

15. WYKŁAD 15: ROZSZERZENIA PIERWIASTNIKOWE. ELEMENTY WYRAŻAJĄCE SIĘ PRZEZ PIERWIASTNIKI. ROZWIĄZALNOŚĆ RÓWNAŃ PRZEZ PIERWIASTNIKI. RÓWNIANIA O DOWOLNYCH WSPÓŁCZYNNIKACH.

15.1. Rozszerzenia pierwiastnikowe. Elementy wyrażające się przez pierwiastniki.

Definicja 15.1. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F .

- (1) Rozszerzenie $F \subset L$ nazywamy **pierwiastnikowym**, gdy istnieją ciała $F = M_0 \subset M_1 \subset \dots \subset M_r = L$ takie, że $M_{i+1} = M_i(a_i)$, $i \in \{0, \dots, r-1\}$ oraz
- gdy $\text{char} F = 0$, to a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in M_i[x]$,
 - gdy $\text{char} F = p$, to a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in M_i[x]$, gdzie $p \nmid n_i$, lub a_i jest pierwiastkiem wielomianu $x^p - x - b_i \in M_i[x]$.

O elemencie ciała $\bar{F}$ mówimy, że **wyraża się przez pierwiastniki**, gdy należy do pewnego rozszerzenia pierwiastnikowego ciała F . Zbiór elementów wyrażających się przez pierwiastniki oznaczamy $r(F)$.

- (2) Rozszerzenie $F \subset L$ nazywamy **rozszerzeniem przez dołączenie pierwiastków stopnia nie większego niż n** , gdy istnieją ciała $F = M_0 \subset M_1 \subset \dots \subset M_r = L$ takie, że $M_{i+1} = M_i(a_i)$, $i \in \{0, \dots, r-1\}$ oraz
- gdy $\text{char} F = 0$, to a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in M_i[x]$, gdzie $n_i \leq n$,
 - gdy $\text{char} F = p$, to a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in M_i[x]$, gdzie $n_i \leq n$ i $p \nmid n_i$, lub a_i jest pierwiastkiem wielomianu $x^p - x - b_i \in M_i[x]$.

O elemencie ciała $\bar{F}$ mówimy, że **wyraża się przez pierwiastniki stopnia nie większego niż n** , gdy należy do pewnego rozszerzenia przez dołączenie pierwiastków stopnia nie większego niż n ciała F . Zbiór elementów wyrażających się przez pierwiastniki stopnia nie większego niż n oznaczamy $r_n(F)$. W szczególności, gdy $n = 2$ i $\text{char} F \neq 2$, to rozszerzenie $F \subset L$ nazywamy **rozszerzeniem przez dołączenie pierwiastków kwadratowych**, gdy istnieją ciała $F = M_0 \subset M_1 \subset \dots \subset M_r = L$ takie, że $M_{i+1} = M_i(a_i)$, $i \in \{0, \dots, r-1\}$ oraz a_i jest pierwiastkiem wielomianu $x^2 - b_i \in M_i[x]$ (gdyż każde rozszerzenie kwadratowe jest ciałem rozkładu wielomianu tej postaci). O elemencie ciała $\bar{F}$ mówimy, że **wyraża się przez pierwiastniki kwadratowe**, gdy należy do pewnego rozszerzenia przez dołączenie pierwiastków kwadratowych ciała F .

- (3) Rozszerzenie $F \subset L$ nazywamy **rozszerzeniem przez dołączenie pierwiastków stopni względnie pierwszych z charakterystyką**, gdy istnieją ciała $F = M_0 \subset M_1 \subset \dots \subset M_r = L$ takie, że $M_{i+1} = M_i(a_i)$, $i \in \{0, \dots, r-1\}$ oraz a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in M_i[x]$, gdzie $p \nmid n_i$, przy czym $\text{char} F = p \neq 0$. O elemencie ciała $\bar{F}$ mówimy, że **wyraża się przez pierwiastniki stopni względnie pierwszych z charakterystyką**, gdy należy do pewnego rozszerzenia przez dołączenie pierwiastków stopni względnie pierwszych z charakterystyką ciała F . Zbiór elementów wyrażających się przez pierwiastniki stopni względnie pierwszych z charakterystyką oznaczamy $r_p^*(F)$.
- (4) Jeżeli F jest podciałem ciała $\mathbb{R}$, to rozszerzenie $F \subset L$ nazywamy **rozszerzeniem przez dołączenie pierwiastków rzeczywistych**, gdy istnieją ciała $F = M_0 \subset M_1 \subset \dots \subset M_r = L$ takie, że $M_{i+1} = M_i(a_i)$, $i \in \{0, \dots, r-1\}$ oraz a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in M_i[x]$, przy czym $a_i \in \mathbb{R}$. O elemencie ciała $\bar{F}$ mówimy, że **wyraża się przez pierwiastniki rzeczywiste**, gdy należy do pewnego rozszerzenia przez dołączenie pierwiastków rzeczywistych ciała F . Zbiór elementów wyrażających się przez pierwiastniki rzeczywiste oznaczamy $r_{\mathbb{R}}(F)$.

