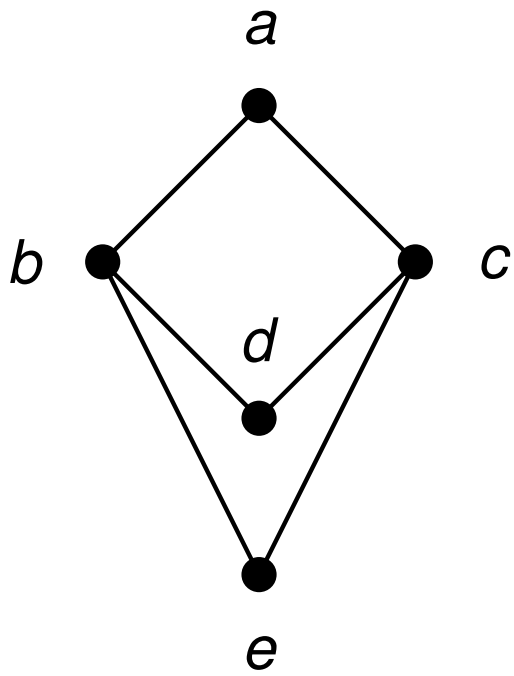
Mamy tutaj:

$x \wedge (y \vee z) = x \wedge 1 = x$

$(x \wedge y) \vee (x \wedge z) = 0 \vee 0 = 0$

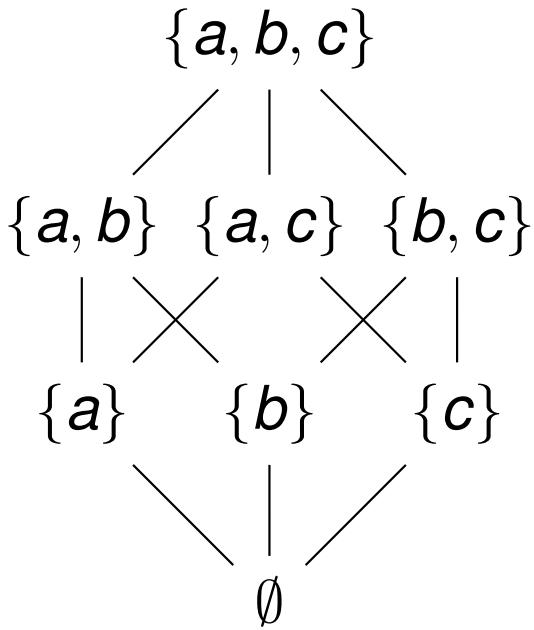
Diagramy Hassego dla struktur, które nie są kratami. Zauważmy, że nie są kratami następujące struktury:

