MATEMATYCZNE PODSTAWY KOGNITYWISTYKI

WYKŁAD 6: STRUKTURY ALGEBRAICZNE

KOGNITYWISTYKA UAM, 2016–2017

JERZY POGONOWSKI
Zakład Logiki i Kognitywistyki UAM
pogon@amu.edu.pl

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. Na poprzednim wykładzie poznaliśmy jeden rodzaj tego typu struktur: zbiory uporządkowane (częściowo, liniowo, dyskretnie, gęsto, w sposób ciągły, dobrze uporządkowane). Słuchacze pamiętają ze szkoły, że 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.).

Każda dyscyplina matematyczna bada jakieś rodzaje struktur. Obecnie obowiązującym standardem jest charakteryzowanie tych 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.

Aksjomatyczne opisy systemów liczbowych powstały dopiero w wieku XIX. Wcześniej określano nowe rodzaje liczb metodą *genetyczną*. W największym skrócie metoda ta polega na tym, że mając jakiś rodzaj liczb (ze stosownymi operacjami arytmetycznymi) zauważamy, że na tych liczbach pewnych operacji wykonać nie można. Rozszerzamy wtedy znane uniwersum liczbowe tak, aby – zacho-

wując „stare" operacje, można było wykonywać na wprowadzonych liczbach także „nowe" operacje. Zobaczymy za chwilę, jak z liczb naturalnych tworzy się liczby całkowite, z całkowitych wymierne, a z wymiernych rzeczywiste, posługując się tą metodą.

Należy podkreślić, że mówiąc o systemach liczbowych mamy zawsze na uwadze jakiś rodzaj liczb wraz z określonymi na nich działaniami arytmetycznymi (oraz, ewentualnie, relacjami porządkowymi). Mówiąc nieco metaforycznie, liczby danego rodzaju tworzą spójną strukturę, w której „miejsce" każdego elementu określone jest przez zależności, w które wchodzi on z innymi elementami. 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.

1 Struktury relacyjne i algebry

Przez *strukturę relacyjną* rozumiemy układ złożony ze zbioru (*uniwersum struktury*) oraz określonych na tym zbiorze relacji i funkcji. Rozważać będziemy jedynie prosty przypadek, gdy owych relacji oraz funkcji jest jedynie skończenie wiele.

Dla dowolnego zbioru A niech A^* oznacza zbiór wszystkich skończonych potęg kartezjańskich zbioru A, czyli $A^* = \{A, A^2, A^3, \ldots\}$.

Strukturą relacyjną nazywamy dowolny układ:

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

gdzie:

1. A jest dowolnym zbiorem;
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 UA^* w zbiór A;
4. $\{a_k : k \in K\}$ jest zbiorem elementów (wyróżnionych) zbioru A.

Zbiory I, J, K są tu dowolnymi zbiorami indeksów. Zwykle są to pewne zbiory skończone (nie jest tak jednak np. gdy przestrzenie topologiczne traktujemy jak struktury relacyjne – wtedy rodzina zbiorów otwartych przestrzeni jest z reguły nieskończona).

Jeśli $\mathbf{A} = (A, \{r_i : i \in I\}, \{f_j : j \in J\}, \{a_k : k \in K\})$ jest strukturą relacyjną, to zbiór A nazywamy *uniwersum* tej struktury i oznaczamy przez $dom(\mathbf{A})$.

UWAGA. Zwykle struktury relacyjne i algebry zapisujemy w ten sposób, że po uniwersum wyliczamy kolejno rozważane relacje i funkcje (ewentualnie też elementy wyróżnione). Tak też będziemy postępowali nieco dalej w tym wykładzie. W ogólnych definicjach na początku piszemy o *zbiorach* relacji, funkcji oraz elementów wyróżnionych, chociaż bardziej właściwe byłoby mówienie o ich *ciągach*, co jednak wymagałoby z kolei uporządkowania zbiorów indeksów i komplikowałoby ogólną postać definicji. Dopuszczamy się więc różnych świństewek w notacji, ufając jednak, że zostanie nam to wybaczone. Gdy przejdziemy do przykładów i zastosowań omawianych pojęć, sytuacja będzie o wiele prostsza pod względem używanej symboliki. Dodajmy jeszcze, że w wielu podręcznikach stosuje się – często bez ostrzeżenia – takie oraz podobne świństewka w notacji. Nie jesteśmy więc osamotnieni i czujemy się zatem trochę usprawiedliwieni, także z nich korzystając. Jak pisał Stanisław Ignacy Witkiewicz:

> *Ciężko jest żyć w plugawej naszej atmosferze,*
> *Czasami, ach, wprost nawet kogoś z boku litość bierze —*
> *Pociecha w tym, że gorzej być plugawcem, ach, samemu,*
> *Bo nic już nie pomoże, ach, takiemu.*

Każdej relacji ze zbioru $\{r_i : i \in I\}$ oraz funkcji ze zbioru $\{f_j : j \in J\}$ można oczywiście w jednoznaczny sposób przypisać jej liczbę argumentów, co pozwala na precyzyjne mówienie o *typie* (*sygnaturze*) rozważanej struktury. Bez wdawania się w szczegóły powiedzmy jedynie, że typ struktury zawiera informację o tym ile argumentów ma każda jej relacja i funkcja oraz w jakiej kolejności uwzględniamy te relacje i funkcje.

Niech $\mathbf{A} = (A, \{r_i : i \in I\}, \{f_j : j \in J\}, \{a_k : k \in K\})$ będzie strukturą relacyjną. Mówimy, że $\mathbf{A}$ jest:

1. *strukturą relacyjną czystą*, gdy $J = K = \emptyset$;
2. *algebrą*, gdy $I = \emptyset$.

W praktyce, czasami używa się terminu *struktura relacyjna* zamiast *struktura relacyjną czysta*, odróżniając w ten sposób struktury wyposażone jedynie w relacje od algebr, czyli struktur wyposażonych jedynie w funkcje. Powinno być również jasne, że np. przez *algebrę uporządkowaną* rozumie się algebrę z dodaną relacją porządkującą uniwersum.

Najczęściej będziemy mieli do czynienia z algebrami z funkcjami jedno- oraz dwuargumentowymi. Zamiast terminu *funkcja* w takich algebrach używa się także terminów: *operacja* lub *działanie* (wewnętrzne). Zgodnie z powszechnym użyciem, będziemy stosowali notację *infiksową*: jeśli np. $\oplus : A \times A \to A$ jest operacją

dwuargumentową, to wartość $\oplus(x, y)$ będziemy często zapisywali w postaci $x \oplus y$. Podobnie, np. dla operacji jednoargumentowej $\ominus : A \to A$ w miejsce $\ominus(x)$ będziemy często pisali $\ominus x$.

Jak pamiętamy z wykładu poświęconego kombinatoryce, istnieje m^n funkcji ze zbioru n-elementowego w zbiór m-elementowy. Tak więc, jeśli A ma n elementów, to na zbiorze A można określić n^{n^2} operacji dwuargumentowych. Tak więc, jest $2^{2^2} = 16$ operacji dwuargumentowych na zbiorze dwuelementowym oraz $3^{3^2} = 19683$ operacji dwuargumentowych na zbiorze trójelementowym.

Dla zbiorów skończonych, operacje na nich określone często wygodnie jest reprezentować odpowiednimi tabelkami: wiersze i kolumny takiej tabelki są numerowane poszczególnymi elementami uniwersum, a na przecięciu wiersza odpowiadającego elementowi x oraz kolumny odpowiadającej elementowi y wpisujemy wartość operacji, np. $x \oplus y$ dla tych argumentów.

Dla przykładu, niech $A = \{0, 1, 2\}$, a operacja $\oplus^3 : A \times A \to A$ niech dla argumentów x oraz y daje wartość równą reszcie z dzielenia $x + y$ przez 3. Wtedy tabelka tej operacji wygląda następująco:

$\oplus^3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Na tym samym zbiorze $A = \{0, 1, 2\}$ zdefiniujmy operację $\otimes^3 : A \times A \to A$. Niech dla argumentów x oraz y daje ona wartość równą reszcie z dzielenia $x \cdot y$ przez 3. Wtedy tabelka tej operacji wygląda następująco:

$\oplus^3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

W edukacji szkolnej słuchacze poznali przykłady struktur relacyjnych oraz algebr, m.in.:
PRZYKŁADY.

1. Zbiór $\mathbb{N}$ liczb naturalnych wraz z operacjami dodawania i mnożenia, uporządkowany przez relację mniejszości.

2. Zbiór $\mathbb{Z}$ liczb całkowitych wraz z operacjami dodawania, odejmowania oraz mnożenia, uporządkowany przez relację mniejszości.

3. Zbiór $\mathbb{Q}$ liczb naturalnych wraz z operacjami dodawania, odejmowania, mnożenia oraz dzielenia, uporządkowany przez relację mniejszości.

4. Zbiór $\mathbb{R}$ liczb rzeczywistych wraz z operacjami dodawania, odejmowania, mnożenia oraz dzielenia, uporządkowany przez relację mniejszości.

