Geometria z Algebrą Liniową I

Arkadiusz Męcel

WYKŁAD 2, 27.10.2020 r.

Na ostatnim wykładzie:

- równania i układy równań liniowych o współczynnikach rzeczywistych,
- układy równoważne,
- rozwiązanie ogólne,
- macierze, macierze układów równań liniowych,
- postać schodkowa i postać schodkowa zredukowana macierzy,
- operacje elementarne na wierszach,
- zapowiedź tematu: ciała, wprowadzenie do ciał reszt modulo liczba pierwsza.

Rola współczynników w układach równań liniowych

Do tej pory współczynnikami równania liniowego U postaci

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

były liczby rzeczywiste, czyli $a_1, a_2, \ldots, a_n, b \in \mathbb{R}$. W takiej sytuacji sprawdzamy, że liczby $s_1, \ldots, s_n$ są rozwiązaniem równania przez wykonanie **operacji** dodawania i mnożenia w $\mathbb{R}$ postaci: $a_1 \cdot s_1 + a_2 \cdot s_2 + \ldots + a_n \cdot s_n$ żądając, by wynikiem było b.

Czy zamiast $\mathbb{R}$ z operacjami $+$ oraz $\cdot$ można rozważać układy równań liniowych, gdzie współczynnikami są **inne zbiory** X z **innymi operacjami** dodawania i mnożenia $\boxplus, \boxtimes$?

Definicja 1.

Niech X będzie zbiorem. Przez X^2 rozumieć będziemy zbiór ciągów postaci (x_1, x_2), gdzie $x_1, x_2 \in X$. **Działaniem dwuargumentowym w zbiorze** X nazywamy każdą funkcję $\omega : X^2 \to X$.

Definicja 1.

Niech X będzie zbiorem. Przez X^2 rozumieć będziemy zbiór ciągów postaci (x_1, x_2), gdzie $x_1, x_2 \in X$. **Działaniem dwuargumentowym w zbiorze** X nazywamy każdą funkcję $\omega : X^2 \to X$.

Przykłady:

zbiór X	działanie ω
liczby rzeczywiste/wymierne/całkowite/naturalne	dodawanie/mnożenie
liczby rzeczywiste	$a \boxplus b = a + b + ab$
zbiór podzbiorów danego zbioru	suma/częśc wspólna
zbiór funkcji ze zbioru X na zbiór X	złożenie

Definicja 1.

Niech X będzie zbiorem. Przez X^2 rozumieć będziemy zbiór ciągów postaci (x_1, x_2), gdzie $x_1, x_2 \in X$. **Działaniem dwuargumentowym w zbiorze** X nazywamy każdą funkcję $\omega : X^2 \to X$.

Przykłady:

zbiór X	działanie ω
liczby rzeczywiste/wymierne/całkowite/naturalne	dodawanie/mnożenie
liczby rzeczywiste	$a \boxplus b = a + b + ab$
zbiór podzbiorów danego zbioru	suma/częśc wspólna
zbiór funkcji ze zbioru X na zbiór X	złożenie

Działaniem dwuargumentowym na zbiorze liczb naturalnych nie jest odejmowanie, bo np. $1 - 3 \notin \mathbb{N}$.

Definicja 2.

Niech $* : X^2 \to X$ będzie działaniem dwuargumentowym na zbiorze X. Mówimy, że $*$ jest działaniem:

- **łącznym**, jeśli dla każdych $a, b, c \in X$ mamy $(a * b) * c = a * (b * c)$,

Definicja 2.

Niech $* : X^2 \to X$ będzie działaniem dwuargumentowym na zbiorze X. Mówimy, że $*$ jest działaniem:

- **łącznym**, jeśli dla każdych $a, b, c \in X$ mamy $(a * b) * c = a * (b * c)$,
- **przemiennym**, jeśli dla każdych $a, b \in X$ mamy $a * b = b * a$.

Definicja 2.

Niech $* : X^2 \to X$ będzie działaniem dwuargumentowym na zbiorze X. Mówimy, że $*$ jest działaniem:

- **łącznym**, jeśli dla każdych $a, b, c \in X$ mamy $(a * b) * c = a * (b * c)$,
- **przemiennym**, jeśli dla każdych $a, b \in X$ mamy $a * b = b * a$.

Przykłady:

- działanie $a \boxplus b = a^2 + b^2$ na zbiorze $\mathbb{R}$ nie jest łączne, bo: $(1 \boxplus 2) \boxplus 3 = 34$, zaś $1 \boxplus (2 \boxplus 3) = 170$.

Definicja 2.

Niech $* : X^2 \to X$ będzie działaniem dwuargumentowym na zbiorze X. Mówimy, że $*$ jest działaniem:

- **łącznym**, jeśli dla każdych $a, b, c \in X$ mamy $(a * b) * c = a * (b * c)$,
- **przemiennym**, jeśli dla każdych $a, b \in X$ mamy $a * b = b * a$.

Przykłady:

- działanie $a \boxplus b = a^2 + b^2$ na zbiorze $\mathbb{R}$ nie jest łączne, bo: $(1 \boxplus 2) \boxplus 3 = 34$, zaś $1 \boxplus (2 \boxplus 3) = 170$.
- działanie $a \boxplus b = a + b + ab$ na zbiorze $\mathbb{R}$ jest łączne i przemienne,

Definicja 2.

Niech $* : X^2 \to X$ będzie działaniem dwuargumentowym na zbiorze X. Mówimy, że $*$ jest działaniem:

- **łącznym**, jeśli dla każdych $a, b, c \in X$ mamy $(a * b) * c = a * (b * c)$,
- **przemiennym**, jeśli dla każdych $a, b \in X$ mamy $a * b = b * a$.

Przykłady:

- działanie $a \boxplus b = a^2 + b^2$ na zbiorze $\mathbb{R}$ nie jest łączne, bo: $(1 \boxplus 2) \boxplus 3 = 34$, zaś $1 \boxplus (2 \boxplus 3) = 170$.
- działanie $a \boxplus b = a + b + ab$ na zbiorze $\mathbb{R}$ jest łączne i przemienne,
- działanie $a \boxtimes b = a^b$ na zbiorze $\mathbb{R}_+$ nie jest przemienne,

Definicja 2.

Niech $* : X^2 \to X$ będzie działaniem dwuargumentowym na zbiorze X. Mówimy, że $*$ jest działaniem:

- **łącznym**, jeśli dla każdych $a, b, c \in X$ mamy $(a * b) * c = a * (b * c)$,
- **przemiennym**, jeśli dla każdych $a, b \in X$ mamy $a * b = b * a$.

Przykłady:

- działanie $a \boxplus b = a^2 + b^2$ na zbiorze $\mathbb{R}$ nie jest łączne, bo: $(1 \boxplus 2) \boxplus 3 = 34$, zaś $1 \boxplus (2 \boxplus 3) = 170$.
- działanie $a \boxplus b = a + b + ab$ na zbiorze $\mathbb{R}$ jest łączne i przemienne,
- działanie $a \boxtimes b = a^b$ na zbiorze $\mathbb{R}_+$ nie jest przemienne,
- złożenie w zbiorze bijekcji (czyli 1-1 i „na”) zbioru $\mathbb{R}$ nie jest przemienne.

Gdy operacje nie mają istotnych własności...

- Niech $\Sigma_{a,b}$ będzie zbiorem złożonym ze wszystkich słów złożonych z liter a, b, np. a, aaa, $abaa$, $bbba$ oraz słowa pustego ϵ,

Gdy operacje nie mają istotnych własności...

- Niech $\Sigma_{a,b}$ będzie zbiorem złożonym ze wszystkich słów złożonych z liter a, b, np. a, aaa, $abaa$, $bbba$ oraz słowa pustego ϵ,
- W $\Sigma_{a,b}$ wprowadzamy działanie dwuargumentowe (tzw. konkatenację) $\cdot$ postaci $w_1 \cdot w_2 = w_1 w_2$, np. $aba \cdot bb = ababb$ lub $\epsilon \cdot abb = abb$.

Gdy operacje nie mają istotnych własności...