Twierdzenie 15.1. Niech F będzie ciałem, niech L będzie rozszerzeniem pierwiastnikowym ciała F , niech $F \subset L_1 \subset L$ i $F \subset L_2 \subset L$ będą rozszerzeniami pierwiastnikowymi. Wówczas:

- (1) jeżeli rozszerzenie $L \subset M$ jest pierwiastnikowe, to również rozszerzenie $F \subset M$ jest pierwiastnikowe;
- (2) jeżeli $F \subset M \subset L$, to rozszerzenie $M \subset L$ jest pierwiastnikowe;
- (3) rozszerzenie $F \subset L_1 L_2$ jest pierwiastnikowe;
- (4) jeżeli $\phi : L \rightarrow \overline{F}$ jest F -włożeniem, to rozszerzenie $F \subset \phi(L)$ jest pierwiastnikowe.

Dowód. (1) Załóżmy, że $F = F_0 \subset F_1 \subset \dots \subset F_r = L$ oraz $L = L_0 \subset L_1 \subset \dots \subset L_s = M$ są ciągami ciał spełniającymi warunki na to, aby rozszerzenia $F \subset L$ i $L \subset M$ były pierwiastnikowe. Wówczas ciąg ciał $F = F_0 \subset F_1 \subset \dots \subset F_r = L = L_0 \subset L_1 \subset \dots \subset L_s = M$ jest ciągiem ciał spełniającym warunek na to, aby rozszerzenie $F \subset M$ było pierwiastnikowe.

- (2) Załóżmy, że $F = F_0 \subset F_1 \subset \dots \subset F_r = L$ jest takim ciągiem ciał, że $F_{i+1} = F_i(a_i)$, gdzie a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in F_i[x]$, gdy $\text{char} F = 0$, lub a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in F_i[x]$, gdzie $p \nmid n_i$, lub a_i jest pierwiastkiem wielomianu $x^p - x - b_i \in F_i[x]$, gdy $\text{char} F = p$. Niech $M_i = FM_i$, $i \in \{0, \dots, r\}$. Wówczas $M = M_0 \subset M_1 \subset \dots \subset M_r = L$ oraz $M_{i+1} = MF_{i+1} = MF_i(a_i) = M_i(a_i)$, gdzie a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in F_i[x] \subset MF_i[x] = M_i[x]$, gdy $\text{char} F = 0$, lub a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in M_i[x]$, gdzie $p \nmid n_i$, lub a_i jest pierwiastkiem wielomianu $x^p - x - b_i \in M_i[x]$, gdy $\text{char} F = p$.
- (3) Załóżmy, że $F = F_0 \subset F_1 \subset \dots \subset F_r = L_1$ oraz $F = F'_0 \subset F'_1 \subset \dots \subset F'_s = L_2$ są ciągami ciał spełniającymi warunki na to, aby rozszerzenia $F \subset L_1$ i $F \subset L_2$ były pierwiastnikowe. Wówczas ciąg ciał $F = F_0 \subset F_1 \subset \dots \subset F_r = L_1 = L_1 F = L_1 F'_0 \subset L_1 F'_1 \subset \dots \subset L_1 F'_s = L_1 L_2$ jest ciągiem ciał spełniającym warunek na to, aby rozszerzenie $F \subset L_1 L_2$ było pierwiastnikowe.
- (4) Załóżmy, że $F = F_0 \subset F_1 \subset \dots \subset F_r = L$ jest takim ciągiem ciał, że $F_{i+1} = F_i(a_i)$, gdzie a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in F_i[x]$, gdy $\text{char} F = 0$, lub a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in F_i[x]$, gdzie $p \nmid n_i$, lub a_i jest pierwiastkiem wielomianu $x^p - x - b_i \in F_i[x]$, gdy $\text{char} F = p$. Niech $M_i = \phi(F_i)$, $i \in \{0, \dots, r\}$. Wówczas $F = \phi(F) = M_0 \subset M_1 \subset \dots \subset M_r = \phi(L)$ oraz $M_{i+1} = \phi(F_{i+1}) = \phi(F_i(a_i)) = \phi(F_i)(\phi(a_i)) = M_i(\phi(a_i))$, gdzie $\phi(a_i)$ jest pierwiastkiem wielomianu $x^{n_i} - \phi(b_i) \in M_i[x]$, gdy $\text{char} F = 0$, lub pierwiastkiem wielomianu $x^{n_i} - \phi(b_i) \in M_i[x]$, gdzie $p \nmid n_i$, lub pierwiastkiem wielomianu $x^p - x - \phi(b_i) \in M_i[x]$, gdy $\text{char} F = p$.

□

Przykład:

