

11. WYKŁAD 11: BAZA I STOPIEŃ ROZSZERZENIA. ELEMENTY ALGEBRAICZNE I PRZESTĘPNE.
ROZSZERZENIA ALGEBRAICZNE I SKOŃCZONE.

11.1. Baza i stopień rozszerzenia.

Uwaga 11.1. Niech F będzie ciałem, L rozszerzeniem ciała F . Wówczas L jest przestrzenią liniową nad ciałem F .

Definicja 11.1. Niech F będzie ciałem, L rozszerzeniem ciała F .

- (1) Wymiar przestrzeni liniowej L nad ciałem F nazywamy **stopniem rozszerzenia** ciała L nad ciałem F i oznaczamy $[L : F]$.
- (2) Bazę przestrzeni liniowej L nad ciałem F nazywamy **bazą rozszerzenia**.

Przykłady:

- (1) Rozważmy ciało $\mathbb{R}$ i jego rozszerzenie $\mathbb{C}$. Wówczas $[\mathbb{C} : \mathbb{R}] = 2$ i bazą rozszerzenia jest $\{1, i\}$.
- (2) Rozważmy dowolne ciało F . Wówczas $[F : F] = 1$ i bazą jest $\{1\}$.
- (3) Rozważmy dowolne ciało F . Wówczas $[F(x) : F] = \infty$.

Twierdzenie 11.1 (o stopniu rozszerzeń w wieży ciał). Niech F, L, M będą ciałami. Niech $F \subset L \subset M$ i niech $[L : F] = n < \infty$, $[M : L] = m < \infty$. Wówczas $[M : F] = nm$.

Dowód. Niech $(\alpha_1, \dots, \alpha_n)$ będzie bazą rozszerzenia $F \subset L$, zaś $(\beta_1, \dots, \beta_m)$ bazą rozszerzenia $L \subset M$. Pokażemy, że

$$(\alpha_1\beta_1, \dots, \alpha_1\beta_m, \alpha_2\beta_1, \dots, \alpha_2\beta_m, \dots, \alpha_n\beta_1, \dots, \alpha_n\beta_m)$$

jest liniowo niezależny nad ciałem F . Ustalmy $x_{11}, \dots, x_{1m}, x_{21}, \dots, x_{2m}, \dots, x_{n1}, \dots, x_{nm} \in F$ i niech

$$x_{11}\alpha_1\beta_1 + \dots + x_{1m}\alpha_1\beta_m + x_{21}\alpha_2\beta_1 + \dots + x_{2m}\alpha_2\beta_m + \dots + x_{n1}\alpha_n\beta_1 + \dots + x_{nm}\alpha_n\beta_m = 0.$$

Wówczas

$$(x_{11}\beta_1 + \dots + x_{1m}\beta_m)\alpha_1 + (x_{21}\beta_1 + \dots + x_{2m}\beta_m)\alpha_2 + \dots + (x_{n1}\beta_1 + \dots + x_{nm}\beta_m)\alpha_n = 0$$

i wobec liniowej niezależności $\alpha_1, \dots, \alpha_n$ otrzymujemy $x_{11}\beta_1 + \dots + x_{1m}\beta_m = 0, \dots, x_{n1}\beta_1 + \dots + x_{nm}\beta_m = 0$. Korzystając z liniowej niezależności $\beta_1, \dots, \beta_m$ otrzymujemy teraz $x_{11} = 0, \dots, x_{1m} = 0, x_{21} = 0, \dots, x_{2m} = 0, \dots, x_{n1} = 0, \dots, x_{nm} = 0$.

