Uniwersytet Wrocławski
Wydział Matematyki i Informatyki
Instytut Matematyczny
specjalność: ogólna

Alicja Kotyla

O nieskończonej teorii Galois

Praca licencjacka
napisana pod kierunkiem
prof. dr. hab. Krzysztofa Krupińskiego

Wrocław 2020

Spis treści

1 Wstęp

Tematem poniższej pracy są wybrane zagadnienia nieskończonej teorii Galois, które omówimy w dalszej części wprowadzenia. Do rozważań dotyczących nieskończonych rozszerzeń niezbędne będą podstawowe wiadomości z zakresu grup proskończonych, które wprowadzimy w rozdziale 2. W rozdziale 3 przybliżymy zaś podstawowe pojęcia i fakty teorii Galois. W szczególności zaprezentowane zostanie twierdzenie mówiące o topologicznym izomorfiźmie między grupą Galois nieskończonego rozszerzenia Galois, a pewną grupą proskończoną, które będzie wielokrotnie używane w dalszej części pracy, gdzie wyliczać będziemy konkretne przykłady grup Galois dla nieskończonych rozszerzeń Galois.

W tym momencie warto wspomnieć o motywacji do powstania poniższej pracy. Przede wszystkim był nią odwrócony problem Galois: czy każda grupa skończona jest grupą Galois pewnego rozszerzenia Galois ciała liczb wymiernych? Problem ten jest otwary, jednak dla niektórych rodzajów grup odpowiedź jest pozytywna. W szczególności zaawansowane twierdzenie Shafarevica dostarcza pozytywnej odpowiedzi w przypadku skończonych grup rozwiązalnych [6].

W rozdziałach 4, 5 zajmiemy się zmodyfikowaną wersją w.w. problemu, czyli będziemy rozważać, które grupy skończone/proskończone pojawiają się jako grupy Galois danego ciała. W szczególności pokażemy, w jaki sposób przedstawione w 5 rozdziale twierdzenie Waterhausa zastosowane do wolnej grupy proskończonej o przeliczalnie wielu generatorach dostarczy ciała, nad którym można zrealizować wszystkie grupy skończone. Z kolei w 4 rozdziale podane zostaną konkretne przykłady grup proskończonych abelowych oraz rozwiązalnych (stopnia 2), które są grupami Galois dla pewnych rozszerzeń Galois m.in ciała $\mathbb{Q}$.

Kolejnym problemem, który był motywacją do powstania poniższej pracy, jest zagadnienie istnienia największego rozszerzenia abelowego oraz rozwiązalnego dla dowolnego ciała K. W rozdziale 6 przedstawimy konstrukcję największego rozszerzenia abelowego dowolnego ciała K, tj. w szczególności pokażemy jego istnienie, zaś w rozdziale 7 dowiedziemy istnienia największego rozszerzenia prorozwiązalnego.

Ostatni rozdział poświęcony zostanie problemowi istnienia największego rozszerzenia rozwiązalnego dowolnego ciała K. W większości rozdział 8 będzie prezentacją artykułu [5], w którym autor przedstawia sposób realizacji splotu $\mathbb{Z}_2 \wr \cdots \wr \mathbb{Z}_2$ jako grupy Galois nad $\mathbb{Q}$. Wiele dowodów w tej pracy było pominiętych lub przedstawionych dość szkicowo. W szczególności lematy: 8.1., 8.4., 8.11., 8.12., 8.27., wniosek 8.28., 8.29., uwaga 8.6. oraz dowód twierdzenia 8.13. nie zostały odnotowane we wspomnianym artykule. Na koniec, po uzasadnieniu, że dla każdego $n < \omega$, n-krotny splot $\mathbb{Z}_2$ jest rozwiązalny stopnia rozwiązalności n, otrzymamy rosnący ciąg rozszerzeń $\mathbb{Q}$ o stopniach rozwiązalności zbiegających do nieskończoności, co prowadzi do konkretnego przykładu rozszerzenia Galois ciała $\mathbb{Q}$ z prorozwiązalną, ale nie rozwiązalną grupą Galois (patrz wniosek 8.29.). Ponadto otrzymamy bardzo istotny wniosek (patrz wniosek 8.28.) - negatywną odpowiedź na postawione wcześniej pytanie o istnienie największego rozszerzenia rozwiązalnego. Wniosek ten wynika również natychmiast ze wspomnianego powyżej tw. Shafarevica. Przedstawiony przez nas argument jest jednak prostszy i dostarcza konkretnej klasy przykładów.

2 Grupy proskończone

W tym rozdziale wprowadzimy kluczowe dla dalszej części pracy pojęcie grupy proskończonej. W tym celu przypomnimy definicję oraz podstawowe własności grupy topologicznej, a następnie zapoznamy czytelnika z pojęciem granicy odwrotnej. Na koniec przedstawimy twierdzenie będące charakteryzacją grup proskończonych, które będzie istotne w pojawiających się w dalszej części rozważaniach dotyczących istnienia największego rozszerzenia prorozwiązalnego.

2.1 Grupy topologiczne

Zaczniemy od wprowadzenia definicji grupy topologicznej. Rozważmy dowolną grupę G. Jeżeli na G jest określona struktura przestrzeni topologicznej w taki sposób, że działanie grupowe oraz branie elementu odwrotnego są odwzorowaniami ciągłymi,

to mówimy, że G jest *grupą topologiczną*.

Uwaga 2.1. Dla dowolnej grupy topologicznej G, będziemy zakładać, że $\{1\}$ jest domkniętym podzbiorem G, czyli G jest przestrzenią T_1. Wówczas, z ciągłości działania w G, $\{x\}$ będzie domknięty dla wszystkich $x \in G$.

Łatwo zauważyć, że dowolna grupa G wyposażona w topologię dyskretną jest naturalnym przykładem grupy topologicznej. Ponadto grupą topologiczną jest również $(\mathbb{R}, +)$ z topologią euklidesową.

Poniżej sformułujemy podstawowe własności grup topologicznych, z których korzystać będziemy w dalszej części pracy.

Lemat 2.2. *Niech G będzie grupą topologiczną.*

1. *Jeżeli H jest otwartą (domknięta) podgrupą G, to dla każdego $g \in G$ warstwy gH, Hg są otwarte (domknięte).*

2. *Każda otwarta podgrupa G jest domknięta. Każda domknięta podgrupa G o skończonym indeksie jest otwarta.*

3. *Jeśli G jest zwarta, to każda otwarta podgrupa G jest skończonego indeksu.*

4. *G jest przestrzenią Hausdorffa.*

Dowód. [4] lemat 0.3.1. □

Uwaga 2.3. W dalszej części pracy dowolną grupę skończoną G będziemy rozumieć jako grupę topologiczną z topologią dyskretną.

2.2 Granice odwrotne

Zanim przejdziemy do definicji granicy odwrotnej, konieczne jest wprowadzenie pojęcia systemu odwrotnego.

Załóżmy, że I jest zbiorem częściowo uporządkowanym przez $\leqslant$. Jeśli dodatkowo $(I, \leqslant)$ spełnia, że dla wszystkich $i, j \in I$, istnieje $k \in I$, taki że $i \leqslant k$ oraz $j \leqslant k$, to $(I, \leqslant)$ nazywamy *zbiorem skierowanym*.

Definicja 2.4. *Systemem odwrotnym przestrzeni topologicznych (odpowiednio, grup topologicznych)* nad zbiorem skierowanym $(I, \leqslant)$ nazywamy rodzinę $(X_i, \varphi_{ij})_{i \geqslant j \in I}$, gdzie X_i jest przestrzenią topologiczną (odpowiednio, grupą topologiczną), a $\varphi_{ij} : X_i \to X_j$ jest ciągła (odpowiednio, ciągłym homomorfizmem), spełniającą następujące warunki:

1. dla każdego $i \in I$, $\varphi_{ii} = id_{X_i}$

2. dla wszystkich $i, j, k \in I$, takich że $i \leqslant j \leqslant k$, zachodzi $\varphi_{ki} = \varphi_{ji}\varphi_{kj}$, tj. następujący diagram jest przemienny:

$$\begin{array}{ccc} X_k & \xrightarrow{\varphi_{kj}} & X_j \\ & \searrow^{\varphi_{ki}} & \downarrow{\scriptstyle \varphi_{ji}} \\ & & X_i \end{array}$$

W dalszej części rozdziału $(I, \leqslant)$ zawsze będzie oznaczać zbiór skierowany. Możemy teraz przejść do pojęcia granicy odwrotnej.

Definicja 2.5. *Granicą odwrotną* $(X, \varphi_i)_{i\in I}$ systemu odwrotnego przestrzeni topologicznych (odpowiednio, grup topologicznych) $(X_i, \varphi_{ij})_{i\geqslant j\in I}$ nazywamy przestrzeń topologiczną (odpowiednio, grupę topologiczną) X wraz z rodziną odwzorowań ciągłych (odpowiednio, ciągłych homomorfizmów) $\{\varphi_i : X \to X_i : i \in I\}$, gdy spełnione są następujące warunki:

1. dla wszystkich $i \geqslant j \in I$, $\varphi_{ij}\varphi_i = \varphi_j$,
2. dla dowolnej przestrzeni topologicznej (odpowiednio, grupy topologicznej) Y i rodziny funkcji ciągłych (odpowiednio, ciągłych homomorfizmów) $\{\phi_i : Y \to X_i : i \in I\}$, spełniających punkt 1. powyżej, istnieje jedyna funkcja ciągła (odpowiednio, ciągły homomorfizm) $\chi : Y \to X$, taki że dla każdego $i \in I$, $\varphi_i\chi = \phi_i$.

Przejdziemy teraz do sformułowania twierdzenia mówiącego o istnieniu granicy odwrotnej oraz jej jedyności (z dokładnością do izomorfizmu).

Twierdzenie 2.6.

1. *Niech $(G_i, \varphi_{ij})_{i\geqslant j\in I}$ będzie systemem odwrotnym grup topologicznych, a $(G, \varphi_i)_{i\in I}$, $(H, \psi_i)_{i\in I}$ będą jego granicami odwrotnymi. Wtedy istnieje topologiczny izomorfizm $\Phi : G \to H$ taki, że dla każdego $i \in I$, $\psi_i\Phi = \varphi_i$.*
2. *Załóżmy, że $(G_i, \varphi_{ij})_{i\geqslant j\in I}$ jest systemem odwrotnym grup topologicznych. Niech*

$$G := \{\bar{g} \in \prod_{i\in I} G_i : (\forall i \geqslant j \in I)\ (\pi_j = \varphi_{ij}\pi_i)\},$$

gdzie π_i są rzutami kanonicznymi:

$$\begin{aligned} \pi_i \colon \prod_{i\in I} G_i &\to G_i \\ (g_i)_{i\in I} &\mapsto g_i. \end{aligned}$$

Załóżmy ponadto, że G jest wyposażony w topologię dziedziczoną z topologii produktowej na $\prod\limits_{i\in I} G_i$. Dla każdego $i \in I$, definiujemy $\psi_i = \pi_i \restriction_G$. Wtedy $(G, \psi_i)_{i\in I}$ jest granicą odwrotną systemu odwrotnego $(G_i, \varphi_{ij})_{i\geqslant j\in I}$.

Dowód. [4], 1.1.4. □

2.3 Grupy proskończone

Zaczniemy od wprowadzenia pojęcia grupy proskończonej.

Definicja 2.7. *Grupą proskończoną* nazywamy granicę odwrotną systemu odwrotnego grup skończonych.

Uwaga 2.8. Każda grupa proskończona jest grupą topologiczną oraz jest zwartą przestrzenią Hausdorffa ([2], 1.2.1). Stąd w szczególności otrzymujemy, że dowolna ciągła bijekcja między grupami proskończonymi jest homeomorfizmem ([4], 0.1.2).

W dalszej części pracy będziemy się zajmować wskazywaniem izomorfizmów między danymi grupami proskończonymi. W tym celu przydatne będzie następujące kryterium:

Lemat 2.9. *Niech $(G_i, \varphi_{ij})_{i \geqslant j \in I}$, $(H_i, \psi_{ij})_{i \geqslant j \in I}$ będą systemami odwrotnymi grup skończonych. Załóżmy, że $f_i : G_i \to H_i$, $i \in I$ są izomorfizmami kompatybilnymi z funkcjami $\varphi_{ij}, \psi_{ij}, i \geqslant j \in I$, tj. dla każdych $i \geqslant j \in I$ następujący diagram jest przemienny:*

$$\begin{array}{ccc} G_j & \xleftarrow{\varphi_{ij}} & G_i \\ {\scriptstyle f_j}\downarrow & & \downarrow{\scriptstyle f_i} \\ H_j & \xleftarrow{\psi_{ij}} & H_i. \end{array}$$

Wtedy funkcja $f : \varprojlim_{i \in I} G_i \to \varprojlim_{i \in I} H_i$ zadana wzorem $f((g_i)_{i \in I}) = (f_i(g_i))_{i \in I}$ jest topologicznym izomorfizmem grup.

Dowód. Łatwo widać, że f przyjmuje wartości w $\varprojlim_{i \in I} H_i$. Sprawdzimy najpierw, że f jest bijekcją.

Rozważmy funkcję $f' : \varprojlim_{i \in I} H_i \to \varprojlim_{i \in I} G_i$ zadaną wzorem $f'((h_i)_{i \in I}) = (f_i^{-1}(h_i))_{i \in I}$. Pokażemy, że $ff' = \mathrm{id}_{\varprojlim_{i \in I} H_i}$ oraz $f'f = \mathrm{id}_{\varprojlim_{i \in I} G_i}$. Ustalmy dowolne $(h_i)_{i \in I} \in \varprojlim_{i \in I} H_i$ oraz $(g_i)_{i \in I} \in \varprojlim_{i \in I} G_i$. Obliczamy

$$ff'((h_i)_{i \in I}) = f((f_i^{-1}(h_i))_{i \in I}) = (f_i(f_i^{-1}(h_i)))_{i \in I} = (h_i)_{i \in I}.$$

Ponadto

$$f'f((g_i)_{i \in I}) = f'((f_i(g_i))_{i \in I}) = (f_i^{-1}(f_i(g_i)))_{i \in I} = (g_i)_{i \in I}.$$

Z dowolności $(h_i)_{i \in I}, (g_i)_{i \in I}$ mamy zatem, że $ff' = \mathrm{id}_{\varprojlim_{i \in I} H_i}$ oraz $f'f = \mathrm{id}_{\varprojlim_{i \in I} G_i}$, a więc f jest bijekcją. Ponadto z założenia $(f_i)_{i \in I}$ są homomorfizmami, a zatem oczywiście f jest homomorfizmem. Otrzymujemy więc, że f jest izomorfizmem.

Pozostaje sprawdzić ciągłość. Ustalmy dowolny zbiór $U \subseteq \varprojlim_{i \in I} H_i$ ze standardowej podbazy, tj. $U = \{(h_i)_{i \in I} \in \varprojlim_{i \in I} H_i : h_{i_0} = h\}$ dla pewnych $i_0 \in I, h \in \varprojlim_{i \in I} H_i$.

Mamy, że $f^{-1}(U) = \{(g_i)_{i\in I} \in \varprojlim_{i\in I} G_i : f((g_i)_{i\in I}) \in U\} = \{(g_i)_{i\in I} \in \varprojlim_{i\in I} G_i : (f_i(g_i))_{i\in I} \in U\} = \{(g_i)_{i\in I} \in \varprojlim_{i\in I} G_i : f_{i_0}(g_{i_0}) = h\} = \{(g_i)_{i\in I} \in \varprojlim_{i\in I} G_i : g_{i_0} = f_{i_0}^{-1}(h)\}$, a więc $f^{-1}(U)$ jest zbiorem ze standardowej podbazy $\varprojlim_{i\in I} G_i$, tj. jest otwarty. Z dowolności U otrzymujemy ciągłość f. Z uwagi 2.8. mamy więc, że f jest homeomorfizmem. Dostajemy zatem, że $\varprojlim_{i\in I} G_i \cong \varprojlim_{i\in I} H_i$ jako grupy topologiczne. □

Przejdziemy teraz do dowodu charakteryzacji grupy proskończonej, która będzie nam niezbędna w pojawiających się w rozdziale 7. rozważaniach dotyczących istnienia największego (a więc również maksymalnego) rozszerzenia prorozwiązalnego dowolnie ustalonego ciała K.

Uwaga 2.10. Niech $(X_i, \varphi_{ij})_{i\geqslant j\in I}$ będzie systemem odwrotnym przestrzeni topologicznych.

1. Zbiory postaci $\pi_i^{-1}(U_i)$, gdzie π_i jest rzutem na i-tą oś oraz $U_i \subseteq X_i$ otwarty, tworzą bazę topologii w $\varprojlim_{i\in I} X_i$.

2. Niech $S \subseteq \varprojlim_{i\in I} X_i$, taki że dla każdego $i \in I$, $\pi_i(S) = X_i$. Wtedy $\overline{S} = \varprojlim_{i\in I} X_i$.

Dowód.

1. [2], 1.1.1.

2. Na mocy punktu 1. wystarczy sprawdzić, że dla dowolnych $i \in I$, $\emptyset \neq U \subseteq X_i$ otwartego, $\pi_i^{-1}(U) \cap S \neq \emptyset$. Ustalmy więc dowolne $i \in I, \emptyset \neq U \subseteq X_i$ otwarty. Wtedy $U \cap \pi_i(S) \neq \emptyset$, a więc również $\pi_i^{-1}(U) \cap S \neq \emptyset$. Stąd, wobec dowolności i oraz U, mamy że dla każdego otwartego $U' \subseteq \varprojlim_{i\in I} X_i$, $U' \cap S \neq \emptyset$, czyli $\overline{S} = \varprojlim_{i\in I} X_i$.

□

Twierdzenie 2.11. *Załóżmy, że G jest grupą topologiczną (Hausdorffa), a $\{G_i\}_{i\in I}$ jest rodziną grup skończonych.*

Wtedy G jest izomorficzna (jako grupa topologiczna) z pewną granicą odwrotną grup $\{G_i\}_{i\in I}$ (gdzie funkcje z systemu skierowanego są surjekcjami) $\iff$ G jest zwarta i posiada bazę otwartych otoczeń elementu neutralnego złożoną z otwarto-domkniętych podgrup normalnych $\{N_i : i \in I\}$, taką że dla wszystkich $i \leqslant j \in I$, $G_i \cong G/N_i$ oraz $N_j \leqslant N_i$.

Dowód. $\Longrightarrow$: Załóżmy, że $(G_i, \varphi_{ij})_{i\geqslant j\in I}$ jest systemem odwrotnym grup skończonych. Dla każdego $i \in I$, G_i jest zwarta, ponieważ jest dyskretna, a więc $(\varprojlim_{i\in I} G_i, \varphi_i)_{i\in I}$ jest zwarta jako podprzestrzeń produktu przestrzeni zwartych, stąd G jest zwarta.

Pokażemy, że rodzina podgrup normalnych $\{\ker\varphi_i : i \in I\}$ tworzy bazę otwartych otoczeń elementu neutralnego e w $\varprojlim_{i\in I} G_i$ oraz dla każdych $i > j \in I$, $\ker\varphi_i \leqslant \ker\varphi_j$.
Weźmy dowolny zbiór otwarty $U \subseteq \varprojlim_{i\in I} G_i$ zawierający e. Z definicji topologii produktowej U jest sumą zbiorów postaci: $\varphi_{i_1}^{-1}(X_{i_1}) \cap ... \cap \varphi_{i_k}^{-1}(X_{i_k})$ dla pewnych $i_1, ..., i_k \in I$, $X_{i_j} \subseteq G_{i_j}$ otwarte. Ustalmy dowolny taki zbiór zawierający e, wtedy dla wszystkich $j = 1, ..., k$, $e_{i_j} \in X_{i_j}$, a zatem $e \in \varphi_{i_1}^{-1}(e_{i_1}) \cap ... \cap \varphi_{i_k}^{-1}(e_{i_k}) \subseteq U$. Zbiór I jest skierowany, a więc istnieje $r \in I$, $i_1, ..., i_k \leqslant r$, a wtedy dla każdego $j = 1, ..., k$, $\varphi_{i_j} = \varphi_{ri_j}\varphi_r$, stąd $\ker\varphi_r \leqslant \ker\varphi_{i_j}$.
Zauważmy więc, że $e \in \ker\varphi_r \subseteq \varphi_{i_1}^{-1}(e_{i_1}) \cap ... \cap \varphi_{i_k}^{-1}(e_{i_j}) \subseteq U$. Dodatkowo φ_i są ciągłe, a więc $\ker\varphi_r$ jest otwarto-domknięty jako przeciwobraz zbioru otwarto-domkniętego. Wobec dowolności zbioru U, $\ker\varphi_i$ są bazą otwartych otoczeń e.

