

1. WYKŁAD

1.1. Definicja ciała.

Definicja 1.1. *Ciałem* nazywamy piątkę $(\mathbb{F}, +, 0, \cdot, 1)$ składającą się z

- zbioru \mathbb{F} ,
- odwzorowania $+: \mathbb{F} \times \mathbb{F} \ni (\alpha, \beta) \mapsto \alpha + \beta \in \mathbb{F}$,
- wyróżnionego elementu $0 \in \mathbb{F}$,
- odwzorowania $\cdot: \mathbb{F} \times \mathbb{F} \ni (\alpha, \beta) \mapsto \alpha \cdot \beta \in \mathbb{F}$,
- wyróżnionego elementu $1 \in \mathbb{F}$

spełniającą następujące warunki:

- (1) (a) $\alpha + \beta = \beta + \alpha$ dla wszystkich $\alpha, \beta \in \mathbb{F}$,
(b) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ dla wszystkich $\alpha, \beta, \gamma \in \mathbb{F}$,
(c) $\alpha + 0 = \alpha$ dla wszystkich $\alpha \in \mathbb{F}$,
(d) dla każdego $\alpha \in \mathbb{F}$ istnieje element $\beta \in \mathbb{F}$ taki, że $\alpha + \beta = 0$;
- (2) (a) $\alpha \cdot \beta = \beta \cdot \alpha$ dla wszystkich $\alpha, \beta \in \mathbb{F}$,
(b) $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$ dla wszystkich $\alpha, \beta, \gamma \in \mathbb{F}$,
(c) $\alpha \cdot 1 = \alpha$ dla wszystkich $\alpha \in \mathbb{F}$,
(d) dla każdego $\alpha \in \mathbb{F}$ takiego, że $\alpha \neq 0$ istnieje element $\beta \in \mathbb{F}$ taki, że $\alpha \cdot \beta = 1$;
- (3) dla wszystkich $\alpha, \beta, \gamma \in \mathbb{F}$

$$\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma).$$

1.1.1. *Uwagi.* Niech $(\mathbb{F}, +, 0, \cdot, 1)$ będzie ciałem.

- (1) Odwzorowanie $(\alpha, \beta) \mapsto \alpha + \beta$ nazywamy *dodawaniem*, a element 0 nazywamy *zerem* lub *elementem neutralnym dodawania*.
- (2) Odwzorowanie $(\alpha, \beta) \mapsto \alpha \cdot \beta$ nazywamy *mnożeniem*, a element 1 nazywamy *jedynką* lub *elementem neutralnym mnożenia*.
- (3) Dla $\alpha \in \mathbb{F}$ element β taki, że $\alpha + \beta = 0$ oznaczamy symbolem $-\alpha$ i nazywamy *elementem przeciwnym do α* .
- (4) Dla $\alpha \in \mathbb{F} \setminus \{0\}$ element β taki, że $\alpha \cdot \beta = 1$ oznaczamy symbolem α^{-1} lub $\frac{1}{\alpha}$ i nazywamy *elementem odwrotnym do α* .
- (5) Własność (1a) z Definicji 1.1 nazywamy *przemiennością dodawania*.
- (6) Własność (1b) z Definicji 1.1 nazywamy *łącznością dodawania*.
- (7) Własność (2a) z Definicji 1.1 nazywamy *przemiennością mnożenia*.
- (8) Własność (2b) z Definicji 1.1 nazywamy *łącznością mnożenia*.
- (9) Własność (3) z Definicji 1.1 nazywamy *rozdzielnością mnożenia względem dodawania*.
- (10) Zazwyczaj opuszczamy symbol mnożenia i wyrażenia postaci $\alpha \cdot \beta$ zapisujemy jako $\alpha\beta$.
- (11) Najczęściej zakładamy również, że $1 \neq 0$.

1.2. Przykłady ciał.

- (1) Niech \mathbb{F} będzie zbiorem dwuelementowym. Nazwijmy jeden z elementów \mathbb{F} zerem, a drugi jedynką. Działania definiujemy tak:

$$\begin{array}{ll} 0 + 0 = 0, & 0 \cdot 0 = 0, \\ 0 + 1 = 1, & 0 \cdot 1 = 0, \\ 1 + 0 = 1, & 1 \cdot 0 = 0, \\ 1 + 1 = 0, & 1 \cdot 1 = 1. \end{array}$$

Otrzymujemy ciało, które oznaczamy symbolem \mathbb{Z}_2 .

