Logika Matematyczna (JiNoI I)

Jerzy Pogonowski

Zakład Logiki Stosowanej UAM
www.logic.amu.edu.pl
pogon@amu.edu.pl

24-25 maja 2007

Plan na dziś:

- Język KRP z symbolami funkcyjnymi.
- Teorie aksjomatyczne w języku KRP.
- Aksjomatyka teorii mnogości ZF.
- Aksjomatyka arytmetyki Robinsona.
- Aksjomatyka teorii algebr Boole'a.
- Aksjomatyka teorii grup.

Język KRP z symbolami funkcyjnymi

Rozważamy teraz język KRP, w którym występują symbole funkcyjne. W najbardziej ogólnym przypadku, mamy przeliczalną liczbę symboli funkcyjnych n-argumentowych dla każdej liczby naturalnej n. Zakładamy też, że język ten zawiera również predykat identyczności, scharakteryzowany w podrozdziale III.5. W pewnych ujęciach, wygodne jest także używanie *operatora deskrypcyjnego* $\iota(x)$; wyrażenie $\iota(x)A(x)$ (gdzie $A(x)$ jest formułą języka KRP o zmiennej wolnej x) czytamy: *jedyne x takie, że $A(x)$*. Operator ten podobny jest składniowo do kwantyfikatorów. W niniejszym ujęciu nie będzie nam on potrzebny.

Jeśli $t, t_1, \ldots, t_n$ są termami, a F jest n-argumentowym symbolem funkcyjnym, to wyrażenie postaci:

$$F(t_1, \ldots, t_n) = t$$

czytamy *wartość funkcji (oznaczanej symbolem) F dla argumentów (oznaczanych symbolami) $t_1, \ldots, t_n$ równa jest (obiektowi oznaczanemu przez term) t.*

Pojęcie termu

Przypomnijmy, że definicja *termu* języka KRP jest indukcyjna:

- (i) wszystkie zmienne indywiduowe x_n oraz wszystkie stałe indywiduowe a_k są termami;
- (ii) jeśli $t_1, \ldots, t_{n_j}$ są dowolnymi termami, a $f_j^{n_j}$ jest symbolem funkcyjnym n_j-argumentowym, to wyrażenie $f_j^{n_j}(t_1, \ldots, t_{n_j})$ jest termem;
- (iii) nie ma innych termów (języka KRP) prócz zmiennych indywiduowych oraz stałych indywiduowych oraz tych termów, które można skonstruować wedle reguły (ii).

Pojęcie funkcji

Funkcje należą do niezbędnika każdego matematyka.
Również we wszelkich naukach empirycznych, w których stosuje się opisy *ilościowe*, niezbędne jest używanie funkcji.
Wreszcie, także w empirycznych naukach Humanistycznych posługiwanie się funkcjami jest codziennością.

Nie będziemy przytaczać tu wszystkich definicji związanych z prawidłowym operowaniem pojęciem funkcji.
Słuchaczki niniejszego kursu wysłuchały kursu *Wstęp do matematyki*, gdzie podano stosowną terminologię, definicje oraz twierdzenia. Przypomnijmy jedynie podstawową definicję.

Pojęcie funkcji

Jeśli $f \subseteq X^n \times Y$ jest relacją, to mówimy, że f jest n-argumentową funkcją ze zbioru X^n w zbiór Y i zapisujemy ten fakt jako $f : X^n \to Y$, gdy:

- $\forall x_1 \in X \ldots \forall x_n \in X \exists y \in Y \ \ (x_1, \ldots, x_n, y) \in f$
- $\forall x_1 \in X \ldots \forall x_n \in X \forall y_1 \in Y \forall y_2 \in Y \ \ (((x_1, \ldots, x_n, y_1) \in f \wedge (x_1, \ldots, x_n, y_2) \in f) \to y_1 = y_2)$.

W zgodzie z powszechnie przyjętymi konwencjami, gdy $f : X^n \to Y$ oraz $(x_1, \ldots, x_n, y) \in f$, to piszemy $f(x_1, \ldots, x_n) = y$ i mówimy, że y jest wartością funkcji f dla argumentów $x_1, \ldots, x_n$.