Na mocy założenia istnieje izomorfizm (topologiczny) $\Phi : \varprojlim_{i\in I} G_i \to G$, a zatem rodzina zbiorów $\{N_i = \Phi(\ker\varphi_i) : i \in I\}$ tworzy bazę otwartych otoczeń elementu neutralnego w G, taką że dla każdych $i > j \in I$, $N_i \leqslant N_j$.

Pozostaje pokazać, że dla każdego $i \in I$, $G_i \cong G/N_i$. Pokażemy najpierw, że dla każdego $i \in I$, $\varphi_i : \varprojlim_{i\in I} G_i \to G_i$ jest surjekcją.
Ustalmy dowolny $k \in I$, $a_k \in G_k$. Dla każdego $k < j \in I$ niech

$$S_j := \{(g_i)_{i\in I} \in \textstyle\prod_{i\in I} G_i : a_k = g_k \text{ oraz dla wszystkich } n < j,\ g_n = \varphi_{jn}(g_j)\}.$$

S_j jest niepusty, ponieważ z założenia dla wszystkich $n < j \in I$, φ_{jn} są surjekcjami. Zauważmy, że $\prod_{i\in I} G_i$ jest zwarty i każdy S_j jest w nim domknięty, ponieważ każda z grup G_i jest dyskretna. Wystarczy sprawdzić, że $\bigcap_{k<n\in I} S_n$ jest niepusty.

Sprawdzimy, że $\{S_n : k < n \in I\}$ ma własność skończonych przekrojów. Wtedy, jako rodzina domkniętych podzbiorów przestrzeni zwartej, będzie miała niepusty przekrój. Ustalmy dowolne $k < n_1, ..., n_s \in I$. Wtedy istnieje $n_1, ..., n_s < t \in I$, stąd $\emptyset \neq S_t \subseteq S_{n_1} \cap ... \cap S_{n_s}$. Zatem $\emptyset \neq \bigcap_{k<n\in I} S_k$, a więc istnieje $(g_i)_{i\in I} \in \varprojlim_{i\in I} G_i$, takie że $\varphi_k((g_i)_{i\in I}) = a_k$.

Ustalmy dowolny $i \in I$, wtedy φ_i jest surjekcją, a więc, na mocy zasadniczego twierdzenia o homomorfizmie grup, $G_i \cong \varprojlim_{i\in I} G_i/\ker\varphi_i \cong G/N_i$.

$\Longleftarrow$: Rozważmy system odwrotny grup skończonych $(G/N_i, \psi_{ij})_{i\geqslant j\in I}$, $\psi_{ij} : G/N_i \to G/N_j$, $\psi_{ij}(gN_i) = gN_j$, gdzie otwarto-domknięte $N_i \lhd G$ tworzą bazę otwartych otoczeń e.

Pokażemy, że $\Psi : G \to \varprojlim_{i\in I} G/N_i$, $\Psi(g) = (gN_i)_{i\in I}$ jest izomorfizmem. Łatwo widać, że Ψ przyjmuje wartości w $\varprojlim_{i\in I} G/N_i$.

Sprawdzimy najpierw, że $\bigcap_{i\in I} N_i = \{e\}$. Oczywiście $\{e\} \subseteq \bigcap_{i\in I} N_i$. Ustalmy dowolny $g \in G, g \neq e$. Z uwagi 2.8. mamy, że G jest Hausdorffa, a więc istnieje otwarte otoczenie $U \subseteq G$ elementu neutralnego e, takie że $g \notin U$. Z założenia istnieje $i \in I$, taki że $N_i \subseteq U$. Otrzymujemy więc, że $g \notin N_i$, czyli w szczególności $g \notin \bigcap_{i\in I} N_i$.

Mamy zatem, że $\bigcap\limits_{i\in I} N_i = \{e\}$. Stąd wnioskujemy, że Ψ jest monomorfizmem, ponieważ $\ker\Psi = \bigcap_{i\in I} N_i = \{e\}$.

Sprawdzimy, że Ψ jest ciągłe. Zauważmy, że dla każdego $i \in I$, złożenie $\Psi\pi_i$, gdzie $\pi_i : \varprojlim\limits_{i\in I} G/N_i \to G/N_i$ jest rzutem na i-tą oś, jest ciągłe (jako odwzorowanie ilorazowe), a więc Ψ jest ciągłe.

Pozostaje sprawdzić, że Ψ jest surjekcją. Ustalmy dowolny $i \in I$, pokażemy, że $\pi_i(\Psi(G)) = G/N_i$.
$\subseteq$: jasne
$\supseteq$: Niech $gN_i \in G/N_i$. Wtedy $g \in G$, a więc $\pi_i(\Psi(g)) = gN_i$.
Mamy więc, że $\Psi(G) = \overline{\Psi(G)} = \varprojlim\limits_{i\in I} G/N_i$, a stąd Ψ jest surjekcją (uwaga 2.10.).

Pokazaliśmy, że Ψ jest izomorfizmem grup topologicznych i na mocy założenia mamy dla każdego $i \in I$, istnieje $\theta_i : G_i \xrightarrow{\cong} G/N_i$. Zdefiniujmy $\varphi_{ij} : G_i \to G_j$, $\varphi_{ij} = \theta_j^{-1}\psi_{ij}\theta_i$ dla dowolnych $i > j \in I$. Zdefiniowane w ten sposób funkcje są surjekcjami jako złożenia surjekcji. Wówczas dla dowolnych $i > j > k \in I$ mamy $\varphi_{jk}\varphi_{ij} = \theta_k^{-1}\psi_{jk}\theta_j\theta_j^{-1}\psi_{ij}\theta_i = \theta_k^{-1}\psi_{ik}\theta_i = \varphi_{ik}$, a więc $(G_i, \varphi_{ij})_{i>j\in I}$ jest systemem odwrotnym. Oczywiście dla dowolnych $i > j \in I$, poniższy diagram jest przemienny:

$$\begin{array}{ccc} G_i & \xrightarrow{\theta_i} & G/N_i \\ {\scriptstyle\varphi_{ij}}\downarrow & & \downarrow{\scriptstyle\psi_{ij}} \\ G_j & \xrightarrow{\theta_j} & G/N_j \end{array}$$

a więc $\varprojlim\limits_{i\in I} G_i \cong \varprojlim\limits_{i\in I} G/N_i$ (lemat 2.9.), czyli $\varprojlim\limits_{i\in I} G_i \cong G$. □

3 Elementy teorii Galois

W początkowej części rozdziału przypomnimy podstawowe definicje oraz fakty dotyczące klasycznej teorii Galois, z których korzystać będziemy w dalszej części pracy. W szczególności sformułujemy zasadnicze twierdzenie teorii Galois dla rozszerzeń skończonych. Następnie zapoznamy czytelnika z topologią Krulla, co pozwoli nam na późniejsze uogólnienie w.w. twierdzenia na rozszerzenia nieskończone. Na koniec pokażemy, jak przy pomocy grup proskończonych, możemy obliczać grupy Galois dla nieskończonych rozszerzeń, co będzie kluczowe w dalszej części pracy.

3.1 Klasyczna teoria Galois

Niech L będzie rozszerzeniem ciała K. Element $a \in L$ nazywamy *algebraicznym* względem ciała K, gdy istnieje niezerowy wielomian $f \in K[x]$, taki że $\hat{f}(a) = 0$. Ciało L nazywamy *rozszerzeniem algebraicznym* ciała K, jeżeli każdy element L jest algebraiczny względem K. Załóżmy ponadto, że każdy niestały wielomian $f \in L[x]$ ma pierwiastek w L. Wówczas L nazywamy *algebraicznie domkniętym. Algebraicznym domknięciem* ciała K nazywamy algebraiczne rozszerzenie K, które jest algebraicznie domknięte i oznaczamy przez $\overline{K}$. Przypomnijmy ponadto, że *ciałem rozkładu*

wielomianu $f \in K[x]$ nazywamy ciało $K(a_1, ..., a_n)$, gdzie $a_1, ..., a_n$ są wszystkimi pierwiastkami f.

Definicja 3.1. Niech L będzie rozszerzeniem ciała K. Dowolny automorfizm $\varphi : L \to L$ będziemy nazywać K-automorfizmem, gdy $\varphi|_K = id_K$.

Twierdzenie 3.2. *Dla każdego ciała K istnieje jego algebraiczne domknięcie. Jest ono jedyne (z dokładnością do K-izomorfizmu).*

Dowód. [1], 2.1.2., twierdzenie 5 i wniosek 2 □

Poniżej sformułujemy dwa lematy, które będą nam niezbędne m.in. przy obliczeniach grup Galois pojawiających się w rozdziale 4.

Lemat 3.3. *Niech $\varphi : K_1 \to K_2$ będzie izomorfizmem ciał i $\overline{\varphi} : K_1[x] \to K_2[x]$ będzie odpowiadającym mu izomorfizmem pierścieni wielomianów. Jeżeli $f_1 \in K_1[x]$ jest nierozkładalny nad K_1, f_1 ma pierwiastek a_1 w rozszerzeniu L_1 ciała K_1 i wielomian $f_2 = \overline{\varphi}(f_1)$ ma pierwiastek a_2 w rozszerzeniu L_2 ciała K_2 to istnieje izomorfizm $\varphi \subseteq \varphi' : L_1 \to L_2$ taki, że $\varphi'(a_1) = a_2$.*

Dowód. [1], 2.1.1., twierdzenie 1 □

Lemat 3.4. *Jeśli $f \in K[x]$ jest wielomianem nierozkładalnym i w pewnych rozszerzeniach L_1, L_2 ciała K wielomian f ma pierwiastki odpowiednio a_1, a_2, to istnieje K-izomorfizm $\varphi : K(a_1) \to K(a_2)$, taki że $\varphi(a_1) = a_2$.*

Dowód. [1], 2.1.1. lemat 2 □

Przypomnijmy, że dla dowolnych ciał $K \subseteq L$, *stopniem rozszerzenia* L względem K nazywamy wymiar L jako przestrzeni liniowej nad K i oznaczamy przez $[L : K]$.

Lemat 3.5. *Jeśli K, L, M są ciałami, $K \subseteq L \subseteq M$, to $[M : K] = [L : K][M : L]$.*

Dowód. [1], 1.3.2., twierdzenie 3 □

Przejdziemy teraz do pojęcia rozszerzenia normalnego oraz rozdzielczego.

Niech K będzie ciałem, F będzie rodziną wielomianów należących do $K[x]$, zaś $A := \{a \in \overline{K} : \bigvee_{f \in F} \hat{f}(a) = 0\}$. Wtedy $K(A)$ jest złożeniem ciał rozkładu wielomianów należących do F. W tej sytuacji $K \subseteq K(A)$ nazywamy *rozszerzeniem normalnym* ciała K.

Lemat 3.6. *Niech L będzie rozszerzeniem algebraicznym K. Wtedy następujące warunki są równoważne:*

1. *L jest rozszerzeniem normalnym ciała K*
2. *Jeśli $\varphi : L \underset{K}{\to} \overline{K}$ jest zanurzeniem, to $\varphi(L) = L$.*
3. *Jeśli wielomian nierozkładalny $f \in K[x]$ ma pierwiastek w L, to rozkłada się w L na czynniki liniowe.*

Dowód. [1], 2.2.1., twierdzenie 1 □

Omówimy teraz rozszerzenia rozdzielcze. Przypomnijmy, że dla dowolnego $a \in \overline{K}$, *wielomianem minimalnym* a nad K nazywamy unormowany, nierozkładalny nad K wielomian należący do $K[x]$, którego pierwiastkiem jest a. Rozszerzenie algebraiczne $K \subseteq L$ nazywamy *rozdzielczym*, gdy każdy $a \in L$ jest elementem rozdzielczym względem K, tj. wielomian minimalny a nad K nie ma pierwiastków wielokrotnych w $\overline{K}$.

Uwaga 3.7. Niech $K \subseteq L$ będzie algebraiczne. Wówczas zbiór

$$\mathrm{sep}_L(K) := \{a \in L : \text{a jest rozdzielczy nad } K\}$$

jest ciałem ([1], 1.3.5., twierdzenie 16). Przez $\overline{K}^{sep}$ oznaczać będziemy $\mathrm{sep}_{\overline{K}}(K)$.

Lemat 3.8. *Jeżeli* $char(K) = 0$*, to każde rozszerzenie algebraiczne ciała* K *jest rozdzielcze.*

Dowód. [1], 1.3.5. □

Możemy teraz wprowadzić pojęcie rozszerzenia Galois. Niech $K \subseteq L$ będzie rozszerzeniem algebraicznym. Zauważmy, że zbiór K-automorfizmów ciała L ze składaniem tworzy grupę. Nazywamy ją *grupą Galois* rozszerzenia $K \subseteq L$ i oznaczamy przez $\mathrm{Gal}(L/K)$.

Definicja 3.9. Rozszerzenie algebraiczne $K \subseteq L$ nazywamy *rozszerzeniem Galois*, gdy dla każdego $a \in L \setminus K$, istnieje automorfizm $\varphi \in \mathrm{Gal}(L/K)$, taki że $\varphi(a) \neq a$.

Poniżej podamy ważną charakteryzację rozszerzeń Galois.

Twierdzenie 3.10. $K \subseteq L$ *jest rozszerzeniem Galois wtedy i tylko wtedy, gdy jest rozszerzeniem normalnym i rozdzielczym.*

Dowód. [1], 2.2.3., twierdzenie 4 □

Ponadto, w dalszej części pracy, ważne będą dla nas następujące własności rozszerzeń Galois.

Lemat 3.11. *Jeśli* $K \subseteq L$ *skończone (tj.* $[L : K] < \infty$*), to* L *jest rozszerzeniem Galois ciała* K *wtedy i tylko wtedy, gdy* $|\mathrm{Gal}(L/K)| = [L : K]$.

Dowód. [1], 2.2.3., wniosek 1 □

Twierdzenie 3.12. *(Artin) Niech* G *będzie skończoną podgrupą* $\mathrm{Aut}(L)$*. Wtedy* $L^G \subseteq L$ *jest rozszerzeniem Galois,* $G = \mathrm{Gal}(L/L^G)$ *oraz* $[L : L^G] = |G|$.

Dowód. [1], 2.2.2. □

Możemy teraz przejść do zasadniczego twierdzenia teorii Galois dla rozszerzeń skończonych.

Twierdzenie 3.13. *(Zasadnicze twierdzenie teorii Galois dla rozszerzeń skończonych) Niech L będzie skończonym rozszerzeniem Galois ciała K, $\mathcal{A}$ będzie rodziną wszystkich ciał M pośrednich między K i L oraz $\mathcal{B}-$ rodziną wszystkich podgrup* $\mathrm{Gal}(L/K)$*. Definiujemy odwzorowania*

$$\Lambda : \mathcal{A} \to \mathcal{B},\ \Lambda(M) = \mathrm{Gal}(L/M),$$

$$\Gamma : \mathcal{B} \to \mathcal{A},\ \Gamma(H) = L^H.$$

Wówczas Λ jest bijekcją i $\Lambda = \Gamma^{-1}$.

Dowód. [1], 2.2.4., twierdzenie 6 □

Wniosek 3.14. *Jeżeli L jest rozszerzeniem Galois ciała K, to ciało pośrednie $K \subseteq M \subseteq L$ jest rozszerzeniem Galois ciała K wtedy i tylko wtedy, gdy grupa* $\mathrm{Gal}(L/M)$ *jest podgrupą normalną grupy* $\mathrm{Gal}(L/K)$*. W tym przypadku grupa* $\mathrm{Gal}(M/K)$ *jest izomorficzna z grupą* $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$*.*

Dowód. [1], 2.2.4., twierdzenie 7 □

Odpowiedniość ta nie zachodzi dla wszystkich rozszerzeń nieskończonych. W szczególności za kontrprzykład może posłużyć rozszerzenie $\mathbb{Q} \subseteq \mathbb{Q}(\{\sqrt{p} : p \text{ jest liczbą pierwszą}\})$ ([7], 5.4.18). W dalszej części rozdziału skupimy się na częściowym uogólnieniu powyższego twierdzenia na rozszerzenia nieskończone. Aby tego dokonać, będziemy musieli rozważać grupę Galois ze specjalną topologią, tj. topologią Krulla.

3.2 Topologia Krulla

Załóżmy, że $K \subseteq L$ jest rozszerzeniem Galois. Przez $\mathcal{L}$ oznaczmy rodzinę wszystkich ciał pośrednich $K \subseteq M \subseteq L$, takich że $K \subseteq M$ jest skończonym rozszerzeniem Galois. Wówczas istnieje jedyna topologia na $\mathrm{Gal}(L/K)$ kompatybilna ze strukturą grupową $\mathrm{Gal}(L/K)$ wyznaczona przez bazę otoczeń elementu neutralnego $\{\mathrm{Gal}(L/M) : M \in \mathcal{L}\}$ ([3], 2.11). Topologię tę nazywamy *topologią Krulla*.

Uwaga 3.15. Jeśli $L \subseteq K$ jest skończonym rozszerzeniem Galois, to topologia Krulla grupy $\mathrm{Gal}(L/K)$ jest dyskretna.

3.3 Zasadnicze twierdzenie Galois w wersji nieskończonej

Rozważenie grupy Galois jako grupy topologicznej z topologią Krulla pozwoli nam na następujące ugólnienie twierdzenia 3.13:

Twierdzenie 3.16. *Niech L będzie rozszerzeniem Galois ciała K. Wówczas przyporządkowanie $M \mapsto \mathrm{Gal}(L/M)$ zadaje bijekcję pomiędzy rodziną ciał pośrednich $K \subseteq M \subseteq L$, a rodziną domkniętych podgrup grupy* $\mathrm{Gal}(L/K)$*. Odwzorowaniem odwrotnym jest wówczas przyporządkowanie $H \mapsto L^H$.*

Dowód. [2], 1.3.1. □

Wniosek 3.17. *Niech $K \subseteq L$ będzie rozszerzeniem Galois. Dla każdej domkniętej $H \leqslant \mathrm{Gal}(L/K)$, $H \trianglelefteq \mathrm{Gal}(L/K)$ wtedy i tylko wtedy, gdy $K \subseteq L^H$ jest rozszerzeniem Galois. Ponadto dla dowolnego rozszerzenia Galois $K \subseteq M$ zawartego w L,*

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M).$$

Dowód. [3], 2.11.3. □

3.4 Zastosowanie grup proskończonych w teorii Galois

Sformułowany poniżej lemat będzie naszym głównym narzędziem przy obliczaniu konkretnych przykładów grup Galois pojawiających się w dalszej części pracy.

Lemat 3.18. *Niech $K \subseteq L$ będzie rozszerzeniem Galois, a $\{K_i\}_{i\in I}$ będzie rodziną skończonych rozszerzeń Galois ciała K zawartych w L indeksowanych zbiorem skierowanym $(I, \leqslant)$, takich że $\bigcup_{i\in I} K_i = L$. Wówczas grupa Galois $\mathrm{Gal}(L/K)$ z topologią Krulla jest topologicznie izomorficzna z grupą proskończoną $\varprojlim_{i\in I} \mathrm{Gal}(K_i/K)$, przy czym $\varprojlim_{i\in I} \mathrm{Gal}(K_i/K)$ jest granicą odwrotną $(\mathrm{Gal}(K_i/K), \psi_{ij})_{i\geqslant j\in I}$,*

$$\begin{aligned} \psi_{ij}\colon \mathrm{Gal}(K_i/K) &\to \mathrm{Gal}(K_j/K) \\ \sigma &\mapsto \sigma|_{K_j}. \end{aligned}$$

Dowód. [2], 1.3. □

3.5 Szczególne klasy rozszerzeń Galois

Przejdziemy teraz do zdefiniowania pewnych klas rozszerzeń Galois, które będziemy rozważać w rozdziałach 6 i 8.

Definicja 3.19. Niech $K \subseteq L$ będzie rozszerzeniem Galois. Jeśli $\mathrm{Gal}(L/K)$ jest grupą rozwiązalną, to $K \subseteq L$ nazywamy *rozszerzeniem rozwiązalnym*. Jeśli ponadto $\mathrm{Gal}(L/K)$ jest grupą abelową, to $K \subseteq L$ nazywamy *rozszerzeniem abelowym*.

