

12. WYKŁAD 12: ALGEBRAICZNE DOMKNIECIE CIAŁA. WIELOKROTNE PIERWIĄSTKI
WIELOMIANÓW. RÓŻNICZKOWANIE WIELOMIANÓW. ELEMENTY ROZDZIELCZE. ROZSZERZENIA
ROZDZIELCZE I POJEDYNCZE. ROZSZERZENIA NORMALNE.

12.1. Algebraiczne domknięcie ciała.

Twierdzenie 12.1. *Niech F będzie ciałem. Następujące warunki są równoważne:*

- (1) F jest algebraicznie domknięte,
- (2) jeżeli L jest ciałem i rozszerzenie $F \subset L$ jest skończone, to $F = L$,
- (3) jeżeli L jest ciałem i rozszerzenie $F \subset L$ jest algebraiczne, to $F = L$.

Dowód. (1) $\Rightarrow$ (3) : Załóżmy, że F jest algebraicznie domknięte i $F \subset L$ jest rozszerzeniem algebraicznym. Niech $\alpha \in L$. Wówczas α jest algebraiczne nad F . Niech $f \in F[x]$ będzie wielomianem minimalnym elementu α . Wówczas f jest nierozkładalny w $F[x]$, a więc liniowy. Zatem $\alpha \in F$.

(3) $\Rightarrow$ (2) : Każde rozszerzenie skończone jest algebraiczne.

(2) $\Rightarrow$ (1) : Niech $f \in F[x]$ i niech L będzie ciałem, w którym f ma pierwiastek, przy czym $F \subset L$. Niech $\alpha \in L$ będzie pierwiastkiem wielomianu f . Wówczas α jest algebraiczny nad F . Zatem $F \subset F(\alpha)$ jest skończone, a więc $F(\alpha) = F$ i $\alpha \in F$. $\square$

Definicja 12.1. *Niech F będzie ciałem, L rozszerzeniem ciała F . Jeżeli*

- (1) L jest ciałem algebraicznie domkniętym,
- (2) $F \subset L$ jest rozszerzeniem algebraicznym,

to L nazywamy algebraicznym domknięciem ciała F i oznaczamy $\overline{F}$.

Przykład:

- (1) Rozważmy ciało $\mathbb{R}$. Wówczas $\mathbb{C}$ jest algebraicznym domknięciem ciała $\mathbb{R}$.

Twierdzenie 12.2. *Niech F będzie ciałem, L rozszerzeniem ciała F , niech ponadto L będzie ciałem algebraicznie domkniętym. Wówczas $F_{alg}(L)$ jest algebraicznym domknięciem ciała F .*

Dowód. Niech $f \in F_{alg}(L)[x]$. Wówczas również $f \in L[x]$, więc f ma pierwiastek $\alpha \in L$. Wobec tego α jest algebraiczny nad ciałem $F_{alg}(L)$, więc rozszerzenie $F_{alg}(L) \subset F_{alg}(L)(\alpha)$ jest algebraiczne. Ponadto $F \subset F_{alg}(L)$ jest algebraiczne, więc $F \subset F_{alg}(L)(\alpha)$ jest algebraiczne. Zatem α jest algebraiczny nad F , a więc $\alpha \in F_{alg}(L)$. $\square$

Wniosek 12.1. *Niech F będzie ciałem. Wówczas istnieje algebraiczne domknięcie $\overline{F}$ ciała F .*

Dowód. Wobec Twierdzenia 10.6 istnieje ciało algebraicznie domknięte L takie, że $F \subset L$. Z kolei wobec Twierdzenia 12.2 $\overline{F} = F_{alg}(L)$. $\square$

Twierdzenie 12.3. *Niech F będzie ciałem, niech L_1, L_2 będą algebraicznymi domknięciami ciała F . Wówczas istnieje F izomorfizm $\phi : L_1 \rightarrow L_2$.*

Dowód poprzedzimy dwoma lematami:

Lemat 12.1. *Niech F, F_1, F_2 będą ciałami i niech $F \subset F_1 \subset F_2$ będą rozszerzeniami algebraicznymi. Niech $\phi_1 : F_1 \rightarrow \overline{F}$ będzie F -zanurzeniem. Wówczas istnieje zanurzenie $\phi_2 : F_2 \rightarrow \overline{F}$ takie, że $\phi_2|_{F_1} = \phi_1$.*

Dowód. Niech

$$\mathcal{R} = \{(L, \phi) : L \text{ jest ciałem, } F_1 \subset L \subset F_2, \phi : L \rightarrow \overline{F} \text{ jest } F\text{-zanurzeniem, } \phi|_{F_1} = \phi_1\}.$$

W rodzinie $\mathcal{R}$ definiujemy relację $\prec$ wzorem:

$$(L, \phi) \prec (L', \phi') \text{ wtedy i tylko wtedy, gdy } L \subset L' \text{ oraz } \phi'|_L = \phi.$$

Bez trudu sprawdzamy, że jest to relacja częściowego porządku. Ponadto $(F_1, \phi_1) \in \mathcal{R}$, a więc $\mathcal{R} \neq \emptyset$. Łatwo jest również sprawdzić, że każdy łańcuch w rodzinie $\mathcal{R}$ ma ograniczenie górne. Wobec lematu Kuratowskiego-Zorna w rodzinie $\mathcal{R}$ istnieje element maksymalny (L_0, ϕ_0) . Pokażemy, że $F_2 = L_0$.