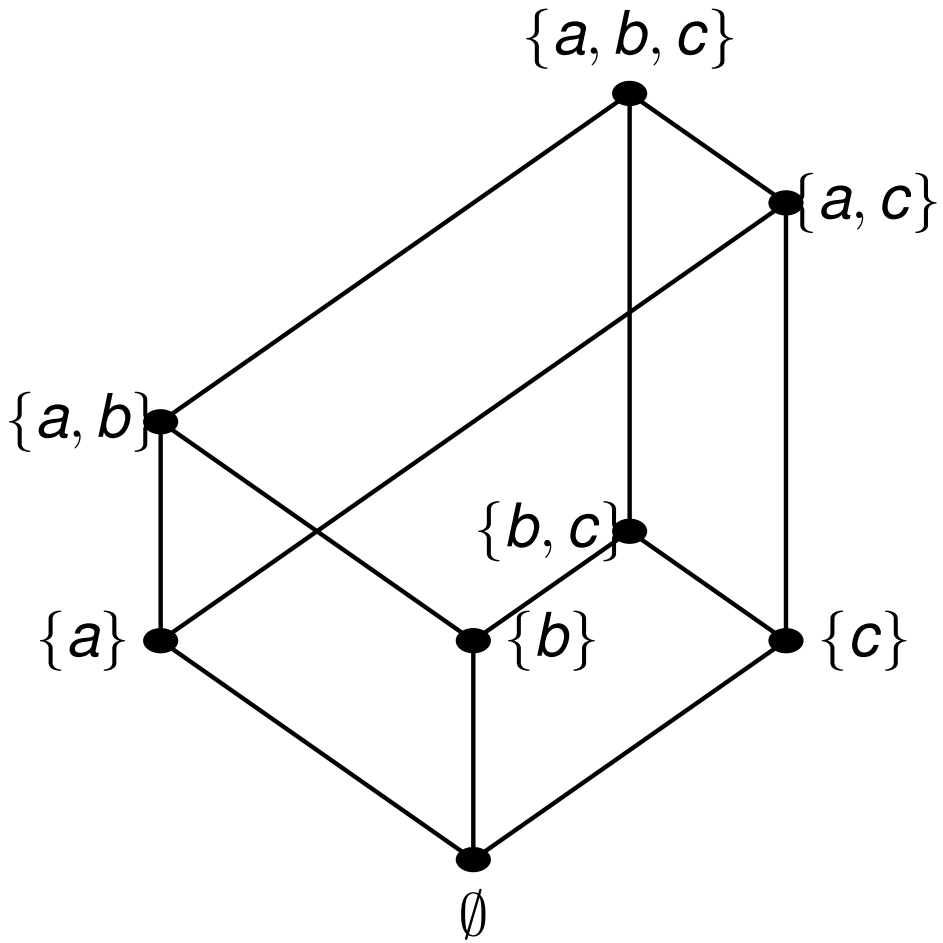


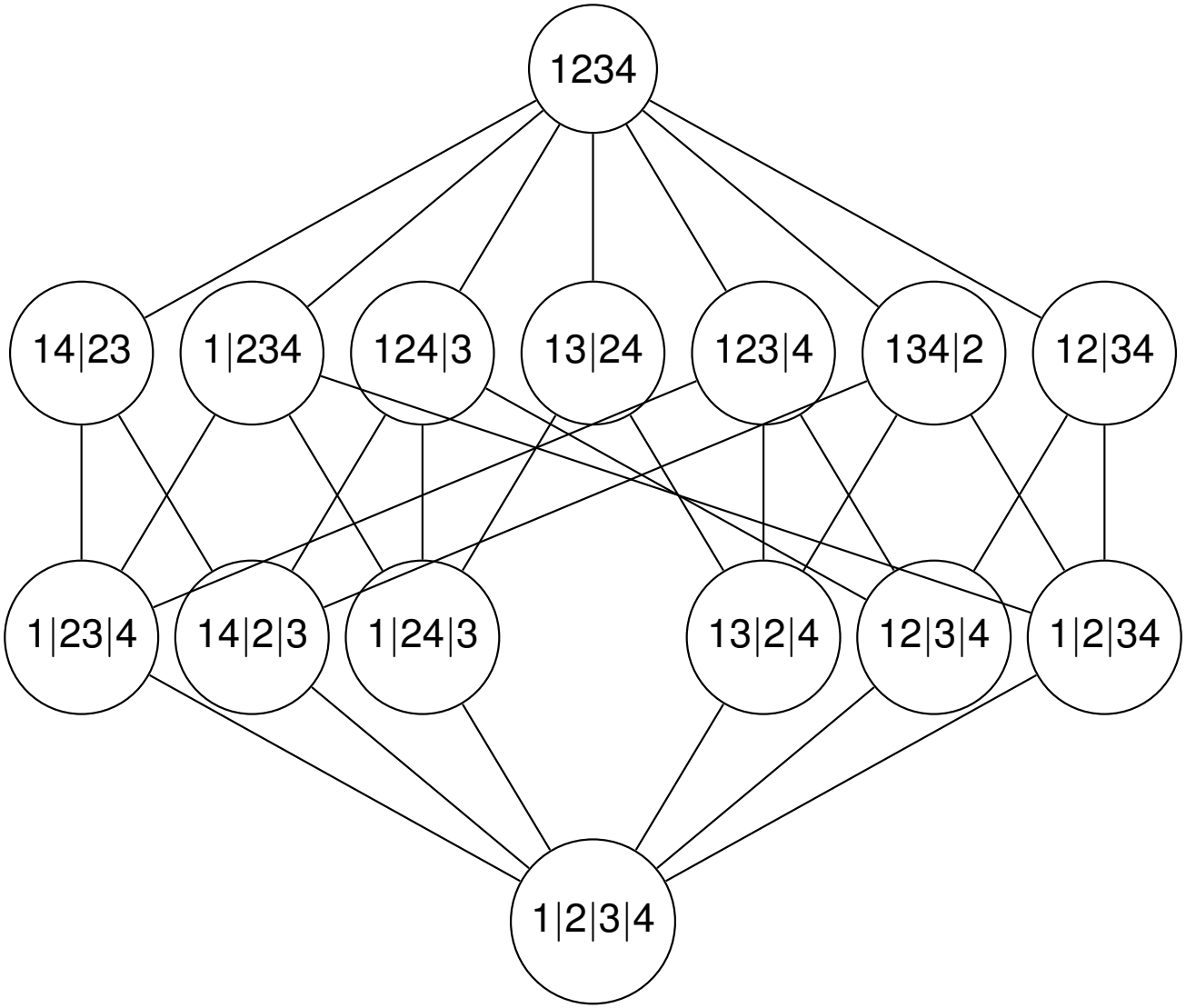


Po lewej: *a* i *c* nie mają kresu górnego; po prawej: *b* i *c* nie mają kresu dolnego.