5. Zbiór wszystkich wielomianów o współczynnikach rzeczywistych wraz z operacjami dodawania i mnożenia wielomianów.

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

Do tej pory zakładaliśmy, że słuchacze posiadają *intuicyjną* wiedzę o tych strukturach. W dalszej części wykładu pokażemy, jak *konstruować* struktury liczb całkowitych, wymiernych oraz rzeczywistych, wychodząc od struktury liczb naturalnych.

UWAGA. We wszystkich dotychczasowych wykładach ilustrowaliśmy wprowadzane pojęcia przykładami czysto matematycznymi, z nielicznymi wyjątkami. Słuchacze mogli odnieść (mylne!) wrażenie, że właściwie matematyka zajmuje się jedynie sama sobą, w oderwaniu od Świata oraz Życia. Pojęcia dotyczące struktur relacyjnych oraz algebr znajdują jednak wielorakie owocne zastosowania. Badamy systemy fizyczne, składające się z obiektów fizycznych i wiążących je relacji, badamy skupiska ludzkie, w których również zachodzą rozmaitego typu zależności, badamy języki etniczne, w których np. ich zasób leksykalny opisywany jest jako struktura relacyjna złożona z *leksemów*, powiązanych zależnościami semantycznymi (synonimia, antonimia, hiponimia, bliskoznaczność, itp.). Wszelkie ilościowe opisy zjawisk korzystają z porządkowych, algebraicznych i innych jeszcze własności funkcji i relacji składających się na te opisy. To, że w niniejszym wykładzie raczej unikamy (z reguły bardzo skomplikowanych) przykładów z Życia spowodowane jest tym, że w pozostających do naszej dyspozycji skromnych ramach czasowych możemy omówić jedynie najbardziej elementarne pojęcia, ilustrując je najprostszymi, matematycznymi przykładami.

1.1 Własności działań

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.

Niech $(A, \circ)$ będzie algebrą z jednym działaniem dwuargumentowym oraz elementem e neutralnym dla tego działania. Powiemy, że y jest elementem *odwrotnym* dla x (względem $\circ$), gdy $x \circ y = y \circ x = e$. Jeśli dla każdego elementu $x \in A$ istnieje dokładnie jeden element odwrotny, to jest on najczęściej oznaczany x^{-1} (z kontekstu wynika, jakie działanie bierzemy pod uwagę). Jeśli działanie ma element neutralny, to jest on wyznaczony jednoznacznie. Jeśli działanie jest łączne oraz istnieje element odwrotny do x, to jest on wyznaczony jednoznacznie.

Niech $(A, \oplus, \otimes)$ będzie algebrą z dwiema operacjami dwuargumentowymi. Powiemy, że operacja $\otimes$ jest względem operacji $\oplus$:

1. *lewostronnie rozdzielna*, gdy $x \otimes (y \oplus z) = (x \otimes y) \oplus (y \otimes z)$, dla wszystkich $x, y, z \in A$;
2. *prawostronnie rozdzielna*, gdy $(y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x)$, dla wszystkich $x, y, z \in A$;
3. *rozdzielna*, gdy jest ona lewo- i prawostronnie rozdzielna.

PRZYKŁADY.

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

1.2 Podstruktury

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 algebrami 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 $x_1, \ldots, x_n \in A_1$ oraz wszystkich n-argumentowych operacji f_j, mamy: $f_j(x_1, \ldots, x_n) \in A_1$.
PRZYKŁADY.

1. 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.

2. Podobnie, strukturę uporządkowaną $(\mathbb{N}, \leqslant)$ traktować możemy jako podstrukturę struktury $(\mathbb{R}, \leqslant)$.

3. Rozważmy zbiór wszystkich *symetrii* trójkąta równobocznego. Ma on sześć elementów: przekształcenie identycznościowe (obrót o 0°), obrót o 120°, obrót o 240° (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 identycznościowego oraz obu wspomnianych obrotów, z operacją składania przekształceń.

1.3 Homomorfizmy i izomorfizmy

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 $f : A_1 \to A_2$ jest *homomorfizmem* $\mathbf{A}_1$ w $\mathbf{A}_2$, gdy dla wszystkich $x_1, \ldots, x_n \in A_1$ 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. $f(f_j^1(x_1, \ldots, x_n)) = f_j^2(f(x_1), \ldots, f(x_n))$

2. jeśli zachodzi $r_i^1(x_1, \ldots, x_n)$, to zachodzi $r_i^2(f(x_1), \ldots, f(x_n))$.

Przypominamy, że funkcja $f : A \to B$ jest:

1. injekcją, gdy dla dowolnych $x, y \in A$: jeśli $f(x) = f(y)$, to $x = y$;

2. surjekcją (funkcją *na*), gdy dla każdego $y \in B$ istnieje $x \in A$ taki, że $y = f(x)$;

3. bijekcją (funkcją $1-1$, funkcją wzajemnie jednoznaczną na), gdy jest injekcją i surjekcją.

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 $\mathbf{A} \cong \mathbf{B}$.

W literaturze używa się terminów:

1. *monomorfizm* dla homomorfizmu, który jest injekcją;

2. *epimorfizm* dla homomorfizmu, który jest surjekcją;

3. *endomorfizm* dla homomorfizmu $\mathbf{A}$ w $\mathbf{A}$;

4. *automorfizm* dla izomorfizmu $\mathbf{A}$ na $\mathbf{A}$.

Często monomorfizmy nazywa się również *włożeniami*. Słuchacze niech nie będą przerażeni lub zbulwersowani tą mnogością terminów. Trzeba i warto pamiętać terminy: homomorfizm oraz izomorfizm. Pozostałe podajemy tu jedynie dla tych słuchaczy, którzy czytając samodzielnie jakiś tekst niespodziewanie natkną się na owe tajemnicze terminy.

PRZYKŁADY.

1. 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:

$f(\emptyset) = 1$

$f(\{1\}) = 2$

$f(\{2\}) = 3$

$f(\{3\}) = 5$

$f(\{1,2\}) = 6$

$f(\{1,3\}) = 10$

$f(\{2,3\}) = 15$

$f(\{1,2,3\}) = 30$

2. Funkcja logarytmiczna $\log : \mathbb{R}_+ \to \mathbb{R}$ jest homomorfizmem struktury $(\mathbb{R}_+, \cdot)$ w strukturę $(\mathbb{R}, +)$. Słuchacze pamiętają ze szkoły, że logarytm z iloczynu równy jest sumie logarytmów:

$$\log(x \cdot y) = \log x + \log y.$$

3. Rozważmy strukturę $\mathbb{K}_4 = (\{e, a, b, c\}, \circ)$, gdzie dwuargumentowe 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

Ta struktura (*grupa czwórkowa Kleina*) jest izomorficzna np. ze strukturą $(\wp(\{x, y\}), \div)$, czyli rodziną wszystkich podzbiorów dowolnego zbioru dwuelementowego wraz z operacją różnicy symetrycznej zbiorów $\div$, którą słuchacze znają z pierwszego wykładu.

Grupa czwórkowa Kleina jest również izomorficzna np. ze strukturą złożoną z wszystkich symetrii rombu (lub prostokąta) nie będącego kwadratem wraz ze składaniem przekształceń jako operacją dwuargumentową. Zauważmy, że rozważanymi symetriami są: identyczność (obrót o 0°), obrót o 180°, oraz dwie symetrie osiowe.

Istnieją dalsze ciekawe struktury izomorficzne z $\mathbb{K}_4$. Zauważmy jednak, że ta struktura nie jest izomorficzna ze strukturą $C_4 = (\{e, a, b, c\}, \bullet)$ (*grupą cykliczną rzędu cztery*), gdzie 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

1.4 Kongruencje

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 $x_1, \ldots, x_n$, wszystkich $y_1, \ldots, y_n$, wszystkich n-argumentowych relacji r_i oraz wszystkich n-argumentowych funkcji f_j:

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

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 $dom(\mathbf{A})$.

Wszystkie kongruencje dowolnej algebry tworzą kratę, będącą podkratą (tzw. kratę *zupełną*, czyli zawierającą kresy dowolnych zbiorów jej elementów) kraty wszystkich równoważności określonych na uniwersum tej algebry.
PRZYKŁADY.

1. 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: $x \equiv y (\text{mod } n)$ 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.
2. Relacja równoliczności zbiorów, określona w rodzinie wszystkich podzbiorów dowolnego zbioru X jest kongruencją struktury $(\wp(X), \cup, \cap)$.
3. W punkcie dotyczącym konstrukcji systemów liczbowych poznamy dalsze relacje kongruencji. Niektóre z nich (w interpretacji geometrycznej) zostały przedstawione w pliku zawierającym szczegółowy plan wykładów, umieszczonym na stronie wykładów.

1.5 Struktury ilorazowe

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:
   $r_i^E([x_1]_E, \ldots, [x_n]_E)$ wtedy i tylko wtedy, gdy $r_i(x_1, \ldots, x_n)$
3. dla każdej n-argumentowej funkcji f_j definiujemy funkcję f_j^E:
   $f_j^E([x_1]_E, \ldots, [x_n]_E) = [f_j(x_1, \ldots, x_n)]_E$

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

Kongruencje związane są z homomorfizmami algebr. Każda funkcja $f : A \to B$ wyznacza pewną relacje równoważności na A. Definiujemy mianowicie: $x \sim_f y$ wtedy i tylko wtedy, gdy $f(x) = f(y)$.