Przypuśćmy, że $F_2 \neq L_0$. Wówczas istnieje element $a \in F_2 \setminus L_0$. Ponieważ rozszerzenie $F \subset F_2$ jest algebraiczne, więc a jest algebraiczny nad F , a tym samym jest też algebraiczny nad L_0 . Niech $f \in L_0[x]$ będzie wielomianem minimalnym elementu a . Niech ponadto $\tilde{\phi}_0 : L_0[x] \rightarrow \overline{F}[x]$ będzie przedłużeniem zanurzenia $\phi_0 : L \rightarrow \overline{F}$ na pierścieniu wielomianów. Wówczas wielomian $\tilde{\phi}_0(f)$ jest nierozkładalny w pierścieniu $\phi_0(L_0)[x]$, jako obraz elementu nierozkładalnego. Ponieważ ciało $\overline{F}$ jest algebraicznie domknięte, więc wielomian $\tilde{\phi}_0(f)$ ma pierwiastek $b \in \overline{F}$. Wobec Twierdzenia 10.2 istnieje przedłużenie izomorfizmu $\phi_0 : L_0 \rightarrow \phi_0(L_0)$ do zanurzenia $\phi'_0 : L_0(a) \rightarrow \phi_0(L_0)(b) \subset \overline{F}$. Wówczas $(L_0, \phi_0) \prec (L_0(a), \phi'_0)$ oraz $L_0 \subsetneq L_0(a)$, więc element (L_0, ϕ_0) nie może być maksymalny w rodzinie $\mathcal{R}$, co daje sprzeczność. $\square$

Lemat 12.2. *Niech F będzie ciałem, L rozszerzeniem algebraicznym ciała F . Wówczas istnieje F -zanurzenie $\phi : L \rightarrow \overline{F}$.*

Dowód. W poprzednim lemacie wystarczy przyjąć $F_2 = L$, $F_1 = F$ oraz $\phi_1 = id_F$. $\square$

Przechodzimy do dowodu Twierdzenia 12.3:

Dowód. Wobec poprzedniego lematu istnieje F -zanurzenie $\phi : L_1 \rightarrow L_2$. Ciało $\phi(L_1)$ jest algebraicznie domknięte. Ponadto rozszerzenie $\phi(L_1) \subset L_2$ jest algebraiczne, a więc $\phi(L_1) = L_2$. $\square$

12.2. Wielokrotne pierwiastki wielomianów. Różniczkowanie wielomianów.

Definicja 12.2. *Niech F będzie ciałem. Wielomian $f \in F[x]$ nazywamy **rozdzielczym**, gdy w każdym rozszerzeniu L ciała F ma on wyłącznie pierwiastki jednokrotne.*

Twierdzenie 12.4 (o wzorach Viete'y²²). *Niech R będzie pierścieniem całkowitym, niech $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in R[x]$ będzie wielomianem unormowanym. Niech $x_1, \dots, x_n \in R$ będą wszystkimi (uwzględniając krotności) pierwiastkami f w pierścieniu R . Wówczas:*

$$\begin{aligned} a_{n-1} &= -(x_1 + \dots + x_n), \\ &\vdots \\ a_{n-k} &= (-1)^k \sum_{i_1, \dots, i_k} x_{i_1} \cdot \dots \cdot x_{i_k}, \\ &\vdots \\ a_0 &= (-1)^n x_1 \cdot \dots \cdot x_n. \end{aligned}$$

Dowód. Dowód otrzymujemy porównując współczynniki przy kolejnych potęgach x 'a w równości:

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = (x - x_1) \cdot (x - x_2) \cdot \dots \cdot (x - x_n).$$

$\square$

²²F. Viete (1540-1603) – matematyk i prawnik francuski.

Definicja 12.3. Niech R będzie pierścieniem, niech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in R[x]$ będzie wielomianem. Wielomian

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1 \in R[x]$$

nazywamy **pochodną** wielomianu f . Wielomian $f^{(k)}(x) = f'(f^{(k-1)}(x))$, gdzie $f^{(1)}(x) = f'(x)$, nazywamy **k -tą pochodną** wielomianu f .

Definicja 12.4. Niech R będzie pierścieniem, niech $f_1, f_2, \dots, f_n \in R[x]$. Wielomian

$$\det \begin{bmatrix} f_1 & f_2 & f_3 & \dots & f_n \\ f_1' & f_2' & f_3' & \dots & f_n' \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_1^{(n-1)} & f_2^{(n-1)} & f_3^{(n-1)} & \dots & f_n^{(n-1)} \end{bmatrix}$$

nazywamy **wrońskianem**²³ wielomianów $f_1, f_2, \dots, f_n \in R[x]$.

Uwaga 12.1. Niech R będzie pierścieniem, niech $f, g \in R[x]$, niech $a \in R$. Wówczas:

- (1) $(f + g)' = f' + g'$,
- (2) $(af)' = af'$,
- (3) $(fg)' = f'g + fg'$,
- (4) $(f^n)' = n f^{n-1} f'$.

Proste dowody pozostawiamy jako ćwiczenie.

Twierdzenie 12.5 (wzór Leibniza). Niech R będzie pierścieniem, niech $f, g \in R[x]$. Wówczas

$$(fg)^{(k)} = \sum_{i=0}^k \binom{k}{i} f^{(k-i)} g^{(i)}.$$

Prosty dowód pozostawiamy jako ćwiczenie.

Twierdzenie 12.6 (wzór Maclaurina). Niech R będzie pierścieniem, niech $f \in R[x]$. Wówczas

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \dots + \frac{f^{(n)}(0)}{n!}x^n,$$

gdzie $n = \deg f$.

Prosty dowód pozostawiamy jako ćwiczenie.

Twierdzenie 12.7 (wzór Taylora). Niech R będzie pierścieniem, niech $f \in R[x]$, $c \in R$. Wówczas

$$f(x+c) = f(c) + \frac{f'(c)}{1!}x + \frac{f''(c)}{2!}x^2 + \dots + \frac{f^{(n)}(c)}{n!}x^n,$$

gdzie $n = \deg f$.

Prosty dowód pozostawiamy jako ćwiczenie.

Twierdzenie 12.8. Niech R będzie pierścieniem, niech $f \in R[x]$, $a \in R$. Wówczas

a jest pierwiastkiem k -krotnym f wtedy i tylko wtedy, gdy $f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0$,
 $f^{(k)}(a) \neq 0$.

²³J. Hoene-Wroński (1776-1853) – matematyk, filozof, fizyk, prawnik i ekonomista polski, autor prac z zakresu analizy zespolonej.