Reguły MDS dla KRP z symbolami funkcyjnymi

Reguły MDS dla kwantyfikatorów w języku KRP z symbolami funkcyjnymi

Reguły MDS dla formuł z kwantyfikatorami różnią się tych sformułowanych w III.1.1. jedynie tym, że zamiast o stałych indywiduowych mówimy w nich o termach.

Poniższe reguły określają, jaką formułę należy dopisać do tworzonej gałęzi, jeśli na gałęzi tej wystąpiła formuła danej postaci. Przypominamy, że $A(t/x)$ oznacza formułę otrzymaną z formuły o zmiennej wolnej x przez zastąpienie wszystkich wolnych wystąpień tej zmiennej termem t.

Reguły MDS dla KRP z symbolami funkcyjnymi

Reguły rozkładu formuł dotyczące kwantyfikatorów mają postać następującą:

- ***Reguła dla formuł generalnie skwantyfikowanych:***

  $R(\forall)$
  $$\begin{array}{c} \forall x\, A(x) \\ | \\ A(t/x) \end{array}$$

  dla każdego termu t występującego na rozważanej gałęzi.

- ***Reguła dla formuł egzystencjalnie skwantyfikowanych:***

  $R(\exists)$
  $$\begin{array}{c} \exists x\, A(x) \\ | \\ A(t/x) \end{array}$$

  dla nowego termu t nie występującego dotąd na rozważanej gałęzi.

Reguły MDS dla KRP z symbolami funkcyjnymi

- ***Reguła dla negacji formuł generalnie skwantyfikowanych:***

  $R(\neg\forall)$
  $$\begin{array}{c} \neg\forall x\, A(x) \\ | \\ \neg A(t/x) \end{array}$$
  dla nowego termu t nie występującego dotąd na rozważanej gałęzi.

- ***Reguła dla negacji formuł egzystencjalnie skwantyfikowanych:***

  $R(\neg\exists)$
  $$\begin{array}{c} \neg\exists x\, A(x) \\ | \\ \neg A(t/x) \end{array}$$
  dla każdego termu t występującego na rozważanej gałęzi.

Reguły $R(\forall)$ oraz $R(\neg\exists)$ są wzmocnione dodatkowym warunkiem: jeśli na gałęzi, której dotyczy ich zastosowanie nie ma jeszcze żadnego termu, to posługujemy się jakimś z góry ustalonym termem.

Aksjomatyka teorii mnogości ZF

Aksjomat ekstensjonalności:

$\forall x \forall y\, (\forall z\, (z \in x \leftrightarrow z \in y) \rightarrow x = y)$

Ten aksjomat stwierdza, że każdy zbiór jest jednoznacznie wyznaczony poprzez swoje elementy.

Aksjomat pary:

$\forall x \forall y \forall z \forall u\, (u \in z \leftrightarrow u = x \vee u = y)$

To aksjomat gwarantujący istnienie pary nieuporządkowanej.

Aksjomat sumy:

$\forall x \forall y \forall z\, (z \in y \leftrightarrow \exists u\, (z \in u \wedge u \in x))$

Aksjomat ten gwarantuje istnienie sumy dowolnej rodziny zbiorów.

Aksjomat zbioru potęgowego:

$\forall x \exists y \forall z\, (z \in y \leftrightarrow \forall u (u \in z \rightarrow u \in x))$

Na mocy tego aksjomatu, dla dowolnego zbioru istnieje zbiór złożony dokładnie ze wszystkich jego podzbiorów.

Schemat wyróżniania:

$\forall x_1 \forall x_2 \ldots \forall x_n \forall y \exists u\, (u \in z \leftrightarrow u \in y \wedge \varphi(u, x_1, x_2, \ldots, x_n))$
gdzie φ jest formułą języka teorii mnogości ZF taką, że z nie jest zmienną wolną w φ, zaś $x_1, x_2, \ldots, x_n$ są zmiennymi wolnymi formuły φ innymi niż u.