Jeśli $f : \mathbf{A} \to \mathbf{B}$ jest homomorfizmem algebry $\mathbf{A}$ na algebrę $\mathbf{B}$, to relacja $\sim_f$ zdefiniowana wzorem: $x \sim_f y$ wtedy i tylko wtedy, gdy $f(x) = f(y)$ jest kongruencją algebry $\mathbf{A}$.

Jeśli, z drugiej strony, E jest kongruencją algebry $\mathbf{A}$, to *odwzorowanie kanoniczne* $\pi_E : \mathbf{A} \to \mathbf{A}/E$ jest homomorfizmem.

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 $\mathbf{A}$.

Mówimy, że algebra $\mathbf{A}$ jest *prosta*, jeśli ma tylko dwie kongruencje: identyczność na $dom(\mathbf{A})$ oraz relację pełną na tym zbiorze.

Wprost z definicji widać, że algebra $\mathbf{A}$ jest prosta wtedy i tylko wtedy, gdy ma dokładnie dwa (z dokładnością do izomorfizmu) obrazy homomorficzne: samą siebie oraz algebrę *zdegenerowaną*, czyli jednoelementową.

PRZYKŁADY.

1. 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:

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

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

2. Rozważmy strukturę $(\wp(\mathbb{N}), \cup, \cap)$ oraz relację $\sim$, zdefiniowaną następująco:

   $A \sim B$ wtedy i tylko wtedy, gdy $1 \in A \cap B$ lub $1 \in \mathbb{N} - (A \cup B)$.

   Relacja $\sim$ jest równoważnością (co łatwo sprawdzić) i ma dokładnie dwie klasy abstrakcji: $[\mathbb{N}]_\sim$ oraz $[\emptyset]_\sim$. Do pierwszej z tych klas należą mianowicie wszystkie zbiory, do których należy liczba 1, a do drugiej wszystkie zbiory, do których nie należy liczba 1. Relacja ta jest kongruencją w strukturze $(\wp(\mathbb{N}), \cup, \cap)$, możemy więc określić działania $\cup^\sim$ oraz $\cap^\sim$ na jej klasach abstrakcji:

$\cup^\sim$	$[\emptyset]_\sim$	$[\mathbb{N}]_\sim$
$[\emptyset]_\sim$	$[\emptyset]_\sim$	$[\mathbb{N}]_\sim$
$[\mathbb{N}]_\sim$	$[\mathbb{N}]_\sim$	$[\mathbb{N}]_\sim$

$\cap^\sim$	$[\emptyset]_\sim$	$[\mathbb{N}]_\sim$
$[\emptyset]_\sim$	$[\emptyset]_\sim$	$[\emptyset]_\sim$
$[\mathbb{N}]_\sim$	$[\emptyset]_\sim$	$[\mathbb{N}]_\sim$

   Jeśli słuchacze dowiedzieli się już na kursie *Wprowadzenie do logiki* o *tabliczkach prawdziwościowych*, to z łatwością rozpoznają strukturę ilorazową $(\wp(\mathbb{N}), \cup, \cap)/_\sim$.

Na strukturach relacyjnych i na algebrach wykonywać można pewne *operacje*: można tworzyć ich sumy, iloczyny, różne rodzaje produktów, itd. W każdym z takich przypadków, oprócz określenia czym są uniwersa struktur otrzymywanych w wyniku takiej operacji trzeba też oczywiście stosownie określić jak operacje złożonej struktury definiowane są w terminach operacji ich struktur składowych. Można też pytać, jakie własności struktury składowych *zachowywane* są prze wykonywane na nich operacje. Jest to ładna problematyka algebraiczna, nie możemy jednak pozwolić sobie na obdarowanie nią słuchaczy, ze względu na ograniczone ramy czasowe tego usługowego kursu.

Struktury relacyjne oraz algebry mogą też być charakteryzowane i porównywane w terminach *semantycznych*, jako *modele* stosownych *teorii* matematycznych. O tej problematyce słuchacze być może usłyszą na bardziej zaawansowanym kursie logiki w przyszłości.

2 Konstrukcje systemów liczbowych

Pokażemy teraz, jak – przy wykorzystaniu pojęć porządkowych oraz algebraicznych – *skonstruować* systemy liczb: całkowitych, wymiernych oraz rzeczywistych, wychodząc od (opisanego aksjomatycznie) systemu liczb naturalnych.

2.1 Arytmetyka liczb naturalnych

Przez *algebrę Peana* rozumiemy każdą algebrę $\mathbf{A} = (A, f, a)$ taką, 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 $X \subset A$, jeśli $a \in X$ oraz $f(x) \in X$, o ile $x \in X$, dla wszystkich $x \in X$, to $X = A$.

Słuchacze z łatwością rozpoznają w powyższych warunkach założenia dotyczące struktury liczb naturalnych, z zerem jako elementem początkowym oraz następnikiem jako funkcją f. Ostatni z powyższych warunków jest oczywiście sformułowaniem zasady indukcji matematycznej.

Istnieje co najmniej jedna algebra Peana, co wynika z aksjomatów teorii mnogości (w szczególności, z aksjomatu nieskończoności, który gwarantuje istnienie co najmniej jednego zbioru nieskończonego).

Co więcej, istnieje – z dokładnością do izomorfizmu, jak mówi się w matematyce – tylko jedna algebra Peana. Oznacza to, innymi słowy, że dowolne dwie algebry Peana są izomorficzne. Ponadto, istnieje dokładnie jedna funkcja ustalająca ten izomorfizm. Dowód tego faktu, wykorzystujący *twierdzenie o definiowaniu przez indukcję* znajdą zainteresowani słuchacze np. w podręczniku Guzicki, Zakrzewski 2005 (strony: 200–202).

Możemy więc liczby naturalne (z wyróżnionym elementem początkowym 0 oraz operacją następnika, którą trochę nieściśle, ale zgodnie z Tradycją oznaczamy jako $f(x) = x + 1$, gdzie 1 jest bezpośrednim następnikiem 0) uważać za ową jedyną algebrę Peana, skoro ma ona te miłe własności, że istnieje i jest dokładnie jedna (z dokładnością do izomorfizmu). Tak też uczynimy: niech $\mathbb{N}$ oznacza odtąd uniwersum jedynej algebry Peana.

Wspomniane już twierdzenie o definiowaniu przez indukcję gwarantuje też, że istnieje dokładnie jedna funkcja dwuargumentowa $+$, która spełnia warunki:

1. $x + 0 = x$
2. $x + (y + 1) = (x + y) + 1$.

Istnieje też dokładnie jedna funkcja dwuargumentowa $\cdot$, która spełnia warunki:

1. $x \cdot 0 = 0$
2. $x \cdot (y + 1) = (x \cdot y) + x$.

Za pomocą funkcji dodawania $+$ możemy zdefiniować *zwykły* (*naturalny*) porządek $\leqslant$ liczb naturalnych: $x \leqslant y$ wtedy i tylko wtedy, gdy istnieje $z \in \mathbb{N}$ taka, że $x + z = y$. Jak zwykle, przez $x < y$ rozumiemy to, że $x \leqslant y$ oraz $x \neq y$.

Można wtedy udowodnić, że relacja $\leqslant$ jest dobrym porządkiem w zbiorze $\mathbb{N}$ (zob. np. Guzicki, Zakrzewski 2005, 204–205).

UWAGI.

1. Nasza podróż po świecie liczb zaczyna się zatem obiecująco: mamy dokładnie jedno uniwersum liczb naturalnych, z jednoznacznie określonymi działaniami dodawania i mnożenia, a ponadto uniwersum to jest dobrze uporządkowane. Gwarancją naszego dobrego samopoczucia jest teoria mnogości, w której aksjomaty *wierzymy*.

2. Giuseppe Peano (1858–1932) podał aksjomatykę dla liczb naturalnych w 1889 roku. Peano ma wielkie zasługi dla arytmetyki, analizy, geometrii, a także logiki matematycznej. W 1861 roku aksjomatykę dla arytmetyki podał Hermann Grassmann, o którym będzie jeszcze mowa.

3. Wspomniane wyżej twierdzenie o definiowaniu przez indukcję w odniesieniu do algebr Peana ma postać następującą:

   TWIERDZENIE. Niech $\mathbf{A} = (A, f, a)$ będzie algebrą Peana i niech $\mathbf{B} = (B, g, b)$ będzie dowolną algebrą tego samego typu. Wtedy istnieje dokładnie jedna funkcja $F : A \to B$ taka, że:

   (a) $F(a) = b$
   (b) $F(f(x)) = g(F(x))$ dla wszystkich $x \in A$.

4. Powyższa charakterystyka liczb naturalnych, odwołująca się do teorii mnogości, zadowala matematyków. Z kolei logicy zainteresowani są charakterystyką liczb naturalnych w pewnym standardowym systemie logicznym, jakim jest *logika pierwszego rzędu* (*klasyczny rachunek predykatów*). Tu napotykamy różne niespodzianki, o czym słuchacze dowiedzą się na dalszych etapach edukacji.