- Niech $\Sigma_{a,b}$ będzie zbiorem złożonym ze wszystkich słów złożonych z liter a, b, np. $a, aaa, abaa, bbba$ oraz słowa pustego ϵ,
- W $\Sigma_{a,b}$ wprowadzamy działanie dwuargumentowe (tzw. konkatenację) $\cdot$ postaci $w_1 \cdot w_2 = w_1 w_2$, np. $aba \cdot bb = ababb$ lub $\epsilon \cdot abb = abb$.
- Rozważamy zbiór $P(\Sigma_{a,b})$ złożony z podzbiorów (także nieskończonych!) zbioru $\Sigma_{a,b}$, np. $\{\epsilon, a, ab\}$, $\{a, aa, aaa, aaaa, \ldots\}$, $\{ab, abab, ababab, \ldots\}$.

Gdy operacje nie mają istotnych własności...

- Niech $\Sigma_{a,b}$ będzie zbiorem złożonym ze wszystkich słów złożonych z liter a, b, np. $a, aaa, abaa, bbba$ oraz słowa pustego ϵ,
- W $\Sigma_{a,b}$ wprowadzamy działanie dwuargumentowe (tzw. konkatenację) $\cdot$ postaci $w_1 \cdot w_2 = w_1 w_2$, np. $aba \cdot bb = ababb$ lub $\epsilon \cdot abb = abb$.
- Rozważamy zbiór $P(\Sigma_{a,b})$ złożony z podzbiorów (także nieskończonych!) zbioru $\Sigma_{a,b}$, np. $\{\epsilon, a, ab\}$, $\{a, aa, aaa, aaaa, \ldots\}$, $\{ab, abab, ababab, \ldots\}$.
- W $P(\Sigma_{a,b})$ wprowadzamy działanie $+$ oznaczające sumę mnogościową zbiorów, np. $\{aba, bb, ab\} + \{a, aa, bb\} = \{aba, bb, ab, a, aa\}$.

Gdy operacje nie mają istotnych własności...

- Niech $\Sigma_{a,b}$ będzie zbiorem złożonym ze wszystkich słów złożonych z liter a, b, np. $a, aaa, abaa, bbba$ oraz słowa pustego ϵ,
- W $\Sigma_{a,b}$ wprowadzamy działanie dwuargumentowe (tzw. konkatenację) $\cdot$ postaci $w_1 \cdot w_2 = w_1 w_2$, np. $aba \cdot bb = ababb$ lub $\epsilon \cdot abb = abb$.
- Rozważamy zbiór $P(\Sigma_{a,b})$ złożony z podzbiorów (także nieskończonych!) zbioru $\Sigma_{a,b}$, np. $\{\epsilon, a, ab\}$, $\{a, aa, aaa, aaaa, \ldots\}$, $\{ab, abab, ababab, \ldots\}$.
- W $P(\Sigma_{a,b})$ wprowadzamy działanie $+$ oznaczające sumę mnogościową zbiorów, np. $\{aba, bb, ab\} + \{a, aa, bb\} = \{aba, bb, ab, a, aa\}$.
- W $P(\Sigma_{a,b})$ wprowadzamy działanie $\cdot$ zdefiniowane w następujący sposób. Zbiór $A \cdot B$ złożony jest ze słów postaci $a \cdot b$, gdzie $a \in A, b \in B$. Np. $\{aba, bb, ab\} \cdot \{a, aa, bb\} = \{abaa, abaaa, ababb, bba, bbaa, bbbb, aba, abbb\}$

Gdy operacje nie mają istotnych własności...

- Niech $\Sigma_{a,b}$ będzie zbiorem złożonym ze wszystkich słów złożonych z liter a, b, np. $a, aaa, abaa, bbba$ oraz słowa pustego ϵ,
- W $\Sigma_{a,b}$ wprowadzamy działanie dwuargumentowe (tzw. konkatenację) $\cdot$ postaci $w_1 \cdot w_2 = w_1 w_2$, np. $aba \cdot bb = ababb$ lub $\epsilon \cdot abb = abb$.
- Rozważamy zbiór $P(\Sigma_{a,b})$ złożony z podzbiorów (także nieskończonych!) zbioru $\Sigma_{a,b}$, np. $\{\epsilon, a, ab\}$, $\{a, aa, aaa, aaaa, \ldots\}$, $\{ab, abab, ababab, \ldots\}$.
- W $P(\Sigma_{a,b})$ wprowadzamy działanie $+$ oznaczające sumę mnogościową zbiorów, np. $\{aba, bb, ab\} + \{a, aa, bb\} = \{aba, bb, ab, a, aa\}$.
- W $P(\Sigma_{a,b})$ wprowadzamy działanie $\cdot$ zdefiniowane w następujący sposób. Zbiór $A \cdot B$ złożony jest ze słów postaci $a \cdot b$, gdzie $a \in A, b \in B$. Np. $\{aba, bb, ab\} \cdot \{a, aa, bb\} = \{abaa, abaaa, ababb, bba, bbaa, bbbb, aba, abbb\}$
- Rozważamy równania liniowe o współczynnikach w $P(\Sigma_{a,b})$, np:

$$\{a, aa\} \cdot x_1 + \{bb\} \cdot x_2 = \{ab, aab, bbb, aaab\},$$

którego **rozwiązaniem są elementy $P(\Sigma_{a,b})$**, czyli: $x_1 = \{b, ab\}$, $x_2 = \{b\}$.

Gdy operacje nie mają istotnych własności...

- Strona, z której piszemy współczynniki. Równania:

$$\{a\} \cdot x_1 = \{abaa\}, \quad x_1 \cdot \{a\} = \{abaa\}$$

mają różne rozwiązania! Przyczyna – nieprzemienność działania $\cdot$.

Gdy operacje nie mają istotnych własności...

- Strona, z której piszemy współczynniki. Równania:

$$\{a\} \cdot x_1 = \{abaa\}, \quad x_1 \cdot \{a\} = \{abaa\}$$

  mają różne rozwiązania! Przyczyna – nieprzemienność działania $\cdot$.

- Brak elementów *przeciwnych* i *odwrotnych*. Mając układ:

$$\begin{cases} \{a\} \cdot x_1 = \{abaa\} \\ \{a\} \cdot x_1 = \{aba\}. \end{cases}$$

  nie sprowadzimy jego *macierzy* do postaci schodkowej lub zredukowanej, co utrudnia sprawdzanie kiedy jest on sprzeczny!

Gdy operacje nie mają istotnych własności...

- Strona, z której piszemy współczynniki. Równania:

$$\{a\} \cdot x_1 = \{abaa\}, \quad x_1 \cdot \{a\} = \{abaa\}$$

  mają różne rozwiązania! Przyczyna – nieprzemienność działania $\cdot$.

- Brak elementów *przeciwnych* i *odwrotnych*. Mając układ:

$$\begin{cases} \{a\} \cdot x_1 = \{abaa\} \\ \{a\} \cdot x_1 = \{aba\}. \end{cases}$$

  nie sprowadzimy jego *macierzy* do postaci schodkowej lub zredukowanej, co utrudnia sprawdzanie kiedy jest on sprzeczny!

- Układy jednorodne nie mają sensu. Trudność z opisem rozwiązań.

Definicja 3.

Ciałem nazywamy piątkę $(K, \boxplus, \boxtimes, 0, 1)$, gdzie K jest zbiorem przynajmniej dwuelementowym z wyróżnionymi elementami $0 \neq 1$, zwanymi zerem i jedynką, zaś $\boxplus$, $\boxtimes$ są dwuargumentowymi działaniami zwanymi dodawaniem i mnożeniem, spełniającymi następujące **aksjomaty ciała**:

1)	$(a \boxplus b) \boxplus c = a \boxplus (b \boxplus c)$	$\forall_{a,b,c \in K}$	łączność dodawania
2)	$a \boxplus b = b \boxplus a$	$\forall_{a,b \in K}$	przemienność dodawania
3)	$a \boxplus 0 = a = 0 \boxplus a$	$\forall_{a \in K}$	własność elementu 0
4)	$a \boxplus b = 0 = b \boxplus a$	$\forall_{a \in K} \exists_{b \in K}$	element przeciwny
5)	$(a \boxtimes b) \boxtimes c = a \boxtimes (b \boxtimes c)$	$\forall_{a,b,c \in K}$	łączność mnożenia
6)	$a \boxtimes b = b \boxtimes a$	$\forall_{a,b \in K}$	przemienność mnożenia
7)	$a \boxtimes 1 = 1 \boxtimes a = a$	$\forall_{a \in K}$	własność elementu 1
8)	$a \boxtimes b = b \boxtimes a = 1$	$\forall_{a \in K \setminus \{0\}} \exists_{b \in K}$	odwrotność dla $a \neq 0$
9)	$a \boxtimes (b \boxplus c) = (a \boxtimes b) \boxplus (a \boxtimes c)$	$\forall_{a,b,c \in K}$	rozdzielność $\boxtimes$ wzgl. $\boxplus$

Elementy: przeciwny i odwrotny.