Krata podzbiorów zbioru trójelementowego. Zauważmy, że diagramy Hassego mogą z pozoru być różne, choć wyznaczają tę samą strukturę:

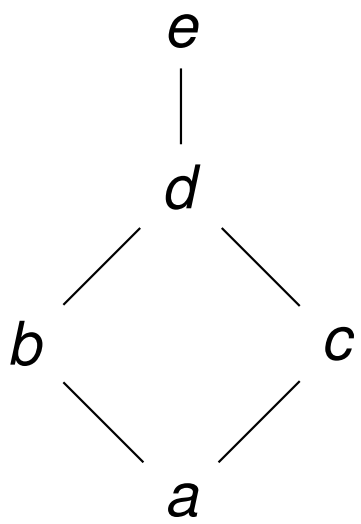






Krata podziałów zbioru $\{1, 2, 3, 4\}$.

Zauważmy, że podzbiór kraty sam może być kratą, ale nie być podkratą rozważanej kraty. Oto przykład takiej sytuacji:

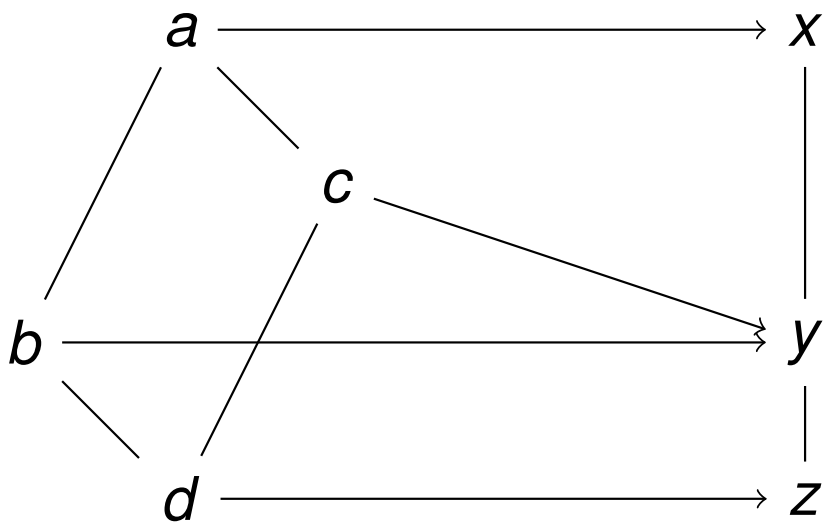


Tutaj $\{a, b, c, d\}$ jest podkratą całej kraty, ale $\{a, b, c, e\}$, choć sam jest kratą, nie jest podkratą całej kraty.

- **Twierdzenie**. Dowolny homomorfizm f krat L_1 i L_2 jest przekształceniem monotonicznym, czyli dla wszystkich $x, y \in L_1$: jeśli $x \leqslant y$, to $f(x) \leqslant f(y)$.
- **Dowód**. Niech $x \leqslant y$. Wtedy $x \vee y = y$, a zatem $f(x \vee y) = f(y)$. Skoro f jest homomorfizmem, to $f(x) \vee f(y) = f(y)$, a to oznacza, że $f(x) \leqslant f(y)$.

□

- Implikacja odwrotna nie zachodzi, co pokazuje następujący kontrprzykład:



- Jeśli $(L, \leqslant)$ jest kratą, to $[a, b] = \{x \in L : a \leqslant x \leqslant b\}$ nazywamy przedziałem o końcach a i b.
- Jeśli $[a, b] = \{a, b\}$, to mówimy, że a bezpośrednio poprzedza b i piszemy wtedy $a \prec b$.
- Łańcuchem jest każdy liniowo uporządkowany podzbiór kraty.
- Antyłańcuchem jest każdy podzbiór kraty złożony wyłącznie z elementów nieporównywalnych względem porządku kraty.
- Element najmniejszy kraty nazywamy jej *zerem* (**0**, o ile istnieje). Element największy kraty nazywamy jej *jedynką* (**1**, o ile istnieje).
- Krata jest *ograniczona z góry (z dołu)* jeśli istnieje jej jedynka (zero). Krata jest ograniczona, jeśli jest ograniczona z góry i z dołu. W kratach ograniczonych $a \wedge \mathbf{1} = a$ i $a \vee \mathbf{0} = a$. W kratach ograniczonych możemy określić pojęcie uzupełnienia elementu kraty. Element b nazywamy uzupełnieniem elementu a, jeśli $a \wedge b = \mathbf{0}$ i $a \vee b = \mathbf{1}$.
- Kratą dualną do kraty $(L, \leqslant)$ nazywamy kratę $(L, \geqslant)$.