- (2) Niech p będzie liczbą pierwszą. Niech $\mathbb{F} = \{0, 1, 2, \dots, p-1\}$. Definiujemy działania

$$\begin{array}{l} +_p : \mathbb{F} \times \mathbb{F} \ni (\alpha, \beta) \mapsto \alpha +_p \beta \in \mathbb{F}, \\ \cdot_p : \mathbb{F} \times \mathbb{F} \ni (\alpha, \beta) \mapsto \alpha \cdot_p \beta \in \mathbb{F} \end{array}$$

kładąc

$$\begin{aligned}\alpha +_p \beta &= \text{reszta z dzielenia } \alpha + \beta \text{ przez } p, \\ \alpha \cdot_p \beta &= \text{reszta z dzielenia } \alpha\beta \text{ przez } p.\end{aligned}$$

Otrzymane ciało oznaczamy symbolem \mathbb{Z}_p . Zazwyczaj opuszczamy też indeks “ p ” przy symbolach mnożenia i dodawania w tym ciele.

- (3) Zbiór \mathbb{Q} liczb wymiernych jest ciałem ze standardowymi operacjami dodawania i mnożenia.
- (4) Zbiór \mathbb{R} liczb rzeczywistych jest ciałem ze standardowymi operacjami dodawania i mnożenia.
- (5) Oznaczmy przez $\mathbb{Q}(\sqrt{2})$ zbiór liczb rzeczywistych postaci $\alpha + \beta\sqrt{2}$, gdzie $\alpha, \beta \in \mathbb{Q}$. Wówczas $\mathbb{Q}(\sqrt{2})$ jest ciałem z operacjami dodawania odziedziczonymi ze zbioru liczb rzeczywistych.

1.3. Ćwiczenia.

- Inne przykłady ciał,
- tabelki dodawania i mnożenia,
- rozwiązywanie prostych równań i układów równań w ciałach (ew. niemożność rozwiązania).

WIELOMIANY

Definicja 1.2. Niech \mathbb{F} będzie ciałem. *Wielomianem o współczynnikach z \mathbb{F}* nazywamy formalny napis postaci

$$f = \alpha_0 + \alpha_1\mathfrak{X} + \alpha_2\mathfrak{X}^2 + \cdots + \alpha_n\mathfrak{X}^n,$$

gdzie $n \in \mathbb{Z}_+$, $\alpha_0, \alpha_1, \dots, \alpha_n \in \mathbb{F}$ i $\alpha_n \neq 0$. Niekiedy stosujemy też zapis $f(\mathfrak{X})$ zamiast f .

Zbiór wielomianów o współczynnikach z \mathbb{F} oznaczamy symbolem $\mathbb{F}[\mathfrak{X}]$.

Zbiór wielomianów o współczynnikach z ciała ma bardzo szczególną strukturę. Wielomiany można dodawać i mnożyć (jak?). Dodawanie wielomianów jest przemienne i łączne, a wielomian zerowy 0 jest elementem neutralnym dodawania wielomianów. Podobnie mnożenie wielomianów jest przemienne i łączne, a wielomian 1 jest elementem neutralnym dla mnożenia. Ponadto mnożenie wielomianów jest rozdzielne względem dodawania. Jednak $\mathbb{F}[\mathfrak{X}]$ nie jest ciałem (jeśli przyjmiemy założenie z uwagi 1.1.1(11)).

Jest jeszcze jeden ciekawy element struktury zbioru $\mathbb{F}[\mathfrak{X}]$. niezerowemu wielomianowi

$$f = \alpha_0 + \alpha_1\mathfrak{X} + \alpha_2\mathfrak{X}^2 + \cdots + \alpha_n\mathfrak{X}^n$$

możemy przypisać dodatnią liczbę całkowitą n . Liczbę tę nazywamy *stopniem wielomianu f* i oznaczamy symbolem $\deg f$. Stopień wielomianu zerowego definiujemy jako $-\infty$.

Stwierdzenie 1.3. *Niech \mathbb{F} będzie ciałem i niech $f, g \in \mathbb{F}[\mathfrak{X}]$. Wówczas*

- (1) $\deg(f + g) \leq \max\{\deg f, \deg g\}$,
- (2) $\deg fg = \deg f + \deg g$.

1.4. Dzielenie wielomianów. Stwierdzenie 1.3 będzie przydatne dla dowodu następującego twierdzenia:

Twierdzenie 1.4 (O dzieleniu wielomianów). *Niech \mathbb{F} będzie ciałem i niech $f, g \in \mathbb{F}[\mathfrak{X}]$. Załóżmy, że $g \neq 0$. Wówczas istnieją wielomiany $q, r \in \mathbb{F}[\mathfrak{X}]$ takie, że*

$$f = qg + r \quad \text{oraz} \quad \deg r < \deg g. \tag{1}$$

Ponadto wielomiany q i r są wyznaczone jednoznacznie przez warunki (1).