Schemat wyróżniania pozwala z elementów danego wprzódy zbioru utworzyć jego podzbiór, złożony z tych elementów, które mają jakąś własność, wyrażalną w języku (pierwszego rzędu) teorii mnogości.
Mamy tu do czynienia nie z jednym aksjomatem, ale właśnie ze schematem nieskończenie wielu aksjomatów.

Aksjomat nieskończoności:

$\exists x\, (\exists y\, (y \in x \wedge \neg \exists z\, (z \in y)) \wedge \forall y\, (y \in x \rightarrow \forall z (\forall u\, (u \in z \leftrightarrow u = y) \rightarrow z \in x)))$
Ten aksjomat stwierdza istnienie (co najmniej jednego) zbioru nieskończonego. Uwaga: to jedyny aksjomat egzystencjalny w tej teorii mnogości.

Schemat zastępowania:
$\forall u(\forall x\forall y\forall z\, (x \in u \wedge \varphi(x,y) \wedge \varphi(x,z) \rightarrow y = z) \rightarrow \exists w\forall v\, (v \in w \leftrightarrow \exists x\, (x \in u \wedge \varphi(x,v))))$
Schemat ten gwarantuje, intuicyjnie mówiąc, że obraz dowolnego zbioru względem jakiejkolwiek funkcji (opisywalnej formułą języka teorii mnogości) także jest zbiorem.
Tu również mamy do czynienia nie z jednym aksjomatem, ale ze schematem nieskończenie wielu aksjomatów.

Aksjomat ufundowania:
$\forall x(\exists u\, (u \in x) \rightarrow \exists y(y \in x \wedge \forall z\, (z \in y \rightarrow \neg z \in x)))$
Aksjomat ufundowania wyklucza istnienie nieskończonych $\in$-zstępujących ciągów zbiorów, tj. takich ciągów $\langle x_1, x_2, x_3, x_4, \ldots\rangle$, że:

$$x_2 \in x_1,\ x_3 \in x_2,\ x_4 \in x_3, \ldots$$

Gdy do tego systemu dołączyć **Aksjomat wyboru**:
$\forall x((\forall y\,(y \in x \rightarrow \exists z\,(z \in y)) \wedge \forall y \forall u\,(y \in x \wedge u \in x \rightarrow y = u \vee \neg \exists v\,(v \in y \wedge v \in u))) \rightarrow \exists w(\forall y\,(y \in x \rightarrow \exists z\,(z \in y \wedge z \in w \wedge \forall v\,(v \in y \wedge v \in w \rightarrow v = z)))))$
To otrzymamy system teorii mnogości nazywany **ZFC**.

Uwaga. Do aksjomatyki teorii ZF należą także aksjomaty dla identyczności:

- $\forall x\ x = x$
- $\forall x \forall y\ x = y \rightarrow y = x$
- $\forall x \forall y \forall z\ x = y \wedge y = z \rightarrow x = z$;
- $\forall x \forall y \forall z\ (x = y \wedge x \in z \rightarrow y \in z)$;
- $\forall x \forall y \forall z\ (x = y \wedge z \in x \rightarrow z \in y)$.

Uwaga. Używane tu (np. w schematach wyróżniania i zastępowania) terminy: nieskończony i przeliczalny należą do metajęzyka.

Aksjomatyka arytmetyki Robinsona

Dodawania i mnożenia liczb naturalnych uczysz się w wieku kilku lat.

Chociaż, gdy się chwilę zastanowisz, to być może dopadnie cię refleksja: skąd właściwie wiesz, jaki jest wynik wykonywania tych operacji (tj. dodawania i mnożenia) na liczbach naturalnych?

Prawdopodobnie, nauczono cię tabliczek dodawania i mnożenia podobnie jak naucza się wierszyków, „na pamięć".

Stosowano przy tym różne heurystyki; np. rysunki jabłuszek, kotków, monet, itp. No i teraz umiesz dodawać i mnożyć.

Czyżby jednak ta ***wiedza*** miała uzasadnienie wyłącznie w owych dogmatycznych rysunkach?