Pozostaje pokazać, że układ

$$(\alpha_1\beta_1, \dots, \alpha_1\beta_m, \alpha_2\beta_1, \dots, \alpha_2\beta_m, \dots, \alpha_n\beta_1, \dots, \alpha_n\beta_m)$$

jest generujący. Ustalmy element $\gamma \in M$. Wówczas $\gamma = \sum_{j=1}^m y_j\beta_j$, dla pewnych $y_1, \dots, y_m \in L$. Ponadto $y_j = \sum_{i=1}^n x_{ij}\alpha_i$, dla pewnych $x_{1j}, \dots, x_{nj} \in F$, $j \in \{1, \dots, m\}$. Wobec tego:

$$\gamma = x_{11}\alpha_1\beta_1 + \dots + x_{1m}\alpha_1\beta_m + x_{21}\alpha_2\beta_1 + \dots + x_{2m}\alpha_2\beta_m + \dots + x_{n1}\alpha_n\beta_1 + \dots + x_{nm}\alpha_n\beta_m.$$

□

Wniosek 11.1. Niech $F_1, \dots, F_r$ będą ciałami. Niech $F_1 \subset F_2 \subset \dots \subset F_r$ i niech $[F_2 : F_1] = n_1, \dots, [F_r : F_{r-1}] = n_{r-1}$. Wówczas $[F_r : F_1] = n_1 \cdot \dots \cdot n_{r-1}$.

Twierdzenie 11.2. Niech F będzie ciałem, niech L_1 i L_2 będą rozszerzeniami ciała F i niech $[L_1 : F] = r_1$, $[L_2 : F] = r_2$. Załóżmy ponadto, że $\text{NWD}(r_1, r_2) = 1$. Wówczas

$$[L_1L_2 : F] = [L_1 : F] \cdot [L_2 : F].$$

Dowód. Ponieważ $F \subset L_1 \subset L_1L_2$ oraz $F \subset L_2 \subset L_1L_2$, więc $r_1|[L_1L_2 : F]$ i $r_2|[L_1L_2 : F]$. Zatem $r_1r_2|[L_1L_2 : F]$. Ponieważ baza L_2 nad F generuje rozszerzenie L_1L_2 nad L_1 , więc $[L_1L_2 : F] \leq [L_2 : F]$. Zatem

$$[L_1L_2 : F] = [L_1L_2 : L_1] \cdot [L_1 : F] \leq [L_2 : F] \cdot [L_1 : F] = r_1r_2,$$

skąd $[L_1L_2 : F] = r_1r_2$. □

11.2. Elementy algebraiczne i przestępne.

Definicja 11.2. Niech F będzie ciałem, L rozszerzeniem ciała F , niech $\alpha \in L$.

- (1) Element α nazywamy **algebraicznym nad F** , jeżeli istnieje wielomian $0 \neq f \in F[x]$ taki, że $f(\alpha) = 0$.
- (2) Element α nazywamy **przestępnym nad F** , jeżeli nie jest algebraiczny.

Przykłady:

- (1) Rozważmy ciało $\mathbb{Q}$ i jego rozszerzenie $\mathbb{C}$. Element $\sqrt{2} \in \mathbb{C}$. Wówczas $\sqrt{2}$ jest algebraiczny nad $\mathbb{Q}$.
- (2) Rozważmy ciało F i jego rozszerzenie $F(x)$. Element $f \in F(x) \setminus F$ jest przestępny nad F .

Uwaga 11.2. Niech F, L, M będą ciałami i niech $F \subset L \subset M$. Wówczas

- (1) jeżeli $\alpha \in F$, to α jest algebraiczny nad F ;
- (2) jeżeli $\alpha \in M$ jest algebraiczny nad F , to jest też algebraiczny nad L .

Uwaga 11.3. Niech F będzie ciałem, L rozszerzeniem ciała F , niech $\alpha \in L$ będzie elementem algebraicznym nad F .

- (1) Zbiór $I_\alpha = \{f \in F[x] : f(\alpha) = 0\}$ jest ideałem maksymalnym.
- (2) Ideał I_α jest ideałem głównym.

Dowód. (1) Z łatwością sprawdzamy, że I_α istotnie jest ideałem. Pokażemy, że jest ideałem pierwszym. Ustalmy $f, g \in F[x]$ i niech $fg \in I_\alpha$. Wówczas $fg(\alpha) = 0$. Wobec tego $f(\alpha) = 0$ lub $g(\alpha) = 0$, a więc $f \in I_\alpha$ lub $g \in I_\alpha$.