4 Przykłady wyliczeń nieskończonych grup Galois

W tym rozdziale zaprezentujemy zastosowanie lematu 3.18. w praktyce, co dostarczy konkretnych przykładów grup proskończonych abelowych i rozwiązalnych, które są grupami Galois pewnych konkretnych rozszerzeń ciał.

Między innymi obliczymy grupy Galois dla pewnych klasycznych rozszerzeń $\mathbb{Q}$ takich jak $\mathbb{Q}$ rozszerzone o pierwiastki kwadratowe ze wszystkich liczb pierwszych oraz $\mathbb{Q}$ rozszerzone o wszystkie pierwiastki z jedynki. Ponadto wyliczymy grupę Galois dla domknięcia algebraicznego dowolnego ciała skończonego $\mathbb{F}_p$.

Przykład 4.1. Niech p będzie liczbą pierwszą oraz $\mathbb{Q}(\zeta_\infty) := \mathbb{Q}(\{\zeta_{p^n} : n \in \mathbb{N}_+\})$, gdzie ζ_{p^n} oznacza pierwiastek pierwotny z jedynki stopnia p^n. Obliczymy grupę

$$\mathrm{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}).$$

W szczególności okaże się ona być proskończoną grupą abelową.

Niech porządek $\leqslant$ na $\mathbb{N}_+$ będzie określony w naturalny sposób. Rozważmy system odwrotny $(\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}), \psi_{nm})_{n \geqslant m \in \mathbb{N}_+}$, gdzie dla dowolnych $n \geqslant m \in \mathbb{N}_+$:

$$\begin{aligned} \psi_{nm} \colon \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) &\to \mathrm{Gal}(\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}) \\ \sigma &\mapsto \sigma|_{\mathbb{Q}(\zeta_{p^m})}. \end{aligned}$$

Zauważmy, że $\mathbb{Q}(\zeta_\infty) = \bigcup\limits_{n \in \mathbb{N}_+} \mathbb{Q}(\zeta_{p^n})$. Ponadto dla każdego $n \in \mathbb{N}_+$, $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_{p^n})$ jest ciałem rozkładu wielomianu cyklotomicznego $x^{p^n} - 1$, a więc jest skończonym rozszerzeniem Galois (3.8., 3.10.). Wówczas z lematu 3.18. mamy, że

$$\mathrm{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) \cong \varprojlim_{n \in \mathbb{N}_+} \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}).$$

Rozważmy zbiór $(\mathbb{Z}^*_{p^n}, \varphi_{nm})_{n \geqslant m \in \mathbb{N}_+}$, gdzie porządek $\leqslant$ na $\mathbb{N}_+$ jest określony w naturalny sposób oraz dla dowolnych $n \geqslant m \in \mathbb{N}_+$ homomorfizm φ_{nm} jest zdefiniowany następująco:

$$\begin{aligned} \varphi_{nm} \colon \mathbb{Z}^*_{p^n} &\to \mathbb{Z}^*_{p^m} \\ a &\mapsto r_{p^m}(a). \end{aligned}$$

Sprawdzimy, że $(\mathbb{Z}^*_{p^n}, \varphi_{nm})_{n \geqslant m \in \mathbb{N}_+}$ jest systemem odwrotnym.

Ustalmy dowolne $k \leqslant m \leqslant n \in \mathbb{N}_+$ oraz $x \in \mathbb{Z}^*_{p^n}$. Zauważmy, że p^k dzieli p^m, czyli $p^m = ap^k$ dla pewnego $a \in \mathbb{N}$. Stąd $x = bp^m + r = abp^k + r$ dla pewnych $b, r \in \mathbb{N}, r < p^m$, a więc $r_{p^k}(x) = r_{p^k}(r) = r_{p^k}(r_{p^m}(x))$. Wobec tego $\varphi_{mk}(\varphi_{nm}(x)) = r_{p^k}(r_{p^m}(x)) = r_{p^k}(x) = \varphi_{nk}(x)$. Z dowolności n, m, k dostajemy, że $(\mathbb{Z}^*_{p^n}, \varphi_{nm})_{n \geqslant m \in \mathbb{N}_+}$ jest systemem odwrotnym.

Przejdziemy do pokazania, że

$$\varprojlim_{n \in \mathbb{N}_+} \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong \varprojlim_{n \in \mathbb{N}_+} \mathbb{Z}^*_{p^n}.$$

Zaczniemy od sprawdzenia, że dla każdego $n \in \mathbb{N}_+$, $\mathbb{Z}^*_{p^n} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$.

Zauważmy, że $\{\zeta^k_{p^n} : k \in \mathbb{Z}^*_{p^n}\}$ jest zbiorem pierwiastków wielomianu cyklotomicznego $\Phi_{p^n}(x)$, który na mocy lematu Gaussa jest nierozkładalny. Oczywiście $\{\zeta^k_{p^n} : k \in \mathbb{Z}^*_{p^n}\}$ jest zbiorem pierwiastków pierwotnych z 1 stopnia p^n, a zatem dla każdego $k \in \mathbb{Z}^*_{p^n}$, $\mathbb{Q}(\zeta_{p^n}) = \mathbb{Q}(\zeta^k_{p^n})$. Z lematu 3.4. otrzymujemy więc, że dla każdego $k \in \mathbb{Z}^*_{p^n}$, istnieje $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$, taki że $\sigma_k(\zeta_{p^n}) = \zeta^k_{p^n}$. Możemy zatem zdefiniować funkcję:

$$\begin{aligned} \theta_n \colon \mathbb{Z}^*_{p^n} &\to \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \\ k &\mapsto \sigma_k, \end{aligned}$$

gdzie $\sigma_k(\zeta_{p^n}) := \zeta_{p^n}^k$. Sprawdzimy, że θ_n jest izomorfizmem.

θ_n jest homomorfizmem, ponieważ dla dowolnych $l, k \in \mathbb{Z}_{p^n}^*$, takich że $kl = ap^n + r$ dla pewnych $a, r \in \mathbb{N}, r < p^n$, mamy $\sigma_{k\cdot p^n l}(\zeta_{p^n}) = \zeta_{p^n}^{k\cdot p^n l} = \zeta_{p^n}^{ap^n}\zeta_{p^n}^r = \zeta_{p^n}^{ap^n+r} = \zeta_{p^n}^{kl} = \sigma_k(\sigma_l(\zeta_{p^n}))$.

Ponadto θ_n jest monomorfizmem, ponieważ $\sigma_k = \mathrm{id}$ wtedy i tylko wtedy, gdy $\sigma_k(\zeta_{p^n}) = \zeta_{p^n}$, co jest równoważne $k = 1$.

Przypomnijmy, że wielomian cyklotomiczny $\Phi_{p^n}(x)$ jest nierozkładalny nad $\mathbb{Q}$ i ma stopień $\varphi(p^n)$ (gdzie przez φ rozumiemy funkcję Eulera). Korzystając z lematu 3.11. otrzymujemy, że $|\operatorname{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})| = \varphi(p^n) = |\mathbb{Z}_{p^n}^*|$, czyli θ_n jest "na". Podsumowując, θ_n jest izomorfizmem.

Ustalmy dowolne $n \geqslant m \in \mathbb{N}_+$. Pokażemy, że poniższy diagram jest przemienny:

$$\begin{array}{ccc} \mathbb{Z}_{p^m}^* & \xleftarrow{\varphi_{nm}} & \mathbb{Z}_{p^n}^* \\ {\scriptstyle\theta_m}\downarrow & & \downarrow{\scriptstyle\theta_n} \\ \operatorname{Gal}(\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}) & \xleftarrow{\psi_{nm}} & \operatorname{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \end{array}$$

Ustalmy dowolny $k \in \mathbb{Z}_{p^n}^*$. Wystarczy sprawdzić, że $\psi_{nm}(\theta_n(k))(\zeta_{p^m}) = \theta_m(\varphi_{nm}(k))(\zeta_{p^m})$. Zauważmy, że dla pewnych $a, b, s \in \mathbb{N}, b < p^m$, $k = ap^m + b$ oraz $\zeta_{p^m} = \zeta_{p^n}^s$. Wówczas

$$\psi_{nm}(\theta_n(k))(\zeta_{p^m}) = \theta_n(k)(\zeta_{p^n}^s) = \zeta_{p^n}^{ks} = \zeta_{p^m}^{ap^m}\zeta_{p^m}^b = \theta_m(\varphi_{nm}(k))(\zeta_{p^m}).$$

Z dowolności k mamy więc, że $\psi_{nm}\theta_n = \theta_m\varphi_{nm}$, tj. diagram jest przemienny. Wówczas $\varprojlim_{n\in\mathbb{N}_+} \operatorname{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_{p^n}^*$ (lemat 2.9.), a stąd $\operatorname{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) \cong \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_{p^n}^*$. Otrzymaliśmy więc przykład proskończonej grupy abelowej, która ma realizację jako grupa Galois nad $\mathbb{Q}$. Zauważmy ponadto, że w ten sposób dostajemy przykład rozszerzenia abelowego.

Uwaga 4.2. Załóżmy, że porządek $\leqslant$ na $\mathbb{N}_+$ jest zadany przez relację podzielności, tj. dla wszystkich $n, m \in \mathbb{N}_+$, $m \leqslant n \iff m|n$. Wtedy $(\mathbb{N}_+, \leqslant)$ jest zbiorem skierowanym. Niech $\mathbb{Q}(\zeta_\infty)$ będzie rozszerzeniem ciała $\mathbb{Q}$ o wszystkie pierwiastki pierwotne z jedności. Wówczas, powtarzając powyższe rozumowanie, otrzymujemy, że $\operatorname{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) \cong \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_n^*$.

Przykład 4.3. Załóżmy, że p jest liczbą pierwszą. Przez $\overline{\mathbb{F}_p}$ oznaczymy algebraiczne domknięcie ciała $\mathbb{F}_p$. Obliczymy $\operatorname{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. W szczególności okaże się ona być proskończoną grupą abelową.

Dla każdego $n \in \mathbb{N}_+$, $\mathbb{F}_{p^n}$ jest ciałem rozkładu $W_{p^n}(x) := x^{p^n-1} - 1$ nad $\mathbb{F}_p$. Zauważmy, że $W'_{p^n}(x) = (p^n - 1)x^{p^n-2} = -x^{p^n-2}$. Mamy więc, że dla każdego $a \in \mathbb{F}_{p^n}$, takiego że $\hat{W_{p^n}}(a) = 0$, wartość funkcji wielomianowej $\hat{W'_{p^n}}$ liczonej w a jest różna od 0, czyli $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ jest rozdzielcze ([7], 3.2.1.). Otrzymujemy zatem, że $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ jest skończonym rozszerzeniem Galois (3.10.). Ponadto $\overline{\mathbb{F}_p} = \bigcup_{n\in\mathbb{N}_+} \mathbb{F}_{p^n}$, czyli z lematu 3.18. dostajemy, że

$$\operatorname{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \varprojlim_{n\in\mathbb{N}_+} \operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p),$$

gdzie $(\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p), \psi_{nm})_{n \geqslant m \in \mathbb{N}_+}$ jest systemem odwrotnym nad zbiorem skierowanym $\mathbb{N}_+$ uporządkowanym przez relację podzielności, zaś homomorfizmy ψ_{nm} są zdefiniowane następująco:

$$\begin{aligned} \psi_{nm} \colon (\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) &\to (\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \\ \sigma &\mapsto \sigma|_{\mathbb{F}_{p^m}}. \end{aligned}$$

Rozważmy automorfizm Frobeniusa:

$$\begin{aligned} \mathrm{Fr}_p \colon \mathbb{F}_{p^n} &\to \mathbb{F}_{p^n} \\ x &\mapsto x^p \end{aligned}$$

Zauważmy, że $\mathbb{F}_{p^n}^{\langle \mathrm{Fr}_p \rangle} = \mathbb{F}_p$. Wówczas $\langle \mathrm{Fr}_p \rangle = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^n}^{\langle \mathrm{Fr}_p \rangle}) = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ (twierdzenie 3.12.), w wyniku czego otrzymujemy następujący izomorfizm:

$$\begin{aligned} \theta_n \colon \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) &\to \mathbb{Z}_n \\ \mathrm{Fr}_p &\mapsto 1. \end{aligned}$$

Podobnie jak w przykładzie 4.1. sprawdzamy, że zbiór $(\mathbb{Z}_n, \varphi_{nm})_{n \geqslant m \in \mathbb{N}_+}$, gdzie $\mathbb{N}_+$ jest uporządkowany przez relację podzielności oraz dla dowolnych $n \geqslant m \in \mathbb{N}_+$,

$$\begin{aligned} \varphi_{nm} \colon \mathbb{Z}_n &\to \mathbb{Z}_m \\ a &\mapsto r_m(a) \end{aligned}$$

jest systemem odwrotnym. Przejdziemy teraz do pokazania, że

$$\varprojlim_{n \in \mathbb{N}_+} \mathbb{Z}_n \cong \varprojlim_{n \in \mathbb{N}_+} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}).$$

Ustalmy dowolne $n \geqslant k \in \mathbb{N}_+$. Sprawdzimy, że poniższy diagram jest przemienny:

$$\begin{array}{ccc} \mathbb{Z}_k & \xleftarrow{\varphi_{nk}} & \mathbb{Z}_n \\ {\scriptstyle \theta_k}\downarrow & & \downarrow{\scriptstyle \theta_n} \\ \mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p) & \xleftarrow{\psi_{nk}} & \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \end{array}$$

Weźmy dowolne $s \in \mathbb{Z}_n, x \in \mathbb{F}_{p^k}$. Niech $a, r \in \mathbb{N}, r < k$ będą takie że $s = ak + r$. Wówczas $\psi_{nk}\theta_n(s)(x) = x^{p^s} = x^{p^r} = \theta_k\varphi_{nk}(s)(x)$. Z dowolności s mamy więc, że $\psi_{nk}\theta_n = \theta_k\varphi_{nk}$, tj. diagram jest przemienny. Z lematu 2.9. otrzymujemy wówczas, że $\varprojlim_{n \in \mathbb{N}_+} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \varprojlim_{n \in \mathbb{N}_+} \mathbb{Z}_n$. Stąd $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \varprojlim_{n \in \mathbb{N}_+} \mathbb{Z}_n$. Otrzymaliśmy więc przykład proskończonej grupy abelowej, która ma realizację jako grupa Galois nad $\mathbb{F}_p$. Zauważmy ponadto, że w ten sposób dostajemy kolejny przykład rozszerzenia abelowego.

Przykład 4.4. Rozważmy ciało $\mathbb{Q}(\sqrt{p_\infty}) := \mathbb{Q}(\{\sqrt{p_i} : i \in \mathbb{N}_+\})$, tj. ciało $\mathbb{Q}$ rozszerzone o zbiór pierwiastków kwadratowych ze wszystkich liczb pierwszych. Obliczymy $\mathrm{Gal}(\mathbb{Q}(\sqrt{p_\infty})/\mathbb{Q})$. Podobnie jak w poprzednich przykładach okaże się ona być proskończoną grupą abelową. Zaczniemy od pokazania, że dla dowolnego $n \in \mathbb{N}_+$,

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}) \cong \prod_{i=1}^{n} \mathbb{Z}_2.$$

Definicja 4.5. Niech K będzie dowolnym ciałem. Elementy $d_1, ..., d_k \in K^*$ nazywamy *2-niezależnymi*, gdy dla każdych $a_1, ..., a_k \in \mathbb{Z}$, jeśli $d_1^{a_1}...d_k^{a_k} \in K^2$, to każdy a_i jest podzielny przez 2.

Przedstawimy teraz ważną własność elementów 2-niezależnych, z której korzystać będziemy również w rozdziale 8.

Lemat 4.6. *Niech K będzie dowolnym ciałem charakterystyki 0. Dla każdych $d_1, ..., d_n \in K^*$ $d_1, ..., d_n$ są 2-niezależne w K wtedy i tylko wtedy, gdy $[K(\sqrt{d_1}, ..., \sqrt{d_n}) : K] = 2^n$.*

Dowód. Ustalmy dowolne $d_1, ..., d_n \in K^*$.
$\Longleftarrow$ Załóżmy a.a., że $d_1, ..., d_n$ są 2- zależne w K. Z definicji to oznacza, że dla pewnych $a_1, ..., a_n \in \mathbb{Z}$ istnieją $q \in K, 1 \leqslant i \leqslant n$, takie że $q^2 = d_1^{a_1}...d_n^{a_n}$ i 2 nie dzieli a_i. Bez straty ogólności $i = n$. Wtedy $a_n = 2b + 1$ dla pewnego $b \in \mathbb{Z}$. Zauważmy, że $d_n = q^2 d_n^{-2b}(d_1^{a_1}...d_{n-1}^{a_{n-1}})^{-1}$, czyli $\sqrt{d_n} \in K(\sqrt{d_1}, ..., \sqrt{d_{n-1}})$. Wówczas $[K(\sqrt{d_1}, ..., \sqrt{d_n}) : K] < [K(\sqrt{d_1}, ..., \sqrt{d_{n-1}}) : K] \leqslant 2^{n-1}$, sprzeczność, ponieważ z założenia $[K(\sqrt{d_1}, ..., \sqrt{d_n}) : K] = 2^n$.
$\Longrightarrow$ Z założenia $d_1, \ldots, d_n \in K$, czyli $[K(\sqrt{d_1}, ..., \sqrt{d_n}) : K] \leqslant 2^n$. Pokażemy przeciwną nierówność. Załóżmy a.a., że $[K(\sqrt{d_1}, ..., \sqrt{d_n}) : K] < 2^n$. To oznacza, że istnieje $1 < i \leqslant n$, taki że $\sqrt{d_i} \in K(\sqrt{d_1}, ..., \sqrt{d_{i-1}})$ (w przeciwnym przypadku otrzymalibyśmy ciąg rozszerzeń stopnia 2 każde:

$$K \subseteq K(\sqrt{d_1}) \subseteq K(\sqrt{d_1})(\sqrt{d_2}) \subseteq ... \subseteq K(\sqrt{d_1}, ..., \sqrt{d_{n-1}})(\sqrt{d_n}),$$

czyli $[K(\sqrt{d_1}, ..., \sqrt{d_n}) : K] = 2^n$).

Niech j będzie najmniejszym takim indeksem, a $J = \{j_1, ..., j_k\}$ będzie minimalnym podzbiorem $\{1, ..., j-1\}$, takim że $\sqrt{d_j} \in K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_k}})$. Z minimalności j, dla każdego $j_i \in J$, $x^2 - d_{j_i}$ jest nierozkładalny nad $K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_{i-1}}}, \sqrt{d_{j_{i+1}}}, ..., \sqrt{d_{j_k}})$, a więc istnieje $\sigma_{j_i} \in \mathrm{Gal}(K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_k}})/K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_{i-1}}}, \sqrt{d_{j_{i+1}}}, ..., \sqrt{d_{j_k}})$, taki że $\sigma_{j_i}(\sqrt{d_{j_s}}) = (-1)^{\delta_{is}}\sqrt{d_{j_s}}$ (gdzie δ_{is} jest funkcją Diraca). Zauważmy, że $K \subseteq K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_{i-1}}}, \sqrt{d_{j_{i+1}}}, ..., \sqrt{d_{j_k}})$, a więc $\sigma_{j_i} \in \mathrm{Gal}(K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_k}})/K)$.

Pokażemy, że dla każdego $j_i \in J$ i każdego $a \in K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_k}})$, $\sigma_{j_i}(a) = a$ wtedy i tylko wtedy, gdy $a \in K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_{i-1}}}, \sqrt{d_{j_{i+1}}}, ..., \sqrt{d_{j_k}})$.

$\Longleftarrow$ Oczywiste, $\sigma_{j_i} \in \mathrm{Gal}(K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_k}})/K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_{i-1}}}, \sqrt{d_{j_{i+1}}}, ..., \sqrt{d_{j_k}}))$.

$\Longrightarrow$ Załóżmy nie wprost, że a należy do $K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_k}})$, $\sigma_{j_i}(a) = a$ oraz a nie należy do $K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_{i-1}}}, \sqrt{d_{j_{i+1}}}, ..., \sqrt{d_{j_k}})$.

