

14. WYKŁAD 14: GRUPA GALOIS WIELOMIANU. ZASADNICZE TWIERDZENIA TEORII GALOIS.
ROZSZERZENIA ROZWIĄZALNE, CYKLICZNE I ABELOWE.

14.1. Grupa Galois wielomianu.

Definicja 14.1. Niech F będzie ciałem, niech $f \in F[x]$, niech L będzie ciałem rozkładu f . Grupę $G(L/F)$ nazywamy **grupą Galois wielomianu f** .

Twierdzenie 14.1. Niech F będzie ciałem, niech L będzie rozszerzeniem normalnym ciała F . Niech $f \in F[x]$ będzie nierozkładalny, niech $a_1, a_2 \in L$ będą pierwiastkami f . Wówczas istnieje $\sigma \in G(L/F)$ taki, że $\sigma(a_1) = a_2$.

Dowód. Wobec Twierdzenia 10.2 istnieje F -izomorfizm $\phi : F(a_1) \rightarrow F(a_2)$ taki, że $\phi(a_1) = a_2$. Z kolei wobec Lematu 12.1 istnieje F -włożenie $\sigma : L \rightarrow \bar{F}$ takie, że $\sigma|_{F(a_1)} = \phi$. Ponieważ rozszerzenie $F \subset L$ jest normalne, więc $\sigma(L) = L$. Zatem $\sigma \in G(L/F)$ oraz $\sigma(a_1) = \phi(a_1) = a_2$. $\square$

Wniosek 14.1. Niech F będzie ciałem, niech L będzie rozszerzeniem normalnym ciała F , niech $F \subset M \subset L$. Wówczas rozszerzenie $F \subset M$ jest normalne wtedy i tylko wtedy, gdy dla każdego $\sigma \in G(L/F)$ zachodzi $\sigma(M) = M$.

Dowód. $(\Rightarrow)$: oczywiste. $(\Leftarrow)$: Ustalmy wielomian nierozkładalny $f \in F[x]$ i niech $a_1 \in M$ będzie jego pierwiastkiem. Ustalmy pierwiastek $a_2 \in L$ wielomianu f , $a_1 \neq a_2$. Wobec powyższego twierdzenia istnieje F -izomorfizm $\sigma : L \rightarrow L$ taki, że $\sigma(a_1) = a_2$. Ponieważ $\sigma(M) = M$, więc $a_2 \in M$, a zatem rozszerzenie $F \subset M$ jest normalne. $\square$

Twierdzenie 14.2. Niech F będzie ciałem, niech $f \in F[x]$, niech L będzie ciałem rozkładu f . Niech $\{a_1, \dots, a_n\}$ będzie zbiorem wszystkich pierwiastków wielomianu f . Wówczas $G(L/F) < S(\{a_1, \dots, a_n\})$. Ponadto, jeżeli $f = f_1 \cdot \dots \cdot f_r$ jest rozkładem f na czynniki nierozkładalne w $F[x]$, to zbiór pierwiastków wielomianu f_i jest orbitą w zbiorze $\{a_1, \dots, a_n\}$ ze względu na działanie grupy $G(L/F)$.

Dowód. Ponieważ każdy automorfizm $\sigma \in G(L/F)$ jest odwzorowaniem różnowartościowym przekształcającym pierwiastki wielomianu f na siebie, więc σ określa pewną permutację zbioru $\{a_1, \dots, a_n\}$. Różnym automorfizmom odpowiadają różne permutacje, zatem $G(L/F)$ jest izomorficzna z pewną podgrupą grupy $S(\{a_1, \dots, a_n\})$.

Ustalmy pierwiastek a_{ij} wielomianu f_i i rozważmy $\text{Orb}(a_{ij})$. Oczywiście każdy $\sigma \in G(L/F)$ przeprowadza pierwiastki wielomianu f_i na pierwiastki wielomianu f_i . Ponadto, wobec Twierdzenia 14.1, jeśli a_{ik} jest pierwiastkiem f_i , to istnieje $\sigma \in G(L/F)$ taki, że $\sigma(a_{ik}) = a_{ij}$. Zatem $a_{ik} \in \text{Orb}(a_{ij})$. $\square$

Wniosek 14.2. Niech F będzie ciałem, niech $f \in F[x]$, niech L będzie ciałem rozkładu f . Niech $\{a_1, \dots, a_n\}$ będzie zbiorem wszystkich pierwiastków wielomianu f . Wówczas $G(L/F)$ działa przechodnio na zbiorze $\{a_1, \dots, a_n\}$ wtedy i tylko wtedy, gdy f jest potęgą wielomianu nierozkładalnego w $F[x]$.