To temat na zajęcia z filozofii matematyki lub, ogólniej, z filozofii nauki. Te zajęcia dotyczą elementarza logicznego, a więc nie znajdziesz w nich wyczerpującej odpowiedzi na tego typu pytania metafizyczne. Ograniczymy się do stwierdzenia, że arytmetykę można zbudować na bazie aksjomatycznej, jako teorię pierwszego rzędu (a więc teorię w języku KRP, z predykatem identyczności oraz symbolami funkcyjnymi).

Tabliczki dodawania i mnożenia zbudować można w Arytmetyce Robinsona. Jest to system aksjomatyczny w języku KRP z identycznością oraz następującymi symbolami funkcyjnymi:

- σ — jednoargumentowy symbol funkcyjny; wyrażenie $\sigma(t)$, gdzie t jest dowolnym termem, czytamy: *następnik* t;
- $\oplus$ — dwuargumentowy symbol funkcyjny; wyrażenie $\oplus(t_1, t_2)$, gdzie t_1, t_2 są dowolnymi termami, czytamy: *suma* t_1 i t_2;
- $\otimes$ — dwuargumentowy symbol funkcyjny; wyrażenie $\otimes(t_1, t_2)$, gdzie t_1, t_2 są dowolnymi termami, czytamy: *iloczyn* t_1 i t_2.

Nadto, w języku Arytmetyki Robinsona używamy stałej indywiduowej $\bigcirc$. Jest to symbol, który czytamy: *zero*.

Aksjomaty.

Aksjomaty dotyczące jedynie predykatu identyczności:

- $\forall x\ x = x$
- $\forall x \forall y\ x = y \rightarrow y = x$
- $\forall x \forall y \forall z\ x = y \wedge y = z \rightarrow x = z$.

Uwaga. Ta grupa aksjomatów występuje we wszystkich teoriach, w których używamy predykatu identyczności.

Warto pamiętać, że ani te aksjomaty, ani inne, w których występuje symbol $=$ identyczności nie gwarantują, że denotacja tego symbolu jest „prawdziwą" równością $=$.

Dla pełnej poprawności, powinniśmy używać innego symbolu dla predykatu identyczności w języku przedmiotowym (np.: $\doteq$), a innego dla relacji identyczności $=$, używanego w metajęzyku.

Nie robimy tego, ufając, iż Słuchaczki są już oswojone z różnicą między językiem przedmiotowym i metajęzykiem i że życzliwie, ze zrozumieniem tolerują tego typu drobne świństewka notacyjne.

Aksjomaty identyczności dla symboli $\bigcirc$, σ, $\oplus$ oraz $\otimes$:

- $\forall x \forall y\ x = y \rightarrow \sigma(x) = \sigma(y)$
- $\forall x \forall y \forall z\ x = y \rightarrow \oplus(x, z) = \oplus(y, z)$
- $\forall x \forall y \forall z\ x = y \rightarrow \oplus(z, x) = \oplus(z, y)$
- $\forall x \forall y \forall z\ x = y \rightarrow \otimes(x, z) = \otimes(y, z)$
- $\forall x \forall y \forall z\ x = y \rightarrow \otimes(z, x) = \otimes(z, y)$.

Uwaga. W aksjomatach tych nie występuje symbol $\bigcirc$, bo nie ma takiej potrzeby; stosowne „Leibnizjańskie" warunki dla $\bigcirc$ są konsekwencją pozostałych aksjomatów.

Aksjomaty specyficzne systemu Arytmetyki Robinsona:

- A_1: $\forall x \forall y\ (x \neq y \rightarrow \sigma(x) \neq \sigma(y))$
- A_2: $\forall x\ \bigcirc \neq \sigma(x)$
- A_3: $\forall x\ (x \neq \bigcirc \rightarrow \exists y\ (x = \sigma(y)))$
- A_4: $\forall x\ \oplus(x, \bigcirc) = x$
- A_5: $\forall x \forall y\ \oplus(x, \sigma(y)) = \sigma(\oplus(x, y))$
- A_6: $\forall x\ \otimes(x, \bigcirc) = \bigcirc$
- A_7: $\forall x \forall y\ \otimes(x, \sigma(y)) = \oplus(\otimes(x, y), x)$.