- Elementy minimalne w $(L - \{\mathbf{0}\}; \leqslant)$ nazywamy *atomami*.
- Elementy maksymalne w $(L - \{\mathbf{1}\}; \leqslant)$ nazywamy *koatomami*.
- Krata jest *atomowa*, jeśli każdy jej niezerowy element jest niemniejszy od pewnego atomu.
- Krata jest *bezatomowa*, jeśli nie ma atomów.
- Każda krata skończona jest atomowa.
- Dla dowolnego zbioru X krata $(\wp(X), \cap, \cup)$ jest atomowa.
- Niech elementami L będą sumy skończonej liczby przedziałów półdomkniętych (tj. $(-\infty, a), [b, c), [d, +\infty), (-\infty, +\infty)$) zbioru liczb rzeczywistych. Wtedy $(L, \cap, \cup)$ jest bezatomowa.
- Niech X będzie zbiorem nieskończonym i niech $\sim \subseteq \wp(X) \times \wp(X)$ będzie relacją taką, że $A \sim B$ zachodzi wtedy i tylko wtedy, gdy $A \div B$ jest zbiorem skończonym. Wtedy $\sim$ jest kongruencją kraty $(\wp(X), \cap, \cup)$. Krata ilorazowa $(\wp(X)/\sim, \cap/\sim, \cup/\sim)$ jest bezatomowa.

- Niepusty podzbiór $\triangle$ kraty $(L; \leqslant)$ nazywamy *ideałem*, gdy:
  1. jeśli $x, y \in \triangle$, to $x \vee y \in \triangle$
  2. jeśli $x \in \triangle$ oraz $y \leqslant x$, to $y \in \triangle$.
- Ideał nazywamy właściwym, jeśli $\triangle \neq L$. Ideał właściwy $\triangle$ nazywamy ideałem pierwszym, jeśli $a \wedge b \in \triangle$ implikuje, że $a \in \triangle$ lub $b \in \triangle$. Jeśli krata L ma zero, to każdy jej ideał zawiera zero.
- Najmniejszy ideał, zawierający zbiór $X \subseteq L$ nazywamy ideałem generowanym przez X. Jeśli $X = \{a\}$, to ideał ten nazywamy ideałem głównym (generowanym przez a) i oznaczamy przez $(a]$.
- Każdy ideał w L jest podkratą kraty L. Zbiór wszystkich ideałów kraty L jest kratą: kresem dolnym dwóch ideałów jest ich iloczyn teoriomnogościowy, a kresem górnym ideał generowany przez ich teoriomnogościową sumę.
- Ideałem maksymalnym nazywamy każdy ideał właściwy, który nie zawiera się w żadnym ideale różnym od niego. W kracie skończonej ideałami maksymalnymi są ideały główne generowane przez koatomy.

- Niepusty podzbiór ∇ kraty $(L; \leqslant)$ nazywamy *filtrem*, gdy:
  1. jeśli $x, y \in \nabla$, to $x \wedge y \in \nabla$
  2. jeśli $x \in \nabla$ oraz $x \leqslant y$, to $y \in \nabla$.
- Filtr w L jest właściwy, jeśli jest różny od L. Każdy filtr w L jest podkratą kraty L. Jeśli krata $(L, \leqslant)$ ma jedynkę $\mathbf{1}$, to zbiór $\{\mathbf{1}\}$ jest jej filtrem, nazywanym *filtrem jednostkowym*.
- Dla dowolnego $x \in L$ zbiór $\{y \in L : x \leqslant y\}$ jest filtrem, nazywanym *filtrem głównym generowanym przez x*. Filtr, który nie jest główny, nazywamy *niegłównym*. Filtr główny, generowany przez $\{a\}$ oznaczamy $[a)$.
- Zbiór wszystkich filtrów kraty L jest kratą: kresem dolnym dwóch filtrów jest tu ich iloczyn teoriomnogościowy, a kresem górnym filtr generowany przez ich teoriomnogościową sumę.
- Filtrem maksymalnym (ultrafiltrem) nazywamy każdy filtr właściwy, który nie jest zawarty w żadnym różnym od niego filtrze. W kracie skończonej filtrami maksymalnymi są filtry główne generowane przez atomy kraty.

Twierdzenie. W dowolnej kracie $(L, \wedge, \vee)$:

1. $(a \wedge b) \vee (a \wedge c) \leqslant a \wedge (b \vee c)$ oraz $a \vee (b \wedge c) \leqslant (a \vee b) \wedge (a \vee c)$
2. Jeśli $c \leqslant a$, to $(a \wedge b) \vee c \leqslant a \wedge (b \vee c)$. Jeśli $a \leqslant c$, to $a \vee (b \wedge c) \leqslant (a \vee b) \wedge c$.
3. $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leqslant (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$

