

13. WYKŁAD 13: LINIOWA NIEZALEŻNOŚĆ CHARAKTERÓW. CIAŁO ELEMENTÓW STAŁYCH. GRUPA GALOIS. ROZSZERZENIA GALOIS.

13.1. Liniowa niezależność charakterów.

Definicja 13.1. Niech $(G, \cdot)$ będzie półgrupą, niech F będzie ciałem. **Charakterem** półgrupy G w ciele F nazywamy dowolny homomorfizm $\chi : G \rightarrow U(F)$.

Przykłady:

- (1) Rozważmy dowolną półgrupę $(G, \cdot)$ i dowolne ciało F . Wówczas $\chi : G \rightarrow U(F)$ dany wzorem $\chi(x) = 1$ jest charakterem. Nazywamy go **charakterem trywialnym**.
- (2) Rozważmy półgrupę $\mathbb{Z}$ i dowolne ciało F . Niech $a \in U(F)$. Wówczas $\chi(n) = a^n$ jest charakterem.
- (3) Rozważmy dowolne ciało F i półgrupę $U(F)$. Wówczas dowolny automorfizm ciała F jest charakterem.

Twierdzenie 13.1 (Artina o liniowej niezależności charakterów). Niech $(G, \cdot)$ będzie półgrupą, niech F będzie ciałem, niech $\chi_1, \dots, \chi_n : G \rightarrow U(F)$ będą parami różnymi charakterami, niech $a_1, \dots, a_n \in F$. Wówczas jeżeli

$$\forall x \in G [a_1\chi_1(x) + \dots + a_n\chi_n(x) = 0],$$

to $a_1 = \dots = a_n = 0$.

Dowód. Dowód prowadzimy indukcyjnie ze względu na n . Teza jest oczywista dla $n = 1$, ustalmy więc $n > 1$ i założmy prawdziwość twierdzenia dla liczb mniejszych od n . Ustalmy też elementy $x, y \in G$. Wobec założenia

$$a_1\chi_1(x) + \dots + a_n\chi_n(x) = 0.$$

Mnożąc obustronnie przez $\chi_n(y)$ otrzymujemy:

$$a_1\chi_1(x)\chi_n(y) + \dots + a_n\chi_n(x)\chi_n(y) = 0.$$

Ponadto, wobec założenia:

$$a_1\chi_1(x)\chi_1(y) + \dots + a_n\chi_n(x)\chi_n(y) = a_1\chi_1(xy) + \dots + a_n\chi_n(xy) = 0,$$

tak więc odejmując stronami powyższe dwie równości otrzymujemy

$$a_1[\chi_n(y) - \chi_1(y)]\chi_1(x) + \dots + a_{n-1}[\chi_n(y) - \chi_{n-1}(y)]\chi_{n-1}(x) = 0.$$

Wobec założenia indukcyjnego $a_i[\chi_n(y) - \chi_i(y)] = 0$, dla $i \in \{1, \dots, n-1\}$. Ponieważ $\chi_1, \dots, \chi_n$ są parami różne, więc wobec dowolności $y \in G$, dla każdego $i \in \{1, \dots, n-1\}$ istnieje $y \in G$ takie, że $\chi_n(y) - \chi_i(y) \neq 0$, a zatem $a_i = 0$, dla $i \in \{1, \dots, n-1\}$. Tym samym $a_n\chi_n(x) = 0$, dla wszelkich $x \in G$ oraz $i \in \{1, \dots, n-1\}$, skąd również $a_n = 0$. $\square$

Wniosek 13.1 (twierdzenie Dedekinda o liniowej niezależności automorfizmów). Niech F będzie ciałem, niech $\sigma_1, \dots, \sigma_n : F \rightarrow F$ będą parami różnymi automorfizmami, niech $a_1, \dots, a_n \in F$. Wówczas jeżeli

$$\forall x \in F [a_1\sigma_1(x) + \dots + a_n\sigma_n(x) = 0],$$

to $a_1 = \dots = a_n = 0$.