Fakt 1.

Niech K będzie ciałem. Dla każdego elementu $a \in K$ istnieje dokładnie jeden element przeciwny do a. Dla każdego niezerowego elementu $b \in K$ istnieje dokładnie jeden element odwrotny do b.

Elementy: przeciwny i odwrotny.

Fakt 1.

Niech K będzie ciałem. Dla każdego elementu $a \in K$ istnieje dokładnie jeden element przeciwny do a. Dla każdego niezerowego elementu $b \in K$ istnieje dokładnie jeden element odwrotny do b.

Dowód (istnienia dokładnie jednego elementu przeciwnego). Załóżmy przeciwnie, że dla pewnych elementów x, x' ciała K mamy $a \boxplus x = 0 = a \boxplus x'$.

Elementy: przeciwny i odwrotny.

Fakt 1.

Niech K będzie ciałem. Dla każdego elementu $a \in K$ istnieje dokładnie jeden element przeciwny do a. Dla każdego niezerowego elementu $b \in K$ istnieje dokładnie jeden element odwrotny do b.

Dowód (istnienia dokładnie jednego elementu przeciwnego). Załóżmy przeciwnie, że dla pewnych elementów x, x' ciała K mamy $a \boxplus x = 0 = a \boxplus x'$. Korzystamy dalej z aksjomatów ciała i powyższej równości:

Elementy: przeciwny i odwrotny.

Fakt 1.

Niech K będzie ciałem. Dla każdego elementu $a \in K$ istnieje dokładnie jeden element przeciwny do a. Dla każdego niezerowego elementu $b \in K$ istnieje dokładnie jeden element odwrotny do b.

Dowód (istnienia dokładnie jednego elementu przeciwnego). Załóżmy przeciwnie, że dla pewnych elementów x, x' ciała K mamy $a \boxplus x = 0 = a \boxplus x'$. Korzystamy dalej z aksjomatów ciała i powyższej równości:

$$x \quad = x \boxplus 0 \qquad \text{(aksjomat 3 - wł. elementu 0)}$$

Elementy: przeciwny i odwrotny.

Fakt 1.

Niech K będzie ciałem. Dla każdego elementu $a \in K$ istnieje dokładnie jeden element przeciwny do a. Dla każdego niezerowego elementu $b \in K$ istnieje dokładnie jeden element odwrotny do b.

Dowód (istnienia dokładnie jednego elementu przeciwnego). Załóżmy przeciwnie, że dla pewnych elementów x, x' ciała K mamy $a \boxplus x = 0 = a \boxplus x'$. Korzystamy dalej z aksjomatów ciała i powyższej równości:

$$\begin{aligned} x &= x \boxplus 0 && \text{(aksjomat 3 - wł. elementu 0)} \\ &= x \boxplus (a \boxplus x') && \text{(równość wyżej)} \end{aligned}$$

Elementy: przeciwny i odwrotny.

Fakt 1.

Niech K będzie ciałem. Dla każdego elementu $a \in K$ istnieje dokładnie jeden element przeciwny do a. Dla każdego niezerowego elementu $b \in K$ istnieje dokładnie jeden element odwrotny do b.

Dowód (istnienia dokładnie jednego elementu przeciwnego). Załóżmy przeciwnie, że dla pewnych elementów x, x' ciała K mamy $a \boxplus x = 0 = a \boxplus x'$. Korzystamy dalej z aksjomatów ciała i powyższej równości:

$$\begin{aligned} x &= x \boxplus 0 && \text{(aksjomat 3 - wł. elementu 0)} \\ &= x \boxplus (a \boxplus x') && \text{(równość wyżej)} \\ &= (x \boxplus a) \boxplus x' && \text{(aksjomat 1 - łączność } \boxplus\text{)} \end{aligned}$$

Elementy: przeciwny i odwrotny.

Fakt 1.

Niech K będzie ciałem. Dla każdego elementu $a \in K$ istnieje dokładnie jeden element przeciwny do a. Dla każdego niezerowego elementu $b \in K$ istnieje dokładnie jeden element odwrotny do b.

Dowód (istnienia dokładnie jednego elementu przeciwnego). Załóżmy przeciwnie, że dla pewnych elementów x, x' ciała K mamy $a \boxplus x = 0 = a \boxplus x'$. Korzystamy dalej z aksjomatów ciała i powyższej równości:

$$\begin{aligned} x &= x \boxplus 0 && \text{(aksjomat 3 - wł. elementu 0)} \\ &= x \boxplus (a \boxplus x') && \text{(równość wyżej)} \\ &= (x \boxplus a) \boxplus x' && \text{(aksjomat 1 - łączność } \boxplus) \\ &= x' \boxplus (a \boxplus x) && \text{(aksjomat 2 - przemienność } \boxplus) \end{aligned}$$

Elementy: przeciwny i odwrotny.

Fakt 1.

Niech K będzie ciałem. Dla każdego elementu $a \in K$ istnieje dokładnie jeden element przeciwny do a. Dla każdego niezerowego elementu $b \in K$ istnieje dokładnie jeden element odwrotny do b.

Dowód (istnienia dokładnie jednego elementu przeciwnego). Załóżmy przeciwnie, że dla pewnych elementów x, x' ciała K mamy $a \boxplus x = 0 = a \boxplus x'$. Korzystamy dalej z aksjomatów ciała i powyższej równości:

$$\begin{aligned} x &= x \boxplus 0 && \text{(aksjomat 3 - wł. elementu 0)} \\ &= x \boxplus (a \boxplus x') && \text{(równość wyżej)} \\ &= (x \boxplus a) \boxplus x' && \text{(aksjomat 1 - łączność } \boxplus) \\ &= x' \boxplus (a \boxplus x) && \text{(aksjomat 2 - przemienność } \boxplus) \\ &= x' \boxplus 0 && \text{(równość wyżej)} \end{aligned}$$

Elementy: przeciwny i odwrotny.

Fakt 1.

Niech K będzie ciałem. Dla każdego elementu $a \in K$ istnieje dokładnie jeden element przeciwny do a. Dla każdego niezerowego elementu $b \in K$ istnieje dokładnie jeden element odwrotny do b.

Dowód (istnienia dokładnie jednego elementu przeciwnego). Załóżmy przeciwnie, że dla pewnych elementów x, x' ciała K mamy $a \boxplus x = 0 = a \boxplus x'$. Korzystamy dalej z aksjomatów ciała i powyższej równości:

$$
\begin{aligned}
x &= x \boxplus 0 && \text{(aksjomat 3 - wł. elementu 0)} \\
&= x \boxplus (a \boxplus x') && \text{(równość wyżej)} \\
&= (x \boxplus a) \boxplus x' && \text{(aksjomat 1 - łączność } \boxplus\text{)} \\
&= x' \boxplus (a \boxplus x) && \text{(aksjomat 2 - przemienność } \boxplus\text{)} \\
&= x' \boxplus 0 && \text{(równość wyżej)} \\
&= x'. && \text{(aksjomat 3 - wł. elementu 0)}
\end{aligned}
$$

Uwaga. W dalszym ciągu, o ile nie prowadzi to do nieporozumień, wprowadzamy następujące umowy:

- dodawanie w ciele K oznaczamy jako $+$,

Uwaga. W dalszym ciągu, o ile nie prowadzi to do nieporozumień, wprowadzamy następujące umowy:

- dodawanie w ciele K oznaczamy jako $+$,
- mnożenie w ciele K oznaczamy jako $\cdot$,

Uwaga. W dalszym ciągu, o ile nie prowadzi to do nieporozumień, wprowadzamy następujące umowy:

- dodawanie w ciele K oznaczamy jako $+$,
- mnożenie w ciele K oznaczamy jako $\cdot$,
- znak mnożenia może być pomijany,

Uwaga. W dalszym ciągu, o ile nie prowadzi to do nieporozumień, wprowadzamy następujące umowy:

- dodawanie w ciele K oznaczamy jako $+$,
- mnożenie w ciele K oznaczamy jako $\cdot$,
- znak mnożenia może być pomijany,
- dla liczby całkowitej dodatniej n oraz $a \in K$ przyjmujemy:

$$a^n = \underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n}.$$

Elementy: przeciwny i odwrotny.