Z definicji, $a = \hat{f}(\sqrt{d_{j_i}})$, gdzie $f \in K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_{i-1}}}, \sqrt{d_{j_{i+1}}}, ..., \sqrt{d_{j_k}})[x]$, a $\hat{f}$ jest odpowiadającą funkcją wielomianową. Przypomnijmy, że $d_{j_i} \in K$, stąd $\hat{f}(\sqrt{d_{j_i}}) = \hat{g}(\sqrt{d_{j_i}})$, dla pewnego $g = (g_k)_{k=0}^{\infty} \in K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_{i-1}}}, \sqrt{d_{j_{i+1}}}, ..., \sqrt{d_{j_k}})[x]$ stopnia 1. Wówczas

$g_0 + g_1(\sqrt{d_{j_i}}) = a = \sigma_{j_i}(a) = g_0 - g_1(\sqrt{d_{j_i}})$, zatem $g_1(\sqrt{d_{j_i}}) = 0$, a więc $a = g_0 \in K(\sqrt{d_{j_1}}, ..., \sqrt{d_{j_{i-1}}}, \sqrt{d_{j_{i+1}}}, ..., \sqrt{d_{j_k}})$, sprzeczność.

Zauważmy, że z powyższej równoważności mamy, że dla każdego $j_i \in J$, $\sigma_{j_i}(\sqrt{d_j}) = -\sqrt{d_j}$, ponieważ w przeciwnym przypadku otrzymalibyśmy sprzeczność z minimalnością zbioru J. Wówczas, dla każdego $j_i \in J$, $\sigma_{j_i}(\frac{\sqrt{d_j}}{\sqrt{d_{j_1}...d_{j_k}}}) = \frac{\sqrt{d_j}}{\sqrt{d_{j_1}...d_{j_k}}}$, czyli $\frac{\sqrt{d_j}}{\sqrt{d_{j_1}...d_{j_k}}} \in \bigcap_{j_i \in J} K(\{\sqrt{d_{j_1}}, ..., \sqrt{d_{j_k}}\} \setminus \{\sqrt{d_{j_i}}\}) = K$, co wynika z minimalności zbioru J. Wtedy oczywiście $d_j \in K^2$, co przeczy 2-niezależności $d_1, ..., d_n$ w K. □

Ustalmy dowolny $n \in \mathbb{N}_+$. Z założenia $p_1, \ldots, p_n$ są liczbami pierwszymi, a więc w szczególności są 2-niezależne w $\mathbb{Q}$. Wówczas z lematu 4.6. otrzymujemy, że dla dowolnego $j \leqslant n$, $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_j}) : \mathbb{Q}] = 2^j$.

Zauważmy, że wtedy $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_j}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{j-1}})] = 2$ (lemat 3.5.). W szczególności oznacza to, że wielomian $x^2 - p_j$ jest nierozkładalny nad $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{j-1}})$. Przypomnijmy, że j był dowolny, a zatem z lematu 3.3. otrzymujemy, że dla każdego ciągu $\overline{\epsilon} := (\epsilon_1, \ldots, \epsilon_n) \in \prod_{i=1}^{n} \mathbb{Z}_2$ istnieje $\sigma_{\overline{\epsilon}} \in \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q})$, taki że dla każdego $1 \leqslant i \leqslant n$, $\sigma_{\overline{\epsilon}}(\sqrt{p_i}) = (-1)^{\epsilon_i}(\sqrt{p_i})$.

Rozważmy homomofizm:

$$\begin{aligned} \theta_n \colon \prod_{i=1}^{n} \mathbb{Z}_2 &\to \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}) \\ \overline{\epsilon} &\mapsto \sigma_{\overline{\epsilon}}. \end{aligned}$$

Zauważmy, że $\theta_n(\epsilon_1, \ldots, \epsilon_n) = \mathrm{id}$ wtedy i tylko wtedy, gdy dla każdego $1 \leqslant i \leqslant n$, $\epsilon_i = 0$, czyli θ_n jest monomorfizmem. Ponadto $|\prod_{i=1}^{n} \mathbb{Z}_2| = 2^n = [\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}]$. Zatem z lematu 3.11. $|\prod_{i=1}^{n} \mathbb{Z}_2| = |\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q})|$. Mamy więc, że θ_n jest izomorfizmem.

Rozważmy system odwrotny $(\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}), \psi_{nm})_{n \geqslant m \in \mathbb{N}_+}$, gdzie porządek $\leqslant$ na $\mathbb{N}_+$ jest określony w naturalny sposób oraz dla dowolnych $n \geqslant m \in \mathbb{N}_+$:

$$\begin{aligned} \psi_{nm} \colon \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}) &\to \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m})/\mathbb{Q}) \\ \sigma &\mapsto \sigma|_{\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_m})}. \end{aligned}$$

Zauważmy, że $\mathbb{Q}(\sqrt{p_\infty}) = \bigcup_{n \in \mathbb{N}_+} \mathbb{Q}(\sqrt{p_1}, \ldots, p_n)$ oraz dla każdego $n \in \mathbb{N}_+$, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ jest skończonym rozszerzeniem Galois, jako ciało charakterystyki 0, będące jednocześnie ciałem rozkładu rodziny wielomianów o współczynnikach z $\mathbb{Q}$. Z lematu 3.18. mamy więc, że

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{p_\infty})/\mathbb{Q}) \cong \varprojlim_{n \in \mathbb{N}_+} \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}).$$

Weźmy ponadto system odwrotny $(\prod_{i=1}^{n}\mathbb{Z}_2, \varphi_{nm})_{n\geqslant m\in\mathbb{N}_+}$, gdzie gdzie porządek $\leqslant$ na $\mathbb{N}_+$ jest określony w naturalny sposób i dla dowolnych $n \geqslant m \in \mathbb{N}_+$:

$$\begin{aligned}\varphi_{nm}\colon \prod_{i=1}^{n}\mathbb{Z}_2 &\to \prod_{i=1}^{m}\mathbb{Z}_2\\ (\epsilon_1,\dots,\epsilon_m,\dots,\epsilon_n) &\mapsto (\epsilon_1,\dots,\epsilon_m).\end{aligned}$$

Pokażemy, że $\varprojlim_{n\in\mathbb{N}_+}\prod_{i=1}^{n}\mathbb{Z}_2 \cong \varprojlim_{n\in\mathbb{N}_+}\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})/\mathbb{Q})$. Ustalmy dowolne $m \leqslant n \in \mathbb{N}_+$. Sprawdzimy, że następujący diagram jest przemienny:

$$\begin{array}{ccc}\prod_{i=1}^{m}\mathbb{Z}_2 & \xleftarrow{\quad\varphi_{nm}\quad} & \prod_{i=1}^{n}\mathbb{Z}_2\\ \downarrow{\scriptstyle\theta_m} & & \downarrow{\scriptstyle\theta_n}\\ \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_m})/\mathbb{Q}) & \xleftarrow{\psi_{nm}} & \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})/\mathbb{Q})\end{array}$$

Ustalmy dowolny $\overline{\epsilon} := (\epsilon_1,\dots,\epsilon_n) \in \prod_{i=1}^{n}\mathbb{Z}_2$ oraz $1 \leqslant k \leqslant m$. Obliczamy $\theta_m(\varphi_{nm}(\overline{\epsilon}))(\sqrt{p_k}) = \theta_m(\epsilon_1,\dots,\epsilon_m)(\sqrt{p_k}) = (-1)^{\epsilon_k}\sqrt{p_k} = \theta_n(\overline{\epsilon})(\sqrt{p_k}) = \psi_{nm}(\theta_n(\overline{\epsilon}))(\sqrt{p_k})$. Każdy automorfizm $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_m})/\mathbb{Q})$ jest jednoznacznie wyznaczony przez $\sigma(\sqrt{p_1}),\dots,\sigma(\sqrt{p_m})$, a więc z dowolności $1 \leqslant k \leqslant m$, dostajemy że $\theta_m(\varphi_{nm}(\overline{\epsilon})) = \psi_{nm}(\theta_n(\overline{\epsilon}))$. Z dowolności $\overline{\epsilon} \in \prod_{i=1}^{n}\mathbb{Z}_2$ otrzymujemy przemienność diagramu. Przypomnijmy, że $n, m \in \mathbb{N}_+$ były dowolne, a więc z lematu 2.9. otrzymujemy $\varprojlim_{n\in\mathbb{N}_+}\prod_{i=1}^{n}\mathbb{Z}_2 \cong \varprojlim_{n\in\mathbb{N}_+}\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})/\mathbb{Q})$. Zatem $\varprojlim_{n\in\mathbb{N}_+}\prod_{i=1}^{n}\mathbb{Z}_2 \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{p_\infty})/\mathbb{Q})$.

Niech $\prod_{i=1}^{\infty}\mathbb{Z}_2$ będzie wyposażony w topologię produktową. Oczywiście wówczas $\prod_{i=1}^{\infty}\mathbb{Z}_2$ jest grupą topologiczną. Łatwo sprawdzić, że $\varprojlim_{n\in\mathbb{N}_+}\prod_{i=1}^{n}\mathbb{Z}_2 \cong \prod_{i=1}^{\infty}\mathbb{Z}_2$. Dokładniej funkcja:

$$\begin{aligned}\Psi\colon \prod_{i=1}^{\infty}\mathbb{Z}_2 &\to \varprojlim_{n\in\mathbb{N}_+}\prod_{i=1}^{n}\mathbb{Z}_2\\ (\epsilon_i)_{i=1}^{\infty} &\mapsto ((\epsilon_1),(\epsilon_1,\epsilon_2),\dots)\end{aligned}$$

jest topologicznym izomorfizmem grup. Jako konkluzję dostajemy, że $\mathrm{Gal}(\sqrt{p_\infty}/\mathbb{Q})$ jest izomorficzna z $\prod_{i=1}^{\infty}\mathbb{Z}_2$.

Przykład 4.7. Weźmy dowolne $p, q \in \mathbb{N}$, takie że p jest liczbą pierwszą oraz $(p, q) = 1$. Przez ζ_{q^n} oznaczamy pierwiastek pierwotny z jedynki stopnia q^n. Niech $\widetilde{\mathbb{F}_p} := \mathbb{F}_p(\{\zeta_{q^n} : n \in \mathbb{N}_+\})$ oraz t będzie elementem przestępnym nad $\widetilde{\mathbb{F}_p}$. Obliczymy

$$\mathrm{Gal}(\widetilde{\mathbb{F}_p}(\{\sqrt[q^n]{t} : n \in \mathbb{N}_+\})/\widetilde{\mathbb{F}_p}(t)).$$

Podobnie jak w poprzednich przykładach okaże się ona być proskończoną grupą abelową.

Ustalmy dowolne $n \in \mathbb{N}_+$. Pokażemy, że $x^{q^n} - t$ jest nierozkładalny nad $\widetilde{\mathbb{F}_p}(t)$. Oczywiście $\widetilde{\mathbb{F}_p}$ jest UFD, a więc także $\widetilde{\mathbb{F}_p}[t]$ jest UFD (twierdzenie Gaussa). Ponadto t jest nierozkładalny w $\widetilde{\mathbb{F}_p}[t]$, ponieważ w przeciwnym przypadku istniałyby $f, g \in \widetilde{\mathbb{F}_p}[t] \setminus \widetilde{\mathbb{F}_p}[t]^*$, takie że $\deg(f), \deg(g) > 0$ oraz $fg = t$. Sprzeczność, ponieważ $\deg(t) = 1$. Zauważmy, że $x^{q^n} - t$ spełnia założenia kryterium Eisensteina dla $p = t$, a więc jest nierozkładalny nad $\widetilde{\mathbb{F}_p}(t)$.

Przypomnijmy, że $(p, q) = 1$, czyli w szczególności p nie dzieli q^n, stąd pochodna formalna $x^{q^n} - t$, która wynosi $q^n x^{q^n-1}$, nie jest równa 0 w $\widetilde{\mathbb{F}_p}(t)[x]$. Zatem skoro $x^{q^n} - t$ jest nierozkładalny, dostajemy że wielomian ten jest rozdzielczy ([7], 3.2.2.). Ponadto $\widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})$ jest ciałem rozładu $x^{q^n} - t$. Wówczas rozszerzenie $\widetilde{\mathbb{F}_p}(t) \subseteq \widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})$ jest Galois (3.10.).

Sprawdzimy, że $\mathrm{Gal}(\widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})/\widetilde{\mathbb{F}_p}(t)) \cong \mathbb{Z}_{q^n}$. Zauważmy, że dla każdego $k \in \mathbb{Z}_{q^n}$, $\zeta_{q^n}^k \sqrt[q^n]{t}$ jest pierwiastkiem wielomianu nierozkładalnego $x^{q^n} - t$. Korzystając z lematu 3.4. otrzymujemy więc, że dla każdego $k \in \mathbb{Z}_{q^n}$, istnieje $\sigma_k \in \mathrm{Gal}(\widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})/\widetilde{\mathbb{F}_p}(t))$, taki że $\sigma_k(\sqrt[q^n]{t}) = \zeta_{q^n}^k \sqrt[q^n]{t}$. Możemy więc zdefiniować funkcję:

$$\begin{aligned} \theta_n \colon \mathbb{Z}_{q^n} &\to \mathrm{Gal}(\widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})/\widetilde{\mathbb{F}_p}(t)) \\ k &\mapsto \sigma_k. \end{aligned}$$

gdzie $\sigma_k(\sqrt[q^n]{t}) := \zeta_{q^n}^k \sqrt[q^n]{t}$. Sprawdzimy, że θ_n jest izomorfizmem. Podobnie jak w przykładzie 4.1. sprawdzamy, że θ_n jest homomorfizmem. Zauważmy, że $\sigma_k = \mathrm{id}$ wtedy i tylko wtedy, gdy $\sigma_k(\sqrt[q^n]{t}) = \sqrt[q^n]{t}$, równoważnie $k = 0$, a zatem θ_n jest monomorfizmem.

Powyżej sprawdziliśmy nierozkładalność $x^{q^n} - t$ nad $\widetilde{\mathbb{F}_p}(t)$. Ponadto $\widetilde{\mathbb{F}_p}(t) \subseteq \widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})$ jest skończonym rozszerzeniem Galois. Z lematu 3.11. mamy więc, że $|\mathrm{Gal}(\widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})/\widetilde{\mathbb{F}_p}(t))| = q^n = |\mathbb{Z}_{q^n}|$. Wówczas monomorfizm θ_n jest "na", to znaczy jest izomorfizmem.

W dalszej części przykładu będziemy zakładać, że $\mathbb{N}_+$ jest uporządkowany przez $\leqslant$ w naturalny sposób. Zauważmy, że $\widetilde{\mathbb{F}_p}(\{\sqrt[q^n]{t} : n \in \mathbb{N}_+\}) = \bigcup_{n \in \mathbb{N}_+} \widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})$. Z lematu 3.18. otrzymujemy, że

$$\mathrm{Gal}(\widetilde{\mathbb{F}_p}(\{\sqrt[q^n]{t} : n \in \mathbb{N}_+\})/\widetilde{\mathbb{F}_p}(t)) \cong \varprojlim_{n \in \mathbb{N}_+} \mathrm{Gal}(\widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})/\widetilde{\mathbb{F}_p}(t)),$$

gdzie $(\mathrm{Gal}(\widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})/\widetilde{\mathbb{F}_p}(t)), \psi_{nm})_{n \geqslant m \in \mathbb{N}_+}$ jest systemem odwrotnym z homomorfizmami ψ_{nm} zdefiniowanymi w następujący sposób:

$$\begin{aligned} \psi_{nm} \colon \mathrm{Gal}(\widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})/\widetilde{\mathbb{F}_p}(t)) &\to \mathrm{Gal}(\widetilde{\mathbb{F}_p}(\sqrt[q^m]{t})/\widetilde{\mathbb{F}_p}(t)) \\ \sigma &\mapsto \sigma|_{\widetilde{\mathbb{F}_p}(\sqrt[q^m]{t})}. \end{aligned}$$

Rozważmy system odwrotny $(\mathbb{Z}_{q^n}, \varphi_{nm})_{n \geqslant m \in \mathbb{N}_+}$, gdzie dla dowolnych $n \geqslant m \in \mathbb{N}_+$:

$$\begin{aligned} \varphi_{nm} \colon \mathbb{Z}_{q^n} &\to \mathbb{Z}_{q^m} \\ k &\mapsto r_{q^m}(k). \end{aligned}$$

Pokażemy, że $\varprojlim_{n\in\mathbb{N}_+} \mathrm{Gal}(\widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})/\widetilde{\mathbb{F}_p}(t)) \cong \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_{q^n}$. Ustalmy dowolne $m \leqslant n \in \mathbb{N}_+$. Sprawdzimy, że poniższy diagram jest przemienny:

$$\begin{array}{ccc} \mathbb{Z}_{q^m} & \xleftarrow{\quad\varphi_{nm}\quad} & \mathbb{Z}_{q^n} \\ {\scriptstyle\theta_m}\downarrow & & \downarrow{\scriptstyle\theta_n} \\ \mathrm{Gal}(\widetilde{\mathbb{F}_p}(\sqrt[q^m]{t})/\widetilde{\mathbb{F}_p}(t)) & \xleftarrow{\psi_{nm}} & \mathrm{Gal}(\widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})/\widetilde{\mathbb{F}_p}(t)). \end{array}$$

Ustalmy dowolne $k \in \mathbb{Z}_{q^n}$. Wówczas $k = aq^m + r$ dla pewnych $a, r \in \mathbb{N}, r < q^m$. Ponadto zauważmy, że $\zeta_{q^m} = \zeta_{q^n}^s$ dla pewnego $s \in \mathbb{N}$. Pokażemy, że $\psi_{nm}(\theta_n(k)) = \theta_m(\varphi_{nm}(k))$. Oczywiście wystarczy sprawdzić, że $\psi_{nm}(\theta_n(k))(\sqrt[q^m]{t}) = \theta_m(\varphi_{nm}(k))(\sqrt[q^m]{t})$. Obliczamy $\psi_{nm}(\theta_n(k))(\sqrt[q^m]{t}) = \sigma_k((\sqrt[q^n]{t})^s) = \zeta_{q^n}^{rs}(\sqrt[q^n]{t})^s = \zeta_{q^m}^r \sqrt[q^m]{t} = \theta_m(\varphi_{nm}(k))(\sqrt[q^m]{t})$. Z dowolności k mamy więc, że diagram jest przemienny. Przypomnijmy, że n, m były dowolne, a więc $\varprojlim_{n\in\mathbb{N}_+} \mathrm{Gal}(\widetilde{\mathbb{F}_p}(\sqrt[q^n]{t})/\widetilde{\mathbb{F}_p}(t)) \cong \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_{q^n}$ (lemat 2.9.), zatem

$$\mathrm{Gal}(\widetilde{\mathbb{F}_p}(\{\sqrt[q^n]{t} : n \in \mathbb{N}_+)/\widetilde{\mathbb{F}_p}(t)) \cong \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_{q^n}.$$

Przykład 4.8. Niech $\mathbb{Q}(\zeta_\infty, t_\infty) := \mathbb{Q}(\{\zeta_n, \sqrt[n]{t} : n \in \mathbb{N}_+\})$ i t będzie elementem przestępnym nad ciałem $\mathbb{Q}$. Obliczymy grupę $\mathrm{Gal}(\mathbb{Q}(\zeta_\infty, t_\infty)/\mathbb{Q}(t))$. W szczególności okaże się być ona proskończoną grupą rozwiązalną stopnia rozwiązalności 2.

Pokażemy najpierw, że dla dowolnego $n \in \mathbb{N}_+$, $\mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(t)) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$, gdzie działanie $\phi : \mathbb{Z}_n^* \to \mathrm{Aut}(\mathbb{Z}_n)$ jest zadane przez mnożenie $\cdot_n$.

Podobnie jak w przykładzie 4.7. pokazujemy, że wielomian $x^n - t \in \mathbb{Q}(t)[x]$ jest nierozkładalny nad $\mathbb{Q}(t)$. Dalej, podobnie jak w wyżej wymienionym przykładzie dowodzimy, że funkcja:

$$\begin{aligned} \theta_{n,1} \colon \mathbb{Z}_n &\to \mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(\zeta_n, t)) \\ k &\mapsto \sigma_k, \end{aligned}$$

gdzie $\sigma_k(\sqrt[n]{t}) := \zeta_n^k \sqrt[n]{t}$, jest izomorfizmem.

Lemat 4.9. *Jeśli $K \subseteq L$ jest rozszerzeniem całkowicie przestępnym i $f \in K[x]$ jest nierozkładalny nad K, to f jest nierozkładalny nad L.*

Dowód. Załóżmy a.a., że $f = gh$ dla pewnych $g, h \in L[x]$, takich że $\deg(g) = n_g > 0$ oraz $\deg(h) = n_h > 0$. Bez straty ogólności możemy założyć, że f, g, h są unormowane. Niech $R_g = \{r_i' : i \leqslant n_g\}$ oraz $R_h = \{r_i' : i \leqslant n_h\}$ będą zbiorami wszystkich pierwiastków w $\overline{K}$ kolejno g oraz h.