5. 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.

Następne rodzaje liczb (całkowite, wymierne, rzeczywiste) skonstruujemy, wykorzystując pojęcie struktury ilorazowej.

2.2 Liczby całkowite

Określamy relację $\approx_1 \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$:

$$(x, y) \approx_1 (u, v) \text{ wtedy i tylko wtedy, gdy } x + v = u + y.$$

Jest to relacja równoważności na zbiorze $\mathbb{N} \times \mathbb{N}$, co nietrudno sprawdzić, wykonując proste rachunki.
UWAGA. Ponieważ będziemy korzystali z kilku relacji równoważności w dalszych konstrukcjach, więc opatrujemy symbol $\approx$ indeksami (podobnie dla kolejno definiowanych operacji na liczbach).

Definiujemy zbiór wszystkich liczb *całkowitych*: $\mathbb{Z} = \mathbb{N}^2/\approx_1$.

Odwzorowanie $\varphi_1 : \mathbb{N} \to \mathbb{Z}$ określone wzorem $\varphi_1(k) = [(k, 0)]_{\approx_1}$ jest iniekcją, co jest widoczne wprost z definicji.

Trzeba jeszcze określić działania arytmetyczne na liczbach całkowitych, ich *dodawanie* $\oplus_1$, ich *odejmowanie* $\ominus_1$ oraz *mnożenie* $\odot_1$; określimy też ich uporządkowanie $\leqslant_1$:

1. $[(x, y)]_{\approx_1} \oplus_1 [(u, v)]_{\approx_1} = [x + u, y + v]_{\approx_1}$
2. $[(x, y)]_{\approx_1} \ominus_1 [(u, v)]_{\approx_1} = [x + v, y + u]_{\approx_1}$
3. $[(x, y)]_{\approx_1} \odot_1 [(u, v)]_{\approx_1} = [x \cdot u + y \cdot v, u \cdot y + x \cdot v]_{\approx_1}$
4. $[(x, y)]_{\approx_1} \leqslant_1 [(u, v)]_{\approx_1}$, jeśli $x + v \leqslant y + u$.

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 $\mathbb{Z}$:
   (a) $\varphi_1(m) \oplus_1 \varphi_1(n) = \varphi_1(m + n)$

(b) $\varphi_1(m) \odot_1 \varphi_1(n) = \varphi_1(m \cdot n)$

Humanistyczny termin „rozszerzenie" zastępujemy oczywiście matematycznym terminem „homomorfizm", a więc trzeba pokazać, że odwzorowanie φ_1 jest homomorfizmem struktury $(\mathbb{N}, \leqslant, +, \cdot)$ w strukturę $(\mathbb{Z}, \leqslant_1 \oplus_1, \odot_1)$.

Proponujemy słuchaczom samodzielne zmierzenie się z wykazaniem poprawności wyżej określonych działań i porządku oraz wykazaniem, że odwzorowanie φ_1 jest homomorfizmem.

Zauważmy jeszcze, że struktura $(\{[(x,0)]_{\approx_1} : x \in \mathbb{N}\}, \leqslant_1, \oplus_1, \odot_1)$, która sama jest podstrukturą struktury $(\mathbb{Z}, \leqslant_1, \oplus_1, \odot_1)$ jest izomorficzna ze strukturą $(\mathbb{N}, \leqslant, +, \cdot)$. 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.

UWAGI.

1. Podana wyżej definicja pochodzi od Hermanna Grassmanna (1809–1877). Grassmann ma zasługi w kilku dziedzinach: w matematyce głównie za sprawą oryginalnego ujęcia przestrzeni wektorowych. Pisał także o krystalografii, elektromagnetyzmie, mechanice. Wreszcie, był wybitnym językoznawcą, o czym słuchacze przekonają się na drugim roku studiów.
2. Interpretację geometryczną powyższej konstrukcji opisaliśmy w pliku zawierającym szczegółowy plan wykładów, dostępnym na stronie wykładów.
3. Liczby całkowite (a właściwie ujemne liczby całkowite) „oswajane" były przez kilka stuleci – początkowo odmawiano liczbom ujemnym prawa do legalnego istnienia w matematyce (a więc np. odrzucano *ujemne* rozwiązania równań liniowych z jedną niewiadomą). Praktyka badań matematycznych zmuszała jednak do rozważania liczb ujemnych. Właściwie dopiero ukazanie, że liczby całkowite tworzą dobrze określoną strukturę algebraiczną zakończyło proces ich oswajania.

4. Reliktem trudności w owym oswajaniu liczb ujemnych bywa trudność rozumienia przez dzieci dlaczego iloczyn liczb ujemnych jest dodatni. Tłumaczy się to w szkole na różne sposoby. Istotne jest to, że ta własność mnożenia liczb całkowitych związana jest z prawem rozdzielności mnożenia względem dodawania.

5. Strukturę $(\mathbb{Z}, \leqslant_1, \oplus_1, \odot_1)$ *wyobrażamy sobie* jako zbiór liniowo (dyskretnie) uporządkowany, bez elementu najmniejszego oraz największego.

2.3 Liczby wymierne

Teraz naszym punktem wyjścia będzie struktura $(\mathbb{Z}, \leqslant_1, \oplus_1, \odot_1)$, zdefiniowana powyżej. Przypominamy, że do jej określenia wykorzystaliśmy liczby naturalne oraz operację ich dodawania. Dla zdefiniowania liczb wymiernych wykorzystamy liczby całkowite oraz operację ich mnożenia.

Określamy relację $\approx_2 \subseteq (\mathbb{Z} \times (\mathbb{Z} - \{0\})) \times (\mathbb{Z} \times (\mathbb{Z} - \{0\}))$ wzorem:

$$(x, y) \approx_2 (u, v) \text{ wtedy i tylko wtedy, gdy } x \odot_1 v = y \odot_1 u.$$

Jest to relacja równoważności, co łatwo sprawdzić stosownym rachunkiem.

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 $\leqslant_2$:

- $[(x, y)]_{\approx_2} \oplus_2 [(u, v)]_{\approx_2} = [((x \odot_1 v) \oplus_1 (y \odot_1 u), (y \odot_1) v]_{\approx_2}$
- $[(x, y)]_{\approx_2} \ominus_2 [(u, v)]_{\approx_2} = [((x \odot_1 v) \ominus_1 (y \odot_1 u), (y \odot_1) v]_{\approx_2}$
- $[(x, y)]_{\approx_2} \odot_2 [(u, v)]_{\approx_2} = [(x \cdot_1 u, y \cdot_1 v)]_{\approx_2}$
- $[(x, y)]_{\approx_2} \oslash_2 [(u, v)]_{\approx_2} = [x \cdot_1 v, y \cdot_1 u]_{\approx_2}$, o ile $[(u, v)]_{\approx_2} \neq [(0, 1)]_{\approx_2}$
- $[(x, y)]_{\approx_2} \oslash_2 [(u, v)]_{\approx_2}$, jeśli $x \cdot_1 v \leqslant_1 y \cdot_1 u$, gdzie $0 <_1 y$, $0 <_1 v$.

Następnie trzeba pokazać, że te definicje są *poprawne* (wynik działania nie zależy od wyboru elementu z klasy abstrakcji) oraz że odwzorowanie $\varphi_2 : \mathbb{Z} \to \mathbb{Q}$ 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 $x \leqslant_1 y$, to $\varphi_2(x) \leqslant_2 \varphi_2(y)$.

Proponujemy słuchaczom samodzielne zmierzenie się z wykazaniem poprawności wyżej określonych działań i porządku oraz wykazaniem, że odwzorowanie φ_2 jest homomorfizmem.

Zauważmy, że:

1. Dla każdej liczby wymiernej $[(x,y)]_{\approx_2}$ mamy:
   $[(x,y)]_{\approx_2} = [(x,1)]_{\approx_2} \oslash_2 [(y,1)]_{\approx_2}$.
2. Liczbę wymierną $[(x,1)]_{\approx_2}$, na mocy Tradycji (oraz faktu, że φ_2 jest izomorfizmem struktur $(\mathbb{Z}, \leqslant_1, \oplus_1, \odot_1)$ oraz $(\{[(x,1)]_{\approx_2} : x \in \mathbb{Z}\}, \leqslant_1, \oplus_1, \odot_1)$) 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. Teraz widzimy, przy jakich założeniach zapis ten jest poprawny.

UWAGA. Zwykle używa się tego samego symbolu $+$ dla dodawania:

1. liczb naturalnych
2. liczb całkowitych
3. liczb wymiernych.

Podobnie, dla mnożenia w tych zbiorach używa się tego samego symbolu: $\cdot$.

Z czysto formalnego punktu widzenia jest to *niepoprawne*. To świństewko notacyjne, umocnione Tradycją, jest usprawiedliwione tym, że operacje $+$ i $\cdot$ określone dla liczb naturalnych „rozszerzają" się jednoznacznie (homomorficznie) do odpowiednich operacji na liczbach całkowitych i wymiernych.