Wniosek 13.2. Niech F będzie ciałem, niech $\alpha_1, \dots, \alpha_n \in F$ będą parami różne, niech $a_1, \dots, a_n \in F$. Wówczas jeżeli

$$\forall k \in \mathbb{Z} [a_1\alpha_1^k + \dots + a_n\alpha_n^k = 0],$$

to $a_1 = \dots = a_n = 0$.

13.2. Ciało elementów stałych. Grupa Galois.

Uwaga 13.1. Niech L będzie ciałem, niech $G \subset \text{Aut} L$. Zbiór wszystkich elementów stałych na wszystkich automorfizmach z G jest podciałem ciała L .

Dowód. Niech $F = \{a \in L : \sigma(a) = a \text{ dla } \sigma \in G\}$. Oczywiście $\sigma(0) = 0$, $\sigma(1) = 1$ dla $\sigma \in G$, zatem $0, 1 \in F$. Ustalmy $a, b \in F$. Wówczas dla $\sigma \in G$

$$\sigma(a + b) = \sigma(a) + \sigma(b) = a + b,$$

zatem $a + b \in F$. Podobnie $a - b, ab, \frac{a}{b}$ (o ile $b \neq 0$) $\in F$. □

Definicja 13.2. Niech L będzie ciałem, niech $G \subset \text{Aut} L$. Ciało

$$\{a \in L : \sigma(a) = a \text{ dla } \sigma \in G\}$$

nazywamy **ciałem elementów stałych** ze względu na zbiór G i oznaczamy L^G .

Wniosek 13.3. Niech L będzie ciałem, niech $F \subset L$ będzie ciałem prostym. Wówczas $F \subset L^{\text{Aut} L}$.

Wniosek 13.4. Niech L będzie ciałem, niech $G_1 \subset G_2 \subset \text{Aut} L$. Wówczas $L^{G_1} \supset L^{G_2}$.

Uwaga 13.2. Niech F będzie ciałem, L rozszerzeniem ciała F . Zbiór wszystkich automorfizmów ciała L stałych na wszystkich elementach z F jest podgrupą grupy $\text{Aut} L$.

Dowód. Niech $G = \{\sigma \in \text{Aut} L : \sigma(a) = a \text{ dla } a \in F\}$. Ustalmy $\sigma_1, \sigma_2 \in G$. Wówczas, dla $a \in F$:

$$\sigma_1 \circ \sigma_2^{-1}(a) = \sigma_1(\sigma_2^{-1}(a)) = \sigma_1(a) = a,$$

a zatem $\sigma_1 \circ \sigma_2^{-1} \in G$. □

Definicja 13.3. Niech F będzie ciałem, L rozszerzeniem ciała F . Grupę

$$\{\sigma \in \text{Aut} L : \sigma(a) = a \text{ dla } a \in F\}$$

nazywamy **grupą Galois** rozszerzenie $F \subset L$ i oznaczamy $G(L/F)$.

Wniosek 13.5. Niech F będzie ciałem, niech $F \subset L \subset M$ będą rozszerzeniami ciała F . Wówczas $G(M/L) < G(M/F)$.

Twierdzenie 13.2 (Artina). Niech L będzie ciałem, niech $G < \text{Aut} L$. Jeżeli $|G| < +\infty$ lub $[L : L^G] < +\infty$, to wówczas $|G| = [L : L^G]$.

Dowód. Załóżmy, że $|G| < +\infty$. Niech $G = \{\sigma_1, \dots, \sigma_n\}$. Ustalmy $a_1, \dots, a_{n+1} \in L$. Wówczas układ równań:

$$\begin{cases} \sigma_1^{-1}(a_1)x_1 + \dots + \sigma_1^{-1}(a_{n+1})x_{n+1} = 0, \\ \vdots \\ \sigma_n^{-1}(a_1)x_1 + \dots + \sigma_n^{-1}(a_{n+1})x_{n+1} = 0 \end{cases}$$

ma niezerowe rozwiązanie, gdyż równań jest w nim mniej niż niewiadomych. Ustalmy więc niezerowe rozwiązanie $b_1, \dots, b_{n+1} \in L$. Możemy założyć, że $b_1 \neq 0$. Oczywiście $\alpha b_1, \dots, \alpha b_{n+1}$, dla $\alpha \in L$, również jest rozwiązaniem tego układu. Pokażemy, że można przyjąć, iż $\sigma_1(b_1) + \sigma_2(b_1) + \dots + \sigma_n(b_1) \neq 0$.