Dowód. Grupa $G(L/F)$ działa przechodnio na $\{a_1, \dots, a_n\}$ wtedy i tylko wtedy, gdy istnieje tylko jedna orbita tego działania, a więc wtedy i tylko wtedy, gdy czynniki nierozkładalne f są jednakowe. $\square$

Wniosek 14.3. Niech F będzie ciałem, niech $f \in F[x]$, niech L będzie ciałem rozkładu f . Niech $\deg f = n$. Wówczas jeśli $|G(L/F)| = n!$, to f jest nierozkładalny w $F[x]$ oraz L jest rozszerzeniem rozdzielczym ciała F .

Dowód. Przypuśćmy, że rozszerzenie $F \subset L$ nie jest rozdzielcze lub f jest rozkładalny w $F[x]$. Jeżeli rozszerzenie $F \subset L$ nie jest rozdzielcze, to f ma pierwiastek wielokrotny. Zatem liczba różnych pierwiastków f jest mniejsza od n , a więc $G(L/F)$ jest grupą permutacji zbioru o mniej niż n elementach, czyli $|G(L/F)| < n!$.

Jeżeli f jest rozkładalny w $F[x]$ i nie ma pierwiastków wielokrotnych, to wobec Wniosku 14.2 grupa $G(L/F)$ działa przechodnio na $\{a_1, \dots, a_n\}$, a więc musi być $G(L/F) < S(\{a_1, \dots, a_n\})$, czyli $|G(L/F)| < n!$. $\square$

14.2. Zasadnicze twierdzenia teorii Galois.

Uwaga 14.1. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F . Niech ponadto:

$$\mathcal{A} = \{M : F \subset M \subset L, M \text{ jest ciałem}\} \text{ oraz } \mathcal{B} = \{H : H < G(L/F)\}.$$

Niech $\alpha : \mathcal{A} \rightarrow \mathcal{B}$ będzie dane wzorem

$$\alpha(M) = G(L/M),$$

niech $\beta : \mathcal{B} \rightarrow \mathcal{A}$ będzie dane wzorem:

$$\beta(H) = L^H.$$

- (1) Odwzorowania α i β są dobrze określone.
- (2) Jeżeli $M_1, M_2 \in \mathcal{A}$ i $M_1 \subset M_2$, to $\alpha(M_1) \supset \alpha(M_2)$.
- (3) Jeżeli $H_1, H_2 \in \mathcal{B}$ i $H_1 \subset H_2$, to $\beta(H_1) \supset \beta(H_2)$.

Dowód. Porównaj Wnioski 13.4 i 13.5. $\square$

Twierdzenie 14.3 (Galois). Niech F będzie ciałem, niech L będzie rozszerzeniem Galois ciała F . W oznaczeniach Uwagi 14.1 odwzorowanie α jest injekcją, a β jest surjekcją. Ponadto, gdy rozszerzenia $F \subset L$ jest skończone, to α i β są względem siebie odwrotne.

Dowód. Ustalmy $M \in \mathcal{A}$. Wobec Wniosku 13.14 rozszerzenie $M \subset L$ jest Galois. Wobec Twierdzenia 13.5 $M = L^{G(L/M)}$, czyli $\beta(\alpha(M)) = M$, a więc w szczególności β jest surjekcją.

Dalej, ustalmy $M_1, M_2 \in \mathcal{A}$ i załóżmy, że $\alpha(M_1) = \alpha(M_2)$. Wobec tego $M_1 = \beta(\alpha(M_1)) = \beta(\alpha(M_2)) = M_2$, więc α jest injekcją.

Założmy, że rozszerzenie $F \subset L$ jest skończone. Wobec Wniosku 13.15 $|G(L/F)| < +\infty$. Ustalmy $H \in \mathcal{B}$. Wobec Wniosku 13.6 $H = G(L/L^H)$, a więc $H = \alpha(\beta(H))$. $\square$

Wniosek 14.4. Niech F będzie ciałem, niech L będzie skończonym rozszerzeniem Galois ciała F . W oznaczeniach Uwagi 14.1 $|\mathcal{A}| < +\infty$.