Definicja 4.

Niech K będzie ciałem.

- Element przeciwny do elementu a oznaczamy jako $-a$.
- Element odwrotny do elementu $a \neq 0$ oznaczamy jako a^{-1} lub $\frac{1}{a}$.

Uwaga: Zamiast pisać $a + (-b)$ piszemy $a - b$, a zamiast ab^{-1} piszemy $\frac{a}{b}$.

Elementy: przeciwny i odwrotny.

Definicja 4.

Niech K będzie ciałem.

- Element przeciwny do elementu a oznaczamy jako $-a$.
- Element odwrotny do elementu $a \neq 0$ oznaczamy jako a^{-1} lub $\frac{1}{a}$.

Uwaga: Zamiast pisać $a + (-b)$ piszemy $a - b$, a zamiast ab^{-1} piszemy $\frac{a}{b}$.

Przykładowe własności (dowody korzystają ponownie z aksjomatów):

- $-(-x) = x$,
- $(-x)y = -(xy) = x(-y)$,
- $(-x)(-y) = xy$,
- $(y^{-1})^{-1} = y$, dla $y \neq 0$.

Dodawanie i domnażanie elementu do równości

Fakt 2.

Niech K będzie ciałem oraz x, y, z, q – elementami ciała K, przy czym $q \neq 0$. Wówczas:

Dodawanie i domnażanie elementu do równości

Fakt 2.

Niech K będzie ciałem oraz x, y, z, q – elementami ciała K, przy czym $q \neq 0$. Wówczas:

1) $x + y = x + z$ implikuje $y = z$

Dodawanie i domnażanie elementu do równości

Fakt 2.

Niech K będzie ciałem oraz x, y, z, q – elementami ciała K, przy czym $q \neq 0$. Wówczas:

1) $x + y = x + z$ implikuje $y = z$
2) $x + y = x$ implikuje $y = 0$

Dodawanie i domnażanie elementu do równości

Fakt 2.

Niech K będzie ciałem oraz x, y, z, q – elementami ciała K, przy czym $q \neq 0$. Wówczas:

1)	$x + y = x + z$	implikuje	$y = z$
2)	$x + y = x$	implikuje	$y = 0$
3)	$qx = qy$	implikuje	$x = y$

Dodawanie i domnażanie elementu do równości

Fakt 2.

Niech K będzie ciałem oraz x, y, z, q – elementami ciała K, przy czym $q \neq 0$. Wówczas:

1)	$x + y = x + z$	implikuje	$y = z$
2)	$x + y = x$	implikuje	$y = 0$
3)	$qx = qy$	implikuje	$x = y$
4)	$qy = q$	implikuje	$y = 1$

Dodawanie i domnażanie elementu do równości

Fakt 2.

Niech K będzie ciałem oraz x, y, z, q – elementami ciała K, przy czym $q \neq 0$. Wówczas:

1)	$x + y = x + z$	implikuje	$y = z$
2)	$x + y = x$	implikuje	$y = 0$
3)	$qx = qy$	implikuje	$x = y$
4)	$qy = q$	implikuje	$y = 1$
5)	$0 \cdot x = 0$		

Dodawanie i domnażanie elementu do równości

Fakt 2.

Niech K będzie ciałem oraz x, y, z, q – elementami ciała K, przy czym $q \neq 0$. Wówczas:

1)	$x + y = x + z$	implikuje	$y = z$
2)	$x + y = x$	implikuje	$y = 0$
3)	$qx = qy$	implikuje	$x = y$
4)	$qy = q$	implikuje	$y = 1$
5)	$0 \cdot x = 0$		
6)	$xy = 0$	implikuje	$x = 0$ lub $y = 0$.

Definicja 5.

- Niech $X = \{x_1, \ldots, x_n\}$ będzie zbiorem skończonym. **Równanie liniowe** na **zbiorze zmiennych** X o **współczynnikach** w ciele K to wyrażenie postaci

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = b, \text{ gdzie } a_1, a_2, \ldots, a_n, b \in K. \tag{1}$$

Rozwiązanie powyższego równania to ciąg $s_1, s_2 \ldots s_n \in K$ taki, że

$$a_1 s_1 + a_2 s_2 + \ldots + a_n s_n = b.$$

Definicja 5.

- Niech $X = \{x_1, \ldots, x_n\}$ będzie zbiorem skończonym. **Równanie liniowe** na **zbiorze zmiennych** X o **współczynnikach** w ciele K to wyrażenie postaci

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b, \text{ gdzie } a_1, a_2, \ldots, a_n, b \in K. \tag{1}$$

  Rozwiązanie powyższego równania to ciąg $s_1, s_2 \ldots s_n \in K$ taki, że

$$a_1s_1 + a_2s_2 + \ldots + a_ns_n = b.$$

- Niech U będzie równaniem (1). Dla każdego $\lambda \in K$ przez λU określamy równanie:

$$\lambda \cdot a_1x_1 + \lambda \cdot a_2x_2 + \ldots + \lambda \cdot a_nx_n = \lambda \cdot b.$$

Definicja 5.

- Niech $X = \{x_1, \ldots, x_n\}$ będzie zbiorem skończonym. **Równanie liniowe** na **zbiorze zmiennych** X o **współczynnikach** w ciele K to wyrażenie postaci

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b, \text{ gdzie } a_1, a_2, \ldots, a_n, b \in K. \tag{1}$$

  Rozwiązanie powyższego równania to ciąg $s_1, s_2 \ldots s_n \in K$ taki, że

$$a_1s_1 + a_2s_2 + \ldots + a_ns_n = b.$$

- Niech U będzie równaniem (1). Dla każdego $\lambda \in K$ przez λU określamy równanie:

$$\lambda \cdot a_1x_1 + \lambda \cdot a_2x_2 + \ldots + \lambda \cdot a_nx_n = \lambda \cdot b.$$

- Niech U' będzie równaniem postaci $a'_1x_1 + a'_2x_2 + \ldots + a'_nx_n = b'$, dla pewnych $a'_1, \ldots, a'_n, b' \in K$. Przez $U + U'$ rozumieć będziemy równanie:

$$(a_1 + a'_1)x_1 + (a_2 + a'_2)x_2 + \ldots + (a_n + a'_n)x_n = b + b'.$$

Fakt 3.

Niech K będzie ciałem. Jeśli $(s_1, \ldots, s_n)$ jest rozwiązaniem równań liniowych U_1 oraz U_2, gdzie $s_1, \ldots, s_n \in K$, to jest też rozwiązaniem każdego równania postaci:

$$\lambda_1 U_1 + \lambda_2 U_2, \text{ gdzie } \lambda_1, \lambda_2 \in K.$$

Dowód.

- Niech $U_1 : a_1 x_1 + \ldots + a_n x_n = b$ oraz $U_2 : a'_1 x_1 + \ldots + a'_n x_n = b'$.

Fakt 3.

Niech K będzie ciałem. Jeśli $(s_1, \ldots, s_n)$ jest rozwiązaniem równań liniowych U_1 oraz U_2, gdzie $s_1, \ldots, s_n \in K$, to jest też rozwiązaniem każdego równania postaci:

$$\lambda_1 U_1 + \lambda_2 U_2, \text{ gdzie } \lambda_1, \lambda_2 \in K.$$

Dowód.