Istotnie, przypuśćmy, że dla wszelkich $b \in L$ zachodzi

$$\sigma_1(bb_1) + \dots + \sigma_n(bb_1) = \sigma_1(b_1)\sigma_1(b) + \dots + \sigma_n(b_1)\sigma_n(b) = 0.$$

Wówczas, wobec twierdzenie Dedekinda o liniowej niezależności automorfizmów, $\sigma_1(b_1) = \dots = \sigma_n(b_1) = 0$, co jest niemożliwe, ponieważ $b_1 \neq 0$ oraz $\sigma_1, \dots, \sigma_n$ są bijekcjami. Zatem dla pewnego $b \in L$, $bb_1, \dots, bb_n$ jest rozwiązaniem układu, dla którego $\sigma_1(bb_1) + \dots + \sigma_n(bb_1) \neq 0$.

Ponieważ $\sigma_i^{-1}(a_1)b_1 + \dots + \sigma_i^{-1}(a_{n+1})b_{n+1} = 0$, dla $i \in \{1, \dots, n\}$, więc $\sigma_i(\sigma_i^{-1}(a_1)b_1 + \dots + \sigma_i^{-1}(a_{n+1})b_{n+1}) = 0$, dla $i \in \{1, \dots, n\}$. Tym samym

$$\begin{aligned} a_1\sigma_1(b_1) + \dots + a_{n+1}\sigma_1(b_{n+1}) &= 0, \\ &\vdots \\ a_1\sigma_n(b_1) + \dots + a_{n+1}\sigma_n(b_{n+1}) &= 0. \end{aligned}$$

Dodając powyższe równania stronami otrzymujemy

$$a_1(\sigma_1 + \dots + \sigma_n)(b_1) + \dots + a_{n+1}(\sigma_1 + \dots + \sigma_n)(b_{n+1}) = 0.$$

Zauważmy, że $(\sigma_1 + \dots + \sigma_n)(b_i) \in L^G$, dla $i \in \{1, \dots, n+1\}$. Istotnie, ustalmy $i \in \{1, \dots, n+1\}$ oraz $j \in \{1, \dots, n\}$. Wówczas

$$\sigma_j(\sigma_1 + \dots + \sigma_n)(b_i) = \sigma_j \circ \sigma_1(b_i) + \dots + \sigma_j \circ \sigma_n(b_i).$$

Ponieważ G jest grupą, więc $\{\sigma_j \circ \sigma_1, \dots, \sigma_j \circ \sigma_n\} = \{\sigma_1, \dots, \sigma_n\}$ i tym samym

$$\sigma_j \circ \sigma_1(b_i) + \dots + \sigma_j \circ \sigma_n(b_i) = \sigma_1 + \dots + \sigma_n(b_i).$$

Ponieważ $\sigma_1(b_1) + \sigma_2(b_1) + \dots + \sigma_n(b_1) \neq 0$, otrzymaliśmy liniową zależność między elementami $a_1, \dots, a_{n+1}$ o współczynnikach z ciała L^G . Wobec tego $[L : L^G] \leq n = |G|$. W szczególności $[L : L^G]$ jest skończony.

Załóżmy teraz, że $[L : L^G] < +\infty$. Niech $w_1, \dots, w_r$ będzie bazą rozszerzenia $L^G \subset L$. Przyuśmy, że istnieją parami różne elementy $\sigma_1, \dots, \sigma_{r+1} \in G$. Wówczas układ równań

$$\begin{cases} \sigma_1(w_1)x_1 + \dots + \sigma_{r+1}(w_1)x_{r+1} = 0, \\ \vdots \\ \sigma_1(w_r)x_1 + \dots + \sigma_{r+1}(w_r)x_{r+1} = 0 \end{cases}$$

ma niezerowe rozwiązanie, gdyż równań jest w nim mniej niż niewiadomych. Ustalmy więc niezerowe rozwiązanie $c_1, \dots, c_{r+1} \in L$. Wobec tego

$$\begin{aligned} \sigma_1(w_1)c_1 + \dots + \sigma_{r+1}(w_1)c_{r+1} &= 0, \\ &\vdots \\ \sigma_1(w_r)c_1 + \dots + \sigma_{r+1}(w_r)c_{r+1} &= 0. \end{aligned}$$