Ze wzorów Viety otrzymujemy, że $g(x) = \sum_{i=0}^{n_g} s_i(r_1, \ldots, r_{n_g}) x^{n_g - 1}$. Ponadto $r_1, \ldots, r_{n_g}$ są pierwiastkami f, a więc są algebraiczne nad ciałem K. Przypomnijmy, że zbiór liczb algebraicznych nad K jest ciałem, stąd dla każdego $0 \leqslant i \leqslant n_g$, $s(r_1, \ldots, r_{n_g})$ jest algebraiczny nad K, ale dla każdego $a \in L \setminus K$, a jest przestępny nad K, a stąd $g \in K[x]$. Analogicznie dowodzimy, że $h \in K[x]$. Stąd f jest rozkładalny nad K, co jest sprzeczne z założeniem. □

Zauważmy, że wielomian cyklotomiczny $\Phi_n(x)$ jest nierozkładalny nad $\mathbb{Q}(\sqrt[n]{t})$ (lemat 4.9.). Wówczas, podobnie jak w przykładzie 4.1., możemy sprawdzić, że funkcja:

$$\begin{aligned}\theta_{n,2}\colon \mathbb{Z}_n^* &\to \mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(\sqrt[n]{t}))\\ k &\mapsto \sigma'_k,\end{aligned}$$

gdzie $\sigma'_k(\zeta_n) := \zeta_n^k$, jest izomorfizmem.

Zauważmy, że dla wszystkich automorfizmów $\sigma_1 \in \mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(\zeta_n, t))$ oraz $\sigma_2 \in \mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(\sqrt[n]{t}))$, $\sigma_1\sigma_2 \in \mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(t))$. Pokażemy, że funkcja:

$$\begin{aligned}\theta_n\colon \mathbb{Z}_n \rtimes \mathbb{Z}_n^* &\to \mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(t))\\ (k_1, k_2) &\mapsto \theta_{n,1}(k_1)\theta_{n,2}(k_2)\end{aligned}$$

jest izomorfizmem.

Zaczniemy od sprawdzenia, że θ_n jest homomorfizmem.

Ustalmy dowolne $(k_1, l_1), (k_2, l_2) \in \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$. Zauważmy, że $\theta_n(k_1, l_1)\theta_n(k_2, l_2)(\zeta_n) = \theta_n(k_1, l_1)(\zeta_n^{l_1}) = \zeta_n^{l_1 \cdot_n l_2} = \theta_n(k_1 +_n (l_1 \cdot_n k_2), l_1 \cdot_n l_2)(\zeta_n)$. Ponadto $\theta_n(k_1, l_1)\theta_n(k_2, l_2)(\sqrt[n]{t}) = \theta_n(k_1, l_1)(\zeta_n^{k_2}\sqrt[n]{t}) = \zeta_n^{k_1 +_n (l_1 \cdot_n k_2)}\sqrt[n]{t} = \theta_n(k_1 +_n (l_1 \cdot_n k_2), l_1 \cdot_n l_2)(\sqrt[n]{t})$. Oczywiście każdy $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(t))$ jest jednoznacznie wyznaczony przez wartości przyjmowane dla ζ_n, $\sqrt[n]{t}$, a zatem $\theta_n(k_1, l_1)\theta_n(k_2, l_2) = \theta_n(k_1 +_n (l_1 \cdot_n k_2), l_1 \cdot_n l_2)$. Z dowolności $(k_1, l_1), (k_2, l_2) \in \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$ otrzymujemy więc, że θ_n jest homomorfizmem. Dodatkowo zauważmy, że $\theta_n(k, l) = \mathrm{id}$ wtedy i tylko wtedy, gdy $\theta_n(k, l)(\zeta_n) = \zeta_n$ oraz $\theta_n(k, l)(\sqrt[n]{t}) = \sqrt[n]{t}$, co jest równoważne $(k, l) = (0, 1)$, to znaczy θ_n jest monomorfizmem.

Ponadto, korzystając z lematów 4.9. i 3.11., możemy zauważyć, że $|\mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(t))| = [\mathbb{Q}(\zeta_n, \sqrt[n]{t}) : \mathbb{Q}(t)] = [\mathbb{Q}(\zeta_n, \sqrt[n]{t}) : \mathbb{Q}(\sqrt[n]{t})][\mathbb{Q}(\sqrt[n]{t}) : \mathbb{Q}(t)] = \varphi(n)n = |\mathbb{Z}_n \rtimes \mathbb{Z}_n^*|$, a więc θ_n jest "na". Zatem θ_n jest izomorfizmem.

Rozważmy system odwrotny $(\mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(t)), \psi_{nm})_{m \leqslant n \in \mathbb{N}_+}$, gdzie porządek $\leqslant$ na $\mathbb{N}_+$ jest zadany przez podzielność oraz dla dowolnych $n \geqslant m \in \mathbb{N}_+$:

$$\begin{aligned}\psi_{nm}\colon \mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(t)) &\to \mathrm{Gal}(\mathbb{Q}(\zeta_m, \sqrt[m]{t})/\mathbb{Q}(t))\\ \sigma &\mapsto \sigma|_{\mathbb{Q}(\zeta_m, \sqrt[m]{t})}.\end{aligned}$$

Zauważmy, że $\mathbb{Q}(\zeta_\infty, t_\infty) = \bigcup_{n \in \mathbb{N}_+} \mathbb{Q}(\zeta_n, \sqrt[n]{t})$. Ponadto dla dowolnego $n \in \mathbb{N}_+$, $\mathbb{Q}(t) \subseteq \mathbb{Q}(\zeta_n, \sqrt[n]{t})$ jest skończonym rozszerzeniem Galois. Wówczas z lematu 3.18. mamy, że

$$\mathrm{Gal}(\mathbb{Q}(\zeta_\infty, t_\infty)/\mathbb{Q}(t)) \cong \varprojlim_{n \in \mathbb{N}_+} \mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(t)).$$

Rozważmy system odwrotny $(\mathbb{Z}_n \rtimes \mathbb{Z}_n^*, \varphi_{nm})_{m \leqslant n \in \mathbb{N}_+}$ gdzie porządek $\leqslant$ na $\mathbb{N}_+$ jest zadany przez podzielność oraz dla dowolnych $n \geqslant m \in \mathbb{N}_+$:

$$\begin{aligned}\varphi_{nm}\colon \mathbb{Z}_n \rtimes \mathbb{Z}_n^* &\to \mathbb{Z}_m \rtimes \mathbb{Z}_m^*\\ (k, l) &\mapsto (r_m(k), r_m(l)).\end{aligned}$$

Pokażemy, że $\varprojlim_{n \in \mathbb{N}_+} \mathbb{Z}_n \rtimes \mathbb{Z}_n^* \cong \varprojlim_{n \in \mathbb{N}_+} \mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(t))$.

Ustalmy dowolne $m \leqslant n \in \mathbb{N}_+$. Sprawdzimy, że następujący diagram jest przemienny:

$$\begin{array}{ccc} \mathbb{Z}_m \rtimes \mathbb{Z}_m^* & \xleftarrow{\quad\varphi_{nm}\quad} & \mathbb{Z}_n \rtimes \mathbb{Z}_n^* \\ \Big\downarrow{\scriptstyle \theta_m} & & \Big\downarrow{\scriptstyle \theta_n} \\ \mathrm{Gal}(\mathbb{Q}(\zeta_m, \sqrt[m]{t})/\mathbb{Q}(t)) & \xleftarrow{\psi_{nm}} & \mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(t)). \end{array}$$

Ustalmy dowolny $(k,l) \in \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$. Pokażemy, że $\theta_m(\varphi_{nm}(k,l)) = \varphi_{nm}(\theta_n(k,l))$. Przypomnijmy, że każdy $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m, \sqrt[m]{t})/\mathbb{Q}(t))$ jest jednoznacznie wyznaczony przez $\sigma(\zeta_m)$ oraz $\sigma(\sqrt[m]{t})$. Podobnie jak w przykładach 4.1., 4.7. sprawdzamy, że $\theta_m(\varphi_{nm}(k,l))(\zeta_m) = \psi_{nm}(\theta_n(k,l))(\zeta_m)$ oraz $\theta_m(\varphi_{nm}(k,l))(\sqrt[m]{t}) = \psi_{nm}(\theta_n(k,l))(\sqrt[m]{t})$, stąd mamy, że $\theta_m(\varphi_{nm}(k,l)) = \psi_{nm}(\theta_n(k,l))$. Z dowolności $(k,l) \in \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$ otrzymujemy przemiennność diagramu. Przypomnijmy, że $n, m \in \mathbb{N}_+$ były dowolne, a więc z lematu 2.9. otrzymujemy

$$\varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_n \rtimes \mathbb{Z}_n^* \cong \varprojlim_{n\in\mathbb{N}_+} \mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[n]{t})/\mathbb{Q}(t)).$$

Rozważmy produkt półprosty (z topologią produktową) $\varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_n \rtimes \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_n^*$ z działaniem danym przez:

$$((a_1, \dots, a_n, \dots), (b_1, \dots, b_n, \dots)) \cdot ((a_1', \dots, a_n', \dots), (b_1', \dots, b_n', \dots)) =$$

$$((a_1 +_1 (b_1 \cdot_1 a_1'), \dots, a_n +_n (b_n \cdot_n a_n'), \dots), (b_1 \cdot_1 b_1', \dots, b_n \cdot_n b_n', \dots)).$$

Definiujemy funkcję:

$$\begin{aligned} \Psi\colon \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_n \rtimes \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_n^* &\to \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_n \rtimes \mathbb{Z}_n^* \\ ((a_1, \dots, a_n, \dots), (b_1, \dots, b_n, \dots)) &\mapsto ((a_i, b_i))_{i=1}^{\infty}. \end{aligned}$$

Standardowo sprawdzamy, że Ψ jest algebraicznym izomorfizmem oraz homeomorfizmem. Wówczas skoro $\varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$ jest grupą topologiczną (proskończoną), to również $\varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_n \rtimes \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_n^*$ jest grupą topologiczną (proskończoną).

Sprawdziliśmy więc, że

$$\mathrm{Gal}(\mathbb{Q}(\zeta_\infty, t_\infty)/\mathbb{Q}(t)) \cong \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_n \rtimes \varprojlim_{n\in\mathbb{N}_+} \mathbb{Z}_n^*.$$

W szczególności dostarcza nam to przykładu proskończonej grupy rozwiązalnej stopnia 2, która ma realizację w postaci grupy Galois.

5 Odwrócony problem Galois

Przypomnijmy, że odwrócony problem Galois jest sformułowany w następujący sposób: Czy każda grupa skończona jest grupą Galois pewnego rozszerzenia ciała liczb wymiernych?

W tym rozdziale udzielimy pozytywnej odpowiedzi na następujące osłabienie tego problemu: Czy istnieje ciało K, takie że wszystkie grupy skończone są grupami Galois pewnego rozszerzenia ciała K? W tym celu przedstawimy twierdzenie Waterhausa, a następnie wprowadzimy definicję wolnej grupy proskończonej o przeliczalnie wielu generatorach, dla której zastosowane w.w. twierdzenie pozwoli nam pokazać istnienie takiego ciała K.

Twierdzenie 5.1. *(Waterhaus) Niech G będzie dowolną grupą proskończoną. Wówczas istnieje rozszerzenie Galois $K \subseteq L$, takie że $G \cong \mathrm{Gal}(L/K)$.*

Dowód. Przedstawiony dowód bazuje na rozdziale 1.3. z [2]. Niech $\mathcal{A}$ będzie rodziną wszystkich otwartych podgrup normalnych grupy G oraz przez T oznaczymy sumę rozłączną $\bigcup\limits_{N\in\mathcal{A}} G/N$.

Zauważmy, że funkcja

$$\begin{aligned} \cdot\colon G \times T &\to T \\ (g, hN) &\mapsto ghN. \end{aligned}$$

jest działaniem G na zbiorze T. Sprawdzimy, że $\cdot$ jest wierne. Ustalmy dowolny $e \neq g \in G$. Z uwagi 2.8. istnieje $U \subseteq G$ otwarty, taki że $e \in U$ i $g^{-1} \notin U$. Wówczas istnieje $N \in \mathcal{A}$, taki że $N \subseteq U$ (twierdzenie 2.11.), tj. w szczególności $gg^{-1}N = N \neq g^{-1}N$. Z dowolności g otrzymujemy zatem wierność działania.

Weźmy dowolne ciało, bez straty ogólności $\mathbb{Q}$ i niech $L := \mathbb{Q}(T)$, gdzie T rozumiemy jako zbiór algebraicznie niezależny nad $\mathbb{Q}$. Z definicji, każdy element $a \in \mathbb{Q}(T)$ jest postaci

$$\frac{f_1(g_{i_1}N_{i_1}, \ldots, g_{i_n}N_{i_n})}{f_2(g_{j_1}N_{j_1}, \ldots, g_{j_k}N_{j_k})}$$

dla pewnych $g_{i_1}N_{i_1}, \ \ldots, \ g_{i_n}N_{i_n}, \ g_{j_1}N_{j_1}, \ldots, \ g_{j_k}N_{j_k} \in T, f_1 \in \mathbb{Q}[x_{i_1}, \ldots, x_{i_n}]$, $f_2 \in \mathbb{Q}[x_{j_1}, \ldots, x_{j_k}]$. Pokażemy, że dla każdego $g \in G$, odwzorowanie:

$$\begin{aligned} \varphi_g\colon L &\to L \\ \frac{f_1(g_{i_1}N_{i_1}, \ldots, g_{i_n}N_{i_n})}{f_2(g_{j_1}N_{j_1}, \ldots, g_{j_k}N_{j_k})} &\mapsto \frac{f_1(gg_{i_1}N_{i_1}, \ldots, gg_{i_n}N_{i_n})}{f_2(gg_{j_1}N_{j_1}, \ldots, gg_{j_k}N_{j_k})} \end{aligned}$$

jest automorfizmem L. Z algebraicznej niezależności T natychmiast wynika, że φ_g jest dobrze określona oraz jest monomorfizmem. Pozostaje sprawdzić, że φ_g jest "na".

Ustalmy dowolny $\frac{f_1(g_{i_1}N_{i_1}, \ldots, g_{i_n}N_{i_n})}{f_2(g_{j_1}N_{j_1}, \ldots, g_{j_k}N_{j_k})} \in L$. Oczywiście $\frac{f_1(g^{-1}g_{i_1}N_{i_1}, \ldots, g^{-1}g_{i_n}N_{i_n})}{f_2(g^{-1}g_{j_1}N_{j_1}, \ldots, g^{-1}g_{j_k}N_{j_k})} \in L$ oraz $\varphi_g\left(\frac{f_1(g^{-1}g_{i_1}N_{i_1}, \ldots, g^{-1}g_{i_n}N_{i_n})}{f_2(g^{-1}g_{j_1}N_{j_1}, \ldots, g^{-1}g_{j_k}N_{j_k})}\right) = \frac{f_1(g_{i_1}N_{i_1}, \ldots, g_{i_n}N_{i_n})}{f_2(g_{j_1}N_{j_1}, \ldots, g_{j_k}N_{j_k})}$. Wobec dowolności $\frac{f_1(g_{i_1}N_{i_1}, \ldots, g_{i_n}N_{i_n})}{f_2(g_{j_1}N_{j_1}, \ldots, g_{j_k}N_{j_k})}$ mamy, że φ_g jest "na". Pokazaliśmy zatem, że $\varphi_g \in \mathrm{Aut}(L)$.

Rozważmy homomorfizm $\Phi : G \to \mathrm{Aut}(L), \Phi(g) = \varphi_g$. Z wierności działania G na T, otrzymujemy, że dla każdego $e \neq g \in G$, istnieje $g'N' \in T \subseteq \mathbb{Q}(T)$, taki że $\varphi_g(g'N') \neq g'N'$. Zatem $\ker\Phi = \{e\}$, czyli Φ jest monomorfizmem. Możemy więc utożsamiać G z podgrupą $\mathrm{Aut}(L)$.

Niech $K := L^G$. Zauważmy, że wówczas $G \leqslant \mathrm{Gal}(L/K)$. Pokażemy, że $G = \mathrm{Gal}(L/K)$.

Zaczniemy od sprawdzenia, że $K \subseteq L$ jest rozszerzeniem Galois. Ustalmy dowolny $a \in L$, wtedy $a \in \mathbb{Q}(g_{i_1}N_{i_1}, \ldots, g_{i_n}N_{i_n})$, gdzie $\{g_{i_1}N_{i_1}, \ldots, g_{i_n}N_{i_n}\}$ jest pewnym skończonym podzbiorem T. Weźmy dowolny $h \in \bigcap_{j=1}^{n} N_{i_j}$, wtedy dla każdego $1 \leqslant j \leqslant n$, $hg_{i_j}N_{i_j} = g_{i_j}h'N_{i_j} = g_{i_j}N_{i_j}$. Dodatkowo $\mathbb{Q}^G = \mathbb{Q}$, a więc 1 należy do $\bigcap_{j=1}^{n} N_{i_j} \subseteq G_a$. Ponadto $\bigcap_{j=1}^{n} N_{i_j}$ otwarty w G i mnożenie w G jest ciągłe, a stąd $G_a = \bigcup_{g \in G_a} g(\bigcap_{j=1}^{n} N_{i_j})$ jest otwarty w G. G jest zwarta (uwaga 2.8.), a zatem $[G : G_a] < \infty$ (lemat 2.2.). Wówczas, na mocy twierdzenia o orbicie i stabilizatorze, $|G \cdot a| = k + 1 < \infty$, czyli $G \cdot a = \{a_0 = a, \ldots, a_k\}$ dla pewnych parami różnych $a_0, \ldots, a_k \in L$. Niech $f(x) := \prod_{i=0}^{k}(x - a_i)$. Zauważmy, że każdy $g \in G$ permutuje elementy $G \cdot a$, zatem $f \in K[x]$. Wówczas a jest algebraiczny i rozdzielczy nad K.

Z dowolności a otrzymujemy więc, że $K \subseteq L$ jest rozszerzeniem rozdzielczym. Ponadto $L = \bigcup\{\text{ciało rozkładu } \prod_{a_i \in G \cdot a}(x - a_i) : a \in L\}$, a więc $K \subseteq L$ normalne, czyli $K \subseteq L$ jest rozszerzeniem Galois (twierdzenie 3.10.).

Pokażemy, że $\Psi : G \to \mathrm{Gal}(L/K)$, $\Psi(g) = g$ jest ciągłe (gdzie $\mathrm{Gal}(L/K)$ rozważamy z topologią Krulla). Ustalmy dowolne skończone rozszerzenie Galois $K \subseteq M$ zawarte w L. Z definicji $\mathrm{Gal}(L/M)$ jest bazowym otoczeniem otwartym elementu neutralnego e w $\mathrm{Gal}(L/K)$. $K \subseteq M$ skończone, a zatem możemy wybrać $a_1, \ldots, a_m \in T$, takie że $M \subseteq K(a_1, \ldots, a_m)$. Wtedy, podobnie jak w omówionym powyżej przypadku G_a, pokazujemy, że dla każdego $1 \leqslant i \leqslant m$, G_{a_i} jest otwarty w G. Wówczas również $\bigcap_{i=1}^{m} G_{a_i}$ otwarty w G. Zauważmy, że $\bigcap_{i=1}^{m} G_{a_i} \subseteq G \cap \mathrm{Gal}(L/M) = \Psi^{-1}(\mathrm{Gal}(L/M))$, a zatem $\Psi^{-1}(\mathrm{Gal}(L/M)) = \bigcup_{g \in G \cap \mathrm{Gal}(L/M)} g(\bigcap_{i=1}^{m} G_{a_i})$ jest otwarty, stąd Ψ jest ciągłe.

Przypomnijmy, że G jest zwarta, a więc, z ciągłości Ψ, G jest zwarta w $\mathrm{Gal}(L/K)$. Stąd G jest domknięta w $\mathrm{Gal}(L/K)$, ponieważ $\mathrm{Gal}(L/K)$ jest Hausdorffa (lemat 2.2.). Skoro G jest domknięta, z twierdzenia 3.16. otrzymujemy, że $G = \mathrm{Gal}(L/L^G) = \mathrm{Gal}(L/K)$.

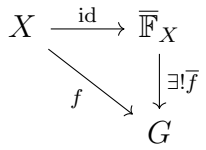
□

Niech X będzie zbiorem, a G - grupą proskończoną. Załóżmy ponadto, że dana jest pewna funkcja $f : X \to G$. Funkcję f nazywamy *zbieżną do e*, gdy dla każdej otwartej podgrupy normalnej H grupy G, zbiór $X \setminus f^{-1}(H)$ jest skończony.