Ponieważ $F[x]$ jest pierścieniem ideałów głównych, więc ideał I_α jest maksymalny.

- (2) Oczywiście. □

Definicja 11.3. Niech F będzie ciałem, L rozszerzeniem ciała F , niech $\alpha \in L$ będzie elementem algebraicznym nad F . Wielomian $f \in F[x]$ taki, że $(f) = I_\alpha$ nazywamy **wielomianem minimalnym** elementu α , a $\deg f$ **stopniem** elementu algebraicznego.

Twierdzenie 11.3. Niech F będzie ciałem, L rozszerzeniem ciała F , niech $\alpha \in L$ będzie elementem algebraicznym nad F . Następujące warunki są równoważne:

- (1) $f \in F[x]$ jest wielomianem minimalnym elementu $\alpha \in L$;
- (2) $f \in F[x]$ jest wielomianem unormowanym, nierozkładalnym i $f(\alpha) = 0$;
- (3) $f \in F[x]$ jest wielomianem unormowanym i najmniejszego stopnia spośród tych wielomianów, które zerują się w α .

Dowód. (1) $\Rightarrow$ (3) : Ustalmy $g \in F[x]$, unormowany i taki, że $g(\alpha) = 0$. Wówczas $g \in I_\alpha$. Zatem $f|g$, a więc $\deg f \leq \deg g$.

(3) $\Rightarrow$ (2) : Przypuśćmy, że f jest rozkładalny. Niech $f = gh$, $g, h \in F[x]$. Możemy założyć, że g i h są unormowane. Ponieważ $f(\alpha) = 0$, więc $g(\alpha) = 0$ lub $h(\alpha) = 0$ i $\deg g < \deg f$ oraz $\deg h < \deg f$ – sprzeczność.

(2) $\Rightarrow$ (1) : Oczywiście $f \in I_\alpha$, więc $(f) \subset I_\alpha$. Ponieważ $F[x]$ jest pierścieniem ideałów głównych i f jest nierozkładalny, więc (f) jest maksymalny. Stąd $(f) = I_\alpha$. $\square$

Przykłady:

- (3) Rozważmy ciało $\mathbb{Q}$, jego rozszerzenie $\mathbb{C}$ i element $\sqrt{2} \in \mathbb{C}$. Wówczas $x^2 - 2$ jest wielomianem minimalnym elementu $\sqrt{2}$. Stopień $\sqrt{2}$ jest więc równy 2.
- (4) Rozważmy ciało $\mathbb{Q}$, jego rozszerzenie $\mathbb{C}$ i element $\xi_p = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$, gdzie $p \in \mathbb{P}$ jest liczbą pierwszą. Wówczas $x^{p-1} + x^{p-2} + \dots + x + 1$ jest wielomianem minimalnym elementu ξ_p . Stopień ξ_p jest więc równy $p - 1$.

Twierdzenie 11.4. *Niech F będzie ciałem, L rozszerzeniem ciała F , niech $\alpha \in L$ będzie elementem algebraicznym nad F stopnia n . Wówczas:*

- (1) $F(\alpha) = \{r(\alpha) : r \in F[x], \deg r \leq n - 1\}$;
- (2) $(1, \alpha, \dots, \alpha^{n-1})$ jest bazą rozszerzenia $F \subset F(\alpha)$;
- (3) $[F(\alpha) : F] = n$.

Dowód. (1) Niech $f \in F[x]$ będzie wielomianem minimalnym elementu α . Niech $\gamma \in F(\alpha)$. Wówczas $\gamma = \frac{h(\alpha)}{g(\alpha)}$, dla pewnych $h, g \in F[x]$, $g(\alpha) \neq 0$. Ponieważ $g(\alpha) \neq 0$, więc $f \nmid g$. Ponieważ f jest nierozkładalny, więc $g \nmid f$. Wobec tego $1 \sim NWD(f, g)$ i tym samym istnieją elementy $u, v \in F[x]$ takie, że $uf + vg = 1$. Zatem $u(\alpha)f(\alpha) + v(\alpha)g(\alpha) = 1$, skąd $v(\alpha)g(\alpha) = 1$ i tym samym $v(\alpha) = \frac{1}{g(\alpha)}$. Wobec tego $\gamma = \frac{h(\alpha)}{g(\alpha)} = h(\alpha)v(\alpha)$. Dzieląc hv przez f otrzymujemy