Dowód. Wobec Wniosku 13.15 $|G(L/F)| < +\infty$. Stąd $|\mathcal{B}| < +\infty$. Wobec twierdzenia Galois również $|\mathcal{A}| < +\infty$. $\square$

Wniosek 14.5. Niech F będzie ciałem, niech L będzie rozszerzeniem Galois ciała F . Wówczas w oznaczeniach Uwagi 14.1:

- (1) $\alpha(M_1 M_2) = \alpha(M_1) \cap \alpha(M_2)$, dla $M_1, M_2 \in \mathcal{A}$;
- (2) $\beta(\langle H_1 \cup H_2 \rangle) = \beta(H_1) \cap \beta(H_2)$, dla $H_1, H_2 \in \mathcal{B}$.

Ponadto, gdy rozszerzenie $F \subset L$ jest skończone, to:

- (3) $\alpha(M_1 \cap M_2) = \langle \alpha(M_1) \cup \alpha(M_2) \rangle$, dla $M_1, M_2 \in \mathcal{A}$;
- (4) $\beta(H_1 \cap H_2) = \beta(H_1) \beta(H_2)$, dla $H_1, H_2 \in \mathcal{B}$.

Dowód. (1) Ustalmy $\phi \in G(L/F)$. Wówczas

$$\begin{aligned} \phi \in \alpha(M_1 M_2) &\Leftrightarrow \phi \in G(L/M_1 M_2) \Leftrightarrow \phi|_{M_1 M_2} = id \Leftrightarrow \phi|_{M_1} = id \wedge \phi|_{M_2} = id \\ &\Leftrightarrow \phi \in \alpha(M_1) \wedge \phi \in \alpha(M_2) \Leftrightarrow \phi \in \alpha(M_1) \cap \alpha(M_2). \end{aligned}$$

(2) Ustalmy $a \in L$. Wówczas

$$a \in \beta(\langle H_1 \cup H_2 \rangle) \Leftrightarrow a \in L^{\langle H_1 \cup H_2 \rangle} \Leftrightarrow a \in L^{H_1} \wedge a \in L^{H_2} \Leftrightarrow a \in \beta(H_1) \cap \beta(H_2).$$

Jeżeli rozszerzenie $F \subset L$ jest skończone, to $\beta(\alpha(M)) = M$ i $\alpha(\beta(H)) = H$, dla $M \in \mathcal{A}$, $H \in \mathcal{B}$.

(3) Wobec (2):

$$\alpha(M_1 \cap M_2) = \alpha(\beta(H_1) \cap \beta(H_2)) = \alpha \circ \beta(\langle H_1 \cup H_2 \rangle) = \langle H_1 \cup H_2 \rangle = \langle \alpha(M_1) \cup \alpha(M_2) \rangle.$$

(4) Wobec (1):

$$\beta(H_1 \cap H_2) = \beta(\alpha(M_1) \cap \alpha(M_2)) = \beta \circ \alpha(M_1 M_2) = M_1 M_2 = \beta(H_1) \beta(H_2).$$

□

Przykład:

(1) Rozważmy ciało $\mathbb{Q}$, wielomian $f(x) = x^3 - 5 \in \mathbb{Q}[x]$ i ciało rozkładu wielomianu f . Wszystkimi pierwiastkami wielomianu f są $\sqrt[3]{5}$, $\frac{-1+i\sqrt{3}}{2}\sqrt[3]{5}$ oraz $\left(\frac{-1+i\sqrt{3}}{2}\right)^2\sqrt[3]{5}$. Wobec tego

$$L = \mathbb{Q}\left(\sqrt[3]{5}, \frac{-1+i\sqrt{3}}{2}\sqrt[3]{5}, \left(\frac{-1+i\sqrt{3}}{2}\right)^2\sqrt[3]{5}\right) = \mathbb{Q}\left(\sqrt[3]{5}, \frac{-1+i\sqrt{3}}{2}\right)$$

jest ciałem rozkładu f . Wobec tego $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[3]{5})] \cdot [\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 2 \cdot 3 = 6$. Ponieważ rozszerzenie $\mathbb{Q} \subset L$ jest rozdzielcze i normalne, więc jest Galois. Wobec Wniosku 13.15 $|G(L/\mathbb{Q})| = 6$. Wobec Twierdzenia 14.2 $G(L/\mathbb{Q}) \cong S(3)$. Wszystkimi podgrupami grupy $S(3)$ są:

- $\{id\}$, $S(3)$,
- $A(3)$,
- H_1 , H_2 , H_3 – grupy złożone z id i jednej transpozycji.