- (1) Rozważmy ciała $\mathbb{Q} \subset \mathbb{Q}(\cos \frac{2}{7}\pi) \subset \mathbb{Q}(\xi_0)$, gdzie $\xi_0 = \cos \frac{2}{7}\pi + i \sin \frac{2}{7}\pi$. Wówczas rozszerzenie $\mathbb{Q} \subset \mathbb{Q}(\xi_0)$ jest pierwiastnikowe, ale rozszerzenie $\mathbb{Q} \subset \mathbb{Q}(\cos \frac{2}{7}\pi)$ nie jest. Istotnie, ξ_0 jest pierwiastkiem wielomianu $x^7 - 1 \in \mathbb{Q}[x]$, więc rozszerzenie $\mathbb{Q} \subset \mathbb{Q}(\xi_0)$ jest pierwiastnikowe. Przypuśćmy, że rozszerzenie $\mathbb{Q} \subset \mathbb{Q}(\cos \frac{2}{7}\pi)$ też jest pierwiastnikowe. ξ_0 jest pierwiastkiem wielomianu $\frac{x^7-1}{x-1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$. Wobec przykładu po Uwadze 9.3 wielomian ten jest nierozkładalny, a więc $[\mathbb{Q}(\xi_0) : \mathbb{Q}] = 6$. Rozszerzenie $\mathbb{Q} \subset \mathbb{Q}(\xi_0)$ jest abelowe. Jediną grupą abelową rzędu 6 jest $\mathbb{Z}_6$, a zatem $G(\mathbb{Q}(\xi_0)/\mathbb{Q}) = \mathbb{Z}_6$. Niech $\sigma \in G(\mathbb{Q}(\xi_0)/\mathbb{Q})$ będzie taki, że $\sigma(\xi_0) = \xi_0^3$. Bez trudu sprawdzamy, że $r(\sigma) = 6$, a więc $G(\mathbb{Q}(\xi_0)/\mathbb{Q}) = \langle \sigma \rangle$. Zauważmy, że $2 \cos \frac{2}{7}\pi = \xi_0 + \overline{\xi_0} = \xi_0 + \xi_0^6$ oraz że jedynie σ^3 oraz σ^0 są stałe na $\xi_0 + \xi_0^6$. Zatem $G(\mathbb{Q}(\xi_0)/\mathbb{Q}(\cos \frac{2}{7}\pi)) = \{id, \sigma^3\}$, skąd $|G(\mathbb{Q}(\cos \frac{2}{7}\pi)/\mathbb{Q})| = 3$, a więc rozszerzenie $\mathbb{Q} \subset \mathbb{Q}(\cos \frac{2}{7}\pi)$ jest cykliczne stopnia 3. Ponieważ każdemu podciału pośredniemu odpowiada podgrupa grupy $G(\mathbb{Q}(\cos \frac{2}{7}\pi)/\mathbb{Q})$, a jej rząd jest liczbą pierwszą, więc $\mathbb{Q} = F_0 \subset F_1 = \mathbb{Q}(\cos \frac{2}{7}\pi)$ jest jedynym możliwym ciągiem takim, że $F_1 = F_0(a)$ oraz a jest pierwiastkiem wielomianu $x^n - b \in \mathbb{Q}[x]$. Niech $G(\mathbb{Q}(\cos \frac{2}{7}\pi)/\mathbb{Q}) = \langle \tau \rangle$. Wówczas $\tau(a)$ jest również pierwiastkiem wielomianu $x^n - b \in \mathbb{Q}[x]$. Zatem $\tau(a) = a\xi_n^s$, gdzie $s \in \mathbb{N}$ oraz ξ_n jest pierwiastkiem pierwotnym stopnia n . Zatem $\xi_n^s \in \mathbb{Q}(\cos \frac{2}{7}\pi)$. Ponieważ $\mathbb{Q}(\cos \frac{2}{7}\pi) \subset \mathbb{R}$, więc

$\xi_n^s \in \{\pm 1\}$. Zatem $\tau(a) = \pm a$ oraz $\tau^2(a) = \pm(\pm a) = a$, a więc τ^2 jest tożsamością na $\mathbb{Q}(\cos \frac{2}{7}\pi)$, co daje sprzeczność z tym, że $r(\tau) = 3$.

Twierdzenie 15.2. *Niech F będzie ciałem, niech L będzie rozszerzeniem przez dołączenie pierwiastków stopnia nie większego niż n lub pierwiastków stopni względnie pierwszych z charakterystyką ciała F , niech $F \subset L_1 \subset L$ i $F \subset L_2 \subset L$ będą rozszerzeniami przez dołączenie pierwiastków stopnia nie większego niż n lub pierwiastków stopni względnie pierwszych z charakterystyką. Wówczas:*

- (1) *jeżeli rozszerzenie $L \subset M$ jest rozszerzeniem przez dołączenie pierwiastków stopnia nie większego niż n lub pierwiastków stopni względnie pierwszych z charakterystyką, to również rozszerzenie $F \subset M$ jest rozszerzeniem przez dołączenie pierwiastków stopnia nie większego niż n lub pierwiastków stopni względnie pierwszych z charakterystyką, odpowiednio;*
- (2) *jeżeli $F \subset M \subset L$, to rozszerzenie $M \subset L$ jest rozszerzeniem przez dołączenie pierwiastków stopnia nie większego niż n lub pierwiastków stopni względnie pierwszych z charakterystyką;*
- (3) *rozszerzenie $F \subset L_1 L_2$ jest rozszerzeniem przez dołączenie pierwiastków stopnia nie większego niż n lub pierwiastków stopni względnie pierwszych z charakterystyką;*
- (4) *jeżeli $\phi : L \rightarrow \bar{F}$ jest F -włożeniem, to rozszerzenie $F \subset \phi(L)$ jest rozszerzeniem przez dołączenie pierwiastków stopnia nie większego niż n lub pierwiastków stopni względnie pierwszych z charakterystyką.*

Dowód pozostawiamy jako ćwiczenie.

Twierdzenie 15.3. *Niech F będzie ciałem, niech L będzie rozszerzeniem przez dołączenie pierwiastków rzeczywistych ciała F , niech $F \subset L_1 \subset L$ i $F \subset L_2 \subset L$ będą rozszerzeniami przez dołączenie pierwiastków rzeczywistych. Wówczas:*

- (1) *jeżeli rozszerzenie $L \subset M$ jest rozszerzeniem przez dołączenie pierwiastków rzeczywistych, to również rozszerzenie $F \subset M$ jest rozszerzeniem przez dołączenie pierwiastków rzeczywistych;*
- (2) *jeżeli $F \subset M \subset L$, to rozszerzenie $M \subset L$ jest rozszerzeniem przez dołączenie pierwiastków rzeczywistych;*
- (3) *rozszerzenie $F \subset L_1 L_2$ jest rozszerzeniem przez dołączenie pierwiastków rzeczywistych.*

Dowód pozostawiamy jako ćwiczenie.