- Niech $U_1 : a_1 x_1 + \ldots + a_n x_n = b$ oraz $U_2 : a'_1 x_1 + \ldots + a'_n x_n = b'$.
- Mamy $a_1 s_1 + \ldots + a_n s_n = b$ oraz $a'_1 s_1 + \ldots + a'_n s_n = b'$.

Fakt 3.

Niech K będzie ciałem. Jeśli $(s_1, \ldots, s_n)$ jest rozwiązaniem równań liniowych U_1 oraz U_2, gdzie $s_1, \ldots, s_n \in K$, to jest też rozwiązaniem każdego równania postaci:

$$\lambda_1 U_1 + \lambda_2 U_2, \text{ gdzie } \lambda_1, \lambda_2 \in K.$$

Dowód.

- Niech $U_1 : a_1 x_1 + \ldots + a_n x_n = b$ oraz $U_2 : a'_1 x_1 + \ldots + a'_n x_n = b'$.
- Mamy $a_1 s_1 + \ldots + a_n s_n = b$ oraz $a'_1 s_1 + \ldots + a'_n s_n = b'$.
- Dla dowolnych $\lambda_1, \lambda_2 \in K$ mamy:

$$\lambda_1 \cdot a_1 s_1 + \ldots + \lambda_1 \cdot a_n s_n = \lambda_1 \cdot b, \quad \lambda_2 \cdot a'_1 s_1 + \ldots + \lambda_2 \cdot a'_n s_n = \lambda_2 \cdot b'.$$

Fakt 3.

Niech K będzie ciałem. Jeśli $(s_1, \ldots, s_n)$ jest rozwiązaniem równań liniowych U_1 oraz U_2, gdzie $s_1, \ldots, s_n \in K$, to jest też rozwiązaniem każdego równania postaci:

$$\lambda_1 U_1 + \lambda_2 U_2, \text{ gdzie } \lambda_1, \lambda_2 \in K.$$

Dowód.

- Niech $U_1 : a_1 x_1 + \ldots + a_n x_n = b$ oraz $U_2 : a'_1 x_1 + \ldots + a'_n x_n = b'$.
- Mamy $a_1 s_1 + \ldots + a_n s_n = b$ oraz $a'_1 s_1 + \ldots + a'_n s_n = b'$.
- Dla dowolnych $\lambda_1, \lambda_2 \in K$ mamy:

$$\lambda_1 \cdot a_1 s_1 + \ldots + \lambda_1 \cdot a_n s_n = \lambda_1 \cdot b, \quad \lambda_2 \cdot a'_1 s_1 + \ldots + \lambda_2 \cdot a'_n s_n = \lambda_2 \cdot b'.$$

- A zatem $(\lambda_1 a_1 + \lambda_2 a'_1) s_1 + \ldots + (\lambda_1 a_n + \lambda_2 a'_n) s_n = \lambda_1 b + \lambda_2 b'$.

Fakt 3.

Niech K będzie ciałem. Jeśli $(s_1, \ldots, s_n)$ jest rozwiązaniem równań liniowych U_1 oraz U_2, gdzie $s_1, \ldots, s_n \in K$, to jest też rozwiązaniem każdego równania postaci:

$$\lambda_1 U_1 + \lambda_2 U_2, \text{ gdzie } \lambda_1, \lambda_2 \in K.$$

Dowód.

- Niech $U_1 : a_1 x_1 + \ldots + a_n x_n = b$ oraz $U_2 : a'_1 x_1 + \ldots + a'_n x_n = b'$.
- Mamy $a_1 s_1 + \ldots + a_n s_n = b$ oraz $a'_1 s_1 + \ldots + a'_n s_n = b'$.
- Dla dowolnych $\lambda_1, \lambda_2 \in K$ mamy:

$$\lambda_1 \cdot a_1 s_1 + \ldots + \lambda_1 \cdot a_n s_n = \lambda_1 \cdot b, \quad \lambda_2 \cdot a'_1 s_1 + \ldots + \lambda_2 \cdot a'_n s_n = \lambda_2 \cdot b'.$$

- A zatem $(\lambda_1 a_1 + \lambda_2 a'_1) s_1 + \ldots + (\lambda_1 a_n + \lambda_2 a'_n) s_n = \lambda_1 b + \lambda_2 b'$.
- A zatem $s_1, \ldots, s_n$ jest rozwiązaniem $\lambda_1 U_1 + \lambda_2 U_2$.

Uwaga. Wszystkie definicje z poprzedniego wykładu: układu równań, macierzy, macierzy układu, rozwiązania ogólnego itd. rozważać można w oparciu o układy złożone z równań liniowych o współczynnikach w dowolnym (ustalonym) ciele K.

Twierdzenie 1.

Następujące operacje przeprowadzają układ U w układ równoważny.

(1) Dodanie do równania innego równania pomnożonego przez liczbę

(2) Zamiana dwóch równań miejscami

(3) Pomnożenie równania przez liczbę różną od zera

Twierdzenie 1.

Następujące operacje przeprowadzają układ U w układ równoważny.

(1) Dodanie do równania innego równania pomnożonego przez liczbę

(2) Zamiana dwóch równań miejscami

(3) Pomnożenie równania przez liczbę różną od zera

Dowód:

- Oczywiste dla operacji (2) i (3).

Twierdzenie 1.

Następujące operacje przeprowadzają układ U w układ równoważny.

(1) Dodanie do równania innego równania pomnożonego przez liczbę

(2) Zamiana dwóch równań miejscami

(3) Pomnożenie równania przez liczbę różną od zera

Dowód:

- Oczywiste dla operacji (2) i (3).
- Niech U' powstaje z U przez dodanie do i-tego równania U_i równania U_j przemnożonego przez $a \in K$. Wtedy U powstaje z U' przez dodanie do i-tego równania $U_i + aU_j$ równania U_j przemnożonego przez $-a \in K$.

Twierdzenie 1.

Następujące operacje przeprowadzają układ U w układ równoważny.

(1) Dodanie do równania innego równania pomnożonego przez liczbę

(2) Zamiana dwóch równań miejscami

(3) Pomnożenie równania przez liczbę różną od zera

Dowód:

- Oczywiste dla operacji (2) i (3).
- Niech U' powstaje z U przez dodanie do i-tego równania U_i równania U_j przemnożonego przez $a \in K$. Wtedy U powstaje z U' przez dodanie do i-tego równania $U_i + aU_j$ równania U_j przemnożonego przez $-a \in K$.
- Na mocy Faktu wyżej: jeśli $(s_1, \ldots, s_n)$ jest rozwiązaniem U_i, U_j, to także jest rozwiązaniem $U_i + aU_j$. A zatem jeśli $(s_1, \ldots, s_n)$ spełnia U, to także U'.

Twierdzenie 1.

Następujące operacje przeprowadzają układ U w układ równoważny.

(1) Dodanie do równania innego równania pomnożonego przez liczbę

(2) Zamiana dwóch równań miejscami

(3) Pomnożenie równania przez liczbę różną od zera

Dowód:

- Oczywiste dla operacji (2) i (3).
- Niech U' powstaje z U przez dodanie do i-tego równania U_i równania U_j przemnożonego przez $a \in K$. Wtedy U powstaje z U' przez dodanie do i-tego równania $U_i + aU_j$ równania U_j przemnożonego przez $-a \in K$.
- Na mocy Faktu wyżej: jeśli $(s_1, \ldots, s_n)$ jest rozwiązaniem U_i, U_j, to także jest rozwiązaniem $U_i + aU_j$. A zatem jeśli $(s_1, \ldots, s_n)$ spełnia U, to także U'.
- Jeśli $(s_1, \ldots, s_n)$ jest rozwiązaniem $U_i + aU_j$ oraz U_j, to jest też rozwiązaniem $U_i = (U_i + aU_j) - aU_j$. A zatem jeśli $(s_1, \ldots, s_n)$ spełnia U', to spełnia U.

Twierdzenie 2.

Niech K będzie ciałem. Każdą macierz $A \in M_{m\times n}(K)$ można:

(i) za pomocą operacji elementarnych typu (1) i (2) sprowadzić do postaci schodkowej,

(ii) za pomocą operacji elementarnych typu (1), (2) i (3) sprowadzić do postaci schodkowej zredukowanej.