- **Dowód**. 1) Ponieważ $b \leqslant b \vee c$ oraz jeśli $y \leqslant x$, to $a \wedge y \leqslant a \wedge x$, więc $a \wedge b \leqslant a \wedge (b \vee c)$. Podobnie, ponieważ $c \leqslant b \vee c$ oraz jeśli $y \leqslant x$, to $a \wedge y \leqslant a \wedge x$, więc $a \wedge c \leqslant a \wedge (b \vee c)$. A zatem $(a \wedge b) \vee (a \wedge c) \leqslant a \wedge (b \vee c)$.
- Dalej, mamy $a \vee (b \wedge c) \leqslant a \vee b$ oraz $a \vee (b \wedge c) \leqslant a \vee c$, a zatem $a \vee (b \wedge c) \leqslant (a \vee b) \wedge (a \vee c)$.
- 2) Niech $c \leqslant a$. Trzeba pokazać, że $a \wedge b \leqslant a \wedge (b \vee c)$ oraz $c \leqslant a \wedge (b \vee c)$. Skoro $b \leqslant b \vee c$, to $a \wedge b \leqslant a \wedge (b \vee c)$. Ponieważ $c \leqslant b \vee c$, więc $a \wedge c \leqslant a \wedge (b \vee c)$. Skoro $c \leqslant a$, to $a \wedge c = c$ oraz $c \leqslant a \wedge (b \vee c)$. A zatem $(a \wedge b) \vee c \leqslant (a \wedge b) \vee (a \wedge c)$. Podobnie pokazujemy, że jeśli $a \leqslant c$, to $a \vee (b \wedge c) \leqslant (a \vee b) \wedge c$.

- 3) Trzeba pokazać, że:
  $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leqslant a \vee b$
  $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leqslant b \vee c$
  $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leqslant c \vee a$.
- Mamy:
  $a \wedge b \leqslant b \leqslant a \vee b$, a więc $a \wedge b \leqslant a \vee b$
  $b \wedge c \leqslant b \leqslant a \vee b$, a więc $b \wedge c \leqslant a \vee b$
  $a \wedge c \leqslant a \leqslant a \vee b$, a więc $c \wedge a \leqslant a \vee b$
- A zatem $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leqslant a \vee b$. W podobny sposób pokazujemy, że $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leqslant b \vee c$ oraz $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leqslant c \vee a$.

- Krata jest *zupełna*, jeśli każdy jej podzbiór ma kres dolny oraz kres górny. Kres dolny zbioru A oznaczamy zwykle przez $\bigwedge A$, a kres górny przez $\bigvee A$. Każda krata zupełna L ma element największy $\mathbf{1} = \bigvee L$ oraz element najmniejszy $\mathbf{0} = \bigwedge L$.
  1. Krata $(\wp(X); \cap, \cup)$ wszystkich podzbiorów zbioru X jest zupełna. Kresem dolnym rodziny podzbiorów jest ich iloczyn, a kresem górnym ich suma.
  2. Krata $(\mathbb{N}_+, \mathit{NWD}, \mathit{NWW})$ nie jest zupełna.
  3. Jeśli $\mathbf{A}$ jest dowolną algebrą, to zarówno rodzina wszystkich jej podalgebr, jak i rodzina wszystkich jej kongruencji jest kratą zupełną.
  4. Jeśli L jest kratą ograniczoną, to kraty jej ideałów i filtrów są zupełne.

- Operatorem domknięcia na zbiorze A nazywamy funkcję, $C : \wp(A) \to \wp(A)$ taką, że:
  1. $X \subseteq C(X)$
  2. $C(C(X)) = C(X)$
  3. jeśli $X \subseteq Y$, to $C(X) \subseteq C(Y)$.
- Jeśli C jest operatorem domknięcia na A, to każdy zbiór $X \subseteq A$ taki, że $X = C(X)$ nazywamy zbiorem C-domkniętym. Rodzina wszystkich zbiorów C-domkniętych jest zamknięta na iloczyny dowolnych swoich podrodzin. Ponadto, rodzina ta jest kratą zupełną. Kresem dolnym zbioru jej elementów jest ich iloczyn, a kresem górnym C-domknięcie ich sumy.
- **Twierdzenie** (o reprezentacji krat zupełnych). Dla dowolnej kraty zupełnej $(L, \leqslant)$ istnieje operator domknięcia C na zbiorze L taki, że $(L, \leqslant)$ jest izomorficzna z kratą wszystkich zbiorów C-domkniętych.
- **Dowód**. Dla $X \subseteq L$ niech $C(X) = (\bigvee X]$. Pokażemy, że C jest operatorem domknięcia.

- *Zwrotność*. Jeśli $a \in X$, to $a \leqslant \bigvee X$, a więc $a \in C(X)$.
- *Idempotencja*. Mamy $\bigvee X \leqslant \bigvee C(X)$. Jeśli $a \in C(X)$, to $a \leqslant \bigvee X$, a zatem $\bigvee C(X) \leqslant \bigvee X$. Mamy więc $\bigvee X = \bigvee C(X)$, a stąd $(\bigvee X] = (\bigvee C(X)]$.
- *Monotoniczność*. Jeśli $X \subseteq Y$, to $\bigvee X \subseteq \bigvee Y$, co implikuje, że $(\bigvee X] \subseteq (\bigvee X]$.
- *Izomorfizm*. Niech $F = \{C(X) : X \subseteq L\}$. Wtedy $(F, \subseteq)$ jest kratą zupełną. Niech $f : L \to F$ będzie funkcją taką, że $f(a) = (a]$ (czyli $f(a) = C(\{a\})$). Wtedy f jest homomorfizmem. Ponieważ $F = \{(a] : a \in L\}$, więc f jest surjekcją. Jeśli $f(a) = f(b)$, to $(a] = (b]$, a zatem $a = b$, czyli f jest injekcją. Pokazaliśmy więc, że $(L, \leqslant) \cong (F, \subseteq)$.