Wobec twierdzenia Galois istnieją 4 ciała pośrednie: $\beta(A(3))$, $\beta(H_1)$, $\beta(H_2)$, $\beta(H_3)$. Wobec Wniosku 13.16:

$$[\beta(A(3)) : \mathbb{Q}] = (S(3) : A(3)) = 2 \text{ oraz } [\beta(H_i) : \mathbb{Q}] = (S(3) : H_i) = 3 \text{ dla } i \in \{1, 2, 3\}.$$

Wobec twierdzenia Galois ciało $\beta(A(3))$ składa się z tych elementów ciała L , które nie ulegają zmianie przy parzystych permutacjach zbioru $\left\{\sqrt[3]{5}, \frac{-1+i\sqrt{3}}{2}\sqrt[3]{5}, \left(\frac{-1+i\sqrt{3}}{2}\right)^2\sqrt[3]{5}\right\}$. Z definicji permutacji parzystej, przy dowolnej permutacji parzystej nie zmienia się liczba

$$\begin{aligned} &\left(\sqrt[3]{5} - \frac{-1+i\sqrt{3}}{2}\sqrt[3]{5}\right) \cdot \left(\sqrt[3]{5} - \left(\frac{-1+i\sqrt{3}}{2}\right)^2\sqrt[3]{5}\right) \\ &\cdot \left(\frac{-1+i\sqrt{3}}{2}\sqrt[3]{5} - \left(\frac{-1+i\sqrt{3}}{2}\right)^2\sqrt[3]{5}\right) = 15i\sqrt{3}. \end{aligned}$$

Zatem $i\sqrt{3} \in \beta(A(3))$ i tym samym $\beta(A(3)) = \mathbb{Q}(i\sqrt{3})$.

Dalej, wobec twierdzenia Galois, ciało $\beta(H_1)$ składa się z tych elementów ciała L , które nie ulegają zmianie przy transpozycji $\left(\sqrt[3]{5}, \frac{-1+i\sqrt{3}}{2}\sqrt[3]{5}\right)$. Elementem takim jest na przykład $\sqrt[3]{5} +$

$\frac{-1+i\sqrt{3}}{2} \sqrt[3]{5} = - \left(\frac{-1+i\sqrt{3}}{2} \right)^2 \sqrt[3]{5}$. Zatem $\beta(H_1) \supset \mathbb{Q} \left(- \left(\frac{-1+i\sqrt{3}}{2} \right)^2 \sqrt[3]{5} \right)$. Ale

$$[\beta(H_1) : \mathbb{Q}] = \left[\mathbb{Q} \left(- \left(\frac{-1+i\sqrt{3}}{2} \right)^2 \sqrt[3]{5} \right) : \mathbb{Q} \right] = 3,$$

więc $\beta(H_1) = \mathbb{Q} \left(- \left(\frac{-1+i\sqrt{3}}{2} \right)^2 \sqrt[3]{5} \right)$.

Analogicznie znajdujemy $\beta(H_2)$, $\beta(H_3)$.

Twierdzenie 14.4 (Galois). *Niech F będzie ciałem, L rozszerzeniem Galois ciała F . Niech w oznaczeniach Uwagi 14.1 $M \in \mathcal{A}$. Wówczas*

- (1) *rozszerzenie $F \subset M$ jest Galois wtedy i tylko wtedy, gdy $G(L/M) \triangleleft G(L/F)$;*
- (2) *jeżeli $G(L/M) \triangleleft G(L/F)$, to $G(M/K) \cong G(L/F)/G(L/M)$.*