Dowiedziemy tylko (i).

Dowód (i).

- Stosujemy zasadę indukcji matematycznej względem liczby m wierszy macierzy. Dla $m = 1$ twierdzenie jest oczywiste.

Dowód (i).

- Stosujemy zasadę indukcji matematycznej względem liczby m wierszy macierzy. Dla $m = 1$ twierdzenie jest oczywiste.
- Załóżmy, że twierdzenie jest udowodnione dla macierzy o co najwyżej $m - 1$ wierszach. Niech $A \in M_{m \times n}(K)$.

Dowód (i).

- Stosujemy zasadę indukcji matematycznej względem liczby m wierszy macierzy. Dla $m = 1$ twierdzenie jest oczywiste.
- Załóżmy, że twierdzenie jest udowodnione dla macierzy o co najwyżej $m - 1$ wierszach. Niech $A \in M_{m \times n}(K)$.
- Jeśli A jest macierzą zerową (to znaczy każdy jej wyraz jest zerem), to oczywiście jest schodkowa.

Dowód (i).

- Stosujemy zasadę indukcji matematycznej względem liczby m wierszy macierzy. Dla $m = 1$ twierdzenie jest oczywiste.
- Załóżmy, że twierdzenie jest udowodnione dla macierzy o co najwyżej $m - 1$ wierszach. Niech $A \in M_{m \times n}(K)$.
- Jeśli A jest macierzą zerową (to znaczy każdy jej wyraz jest zerem), to oczywiście jest schodkowa.
- Niech s będzie numerem pierwszej niezerowej kolumny macierzy A.

- Wybierzmy takie r, że $a_{rs} \neq 0$. Zamieniamy miejscami wiersze: pierwszy i r-ty (operacja typu (2)).

- Za pomocą operacji (1) zerujemy wszystkie, poza pierwszym, wyrazy w s-tej kolumnie (od i-tego wiersza odejmujemy pierwszy przemnożony przez $\frac{a_{is}}{a_{1s}}$). Otrzymujemy w ten sposób macierz $A' = [a'_{ij}]$, w której kolumny o numerach $1, \ldots, s-1$ są zerowe oraz $a'_{1s} \neq 0$ i $a'_{is} = 0$, dla $i > 1$.

- Niech $A'' \in M_{(m-1)\times n}(K)$ będzie macierzą otrzymaną z A' przez usunięcie pierwszego wiersza. Stosujemy do A'' założenie indukcyjne. Pierwsze s kolumn macierzy A'' jest zerowe i żadne operacje typu (1), (2) na wierszach tego nie zmienią. Otrzymujemy macierz, która wraz z pierwszym wierszem macierzy A' tworzy macierz A''' w postaci schodkowej. Oczywiście A''' jest uzyskana z A przez ciąg operacji typu (1) i (2).

Przykłady ciał

- ciało dwuelementowe $\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

- ciało trzyelementowe $\mathbb{Z}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Przykłady ciał

- ciało czteroelementowe $\mathbb{Z}_4$? Nie!

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Wspomnieliśmy, że $ab = 0$ implikuje $a = 0$ lub $b = 0$.

Przykłady ciał

- ciało czteroelementowe

+	0	1	a	b
0	0	1	a	b
1	1			
a	a			
b	b			

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a		
b	0	b		

Przykłady ciał

- ciało czteroelementowe

+	0	1	a	b
0	0	1	a	b
1	1			
a	a			
b	b			

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a		?
b	0	b	?	

Przykłady ciał

- ciało czteroelementowe

+	0	1	a	b
0	0	1	a	b
1	1			
a	a			
b	b			

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a		1
b	0	b	1	

Przykłady ciał

- ciało czteroelementowe

+	0	1	a	b
0	0	1	a	b
1	1			
a	a			
b	b			

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Przykłady ciał

- ciało czteroelementowe

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Piątka $(\{0, 1, a, b\}, +, \cdot, 0, 1)$ jest ciałem! Uwaga: $a^2 + a + 1 = 0$.

Przykłady ciał

- ciało $\mathbb{Z}_p$ reszt z dzielenia modulo liczba pierwsza p na zbiorze $\{0, 1, \ldots, p-1\}$:

Przykłady ciał

- ciało $\mathbb{Z}_p$ reszt z dzielenia modulo liczba pierwsza p na zbiorze $\{0, 1, \ldots, p-1\}$:
  - łączność i przemienność dodawania i mnożenia modulo p – łatwe (jeśli $p|a_1 - b_1$ oraz $p|a_2 - b_2$, to $p|(a_1 + a_2) - (b_1 + b_2)$ oraz $p|(a_1 a_2 - b_1 b_2)$),

Przykłady ciał

- ciało $\mathbb{Z}_p$ reszt z dzielenia modulo liczba pierwsza p na zbiorze $\{0, 1, \ldots, p-1\}$:
  - łączność i przemienność dodawania i mnożenia modulo p – łatwe (jeśli $p|a_1 - b_1$ oraz $p|a_2 - b_2$, to $p|(a_1 + a_2) - (b_1 + b_2)$ oraz $p|(a_1 a_2 - b_1 b_2)$),
  - $0, 1$ jako elementy neutralne dodawania i mnożenia – łatwe,

Przykłady ciał

- ciało $\mathbb{Z}_p$ reszt z dzielenia modulo liczba pierwsza p na zbiorze $\{0, 1, \ldots, p-1\}$:
  - łączność i przemienność dodawania i mnożenia modulo p – łatwe (jeśli $p|a_1 - b_1$ oraz $p|a_2 - b_2$, to $p|(a_1 + a_2) - (b_1 + b_2)$ oraz $p|(a_1 a_2 - b_1 b_2)$),
  - $0, 1$ jako elementy neutralne dodawania i mnożenia – łatwe,
  - istnienie elementu przeciwnego – łatwe

Przykłady ciał

- ciało $\mathbb{Z}_p$ reszt z dzielenia modulo liczba pierwsza p na zbiorze $\{0, 1, \ldots, p-1\}$:
  - łączność i przemienność dodawania i mnożenia modulo p – łatwe (jeśli $p|a_1 - b_1$ oraz $p|a_2 - b_2$, to $p|(a_1 + a_2) - (b_1 + b_2)$ oraz $p|(a_1 a_2 - b_1 b_2)$),
  - $0, 1$ jako elementy neutralne dodawania i mnożenia – łatwe,
  - istnienie elementu przeciwnego – łatwe
  - rozdzielność – łatwe

Przykłady ciał

- ciało $\mathbb{Z}_p$ reszt z dzielenia modulo liczba pierwsza p na zbiorze $\{0, 1, \ldots, p-1\}$:
  - łączność i przemienność dodawania i mnożenia modulo p – łatwe (jeśli $p|a_1 - b_1$ oraz $p|a_2 - b_2$, to $p|(a_1 + a_2) - (b_1 + b_2)$ oraz $p|(a_1 a_2 - b_1 b_2)$),
  - $0, 1$ jako elementy neutralne dodawania i mnożenia – łatwe,
  - istnienie elementu przeciwnego – łatwe
  - rozdzielność – łatwe
  - istnienie elementu odwrotnego – wymaga tzw. Lematu Bezout lub twierdzenia o istnieniu i jednoznaczności rozkładu liczby całkowitej > 1 na czynniki pierwsze.

Przykłady ciał

- ciało $\mathbb{Z}_p$ reszt z dzielenia modulo liczba pierwsza p na zbiorze $\{0, 1, \ldots, p-1\}$:
  - łączność i przemienność dodawania i mnożenia modulo p – łatwe (jeśli $p|a_1 - b_1$ oraz $p|a_2 - b_2$, to $p|(a_1 + a_2) - (b_1 + b_2)$ oraz $p|(a_1 a_2 - b_1 b_2)$),
  - $0, 1$ jako elementy neutralne dodawania i mnożenia – łatwe,
  - istnienie elementu przeciwnego – łatwe
  - rozdzielność – łatwe
  - istnienie elementu odwrotnego – wymaga tzw. Lematu Bezout lub twierdzenia o istnieniu i jednoznaczności rozkładu liczby całkowitej > 1 na czynniki pierwsze.