Dowód. $(\Rightarrow)$: Załóżmy, że a jest k -krotnym pierwiastkiem f . Wobec tego istnieje wielomian $g \in R[x]$ taki, że

$$f(x) = (x - a)^k g(x) \text{ oraz } g(a) \neq 0.$$

Tym samym

$$f'(x) = (x - a)^{k-1} [kg(x) + (x - a)g'(x)] = (x - a)^{k-1} h(x),$$

gdzie $h(a) \neq 0$. Jeżeli $k - 1 > 0$, to

$$f''(x) = (x - a)^{k-2} h_1(x),$$

gdzie $h_1(a) \neq 0$. Postępując indukcyjnie po $k - 1$ krokach otrzymujemy

$$\begin{aligned} f^{(k-1)}(x) &= (x - a)h_{k-2}(x) \text{ oraz } h_{k-2}(x) \neq 0, \\ f^{(k)}(x) &= h_{k-2}(x) + (x - a)h'_{k-2}(x), \end{aligned}$$

a więc $f^{(k)}(a) \neq 0$ oraz $f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0$, $f^{(k)}(a) \neq 0$.

$(\Leftarrow)$: Załóżmy, że $f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0$, $f^{(k)}(a) \neq 0$. Niech l będzie krotnością pierwiastka a . Gdyby $l < k$ lub $l > k$, to otrzymujemy sprzeczność z udowodnioną już częścią twierdzenia. $\square$

Wniosek 12.2. Niech F będzie ciałem, niech $f \in F[x]$ i niech $g \sim NWD(f, f')$. Wówczas jeśli $a \in F$ jest pierwiastkiem wielokrotnym wielomianu f , to a jest też pierwiastkiem wielomianu g .

Dowód. Załóżmy, że $g(x) \sim NWD(f(x), f'(x))$. Wówczas istnieją wielomiany $u, v \in F[x]$ takie, że

$$uf + vf' = g.$$

Wobec Twierdzenia 12.8 $f(a) = 0$ oraz $f'(a) = 0$, a zatem $g(a) = 0$. $\square$

Wniosek 12.3. Niech F będzie ciałem, niech $f \in F[x]$. Wówczas każdy pierwiastek f (w dowolnym ciele) jest jednokrotny wtedy i tylko wtedy, gdy $NWD(f, f') \sim 1$.

Dowód. $(\Leftarrow)$: Przypuśćmy, że $a \in F$ jest pierwiastkiem wielokrotnym. Wobec Twierdzenia 12.8 $f(a) = 0$ oraz $f'(a) = 0$, a zatem $x - a \mid f(x)$ oraz $x - a \mid f'(x)$, co daje sprzeczność.

$(\Rightarrow)$: Przypuśćmy, że $NWD(f, f') \sim g \neq 1$. Wówczas $\deg g > 0$ oraz istnieje element $a \in \overline{F}$ taki, że $g(a) = 0$. Zatem $f(a) = 0$ oraz $f'(a) = 0$, więc a jest pierwiastkiem wielokrotnym f , co znów daje sprzeczność. $\square$

Wniosek 12.4. Niech F będzie ciałem, niech $f \in F[x]$, niech ponadto $\text{char} F = 0$. Wówczas jeżeli f jest nierozkładalny w $F[x]$, to ma wyłącznie pierwiastki jednokrotne (w dowolnym ciele).

Dowód. Niech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in F[x]$, gdzie $a_n \neq 0$. Wówczas $f'(x) = na_n x^{n-1} + (n-1)a_{n-1} x^{n-2} + \dots + 2a_2 x + a_1 \neq 0$. Ponadto $\deg f' = n - 1$, więc $f \nmid f'$. Ponieważ f jest nierozkładalny, więc $NWD(f, f') \sim 1$ i wobec udowodnionego powyżej wniosku każdy pierwiastek f w dowolnym ciele jest jednokrotny. $\square$

12.3. Elementy rozdzielcze.

Definicja 12.5. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F , niech $\alpha \in L$ będzie elementem algebraicznym nad F . Element ten nazywamy **rozdzielczym** nad F , gdy jego wielomian minimalny jest rozdzielczy.

Przykłady:

- (1) Rozważmy ciało $\mathbb{Q}$ i jego rozszerzenie $\mathbb{C}$ oraz element $\sqrt{2} \in \mathbb{C}$. Wówczas $\sqrt{2}$ jest rozdzielnym nad $\mathbb{Q}$.

Uwaga 12.2. Niech F będzie ciałem, niech $f \in F[x]$.

- (1) Jeżeli $\text{char} F = 0$, to $f' \equiv 0$ wtedy i tylko wtedy, gdy $\deg f = 0$.
 (2) Jeżeli $\text{char} F = p$, to $f' \equiv 0$ wtedy i tylko wtedy, gdy $f(x) = g(x^p)$ dla pewnego $g \in F[x]$.

Dowód. (1) $(\Leftarrow)$: oczywiste. $(\Rightarrow)$: Niech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. Wówczas $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1$. Ponieważ $f' \equiv 0$, więc $n a_n = \dots = 2 a_2 = a_1 = 0$. Skoro $\text{char} F = 0$, oznacza to, że $a_n = \dots = a_1 = 0$.

- (2) $(\Leftarrow)$: Jeżeli $f(x) = g(x^p)$ oraz $\text{char} F = p$, to wówczas:

$$f'(x) = (g(x^p))' = g'(x^p) p x^{p-1} = 0.$$

$(\Rightarrow)$: Niech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. Wówczas $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1$. Ponieważ $f' \equiv 0$, więc $n a_n = \dots = 2 a_2 = a_1 = 0$. Skoro $\text{char} F = p$, więc $a_j = 0$ dla $p \nmid j$, $j \in \{1, \dots, n\}$. Zatem $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \dots = g(x^p)$. □

Twierdzenie 12.9. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F , niech $\alpha \in L$ będzie elementem algebraicznym nad F .