□

- Mówimy, że krata $(L, \leqslant)$ jest *modularna*, jeśli dla wszystkich $a, b, c \in L$: jeżeli $c \leqslant a$, to $a \wedge (b \vee c) = (a \wedge b) \vee c$.
  1. Krata M_3 (diament) jest modularna.
  2. Krata N_5 (pentagon) nie jest modularna.
  3. Dowolny łańcuch jest kratą modularną.
  4. Krata jest modularna wtedy i tylko wtedy, gdy nie zawiera jako podkraty kraty N_5.
  5. Krata jest modularna wtedy i tylko wtedy, gdy $((a \wedge c) \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$.

- Mówimy, że krata $(L, \leqslant)$ jest *dystrybutywna*, jeśli dla wszystkich $x, y, z \in X$:
  A. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
  B. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.
  1. Warunki A i B są równoważne.
  2. Krata wszystkich podzbiorów dowolnego zbioru X jest dystrybutywna.
  3. Krata M_3 (diament) nie jest dystrybutywna.
  4. Krata N_5 (pentagon) nie jest dystrybutywna.
  5. Każda krata dystrybutywna jest modularna.
  6. Każda krata, która ma mniej niż 5 elementów jest dystrybutywna.
- **Twierdzenie** (Birkhoff). Następujące warunki są równoważne:
  1. Krata $(L, \wedge, \vee)$ jest dystrybutywna.
  2. W kracie $(L, \wedge, \vee)$ spełniony jest warunek:
     $(x \wedge y) \vee (x \wedge z) \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$.
  3. $(L, \wedge, \vee)$ nie zawiera, jako podkraty, ani N_5 ani M_3.

- **Twierdzenie**. Niech $(L, \wedge, \vee)$ będzie kratą dystrybutywną z zerem **0** i jedynką **1**. Wtedy istnieje co najwyżej jedno uzupełnienie dowolnego jej elementu.
- **Dowód**. Przypuśćmy, że element a ma dwa różne uzupełnienia a_1 i a_2. Wtedy:
  1. $a_1 =$
  2. $\mathbf{1} \wedge a_1 =$
  3. $(a \vee a_2) \wedge a_1 =$
  4. $(a \wedge a_1) \vee (a_2 \wedge a_1) =$
  5. $\mathbf{0} \vee (a_2 \wedge a_1) =$
  6. $a_2 \wedge a_1$.
- Tak więc, $a_1 \leqslant a_2$. Zamieniając w powyższym rozumowaniu a_1 na a_2 oraz a_2 na a_1 otrzymamy $a_2 \leqslant a_1$.
- Ostatecznie więc $a_1 = a_2$.

W kratach M_3 i N_5 pewne elementy mają więcej niż jedno uzupełnienie.