Dowód. (1) ($\Leftarrow$) : Ustalmy F -zanurzenie $\psi' : M \rightarrow \bar{F}$. Wobec Lematu 12.1 istnieje F -zanurzenie $\psi'' : L \rightarrow \bar{F}$ takie, że $\psi''|_M = \psi'$. Ponieważ rozszerzenie $F \subset L$ jest normalne, więc $\psi''(L) = L$. Wobec tego $\psi = \psi''|_L \in G(L/F)$. Ponieważ $G(L/M) \triangleleft G(L/F)$, więc dla $\phi \in G(L/M)$ mamy $\psi^{-1} \circ \phi \circ \psi \in G(L/M)$. Wobec tego dla $a \in M$ zachodzi $\psi^{-1} \circ \phi \circ \psi(a) = a$, czyli $\phi \circ \psi(a) = \psi(a)$. Wobec tego $\psi(a) \in L^{G(L/M)}$. Ponieważ rozszerzenie $F \subset L$ jest Galois, więc i rozszerzenie $M \subset L$ jest Galois, a zatem $L^{G(L/M)} = M$. Zatem $\psi(a) \in M$, czyli $\psi(M) \subset M$. Analogicznie $\psi^{-1}(M) \subset M$, czyli $M \subset \psi(M)$. Wobec tego $M = \psi(M) = \psi'(M)$, a zatem rozszerzenie $F \subset M$ jest normalne. Ponieważ rozszerzenie $F \subset L$ jest rozdzielcze, więc i rozszerzenie $F \subset M$ jest rozdzielcze, a więc i Galois.

($\Rightarrow$) : Ustalmy $\psi \in G(L/F)$. Wówczas $\psi' = \psi|_M$ jest F -zanurzeniem ciała M w ciało $\bar{F}$. Ponieważ rozszerzenie $F \subset M$ jest normalne, więc $\psi'(M) = M$. Zatem $\psi' \in G(M/K)$. Zdefiniujmy odwzorowanie $\sigma : G(L/F) \rightarrow G(M/K)$ wzorem

$$\sigma(\psi) = \psi|_M.$$

Odwzorowanie σ jest dobrze określone. Oczywiście σ jest homomorfizmem grup. Jest to też surjekcja, gdyż jeśli $\psi' \in G(M/K)$, to wobec Lematu 12.1 istnieje F -zanurzenie $\psi : L \rightarrow \bar{F}$ takie, że $\psi|_M = \psi'$ i skoro rozszerzenie $F \subset L$ jest normalne, to $\psi \in G(L/F)$. Na koniec

$$\psi \in \ker \sigma \Leftrightarrow \sigma(\psi) = id \Leftrightarrow \psi|_M = id \Leftrightarrow \psi \in G(L/M).$$

Zatem $\ker \sigma = G(L/M)$ i tym samym $G(L/M) \triangleleft G(L/F)$.

- (2) Dla dowodu części (2) wystarczy skorzystać z twierdzenia o izomorfizmie dla homomorfizmu σ :

$$G(M/K) \cong G(L/F)/G(L/M).$$

□

Wniosek 14.6. *Niech F będzie ciałem, niech L będzie skończonym rozszerzeniem Galois ciała F . Niech $G(L/F) = G_1 \oplus \dots \oplus G_n$. W oznaczeniach Uwagi 14.1 istnieją $M_1, \dots, M_n \in \mathcal{A}$ takie, że*

- $M_i \cap M_j = F$, $i \neq j$,
- $M_i M_j = L$, $i \neq j$,
- rozszerzenia $F \subset M_i$ są Galois,
- $G(M_i/F) = G_i$.

Dowód. Dowód prowadzimy przez indukcję ze względu na n . Dla $n = 2$ niech $M_1 = \beta(G_1)$, $M_2 = \beta(G_2)$. Wobec Wniosku 14.5:

$$M_1 \cap M_2 = \beta(G_1) \cap \beta(G_2) = \beta(\langle G_1 \cup G_2 \rangle) = \beta(G(L/F)) = F$$

oraz

$$M_1 M_2 = \beta(G_1) \beta(G_2) = \beta(G_1 \cap G_2) = \beta(\{id\}) = L.$$

Ponadto $G_1, G_2 \triangleleft G(L/F)$, więc wobec Twierdzenia 14.4 rozszerzenia $F \subset M_1$, $F \subset M_2$ są Galois. Oczywiście $G(M_1/F) = G_1$ oraz $G(M_2/F) = G_2$. Dowód przypadku $n > 2$ pozostawiamy jako ćwiczenie. $\square$

14.3. Rozszerzenia rozwiązalne, cykliczne i abelowe.

Definicja 14.2. Niech F będzie ciałem, L rozszerzeniem Galois ciała F . Jeżeli grupa $G(L/F)$ jest rozwiązalna (lub, odpowiednio, cykliczna, abelowa), to rozszerzenie $F \subset L$ nazywamy **rozwiązalnym** (lub, odpowiednio, **cyklicznym**, **abelowym**).