Modelem zamierzonym dla tych aksjomatów jest struktura, której uniwersum jest zbiór wszystkich (i tylko!) liczb naturalnych, a denotacjami poszczególnych terminów pozalogicznych są:

- symbolu $\bigcirc$ — liczba zero;
- symbolu σ — operacja następnika;
- symbolu $\oplus$ — operacja dodawania;
- symbolu $\otimes$ — operacja mnożenia.

Proste pytania

Jeśli aksjomaty te wydają ci się oczywiste, to witaj we Wspólnocie Intelektualnej Ludzkości!

Nie są chyba znani osobnicy, którym zdania te wydawałyby się fałszywe, przy podanej powyżej interpretacji zamierzonej.

Powstaje naturalnie pytanie: czy z tych aksjomatów ***wynikają*** (przy interpretacji symbolu $=$ jako relacji identyczności) **dokładnie wszystkie** prawdy arytmetyczne?

Proste pytania

Odpowiedzi na to, wydawałoby się proste, pytanie dostarczają ważne twierdzenia metalogiczne (o których opowiemy na wykładach dotyczących funkcji rekurencyjnych).

Odpowiedź jest **negatywna**; chociaż każde zdanie wyprowadzalne z aksjomatów jest prawdziwe w zamierzonej interpretacji, to jednak nie wszystkie zdania prawdziwe w tej interpretacji są wyprowadzalne z aksjomatów.

Ma to też związek z **nierozstrzygalnością** KRP.

Pierwsze trzy z powyższych aksjomatów mają gwarantować, że uniwersum interpretacji zamierzonej jest poprawnie utworzoną kolejką: na początku jest zero, potem następnik zera (czyli jedynka), potem następnik następnika zera (czyli następnik jedynki, a więc dwójka), i tak dalej. Za każdą liczbą naturalną jest dokładnie jedna liczba większa od niej o jeden, a od każdej liczby naturalnej jest tylko *skończenie* wiele „kroków wstecz", do zera.
Uwaga: pojęcia **skończoności** nie można wyrazić w języku pierwszego rzędu; ten intuicyjny komentarz czyniony jest w metajęzyku.

Aksjomaty A_4 oraz A_5 charakteryzują dodawanie, natomiast A_6 oraz A_7 ustalają własności mnożenia. Nie obawiaj się: w charakterystykach tych ***nie*** popełnia się błędnego koła.
Pokażemy teraz, jak uzyskać dowód prostej prawdy arytmetycznej w Arytmetyce Robinsona.
Oto dowód, iż $\oplus(\sigma(\sigma(\bigcirc)), \sigma(\sigma(\bigcirc))) = \sigma(\sigma(\sigma(\sigma(\bigcirc))))$, czyli że dwa i dwa jest cztery:

2+2=4

1.	$\forall x \ \oplus(x, \bigcirc) = x$	aksjomat A_4
2.	$\forall x \forall y \ \oplus(x, \sigma(y)) = \sigma(\oplus(x, y))$	aksjomat A_5
3.	$\neg(\oplus(\sigma(\sigma(\bigcirc)), \sigma(\sigma(\bigcirc))) = \sigma(\sigma(\sigma(\sigma(\bigcirc)))))$	z. d. n.
4.	$\oplus(\sigma(\sigma(\bigcirc)), \bigcirc) = \sigma(\sigma(\bigcirc))$	$R(\forall)$ dla $\sigma(\sigma(\bigcirc))$ w A_4
5.	$\forall y \ \oplus(\sigma(\sigma(\bigcirc)), \sigma(y)) = \sigma(\oplus(\sigma(\sigma(\bigcirc)), y))$	$R(\forall)$ dla $\sigma(\sigma(\bigcirc))$ w A_5
6.	$\oplus(\sigma(\sigma(\bigcirc)), \sigma(\bigcirc)) = \sigma(\oplus(\sigma(\sigma(\bigcirc)), \bigcirc))$	$R(\forall)$ dla $\bigcirc$ w 5.
7.	$\oplus(\sigma(\sigma(\bigcirc)), \sigma(\sigma(\bigcirc))) = \sigma(\oplus(\sigma(\sigma(\bigcirc)), \sigma(\bigcirc)))$	$R(\forall)$ dla $\sigma(\bigcirc)$ w 5.
8.	$\oplus(\sigma(\sigma(\bigcirc)), \sigma(\sigma(\bigcirc))) = \sigma(\oplus(\sigma(\sigma(\bigcirc)), \bigcirc))$	6. i 7., $R(=)$
9.	$\oplus(\sigma(\sigma(\bigcirc)), \sigma(\sigma(\bigcirc))) = \sigma(\sigma(\sigma(\sigma(\bigcirc))))$	4. i 8., $R(=)$
10.	$\times_{3,9}$	Sprzeczność: $3, 9$.