W dalszym ciągu będziemy postępowali zgodnie ze wspomnianym zwyczajem, także dla innych funkcji i relacji w $\mathbb{Z}$ i $\mathbb{Q}$ używając symboli już wykorzystanych dla liczb naturalnych. Z kontekstu zawsze powinno być jasne, do jakiego rodzaju liczb stosujemy te operacje i relacje.

UWAGI.

1. Powyższa definicja liczb wymiernych również pochodzi od Hermanna Grassmanna.

2. Liczby wymierne (dodatnie) „oswojone” zostały w matematyce wcześniej niż liczby całkowite ujemne. Tak więc, porządek logiczny w konstruowaniu systemów liczbowych metodą genetyczną nie musi pokrywać się z porządkiem historycznym badania tych systemów.

3. Strukturę $(\mathbb{Q}, \leqslant_2, \oplus_2, \odot_2, \oslash_2)$ *wyobrażamy sobie* jako zbiór przeliczalny uporządkowany liniowo w sposób gęsty (ale nie ciągły!), bez elementu najmniejszego oraz bez elementu największego. Może warto w tym miejscu dodać, że istnieje tylko jeden (z dokładnością do izomorfizmu) tego typu porządek.

4. Przypominamy, że w poprzednim wykładzie pokazaliśmy, jak jeszcze *wyobrażać sobie* możemy liczby wymierne (drzewa: Calkina-Wilfa oraz Sterna-Brocota).

5. Z działaniami arytmetycznymi na ułamkach oswajamy się dość wcześnie w edukacji szkolnej. Nie mamy też większych trudności ze sprowadzaniem ułamków do postaci *zredukowanej*, w której licznik i mianownik ułamka są *względnie pierwsze* (nie mają wspólnego dzielnika różnego od 1).

2.4 Liczby rzeczywiste

W literaturze przedmiotu znanych jest kilkanaście propozycji zdefiniowania liczb rzeczywistych. Choć wielkości *niewspółmierne* znane były już starożytnym Grekom, to pierwsze w pełni precyzyjne charakterystyki liczb *niewymiernych* (a w konsekwencji, także pierwsze precyzyjne charakterystyki wszystkich liczb *rzeczywistych*) podano dopiero w XIX wieku. Najbardziej znane są propozycje Richarda Dedekinda (1831–1916) oraz Georga Cantora (1845–1918).

Konstrukcje liczb rzeczywistych różnią się od poprzednich konstrukcji (liczb całkowitych z naturalnych oraz wymiernych z całkowitych) tym, że dla określenia poszczególnej liczby rzeczywistej musimy odwoływać się do pewnego (nieskończonego) *zbioru* liczb wymiernych.

2.5 Definicja Dedekinda

Richard Dedekind podał definicję liczb rzeczywistych w 1872 roku w słynnej rozprawie *Stetigkeit und Irrationale Zahlen* (*Ciągłość i liczby niewymierne*). Definicja ta odwołuje się do struktury porządkowej zbioru $\mathbb{Q}$ wszystkich liczb wymiernych: jest to, jak pamiętamy, gęsty porządek bez elementu najmniejszego i bez elementu największego. Pamiętamy też, że nie każdy ograniczony z góry zbiór liczb wymiernych posiada kres górny, czyli że (zwykły) porządek liczb wymiernych nie

jest ciągły. Chcemy teraz stworzyć uniwersum liczbowe uporządkowane w sposób ciągły i to tak, aby zdefiniowane w nim operacje arytmetyczne były zgodne z tym porządkiem oraz rozszerzały znane operacje arytmetyczne na liczbach wymiernych.

Pomysł Dedekinda był rewelacyjnie prosty: każda liczba rzeczywista może być utożsamiona z (nieskończonym) zbiorem wszystkich liczb wymiernych od niej *mniejszych*. Ponieważ liczby rzeczywiste dopiero *stwarzamy* (konstruujemy), więc odwołać trzeba się w takiej charakterystyce tylko do samych liczb wymiernych, a dokładniej do *odcinków początkowych* w zbiorze liczb wymiernych (zob. poprzedni wykład).

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

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

Inaczej mówiąc, liczba rzeczywista w tym rozumieniu to dowolny niepusty właściwy odcinek początkowy zbioru $\mathbb{Q}$ bez elementu największego. Używamy standardowego oznaczenia $\mathbb{R}$ dla tego zbioru. Za chwilę przekonamy się, że zbiór tak określonych liczb rzeczywistych jest uporządkowany w sposób ciągły, a więc nie tak samo, jak wyjściowy zbiór $\mathbb{Q}$.

Nieco upraszczamy oryginalną konstrukcję Dedekinda. Rozpatrywał on mianowicie tzw. *przekroje* zbioru $\mathbb{Q}$ (dziś nazywane słusznie *przekrojami Dedekinda*), a jego konstrukcja znajduje zastosowanie w przypadku dowolnych zbiorów uporządkowanych liniowo.

Przekrojem Dedekinda nazywamy każdą parę (A, B) niepustych podzbiorów zbioru ostro liniowo uporządkowanego $(X, \prec)$ taką, że:

1. $A \cup B = X$
2. $a \prec b$ dla wszystkich $a \in A$ oraz $b \in B$.

A jest klasą *dolną*, a B klasą *górną* przekroju (A, B).

Łatwo widać, że w przypadku dowolnego zbioru liniowo uporządkowanego przekrój Dedekinda (A, B) może być jednej z następujących postaci:

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

2. W zbiorze A istnieje element największy i w zbiorze B nie istnieje element najmniejszy.

3. W zbiorze A nie istnieje element największy i w zbiorze B istnieje element najmniejszy.

4. W zbiorze A nie istnieje element największy i w zbiorze B nie istnieje element najmniejszy.

Zauważmy, że uporządkowanym liniowo zbiorze $\mathbb{Z}$ liczb całkowitych każdy przekrój wyznacza skok. Z kolei, jeśli zbiór jest uporządkowany w sposób gęsty (jak np. zbiór $\mathbb{Q}$), to żaden jego przekrój nie wyznacza skoku.

Wróćmy teraz do zbioru $\mathbb{Q}$. W drugim oraz trzecim z rozważanych wyżej czterech przypadków mówimy, że przekrój (A, B) wyznaczony jest przez liczbę x, jeśli x jest elementem największym w A lub, odpowiednio, najmniejszym w B. Właściwie można te przypadki rozpatrywać tak samo, a więc wystarczy rozważyć np. przypadek trzeci. Dalej, mówimy, że przekrój (A, B) wyznacza *lukę*, jeśli zachodzi przypadek czwarty (w zbiorze A nie istnieje element największy i w zbiorze B nie istnieje element najmniejszy). Tak więc, w zbiorze uporządkowanym w sposób gęsty wystarczy rozważać jedynie przypadki: trzeci i czwarty. Zauważmy, że każdy przekrój z tych przypadków jest jednoznacznie wyznaczony przez swoją klasę dolną (która nie ma elementu największego).

Powyższa definicja zbioru $\mathbb{R}$ jest dopiero początkiem dalszych konstrukcji. Trzeba mianowicie określić w $\mathbb{R}$ relację porządku oraz operacje arytmetyczne.

$\mathbb{R}$ jest rodziną zbiorów, a więc naturalne wydaje się wykorzystanie relacji inkluzji do określenia porządku w $\mathbb{R}$. Definiujemy zatem dla $A, B \in \mathbb{R}$: $A \leqslant_D B$ wtedy i tylko wtedy, gdy $A \subseteq B$. Wtedy oczywiście $A <_D B$ dokładnie wtedy, gdy $A \subset B$.

Zauważmy dwie rzeczy:

1. Każda liczba wymierna x wyznacza liczbę rzeczywistą $O(x) = \{y \in \mathbb{Q} : y < x\}$. Niech $\mathbb{Q}^o = \{O(x) : x \in \mathbb{Q}\}$. Wtedy $\mathbb{Q}^o$ jest izomorficzną (względem porządku) kopią $\mathbb{Q}$, co łatwo sprawdzić prostym rachunkiem.

2. 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.:

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

Liczby rzeczywiste, które są elementami zbioru $\mathbb{R} - \mathbb{Q}^o$ nazywamy *liczbami niewymiernymi*.

Zbadamy teraz własności zdefiniowanego przed chwilą porządku liczb rzeczywistych. Zachodzi następujące twierdzenie:
TWIERDZENIE. *Zbiór $\mathbb{R}$ jest uporządkowany w sposób ciągły przez relację $\leqslant_D$. Ponadto, zbiór $\mathbb{Q}^o$ jest* gęsty *w $\mathbb{R}$, czyli dla każdych $x, y \in \mathbb{R}$, jeśli $x <_D y$, to istnieje $z \in \mathbb{Q}^o$ taki, że $x <_D z$ oraz $z <_D y$.*
SZKIC DOWODU. Szczegółowy dowód znajdą słuchacze w podręczniku Guzicki, Zakrzewski 2005, na stronach 212–213. Tutaj ograniczymy się jedynie do naszkicowania głównych idei.

1. *Porządek $\leqslant_D$ jest liniowy*. Ten fakt wynika z tego, że każda liczba rzeczywista jest odcinkiem początkowym liniowo uporządkowanego zbioru $\mathbb{Q}$.