Twierdzenie 15.4. *Niech F będzie ciałem, niech L będzie rozszerzeniem pierwiastnikowym i rozdzielczym ciała F . Wówczas istnieje rozszerzenie $L \subset M$ takie, że $F \subset M$ jest pierwiastnikowe i Galois.*

Dowód. Wobec twierdzenia Abela o elemencie pierwotnym $L = F(b)$ dla pewnego elementu $b \in L$. Niech $f \in F[x]$ będzie wielomianem minimalnym elementu b , niech $b = b_1, b_2, \dots, b_n$ będą wszystkimi pierwiastkami f . Wobec Twierdzenia 14.1 istnieją F -izomorfizmy $\tau_j : F(b) \rightarrow F(b_j)$ takie, że $\tau_j(b) = b_j$. Z kolei wobec Twierdzenia 15.1 (4) rozszerzenia $F \subset F(b_j)$ są pierwiastnikowe, a więc i rozszerzenie $F \subset F(b_1) \dots F(b_n) = F(b_1, \dots, b_n) = M$ jest pierwiastnikowe. Jako ciało rozkładu wielomianu rozdzielczego jest to rozszerzenie Galois. Oczywiście $L \subset M$. $\square$

Twierdzenie 15.5. *Niech F będzie ciałem, niech L będzie rozdzielczym rozszerzeniem przez dołączenie pierwiastków stopnia nie większego niż n lub pierwiastków stopni względnie pierwszych z charakterystyką ciała F . Wówczas istnieje rozszerzenie $L \subset M$ takie, że $F \subset M$ jest rozszerzeniem Galois przez dołączenie pierwiastków stopnia nie większego niż n lub pierwiastków stopni względnie pierwszych z charakterystyką, odpowiednio.*

Dowód pozostawiamy jako ćwiczenie.

Twierdzenie 15.6. *Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F . Wówczas:*

- (1) $r(F)$, $r_n(F)$, $r_{p^*}(F)$ i $r_{\mathbb{R}}(F)$ są ciałami;
- (2) $r(F) = r(r(F))$, $r_n(F) = r_n(r_n(F))$, $r_{p^*}(F) = r_{p^*}(r_{p^*}(F))$ i $r_{\mathbb{R}}(F) = r_{\mathbb{R}}(r_{\mathbb{R}}(F))$;
- (3) jeśli $\phi : \overline{F} \rightarrow \overline{F}$ jest F -izomorfizmem, to $\phi(r(F)) = r(F)$, $\phi(r_n(F)) = r_n(F)$, $\phi(r_{p^*}(F)) = r_{p^*}(F)$ i $\phi(r_{\mathbb{R}}(F)) = r_{\mathbb{R}}(F)$.

Dowód. (1) Ustalmy $a, b \in r(F)$, $b \neq 0$. Niech L_1 i L_2 będą takimi rozszerzeniami pierwiastnikowymi, że $a \in L_1$, $b \in L_2$. Wobec Twierdzenia 15.1 (3) rozszerzenie $F \subset L_1 L_2$ jest pierwiastnikowe, a więc $L_1 L_2 \subset r(F)$. Oczywiście $a \pm b, ab, \frac{a}{b} \in L_1 L_2 \subset r(F)$. Analogicznie pokazujemy, że $r_n(F)$, $r_{p^*}(F)$ i $r_{\mathbb{R}}(F)$ są ciałami.

- (2) Niech $x^n - a \in r(F)[x]$, gdzie $p \nmid n$ oraz $\text{char } F = p$. Pokażemy, że w $r(F)[x]$ wielomian $x^n - a$ rozkłada się na czynniki liniowe. Istotnie, ponieważ $a \in r(F)$, więc istnieje rozszerzenie pierwiastnikowe L takie, że $a \in L$. Niech b będzie dowolnym pierwiastkiem $x^n - a$. Oczywiście $L \subset L(b)$ jest pierwiastnikowe. Wobec Twierdzenia 15.1 (1) rozszerzenie $F \subset L(b)$ jest pierwiastnikowe, a zatem $b \in r(F)$. W podobny sposób pokazujemy, że w $r(F)[x]$ wielomian $x^p - x - a$ rozkłada się na czynniki liniowe.

Wobec tego każdy element pierwiastnikowy względem $r(F)$ należy do $r(F)$, czyli $r(r(F)) \subset r(F)$. Oczywiście też $r(F) \subset r(r(F))$. Podobnie dowodzimy, że $r_n(F) = r_n(r_n(F))$, $r_{p^*}(F) = r_{p^*}(r_{p^*}(F))$ i $r_{\mathbb{R}}(F) = r_{\mathbb{R}}(r_{\mathbb{R}}(F))$.

- (3) Pokażemy, że $\phi(r(F)) \subset r(F)$. Ustalmy w tym celu $a \in r(F)$. Niech $F \subset L$ będzie pierwiastnikowe i niech $a \in L$. Wówczas $\phi(a) \in \phi(L)$ i wobec Twierdzenia 15.1 (4) $\phi(a)$ wyraża się przez pierwiastniki względem F . Zatem $\phi(a) \in r(F)$.