Twierdzenie 14.5. Niech F będzie ciałem, L rozszerzeniem abelowym ciała F , niech $F \subset M \subset L$. Wówczas rozszerzenia $F \subset M$ i $M \subset L$ są abelowe.

Dowód. Ponieważ każda podgrupa grupy abelowej jest normalna, więc $G(L/M) \triangleleft G(L/F)$. Wobec Twierdzenia 14.4 rozszerzenie $F \subset M$ jest Galois. Ponieważ rozszerzenie $F \subset L$ jest Galois, więc i $M \subset L$ jest Galois. Ponieważ $G(L/M) < G(L/F)$, więc $G(L/M)$ jest abelowa. Dalej, ponieważ $G(M/K) \cong G(L/F)/G(L/M)$, więc $G(M/F)$ też jest abelowa. $\square$

Twierdzenie 14.6. Niech F będzie ciałem, L rozszerzeniem cyklicznym ciała F , niech $F \subset M \subset L$. Wówczas rozszerzenia $F \subset M$ i $M \subset L$ są cykliczne.

Dowód przebiega analogicznie jak w poprzednim twierdzeniu i pozostawiamy go jako proste ćwiczenie.

Twierdzenie 14.7. Niech F będzie ciałem, L rozszerzeniem rozwiązalnym ciała F , niech $F \subset M \subset L$. Wówczas rozszerzenie $M \subset L$ jest rozwiązalne. Ponadto, jeżeli rozszerzenie $F \subset M$ jest Galois, to jest też rozwiązalne. Na odwrót, jeżeli rozszerzenia $F \subset M$ i $M \subset L$ są rozwiązalne, to rozszerzenie $F \subset L$ jest rozwiązalne.

Dowód. Ponieważ $F \subset L$ jest Galois, więc i $M \subset L$ jest Galois. Ponieważ $G(L/M) < G(L/F)$, więc grupa $G(L/M)$ jest rozwiązalna. Jeżeli rozszerzenie $F \subset M$ jest Galois, to wobec Twierdzenia 14.4 $G(L/M) \triangleleft G(L/F)$, a stąd $G(M/K) \cong G(L/F)/G(L/M)$, więc $G(M/F)$ jest rozwiązalna. Jeżeli $F \subset M$ i $M \subset L$ są rozwiązalne, to wobec Twierdzenia 14.4 $G(L/M) \triangleleft G(L/F)$. Skoro $G(L/M)$ jest rozwiązalna i $G(M/K) \cong G(L/F)/G(L/M)$, to $G(L/F)$ jest rozwiązalna. $\square$

Uwaga 14.2. Niech F będzie ciałem, niech L będzie skończonym i abelowym ciałem F . Wówczas istnieją ciała $M_1, \dots, M_n$, $F \subset M_i \subset L$, $i \in \{1, \dots, n\}$, takie, że

- $M_i \cap M_j = F$, $i \neq j$,
- $M_i M_j = L$, $i \neq j$,
- rozszerzenia $F \subset M_i$ są cykliczne,
- $[M_i : F]$ jest potęgą liczby pierwszej.

Dowód. Wynika bezpośrednio z Wniosku 14.6 i tego, że skończona grupa abelowa jest sumą prostą grup cyklicznych. $\square$

Twierdzenie 14.8. Niech F będzie ciałem, niech L będzie skończonym rozszerzeniem Galois ciała F . Następujące warunki są równoważne:

- (1) rozszerzenie $F \subset L$ jest rozwiązalne;
- (2) istnieje ciąg ciał $F = F_0 \subset F_1 \subset \dots \subset F_r = L$ taki, że każde z rozszerzeń $F_i \subset F_{i+1}$ jest cykliczne, $i \in \{0, \dots, r-1\}$ oraz $[F_{i+1} : F_i]$ jest liczbą pierwszą;
- (3) istnieje ciąg ciał $F = F'_0 \subset F'_1 \subset \dots \subset F'_s = L$ taki, że każde z rozszerzeń $F'_i \subset F'_{i+1}$ jest abelowe, $i \in \{0, \dots, s-1\}$.