- (1) Jeżeli $\text{char} F = 0$, to α jest rozdzielnym.
 (2) Jeżeli $\text{char} F = p$, to α jest rozdzielnym wtedy i tylko wtedy, gdy wielomian minimalny elementu α nie jest postaci $f(x) = g(x^p)$ dla pewnego $g \in F[x]$.

Dowód. Niech $f \in F[x]$ będzie wielomianem minimalnym elementu α . Ponieważ $\deg f' < \deg f$, więc $\text{NWD}(f, f') \approx 1$ wtedy i tylko wtedy, gdy $f' \equiv 0$. Wobec Wniosku 12.3 α nie jest rozdzielnym wtedy i tylko wtedy, gdy $f' \equiv 0$ i wobec uwagi poprzedzającej twierdzenie otrzymujemy tezę. □

Wniosek 12.5. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F , niech $\alpha \in L$ będzie elementem algebraicznym nad F . Jeżeli $\text{char} F = p$, to istnieje $n \in \mathbb{N}$ takie, że α^{p^n} jest rozdzielnym.

Dowód. Niech $f \in F[x]$ będzie wielomianem minimalnym elementu α . Niech ponadto $n = \max\{k \in \mathbb{N} : p^k \text{ jest dzielnikiem wszystkich stopni jednomianów w } f\}$. Wówczas $f(x) = g(x^{p^n})$ oraz nie każdy jednomian w g ma stopień podzielny przez p . Zatem $g' \not\equiv 0$. Ponadto, skoro f jest nierozkładalny, to g jest rozkładalny. Dalej, $g(\alpha^{p^n}) = f(\alpha) = 0$. Zatem α^{p^n} jest rozdzielnym nad F . □

Twierdzenie 12.10. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F , niech $\alpha \in L$ będzie elementem algebraicznym nad F . Jeżeli $\text{char} F = p$, to α jest rozdzielnym wtedy i tylko wtedy, gdy $F(\alpha) = F(\alpha^p)$.

Dowód. $(\Rightarrow)$: Niech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ będzie wielomianem minimalnym elementu α . Ponieważ α jest rozdzielnym, więc $f' \not\equiv 0$. Pokażemy, że wielomian $f_p(x) = a_0^p + a_1^p x + \dots + a_n^p x^n$ jest nierozkładalny i $f'_p \not\equiv 0$.

Istotnie, ponieważ $f' \not\equiv 0$, więc istnieje jednomian $a_r x^r$ w $f(x)$ taki, że $p \nmid r$. Wobec tego jednomian $a_r^p x^r$ w $f_p(x)$ jest stopnia r , a zatem $f'_p \not\equiv 0$. Przypuśćmy, że istnieje $g \in F[x]$ taki, że $g|f_p$ oraz $\deg g \geq 1$. Wówczas $g(x^p)|f_p(x^p) = a_0^p + a_1^p x^p + \dots + a_n^p x^{np} = (a_0 + a_1 x + \dots + a_n x^n)^p = [f(x)]^p$. Ponieważ f jest nierozkładalny, więc $g(x^p) = (f(x))^m$, $1 \leq m < p$. Zatem $0 = g'(x^p) p x^{p-1} = m [f(x)]^{m-1} f'(x)$, skąd $f' \equiv 0$, co daje sprzeczność.

Zauważmy, że ponadto $f_p(\alpha^p) = a_0^p + a_1^p \alpha^p + \dots + a_n^p \alpha^{np} = [f(\alpha)]^p = 0$. Ponieważ $\deg f = \deg f_p = n$, więc $[F(\alpha) : F] = [F(\alpha^p) : F] = n$. Skoro $F(\alpha^p) \subset F(\alpha)$, więc $F(\alpha) = F(\alpha^p)$.

($\Leftarrow$) : Załóżmy, że α nie jest rozdzielnym nad F . Wówczas jego wielomian minimalny jest postaci $f(x) = g(x^p)$. Ponieważ f jest nierozkładalny, więc g jest nierozkładalny. Ponadto $\deg f = p \deg g > \deg g$ oraz $g(\alpha^p) = f(\alpha) = 0$. Zatem $[F(\alpha) : F] = \deg f > \deg g = [F(\alpha^p) : F]$. Skoro $F(\alpha^p) \subset F(\alpha)$, więc $F(\alpha^p) \not\subset F(\alpha)$. $\square$

12.4. Rozszerzenia rozdzielcze i pojedyncze.

Definicja 12.6. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F . Rozszerzenie to nazywamy **rozdzielczym**, gdy każdy element $\alpha \in L$ jest rozdzielnym nad F . Rozszerzenie nazywamy **pojedynczym**, gdy istnieje element $\alpha \in L$ taki, że $L = F(\alpha)$.

Twierdzenie 12.11. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F , niech $\alpha_1, \dots, \alpha_n \in L$ będą rozdzielczymi. Wówczas rozszerzenie $F \subset F(\alpha_1, \dots, \alpha_n)$ jest rozdzielcze.

Dowód twierdzenia poprzedzimy dwoma lematami.

Lemat 12.3. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F , niech elementy $\alpha_1, \dots, \alpha_n \in L$ będą rozdzielczymi. Jeżeli $\text{char} F = p$, to wówczas $F(\alpha_1, \dots, \alpha_n) = F(\alpha_1^p, \dots, \alpha_n^p)$.

Dowód. Wobec Twierdzenia 12.10 $F(\alpha_i) = F(\alpha_i^p)$, dla $i \in \{1, \dots, n\}$. Wobec tego

$$F(\alpha_1, \dots, \alpha_n) = F(\alpha_1)F(\alpha_2) \dots F(\alpha_n) = F(\alpha_1^p)F(\alpha_2^p) \dots F(\alpha_n^p) = F(\alpha_1^p, \alpha_2^p, \dots, \alpha_n^p).$$

$\square$

Lemat 12.4. Niech F będzie ciałem, niech L będzie skończonym rozszerzeniem ciała F . Jeżeli $\text{char} F = p$, to rozszerzenie $F \subset L$ jest rozdzielcze wtedy i tylko wtedy, gdy $FL^p = L^{24}$.