Rozumując analogicznie dla ϕ^{-1} pokazujemy, że $r(F) \subset \phi(r(F))$. Podobnie dowodzimy, że $\phi(r_n(F)) = r_n(F)$, $\phi(r_{p^*}(F)) = r_{p^*}(F)$ i $\phi(r_{\mathbb{R}}(F)) = r_{\mathbb{R}}(F)$. □

Definicja 15.2. *Niech F będzie ciałem. Ciało $r(F)$ nazywamy **domknięciem pierwiastnikowym** ciała F .*

Twierdzenie 15.7. *Niech F będzie ciałem, niech $F \subset L \subset M$. Wówczas:*

- (1) $r(F) \subset r(L)$, $r_n(F) \subset r_n(L)$, $r_{p^*}(F) \subset r_{p^*}(L)$ i $r_{\mathbb{R}}(F) \subset r_{\mathbb{R}}(L)$;
- (2) jeśli $L \subset r(F)$ i $M \subset r(L)$, to $M \subset r(F)$; jeśli $L \subset r_n(F)$ i $M \subset r_n(L)$, to $M \subset r_n(F)$; jeśli $L \subset r_{p^*}(F)$ i $M \subset r_{p^*}(L)$, to $M \subset r_{p^*}(F)$; jeśli $L \subset r_{\mathbb{R}}(F)$ i $M \subset r_{\mathbb{R}}(L)$, to $M \subset r_{\mathbb{R}}(F)$.

Dowód. (1) oczywiste.

- (2) Wobec założeń i części (1) twierdzenia, $M \subset r(L) \subset r(r(F)) = r(F)$. Podobnie dowodzimy dla $r_n(F)$, $r_{p^*}(F)$ i $r_{\mathbb{R}}(F)$. □

Twierdzenie 15.8. *Niech F będzie ciałem, niech L będzie skończonym rozszerzeniem ciała F . Niech $L \subset r_n(F)$. Wówczas każdy dzielnik pierwszy liczby $[L : F]$ jest nie większy niż n .*

Dowód. Ustalmy $a \in r_n(F)$ i niech

$$F = F_0 \subset F_1 \subset \dots \subset F_r$$

będzie ciągiem spełniającym warunek na to, aby $a \in F_r$ i $F \subset F_r$ było rozszerzeniem przez dołączenie pierwiastków stopni nie większych niż n . W szczególności $F(a) \subset F_r$, a więc

$$[F(a) : F][F_r : F] = [F_r : F_{r-1}] \cdot \dots \cdot [F_1 : F].$$

Oczywiście $[F_i : F_{i-1}] \leq n$ dla $i \in \{1, \dots, r\}$, a zatem każdy dzielnik pierwszy liczby $[F(a) : F]$ nie przekracza n . Z dowolności a i z tego, że $L \subset r_n(F)$ wynika teza. $\square$

Wniosek 15.1. *Niech F będzie ciałem, niech L będzie skończonym rozszerzeniem ciała F . Niech $L \subset r_2(F)$. Wówczas $[L : F]$ jest potęgą liczby 2.*

Przykład:

- (2) Rozważmy $a = \sqrt[3]{3 + \sqrt{7}}$. Wówczas $a \in r(\mathbb{Q})$, $a \in r_{\mathbb{R}}(\mathbb{Q})$, ale $a \notin r_2(\mathbb{Q})$. Istotnie, $a \in r(\mathbb{Q})$ z uwagi na ciąg $\mathbb{Q} \subset \mathbb{Q}(\sqrt{7}) \subset \mathbb{Q}(a)$. Oczywiście też $a \in r_{\mathbb{R}}(\mathbb{Q})$. Niech $f(x) = x^6 - 6x^3 + 2 \in \mathbb{Q}[x]$. Wówczas $f(a) = 0$ oraz wobec kryterium Eisensteina f jest nierozkładalny. Zatem $[\mathbb{Q}(a) : \mathbb{Q}] = 6$ oraz $6 \neq 2^k$, więc $a \notin r_2(\mathbb{Q})$.

Lemat 15.1. *Niech F będzie ciałem, $\text{char} F = 0$ lub $\text{char} F = p$ i $p \nmid n$, niech L będzie rozszerzeniem cyklicznym stopnia n ciała F . Wówczas $L \subset r_n(F)$.*

Dowód. Niech ξ_j , $j \in \mathbb{N}$, oznacza pierwiastek pierwotny stopnia j z jedynki. Pokażemy, że $\xi_n \in \overline{F}$. Rozważmy w tym celu wielomian $x^n - 1 \in F[x]$. Ponieważ $p \nmid n$, więc $NWD(x^n - 1, (x^n - 1)') \sim 1$, zatem $x^n - 1$ jest rozdzielnicy. Zatem $x^n - 1$ ma n różnych pierwiastków w $\overline{F}$, w tym również ξ_n .