Definicja 5.2. Niech $\hat{F}$ będzie grupą proskończoną, a X będzie podzbiorem $\hat{F}$ spełniającym $e \notin X$. Grupę $\hat{F}$ nazywamy *wolną grupą proskończoną* o wolnym zbiorze generatorów X i oznaczamy przez $\overline{\mathbb{F}}_X$, gdy spełnia ona następujące warunki:

1. $\hat{F} = \overline{\langle X \rangle}$ i inkluzja $\iota : X \to \hat{F}$ jest zbieżna do e,
2. dla każdej zbieżnej do e funkcji f ze zbioru X w grupę proskończoną $G = \overline{\langle f(X) \rangle}$, istnieje jedyny epimorfizm grup topologicznych $\overline{f} : \overline{\mathbb{F}}_X \to G$, taki że

następujący diagram jest przemienny:



Uwaga 5.3. Dla dowolnego zbioru X istnieje wolna grupa proskończona $\overline{\mathbb{F}}_X$ o wolnym zbiorze generatorów X.

Dowód. [2] 17.4. □

Wniosek 5.4. *Istnieje ciało K, takie że każdą grupę skończoną możemy zrealizować jako grupę Galois nad K.*

Dowód. Rozważmy wolną grupę proskończoną $\overline{\mathbb{F}}_X$ o wolnym zbiorze generatorów X mocy $\aleph_0$. Niech $X = \{x_0, x_1, \dots\}$ dla parami różnych x_i. Z twierdzenia Waterhausa otrzymujemy pewne rozszerzenie Galois $K \subseteq L$, takie że $\mathrm{Gal}(L/K) \cong \overline{\mathbb{F}}_X$. Bez straty ogólności, w dalszej części dowodu będziemy w.w. grupy ze sobą utożsamiać. Ustalmy dowolną grupę skończoną H i załóżmy, że $H = \{h_0, \dots, h_n\}$ dla parami różnych h_i. Niech funkcja $f : X \to H$ będzie zdefiniowana następująco:

$$f(x_i) = \begin{cases} h_i, & \text{gdy } 0 \leqslant i \leqslant n \\ e & \text{w przeciwnym przypadku.} \end{cases}$$

Zauważmy, że f jest zbieżna do e. Z definicji wolnej grupy proskończonej istnieje jedyny epimorfizm $\overline{f} : \overline{\mathbb{F}}_X \to H$, taki że $\overline{f}\,\mathrm{id} = f$. Z zasadniczego twierdzenia o homomorfiźmie grup mamy, że $\overline{\mathbb{F}}_X/\ker\overline{f} \cong H$. Zauważmy, że $\ker\overline{f}$ jest domkniętą podgrupą normalną $\overline{\mathbb{F}}_X$, a więc istnieje $K \subseteq K' \subseteq L$, takie że $K \subseteq K'$ Galois i $\mathrm{Gal}(L/K') = \ker\overline{f}$ (3.16., 3.17.). Otrzymujemy zatem:

$$\mathrm{Gal}(K'/K) \;\cong\; \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/K') \;=\; \overline{\mathbb{F}}_X/\ker\overline{f} \;\cong\; H.$$

□

6 Największe rozszerzenie abelowe

W tym rozdziale skupimy się na terminie największego (w sensie inkluzji) rozszerzenia abelowego ciała K, które oznaczać będziemy przez K^{ab}. W szczególności uzasadnimy istnienie takiego rozszerzenia oraz opiszemy grupę $\mathrm{Gal}(K^{ab}/K)$ w terminach grupy $\mathrm{Gal}(\overline{K}^{sep}/K)$.

6.1 Istnienie największego rozszerzenia abelowego

Niech K będzie dowolnym ciałem. Zaczniemy od pokazania istnienia największego (a więc także maksymalnego) rozszerzenia abelowego $K \subseteq K^{ab}$.

Lemat 6.1. *Niech $\{L_i \subseteq \overline{K} : i \in I\}$ będzie rodziną rozszerzeń abelowych ciała K. Wówczas również złożenie $\{L_i\}_{i\in I}$ jest rozszerzeniem abelowym K.*

Dowód. Przez L' oznaczmy złożenie $\{L_i\}_{i\in I}$. Z definicji rozszerzenia abelowego, dla każdego $i \in I$, $K \subseteq L_i$ jest rozszerzeniem rozdzielczym. Elementy rozdzielcze nad K tworzą ciało (uwaga 3.7.), a więc $K \subseteq L'$ jest rozdzielcze. Ponadto dla każdego $i \in I$, L_i jest ciałem rozkładu rodziny wielomianów o współczynnikach z K, a zatem również L' jest ciałem rozkładu rodziny wielomianów o współczynnikach z K, tj. $K \subseteq L'$ jest normalne. Wówczas $K \subseteq L'$ jest rozszerzeniem Galois (3.10.).

Pozostaje pokazać, że $\mathrm{Gal}(L'/K)$ jest abelowa. Dla każdego $\sigma \in \mathrm{Gal}(L'/K)$ i dla każdego $i \in I$, $\sigma|_{L_i} \in \mathrm{Gal}(L_i/K)$, ponieważ $K \subseteq L_i$ jest normalne. Wówczas możemy zdefiniować następujący homomorfizm:

$$\begin{aligned}\Psi\colon\ \mathrm{Gal}(L'/K) &\to \prod_{i\in I} \mathrm{Gal}(L_i/K)\\ \sigma &\mapsto (\sigma|_{L_i})_{i\in I}.\end{aligned}$$

Zauważmy, że skoro L' jest złożeniem $\{L_i\}_{i\in I}$, to $\Psi(\sigma) = (\mathrm{id}_{L_i})_{i\in I}$ jest równoważne $\sigma = id_{L'}$, a więc Ψ jest monomorfizmem. Ponadto $\prod\limits_{i\in I} \mathrm{Gal}(L_i/K)$ jest grupą abelową, jako produkt grup abelowych. Mamy więc, że $\mathrm{Gal}(L'/K)$ zanurza się homomorficznie w grupie abelowej, a więc jest grupą abelową. Wówczas otrzymujemy, że $K \subseteq L'$ jest rozszerzeniem abelowym. □

Wniosek 6.2. *Przez $\mathcal{A}$ oznaczmy rodzinę wszystkich rozszerzeń abelowych ciała K. Z definicji $\mathcal{A}$ złożenie wszystkich ciał z $\mathcal{A}$ jest największym w sensie inkluzji (a więc i maksymalnym) rozszerzeniem abelowym ciała K.*

6.2 Opis grupy Galois dla największego rozszerzenia abelowego

Ustalmy dowolne ciało K. Przez G będziemy oznaczać grupę $\mathrm{Gal}(\overline{K}^{sep}/K)$ (z topologią Krulla). W dalszej części zaprezentujemy w jaki sposób możemy wyrazić grupę $\mathrm{Gal}(K^{ab}/K)$ przy użyciu grupy G, tj. pokażemy że $\mathrm{Gal}(K^{ab}/K) \cong G/\overline{[G,G]}$. Odnotujmy następującą uwagę, która wynika wprost z twierdzenia 3.16.

Uwaga 6.3. Niech L będzie ciałem, takim że $K \subseteq L \subseteq \overline{K}^{sep}$. Wtedy $\mathrm{Gal}(\overline{K}^{sep}/L)$ jest domknięta w G.

Stwierdzenie 6.4. $\mathrm{Gal}(K^{ab}/K) \cong G/\overline{[G,G]}$

Dowód. Rozważmy grupy $\mathrm{Gal}(\overline{K}^{sep}/K^{ab})$ oraz $\mathrm{Gal}(\overline{K}^{sep}/\overline{K}^{sep\overline{[G,G]}})$. Na mocy lematu 6.3. są one domknięte w G. Pokażemy, że

$$(*)\quad \mathrm{Gal}(\overline{K}^{sep}/K^{ab}) = \mathrm{Gal}(\overline{K}^{sep}/\overline{K}^{sep\overline{[G,G]}}).$$

Wówczas z 3.16. otrzymamy, że $K^{ab} = \overline{K}^{sep\overline{[G,G]}}$, a więc z 3.17. dostaniemy:

$$\mathrm{Gal}(K^{ab}/K) = \mathrm{Gal}(\overline{K}^{sep\overline{[G,G]}}/K) \cong G/\overline{[G,G]}.$$

Przechodzimy do dowodu $(*)$.
$\subseteq$: Zauważmy, że $\mathrm{Gal}(\overline{K}^{sep\overline{[G,G]}}/K) \cong G/\overline{[G,G]}$ (z 3.17.), tj. $\mathrm{Gal}(\overline{K}^{sep\overline{[G,G]}}/K)$ jest abelowa. Stąd $K \subseteq \overline{K}^{sep\overline{[G,G]}}$ jest rozszerzeniem abelowym. Otrzymujemy więc, że $\overline{K}^{sep\overline{[G,G]}} \subseteq K^{ab}$, a zatem $\mathrm{Gal}(\overline{K}^{sep}/K^{ab}) \subseteq \mathrm{Gal}(\overline{K}^{sep}/\overline{K}^{sep\overline{[G,G]}})$.
$\supseteq$: Skoro $\mathrm{Gal}(\overline{K}^{sep}/\overline{K}^{sep\overline{[G,G]}})$ domknięta w G (lemat 6.3.), to z 3.16. w szczególności mamy, że $\mathrm{Gal}(\overline{K}^{sep}/\overline{K}^{sep\overline{[G,G]}}) = \overline{[G,G]}$. Ponadto z lematu 6.3. $\mathrm{Gal}(\overline{K}^{sep}/K^{ab})$ jest domknięta w G. Wystarczy zatem sprawdzić, że $[G,G] \subseteq \mathrm{Gal}(\overline{K}^{sep}/K^{ab})$. Oczywiście $[G,G] \leqslant G$. Pokażemy, że dla dowolnych $\varphi, \psi \in G$ oraz dla każdego $a \in K^{ab}$, $\psi\varphi\psi^{-1}\varphi^{-1}(a) = a$.

Ustalmy dowolne $\varphi, \psi \in G$, $a \in K^{ab}$, wtedy $\psi|_{K^{ab}}, \varphi|_{K^{ab}} \in \mathrm{Gal}(K^{ab}/K)$, a zatem: $\psi\varphi\psi^{-1}\varphi^{-1}(a) = a$, stąd $[G,G] \subseteq \mathrm{Gal}(\overline{K}^{sep}/K^{ab})$. □

Uwaga 6.5. Niech $K \subseteq L$ będzie dowolnym rozszerzeniem ciał. Przez G oznaczmy $\mathrm{Gal}(L/K)$. Wówczas, rozumując jak wyżej, możemy pokazać istnienie największego rozszerzenia abelowego K zawartego w L (ozn. L'). Ponadto, podobnie jak wyżej, $\mathrm{Gal}(L'/K) \cong G/\overline{[G,G]}$.

7 Największe rozszerzenie prorozwiązalne

W tym rozdziale uzasadnimy istnienie największego (a więc także maksymalnego) rozszerzenie prorozwiązalnego dowolnego ustalonego ciała K.

Zacznijmy od wyjaśnienia pojecia rozszerzenia prorozwiązalnego. Podobnie jak w przypadku omawianego w poprzednim rozdziale rozszerzenia abelowego, $K \subseteq L$ nazywamy *rozszerzeniem prorozwiązalnym*, gdy jest rozszerzeniem Galois i $\mathrm{Gal}(L/K)$ jest grupą prorozwiązalną, to znaczy jest granicą odwrotną skończonych grup rozwiązalnych. Zaczniemy od przedstawienia wynikającej z twierdzenia 2.11. charaktryzacji grup prorozwiązalnych, z której korzystać będziemy w dalszej części.

Wniosek 7.1. *Grupa zwarta (Hausdorffa) G jest prorozwiązalna wtedy i tylko wtedy, gdy ma bazę $\mathcal{N}$ otwartych otoczeń elementu neutralnego złożoną z otwarto-domkniętych podgrup normalnych, taką że G/N jest rozwiązalna dla każdego $N \in \mathcal{N}$.*

Dowód.
$\Longrightarrow$: Z założenia $G = \varprojlim_{i \in I} G_i$ dla pewnego systemu odwrotnego skończonych grup rozwiązalnych $(G_i, \varphi_{ij})_{i \geqslant j \in I}$. Z twierdzenia 2.11. otrzymujemy więc, że G posiada bazę otwartych otoczeń elementu neutralnego złożoną z otwarto-domkniętych podgrup normalnych $\{N_i : i \in I\}$, taką że dla każdego $i \in I$, $G/N_i \cong G_i$. W szczególności oznacza to, że dla każdego $i \in I$, G/N_i jest rozwiązalna.
$\Longleftarrow$: Z założenia G ma bazę $\mathcal{N}$ otwartych otoczeń elementu neutralnego złożoną z otwarto- domkniętych podgrup normalnych. Niech I będzie dowolnym zbiorem równolicznym z $\mathcal{N}$, wówczas w naturalny sposób indeksujemy elementy $\mathcal{N}$ zbiorem I otrzymując $\mathcal{N} = \{N_i : i \in I\}$. Zadajemy porządek na zbiorze I następująco: $i \leqslant j$

wtedy i tylko wtedy, gdy $N_j \leqslant N_i$. Zauważmy, że wtedy $(I, \leqslant)$ jest zbiorem skierowanym. Ponadto dla każdego $i \in I$, $G_i := G/N_i$ jest skończoną grupą rozwiązalną (z założenia i 2.2.). Wówczas G jest prorozwiązalna (2.11.). □

Uwaga 7.2. Niech G będzie dowolną grupą prorozwiązalną. Wówczas dla każdej otwarto-domkniętej podgrupy normalnej $N \trianglelefteq G$, G/N jest skończoną grupą rozwiązalną.

Dowód. Z wniosku 7.1. istnieje $N' \subseteq N$, taki że N' jest otwarto-domkniętą podgrupą normalną G oraz G/N' jest rozwiązalna. Wówczas także G/N jest rozwiązalna jako obraz grupy rozwiązalnej przez epimorfizm

$$\begin{aligned} \pi \colon G/N' &\to G/N \\ gN' &\mapsto gN. \end{aligned}$$

□

Podobnie jak w przypadku największego rozszerzenia abelowego, konstruując największe rozszerzenie prorozwiązalne rozważać będziemy pewien produkt grup prorozwiązalnych. Pokażemy najpierw, że dowolny produkt grup prorozwiązalnych jest grupą prorozwiązalną.

Lemat 7.3. *Niech $\{G_i\}_{i\in I}$ będzie rodziną grup prorozwiązalnych. Wówczas $G = \prod_{i\in I} G_i$ jest prorozwiązalna.*

Dowód. Zauważmy, że G jest zwartą przestrzenią Hausdorffa jako produkt zwartych przestrzeni Hausdorffa.

Rozważmy zbiór F wszystkich funkcji f, takich że $\operatorname{dom} f \in [I]^{<\omega}$, $\operatorname{rng} f \subseteq \mathcal{P}(\bigcup_{i\in I} G_i)$ i dla każdego $i \in \operatorname{dom} f$, $f(i)$ jest otwarto-domkniętą podgrupą normalną grupy G_i. Wtedy dla $f \in F$, definiujemy $N_f := \prod_{i\in \operatorname{dom} f} f(i) \times \prod_{i\in I\setminus \operatorname{dom} f} G_i$. Zauważmy, że wówczas N_f jest otwarto-domkniętą podgrupą normalną G. Ponadto G/N_f jest izomorficzna z produktem $\prod_{i\in \operatorname{dom}(f)} G_i/f(i)$, a więc jest skończoną grupą rozwiązalną na mocy uwagi 7.2. Pokażemy, że rodzina $\mathcal{N} = \{N_f : f \in F\}$ jest bazą otwartych otoczeń elementu neutralnego w G.

Ustalmy dowolny zbiór otwarty $U \subseteq G$ zawierający e. Z definicji topologii produktowej zbiór U jest sumą zbiorów postaci $\pi_{i_1}^{-1}(X_{i_1}) \cap \ldots \cap \pi_{i_n}^{-1}(X_{i_n})$ dla pewnego $J = \{i_1, \ldots, i_n\} \in [I]^{<\omega}$ i $X_{i_j} \subseteq G_{i_j}$ otwartych. Weźmy dowolny taki zbiór zawierający e. Wtedy dla każdego $j = 1, \ldots, n$, $e_{i_j} \in X_{i_j}$, a więc istnieje $N_{i_j} \subseteq X_{i_j}$ otwarto-domknięty dzielnik normalny G_{i_j}. Zauważmy, że funkcja $f = \{(i_1, N_{i_1}), \ldots, (i_n, N_{i_n})\}$ należy do F oraz $N_f = \pi_{i_1}^{-1}(N_{i_1}) \cap \ldots \cap \pi_{i_n}^{-1}(N_{i_n}) \subseteq U$. Z dowolności U, $\mathcal{N}$ jest bazą otwarto-domkniętych otoczeń e w G.

Z wniosku 7.1. otrzymujemy więc, że G jest prorozwiązalna. □

Lemat 7.4. *Każda domknięta podgrupa grupy prorozwiązalnej jest prorozwiązalna.*

Dowód. Niech H będzie dowolną domknięta podgrupą grupy prorozwiązalnej G. Oczywiście H jest zwartą przestrzenią Hausdorffa. Ustalmy dowolny zbiór otwarty $U \subseteq H$, do którego należy e. Z wniosku 7.1. G ma bazę $\mathcal{N}$ otwartych otoczeń elementu neutralnego złożoną z otwarto-domkniętych podgrup normalnych, takich że G/N jest rozwiązalna dla każdego $N \in \mathcal{N}$. Istnieje więc $N \in \mathcal{N}$, taki że $N \cap H \subseteq U$. Zauważmy ponadto, że $N \cap H$ jest otwarto-domknięty w H oraz H/N jest rozwiązalna, jako podgrupa grupy rozwiązalnej. Zbiór U był dowolny, a więc otrzymujemy, że H bazę $\mathcal{N}'$ otwartych otoczeń elementu neutralnego złożoną z otwarto-domkniętych podgrup normalnych, taką że H/N jest rozwiązalna dla każdego $N \in \mathcal{N}'$. Wówczas H jest prorozwiązalna (wniosek 7.1.). □

Zauważmy, że wprost z lematów 7.3., 7.4. otrzymujemy również, że każda domknięta podgrupa produktu grup prorozwiązalnych jest prorozwiązalna.

Stwierdzenie 7.5. *Każde ciało K posiada największe (a więc i maksymalne) rozszerzenie prorozwiązalne.*

Dowód. Niech $\mathcal{A}$ będzie rodziną wszystkich prorozwiązalnych rozszerzeń K zawartych w $\bar{K}$, zaś M będzie złożeniem wszystkich ciał z $\mathcal{A}$. Pokażemy, że $K \subseteq M$ jest prorozwiązalne.

Zauważmy, że $K \subseteq M$ jest rozszerzeniem Galois jako złożenie rozszerzeń Galois. Wystarczy zatem pokazać, że $\mathrm{Gal}(M/K)$ jest prorozwiązalna.

Rozważmy zanurzenie $\Psi : \mathrm{Gal}(M/K) \to \prod_{L\in\mathcal{A}} \mathrm{Gal}(L/K), \Psi(\sigma) = (\sigma|L)_{L\in\mathcal{A}}$, gdzie każdą z grup Galois rozważamy oczywiście z topologią Krulla, a ich produkt z topologią produktową. Pokażemy, że Ψ jest ciągłe. Ustalmy dowolne $L \in \mathcal{A}$. Wystarczy pokazać, że $\Psi_L = \pi_L\Psi$ jest ciągłe, gdzie π_L jest rzutem.

Weźmy dowolne $K \subseteq L' \subseteq L$, takie że $K \subseteq L'$ jest skończone i Galois, wtedy $\mathrm{Gal}(L/L')$ jest otwarta w $\mathrm{Gal}(L/K)$.

$\Psi_L^{-1}(\mathrm{Gal}(L/L') = \{\sigma \in \mathrm{Gal}(M/K) : \sigma|_{L'} = id_{L'}\} = \mathrm{Gal}(M/L')$. Zauważmy, że $\mathrm{Gal}(M/L')$ jest otwarta w $\mathrm{Gal}(M/K)$, a więc z dowolności L' Ψ_L jest ciągłe, a stąd również Ψ jest ciągłe.