Rozszerzymy teraz system arytmetyki Robinsona poprzez dodanie do jego aksjomatów ***schematu*** aksjomatów, zwanego ***zasadą indukcji***. Otrzymany w ten sposób system nazywa się **Arytmetyką Peana**.

Stałe pozalogiczne Arytmetyki Peana są takie same, jak w Arytmetyce Robinsona. Również pierwsze siedem aksjomatów jest wspólnych dla obu systemów. Nowy w aksjomatyce Peana jest:

- P_8: $A(\bigcirc) \wedge \forall x\,(A(x) \rightarrow A(\sigma(x))) \rightarrow \forall x\, A(x)$

(dla dowolnej formuły A, o jednej zmiennej wolnej, języka Arytmetyki Peana).
P_8 nie jest jednym aksjomatem, lecz schematem (przeliczalnie wielu) aksjomatów. P_8 nazywamy **zasadą indukcji**.

O Arytmetyce Peana będziemy mówić nieco później, na III roku studiów.

Teoria algebr Boole'a

Teoria algebr Boole'a: pierwsza aksjomatyka.

Język teorii algebr Boole'a jest językiem KRP z identycznością oraz:

- symbolem funkcyjnym dwuargumentowym $\boxplus$, nazywającym *kres górny* (swoich argumentów);
- symbolem funkcyjnym dwuargumentowym $\boxtimes$, nazywającym *kres dolny* (swoich argumentów);
- symbolem funkcyjnym jednoargumentowym $\boxminus$, nazywającym *dopełnienie* (swojego argumentu);

Aksjomaty identyczności dla symboli $\boxplus$, $\boxtimes$, $\boxminus$:

- $\forall x \forall y \forall z\; x = y \rightarrow \boxplus(x, z) = \boxplus(y, z)$
- $\forall x \forall y \forall z\; x = y \rightarrow \boxtimes(x, z) = \boxtimes(y, z)$
- $\forall x \forall y \forall z\; x = y \rightarrow \boxplus(z, x) = \boxplus(z, y)$
- $\forall x \forall y \forall z\; x = y \rightarrow \boxtimes(z, x) = \boxtimes(z, y)$
- $\forall x \forall y\; x = y \rightarrow \boxminus(x) = \boxminus(y)$.

Teoria algebr Boole'a

Aksjomaty specyficzne teorii algebr Boole'a:

- B_1^1: $\forall x \forall y \ \boxplus(x, y) = \boxplus(y, x)$
- B_2^1: $\forall x \forall y \ \boxtimes(x, y) = \boxtimes(y, x)$
- B_3^1: $\forall x \forall y \forall z \ \boxplus(x, \boxplus(y, z)) = \boxplus(x, \boxplus(y, z))$
- B_4^1: $\forall x \forall y \forall z \ \boxtimes(x, \boxtimes(y, z)) = \boxtimes(x, \boxtimes(y, z))$
- B_5^1: $\forall x \forall y \ \boxplus(\boxtimes(x, y), y) = y$
- B_6^1: $\forall x \forall y \ \boxtimes(\boxplus(x, y), y) = y$
- B_7^1: $\forall x \forall y \forall z \ \boxplus(x, \boxtimes(y, z)) = \boxtimes(\boxplus(x, y), \boxplus(x, z))$
- B_8^1: $\forall x \forall y \forall z \ \boxtimes(x, \boxplus(y, z)) = \boxplus(\boxtimes(x, y), \boxtimes(x, z))$
- B_9^1: $\forall x \forall y \ \boxplus(\boxtimes(x, \boxminus(x)), y) = y$
- B_{10}^1: $\forall x \forall y \ \boxtimes(\boxplus(x, \boxminus(x)), y) = y$.