Wobec Wniosku 13.13 $G(L(\xi_n)/F(\xi_n)) = G(LF(\xi_n)/FF(\xi_n)) < G(L/F)$. A zatem rozszerzenie $F(\xi_n) \subset L(\xi_n)$ jest cykliczne oraz $[L(\xi_n) : F(\xi_n)] = r$, gdzie $r|n$. Niech $n = rs$. Wówczas $\xi_r = \xi_n^s \in F(\xi_n)$. Wobec twierdzenia Lagrange'a-Kummera²⁵ istnieje $b \in L(\xi_n)$ takie, że $L(\xi_n) = F(\xi_n)(b)$ oraz b jest pierwiastkiem wielomianu $x^r - a$ dla pewnego $a \in F(\xi_n)$. Stąd $F \subset F(\xi_n) \subset L(\xi_n)$ jest ciągiem ciał spełniających warunek na to, aby rozszerzenie $F \subset L(\xi_n)$ było rozszerzeniem przez dołączenie pierwiastków stopni co najwyżej n . Zatem $L(\xi_n) \subset r_n(F)$ i tym bardziej $L \subset r_n(F)$. $\square$

Lemat 15.2. *Niech F będzie ciałem, $\text{char} F = p$, niech L będzie rozszerzeniem cyklicznym stopnia p ciała F . Wówczas $L \subset r_p(F)$.*

Dowód. Wynika bezpośrednio z twierdzenia Artina-Schreiera²⁶ $\square$

Twierdzenie 15.9. *Niech F będzie ciałem, niech L będzie skończonym i rozwiązalnym rozszerzeniem ciała F . Niech ponadto n będzie największym dzielnikiem pierwszym liczby $[L : F]$. Wówczas $L \subset r_n(F)$.*

Dowód. Dowód prowadzimy poprzez indukcję względem liczby dzielników pierwszych liczby $[L : F]$. Jeżeli $[L : F] = p$, to teza wynika z Lematu 15.1, gdy $\text{char} F \neq p$, lub z Lematu 15.2, gdy $\text{char} F = p$.

²⁵**Twierdzenie** (Lagrange'a-Kummera): Niech F będzie ciałem, $\text{char} F = 0$ lub $\text{char} F = p$ i $p \nmid n$, niech L będzie rozszerzeniem ciała F . Niech ξ_0 będzie pierwiastkiem pierwotnym z jedynki stopnia n . Jeżeli $\xi_0 \in F$, to wówczas:

- (1) jeśli rozszerzenie $F \subset L$ jest cykliczne i $[L : F] = n$, to istnieje element $b \in L$ taki, że $L = F(b)$ i b jest pierwiastkiem wielomianu $x^n - a \in F[x]$, dla pewnego $a \in F$;
- (2) jeśli $a \in F$ i b jest pierwiastkiem wielomianu $x^n - a \in F[x]$, to rozszerzenie $F \subset F(b)$ jest cykliczne, $[F(b) : F] = d$, $d|n$ oraz $b^d \in F$.

Szczegółowy dowód nieznacznie przekracza ramy tego wykładu (wykorzystuje pojęcie tzw. śladu elementu i 90-te twierdzenie Hilberta) i zostanie tu pominięty.

²⁶**Twierdzenie** (Artina-Schreiera): Niech F będzie ciałem, $\text{char} F = p$, niech L będzie rozszerzeniem ciała F . Wówczas:

- (1) jeśli rozszerzenie $F \subset L$ jest cykliczne i $[L : F] = p$, to istnieje element $b \in L$ taki, że $L = F(b)$ i b jest pierwiastkiem wielomianu $x^p - x - a \in F[x]$, dla pewnego $a \in F$;
- (2) jeśli $a \in F$ i b jest pierwiastkiem wielomianu $x^p - x - a \in F[x]$ i dodatkowo $b \in F$, to wszystkie pierwiastki wielomianu $x^p - x - a$ należą do F , a jeśli $b \notin F$, to $x^p - x - a$ jest nierozkładalny w $F[x]$, rozszerzenie $F \subset F(b)$ jest cykliczne oraz $[F(b) : F] = p$.

Szczegółowy dowód nieznacznie przekracza ramy tego wykładu (wykorzystuje pojęcie tzw. śladu elementu i 90-te twierdzenie Hilberta) i zostanie tu pominięty.

Założmy, że $[L : F]$ jest iloczynem l czynników pierwszych oraz że twierdzenie jest prawdziwe dla rozszerzeń L' dla których liczba $[L' : F]$ ma mniej niż l dzielników pierwszych. Grupa rozwiązalna, której rząd nie jest liczbą pierwszą, nie jest prosta, istnieje zatem $H \triangleleft G(L/F)$ taka, że $1 < |H| < |G(L/F)|$. Niech $M = L^H$. Wówczas $F \subset M \subset L$ oraz rozszerzenia $F \subset M$ i $M \subset L$ są rozwiązalne. Ponadto $G(L/M) = H$ oraz $G(M/F) \cong G(L/F)/H$. Wobec założenia indukcyjnego $M \subset r_k(F)$ oraz $L \subset r_m(M)$, gdzie k i m są największymi dzielnikami pierwszymi liczb $[M : F] = |G(L/F)/H|$ i $[L : M] = |H|$, odpowiednio. Zatem $k, m \leq n$ i stąd $M \subset r_n(F)$ oraz $L \subset r_n(r_n(F)) = r_n(F)$. $\square$

Wniosek 15.2. Niech F będzie ciałem, niech L będzie rozszerzeniem Galois ciała F , niech $[L : F]$ będzie potęgą dwójki. Wówczas $L \subset r_2(F)$.

Dowód. Wynika bezpośrednio z Uwagi 14.3. $\square$

Twierdzenie 15.10. Niech F będzie ciałem, niech L będzie skończonym rozszerzeniem Galois ciała F . Niech $L \subset r(F)$. Wówczas grupa $G(L/F)$ jest rozwiązalna.