Ustalmy $a \in L$. Niech $a_1, \dots, a_r \in L^G$ będą takimi elementami, że $a = a_1w_1 + \dots + a_rw_r$. Wobec tego

$$\begin{aligned} \sigma_1(a) &= a_1\sigma_1(w_1) + \dots + a_r\sigma_1(w_r), \\ &\vdots \\ \sigma_{r+1}(a) &= a_1\sigma_{r+1}(w_1) + \dots + a_r\sigma_{r+1}(w_r), \end{aligned}$$

skąd

$$\begin{aligned} &c_1\sigma_1(a) + \dots + c_{r+1}\sigma_{r+1}(a) \\ &= c_1(a_1\sigma_1(w_1) + \dots + a_r\sigma_1(w_r)) + \dots + c_{r+1}(a_1\sigma_{r+1}(w_1) + \dots + a_r\sigma_{r+1}(w_r)) \\ &= a_1(\sigma_1(w_1)c_1 + \dots + \sigma_{r+1}(w_1)c_{r+1}) + \dots + a_r(\sigma_1(w_r)c_1 + \dots + \sigma_{r+1}(w_r)c_{r+1}) \\ &= 0 + \dots + 0 = 0. \end{aligned}$$

Wobec dowolności $a \in L$, $c_1\sigma_1 + \dots + c_{r+1}\sigma_{r+1} = 0$, a więc, wobec twierdzenia Dedekinda o liniowej niezależności automorfizmów, $c_1 = \dots = c_{r+1} = 0$, co jest sprzecznością. Zatem $[L : L^G] \geq |G|$. W szczególności G jest skończona. Łącząc otrzymane rezultaty dostajemy tezę. $\square$

Wniosek 13.6. Niech F będzie ciałem, L rozszerzeniem skończonym ciała F . Wówczas $|G(L/F)| < +\infty$ oraz $|G(L/F)|[L : F]$.

Dowód. Z definicji grupy Galois $F \subset L^{G(L/F)} \subset L$. Wobec tego $[L : L^{G(L/F)}] < +\infty$ i wobec twierdzenia Artina $|G(L/F)| = [L : L^{G(L/F)}][L : F]$. $\square$

Wniosek 13.7. Niech L będzie ciałem, niech $G < \text{Aut} L$. Jeżeli $|G| < +\infty$, to $G(L/L^G) = G$.

Dowód. Oczywiście $G \subset G(L/L^G)$. Wobec twierdzenia Artina i Wniosku 13.6 $|G(L/L^G)| \leq [L : L^G] = |G|$. $\square$

Wniosek 13.8. Niech L będzie ciałem, niech $G < \text{Aut} L$. Jeżeli $|G| < +\infty$, to $L^G = L^{G(L/L^G)}$.

13.3. Rozszerzenia Galois.

Definicja 13.4. Niech F będzie ciałem, L rozszerzeniem algebraicznym ciała F . Rozszerzenie $F \subset L$ nazywamy **rozszerzeniem Galois**, jeżeli istnieje grupa $G < \text{Aut} L$ taka, że $F = L^G$.

Twierdzenie 13.3. Niech F będzie ciałem, L rozszerzeniem algebraicznym ciała F . Wówczas rozszerzenie $F \subset L$ jest Galois wtedy i tylko wtedy, gdy jest rozdzielcze i normalne.