2. *Zbiór $\mathbb{Q}^o$ jest gęsty w $\mathbb{R}$*. To wynika z nietrudnego rachunku, uwzględniającego fakt, że liczby rzeczywiste zdefiniowaliśmy jako odcinki początkowe nie mające elementu największego.

3. *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 $\mathbb{Q} - A$).

4. *Porządek $\leqslant_D$ 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 $\bigcup S = \sup S$.

Twierdzenie powyższe charakteryzuje zatem własności porządkowe zbioru $\mathbb{R}$.
W zbiorze $\mathbb{R}$ wprowadzamy działania arytmetyczne w następujący sposób:

1. *Suma*. Jeśli $a, b \in \mathbb{R}$, to niech:

$$a \oplus_D b = \{x \oplus_2 y : x \in a \text{ oraz } y \in b\}.$$

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

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

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

   (a) Jeśli $a >_D O(0)$ oraz $b >_D O(0)$, to niech:

   $$a \odot_D b = \{x \odot_2 y : x > 0, y > 0, x \in a, y \in b\} \cup \{x \in \mathbb{Q} : x \leqslant 0\}.$$

   (b) Jeśli $a = O(0)$ lub $b = O(0)$, to $a \odot_D b = O(0)$.

   (c) Jeśli $a <_D O(0)$ oraz $b <_D O(0)$, to $a \odot_D b = (-_D a) \odot_D (-_D b)$

   (d) Jeśli $a <_D O(0)$ oraz $b >_D O(0)$, to $a \odot_D b = -_D((-_D a) \odot_D b)$

   (e) Jeśli $a >_D O(0)$ oraz $b <_D O(0)$, to $a \odot_D b = -_D(a \odot_D (-_D b))$.

Należy oczywiście wykazać, że wymienione operacje prowadzą od liczb rzeczywistych do liczb rzeczywistych oraz sprawdzić, że operacje te mają znane ze szkoły własności, charakterystyczne dla działań arytmetycznych na liczbach rzeczywistych. Można też wykazać, że struktury:

$$(\mathbb{Q}^o, \oplus_D, \odot_D, O(0), O(1)) \quad \text{oraz} \quad (\mathbb{Q}, \oplus_2, \odot_2, 0, 1)$$

są izomorficzne. Te fakty, wraz z przyjętymi wcześniej konwencjami upraszczania zapisów pozwalają wreszcie nadać rozumny sens ciągowi inkluzji znanemu z edukacji szkolnej:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

Rozumiemy teraz, że inkluzje te oznaczać mają, że każdą z kolejno rozważanych struktur można homomorficznie włożyć w jej sąsiadkę z prawej.
UWAGI.

1. Zauważmy, że że w myśl definicji Dedekinda, każda liczba rzeczywista jest utożsamiana z pewnym (nieskończonym) zbiorem liczb wymiernych.

2. Pamiętajmy, że definicja Dedekinda odwołuje się do własności porządkowych zbioru wszystkich liczb wymiernych.

3. Ponieważ zbiór $\mathbb{Q}^o$ jest gęsty w $\mathbb{R}$, więc między każdymi dwiema liczbami rzeczywistymi (w szczególności: między każdymi dwiema niewymiernymi liczbami rzeczywistymi) znajduje się liczba wymierna (a nawet nieskończenie wiele liczb wymiernych). Z kolei, między każdymi dwiema liczbami wymiernymi znajduje się co najmniej jedna liczba rzeczywista (a nawet nieskończenie wiele liczb rzeczywistych; w szczególności, również nieskończenie wiele liczb niewymiernych).

2.6 Definicja Cantora

Definicja liczb rzeczywistych zaproponowana przez Georga Cantora odwołuje się do ciągów liczb wymiernych, które zachowują się – mówiąc bardzo metaforycznie – w grzeczny sposób, których wyrazy nie rozbiegają się szaleńczo, oddalając się od siebie. To oczywiście tylko żart.

Niech $\mathbb{SEQ}$ będzie zbiorem wszystkich *ciągów podstawowych liczb wymiernych*, tj. zbiorem:

$\{f : f : \mathbb{N} \to \mathbb{Q}$ oraz dla każdej $k \in \mathbb{N}$ istnieje $m_0 \in \mathbb{N}$ taka,
że dla wszystkich $m, n > m_0$ zachodzi $|f(n) - f(m)| < \frac{1}{k+1}\}$.

Na zbiorze $\mathbb{SEQ}$ określamy relację $\approx_3$ wzorem:

$f \approx_3 g$ wtedy i tylko wtedy, gdy dla każdej $k \in \mathbb{N}$ istnieje $m_0 \in \mathbb{N}$ taka, że dla wszystkich $n > m_0$ zachodzi: $|f(n) - f(m)| < \frac{1}{k+1}$.

Wtedy $\approx_3$ jest relacją równoważności na $\mathbb{SEQ}$, co nietrudno sprawdzić rachunkiem. *Definiujemy* zbiór wszystkich liczb *rzeczywistych* (w sensie Cantora): $\mathbb{R} = \mathbb{SEQ}/\approx_3$.

Funkcja $\varphi_3 : \mathbb{Q} \to \mathbb{R}$ zdefiniowana wzorem $\varphi_3(q) = [c_q]_{\approx_3}$ (gdzie c_q jest ciągiem stale równym q) jest iniekcją.

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

1. $[f]_{\approx_3} \oplus_3 [g]_{\approx_3} = [f \uplus g]_{\approx_3}$ (*dodawanie*)
2. $[f]_{\approx_3} \odot_3 [g]_{\approx_3} = [f \otimes g]_{\approx_3}$ (*mnożenie*)

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

1. $(f \uplus g)(n) = f(n) \oplus_2 g(n)$, dla $n \in \mathbb{N}$
2. $(f \otimes g)(n) = f(n) \odot_2 g(n)$, dla $n \in \mathbb{N}$.

Można udowodnić, że wszystkie te definicje są poprawne i że adekwatnie określają działania arytmetyczne w $\mathbb{R}$. Będziemy jeszcze wracać do tej charakterystyki zbioru liczb rzeczywistych.

UWAGI.

1. Zauważmy, że w myśl definicji Cantora, każda liczba rzeczywista jest utożsamiana z pewnym zbiorem ciągów liczb wymiernych.
2. Każdy ciąg podstawowy ma tę własność, że począwszy od pewnego miejsca, jego kolejne wyrazy są sobie dowolnie bliskie.

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

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

Dodajmy jeszcze informację, która z pewnością wszystkich ucieszy: w dalszych wykładach będziemy używali tego samego symbolu $+$ dla operacji dodawania, zaś symbolu $\cdot$ dla operacji mnożenia we wszystkich zbiorach liczbowych: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, zgodnie z powszechnie przyjętą praktyką. Subtelności w oznaczeniach operacji arytmetycznych definiowanych powyżej były potrzebne dla ukazania istoty przeprowadzanych konstrukcji. Proszę pamiętać, że jeśli „rozmawiamy" z komputerem (czyli z programem komputerowym), to trzeba ściśle przestrzegać reguł składni używanego w takiej „konwersacji" języka i nie można tego samego symbolu używać w różnych znaczeniach. Nasza intelektualna wyższość nad komputerami przejawia się m.in. w tym, że możemy sobie pozwolić na tego rodzaju świństewka w notacji, hołdując własnemu lenistwu oraz Tradycji.

3 Kraty i algebry Boole'a: definicja algebraiczna

Omawiane na poprzednim wykładzie *kraty* oraz *algebry Boole'a* definiować można na sposób algebraiczny, przez określenie stosownych operacji na ich elementach. Przy tym, obie definicje (porządkowa i algebraiczna są zgodne: z każdej z nich można otrzymać pozostałą).

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:

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

PRZYKŁADY.

1. 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.

2. Zbiór potęgowy $\wp(X)$ dowolnego zbioru X jest algebrą Boole'a (a więc także kratą): zerem algebry jest zbiór pusty $\emptyset$, jej jedynką jest zbiór X, a operacjami $\sqcup$ oraz $\sqcap$ są, odpowiednio, operacje sumy i iloczynu zbiorów. Uzupełnieniem elementu $Y \subseteq X$ tej algebry jest dopełnienie $Y' = X - Y$.

3. 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 $x = y = 1$

   $\ominus(0) = 1, \ominus(1) = 0.$

   Słuchacze z łatwością rozpoznają w tych operacjach *funkcje prawdziwościowe*, odpowiadające, kolejno: alternatywie nierozłącznej, koniunkcji oraz negacji.

4. Każda algebra Boole'a jest izomorficzna z pewnym ciałem zbiorów.

Kraty, algebry Boole'a oraz inne rodzaje algebr (np. *algebry Heytinga*) mają ścisłe związki z logiką matematyczną, o czym słuchacze przekonają się w trakcie dalszych studiów.
UWAGA. Ze względu na pewne nawyki, zwykle stosujemy notację *infiksową* (symbol funkcji między symbolami argumentów) dla operacji w kratach, 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 $\ominus(x)$.