Dowód. ($\Rightarrow$) : Ustalmy $a \in L$. Ponieważ a jest rozdzielnym, więc $F(a) = F(a^p)$. Ponieważ $F(a^p) \subset FL^p$, więc $a \in FL^p$, zatem $L \subset FL^p$. Oczywiście zawsze $FL^p \subset L$.

($\Leftarrow$) : Zdefiniujmy odwzorowanie $\Phi : L \rightarrow L^p$ wzorem $\Phi(a) = a^p$. Oczywiście Φ jest izomorfizmem. Wobec tego dla $b \in L$ mamy $[\Phi(L) : \Phi(F(b))] = [L : F(b)] < \infty$. Wobec Twierdzenia 11.10 $[F\Phi(L) : F\Phi(F(b))] \leq [\Phi(L) : \Phi(F(b))] < \infty$. Ponadto $F\Phi(L) = FL^p = L$ oraz $F\Phi(F(b)) = FF^p(b^p) = F(b^p)$. Wobec tego $[L : F(b^p)] \leq [L : F(b)] < \infty$. Zatem

$$[L : F(b^p)] = [L : F(b)] \cdot [F(b) : F(b^p)] \geq [L : F(b^p)] \cdot [F(b) : F(b^p)].$$

Stąd $[F(b) : F(b^p)] = 1$, czyli $F(b) = F(b^p)$. Zatem $b \in L$ jest rozdzielnym i rozszerzenie $F \subset L$ jest rozdzielcze. $\square$

Przechodzimy do dowodu Twierdzenia 12.11:

Dowód. Załóżmy, że $\text{char} F = 0$. Teza wynika z Twierdzeń 11.8 i 12.9. Załóżmy, że $\text{char} F = p$. Ponieważ $\alpha_1, \dots, \alpha_n \in L$ są algebraiczne, więc wobec Twierdzenia 11.8 $[F(\alpha_1, \dots, \alpha_n) : F] < \infty$. Dalej, wobec pierwszego lematu:

$$F[F(\alpha_1, \dots, \alpha_n)]^p = FF^p(\alpha_1^p, \dots, \alpha_n^p) = F(\alpha_1^p, \dots, \alpha_n^p) = F(\alpha_1, \dots, \alpha_n),$$

a wobec drugiego lematu rozszerzenie $F \subset F(\alpha_1, \dots, \alpha_n)$ jest rozdzielcze. $\square$

Twierdzenie 12.12 (Abela o elemencie pierwotnym). Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F , niech $\alpha_1, \dots, \alpha_n \in L$ będą rozdzielczymi. Wówczas istnieje taki element rozdzielnym $\alpha \in L$, że $F(\alpha) = F(\alpha_1, \dots, \alpha_n)$.

²⁴Przypomnijmy, że **potęga ciała** L zdefiniowana jest $L^p = \Phi(L)$, gdzie $\Phi : L \rightarrow L$ dane jest wzorem $\Phi(a) = a^p$

Dowód. Dowód prowadzimy indukcyjnie względem n . Niech $n = 2$. Załóżmy, że $|F| < \infty$. Wobec Twierdzenia 11.8 rozszerzenie $F \subset F(\alpha_1, \alpha_2)$ jest skończone, a więc $|F(\alpha_1, \alpha_2)| < \infty$. Niech $|F(\alpha_1, \alpha_2)| = p^n$, gdzie $p = \text{char} F$. Ponieważ grupa mnożeniowa ciała skończonego jest cykliczna, więc $\langle \alpha \rangle = F(\alpha_1, \alpha_2)^*$, dla pewnego $\alpha \in F(\alpha_1, \alpha_2)^*$. Oczywiście $F(\alpha_1, \alpha_2) = F(\alpha)$ i skoro $|F(\alpha_1, \alpha_2)| = p^n - 1$, więc $\alpha^{p^n-1} = 1$. Tym samym α jest pierwiastkiem wielomianu $f(x) = x^{p^n-1} - 1 \in F[x]$. Bez trudu sprawdzamy, że $NWD(f, f') \sim 1$, a więc f nie ma pierwiastków wielokrotnych, czyli α jest rozdzielczy.

Założmy, teraz, że $|F| = \infty$. Niech $f \in F[x]$ będzie wielomianem minimalnym α_1 , zaś $g \in F[x]$ wielomianem minimalnym α_2 . Ponieważ α_1, α_2 są rozdzielcze, więc f i g nie mają pierwiastków wielokrotnych. Niech $\alpha_1, a_1, \dots, a_n \in L$ będą pierwiastkami f , a $\alpha_2, b_2, \dots, b_m \in L$ pierwiastkami g . Ponieważ $|F| = \infty$, więc istnieje element $\delta \in F$ taki, że

$$\alpha_1 + \delta\alpha_2 \neq a_i + \delta b_j, \text{ dla } i \in \{2, \dots, n\}, j \in \{2, \dots, m\},$$

czyli taki, że

$$\delta \neq \frac{a_i - \alpha_1}{\alpha_2 - b_j}, \text{ dla } i \in \{2, \dots, n\}, j \in \{2, \dots, m\}.$$