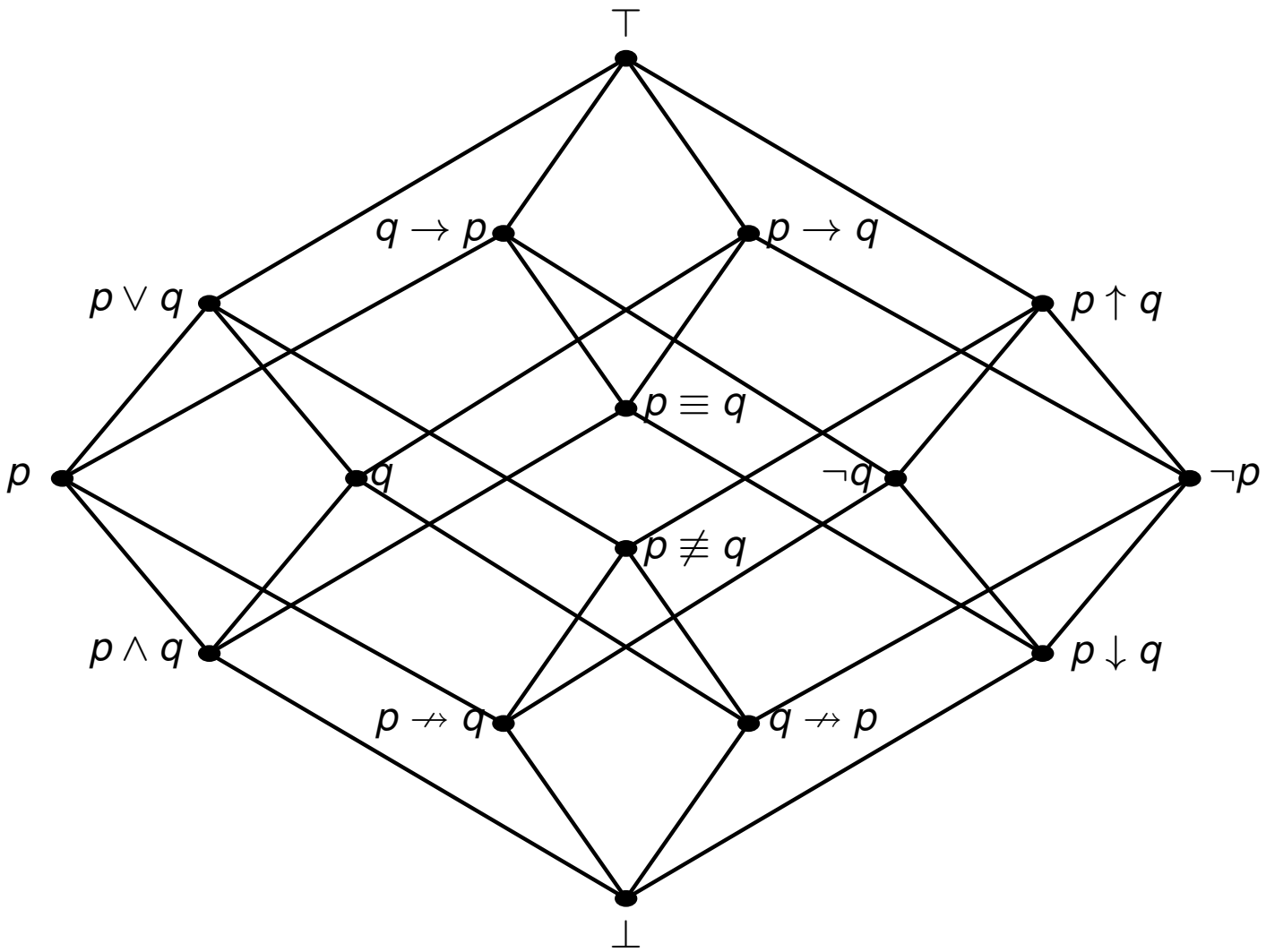
Algebrę $(B, \wedge, \vee, -, 0, 1)$ nazywamy *algebrą Boole'a*, jeśli $(B, \wedge, \vee, 0, 1)$ jest kratą dystrybutywną z zerem 0 i jedynką 1, $-$ jednoargumentową operacją uzupełnienia, dla każdego elementu $x \in B$ istnieje jego *uzupełnienie*, czyli element $-x$ (oznaczany też przez x') taki, że:

1. $(x \vee (-x)) = 1$
2. $(x \wedge (-x)) = 0$.

Tak więc, algebra $(B, \wedge, \vee, -, 0, 1)$ jest algebrą Boole'a, jeśli spełnia ona następujące warunki:

$(B1)$	$a \wedge b = b \wedge a$	$(B1')$	$a \vee b = b \vee a$
$(B2)$	$a \wedge a = a$	$(B2')$	$a \vee a = a$
$(B3)$	$a \wedge (b \wedge c) = (a \wedge b) \wedge c$	$(B3')$	$a \vee (b \vee c) = (a \vee b) \vee c$
$(B4)$	$a \wedge 1 = a$	$(B4)'$	$a \vee 0 = a$
$(B5)$	$a \wedge (-a) = 0$	$(B5)'$	$a \vee (-a) = 1$
$(B6)$	$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$		

- $\mathbf{2} = (\{0,1\}, \wedge, \vee, -, 0, 1)$, gdzie $(\{0,1\}, \wedge, \vee)$ jest dwuelementową kratą, $-0 = 1$, $-1 = 0$.
- $\mathbf{1} = (\{\emptyset\}, \wedge, \vee, -, \emptyset, \emptyset)$.
- $(\wp(X), \cap, \cup, -, \emptyset, X)$ jest algebrą Boole'a, dla dowolnego zbioru X.
- Każde ciało zbiorów jest algebrą Boole'a.
- Niech T będzie zbiorem tez klasycznego rachunku zdań (przy ustalonej aksjomatyce i regułach wnioskowania). Relacja $\sim$ określona dla formuł φ, ψ języka tego rachunku przez warunek: $\varphi \sim \psi$ wtedy i tylko wtedy, gdy $\varphi \leftrightarrow \psi \in T$ jest równoważnością. Jej klasy równoważności tworzą algebrę Boole'a:
  - $[\varphi \wedge \psi]_\sim = [\varphi]_\sim \wedge [\psi]_\sim$,
  - $[\varphi \vee \psi]_\sim = [\varphi]_\sim \vee [\psi]_\sim$,
  - $[\neg\psi]_\sim = -[\psi]_\sim$,
  - $0 = [\bot]_\sim$,
  - $1 = [\top]_\sim$.
- $(\{a, b\}, \wedge, \vee, -, 0, 1)$, gdzie $a \neq b$, $a \wedge b = 0$, $a \vee b = 1$ (wtedy $b = -a$) jest algebrą Boole'a.