$$hv = fq + r \text{ oraz } \deg r \leq \deg f - 1 = n - 1.$$

Ponadto $h(\alpha)v(\alpha) = f(\alpha)g(\alpha) + r(\alpha) = r(\alpha)$, więc $\gamma = r(\alpha)$ i $\deg r \leq n - 1$.

- (2) To, że układ $(1, \alpha, \dots, \alpha^{n-1})$ generuje $F(\alpha)$. Pozostaje wykazać, że jest to układ liniowo niezależny. Przypuśćmy, że istnieją elementy $c_0, c_1, \dots, c_{n-1} \in F$ takie, że $c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} = 0$. Wówczas wielomian $g(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ jest unormowany, $g(\alpha) = 0$ oraz $\deg g = n - 1 < n = \deg f$, co stanowi sprzeczność.
- (3) Wynika natychmiast z części (1). $\square$

Przykład:

- (5) Rozważmy ciało $\mathbb{Q}$ i jego rozszerzenie $\mathbb{C}$ oraz element $\sqrt[3]{5} \in \mathbb{C}$. Wówczas $\mathbb{Q}(\sqrt[3]{5}) = \{a_0 + a_1\sqrt[3]{5} + a_2\sqrt[3]{25} : a_0, a_1, a_2 \in \mathbb{Q}\}$.

Definicja 11.4. *Niech F będzie ciałem, L rozszerzeniem ciała F , niech $\alpha \in L$ będzie elementem algebraicznym nad F stopnia n . Bazę $(1, \alpha, \dots, \alpha^{n-1})$ rozszerzenia $F \subset F(\alpha)$ nazywamy **bazą potęgową**.*

Uwaga 11.4. *Niech F będzie ciałem, L rozszerzeniem ciała F , niech $\alpha \in L$. Wówczas α jest algebraiczny nad F wtedy i tylko wtedy, gdy $[F(\alpha) : F] < \infty$.*

Dowód. ($\Rightarrow$): wynika wprost z Twierdzenia 11.4.

($\Leftarrow$): Załóżmy, że $[F(\alpha) : F] = n < \infty$. Wówczas elementy $1, \alpha, \alpha^2, \dots, \alpha^n$ są liniowo zależne, więc istnieją elementy $a_0, a_1, \dots, a_n \in F$ takie, że $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$, a więc α jest algebraiczny. $\square$

Twierdzenie 11.5. *Niech F będzie ciałem, L rozszerzeniem ciała F , niech $\alpha_1, \dots, \alpha_n \in L$ będą elementami algebraicznymi nad F . Wówczas*

- (1) $[F(\alpha_1, \dots, \alpha_n) : F] < \infty$;
- (2) $F(\alpha_1, \dots, \alpha_n) = \{r(\alpha_1, \dots, \alpha_n) : r \in F[x_1, \dots, x_n]\}$.

11.3. Rozszerzenia algebraiczne i skończone.

Definicja 11.5. Niech F będzie ciałem, L rozszerzeniem ciała F . Rozszerzenie to nazywamy **rozszerzeniem algebraicznym**, gdy każdy element ciała L jest algebraiczny nad F . Rozszerzenie nazywamy **skończonym**, gdy $[L : F] < \infty$.

Twierdzenie 11.6. Każde rozszerzenie skończone jest algebraiczne.

Dowód. Załóżmy, że $F \subset L$ jest rozszerzeniem skończonym, $[L : F] = n < \infty$. Niech $\alpha \in L$. Wówczas $F \subset F(\alpha) \subset L$, więc $[F(\alpha) : F] \leq [L : F] < \infty$. Zatem α jest algebraiczny nad F . $\square$

Przykład:

- (1) Rozważmy ciało $\mathbb{Q}$ i jego rozszerzenie $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots)$. Wówczas jest to rozszerzenie algebraiczne, ale nie jest skończone.