Skoro Ψ jest ciągłym izomorfizmem, $\mathrm{Gal}(L/K)$ jest zwarta, $\prod_{L\in\mathcal{A}} \mathrm{Gal}(L/K)$ jest Hausdorffa, to Ψ jest homeomorfizmem na swoj obraz i $\operatorname{im}\Psi$ jest domknięty.

Mamy więc $\mathrm{Gal}(M/K) \cong \Psi(\mathrm{Gal}(M/K)) \leqslant \prod_{L\in\mathcal{A}} \mathrm{Gal}(L/K)$. Otrzymujemy więc, że $\mathrm{Gal}(M/K)$ jest prorozwiązalna jako domknięta podgrupa produktu grup prorozwiązalnych, a więc $K \subseteq M$ jest rozszerzeniem prorozwiązalnym. Zatem z definicji rodziny $\mathcal{A}$ otrzymujemy, że to rozszerzenie jest największe względem inkluzji. □

8 Największe rozszerzenie rozwiązalne

W tym rozdziale skupimy się na rozszerzeniach rozwiązalnych. Jednym z wniosków będzie fakt, że nie istnieje największe (równoważnie maksymalne) rozszerzenie

rozwiązalne ciała $\mathbb{Q}$. Aby to pokazać, posłużymy się przykładem ciągu rozszerzeń $\mathbb{Q}$ o stopniach rozwiązalności zbiegających do nieskończoności, który zaprezentowany został w artykule [5].

Zaczniemy od uzasadnienia wspomnianej wcześniej równoważności między istnieniem największego rozszerzenia rozwiązalnego ciała $\mathbb{Q}$, a istnieniem maksymalnego takiego rozszerzenia. Fakt ten przedstawimy w ogólnej wersji dla dowolnego ciała K.

Lemat 8.1. *K ma maksymalne rozszerzenie rozwiązalne wtedy i tylko wtedy, gdy K ma największe rozszerzenie rozwiązalne.*

Dowód.
$\Longleftarrow$: Z definicji element największy w porządku jest w szczególności elementem maksymalnym.
$\Longrightarrow$: Niech $K \subseteq L$ będzie maksymalnym rozszerzeniem rozwiązalnym. Załóżmy a.a., że dla pewnego $K \subseteq M \subseteq \overline{K}$ rozwiązalnego mamy $M \not\subseteq L$. Wtedy (wobec maksymalności L) również $L \not\subseteq M$, a więc $L \subsetneq LM$.

Pokażemy, że $K \subseteq LM$ jest rozwiązalne. Oczywiście $K \subseteq LM$ jest rozszerzeniem Galois.
Pozostaje sprawdzić, że $\mathrm{Gal}(LM/K)$ jest rozwiązalna, w tym celu pokażemy, że $\mathrm{Gal}(LM/K)$ zanurza się w grupie $\mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$, która jest rozwiązalna jako skończony produkt grup rozwiązalnych.

Rozważmy homomorfizm

$$\begin{aligned} \Psi\colon \mathrm{Gal}(LM/K) &\to \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K) \\ \sigma &\mapsto (\sigma|_L, \sigma|_M) \end{aligned}$$

Zauważmy, że Ψ jest różnowartościowy, ponieważ dla dowolnego $\sigma \in \mathrm{Gal}(LM/K)$, $\Psi(\sigma) = (\mathrm{id}_L, \mathrm{id}_M)$ wtedy i tylko wtedy, gdy $\sigma|L = \mathrm{id}_L$ oraz $\sigma|M = \mathrm{id}_M$, co jest równoważne $\sigma = \mathrm{id}_{LM}$.

Pokazaliśmy zatem, że $\mathrm{Gal}(LM/K) \cong \Psi(\mathrm{Gal}(LM/K)) \leqslant \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$, czyli $\mathrm{Gal}(LM/K)$ jest grupą rozwiązalną.

Mamy zatem, że $K \subseteq LM \subseteq \bar{K}$ jest rozwiązalne i $L \subsetneq LM$, co daje sprzeczność z maksymalnością L, a więc L jest największym rozszerzeniem rozwiązalnym K. $\square$

W dalszej części będziemy zakładać, że $n < \omega$ oznaczać będzie, że n jest liczbą naturalną większą od 0.

Definicja 8.2. Niech G będzie dowolną grupą, (H, X) będzie grupą permutacji, a G^X - grupą wszystkich funkcji z X w G z mnożeniem punktowym.

Splotem $G \wr H$ będziemy nazywać produkt półprosty $G^X \rtimes_\phi H$, gdzie działanie $\phi : H \to \mathrm{Aut}(G^X)$ definiujemy jako $h \cdot_\phi \theta(x) = \theta(h^{-1}(x))$.

Uwaga 8.3. Jeśli dodatkowo (G, Y) jest grupą permutacji, to $G \wr H$ działa na zbiorze $Y \times X$ w następujący sposób: $(g, h) \cdot (y, x) := (g(hx)y, hx)$.

Lemat 8.4. *Niech (H, Z), (F, Y), (G, X) będą grupami permutacji. Wówczas istnieje izomorfizm*

$$\Psi : (H \wr (F \wr G), Z \times Y \times X) \xrightarrow{\cong} ((H \wr F) \wr G, Z \times Y \times X)$$

zachowujący działanie grupy $H \wr (F \wr G)$ na zbiorze $Z \times Y \times X$, to znaczy, taki że dla dowolnych $(h; f, g) \in H \wr (F \wr G), (z, y, x) \in Z \times Y \times X$, zachodzi:

$$(h; f, g) \cdot (z, y, x) = \Psi(h; f, g) \cdot (z, y, x)$$

Dowód. Definiujemy

$$\begin{aligned} \Psi \colon H \wr (F \wr G) &\to (H \wr F) \wr G \\ (h; f, g) &\mapsto (\theta, g) \end{aligned}$$

gdzie

$$\begin{aligned} \theta \colon X &\to H \wr F \\ x &\mapsto (\tilde{h}, f(x)) \end{aligned}$$

przy czym $\tilde{h} : Y \to H$ zadana przez $\tilde{h}(y) = h(y, x)$.

Pokażemy najpierw, że Ψ jest homomorfizmem.

Ustalmy dowolne $(h; f, g), (h'; f', g') \in H \wr (F \wr G)$. Z definicji działania w produkcie półprostym: $(h; f, g)(h'; f', g') = (h((f, g) \cdot h'), f(g \cdot f'), gg')$.

Niech $(\theta_1, gg') := \Psi(h((f, g) \cdot h'), f(g \cdot f'), gg')$; $(\theta, g) := \Psi(h; f, g)$ oraz $(\theta', g') := \Psi(h'; f', g')$. Zauważmy, że $(\theta, g)(\theta', g') = (\theta(g \cdot \theta'), gg')$. Zatem wystarczy sprawdzić, że $\theta_1 = \theta(g \cdot \theta')$.

Ustalmy dowolny $x \in X$. Wówczas $\theta_1(x) = (\tilde{h_1}, f(x)f'(g^{-1}x))$, gdzie

$$\begin{aligned} \tilde{h_1} \colon Y &\to H \\ y &\mapsto h(y, x)h'(f(x)^{-1}y, g^{-1}x). \end{aligned}$$

Z drugiej strony $\theta(g \cdot \theta')(x) = \theta(x)(g \cdot \theta')(x) = (\tilde{h}, f(x))(\tilde{h'}, f'(g^{-1}x))$, gdzie

$$\begin{aligned} \tilde{h'} \colon Y &\to H \\ y &\mapsto h'(y, g^{-1}x). \end{aligned}$$

Wówczas $(\tilde{h}, f(x))(\tilde{h'}, f'(g^{-1}x)) = (\tilde{h}(f(x) \cdot \tilde{h'}), f(x)f'(g^{-1}x))$ i dla dowolnego $y \in Y$ mamy:

$$\tilde{h}(f(x) \cdot \tilde{h'})(y) = h(y, x)h'(f(x)^{-1}y, g^{-1}x) = \tilde{h_1}(y).$$

Pokazaliśmy więc, że Ψ jest homomorfizmem. Sprawdzimy, że Ψ jest monomorfizmem. Ustalmy dowolne $(h; f, g) \neq (h'; f', g') \in H \wr (F \wr G)$. Bez straty ogólności załóżmy, że $g = g'$ oraz $h' \neq h$ lub $f' \neq f$, to znaczy istnieje $(y, x) \in Y \times X$, taki że $h'(y, x) \neq h(y, x)$ lub istnieje $x' \in X$, taki że $f(x') \neq f'(x')$. Wtedy $\Psi(h; f, g) \neq \Psi(h'; f', g')$.

Pokażemy, że Ψ jest "na". Ustalmy dowolny $(\alpha, g) \in (H \wr F) \wr G)$, to znaczy $\alpha \in (H \wr F)^X, g \in G$. Z defnicji F^X jest zbiorem wszystkich funkcji z X w F, czyli w szczególności $f := \pi_2\alpha \in F^X$ (gdzie π_2 jest rzutem na drugą oś). Podobnie w $H^{Y \times X}$ jest zbiorem wszystkich funkcji z $Y \times X$ w H, zatem w szczególności funkcja:

$$\begin{aligned} h \colon Y \times X &\to H \\ (y, x) &\mapsto \pi_1(\alpha(x))(y) \end{aligned}$$

gdzie π_1 jest rzutem na pierwszą oś, jest elementem $H^{Y\times X}$. Zauważmy, że $\Psi(h;f,g) = (\alpha, g)$. Wobec dowolności (α, g), Ψ jest "na". Pokazaliśmy zatem, że Ψ jest izomorfizmem.

Przejdziemy teraz do uzasadnienia, że Ψ zachowuje działanie grupy $H \wr (F \wr G)$ na zbiorze $Z \times Y \times X$. Ustalmy dowolne $(z, y, x) \in Z \times Y \times X, (h; f, g) \in H \wr (F \wr G)$. Wówczas:

$$(h; f, g) \cdot (z, y, x) = (h((f, g) \cdot (y, x))z, (f, g) \cdot (y, x)) = (h(f(gx)y, gx)z, f(gx)y, gx).$$

Z drugiej strony

$$\Psi(h; f, g) = (\theta, g) \cdot (z, y, x) = (\theta(gx)(z, y), gx) = ((\tilde{h}, (f(gx))(z, y), gx) =$$

$$(h(f(gx)y, gx)z, f(gx)y, gx),$$

a więc działanie jest zachowywane. □

W dalszej części będziemy rozważać ciąg wielomianów o współczynnikach wymiernych $(f_n)_{n<\omega}$ zdefiniowany następująco:

$$f_1(x) = x^2 + 2$$

$$f_{n+1}(x) = f_n(f_1(x)).$$

Niech dodatkowo $c_n = f_n(0), K_0 = \mathbb{Q}$, zaś K_{n+1} będzie ciałem rozkładu wielomianu f_{n+1} nad ciałem K_n. Zauważmy, że ciąg ciał $(K_n)_{n=0}^{\infty}$ jest wstępujący. Ponadto dla każdego $n < \omega$, $\mathbb{Q} \subseteq K_n$ jest rozszerzeniem Galois.

Uwaga 8.5. Wprost z definicji $(f_n)_{n<\omega}$ otrzymujemy, że dla dowolnego $k < n$, $f_k(f_{n-k}(x)) = f_n(x) = f_{n-k}(f_k(x))$.

Uwaga 8.6. Dla każdego $n < \omega$, $f_n(x)$ jest moniczny.

Dowód. Indukcja względem n. Dla $n = 1$, $f_n(x) = x^2+2$, czyli uwaga jest prawdziwa. Załóżmy, że $n > 1$ i uwaga jest prawdziwa dla wszystkich $k < n$. Niech $f_{n-1}(x) = \sum_{i=0}^{2^{n-1}} b_i x^i$. Z założenia indukcyjnego $b_{2^{n-1}} = 1$. Zauważmy, że $f_n(x) = f_{n-1}(f_1(x)) = \sum_{i=0}^{2^{n-2}} b_i(f_1(x))^i + b_{2^{n-1}} f_1(x)^{2^{n-1}} = \sum_{i=0}^{2^{n-2}} b_i(f_1(x))^i + b_{2^{n-1}} \sum_{j=0}^{2^{n-1}} \binom{2^{n-1}}{j} (x^2)^{2^{n-1}-j} 2^j = \sum_{i=0}^{2^{n-2}} b_i(f_1(x))^i + b_{2^{n-1}} \sum_{j=1}^{2^{n-1}} \binom{2^{n-1}}{j} (x^2)^{2^{n-1}-j} 2^j + b_{2^{n-1}} \binom{2^{n-1}}{0} x^{2^n}$. Ostatni składnik powyższej sumy, to jedyny w którym występuje x^{2n} i z założenia indukcyjnego $b_{2^{n-1}} = 1$. Pokazaliśmy zatem, że f_n jest moniczny. □

Uwaga 8.7. Dla każdego $n < \omega$, f_n jest nierozkładalny nad $\mathbb{Q}$.

Dowód. Przez indukcję względem n sprawdzimy, że f_n spełnia założenia kryterium Eisensteina dla $p = 2$. Dla $n = 1, f_n(x) = x^2 + 2$, a więc są one spełnione. Ustalmy więc, że $n > 1$ i dla każdego $k < n$, f_k spełnia wyżej wymienione założenia. Niech

$f_n(x) = \sum_{i=0}^{2^n} a_i x^i$ oraz $f_{n-1} = \sum_{i=0}^{2^{n-1}} b_i x^i$. Zauważmy, że wtedy $f_n(x) = \sum_{i=0}^{2^{n-1}} b_i (x^2+2)^i = \sum_{i=0}^{2^{n-1}} b_i \sum_{j=0}^{i} \binom{i}{j} 2^j x^{2(i-j)} = \sum_{i=0}^{2^{n-1}} b_i (x^{2i} + 2ix^{2(i-1)} + \cdots + 2^{i-1} i x^2 + 2^i)$. W powyższej sumie dla każdego $i < 2^{n-1}$, każdy współczynnik występujący przy x^i jest podzielny przez 2, a więc a_i jest podzielny przez 2. Ponadto 2 nie dzieli a_{2^n}, ponieważ z wcześniejszej uwagi f_n jest moniczny. Pozostaje sprawdzić, że 4 nie dzieli a_0. Zauważmy, że $r_4(a_0) = r_4(f_n(0)) = r_4(f_{n-1}(2)) = r_4(b_0 + 2b_1 + \cdots + 2^{2^{n-1}} b_{2^{n-1}}) = r_4(b_0)$, zatem korzystając z założenia indukcyjnego $r_4(a_0) \neq 0$. Pokazaliśmy więc, że f_n spełnia założenia kryterium Eisensteina dla $p = 2$, zatem f_n jest nierozkładalny nad $\mathbb{Q}$. □

Wniosek 8.8. *Dla każdego $n < \omega$, f_n jest rozdzielczy nad $\mathbb{Q}$.*

Uwaga 8.9. Przez $\mathbb{Z}_2$ będziemy oznaczać $(\mathbb{Z}_2, +_2)$. Działanie $\mathbb{Z}_2$ na zbiorze $\{0,1\}$ będzie dane przez działanie $\mathbb{Z}_2$ na $\mathbb{Z}_2$ przez translacje.

Ustalmy dowolny $1 < n < \omega$. Niech $a_0, \ldots, a_{2^{n-1}-1}$ będą parami różnymi pierwiastkami f_{n-1} oraz $b_0, \ldots, b_{2^n-1}$ będą parami różnymi pierwiastkami f_n. Zauważmy, że $f_n = \prod_{i=0}^{2^{n-1}-1} (x^2 + 2 - a_i)$, stąd dla każdego a_i oraz dla każdego $\epsilon \in \{0,1\}$, $(-1)^\epsilon \sqrt{a_i - 2}$ jest pierwiastkiem f_n. W ten sposób każdy b_j można jednoznacznie przestawić jako parę (i_j, ϵ_j), taką że $b_j = (-1)^{\epsilon_j} \sqrt{a_{i_j} - 2}$.

Rozumując rekurencyjnie dostajemy naturalne utożsamienia między zbiorami $\{b_0, \ldots, b_{2^n-1}\}$, $\{0, \ldots, 2^n - 1\}$, $\mathbb{Z}_2 \times \{0, \ldots, 2^{n-1} - 1\}$, $\mathbb{Z}_2^n$ oraz $\{0, \ldots, 2^{n-1} - 1\} \times \mathbb{Z}_2$ zadane przez:

$$b_j \mapsto j \mapsto (\epsilon_j, i_j) \mapsto (\epsilon_0^j, \ldots, \epsilon_{n-1}^j) \mapsto (i'_j, \epsilon'_j)$$

dla odpowiednich $\epsilon_0^j, \ldots, \epsilon_n^j \in \mathbb{Z}_2$, gdzie i'_j odpowiada ciągowi $(\epsilon_0^j, \ldots, \epsilon_{n-2}^j)$ oraz $\epsilon'_j := \epsilon_{n-1}^j$.

Rekurencyjnie definiujemy ciąg grup $(G_n, \{0, \ldots, 2^n - 1\})$ następująco:
$G_1 := \mathbb{Z}_2$
$G_n := G_{n-1} \wr \mathbb{Z}_2$ z działaniem $(g, \epsilon) \cdot_n j = (g(\epsilon \epsilon'_j) \cdot_{n-1} i'_j, \epsilon \cdot_1 \epsilon'_j)$.

Dla uproszczenia notacji w dalszej części $+_2$ będziemy pomijać, jeśli z kontekstu będzie wynikać, że wykonujemy działanie w grupie $(\mathbb{Z}_2, +_2)$.

Uwaga 8.10. Dla każdego $n < \omega$, $|G_n| = 2^{2^{n-1} + 2^{n-2} + \ldots + 2 + 1}$

Dowód. Przeprowadzimy indukcję względem n. Jeśli $n = 1$, to $|G_1| = |\mathbb{Z}_2| = 2$. Załóżmy więc, że $n > 1$ i dla każdego $k < n$ teza zachodzi. Wówczas $|G_n| = |G_{n-1} \wr \mathbb{Z}_2| = 2(2^{2^{n-2} + 2^{n-3} + \ldots + 2 + 1})^2 = 2^{2^{n-1} + 2^{n-2} + \ldots + 2 + 1}$. □

W dalszej części, dla dowolnej grupy G, przez G^{ab} oznaczać będziemy $G/[G,G]$.

Lemat 8.11. *Dla każdego $n < \omega$, $G_n^{ab} \cong \prod_{i=1}^{n} \mathbb{Z}_2$.*

Dowód. Indukcja względem n. Jeśli $n = 1$, to $G_n = \mathbb{Z}_2$, a więc jest grupą abelową, zatem $G_n^{ab} \cong \mathbb{Z}_2$.

Niech $n > 1$ i załóżmy, że lemat zachodzi dla $k < n$. Dowolny element $(f, \epsilon) \in G_n$, taki że $f(0) = g, f(1) = h$, możemy przedstawić jako $(g, h; \epsilon)$. Pokażemy najpierw, że dla każdego $g \in G_{n-1}$, $(g, g^{-1}; 0) \in (G_n)'$. Ustalmy dowolny $g \in G_{n-1}$. Zauważmy, że wtedy $(g, g^{-1}; 0) = (e, g^{-1}; 1)(e, g; 1) = (e, e; 1)(g^{-1}, e; 0)(e, e; 1)(g, e; 0) = (e, e; 1)(g^{-1}, e; 0)(e, e; 1)^{-1}(g^{-1}, e; 0)^{-1}$, a więc $(g, g^{-1}; 0) \in (G_n)'$.

Rozważmy epimorfizm

$$\begin{aligned} \Psi \colon G_{n-1} \wr \mathbb{Z}_2 &\to G_{n-1}^{ab} \times \mathbb{Z}_2 \\ (g_0, g_1; \epsilon) &\mapsto (g_0 g_1 (G_{n-1})', \epsilon). \end{aligned}$$

Pokażemy, że $\ker \Psi = (G_n)'$. Ustalmy dowolny $(g_0, g_1; \epsilon) \in \ker \Psi$. Wtedy $\epsilon = 0$ oraz $g_0 g_1 \in (G_{n-1})'$, to znaczy $g_0 g_1 = aba^{-1}b^{-1}$ dla pewnych $a, b \in G_{n-1}$, a stąd $(g_0 g_1, e; 0) = (a, e; 0)(b, e; 0) \cdot (a, e; 0)^{-1}(b, e; 0)^{-1} \in (G_n)'$.