Używając wyżej notacji *prefiksowej* (symbol funkcji przed symbolami argumentów) nie czyniliśmy tego złośliwie, ale chcieliśmy oswoić słuchaczy z przechodzeniem od jednej notacji do drugiej. Umiejętność operowania na symbolach jest jedną z cech wyróżniających nasz gatunek od innych Stworzeń. To dzięki niej jesteśmy zdolni tworzyć i rozumieć poezję, malarstwo, matematykę. Posługiwanie się językiem wymaga bardzo zaawansowanych operacji na symbolach. Wbrew niektórym potocznym mniemaniom, o wiele prostsze jest *trafne* przetwarzanie informacji w językach sztucznych (logiki i matematyki) niż w językach etnicznych.

DODATKI

Podobnie jak w poprzednim wykładzie, poniżej zamieszczamy garść informacji uzupełniających tematykę wykładu. Czynimy to w przekonaniu, że studenci kognitywistyki UAM już od pierwszego roku studiów są uzależnieni od *ciekawości poznawczej*. Jak się wydaje, jedyną terapią takiego uzależnienia jest pogłębianie owego nałogu.

4 Dodatek: inne rodzaje liczb

Liczby: naturalne, całkowite, wymierne, a nawet liczby rzeczywiste są dość dobrze „oswojone" już w edukacji szkolnej. We współczesnych zastosowaniach matematyki (np. w fizyce) istotną rolę odgrywają inne jeszcze rodzaje liczb. Byłoby przesadą omawianie bardziej skomplikowanych systemów liczbowych w niniejszym elementarnym usługowym kursie matematyki. Zachęcamy jednak zainteresowanych słuchaczy do poświęcenia jakiegoś wieczoru (powiedzmy, w miłym towarzystwie koleżanki lub kolegi) na samodzielne znalezienie informacji o tego typu strukturach.

4.1 Liczby zespolone

Pewne intuicje o tych liczbach zawiera plik z szczegółowym omówieniem tematów wykładów, umieszczony na stronie wykładów. Dla wygody tych czytelników, którzy dotarli do tego miejsca tekstu przytaczamy niżej stosowny fragment.

Liczby zespolone można charakteryzować aksjomatycznie, można też wprowadzić je na wiele innych sposobów. Stosunkowo prosty jest sposób podany przez Hamiltona. W tej reprezentacji liczby zespolone traktowane są jako pary liczb rzeczywistych. Działania arytmetyczne dodawania $\oplus$ oraz mnożenia $\otimes$ zdefiniowane są następująco (poprzez operacje dodawania, odejmowania i mnożenia liczb rzeczywistych):

1. $(a, b) \oplus (c, d) = (a + c, b + d)$
2. $(a, b) \otimes (c, d) = (a \cdot c - b \cdot d, a \cdot d + b \cdot c)$.

Liczby rzeczywiste utożsamiać można z liczbami zespolonymi o postaci $(a, 0)$.
Wprowadza się oznaczenie $i = (0, 1)$. Wtedy $i^2 = (0, 1) \otimes (0, 1) = (-1, 0)$.
Liczby zespolone o postaci (a, b) zwykło się zapisywać w formie $a + b \cdot i$.

W interpretacji geometrycznej przedstawia się liczby zespolone na *płaszczyźnie zespolonej*. Narysujmy kartezjański układ współrzędnych. Na osi odciętych

jednostką jest 1, na osi rzędnych jednostką jest i. Liczbę zespoloną $z = a + bi$ interpretujemy jako punkt na tej płaszczyźnie o współrzędnych (a, b). Połączmy odcinkiem punkt (a, b) z początkiem układu współrzędnych $(0, 0)$. Niech odcinek ten tworzy z osią odciętych kąt φ. Długość tego odcinka wynosi $r = \sqrt{a^2 + b^2}$. Liczbę tę nazywamy *modułem* liczby zespolonej $z = a + bi$ i oznaczamy przez $|z|$. Liczbą *sprzężoną* z liczbą $z = a + bi$ jest liczba $\overline{z} = a - bi$.

Jeśli $z = a + bi$, to a nazywamy częścią *rzeczywistą* liczby z (oznaczaną przez $Re(z)$), zaś b jej częścią *urojoną* (oznaczaną przez $Im(z)$). Zauważmy, że dla $z = a + bi$, $r = \sqrt{a^2 + b^2}$ oraz φ określonego wyżej mamy:

$$z = r(\cos\varphi + i\sin\varphi).$$

Jest to przedstawienie liczby zespolonej z we współrzędnych *biegunowych*.

Dodawanie oraz mnożenie liczb zespolonych przyjmuje szczególnie prostą postać w powyższej geometrycznej interpretacji. Być może będziemy mieli okazję, aby później podać szczegóły.

Zbiór wszystkich liczb zespolonych będziemy oznaczać przez $\mathbb{C}$. Liczb zespolonych ***nie*** jest *tyle samo*, co liczb naturalnych. Liczb zespolonych jest *tyle samo*, co liczb rzeczywistych.

Zachodzi PODSTAWOWE TWIERDZENIE ALGEBRY: każdy wielomian zespolony (różny od stałej) ma co najmniej jeden pierwiastek zespolony.

4.2 Kwaterniony

Za datę poczęcia systemu kwaternionów uznaje się 16 października 1843 roku – dzień, w którym Wiliam Hamilton ustalił dla nich reguły mnożenia. Kwaterniony miały swoje chwile świetności – były bardzo modnym tematem badań w wieku XIX, potem stały się na długi czas jedynie ciekawostką matematyczną. Obecnie okazuje się, że to właśnie algebra kwaternionów, algebra oktonionów oraz pewne inne dość szczególne algebry mają istotne zastosowania w naukach empirycznych, np. w fizyce, a także w sztuce.

Pytanie o możliwe uogólnienia znanych ciał liczb rzeczywistych $\mathbb{R}$ oraz liczb zespolonych $\mathbb{C}$ jest całkiem naturalne. Jedną z reprezentacji liczb zespolonych jest traktowanie ich jako par $(a, b{\cdot}i)$, gdzie a oraz b są liczbami rzeczywistymi, zaś i jest jednostką urojoną (dla pełnej symetrii moglibyśmy pisać te pary w postaci $(a \cdot 1, b \cdot i)$). Dobrze określone są na tak rozumianych liczbach zespolonych podstawowe działania arytmetyczne. Nasuwa się zatem pytanie: czy można odpowiedniki tych podstawowych działań określić także dla trójek, czwórek, itd. liczb rzeczywistych – ogólnie, dla dowolnych n-tek liczb rzeczywistych, w taki sposób, aby otrzymana struktura algebraiczna miała pożądane własności.

Współcześnie rozumiemy kwaterniony jako czterowymiarową przestrzeń wektorową nad ciałem liczb rzeczywistych. Dla kwaternionów określone są zatem: ich dodawanie, mnożenie przez skalar oraz mnożenie. Pierwsze dwie z tych operacji definiujemy tak, jak zwykle robi się to w wielowymiarowych przestrzeniach wektorowych. Natomiast mnożenie kwaternionów jest w pełni określone, gdy podamy tabliczkę mnożenia dla wektorów bazy przestrzeni $\mathbb{H}$. Tradycyjnie wektory bazy oznaczamy przez $1, i, j, k$. Mnożenie jest jednoznacznie wyznaczone przez równania:

$$i^2 = j^2 = k^2 = ijk = -1.$$

Oczywiście można też określić mnożenie stosowną tabelką:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Myślimy o kwaternionach także jako o czterowymiarowej unormowanej algebrze z dzieleniem nad liczbami rzeczywistymi. Używa się też terminu *pierścień z dzieleniem*, dla oznaczenia struktury, która spełnia wszystkie aksjomaty ciała, z wyjątkiem przemienności mnożenia. Takim pierścieniem z dzieleniem jest też, oprócz $\mathbb{H}$, także struktura określona tak samo jak $\mathbb{H}$, przy czym zastępujemy w jej definicji liczby rzeczywiste liczbami wymiernymi.

Kwaterniony zapisuje się w różnych notacjach, np.:

1. (a, bi, cj, dk) lub $(a+bi+cj+dk)$, gdzie a, b, c, d są liczbami rzeczywistymi
2. $(r, \overrightarrow{v})$, gdzie r jest liczbą rzeczywistą, a $\overrightarrow{v}$ wektorem (który utożsamiamy z trójką liczb rzeczywistych)

Jeśli wektory bazy przedstawimy w postaci:

$$\begin{aligned} 1 &= (1,0,0,0) \\ i &= (0,1,0,0) \\ j &= (0,0,1,0) \\ k &= (0,0,0,1), \end{aligned}$$

to dodajemy kwaterniony dodając ich współrzędne, mnożymy przez skalar mnożąc przezeń współrzędne, natomiast mnożenie kwaternionów podaje wzór:

$$
\begin{aligned}
&(a_1b_1c_1d_1)(a_2b_2c_2d_2) = \\
&(a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2, \\
&a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2, \\
&a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2, \\
&a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2).
\end{aligned}
$$

Jeśli $(a + bi + cj + dk)$ jest dowolnym kwaternionem, to liczbę rzeczywistą a nazywamy jego częścią skalarną, a $(bi + cj + dk)$ jego częścią wektorową.