Dowód. Założmy, że $F = F_0 \subset F_1 \subset \dots \subset F_r = L$ jest takim ciągiem ciał, że $F_{i+1} = F_i(a_i)$, gdzie a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in F_i[x]$, gdy $\text{char} F = 0$, lub a_i jest pierwiastkiem wielomianu $x^{n_i} - b_i \in F_i[x]$, gdzie $p \nmid n_i$, lub a_i jest pierwiastkiem wielomianu $x^p - x - b_i \in F_i[x]$, gdy $\text{char} F = p$. Dowód prowadzimy przez indukcję względem liczby r . Dla $r = 0$ teza jest oczywista. Założmy więc, że $r \geq 1$ i że twierdzenie zachodzi dla rozszerzeń, dla których istnieją odpowiednie ciągi ciał o długościach $0, 1, \dots, r-1$. Ponieważ rozszerzenia $F \subset L$ i $F \subset F_1$ są Galois, więc $F \subset LF_1$ też jest Galois, a wraz z nim $F_1 \subset LF_1$ jest Galois. Ponieważ $L \subset r(F) \subset r(F_1)$, więc $LF_1 \subset r(F_1)$. Rozważmy ciąg ciał

$$F_1 \subset F_2 \subset \dots \subset F_r.$$

Oczywiście $LF_1 \subset F_r$, więc z założenia indukcyjnego rozszerzenie $F_1 \subset LF_1$ jest rozwiązalne. Dalej, wobec twierdzeń Lagrange'a-Kumera i Artina-Schreiera rozszerzenie $F \subset F_1$ jest rozwiązalne. Wobec tego rozszerzenie $F \subset LF_1$ jest rozwiązalne. Ponieważ $F \subset L \subset LF_1$, więc też $F \subset L$ jest rozwiązalne. $\square$

Wniosek 15.3. Niech F będzie ciałem, niech L będzie skończonym rozszerzeniem Galois ciała F . Niech ponadto n będzie największym dzielnikiem pierwszym liczby $[L : F]$. Wówczas następujące warunki są równoważne:

- (1) $L \subset r_n(F)$;
- (2) $L \subset r(F)$;
- (3) grupa $G(L/F)$ jest rozwiązalna.

Dowód. Implikacja (1) $\Rightarrow$ (2) jest oczywista, wynikanie (2) $\Rightarrow$ (3) jest treścią Twierdzenia 15.10, a wnioskowanie (3) $\Rightarrow$ (1) tezą Twierdzenia 15.9. $\square$

Definicja 15.3. Niech f będzie ciałem, niech $f \in F[x]$. Mówimy, że równanie $f(x) = 0$ jest **rozwiązalne przez pierwiastniki**, gdy każdy pierwiastek wielomianu f należy do $r(F)$.

Wniosek 15.4. Niech F będzie ciałem, niech $f \in F[x]$ będzie wielomianem rozdzielczym. Wówczas równanie $f(x) = 0$ jest rozwiązalne przez pierwiastniki wtedy i tylko wtedy, gdy grupa Galois wielomianu f jest rozwiązalna.

Dowód. Niech L będzie ciałem rozkładu wielomianu f . Ponieważ f jest rozdzielczy, więc rozszerzenie $F \subset L$ jest rozdzielcze, a więc Galois. Wobec Wniosku 15.3 grupa $G(L/F)$ jest rozwiązalna wtedy i tylko wtedy, gdy $L \subset r(F)$, czyli gdy wszystkie pierwiastki wielomianu f wyrażają się przez pierwiastniki. $\square$

15.2. Rozwiązalność równań przez pierwiastniki. Równania o dowolnych współczynnikach.

Lemat 15.3. Niech F będzie ciałem, niech $F \subset M$ i $F \subset L$ będą rozszerzeniami ciała F . Niech $\alpha : L \rightarrow M$ będzie izomorfizmem. Wówczas $G(L/F) \cong G(\alpha(L)/\alpha(F))$.

Dowód. Ustalmy $\phi \in G(L/F)$. Wówczas dla $a \in \alpha(F)$ istnieje $b \in F$ takie, że $a = \alpha(b)$, a zatem $\alpha \circ \phi \circ \alpha^{-1}(a) = \alpha \circ \phi \circ \alpha^{-1} \circ \alpha(b) = \alpha \circ \phi(b) = \alpha(b) = a$. Zatem $\alpha \circ \phi \circ \alpha^{-1} \in G(\alpha(L)/\alpha(F))$. Ponadto dla $\phi, \psi \in G(L/F)$ zachodzi:

$$\alpha \circ \phi \circ \psi \circ \alpha^{-1} = \alpha \circ \phi \circ \alpha^{-1} \circ \alpha \circ \psi \circ \alpha^{-1},$$

zatem odwzorowanie $\sigma : G(L/F) \rightarrow G(\alpha(L)/\alpha(F))$ dane wzorem $\sigma(\phi) = \alpha \circ \phi \circ \alpha^{-1}$ jest dobrze określonym homomorfizmem grup. Odwzorowanie $\tau : G(\alpha(L)/\alpha(F)) \rightarrow G(L/F)$ dane wzorem $\tau(\psi) = \alpha^{-1} \circ \psi \circ \alpha$ jest do niego odwrotne, tak więc σ jest izomorfizmem. $\square$

Twierdzenie 15.11. Niech F będzie ciałem, niech $a_1, \dots, a_n$ będą algebraicznie niezależne nad F , niech

$$f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in F(a_1, \dots, a_n)[x].$$

Wówczas grupa Galois wielomianu f względem ciała $F(a_1, \dots, a_n)$ jest izomorficzna z $S(n)$.