Twierdzenie 11.7. Każde rozszerzenie skończone jest skończenie generowane.

Dowód. Załóżmy, że $F \subset L$ jest rozszerzeniem skończonym, a $(\alpha_1, \dots, \alpha_n)$ bazą tego rozszerzenia. Wówczas $L = F(\alpha_1, \dots, \alpha_n)$. $\square$

Przykład:

- (2) Rozważmy dowolne ciało F i jego rozszerzenie $F(x)$. Wówczas jest to rozszerzenie skończenie generowane, ale nie jest skończone.

Twierdzenie 11.8. Niech F będzie ciałem, L rozszerzeniem ciała F , niech $\alpha_1, \dots, \alpha_n \in L$. Następujące warunki są równoważne:

- (1) $\alpha_1, \dots, \alpha_n \in L$ są elementami algebraicznymi nad F ;
- (2) $F \subset F(\alpha_1, \dots, \alpha_n)$ jest rozszerzeniem skończonym;
- (3) $F \subset F(\alpha_1, \dots, \alpha_n)$ jest rozszerzeniem algebraicznym.

Uwaga 11.5. Niech F będzie ciałem, L rozszerzeniem ciała F . Niech $S \subset L$ będzie zbiorem elementów algebraicznych nad ciałem F . Wówczas $F \subset F(S)$ jest rozszerzeniem algebraicznym.

Twierdzenie 11.9. Niech F, L, M będą ciałami i niech $F \subset L \subset M$. Wówczas

$F \subset M$ jest skończone wtedy i tylko wtedy, gdy $F \subset L$ i $L \subset M$ są skończone.

Twierdzenie 11.10. Niech F, L, M, N będą ciałami i niech $F \subset L \subset M$. Niech ponadto $N \subset L$. Wówczas jeżeli $F \subset M$ jest skończone, to $NF \subset NM$ jest skończone i $[NM : NF] \leq [M : F]$.

Dowód. Niech $(\alpha_1, \dots, \alpha_n)$ będzie bazą rozszerzenia $F \subset M$. Wówczas $M = F(\alpha_1, \dots, \alpha_n)$. Wobec tego $NM = NF(\alpha_1, \dots, \alpha_n)$. Ponieważ $[M : F] < \infty$ więc $\alpha_1, \dots, \alpha_n$ są algebraiczne nad F , a więc także nad NF . Zatem dla $\gamma \in NM$, $\gamma = g(\alpha_1, \dots, \alpha_n)$, gdzie $g \in NF[x_1, \dots, x_n]$. Ponadto $\alpha_1^{k_1}, \dots, \alpha_n^{k_n} \in M$, dla $k_1, \dots, k_n \geq 0$, więc $\alpha_1^{k_1} \cdot \dots \cdot \alpha_n^{k_n} = c_1 \alpha_1 + \dots + c_n \alpha_n$, dla pewnych $c_1, \dots, c_n \in F$. Zatem dla dowolnego $g \in NF[x_1, \dots, x_n]$ zachodzi $g(\alpha_1, \dots, \alpha_n) = d_1 \alpha_1 + \dots + d_n \alpha_n$, dla pewnych $d_1, \dots, d_n \in NF$. Stąd $[NM : NF] \leq n = [M : F]$. $\square$

Wniosek 11.2. Niech F będzie ciałem, niech L_1 i L_2 będą rozszerzeniami skończonymi ciała F . Wówczas $F \subset L_1 L_2$ jest rozszerzeniem skończonym oraz $[L_1 L_2 : F] \leq [L_1 : F] \cdot [L_2 : F]$.

Dowód. Wobec Twierdzenia 11.10 $[L_1 L_2 : L_1] \leq [L_2 : F]$, więc $[L_1 L_2 : F] = [L_1 L_2 : L_1][L_1 : F] \leq [L_1 : F] \cdot [L_2 : F]$. $\square$

Twierdzenie 11.11. Niech F, L, M będą ciałami i niech $F \subset L \subset M$. Wówczas

$F \subset M$ jest algebraiczne wtedy i tylko wtedy, gdy $F \subset L$ i $L \subset M$ są algebraiczne.