Pokażemy, że $F(\alpha_1, \alpha_2) = F(\alpha_1 + \delta\alpha_2)$. Oczywiście $F(\alpha_1, \alpha_2) \supset F(\alpha_1 + \delta\alpha_2)$, ponieważ $\alpha_1 + \delta\alpha_2 \in F(\alpha_1, \alpha_2)$. Niech $h(x) = f(\alpha_1 + \delta\alpha_2 - \delta x) \in F(\alpha_1 + \delta\alpha_2)[x]$. Oczywiście $h(\alpha_2) = f(\alpha_1) = 0$. Ponadto $h(b_j) \neq 0$ dla $j \in \{2, \dots, m\}$; istotnie, gdyby $h(b_j) = 0$, dla pewnego $j \in \{2, \dots, m\}$, to $f(\alpha_1 + \delta\alpha_2 - \delta b_j) = h(b_j) = 0$, czyli $\alpha_1 + \delta\alpha_2 - \delta b_j = a_i$ dla pewnego $i \in \{2, \dots, n\}$, ale wtedy $\alpha_1 + \delta\alpha_2 = a_i + \delta b_j$, co jest sprzecznością. Zatem α_2 jest jedynym wspólnym pierwiastkiem h i g . Wobec tego $NWD(g(x), h(x)) \sim x - \alpha_2$. Ponieważ $g(x), h(x) \in F(\alpha_1 + \delta\alpha_2)[x]$, więc $x - \alpha_2 \in F(\alpha_1 + \delta\alpha_2)[x]$, skąd w szczególności $\alpha_2 \in F(\alpha_1 + \delta\alpha_2)$. Ponadto $\alpha_1 = \alpha_1 + \delta\alpha_2 - \delta\alpha_2 \in F(\alpha_1 + \delta\alpha_2)$, czyli $F(\alpha_1, \alpha_2) \subset F(\alpha_1 + \delta\alpha_2)$.

Pozostaje wykazać, że $\alpha_1 + \delta\alpha_2$ jest rozdzielczy nad F . Oczywiście $\alpha_1 + \delta\alpha_2$ jest algebraiczny. Jeżeli $\text{char} F = 0$, to teza wynika z Twierdzenia 12.9. Załóżmy więc, że $\text{char} F = p$. Wobec Twierdzenia 12.10 $F(\alpha_1) = F(\alpha_1^p)$ oraz $F(\alpha_2) = F(\alpha_2^p)$. Tym samym $F(\alpha_1, \alpha_2) = F(\alpha_1^p, \alpha_2^p)$. Ponieważ $\alpha_1 \in F(\alpha_1 + \delta\alpha_2)$, więc

$$\alpha_1 = d_0 + d_1(\alpha_1 + \delta\alpha_2) + \dots + d_r(\alpha_1 + \delta\alpha_2)^r,$$

dla pewnych $d_0, d_1, \dots, d_r \in F$. Stąd

$$\alpha_1^p = d_0^p + d_1^p(\alpha_1 + \delta\alpha_2)^p + \dots + d_r^p(\alpha_1 + \delta\alpha_2)^{rp} \in F(\alpha_1 + \delta\alpha_2).$$

Analogicznie $\alpha_2^p \in F(\alpha_1 + \delta\alpha_2)$. Zatem $F(\alpha_1 + \delta\alpha_2) = F(\alpha_1, \alpha_2) = F(\alpha_1^p, \alpha_2^p) \subset F((\alpha_1 + \delta\alpha_2)^p)$. Ponadto $F((\alpha_1 + \delta\alpha_2)^p) \subset F(\alpha_1 + \delta\alpha_2)$, więc wobec Twierdzenia 12.10 element $\alpha_1 + \delta\alpha_2$ jest rozdzielczy. Dowód dla wyższych n prowadzimy analogicznie. $\square$

Wniosek 12.6. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F , niech $\alpha_1, \dots, \alpha_n \in L$ będą algebraiczne. Jeżeli $\text{char} F = 0$, to istnieje taki element algebraiczny $\alpha \in L$, że $F(\alpha) = F(\alpha_1, \dots, \alpha_n)$.

Wniosek 12.7. Niech F będzie ciałem, niech L będzie rozszerzeniem rozdzielczym i skończonym ciała F . Wówczas istnieje taki element $\alpha \in L$, że $L = F(\alpha)$.

Uwaga 12.3. Niech F będzie ciałem, niech $L = F(\alpha)$ będzie rozszerzeniem algebraicznym ciała F . Wówczas jest to rozszerzenie skończone.

Powyższa uwaga oznacza, że rozszerzenie pojedyncze i algebraiczne jest skończone oraz, na odwrót, rozszerzenie skończone i rozdzielcze jest pojedyncze.

Wniosek 12.8. Niech F będzie ciałem, niech L będzie rozszerzeniem skończonym ciała F . Jeżeli $\text{char} F = 0$, to istnieje taki element $\alpha \in L$, że $L = F(\alpha)$.

Powyższy wniosek oznacza, że w zakresie ciał o charakterystyce zero rozszerzenia algebraiczne skończone i algebraiczne pojedyncze to to samo.

Uwaga 12.4. Niech F będzie ciałem, niech L będzie rozszerzeniem algebraicznym ciała F . Zbiór

$$F_S(L) = \{a \in L : a \text{ jest rozdzielczy}\}$$

jest ciałem i $F_S(L)$ jest rozszerzeniem rozdzielczym ciała F .

Dowód. Ustalmy $a, b \in F_S(L)$. Wobec Twierdzenia 12.11, $F(a, b) \subset F_S(L)$. Wobec tego $a+b, ab, -a, a^{-1} \in F_S(L)$. $\square$

Wniosek 12.9. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F . Niech ponadto rozszerzenia $F \subset L_1 \subset L$ oraz $F \subset L_2 \subset L$ będą rozdzielcze. Wówczas rozszerzenie $L_1 L_2$ ciała F jest rozdzielcze.

Dowód. Wobec powyższej uwagi, $L_1, L_2 \subset F_S(L)$. W szczególności $L_1 L_2 \subset F_S(L)$. $\square$

Definicja 12.7. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F . Ciało $F_S(L)$ nazywamy **domknięciem rozdzielczym ciała F w L** , a ciało $F_S(\bar{F})$ **domknięciem rozdzielczym ciała F** .

Twierdzenie 12.13. Niech F będzie ciałem, niech L będzie rozszerzeniem rozdzielczym ciała F , a M rozszerzeniem rozdzielczym ciała L . Wówczas M jest rozszerzeniem rozdzielczym ciała F .

Dowód. Teza wynika z Twierdzenia 12.11 w przypadku, gdy $\text{char} F = 0$. Załóżmy, że $\text{char} F = p$ i ustalmy $a \in M$. Wobec Twierdzenia 11.11 a jest algebraiczny nad F . Wobec Wniosku 12.5 istnieje $n \in \mathbb{N}$ takie, że a^{p^n} jest rozdzielczy. Pokażemy, że rozszerzenie $F \subset L(a^{p^n})$ jest rozdzielcze.