Dowód. ($\Rightarrow$) : Załóżmy, że $G < \text{Aut} L$ jest taką grupą, że $F = L^G$. Ustalmy $a \in L$ i niech $f \in F[x]$ będzie jej wielomianem minimalnym. Wystarczy pokazać, że f rozkłada się w L na różne czynniki liniowe. Dla $\sigma \in G$ mamy $f(\sigma(a)) = \sigma(f(a)) = \sigma(0) = 0$. Wobec tego $\sigma(a)$ jest pierwiastkiem f , a więc zbiór $\{\sigma(a) : \sigma \in G\}$ jest skończony. Niech zatem $\{\sigma(a) : \sigma \in G\} = \{\sigma_1(a), \dots, \sigma_r(a)\}$, gdzie $\sigma_1, \dots, \sigma_r \in G$ są parami różne. Ponieważ $\sigma_i(a)$, $i \in \{1, \dots, r\}$, są pierwiastkami f , więc $\sigma(\sigma_i(a)) \in \{\sigma_1(a), \dots, \sigma_r(a)\}$, dla $\sigma \in G$. Niech

$$g(x) = (x - \sigma_1(a)) \cdot \dots \cdot (x - \sigma_r(a)).$$

Wówczas

$$g(x) = (x - \sigma_1(a)) \cdot \dots \cdot (x - \sigma_r(a)) = (x - \sigma(\sigma_1(a))) \cdot \dots \cdot (x - \sigma(\sigma_r(a))) = (\sigma g)(x),$$

dla $\sigma \in G$, a więc każdy współczynnik g należy do $L^G = F$. Zatem $g \in F[x]$. Ponieważ pierwiastki g są jednokrotne i każdy z nich jest pierwiastkiem f , więc $g|f$. Ponieważ f jest nierozkładalny, więc $f = cg$, dla $c \in U(F)$. Tym samym f jest iloczynem różnych czynników liniowych z $L[x]$.

($\Leftarrow$) : Załóżmy, że $F \subset L$ jest rozdzielcze i normalne. Wówczas dla $a \in L$ i wielomianu minimalnego $f \in F[x]$ tego elementu, f jest iloczynem różnych wielomianów liniowych z $L[x]$. Pokażemy, że żaden element ze zbioru $L \setminus F$ nie jest stały ze względu na $G(L/F)$.

Ustalmy $a \in L \setminus F$. Niech f będzie wielomianem minimalnym a . Wówczas $\deg f > 1$, więc istnieje $b \in L$, $b \neq a$, taki, że $f(b) = 0$. Wobec Twierdzenia 10.2 istnieje F -izomorfizm $\phi : F(a) \rightarrow F(b)$ taki, że $\phi(a) = b$. Z kolei wobec Lematu 12.1 istnieje F -izomorfizm $\psi : \overline{F} \rightarrow \overline{F}$ taki, że $\psi|_{F(a)} = \phi$. Ponieważ rozszerzenie $F \subset L$ jest normalne, więc $\psi(L) = L$. Zatem ψ jest F -automorfizmem ciała L , $\psi|_L \in G(L/F)$ oraz $\psi(a) = b \neq a$.

Reasumując, $L^{G(L/F)} = F$, czyli rozszerzenie $F \subset L$ jest Galois. $\square$

Wniosek 13.9. Niech F będzie ciałem, niech $\text{char} F = 0$, niech $F \subset L$ będzie rozszerzeniem algebraicznym. Wówczas jest to rozszerzenie Galois wtedy i tylko wtedy, gdy jest normalne.

Wniosek 13.10. Niech F będzie ciałem, niech $F \subset L$ będzie rozszerzeniem skończonym. Wówczas jest to rozszerzenie Galois wtedy i tylko wtedy, gdy L jest ciałem rozkładu wielomianu rozdzielczego $f \in F[x]$.

Dowód. Wynika bezpośrednio z Uwagi 12.5 i definicji rozszerzenia rozdzielczego. $\square$

Twierdzenie 13.4. Niech F będzie ciałem, niech $\{L_i : i \in I\}$ będzie rodziną rozszerzeń Galois ciała F . Wówczas rozszerzenie $F \subset \bigcap_{i \in I} L_i$ jest Galois.

Dowód. Wynika bezpośrednio z Twierdzenia 12.16. □

Wniosek 13.11. Niech F będzie ciałem, $F \subset L$ rozszerzeniem ciała F . Niech $F \subset L_1 \subset L$, $F \subset L_2 \subset L$ będą rozszerzeniami Galois. Wówczas $F \subset L_1 L_2$ jest Galois. Ponadto grupa Galois $G(L_1 L_2 / F)$ jest izomorficzna z podgrupą grupy $G(L_1 / F) \oplus G(L_2 / F)$.