Dowód. Niech $M = F(S_1, \dots, S_n)$, gdzie $S_1, \dots, S_n \in F[x_1, \dots, x_n]$ są wielomianami symetrycznymi podstawowymi zmiennych $x_1, \dots, x_n$.²⁷ Elementy $S_1, \dots, S_n$ są algebraicznie niezależne nad ciałem F . Ponieważ elementy $a_1, \dots, a_n$ również są algebraicznie niezależne nad F , istnieje F -izomorfizm $\phi : F(a_1, \dots, a_n) \rightarrow F(S_1, \dots, S_n)$ taki, że $\phi(a_i) = S_i$, $i \in \{1, \dots, n\}$. Niech $\phi^* : F(a_1, \dots, a_n)[x] \rightarrow F(S_1, \dots, S_n)[x]$ będzie izomorfizmem pierścieni wielomianów indukowanym przez ϕ . W szczególności

$$\phi^*(f)(x) = x^n + S_1x^{n-1} + \dots + S_{n-1}x + S_n.$$

Wobec wzorów Viete'y pierwiastkami wielomianu $\phi^*(f)$ są elementy $-x_1, -x_2, \dots, -x_n$. Zatem ciałem rozkładu wielomianu $\phi^*(f)$ jest $L = F(x_1, \dots, x_n)$. Niech L' będzie ciałem rozkładu wielomianu $f \in$

²⁷**Definicja:** Niech $n \in \mathbb{N}$, niech R będzie pierścieniem. Wielomian $f \in R[x_1, \dots, x_n]$ nazywamy **wielomianem symetrycznym**, gdy

$$\forall \sigma \in S(n) [f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})].$$

Zbiór wielomianów symetrycznych oznaczamy $R_{\text{sym}}[x_1, \dots, x_n]$.

Uwaga: Niech $n \in \mathbb{N}$, niech R będzie pierścieniem. Wówczas $R_{\text{sym}}[x_1, \dots, x_n]$ jest pierścieniem.

Definicja: Niech $n \in \mathbb{N}$, niech R będzie pierścieniem. Wielomiany

$$\begin{aligned} S_1(x_1, \dots, x_n) &= x_1 + \dots + x_n \\ S_2(x_1, \dots, x_n) &= x_1x_2 + \dots + x_1x_n + x_2x_3 + \dots + x_2x_n + \dots + x_{n-1}x_n \\ &\vdots \\ S_k(x_1, \dots, x_n) &= \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1}x_{i_2} \cdot \dots \cdot x_{i_k} \\ &\vdots \\ S_n(x_1, \dots, x_n) &= x_1 \cdot \dots \cdot x_n \end{aligned}$$

nazywamy **wielomianami symetrycznymi podstawowymi** zmiennych $x_1, \dots, x_n$.

Twierdzenie: Niech $n \in \mathbb{N}$, niech F będzie ciałem. Wówczas wielomiany symetryczne podstawowe $S_1, \dots, S_n \in F[x_1, \dots, x_n]$ są algebraicznie niezależne nad F .

Twierdzenie (zasadnicze twierdzenie teorii wielomianów symetrycznych): Niech $n \in \mathbb{N}$, niech F będzie ciałem. Wówczas:

$$F_{\text{sym}}[x_1, \dots, x_n] = F[S_1(x_1, \dots, x_n), \dots, S_n(x_1, \dots, x_n)].$$

Proste, aczkolwiek raczej żmudne rachunkowo dowody powyższych twierdzeń pomijamy

$F(a_1, \dots, a_n)[x]$. Wobec Twierdzenia 10.4 istnieje izomorfizm $\alpha : L' \rightarrow L$ taki, że $\alpha|_{F(a_1, \dots, a_n)} = \phi$. Wobec Lematu 15.3 $G(L'/F(a_1, \dots, a_n)) \cong G(F(x_1, \dots, x_n)/F(S_1, \dots, S_n))$.

Pokażemy, że $G(F(x_1, \dots, x_n)/F(S_1, \dots, S_n)) \cong S(n)$. Istotnie, niech $\sigma \in S(n)$. Zdefiniujmy odwzorowanie $\sigma^* : F(x_1, \dots, x_n) \rightarrow F(x_1, \dots, x_n)$ wzorem

$$\sigma^*(g(x_1, \dots, x_n)) = g(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Oczywiście σ^* jest automorfizmem ciała $F(x_1, \dots, x_n)$. Niech $G = \{\sigma^* \in \text{Aut} L : \sigma \in S(n)\}$. Oczywiście G jest grupą i $G \cong S(n)$. Zgodnie z definicją, $F(x_1, \dots, x_n)^G \cong F_{\text{sym}}(x_1, \dots, x_n)$. Ale $F_{\text{sym}}(x_1, \dots, x_n) = F(S_1, \dots, S_n)$. $\square$

Twierdzenie 15.12. *Abela-Ruffini'ego] Niech f będzie ciałem, niech $a_1, \dots, a_n$ będą algebraicznie niezależne nad ciałem F , niech*

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \in F(a_1, \dots, a_n)[x].$$

Wówczas równanie $f(x) = 0$ jest rozwiązywalne w pierwiastnikach wtedy i tylko wtedy, gdy $n \leq 4$.

Dowód. Wobec Wniosku 15.4 równanie $f(x) = 0$ jest rozwiązywalne w pierwiastnikach wtedy i tylko wtedy, gdy grupa Galois wielomianu f nad $F(a_1, \dots, a_n)$ jest rozwiązalna. Wobec poprzedniego twierdzenia ma to miejsce wtedy i tylko wtedy, gdy $S(n)$ jest rozwiązalna, czyli gdy $n \leq 4$ na mocy Uwagi 5.3. $\square$