Dowód. Stosujemy metodę indukcji matematycznej. Dla $\deg f < \deg g$ warunki (1) są spełnione przez $q = 0$ i $r = f$. Załóżmy teraz, że $n = \deg f \geq \deg g$, i że twierdzenie jest prawdziwe dla wielomianów f' takich, że $\deg f' < n$. Niech

$$\begin{aligned}f &= \alpha_0 + \alpha_1\mathfrak{X} + \cdots + \alpha_n\mathfrak{X}^n, \\ g &= \beta_0 + \beta_1\mathfrak{X} + \cdots + \beta_m\mathfrak{X}^m\end{aligned} \tag{2}$$

Rozważmy wielomian $h = f - \frac{\alpha_n}{\beta_m} \mathfrak{X}^{n-m} g$. Rozpisując f i g zgodnie z (2) widzimy, że $\deg h < n$. Zatem istnieją p i r takie, że $h = pg + r$ i $\deg r < \deg g$. Teraz, skoro

$$f = h + \frac{\alpha_n}{\beta_m} \mathfrak{X}^{n-m} g = \left(p + \frac{\alpha_n}{\beta_m} \mathfrak{X}^{n-m}\right)g + r,$$

wielomiany $q = p + \frac{\alpha_n}{\beta_m} \mathfrak{X}^{n-m}$ i r spełniają warunki (1).

Udowodniliśmy więc istnienie rozkładu (1). Jedyność wielomianów q i r jest również łatwa: przypuśćmy, że $f = q'g + r'$, gdzie $\deg r' < \deg g$. Oznacza to, że

$$qg + r = q'g + r'.$$

Lub

$$(q - q')g = r' - r. \quad (3)$$

Rozważmy teraz stopień lewej strony (3). Jeśli $q' \neq q$, to ów stopień jest większy lub równy $\deg g$. Z drugiej strony stopień prawej strony (3) jest mniejszy lub równy $\max\{\deg r, \deg r'\} < \deg g$. Tak więc przypuszczenie, że $q' \neq q$ prowadzi do sprzeczności, a w konsekwencji mamy $q = q'$. W takim razie lewa strona (3) jest równa 0, a co za tym idzie $r = r'$. \square

1.5. Pierwiastki wielomianów.

Definicja 1.5. Niech \mathbb{F} będzie ciałem i niech $f \in \mathbb{F}[\mathfrak{X}]$:

$$f(\mathfrak{X}) = \alpha_0 + \alpha_1 \mathfrak{X} + \alpha_2 \mathfrak{X}^2 + \cdots + \alpha_n \mathfrak{X}^n.$$

(1) *Wartością wielomianu f w $\xi \in \mathbb{F}$ nazywamy skalar*

$$\alpha_0 + \alpha_1 \xi + \alpha_2 \xi^2 + \cdots + \alpha_n \xi^n.$$

Wartość f w ξ oznaczamy symbolem $f(\xi)$.

(2) *Pierwiastkiem f nazywamy taki skalar $\xi \in \mathbb{F}$, że $f(\xi) = 0$.*

Twierdzenie 1.6 (Bezout). *Niech \mathbb{F} będzie ciałem i niech $f \in \mathbb{F}[\mathfrak{X}]$. Wówczas $\xi \in \mathbb{F}$ jest pierwiastkiem wielomianu f wtedy i tylko wtedy, gdy istnieje wielomian $g \in \mathbb{F}[\mathfrak{X}]$ taki, że*

$$f = (\mathfrak{X} - \xi)g. \quad (4)$$

Dowód. Jeśli zapis (4) jest możliwy, to oczywiście $f(\xi) = 0$. Załóżmy więc, że ξ jest pierwiastkiem f i podzielmy wielomian f przez $(\mathfrak{X} - \xi)$. Mamy

$$f = (\mathfrak{X} - \xi)g + r,$$

gdzie $r \in \mathbb{F}[\mathfrak{X}]$ jest wielomianem stopnia mniejszego niż $\mathfrak{X} - \xi$, czyli wielomianem stałym. Biorąc wartość obu stron w ξ otrzymujemy $r = 0$. \square

Wniosek 1.7. *Wielomian stopnia n może mieć co najwyżej n -pierwiastków.*

Definicja 1.8. Niech \mathbb{F} będzie ciałem i niech $f \in \mathbb{F}[\mathfrak{X}]$. Niech $\xi \in \mathbb{F}$ będzie pierwiastkiem wielomianu f . *Krotnością pierwiastka ξ nazywamy największe $n \in \mathbb{N}$ takie, że istnieje $g \in \mathbb{F}[\mathfrak{X}]$ taki, że*

$$f = (\mathfrak{X} - \xi)^n g.$$

Ciało \mathbb{F} nazwiemy *algebraicznie domkniętym*, jeśli każdy wielomian $f \in \mathbb{F}[\mathfrak{X}]$ ma n pierwiastków licząc z krotnościami (pierwiastek krotności k liczymy jako k pierwiastków).

1.6. Zadania.

- (1) Przekonaj się o prawdziwości wszystkich stwierdzeń zawartych w akapicie po definicji 1.2.
- (2) Podaj dowód stwierdzenia 1.3.