Lemat Bezout

Dla niezerowej liczby całkowitej a oraz dowolnej liczby całkowitej b istnieją takie liczby całkowite x, y, że:

$$ax + by = NWD(a, b).$$

Przykłady ciał

Definicja 6

Niech $(L, +, \cdot, 0, 1)$ będzie ciałem oraz niech $K \subseteq L$. Powiemy, że K jest **podciałem** ciała L, jeśli $0, 1 \in K$ oraz:

- dla każdych $a, b \in K$ mamy $a + b \in K$ oraz $a \cdot b \in K$,
- dla każdego $a \in K$ mamy $-a \in K$,
- dla każdego niezerowego $b \in K$ mamy $b^{-1} \in K$.

Przykład. Ciało liczb wymiernych $(\mathbb{Q}, +, \cdot, 0, 1)$ jest podciałem ciała $\mathbb{R}$.

Przykłady ciał

Fakt 4.

Rozważmy podzbiór $\mathbb{Q}(\sqrt{2})$ w ciele liczb rzeczywistych złożony ze wszystkich elementów postaci

$$\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Ograniczenie działań na $\mathbb{R}$ zadaje na $\mathbb{Q}(\sqrt{2})$ strukturę podciała.

Przykłady działań w $\mathbb{Q}(\sqrt{2})$

- $(2 + \sqrt{2}) + (3 + \frac{1}{2}\sqrt{2}) = 5 + \frac{3}{2}\sqrt{2}$.
- $(1 - \sqrt{2}) \cdot (1 + \sqrt{2}) = -1 + 0 \cdot \sqrt{2}$.
- elementem odwrotnym do $3 - 2\sqrt{2}$ jest element $3 + 2\sqrt{2}$.

Przykłady ciał

Fakt 5.

Każde podciało ciała liczb wymiernych $\mathbb{Q}$ równe jest $\mathbb{Q}$.

Przykłady ciał

Fakt 5.

Każde podciało ciała liczb wymiernych $\mathbb{Q}$ równe jest $\mathbb{Q}$.

Idea dowodu:

1. Jeśli K jest podciałem ciała L, to skoro $1 \in K$, to też

$$1+1 \in K, 1+1+1 \in K, 1+1+1+1 \in K, \textit{itd}.$$

Przykłady ciał

Fakt 5.

Każde podciało ciała liczb wymiernych $\mathbb{Q}$ równe jest $\mathbb{Q}$.

Idea dowodu:

1. Jeśli K jest podciałem ciała L, to skoro $1 \in K$, to też

$$1+1 \in K, 1+1+1 \in K, 1+1+1+1 \in K, \textit{itd}.$$

2. Jeśli K jest podciałem $\mathbb{Q}$, to K zawiera wszystkie liczby całkowite dodatnie.

Przykłady ciał

Fakt 5.

Każde podciało ciała liczb wymiernych $\mathbb{Q}$ równe jest $\mathbb{Q}$.

Idea dowodu:

1. Jeśli K jest podciałem ciała L, to skoro $1 \in K$, to też

$$1+1 \in K, 1+1+1 \in K, 1+1+1+1 \in K, \textit{itd}.$$

2. Jeśli K jest podciałem $\mathbb{Q}$, to K zawiera wszystkie liczby całkowite dodatnie.
3. Jeśli niezerowy element $a \in K$, to $-a$ oraz a^{-1} również należą do K.

Przykłady ciał

Fakt 5.

Każde podciało ciała liczb wymiernych $\mathbb{Q}$ równe jest $\mathbb{Q}$.

Idea dowodu:

1. Jeśli K jest podciałem ciała L, to skoro $1 \in K$, to też

$$1+1 \in K, 1+1+1 \in K, 1+1+1+1 \in K, \textit{itd}.$$

2. Jeśli K jest podciałem $\mathbb{Q}$, to K zawiera wszystkie liczby całkowite dodatnie.
3. Jeśli niezerowy element $a \in K$, to $-a$ oraz a^{-1} również należą do K.
4. Jeśli K jest podciałem $\mathbb{Q}$, to zawiera wszystkie liczby całkowite i ich odwrotności.

Przykłady ciał

Fakt 5.

Każde podciało ciała liczb wymiernych $\mathbb{Q}$ równe jest $\mathbb{Q}$.

Idea dowodu:

1. Jeśli K jest podciałem ciała L, to skoro $1 \in K$, to też

$$1+1 \in K, 1+1+1 \in K, 1+1+1+1 \in K, \textit{itd}.$$

2. Jeśli K jest podciałem $\mathbb{Q}$, to K zawiera wszystkie liczby całkowite dodatnie.
3. Jeśli niezerowy element $a \in K$, to $-a$ oraz a^{-1} również należą do K.
4. Jeśli K jest podciałem $\mathbb{Q}$, to zawiera wszystkie liczby całkowite i ich odwrotności.
5. jeśli K jest podciałem $\mathbb{Q}$ oraz $a, b \in K$, to $a+b \in K$ oraz $a \cdot b \in K$.

Przykłady ciał

Fakt 6.

Rozważmy dowolną rodzinę podciał K_t ciała L, gdzie $t \in T$. Wówczas część wspólna wszystkich ciał K_t jest podciałem ciała K.

Fakt 7.

Dla każdego podciała K ciała L oraz podzbioru S zbioru L istnieje najmniejsze podciało $K(S)$ ciała L, które zawiera jednocześnie ciało K oraz zbiór S.

Przykład: najmniejszym podciałem ciała $\mathbb{R}$ zawierającym $\mathbb{Q}$ oraz $\sqrt{2}$ jest $\mathbb{Q}(\sqrt{2})$.

Przykłady ciał
Inne podciała ciała liczb rzeczywistych:

- ciała $\mathbb{Q}(\sqrt{p})$, gdzie p jest liczbą pierwszą,
- ciała $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, gdzie p, q są liczbami pierwszymi,
- najmniejsze ciało zawierające $\mathbb{Q}$ i pierwiastki z wszystkich liczb pierwszych,
- ciało liczb algebraicznych (za tydzień),
- ciała typu $\mathbb{Q}(\pi)$, $\mathbb{Q}(\sqrt{2}, \pi)$, $\mathbb{Q}(\pi, \pi^2, \pi^3, \ldots)$ itd.

Przykłady ciał

Kilka uwag o ciałach skończonych.

- Opisane ciało czteroelementowe, to najmniejsze ciało zawierające $\mathbb{Z}_2$ oraz pierwiastek równania $x^2 + x + 1 = 0$, które nie ma rozwiązań w ciele $\mathbb{Z}_2$.

Przykłady ciał

Kilka uwag o ciałach skończonych.

- Opisane ciało czteroelementowe, to najmniejsze ciało zawierające $\mathbb{Z}_2$ oraz pierwiastek równania $x^2 + x + 1 = 0$, które nie ma rozwiązań w ciele $\mathbb{Z}_2$.
- Istnieje ciało o 9 elementach, które zawiera $\mathbb{Z}_3$, składa się z elementów postaci $a + b\delta$, gdzie $a, b \in \mathbb{Z}_3$ oraz δ spełnia zależność $\delta^2 + 2\delta + 2 = 0$. Równanie $x^2 + 2x + 2$ nie ma rozwiązań w $\mathbb{Z}^3$.

Przykłady ciał
Kilka uwag o ciałach skończonych.

- Opisane ciało czteroelementowe, to najmniejsze ciało zawierające $\mathbb{Z}_2$ oraz pierwiastek równania $x^2 + x + 1 = 0$, które nie ma rozwiązań w ciele $\mathbb{Z}_2$.
- Istnieje ciało o 9 elementach, które zawiera $\mathbb{Z}_3$, składa się z elementów postaci $a + b\delta$, gdzie $a, b \in \mathbb{Z}_3$ oraz δ spełnia zależność $\delta^2 + 2\delta + 2 = 0$. Równanie $x^2 + 2x + 2$ nie ma rozwiązań w $\mathbb{Z}^3$.
- **Fakt.** Ciało K zawiera ciało $\mathbb{Z}_p$ wtedy i tylko wtedy, gdy $\underbrace{1 + 1 + \ldots + 1}_{p} = 0$.