Dowód. Wobec Uwagi 12.7 i Wniosku 12.9 rozszerzenie $F \subset L_1 L_2$ jest Galois. Dla dowodu drugiej tezy zdefiniujmy odwzorowanie $\phi : G(L_1 L_2 / F) \rightarrow G(L_1 / F) \oplus G(L_2 / F)$ wzorem

$$\phi(\sigma) = (\sigma|_{L_1}, \sigma|_{L_2}).$$

Ponieważ rozszerzenia $F \subset L_1$ i $F \subset L_2$ są normalne, więc dla $\sigma \in G(L_1 L_2 / F)$ otrzymujemy $\sigma|_{L_1}(L_1) = L_1$ oraz $\sigma|_{L_2}(L_2) = L_2$, a więc odwzorowanie ϕ jest dobrze określone. Oczywiście ϕ jest homomorfizmem grup. Ponadto

$$\sigma \in \ker \phi \Leftrightarrow \sigma|_{L_1} = id_{L_1} \wedge \sigma|_{L_2} = id_{L_2} \Rightarrow \sigma = id_{L_1 L_2},$$

więc $G(L_1 L_2 / F) \cong \phi(G(L_1 L_2 / F)) < G(L_1 / F) \oplus G(L_2 / F)$. □

Wniosek 13.12. Niech F będzie ciałem, $F \subset L$ rozszerzeniem ciała F . Niech $F \subset L_1 \subset L$, $F \subset L_2 \subset L$ będą skończonymi rozszerzeniami Galois, niech $[L_1 : F] = r_1$, $[L_2 : F] = r_2$. Jeżeli $NWD(r_1, r_2) = 1$, to $G(L_1 L_2 / F) \cong G(L_1 / F) \oplus G(L_2 / F)$.

Dowód. Wobec poprzedniego wniosku wystarczy pokazać, że $|G(L_1 L_2 / F)| = |G(L_1 / F) \oplus G(L_2 / F)|$. Ponieważ rozszerzenia $F \subset L_1$, $F \subset L_2$ i $F \subset L_1 L_2$ są Galois, więc $|G(L_1 L_2 / F)| = [L_1 L_2 : F]$, $|G(L_1 / F)| = [L_1 : F]$ i $|G(L_2 / F)| = [L_2 : F]$. Wobec Twierdzenia 11.2 $[L_1 L_2 : F] = [L_1 : F] \cdot [L_2 : F]$. Ponieważ $|G(L_1 / F) \oplus G(L_2 / F)| = |G(L_1 / F)| \cdot |G(L_2 / F)|$, otrzymujemy tezę. □

Wniosek 13.13. Niech F będzie ciałem, L rozszerzeniem ciała F . Niech $F \subset M \subset L$ będzie rozszerzeniem Galois, niech $F \subset N \subset L$ będzie dowolnym rozszerzeniem. Wówczas rozszerzenie $FN \subset MN$ jest Galois. Ponadto $G(MN / FN)$ jest izomorficzna z podgrupą grupy $G(M / F)$.

Dowód. Wobec Uwagi 12.8 rozszerzenie $FN \subset MN$ jest normalne. Ponieważ każdy element M jest rozdzielnym nad F , więc jest też rozdzielnym nad FN . Wobec tego rozszerzenie $FN \subset MN$ jest rozdzielcze. Zatem $FN \subset MN$ jest Galois. Zdefiniujmy odwzorowanie $\phi : G(MN / FN) \rightarrow G(M / F)$ wzorem:

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

Ponieważ rozszerzenie $F \subset M$ jest normalne, więc dla $\sigma \in G(MN / FN)$ otrzymujemy $\sigma|_M(M) = M$. Oczywiście jest F -automorfizmem. Zatem ϕ jest dobrze określone. Oczywiście ϕ jest homomorfizmem grup. Ponadto:

$$\sigma \in \ker \phi \Leftrightarrow \sigma|_M = id \Leftrightarrow \sigma_{MN} = id \Leftrightarrow \sigma = id_{MN},$$

więc $G(MN / FN) \cong \phi(G(MN / FN)) < G(M / F)$. □

Wniosek 13.14. Niech F będzie ciałem, niech $F \subset M \subset L$ i niech $F \subset L$ będzie Galois. Wówczas $M \subset L$ jest rozszerzeniem Galois.