Oczywiście rozszerzenie $F \subset L(a^{p^n})$ jest algebraiczne. Ustalmy $b \in L(a^{p^n})$. Wówczas $b = b_0 + b_1 a^{p^n} + \dots + b_m a^{p^{nm}}$, dla pewnych $b_0, \dots, b_m \in L$. Ponieważ elementy $b_0, \dots, b_m, a^{p^n}$ są rozdzielcze, są elementami ciała $F_S(M)$, więc w szczególności b jest rozdzielczy.

Ponieważ $a, a^p, a^{p^2}, \dots, a^{p^n}$ są rozdzielcze nad L , więc wobec Twierdzenia 12.10:

$$L(a) = L(a^p), L(a^p) = L(a^{p^2}), \dots, L(a^{p^{n-1}}) = L(a^{p^n}).$$

Zatem $L(a) = L(a^{p^n})$, skąd $L(a) = L(a^{p^n}) \supset F$ jest rozdzielcze. Zatem a jest rozdzielczy. $\square$

12.5. Rozszerzenia normalne.

Twierdzenie 12.14. Niech F będzie ciałem, niech L będzie rozszerzeniem algebraicznym ciała F . Następujące warunki są równoważne:

(1) istnieje rodzina wielomianów $\mathcal{F} \subset F[x]$ taka, że $L = F(A)$, gdzie

$$A = \{a \in \bar{F} : \exists f \in \mathcal{F}[f(a) = 0]\};$$

(2) jeżeli wielomian nierozkładalny $g \in F[x]$ ma pierwiastek w ciele L , to g rozkłada się w $L[x]$ na czynniki liniowe;

(3) jeżeli $\alpha \in L$ oraz $\phi : F(\alpha) \rightarrow \bar{F}$ jest F -włożeniem, to $\phi(F(\alpha)) \subset L$;

(4) jeżeli $F \subset M \subset L$ i $\phi : M \rightarrow \bar{F}$ jest F -włożeniem, to $\phi(M) \subset L$;

(5) jeżeli $\phi : L \rightarrow \bar{F}$ jest F -włożeniem, to $\phi(L) = L$.

Dowód. (1) $\Rightarrow$ (5) : Załóżmy, że $\mathcal{F} \subset F[x]$, $A = \{a \in \bar{F} : \exists f \in \mathcal{F}[f(a) = 0]\}$, $L = F(A)$. Ustalmy $f \in \mathcal{F}$ i niech $a \in A$ będzie pierwiastkiem wielomianu f . Ustalmy F -włożenie $\phi : L \rightarrow \bar{F}$. Ponieważ $f(a) = 0$, więc $0\phi(f(a)) = f(\phi(a))$, a zatem $\phi(a) \in A$. Stąd $\phi(A) = A$, więc $\phi(L) = \phi(F(A)) = F(\phi(A)) = F(A) = L$.

(5) $\Rightarrow$ (4) : Ustalmy $F \subset M \subset L$ oraz F -włożenie $\phi : M \rightarrow \bar{F}$. Wobec Lematu 12.1 istnieje przedłużenie $\psi : L \rightarrow \bar{F}$ włożenia ϕ . Wówczas $\psi(L) = L$ i skoro $\phi(M) \subset \psi(L)$, więc $\phi(M) \subset L$.

(4) $\Rightarrow$ (3) : oczywiste.

(3) $\Rightarrow$ (2) : Ustalmy wielomian nierozkładalny $g \in F[x]$. Niech $\alpha_1 \in L$ oraz $\alpha_2 \in \overline{F}$ będą pierwiastkami g . Oczywiście $F \subset F(\alpha_1) \subset L$. Wobec Twierdzenia 10.2 istnieje F -izomorfizm $\phi : F(\alpha_1) \rightarrow F(\alpha_2)$. Wówczas $\phi(F(\alpha_1)) = F(\alpha_2) \subset L$, a zatem $\alpha_2 \in L$. Wobec dowolności wyboru α_2 otrzymujemy tezę.

(2) $\Rightarrow$ (1) : Dla $a \in L$ niech $g_a \in F[x]$ będzie wielomianem minimalnym a . Ponieważ wszystkie pierwiastki g_a należą do L , więc ciało rozkładu wielomianu g_a zawarte jest w L dla $a \in L$. Jeżeli więc $\mathcal{F} = \{g_a \in F[x] : a \in L\}$ i $A = \{a \in \overline{F} : \exists g \in \mathcal{F}[g(a) = 0]\}$, to $L = F(A)$. $\square$

Definicja 12.8. Niech F będzie ciałem, niech L będzie rozszerzeniem algebraicznym ciała F . Jeżeli spełniony jest jeden z równoważnych warunków poprzedniego twierdzenia, to rozszerzenie to nazywamy **normalnym**.

Uwaga 12.5. Niech F będzie ciałem, niech L będzie rozszerzeniem skończonym ciała F . Wówczas

$F \subset L$ jest normalne wtedy i tylko wtedy, gdy L jest ciałem rozkładu pewnego wielomianu $f \in F[x]$.

Dowód. ($\Leftarrow$) : oczywiste. ($\Rightarrow$) : Załóżmy, że $\mathcal{F} \subset F[x]$, $A = \{a \in \overline{F} : \exists f \in \mathcal{F}[f(a) = 0]\}$, $L = F(A)$. Ponieważ rozszerzenie $F \subset L$ jest skończone, więc istnieją elementy $a_1, \dots, a_n \in A$ takie, że $L = F(a_1, \dots, a_n)$. Niech $f_i \in F[x]$ będzie wielomianem minimalnym elementu a_i dla $i \in \{1, \dots, n\}$. Niech $f = f_1 \cdot \dots \cdot f_n \in F[x]$ i niech M będzie ciałem rozkładu f . Wówczas ciało rozkładu każdego z f_i jest zawarte w M , więc $M \subset L$. Ponadto, skoro $L = F(a_1, \dots, a_n)$, to $L \subset M$. Zatem $L = M$. $\square$

Twierdzenie 12.15. Niech F będzie ciałem, niech M będzie rozszerzeniem algebraicznym ciała F . Wówczas istnieje rozszerzenie L ciała M takie, że rozszerzenie $F \subset L$ jest normalne.