$\top$
$q \to p$
$p \to q$
$p \vee q$
$p \uparrow q$
$p \equiv q$
p
q
$\neg q$
$\neg p$
$p \not\equiv q$
$p \wedge q$
$p \downarrow q$
$p \not\to q$
$q \not\to p$
$\bot$

Twierdzenie (o reprezentacji algebr Boole'a). Każda algebra Boole'a jest izomorficzna z pewnym ciałem zbiorów.

- Atomy algebry Boole'a $\mathbf{A} = (A, \wedge, \vee, -, 0, 1)$ to atomy kraty $(A, \wedge, \vee)$.
- Mówimy, że algebra $\mathbf{A} = (A, \wedge, \vee, -, 0, 1)$ jest atomowa (bezatomowa), gdy krata $(A, \wedge, \vee)$ jest atomowa (bezatomowa). Zbiór atomów algebry $\mathbf{A}$ oznaczamy przez $At(\mathbf{A})$.
- Mówimy, że algebra $\mathbf{A} = (A, \wedge, \vee, -, 0, 1)$ jest atomistyczna, gdy każdy jej element jest sumą atomów.
  Twierdzenie. Algebra Boole'a $\mathbf{A}$ jest atomowa wtedy i tylko wtedy, gdy jest atomistyczna.

Twierdzenie. Algebra Boole'a $\mathbf{A}$ jest atomowa i zupełna wtedy i tylko wtedy, gdy jest izomorficzna z ciałem *wszystkich* podzbiorów pewnego zbioru.

Twierdzenie. Dowolne dwie przeliczalne bezatomowe algebry Boole'a są izomorficzne.

Rozszerzanie dziedzin liczbowych:

Równanie	Nie ma rozwiązania w	Ma rozwiązanie w
$x + 3 = 0$	$\mathbb{N}$	$\mathbb{Z}$
$2x = 3$	$\mathbb{Z}$	$\mathbb{Q}$
$x^2 = 2$	$\mathbb{Q}$	$\mathbb{R}$
$x^2 + 1 = 0$	$\mathbb{R}$	$\mathbb{C}$

Każdy wielomian jednej zmiennej stopnia n o współczynnikach z $\mathbb{C}$ ma w $\mathbb{C}$ liczbę łącznych krotności pierwiastków równą n.
Ciało $\mathbb{C}$ jest algebraicznie domknięte.
Najwcześniej „oswojone” zbiory liczbowe: $\mathbb{N}$ i $\mathbb{Q}_+$.
Teoria liczb rzeczywistych: wiek XIX.
Długie „oswajanie” zbiorów liczbowych $\mathbb{Z}$ i $\mathbb{C}$.
Aksjomat Archimedesa i struktury niearchimedesowe.
Arytmetyka (nieskończonych) liczb porządkowych i kardynalnych.

Które własności działań arytmetycznych są „naturalne”?

przemienność	$a+b=b+a$, $a\cdot b=b\cdot a$
łączność	$(a+b)+c=a+(b+c)$, $(a\cdot b)\cdot c=a\cdot(b\cdot c)$
rozdzielność	$a\cdot(b+c)=a\cdot b+a\cdot c$
potęgowanie	$a^{b+c}=a^b\cdot a^c$, $(a^b)^c=a^{b\cdot c}$, $(a\cdot b)^c=a^c\cdot b^c$

Wszystkie te prawa obowiązują w: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
„Naturalne” (zgodne z działaniami arytmetycznymi) struktury porządkowe w systemach liczbowych:

- $\mathbb{N}$: dyskretny porządek $<$ z elementem najmniejszym, bez elementu największego;
- $\mathbb{Z}$: dyskretny porządek $<$ bez elementu najmniejszego i największego;
- $\mathbb{Q}$: gęsty porządek $<$ bez elementu najmniejszego i największego;
- $\mathbb{R}$: ciągły porządek $<$ bez elementu najmniejszego i największego;
- $\mathbb{C}$: nie istnieje porządek zgodny z działaniami arytmetycznymi.

Definiowanie i rozszerzanie systemów liczbowych:

- Metoda genetyczna.
- Metoda aksjomatyczna.

Reprezentacje systemów liczbowych:

- Zapis liczb przy różnych podstawach.
- Reprezentacje geometryczne.

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.
- Własności działań: łączność, przemienność, rozdzielność.
- Homomorfizm, izomorfizm.
- Kongruencja.
- Struktura ilorazowa.
- Grupa, pierścień, ciało.
- Kraty i algebry Boole'a.