<u>Wykład I</u> Algebra

Algebra – jeden z najstarszych działów matematyki powstały już w starożytności. Słowo *algebra* pochodzi z tytułu dzieła uczonego arabskiego Al Chuwarizmiego (VIII/IX wiek) *Hisab al-dżabr wa'l-mukabala* (*O odtwarzaniu i przeciwstawianiu*) dotyczącego przenoszenia wyrazów o współczynnikach ujemnych z jednej strony równania na drugą oraz skracania równań stronami. Początkowo, jak wskazuje pochodzenie jej nazwy, algebra zajmowała się rozwiązywaniem równań pierwszego i drugiego stopnia o współczynnikach liczbowych. Nieudane próby znalezienia wzorów na pierwiastki równań wyższych stopni zahamowały na pewien czas rozwój algebry w tym kierunku. Dopiero odkrycie w 1832 roku przez matematyka francuskiego Évariste'a Galois warunków koniecznych i dostatecznych na istnienie takich wzorów zapoczątkowało nowy kierunek badań noszący nazwę teorii Galois. Kilka lat wcześniej matematyk norweski Niels Abel wykazał, że nie istnieją ogólne wzory na pierwiastki równań stopnia wyższego niż czwarty.

Wikipedia

Algebra obecnie - nauka o strukturach algebraicznych

<u>Zalecany podręcznik:</u> Bolesław Gleichgewicht, *Algebra,*
Oficyna Wydawnicza GiS, Wrocław 2004

<u>Terminologia i symbolika</u>

<u>Symbolika logiczna</u>

Implikacja o poprzedniku p i następniku q: $p \Rightarrow q$

Równoważność zdań p i q: $p \Leftrightarrow q$

Koniunkcja zdań p i q: $p \wedge q$

Alternatywa zdań p, q: $p \vee q$

Prawdziwość logiczna (1- prawda, 0 - fałsz)

p	q	$p \Rightarrow q$	$p \Leftrightarrow q$	$p \wedge q$	$p \vee q$
1	1	1	1	1	1
1	0	0	0	0	1
0	1	1	0	0	1
0	0	1	1	0	0

Wykład I cd. Algebra

Symbolika teorii mnogości

a jest elementem zbioru *A*: $a \in A$
a nie jest elementem zbioru *A*: $a \notin A$
A jest zbiorem elementów x należących do *X* spełniających warunek $\varphi(x)$:
$A = \{x \in X : \varphi(x)\}$

kwantyfikator ogólny: $\forall$
kwantyfikator szczegółowy: $\exists$

Zbiór pusty: ϕ

Zbiór *A* jest podzbiorem *B*: $A \subset B$ tzn. $\forall x \in A \Rightarrow x \in B$ (*B* zawiera *A*)
zachodzą związki: $A \subset A$ i $(A \subset B) \wedge (B \subset C) \Rightarrow (A \subset C)$

Zbiór *A* = *B*: $(x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)$ lub $x \in A \Leftrightarrow x \in B$

Iloczyn (część wspólna) zbiorów *A* i *B*: $A \cap B = \{x : x \in A \wedge x \in B\}$

Suma zbiorów *A* i *B*: $A \cup B = \{x : x \in A \vee x \in B\}$

Różnica zbiorów *A* i *B*: $A \setminus B = \{x : x \in A \wedge x \notin B\}$

N - zbiór liczb naturalnych, $0 \notin \mathbf{N}$
Z - zbiór liczb całkowitych
Q - zbiór liczb wymiernych
(każdą liczbę wymierną można przedstawić jako n/m, $n \in \mathbf{Z}$, $m \in \mathbf{Z}$)
R - zbiór liczb rzeczywistych

Iloczyn kartezjański zbiorów *A* i *B*: $A \times B = \{(x, y) : x \in A \wedge y \in B\}$

<u>Wykład I cd.</u> Algebra

<u>Funkcje i działania</u>

<u>Funkcja $f: X \to Y$</u>

Przyporządkowanie każdemu elementowi ze zbioru X (dziedziny) jednego i tylko jednego elementu ze zbioru Y (zbioru wartości).