Dowód. Dla $a \in M$ niech $f_a \in F[x]$ oznacza wielomian minimalny elementu a . Kładąc $\mathcal{F} = \{f_a \in F[x] : a \in M\}$, $A = \{a \in \overline{F} : \exists f \in \mathcal{F}[f(a) = 0]\}$ i $L = F(A)$ otrzymujemy tezę. $\square$

Twierdzenie 12.16. Niech F będzie ciałem, niech $\{L_i : i \in I\}$ będzie rodziną rozszerzeń normalnych ciała F . Wówczas rozszerzenie $F \subset \bigcap_{i \in I} L_i$ jest normalne.

Dowód. Ustalmy wielomian nierozkładalny $f \in F[x]$ i niech $\alpha \in \bigcap_{i \in I} L_i$ będzie pierwiastkiem wielomianu f . Wówczas $\alpha \in L_i$ dla $i \in I$. Ponieważ $L_i \supset F$ są rozszerzeniami normalnymi, $i \in I$, więc wszystkie pierwiastki f należą do L_i dla $i \in I$. Zatem wszystkie pierwiastki f należą do $\bigcap_{i \in I} L_i$, skąd $F \subset \bigcap_{i \in I} L_i$ jest normalne. $\square$

Definicja 12.9. Niech F będzie ciałem, niech M będzie rozszerzeniem algebraicznym ciała F . Najmniejsze (w sensie inkluzji) rozszerzenie L ciała M takie, że $F \subset L$ jest normalne nazywamy **domknięciem normalnym** rozszerzenia $F \subset M$.

Uwaga 12.6. Niech F będzie ciałem.

- (1) Jeżeli rozszerzenie $F \subset M$ jest skończone oraz $F \subset M \subset L$ jest jego domknięciem normalnym, to rozszerzenie $F \subset L$ jest skończone.
- (2) Jeżeli rozszerzenie $F \subset M$ jest rozdzielcze oraz $F \subset M \subset L$ jest jego domknięciem normalnym, to rozszerzenie $F \subset L$ jest rozdzielcze.

Dowód. (1) Załóżmy, że rozszerzenie $F \subset M$ jest skończone. Wówczas $M = F(a_1, \dots, a_n)$, gdzie $a_1, \dots, a_n$ jest bazą rozszerzenia $F \subset M$. Niech $f_i \in F[x]$ będzie wielomianem minimalnym elementu a_i dla $i \in \{1, \dots, n\}$. Niech $f = f_1 \cdot \dots \cdot f_n \in F[x]$ i niech M będzie ciałem rozkładu f . Wówczas $L \supset M$ oraz $M \supset F$ jest normalne.

- (2) Załóżmy, że $F \subset M$ jest rozdzielcze. Niech L będzie rozszerzeniem normalnym ciała F zawierającym M . Rozważmy ciało $F \subset F_S(L) \subset L$. Wówczas oczywiście $M \subset F_S(L)$. Ustalmy wielomian nierozkładalny $f \in F[x]$ i niech $\alpha \in F_S(L)$ będzie pierwiastkiem f . Ponieważ rozszerzenie $F \subset L$ jest normalne i $\alpha \in L$, więc wszystkie pierwiastki f należą do L . Ponieważ α jest rozdzielczy, więc każdy pierwiastek f jest rozdzielczy. Zatem każdy pierwiastek f należy do $F_S(L)$, a więc $F_S(L)$ jest normalne. □

Uwaga 12.7. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F . Niech rozszerzenia $F \subset L_1 \subset L$ i $F \subset L_2 \subset L$ będą normalne. Wówczas rozszerzenie $F \subset L_1 L_2$ jest normalne.

Dowód. Załóżmy, że $\mathcal{F}_1 \subset F[x]$, $A_1 = \{a \in \overline{F} : \exists f \in \mathcal{F}_1[f(a) = 0]\}$, $L_1 = F(A_1)$ oraz $\mathcal{F}_2 \subset F[x]$, $A_2 = \{a \in \overline{F} : \exists f \in \mathcal{F}_2[f(a) = 0]\}$, $L_2 = F(A_2)$. Wówczas $L_1 L_2 = F(A_1 \cup A_2)$ i $A_1 \cup A_2$ jest zbiorem wszystkich pierwiastków wielomianów należących do rodziny $\mathcal{F}_1 \cup \mathcal{F}_2$. □

Uwaga 12.8. Niech F będzie ciałem, niech L będzie rozszerzeniem normalnym ciała F , zaś M dowolnym rozszerzeniem ciała F . Wówczas rozszerzenie $FM \subset LM$ jest normalne.

Dowód. Załóżmy, że $\mathcal{F} \subset F[x]$, $A = \{a \in \overline{F} : \exists f \in \mathcal{F}[f(a) = 0]\}$, $L = F(A)$. Wówczas $\mathcal{F} \subset FM[x]$ oraz $LM = FM(A)$, a zatem $FM \subset LM$ jest rozszerzeniem normalnym. □

Twierdzenie 12.17. Niech F będzie ciałem, niech $F \subset M \subset L$ i niech $F \subset L$ będzie rozszerzeniem normalnym. Wówczas rozszerzenie $M \subset L$ jest normalne.

Dowód. Wynika z Uwagi 12.8 dla $FM = M$ oraz $LM = L$. □

Przykład:

- (1) Twierdzenie o wieży ciał nie jest prawdziwe dla rozszerzeń normalnych: rozszerzenie $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ jest normalne i rozszerzenie $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ jest normalne, ale rozszerzenie $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ nie jest normalne.