Dowód. (1) $\Rightarrow$ (2): Załóżmy, że grupa $G(L/F)$ jest rozwiązalna. Wobec tego istnieje ciąg grup $G(L/F) = G_0 \supset G_1 \supset \dots \supset G_r = \{id\}$ taki, że $G_{i+1} \triangleleft G_i$, dla $i \in \{0, \dots, r-1\}$, oraz grupa G_i/G_{i+1} jest cykliczna o rzędzie będącym liczbą pierwszą, $i \in \{0, \dots, r-1\}$. Niech $F_i = L^{G_i}$, $i \in \{0, \dots, r-1\}$. Wówczas $F = F_0 \subset F_1 \subset \dots \subset F_r = L$ oraz $G_i = G(L/F_i)$, $i \in \{0, \dots, r-1\}$. Rozważmy ciąg $F_i \subset F_{i+1} \subset L$, dla ustalonego $i \in \{0, \dots, r-1\}$. Oczywiście $F_i \subset L$ jest rozszerzeniem Galois. Wobec Twierdzenia 14.4 skoro $G_{i+1} \triangleleft G_i$, więc $F_i \subset F_{i+1}$ jest rozszerzeniem Galois. Ponadto

$$G(F_{i+1}/F_i) \cong G(L/F_i)/G(L/F_{i+1}) = G_i/G_{i+1},$$

więc rozszerzenie $F_i \subset F_{i+1}$ jest cykliczne.

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

(3) $\Rightarrow$ (1): Ponieważ rozszerzenie $F \subset L$ jest Galois, więc rozszerzenia $F'_i \subset L$ też są Galois, $i \in \{0, \dots, s-1\}$. Rozważmy ciąg $F'_i \subset F'_{i+1} \subset L$, dla ustalonego $i \in \{0, \dots, s-1\}$. Ponieważ rozszerzenie $F'_i \subset F'_{i+1}$ jest abelowe, więc wobec Twierdzenia 14.4 $G(L/F'_{i+1}) \triangleleft G(L/F'_i)$ oraz $G(F'_{i+1}/F'_i) \cong G(L/F'_i)/G(L/F'_{i+1})$. Niech $G_i = G(L/F'_i)$. Wówczas $G(L/F) = G_0 \supset G_1 \supset \dots \supset G_s = \{id\}$, $G_{i+1} \triangleleft G_i$ oraz grupa G_i/G_{i+1} jest abelowa, $i \in \{0, \dots, s-1\}$. Zatem $G(L/F)$ jest rozwiązalna. $\square$

Twierdzenie 14.9. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F . Jeżeli $F \subset L_1 \subset L$ i $F \subset L_2 \subset L$ są rozszerzeniami abelowymi, to wówczas rozszerzenie $F \subset L_1 L_2$ też jest abelowe.

Dowód. Oczywiście rozszerzenie $F \subset L_1 L_2$ jest Galois oraz $G(L_1 L_2/F) < G(L_1/F) \oplus G(L_2/F)$. Ponieważ grupy $G(L_1/F)$ i $G(L_2/F)$ są abelowe, więc $G(L_1/F) \oplus G(L_2/F)$ jest grupą abelową i tym samym $G(L_1 L_2/F)$ jest abelowa. Zatem rozszerzenie $F \subset L_1 L_2$ jest abelowe. $\square$

Twierdzenie 14.10. Niech F będzie ciałem, niech L będzie rozszerzeniem ciała F . Jeżeli $F \subset L_1 \subset L$ i $F \subset L_2 \subset L$ są rozszerzeniami rozwiązalnymi, to wówczas rozszerzenie $F \subset L_1 L_2$ też jest rozwiązalne.

Dowód przebiega analogicznie jak w poprzednim twierdzeniu i pozostawiamy go jako proste ćwiczenie.

Uwaga 14.3. Niech F będzie ciałem, niech L będzie rozszerzeniem Galois ciała F , niech $[L : F]$ będzie potęgą liczby pierwszej. Wówczas rozszerzenie $F \subset L$ jest rozwiązalne.

Dowód. Jeżeli $[L : F]$ jest potęgą jakiejś liczby pierwszej, to $G(L/F)$ jest p -grupą, a zatem jest rozwiązalna. $\square$