Dowód. Wynika bezpośrednio z Twierdzenia 12.17. □

Twierdzenie 13.5. Niech F będzie ciałem, L rozszerzeniem algebraicznym ciała F . Wówczas jest to rozszerzenie Galois wtedy i tylko wtedy, gdy $F = L^{G(L/F)}$.

Dowód. $(\Leftarrow)$: oczywiste. $(\Rightarrow)$: Załóżmy, że $F = L^G$ dla pewnej grupy $G < \text{Aut} L$. Ponieważ dla $\sigma \in G$ zachodzi $\sigma|_F = \sigma|_{L^G} = \text{id}$, więc $G \subset G(L/F)$. Wobec tego $L^G \supset L^{G(L/F)}$. Ale oczywiście też $L^G = F \subset L^{G(L/F)}$. Zatem $F = L^G = L^{G(L/F)}$. $\square$

Wniosek 13.15. *Niech F będzie ciałem, L rozszerzeniem skończonym ciała F . Wówczas jest to rozszerzenie Galois wtedy i tylko wtedy, gdy $|G(L/F)| = [L : F]$.*

Dowód. Wobec twierdzenia Artina $|G(L/F)| = [L : L^{G(L/F)}]$. Ponieważ $L \supset L^{G(L/F)} \supset F$ więc $|G(L/F)| = [L : F]$ wtedy i tylko wtedy, gdy $F = L^{G(L/F)}$. Wobec powyższego twierdzenia otrzymujemy tezę. $\square$

Wniosek 13.16. *Niech F będzie ciałem, niech $F \subset M \subset L$ będą rozszerzeniami skończonymi, niech $F \subset L$ będzie rozszerzeniem Galois. Wówczas $[L : M] = |G(L/M)|$ oraz $[M : F] = (G(L/F) : G(L/M))$.*

Dowód. Rozszerzenie $M \subset L$ jest Galois, więc wobec powyższego wniosku $[L : M] = |G(L/M)|$. Ponadto:

$$[M : F] = \frac{[L : F]}{[L : M]} = \frac{|G(L/F)|}{|G(L/M)|} = (G(L/F) : G(L/M)).$$

$\square$

Przykłady:

- (1) Rozważmy rozszerzenie $\mathbb{R} \subset \mathbb{C}$. Jest to rozszerzenie Galois. Istotnie, zdefiniujemy odwzorowanie $\sigma : \mathbb{C} \rightarrow \mathbb{C}$ wzorem

$$\sigma(z) = \bar{z}.$$

Oczywiście $\sigma \in G(\mathbb{C}/\mathbb{R})$. Ponadto $\text{id}_{\mathbb{C}} \in G(\mathbb{C}/\mathbb{R})$. Tym samym $|G(\mathbb{C}/\mathbb{R})| \geq 2$. Z drugiej strony $|G(\mathbb{C}/\mathbb{R})| \leq [\mathbb{C} : \mathbb{R}] = 2$, zatem $|G(\mathbb{C}/\mathbb{R})| = [\mathbb{C} : \mathbb{R}]$ i $\mathbb{R} \subset \mathbb{C}$ jest rozszerzeniem Galois.

- (2) Rozważmy rozszerzenie $F \subset L$, gdzie F jest dowolnym ciałem takim, że $\text{char} F \neq 2$ oraz $[L : F] = 2$. Jest to rozszerzenie Galois. Istotnie, ponieważ $[L : F] = 2$, więc dla $a \in L \setminus F$ otrzymujemy $[F(a) : F] = 2$. Wobec tego, jeśli f jest wielomianem minimalnym a , to $\deg f = 2$. Ponieważ $\text{char} F \neq 2$, więc $f' \neq 0$, a zatem f jest rozdzielnym. Tym samym $f(x) = (x - a)(x - b)$, gdzie $a \neq b$. Skoro $f(x) \in F[x] \subset L[x]$ oraz $x - a \in L[x]$, to również $x - b \in L[x]$, a więc $b \in L$. Tym samym $F(b) = L = F(a)$, istnieje więc F -izomorfizm $\phi : F(a) \rightarrow F(b)$ taki, że $\phi(a) = b$. Oczywiście $\phi \in G(L/F)$ i skoro $a \neq b$, więc $\phi \neq \text{id}_L$. Tym samym $|G(L/F)| \geq 2$. Z drugiej strony $|G(L/F)| \leq [L : F] = 2$, zatem $|G(L/F)| = [L : F]$ i $F \subset L$ jest rozszerzeniem Galois.