Mnożenie kwaternionów zapisanych w notacji wektorowej określone jest wzorem:

$$(r_1, \overrightarrow{v}_1)(r_2, \overrightarrow{v}_2) = (r_1r_2 - \overrightarrow{v}_1 \cdot \overrightarrow{v}_2, r_1\overrightarrow{v}_2 + r_2\overrightarrow{v}_1 + \overrightarrow{v}_1 \times \overrightarrow{v}_2),$$

gdzie $\overrightarrow{v}_1 \cdot \overrightarrow{v}_2$ jest iloczynem skalarnym wektorów $\overrightarrow{v}_1$ oraz $\overrightarrow{v}_2$, natomiast $\overrightarrow{v}_1 \times \overrightarrow{v}_2$ jest ich iloczynem wektorowym. Jeśli mianowicie $\overrightarrow{v}_1 = (b_1, c_1, d_1)$ oraz $\overrightarrow{v}_2 = (b_2, c_2, d_2)$, to:

1. $\overrightarrow{v}_1 \cdot \overrightarrow{v}_2 = b_1b_2 + c_1c_2 + d_1d_2$
2. $\overrightarrow{v}_1 \times \overrightarrow{v}_2 = \begin{vmatrix} i & j & k \\ b_1 & c_1 & d_1 \\ b_2 & c_2 & d_2 \end{vmatrix}$

Kwaternionem sprzężonym do kwaternionu $q = a + bi + cj + dk$ nazywamy kwaternion $q^* = a - bi - cj - dk$. W zbiorze kwaternionów wprowadza się normę:

$$||q|| = \sqrt{qq^*}.$$

Jest to norma multiplikatywna, czyli $||pq|| = ||p||\,||q||$. Wprost z tej definicji wynika, że:

$$||a + bi + cj + dk|| = \sqrt{a^2 + b^2 + c^2 + d^2}.$$

Norma służyć może do wprowadzenia w $\mathbb{H}$ odległości:

$$d(p, q) = ||p - q||.$$

Kwaterniony jednostkowe to te, których norma równa jest 1. Możemy je przedstawiać także w postaci wykładniczej:

$$e^{\alpha\overrightarrow{v}} = (\cos\alpha, \sin\alpha\,\overrightarrow{v}).$$

Nie miejsce tutaj na zagłębianie się w szczegóły dotyczące kwaternionów. Tytułem przykładu wspomnimy jedynie kilka ich ważnych własności:

1. Zbiór $\{1, -1, i, -i, j, -j, k, -k\}$ (wraz z operacją mnożenia kwaternionów) tworzy grupę, tradycyjnie oznaczaną przez Q_8.

2. Kwaterniony jednostkowe tworzą sferę S^3 w przestrzeni czterowymiarowej.

3. Kwaterniony związane są z obrotami w przestrzeni trójwymiarowej. Dokładniej, kwaterniony jednostkowe odwzorować można na elementy grupy SO^3 obrotów w przestrzeni trójwymiarowej. Każdemu kwaternionowi q przypiszmy mianowicie obrót T_q według wzoru:

   $$T_q(x) = qxq^{-1}.$$

   Wtedy zachodzą m.in. następujące fakty:

   (a) Przekształcenie T_q jest obrotem w trójwymiarowej przestrzeni kwaternionów urojonych.

   (b) Jeśli kwaternion q wyrazimy w postaci wykładniczej $e^{\alpha \overrightarrow{v}}$, to T_q jest obrotem o kąt 2α wokół osi $\overrightarrow{v}$.

4. Kwaterniony jednostkowe nazywane bywają *wersorami*. Każdy wersor jest zatem postaci:

   $$e^{\alpha r} = \cos a + r \sin \alpha,$$

   przy czym $r^2 = -1$ oraz $\alpha \in [0, \pi)$. Każdemu kwaternionowi q odpowiada pewien wersor $\hat{q}$:

   $$\hat{q} = \frac{q}{||q||}.$$

   Używa się też oznaczenia $\mathbf{U}q$ zamiast $\hat{q}$.

Współczesne zastosowania kwaternionów są wielce różnorodne, zarówno w samej matematyce, jak też w naukach empirycznych oraz technice i sztuce (w szczególności, w grafice komputerowej).

* * *

Istnieje bardzo wiele innych jeszcze rodzajów liczb, z których niektóre mają niezwykle istotne zastosowania w nauce, w sztuce, w refleksji nad Życiem. Proponujemy ewentualnie zainteresowanym słuchaczom samodzielnie poszukać informacji np. o liczbach *p-adycznych* oraz *hiperrzeczywistych*. Jesteśmy przekonani, że w każde z tych poszukiwań dostarczy naprawdę frapującej Przygody Poznawczej.

5 Dodatek: grupy, pierścienie, ciała, przestrzenie liniowe

Świat struktur relacyjnych i algebr jest niezmiernie bogaty. Podajemy definicje kilku najważniejszych rodzajów struktur algebraicznych, wraz z prostymi przykładami.

5.1 Grupy

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*).
PRZYKŁADY.

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. Liczby rzeczywiste z operacją dodawania tworzą grupę. Podobnie, liczby wymierne (lub całkowite) z operacją dodawania tworzą grupę. Liczby naturalne z operacją dodawania nie tworzą grupy (gdyż nie dla każdego elementu istnieje element odwrotny).

5.2 Pierścienie

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*.

PRZYKŁADY.

1. Przykładem pierścienia (z jednością, bez dzielników zera, z przemiennym mnożeniem) jest zbiór $\mathbb{Z}$ wszystkich liczb całkowitych ze „zwykłym" dodawaniem oraz mnożeniem. Jest to zatem dziedzina całkowitości.

2. Wszystkie wielomiany o współczynnikach rzeczywistych tworzą pierścień. Operacjami są tu: dodawanie i mnożenie wielomianów.

3. Rozważmy zbiór $\mathbb{R} \times \mathbb{R}$ wraz z operacjami dodawania $\oplus$ i mnożenia $\otimes$ par liczb:

   $(a, b) \oplus (c, d) = (a + c, b + d)$

   $(a, b) \otimes (c, d) = (a \cdot b, c \cdot d)$

Wtedy $(\mathbb{R} \times \mathbb{R}, \oplus, \otimes)$ jest pierścieniem, w którym mnożenie jest przemienne, elementem neutralnym dodawania jest para $(0, 0)$, jednością jest para $(1, 1)$. Istnieją w nim dzielniki zera, ponieważ mamy np.: $(1, 0) \otimes (0, 1) = (0, 0)$. Ta struktura nie jest zatem dziedziną całkowitości.

5.3 Ciała

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.
PRZYKŁADY.

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, ze stosownie określonymi (zob. plik ze szczegółowym omówieniem planu wykładów, umieszczony na stronie wykładów) 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.

5.4 Przestrzenie liniowe

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

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 przeciwny (odwrotny 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 zastosowaniach rozważa się przestrzenie wektorowe nad różnego rodzaju ciałami.

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 $\| x \boxminus y \|$.

PRZYKŁADY.

1. Każde ciało $\mathbb{K}$ można uważać za przestrzeń liniową nad ciałem $\mathbb{K}$ ujmowanym jako ciało skalarów.
2. Każdy zbiór $\mathbb{R}^n$ $(n \geqslant 1)$ tworzy przestrzeń liniową nad ciałem liczb rzeczywistych $\mathbb{R}$.
3. 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:
   (a) $(f \boxplus g)(x) = f(x) + g(x)$

(b) $a \boxtimes f(x) = a \cdot f(x)$.

4. 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 $x \in \mathbb{R}$.

6 Zachęta do refleksji

1. 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?

2. Składanie obrotów na płaszczyźnie jest przemienne. Czy przemienne jest składanie obrotów w przestrzeni trójwymiarowej?

3. Zakresy pojęć są zbiorami, a więc można na nich wykonywać operacje boolowskie. Jaką strukturę tworzy zestaw wszystkich zakresów pojęć *rzeczywiście* używanych w danym języku?

4. Czy oprócz grup, pierścieni, ciał, przestrzeni liniowych istnieją inne ważne struktury matematyczne?

7 Podsumowanie

To, co należy zapamiętać z niniejszego wykładu:

1. Struktura relacyjna, algebra, podstruktura, struktura ilorazowa.

2. Homomorfizm, izomorfizm.

3. Kongruencja.

4. System liczb rzeczywistych: definicja Dedekinda i definicja Cantora.

5. Kraty i algebry Boole'a.

8 Wybrane pozycje bibliograficzne

Guzicki, W., Zakrzewski, P. 2005. *Wykłady ze wstępu do matematyki. Wprowadzenie do teorii mnogości.* Wydawnictwo Naukowe PWN, Warszawa.

Mirkowska, G. 2003. *Elementy matematyki dyskretnej.* Wydawnictwo Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych, Warszawa.

Musielak, H., Musielak, J. 2004. *Analiza matematyczna*. Wydawnictwo Naukowe UAM, Poznań.

Rutkowski, J. 2000. *Algebra abstrakcyjna w zadaniach*. Wydawnictwo Naukowe PWN, Warszawa.