Teoria algebr Boole'a

Teoria algebr Boole'a: druga aksjomatyka.
Język teorii algebr Boole'a jest językiem KRP z identycznością oraz:

- symbolem funkcyjnym dwuargumentowym $\boxplus$, nazywającym *kres górny* (swoich argumentów);
- symbolem funkcyjnym dwuargumentowym $\boxtimes$, nazywającym *kres dolny* (swoich argumentów);
- symbolem funkcyjnym jednoargumentowym $\boxminus$, nazywającym *dopełnienie* (swojego argumentu);
- stałą indywiduową $\triangledown$, nazywającą *jedynkę* (element największy) algebry;
- stałą indywiduową $\vartriangle$, nazywającą *zero* (element najmniejszy) algebry.

Teoria algebr Boole'a

Aksjomaty identyczności dla symboli $\boxplus$, $\boxtimes$, $\boxminus$, $\triangledown$ oraz $\vartriangle$:

- $\forall x \forall y \forall z\ x = y \rightarrow \boxplus(x, z) = \boxplus(y, z)$
- $\forall x \forall y \forall z\ x = y \rightarrow \boxtimes(x, z) = \boxtimes(y, z)$
- $\forall x \forall y \forall z\ x = y \rightarrow \boxplus(z, x) = \boxplus(z, y)$
- $\forall x \forall y \forall z\ x = y \rightarrow \boxtimes(z, x) = \boxtimes(z, y)$
- $\forall x \forall y\ x = y \rightarrow \boxminus(x) = \boxminus(y)$.

Uwaga. Naprawdę potrzebne są tylko dwa pierwsze z tych aksjomatów. Pozostałe można wyprowadzić z innych aksjomatów teorii algebr Boole'a.

Teoria algebr Boole'a

Aksjomaty specyficzne teorii algebr Boole'a:

- B_2^1: $\forall x \ \boxplus(x, \vartriangle) = x$
- B_2^2: $\forall x \ \boxtimes(x, \triangledown) = x$
- B_2^3: $\forall x \ \boxplus(x, \boxminus(x)) = \triangledown$
- B_2^4: $\forall x \ \boxtimes(x, \boxminus(x)) = \vartriangle$
- B_2^5: $\forall x \forall y \ \boxplus(x, y) = \boxplus(y, x)$
- B_2^6: $\forall x \forall y \ \boxtimes(x, y) = \boxtimes(y, x)$
- B_2^7: $\forall x \forall y \forall z \ \boxplus(x, \boxtimes(y, z)) = \boxtimes(\boxplus(x, y), \boxplus(x, z))$
- B_2^8: $\forall x \forall y \forall z \ \boxtimes(x, \boxplus(y, z)) = \boxplus(\boxtimes(x, y), \boxtimes(x, z))$

Teoria algebr Boole'a

Interpretacjami aksjomatów teorii algebr Boole'a są (oczywiście!) algebry Boole'a, tj. struktury postaci:

$$\langle A, \boxplus_A, \boxtimes_A, \boxminus_A, \nabla_A, \triangle_A \rangle$$

gdzie A jest pewnym zbiorem, a $\boxplus_A$ i $\boxtimes_A$ są dwuargumentowymi operacjami na A, $\boxminus_A$ operacją jednoargumentową na A i ∇_A oraz $\triangle_A$ są wyróżnionymi elementami zbioru A (jedynką i zerem algebry, odpowiednio).

W każdej algebrze Boole'a można określić częściowy porządek $\leqslant_A$:
$x \leqslant_A y$ wtedy i tylko wtedy, gdy $x = \boxtimes_A(x, y)$
lub, równoważnie:
$x \leqslant_A y$ wtedy i tylko wtedy, gdy $y = \boxplus_A(x, y)$.