Dowód. ($\Rightarrow$) : oczywiste.

($\Leftarrow$) : Ustalmy $\gamma \in M$. Ponieważ rozszerzenie $L \subset M$ jest algebraiczne, więc istnieją elementy $b_0, b_1, \dots, b_n \in L$ takie, że $b_0 + b_1\gamma + \dots + b_n\gamma^n = 0$. Niech $g(x) = b_0 + b_1x + \dots + b_nx^n$. Wówczas $g \in F(b_0, b_1, \dots, b_n)[x]$ i γ jest algebraiczny nad ciałem $F(b_0, b_1, \dots, b_n)$. Wobec tego rozszerzenie $F(b_0, b_1, \dots, b_n) \subset F(b_0, b_1, \dots, b_n)(\gamma)$ jest skończone. Ponieważ rozszerzenie $F \subset L$ jest algebraiczne, więc elementy $b_0, b_1, \dots, b_n \in L$ są algebraiczne nad F i wobec tego rozszerzenie $F \subset F(b_0, b_1, \dots, b_n)$ jest skończone. Zatem i rozszerzenie $F \subset F(b_0, b_1, \dots, b_n)(\gamma)$ jest skończone, a więc i algebraiczne. Tym samym element γ jest algebraiczny nad ciałem F . $\square$

Twierdzenie 11.12. Niech F będzie ciałem, L rozszerzeniem ciała F , niech $\alpha, \beta \in L$ będą algebraiczne nad ciałem F . Wówczas elementy $\alpha \pm \beta$, $\alpha \cdot \beta$ oraz $\frac{\alpha}{\beta}$ (o ile $\beta \neq 0$) są algebraiczne nad F .

Dowód. Ponieważ α i β są algebraiczne nad ciałem F , więc rozszerzenie $F \subset F(\alpha, \beta)$ jest skończone, a więc i algebraiczne. Oczywiście $\alpha \pm \beta$, $\alpha \cdot \beta$ oraz $\frac{\alpha}{\beta}$ są elementami ciała $F(\alpha, \beta)$. $\square$

Wniosek 11.3. Niech F będzie ciałem, L rozszerzeniem ciała F . Niech

$$F_{alg}(L) = \{\alpha \in L : \alpha \text{ jest algebraiczny nad } F\}.$$

Wówczas $F_{alg}(L)$ jest ciałem.

Wniosek 11.4. Niech F będzie ciałem, niech L_1 i L_2 będą rozszerzeniami algebraicznymi ciała F . Wówczas rozszerzenie $F \subset L_1L_2$ też jest algebraiczne.

Dowód. Niech L będzie rozszerzeniem ciała F zawierającym ciała L_1 i L_2 . Ponieważ rozszerzenia $F \subset L_1$ oraz $F \subset L_2$ są algebraiczne, więc $L_1, L_2 \subset F_{alg}(L)$. Wobec tego $L_1L_2 \subset F_{alg}(L)$ i rozszerzenie $F \subset L_1L_2$ jest algebraiczne. $\square$

Definicja 11.6. Niech F będzie ciałem, L rozszerzeniem ciała F .

- (1) Ciało $F_{alg}(L)$ nazywamy **domknięciem algebraicznym ciała F w ciele L** .
- (2) Jeżeli $F = F_{alg}(L)$ to mówimy, że F jest **algebraicznie domknięte w L** .

Przykład:

- (3) Rozważmy ciało $\mathbb{Z}_2$ i ciało czteroelementowe L zawierające $\mathbb{Z}_2$ jako podciało proste, a więc w szczególności rozszerzenie ciała $\mathbb{Z}_2$. Wówczas $\mathbb{Z}_2$ jest algebraicznie domknięte w L , ale oczywiście $\mathbb{Z}_2$ nie jest algebraicznie domknięte.