- (3) Rozważmy rozszerzenie $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$. Nie jest to rozszerzenie Galois. Istotnie

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

są wszystkimi pierwiastkami wielomianu $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Spośród nich tylko $\sqrt[3]{2} \in \mathbb{R}$, a zatem $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$. Przy dowolnym $\sigma \in G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ liczba $\sqrt[3]{2}$ musi przejść na pierwiastek $f(x)$ leżący w $\mathbb{Q}(\sqrt[3]{2})$, czyli na $\sqrt[3]{2}$. Ponieważ każdy element $a \in \mathbb{Q}(\sqrt[3]{2})$ jest postaci $a = g(\sqrt[3]{2})$, dla $g \in \mathbb{Q}[x]$, więc

$$\sigma(a) = \sigma(g(\sqrt[3]{2})) = g(\sigma(\sqrt[3]{2})) = g(\sqrt[3]{2}) = a.$$

Zatem $\sigma = \text{id}$, skąd $|G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1 < 3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$.

Uwaga 13.3. *Niech F będzie ciałem, niech $F \subset M$ będzie rozszerzeniem rozdzielczym. Domknięcie normalne $F \subset M \subset L$ rozszerzenia $F \subset M$ jest rozszerzeniem Galois.*

Dowód. Wobec Uwagi 12.6 rozszerzenie $F \subset L$ jest rozdzielcze. Oczywiście jest też normalne, a więc jest to rozszerzenie Galois. $\square$

Definicja 13.5. Niech F będzie ciałem, niech $F \subset M$ będzie rozszerzeniem rozdzielczym. Najmniejsze rozszerzenie $M \subset L$ takie, że $F \subset L$ jest normalne nazywamy **domknięciem Galois** rozszerzenia $F \subset M$.

Uwaga 13.4. Niech F będzie ciałem, niech $F \subset L$ będzie rozszerzeniem algebraicznym. Wówczas $G(L/F_S(L)) = \{id_L\}$ oraz $G(L/F)$ jest izomorficzna z podgrupą grupy $G(F_S(L)/F)$.

Dowód. Pokażemy najpierw, że $G(L/F_S(L)) = \{id_L\}$. Teza ta jest oczywista, jeżeli $\text{char} F = 0$. Załóżmy więc, że $\text{char} F = p$ i ustalmy $\sigma \in G(L/F_S(L))$ oraz $a \in L \setminus F_S(L)$. Wobec Wniosku 12.5 dla pewnego $n \in \mathbb{N}$ $a^{p^n} \in F_S(L)$. Wówczas $a^{p^n} = \sigma(a^{p^n}) = (\sigma(a))^{p^n}$, czyli $(\sigma(a) - a)^{p^n} = 0$, skąd $\sigma(a) = a$. Zatem $\sigma = id_L$.

Pokażemy, że $G(L/F)$ jest izomorficzna z podgrupą grupy $G(F_S(L)/F)$. Zdefiniujmy w tym celu odwzorowanie $\phi : G(L/F) \rightarrow G(F_S(L)/F)$ wzorem

$$\phi(\sigma) = \sigma|_{F_S(L)}.$$

Oczywiście dla $a \in F_S(L)$ oraz $\sigma \in G(L/F)$ otrzymujemy $\sigma(a) \in F_S(L)$, więc ϕ jest dobrze określone. Oczywiście ϕ jest homomorfizmem grup. Ponadto

$$\sigma \in \ker \phi \Leftrightarrow \sigma|_{F_S(L)} = id_{F_S(L)} \Rightarrow \sigma \in G(L/F_S(L)) = \{id_L\},$$

a więc $G(L/F) \cong \phi(G(L/F)) < G(F_S(L)/F)$. $\square$