Przykłady ciał
Kilka uwag o ciałach skończonych.

- Opisane ciało czteroelementowe, to najmniejsze ciało zawierające $\mathbb{Z}_2$ oraz pierwiastek równania $x^2 + x + 1 = 0$, które nie ma rozwiązań w ciele $\mathbb{Z}_2$.
- Istnieje ciało o 9 elementach, które zawiera $\mathbb{Z}_3$, składa się z elementów postaci $a + b\delta$, gdzie $a, b \in \mathbb{Z}_3$ oraz δ spełnia zależność $\delta^2 + 2\delta + 2 = 0$. Równanie $x^2 + 2x + 2$ nie ma rozwiązań w $\mathbb{Z}^3$.
- **Fakt.** Ciało K zawiera ciało $\mathbb{Z}_p$ wtedy i tylko wtedy, gdy $\underbrace{1 + 1 + \ldots + 1}_{p} = 0$.
- **Twierdzenie.** Każde ciało skończone zawiera pewne ciało $\mathbb{Z}_p$ i ma p^r elementów, dla pewnej liczby pierwszej p i liczby całkowitej dodatniej r.

Definicja 7.

Ciało liczb zespolonych to piątka $(\mathbb{R}^2, +, \cdot, (0,0), (1,0))$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, w którym działania $+, \cdot$ określone są wzorami:

$$(a,b) + (c,d) = (a+c, b+d), \quad (a,b) \cdot (c,d) = (ac - bd, ad + bc),$$

a elementami neutralnymi tych działań są odpowiednio $(0,0), (1,0)$. Ciało to oznaczamy jako $\mathbb{C}$.

Definicja 7.

Ciało liczb zespolonych to piątka $(\mathbb{R}^2, +, \cdot, (0,0), (1,0))$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, w którym działania $+, \cdot$ określone są wzorami:

$$(a,b) + (c,d) = (a+c, b+d), \quad (a,b) \cdot (c,d) = (ac - bd, ad + bc),$$

a elementami neutralnymi tych działań są odpowiednio $(0,0), (1,0)$. Ciało to oznaczamy jako $\mathbb{C}$.

Na przykład:

- $(3,0) + (4,0) = (7,0)$,

Definicja 7.

Ciało liczb zespolonych to piątka $(\mathbb{R}^2, +, \cdot, (0,0), (1,0))$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, w którym działania $+, \cdot$ określone są wzorami:

$$(a,b) + (c,d) = (a+c, b+d), \quad (a,b) \cdot (c,d) = (ac - bd, ad + bc),$$

a elementami neutralnymi tych działań są odpowiednio $(0,0), (1,0)$. Ciało to oznaczamy jako $\mathbb{C}$.

Na przykład:

- $(3,0) + (4,0) = (7,0)$,
- $(0,1) + (1,0) = (1,1)$,

Definicja 7.

Ciało liczb zespolonych to piątka $(\mathbb{R}^2, +, \cdot, (0,0), (1,0))$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, w którym działania $+, \cdot$ określone są wzorami:

$$(a,b) + (c,d) = (a+c, b+d), \quad (a,b) \cdot (c,d) = (ac - bd, ad + bc),$$

a elementami neutralnymi tych działań są odpowiednio $(0,0), (1,0)$. Ciało to oznaczamy jako $\mathbb{C}$.

Na przykład:

- $(3,0) + (4,0) = (7,0)$,
- $(0,1) + (1,0) = (1,1)$,
- $(0,1) \cdot (0,1) = (-1,0)$,

Definicja 7.

Ciało liczb zespolonych to piątka $(\mathbb{R}^2, +, \cdot, (0,0), (1,0))$, którego elementami są wszystkie uporządkowane pary liczb rzeczywistych, w którym działania $+, \cdot$ określone są wzorami:

$$(a,b) + (c,d) = (a+c, b+d), \quad (a,b) \cdot (c,d) = (ac - bd, ad + bc),$$

a elementami neutralnymi tych działań są odpowiednio $(0,0), (1,0)$. Ciało to oznaczamy jako $\mathbb{C}$.

Na przykład:

- $(3,0) + (4,0) = (7,0)$,
- $(0,1) + (1,0) = (1,1)$,
- $(0,1) \cdot (0,1) = (-1,0)$,
- $(2,1) \cdot (2,-1) = (5,0)$.

Uwagi wstępne

- Jeśli $(a,b) \neq (0,0)$, to $(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$, bo

$$(a,b) \cdot \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(\frac{a^2+b^2}{a^2+b^2}, \frac{-ab+ab}{a^2+b^2}\right) = (1,0).$$

Uwagi wstępne

- Jeśli $(a,b) \neq (0,0)$, to $(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$, bo

$$(a,b) \cdot \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(\frac{a^2+b^2}{a^2+b^2}, \frac{-ab+ab}{a^2+b^2}\right) = (1,0).$$

- Podzbiór $\{(r,0) \mid r \in \mathbb{R}\}$ jest podciałem $\mathbb{C}$, które *zachowuje się* jak $\mathbb{R}$.

Uwagi wstępne

- Jeśli $(a, b) \neq (0, 0)$, to $(a, b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$, bo

$$(a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = \left(\frac{a^2 + b^2}{a^2 + b^2}, \frac{-ab + ab}{a^2 + b^2}\right) = (1, 0).$$

- Podzbiór $\{(r, 0) \mid r \in \mathbb{R}\}$ jest podciałem $\mathbb{C}$, które *zachowuje się* jak $\mathbb{R}$.
- Liczbę postaci $(a, 0)$ będziemy zapisywać jako a, dla każdego $a \in \mathbb{R}$, zaś liczbę $(0, 1)$ oznaczać będziemy jako i.

Uwagi wstępne

- Jeśli $(a, b) \neq (0, 0)$, to $(a, b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$, bo

$$(a, b) \cdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = \left(\frac{a^2 + b^2}{a^2 + b^2}, \frac{-ab + ab}{a^2 + b^2}\right) = (1, 0).$$

- Podzbiór $\{(r, 0) \mid r \in \mathbb{R}\}$ jest podciałem $\mathbb{C}$, które *zachowuje się* jak $\mathbb{R}$.
- Liczbę postaci $(a, 0)$ będziemy zapisywać jako a, dla każdego $a \in \mathbb{R}$, zaś liczbę $(0, 1)$ oznaczać będziemy jako i.
- Mamy $(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + bi$ oraz $i^2 = -1$.

Uwagi wstępne

- Jeśli $(a,b) \neq (0,0)$, to $(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$, bo

$$(a,b) \cdot \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(\frac{a^2+b^2}{a^2+b^2}, \frac{-ab+ab}{a^2+b^2}\right) = (1,0).$$

- Podzbiór $\{(r,0) \mid r \in \mathbb{R}\}$ jest podciałem $\mathbb{C}$, które *zachowuje się* jak $\mathbb{R}$.
- Liczbę postaci $(a,0)$ będziemy zapisywać jako a, dla każdego $a \in \mathbb{R}$, zaś liczbę $(0,1)$ oznaczać będziemy jako i.
- Mamy $(a,b) = (a,0) + (0,b) = (a,0) + (b,0) \cdot (0,1) = a + bi$ oraz $i^2 = -1$.
- Jeśli $z = a + bi$, to
  - liczbę a nazywamy **częścią rzeczywistą** liczby z i oznaczamy $\operatorname{Re} z$,
  - liczbę b nazywamy **częścią urojoną** liczby z i oznaczamy $\operatorname{Im} z$.
  - liczbę $a - bi$ nazywamy **liczbą sprzężoną** do z i oznaczamy $\overline{z}$,
  - liczbę $\sqrt{a^2+b^2}$ nazywamy **modułem** liczby z i oznaczamy $|z|$.

Za tydzień:

- interpretacja geometryczna liczby zespolonej, postać trygonometryczna,
- wielomiany o współćzynnnikach w ciele i ich pierwiastki,
- zasadnicze twierdzenie algebry (bez dowodu).