Przykłady algebr Boole'a

- **Algebra podzbiorów**. Wszystkie podzbiory dowolnego zbioru U wraz z operacjami teoriomnogościowymi: sumy (kres górny), iloczynu (kres dolny), dopełnienia (do U), zbiorem U jako jedynką oraz zbiorem pustym $\emptyset$ jako zerem tworzą algebrę Boole'a.
- **Algebra wartości logicznych**. Funktory odpowiadające alternatywie nierozłącznej, koniunkcji oraz negacji spełniają aksjomaty teorii algebr Boole'a. Tak więc, zbiór dwuelementowy złożony z obiektów nazywanych Prawdą oraz Fałszem wraz z tymi funktorami tworzy algebrę Boole'a.

Teoria grup

W tym przypadku używany język to język KRP z identycznością oraz:

- jednym dwuargumentowym symbolem funkcyjnym $\boxdot$, nazywającym *działanie* w grupie;
- jedną stałą indywiduową ε nazywającą element *neutralny* (względem działania) w grupie.

Aksjomaty teorii grup w tym języku:
Aksjomaty identyczności dla symboli $\boxdot$ oraz ε:

$$\forall x \forall y \forall z \; x = y \rightarrow \boxdot(x, z) = \boxdot(y, z)$$
$$\forall x \forall y \forall z \; x = y \rightarrow \boxdot(z, x) = \boxdot(z, y).$$

Aksjomaty specyficzne:

- G_1^2: $\forall x \forall y \; \boxdot(x, \boxdot(y, z)) = \boxdot(\boxdot(x, y), z)$
- G_2^2: $\forall x \; \boxdot(x, \varepsilon) = x$
- G_3^2: $\forall x \; \boxdot(\varepsilon, x) = x$
- G_4^2: $\forall x \exists y \; \boxdot(x, y) = \varepsilon$
- G_5^2: $\forall x \exists y \; \boxdot(y, x) = \varepsilon$.

Dowód jedyności elementu neutralnego, tj. zdania:

(G_6^2) $\forall z(\forall x\,(\boxdot(x,z)=x \wedge \boxdot(z,x)=x) \rightarrow \varepsilon = z)$.

1.	$\forall x\ \boxdot(x,\varepsilon)=x$	aksjomat G_2^2
2.	$\forall x\ \boxdot(\varepsilon,x)=x$	aksjomat G_3^2
3.	$\neg\forall z(\forall x\,(\boxdot(x,z)=x \wedge \boxdot(z,x)=x) \rightarrow \varepsilon = z)$	negacja G_6^2 (zał. dowodu nie wprost)
4.	$\neg(\forall x\,(\boxdot(x,a)=x \wedge \boxdot(a,x)=x) \rightarrow \varepsilon = a)$	$R(\neg\forall)$, 3
5_g. 5_d.	$\forall x\,(\boxdot(x,a)=x \wedge \boxdot(a,x)=x)$ $\neg\varepsilon = a$	$R(\neg\rightarrow)$, 4
6.	$\boxdot(a,\varepsilon)=a$	$R(\forall)$ dla a, 1
7.	$\boxdot(\varepsilon,a)=a$	$R(\forall)$ dla a, 2
8.	$\boxdot(\varepsilon,a)=\varepsilon \wedge \boxdot(a,\varepsilon)=\varepsilon$	$R(\forall)$ dla ε, 5_g
9_g. 9_d.	$\boxdot(\varepsilon,a)=\varepsilon$ $\boxdot(a,\varepsilon)=\varepsilon$	$R(\wedge)$, 8
10.	$\varepsilon = a$	$R(=)$, 9_g, 7
11.	$\times_{5_d,10}$	Sprzeczność: $5_d, 10$.

Przykłady grup

- Zbiór liczb całkowitych z działaniem dodawania oraz zerem jako elementem neutralnym tworzy grupę.
- Zbiór liczb rzeczywistych różnych od zera z działaniem mnożenia oraz jedynką jako elementem neutralnym tworzy grupę.
- Zbiór wszystkich wzajemnie jednoznacznych odwzorowań danego zbioru na siebie tworzy grupę. Działaniem jest tu złożenie funkcji, a elementem neutralnym funkcja identycznościowa.

Koniec

Na następnym, ostatnim wykładzie powiemy o:

- pewnych metalogicznych własnościach KRP;
- tematach egzaminacyjnych.