<u>Funkcja różnowartościowa $f: X \to Y$</u>

$\forall x_1, x_2 \in X, \quad x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ lub $\forall x_1, x_2 \in X, \quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

<u>Funkcja odwrotna $f^{-1}: Y \to X$</u> do funkcji <u>$f: X \to Y$</u>

$\forall y \in Y \quad \exists x \in X \quad y = f(x) \Rightarrow x = f^{-1}(y)$

<u>Działanie</u> w niepustym zbiorze A nazywamy każde odwzorowanie kwadratu kartezjańskiego $A \times A$ w A ($A \times A \to A$) $\forall a, b \in A \quad \exists c \in A \quad c = a \circ b$

<u>Działanie przemienne</u> $\forall a, b \in A \quad a \circ b = b \circ a$

<u>Działanie łączne</u> $\forall a, b, c \in A \quad a \circ (b \circ c) = (b \circ a) \circ c$

<u>Element neutralny działania</u> $\exists e \in A \quad \forall a \in A \quad a \circ e = e \circ a = a$

<u>Grupa</u>

Zbiór G, w którym określone jest działanie nazywamy grupą jeśli

1) działanie $\circ$ jest łączne,
2) istnieje w G element neutralny e (jedność),
3) każdy element ma element odwrotny: $\forall g \in G \quad \exists g^{-1} \in G \quad g^{-1} \circ g = g \circ g^{-1} = e$.

<u>Grupa przemienna</u> (abelowa) $\forall g, h \in G \quad g \circ h = h \circ g$

Twierdzenie 1: $\forall g \in G \quad (g^{-1})^{-1} = g$

Twierdzenie 2: $\forall g, h \in G \quad (g \circ h)^{-1} = h^{-1} \circ g^{-1}$

<u>Podgrupa H grupy G</u>: podzbiór H grupy G z działaniem grupowym, takim jak w grupie G, będący grupą.

<u>Wykład I cd.</u> Algebra

<u>Pierścienie i ciała</u>

Rozdzielczość działania $\otimes$ względem działania $\oplus$: $a\otimes(b\oplus c)=(a\otimes b)\oplus(a\otimes c)$

<u>Pierścieniem</u> nazywamy zbiór *R*, w którym są dwa działania $\otimes$ i $\oplus$, jeśli spełnione są warunki:

1) *R* jest grupą abelową z działaniem $\oplus$,
2) działanie $\otimes$ jest rozdzielna względem działania $\oplus$:
   $\forall a,b,c\in R \quad a\otimes(b\oplus c)=(a\otimes b)\oplus(a\otimes c)$,
3) działanie $\otimes$ jest łączne:
   $\forall a,b,c\in R \quad a\otimes(b\otimes c)=(a\otimes b)\otimes c$.

<u>Ciałem</u> jest pierścień *K*, który spełnia następujące warunki:

1) *K* ma więcej niż jeden element,
2) $K\setminus\{0\}$ jest grupą abelową względem $\otimes$ (0 element naturalny $\oplus$).

Ciało to zbiór *K* z dwoma działaniami $\otimes$ i $\oplus$ spełniającymi warunki:

1) $\forall a,b,c\in K \quad a\oplus(b\oplus c)=(a\oplus b)\oplus c$,
2) $\exists e\in K \quad a\oplus 0=0\oplus a=a$,
3) $\forall a\in K \quad \exists a'\in K \quad a\oplus a'=a'\oplus a=0$,
4) $\forall a,b\in K \quad a\oplus b=b\oplus a$,
5) $\forall a,b,c\in K \quad a\otimes(b\otimes c)=(a\otimes b)\otimes c$,
6) $\exists e\in K \quad a\otimes e=e\otimes a=a$,
7) $\forall a\in K \quad \exists a^{-1}\in K \quad a\otimes a^{-1}=a^{-1}\otimes a=e$,
8) $\forall a,b\in K \quad a\otimes b=b\otimes a$,
9) $\forall a,b,c\in K \quad a\otimes(b\oplus c)=(a\otimes b)\oplus(a\otimes c)$,

1), 2), 3) *K* grupą ze względu na $\oplus$; 4) *K* grupą abelową ze względu na $\oplus$;
5), 6), 7) *K* grupą ze względu na $\otimes$; 8) *K* grupą abelową ze względu na $\otimes$;
9) rozdzielczość działania $\otimes$ względem działania $\oplus$.

Podzbiór $P\subset K$ jest <u>podciałem</u> ciała *K*, jeśli

1) $0,e\in P$,
2) $\forall a,b\in P \quad \exists c\in P \quad a\oplus b=c$,
3) $\forall a,b\in P \quad \exists c\in P \quad a\otimes b=c$.

Wykład I cd. Algebra

Odwzorowania

Funkcja $f: X \to Y$ jest odwzorowaniem zbioru X na Y, jeśli
$\forall y \in Y \quad \exists x \in X \quad y = f(x)$.

Jeśli f jest różnowartościowa to odwzorowanie zbioru X na Y jest wzajemnie jednoznaczne, jest bijekcją.

Odwzorowanie f grupy G z działaniem $\circ$ na grupę H z działaniem $\bullet$ jest izomorfizmem (H jest izomorficznym obrazem G), jeśli

1) f jest bijekcją,
2) $\forall a, b \in G \quad f(a \circ b) = f(a) \bullet f(b)$.