Powyżej sprawdziliśmy, że $(g_1, g_1^{-1}; 0) \in (G_n)'$, stąd $(g_0, g_1; 0)(G_n)' = (g_0, g_1; 0)(g_1, g_1^{-1}; 0)(G_n)'$, a więc $(g_0, g_1; 0)(G_n)' = (g_0 g_1, e; 0)(G_n)' = (G_n)'$. Wobec dowolności $(g_0, g_1, \epsilon) \in \ker \Psi$, otrzymujemy $\ker \Psi \subseteq (G_n)'$.

Ponadto $G_n / \ker \Psi \cong G_n^{ab} \times \mathbb{Z}_2$, jest abelowa. Stąd $\ker \Psi = (G_n)'$ oraz $G_n/(G_n)' \cong G_{n-1}^{ab} \times \mathbb{Z}_2$. Dodatkowo z założenia indukcyjnego $G_{n-1}^{ab} \cong \prod_{i=1}^{n-1} \mathbb{Z}_2$, zatem $G_n^{ab} \cong \prod_{i=1}^{n} \mathbb{Z}_2$. □

Lemat 8.12. *Dla każdego $n < \omega$, istnieje izomorfizm grupy $\mathbb{Z}_2 \wr G_n$ w grupę $G_n \wr \mathbb{Z}_2$ zachowujący działanie $\mathbb{Z}_2 \wr G_n$ na zbiorze $\{0, \ldots, 2^{n+1} - 1\}$ zadane przez $(f, g) \cdot j = (f(gi_j)\epsilon_j, gi_j)$ (gdzie (i_j, ϵ_j) jest parą odpowiadającą j w sposób opisany powyżej).*

Dowód. Przeprowadzimy indukcję względem n. Dla $n = 1$ zachodzi $G_n \wr \mathbb{Z}_2 = \mathbb{Z}_2 \wr \mathbb{Z}_2 = \mathbb{Z}_2 \wr G_n$. Pozostaje sprawdzić, że dla dowolnych $(f, \epsilon) \in \mathbb{Z}_2 \wr \mathbb{Z}_2$ oraz $j \in \{0, \ldots, 3\}$, $(f, \epsilon) \cdot_2 j = (f, \epsilon) \cdot j$. Ustalmy więc dowolny $j \in \{0, \ldots, 3\}$, który w opisany powyżej sposób utożsamiamy z (i_j, ϵ_j) oraz (ϵ'_j, i'_j). Zauważmy, że $(i_j, \epsilon_j) = (\epsilon'_j, i'_j)$. Wówczas, dla dowolnego $(f, \epsilon) \in \mathbb{Z}_2$, $(f, \epsilon) \cdot_2 j = (f(\epsilon\epsilon'_j)i'_j, \epsilon\epsilon'_j) = (f(\epsilon i_j)\epsilon_j, \epsilon i_j) = (f, \epsilon) \cdot j$, a więc dla $n = 1$ lemat zachodzi. Załóżmy więc, że $n > 1$ i dla każdego $k < n$ lemat jest prawdziwy.

Z założenia indukcyjnego mamy pewien $\Lambda : \mathbb{Z}_2 \wr G_{n-1} \xrightarrow{\cong} G_{n-1} \wr \mathbb{Z}_2$ zachowujący działanie $\mathbb{Z}_2 \wr G_{n-1}$ na zbiorze $\{0, ..., 2^n - 1\}$. Z lematu 8.2. $\mathbb{Z}_2 \wr (G_{n-1} \wr \mathbb{Z}_2) \cong (\mathbb{Z}_2 \wr G_{n-1}) \wr \mathbb{Z}_2$ zachowując działanie, zatem wystarczy pokazać, że

$$\begin{aligned} \Psi \colon (\mathbb{Z}_2 \wr G_{n-1}) \wr \mathbb{Z}_2 &\to (G_{n-1} \wr \mathbb{Z}_2) \wr \mathbb{Z}_2 \\ (f, \epsilon) &\mapsto (\Lambda f, \epsilon) \end{aligned}$$

gdzie Λf jest złożeniem funkcji, jest izomorfizmem zachowującym działanie $(\mathbb{Z}_2 \wr G_{n-1}) \wr \mathbb{Z}_2$ na zbiorze $\{0, \ldots, 2^{n+1} - 1\}$.

Sprawdzimy, że Ψ jest różnowartościowa. Ustalmy dowolne $(f_1, \epsilon_1) \neq (f_2, \epsilon_2)$ należące do $(\mathbb{Z}_2 \wr G_{n-1}) \wr \mathbb{Z}_2$. Bez straty ogólności niech $\epsilon_1 = \epsilon_2$, wówczas istnieje $\epsilon \in \mathbb{Z}_2$

taki, że $f_1(\epsilon) \neq f_2(\epsilon)$. Przypomnijmy, że Λ jest w szczególności różnowartościowa, stąd $\Lambda(f_1(\epsilon)) \neq \Lambda(f_2(\epsilon))$, a więc $\Lambda f_1 \neq \Lambda f_2$, czyli $\Psi((f_1, \epsilon_1)) \neq \Psi((f_2, \epsilon_2))$. Oczywiście Ψ jest "na", ponieważ dla dowolnego $(f, \epsilon) \in (G_{n-1} \wr \mathbb{Z}_2) \wr \mathbb{Z}_2$, mamy $(\Lambda^{-1} f, \epsilon) \in (\mathbb{Z}_2 \wr G_{n-1}) \wr \mathbb{Z}_2$.

Pokażemy, że Ψ jest homomorfizmem. Ustalmy dowolne $(f_1, \epsilon_1), (f_2, \epsilon_2)$ należące do $(\mathbb{Z}_2 \wr G_{n-1}) \wr \mathbb{Z}_2$, wówczas $\Psi((f_1, \epsilon_1)(f_2, \epsilon_2)) = \Psi(f_1(\epsilon_1 \cdot f_2), \epsilon_1\epsilon_2) = (\Lambda(f_1(\epsilon_1 \cdot f_2)), \epsilon_1\epsilon_2) = (\Lambda f_1 \Lambda(\epsilon_1 \cdot f_2), \epsilon_1\epsilon_2)$, gdzie ostatnia równość zachodzi, ponieważ Λ jest z założenia indukcyjnego homomorfizmem.

Z drugiej strony $\Psi(f_1, \epsilon_1)\Psi(f_2, \epsilon_2) = (\Lambda f_1, \epsilon_1)(\Lambda f_2, \epsilon_2) = (\Lambda f_1(\epsilon_1 \cdot \Lambda f_2), \epsilon_1\epsilon_2)$. Oczywiście dla dowolnego $\epsilon \in \mathbb{Z}_2$ zachodzi $\epsilon_1 \cdot \Lambda f_2(\epsilon) = \Lambda(f_2(\epsilon_1^{-1}\epsilon)) = \Lambda(\epsilon_1 \cdot f_2)(\epsilon)$, zatem Ψ jest homomorfizmem.

Pozostaje sprawdzić, że Ψ zachowuje działanie $(\mathbb{Z}_2 \wr G_{n-1}) \wr \mathbb{Z}_2$ na zbiorze $\{0, ..., 2^{n+1} - 1\}$
Ustalmy dowolne $j \in \{0, \ldots, 2^{n+1} - 1\}$ oraz $(f, \epsilon) \in (\mathbb{Z}_2 \wr G_{n-1}) \wr \mathbb{Z}_2$. Wówczas $\Psi(f, \epsilon) \cdot j = (\Lambda f, \epsilon) \cdot j = (\Lambda f(\epsilon\epsilon_j) \cdot i_j, \epsilon\epsilon_j)$. Z założenia indukcyjnego Λ zachowuje działanie, a więc $(\Lambda f(\epsilon\epsilon_j) \cdot i_j, \epsilon\epsilon_j) = (f(\epsilon\epsilon_j) \cdot i_j, \epsilon\epsilon_j) = (f, \epsilon) \cdot j$.

Pokazaliśmy więc, że $\mathbb{Z}_2 \wr G_n \cong G_n \wr \mathbb{Z}_2$ zachowując działanie. □

Twierdzenie 8.13. *Dla każdego $n < \omega$, $\mathrm{Gal}(K_n/\mathbb{Q})$ zanurza się w G_n z zachowaniem działania na zbiorze $\{0, \ldots, 2^n - 1\}$.*

Dowód. Indukcja względem n. Dla $n = 1$ oczywiście $\mathrm{Gal}(K_n/\mathbb{Q}) \cong \mathbb{Z}_2$ zachowując działanie, załóżmy więc, że $n > 1$ i twierdzenie jest prawdziwe dla $k < n$. W opisany wcześniej sposób utożsamiamy zbiór pierwiastków f_n ze zbiorem par $\{(\epsilon, i) : 0 \leqslant i \leqslant 2^{n-1} - 1, 0 \leqslant \epsilon \leqslant 1\}$. Zauważmy, że dla każdych $r \leqslant k < \omega$ dowolny $\sigma \in \mathrm{Gal}(K_k/\mathbb{Q})$ permutuje pierwiastki f_r, więc σ możemy w naturalny sposób traktować jako permutację zbioru $\{0, \ldots, 2^r - 1\}$.

Ustalmy dowolny $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$, $\mathbb{Q} \subseteq K_{n-1}$ jest normalne, a więc $\sigma|_{K_{n-1}} \in \mathrm{Gal}(K_{n-1}/\mathbb{Q})$. Ponadto, dla ustalonego i, σ wyznacza $\sigma_i \in \mathbb{Z}_2$ w następujący sposób

$$\sigma(\epsilon, i) = (\sigma_i\epsilon, \sigma|_{K_{n-1}} i)(= (\sigma_i\epsilon, \sigma i)).$$

Wówczas w naturalny sposób σ wyznacza permutację zbioru

$$\{(\epsilon, i) : 0 \leqslant i \leqslant 2^{n-1} - 1, 0 \leqslant \epsilon \leqslant 1\}.$$

Rozważmy:

$$\begin{aligned} \Psi\colon \mathrm{Gal}(K_n/\mathbb{Q}) &\to \mathbb{Z}_2 \wr \mathrm{Gal}(K_{n-1}/\mathbb{Q}) \\ \sigma &\mapsto (\sigma|_{K_{n-1}} \cdot \theta_\sigma, \sigma|_{K_{n-1}}). \end{aligned}$$

Gdzie:

$$\begin{aligned} \theta_\sigma\colon \{0, ..., 2^{n-1} - 1\} &\to \mathbb{Z}_2 \\ i &\mapsto \sigma_i. \end{aligned}$$

Sprawdzimy, że Ψ jest homomorfizmem. Niech $\sigma, \tau \in \mathrm{Gal}(K_n/\mathbb{Q})$.
$\Psi(\sigma\tau) = ((\sigma\tau)|_{K_{n-1}} \cdot \theta_{\sigma\tau}, (\sigma\tau)|_{K_{n-1}})$, a $\Psi(\sigma)\Psi(\tau) = (\sigma|_{K_{n-1}} \cdot \theta_\sigma,\ \sigma|_{K_{n-1}})(\tau|_{K_{n-1}} \cdot \theta_\tau, \tau|_{K_{n-1}}) = (\sigma|_{K_{n-1}} \cdot \theta_\sigma(\sigma|_{K_{n-1}} \cdot (\tau|_{K_{n-1}} \cdot \theta_\tau)), (\sigma\tau)|_{K_{n-1}})$.
Ustalmy dowolny $0 \leqslant i \leqslant 2^{n-1} - 1$, wtedy

$$((\sigma\tau)|_{K_{n-1}} \cdot \theta_{(\sigma\tau)})(i) = (\sigma\tau)_{(\sigma\tau)^{-1}(i)}$$

$$(\sigma|_{K_{n-1}} \cdot \theta_\sigma(\sigma|_{K_{n-1}} \cdot (\tau|_{K_{n-1}} \cdot \theta_\tau)))(i) = \theta_\sigma(\sigma^{-1}(i))(\tau|_{K_{n-1}} \cdot \theta_\tau(\sigma^{-1}(i))) = \sigma_{\sigma^{-1}(i)}\tau_{(\sigma\tau)^{-1}(i)}.$$

Zauważmy, że dla każdego ϵ zachodzi

$$(\sigma\tau)(\epsilon, (\sigma\tau)^{-1}(i)) = \sigma(\tau_{(\sigma\tau)^{-1}(i)}(\epsilon), \tau(\sigma\tau)^{-1}(i)) = \sigma(\tau_{(\sigma\tau)^{-1}(i)}(\epsilon), \sigma^{-1}(i)) = (\sigma_{\sigma^{-1}(i)}(\tau_{(\sigma\tau)^{-1}(i)}(\epsilon)), i).$$

Z drugiej strony $(\sigma\tau)(\epsilon, (\sigma\tau)^{-1}(i)) = ((\sigma\tau)_{(\sigma\tau)^{-1}(i)}(\epsilon), i)$, stąd $\Psi(\sigma\tau) = \Psi(\sigma)\Psi(\tau)$, a więc Ψ jest homomorfizmem.

Ψ jest monomorfizmem, ponieważ $\Psi(\sigma) = \mathrm{id}$ wtedy i tylko wtedy, gdy dla każdej pary (i, ϵ), $\sigma(i) = i$ oraz $\sigma_i = 0$ (równoważnie, $\sigma_i\epsilon = \epsilon$), co jest równoważne $\sigma = \mathrm{id}_{K_n}$.

Sprawdzimy, że Ψ zachowuje działanie. Ustalmy dowolny $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$ oraz $j \in \{0, \ldots, 2^n - 1\}$, któremu odpowiada para (ϵ, i). Wtedy $\sigma \cdot j = (\theta_\sigma(i)\epsilon, \sigma i)$.

Z drugiej strony $\Psi(\sigma) \cdot j = (\sigma|_{K_{n-1}} \cdot \theta_\sigma, \sigma|_{K_{n-1}}) \cdot (\epsilon, i) = (\theta_\sigma(i)\epsilon, \sigma i)$. Zatem Ψ zachowuje działanie. Przejdziemy do pokazania, że $\mathbb{Z}_2 \wr \mathrm{Gal}(K_{n-1}/\mathbb{Q})$ zanurza się w $\mathbb{Z}_2 \wr G_{n-1}$ zachowując działanie na $\{0, \ldots, 2^n - 1\}$.

Przypomnijmy, że z założenia indukcyjnego istnieje $\Gamma : \mathrm{Gal}(K_{n-1}/\mathbb{Q}) \to G_{n-1}$, monomorfizm zachowujący działanie na zbiorze $\{0, \ldots, 2^{n-1} - 1\}$. Rozważmy:

$$\begin{aligned} \Lambda \colon \mathbb{Z}_2 \wr \mathrm{Gal}(K_{n-1}/\mathbb{Q}) &\to \mathbb{Z}_2 \wr G_{n-1} \\ (\theta, \sigma) &\mapsto (\theta, \Gamma(\sigma)). \end{aligned}$$

Oczywiście Λ jest różnowartościowa, ponieważ Γ jest różnowartościowa.

Sprawdzimy, że Λ jest homorfizmem. Ustalmy dowolne $(\theta_1, \sigma_1), (\theta_2, \sigma_2)$ należące do $\mathbb{Z}_2 \wr \mathrm{Gal}(K_{n-1}/\mathbb{Q})$. Wyliczamy, że $\Lambda((\theta_1, \sigma_1) \cdot (\theta_2, \sigma_2)) = \Lambda(\theta_1(\sigma_1 \cdot \theta_2), \sigma_1\sigma_2) = (\theta_1(\sigma_1 \cdot \theta_2), \Gamma(\sigma_1\sigma_2))$.

Z drugiej strony $\Lambda(\theta_1, \sigma_1)\Lambda(\theta_2, \sigma_2) = (\theta_1(\Gamma(\sigma_1) \cdot \theta_2), \Gamma(\sigma_1\sigma_2))$. Zauważmy, że założenia indukcyjnego dla dowolnego $i \in \{0, \ldots, 2^{n-1} - 1\}$, $\sigma_1^{-1}i = \Gamma(\sigma_1^{-1})i = \Gamma(\sigma_1)^{-1}i$, a więc dla każdego $i \in \{0, \ldots, 2^{n-1} - 1\}$, $\theta_1(\Gamma(\sigma_1) \cdot \theta_2)(i) = \theta_1(\sigma_1 \cdot \theta_2)(i)$. Zatem Λ jest homomorfizmem.

Pokażemy, że Λ zachowuje działanie. Ustalmy dowolne $j \in \{0, \ldots, 2^n - 1\}$, któremu odpowiada para (ϵ, i) oraz $(\theta, \sigma) \in \mathbb{Z}_2 \wr \mathrm{Gal}(K_{n-1}/\mathbb{Q})$, wtedy $(\theta, \sigma) \cdot (\epsilon, i) = (\theta(\sigma i)\epsilon, \sigma i)$.

Z drugiej strony $\Lambda(\theta, \sigma) \cdot (\epsilon, i) = (\theta, \Gamma(\sigma)) \cdot (\epsilon, i) = (\theta(\Gamma(\sigma)i)\epsilon, \Gamma(\sigma)i) = (\theta(\sigma i)\epsilon, \sigma i)$, a więc działanie jest zachowywane.

Pokazaliśmy, że $\Lambda\Psi : \mathrm{Gal}(K_n/\mathbb{Q}) \to \mathbb{Z}_2 \wr G_{n-1}$ jest zanurzeniem zachowującym działanie na zbiorze $\{0, \ldots, 2^n - 1\}$, co w połączeniu z lematem 8.12. dowodzi istnienia zanurzenia $\mathrm{Gal}(K_n/\mathbb{Q})$ w G_n zachowującego działanie. □

Wniosek 8.14. *Dla każdego $n < \omega$, $\mathrm{Gal}(K_{n+1}/\mathbb{Q}) \cong G_{n+1}$ wtedy i tylko wtedy, gdy $\mathrm{Gal}(K_n/\mathbb{Q}) \cong G_n$ i $[K_{n+1} : K_n] = 2^{2^n}$.*

Dowód. Ustalmy dowolny $n < \omega$.
$\Longrightarrow$: Z założenia $\mathrm{Gal}(K_{n+1}/\mathbb{Q}) \cong G_{n+1}$, czyli z uwagi 8.10., $|\mathrm{Gal}(K_{n+1}/\mathbb{Q})| = 2^{2^n+2^{n-1}+\ldots+2+1}$. Z twierdzenia 8.13., $\mathrm{Gal}(K_n/\mathbb{Q})$ zanurza się w G_n, zatem $|\mathrm{Gal}(K_n/\mathbb{Q})| \leqslant 2^{2^{n-1}+2^{n-2}+\ldots+2+1}$. Wówczas $[K_{n+1} : K_n] = \frac{[K_{n+1}:\mathbb{Q}]}{[K_n:\mathbb{Q}]} = \frac{|\mathrm{Gal}(K_{n+1}/\mathbb{Q})|}{|\mathrm{Gal}(K_n/\mathbb{Q})|} \geqslant 2^{2^n}$. Z drugiej strony, $f_{n+1}(x) = \prod_{i=0}^{2^n-1}(x^2 + 2 - a_i)$ gdzie $a_0, \ldots, a_{2^n-1} \in K_n$ są parami różnymi pierwiastkami f_n, a więc $K_{n+1} = K_n(\sqrt{a_0 - 2}, \ldots, \sqrt{a_{2^n-1} - 2})$, czyli $[K_{n+1} : K_n] \leqslant 2^{2^n}$.

Mamy więc, że $[K_{n+1} : K_n] = 2^{2^n}$, stąd $|\mathrm{Gal}(K_n/\mathbb{Q})| = \frac{[K_{n+1}:\mathbb{Q}]}{[K_{n+1}:K_n]} = 2^{2^{n-1}+\ldots+2+1}$, czyli zanurzenie $\mathrm{Gal}(K_n/\mathbb{Q})$ w G_n jest izomorfizmem.
$\Longleftarrow$: Z twierdzenia 8.13., $\mathrm{Gal}(K_{n+1}/\mathbb{Q})$ zanurza się w G_{n+1}, czyli wystarczy pokazać, że $|\mathrm{Gal}(K_{n+1}/\mathbb{Q})| = 2^{2^n+2^{n-1}+\ldots+2+1}$.

Zauważmy, że $|\mathrm{Gal}(K_{n+1}/\mathbb{Q})| = |\mathrm{Gal}(K_n/\mathbb{Q})| \cdot [K_{n+1} : K_n] = (2^{2^{n-1}+2^{n-2}+\ldots+2+1}) \cdot 2^{2^n} = 2^{2^n+2^{n-1}+\ldots+2+1}$. □

Przejdziemy teraz do pokazania, że powyższe zanurzenie grupy $\mathrm{Gal}(K_n/\mathbb{Q})$ w G_n jest izomorfizmem.

Lemat 8.15. *Załóżmy, że $(M, +)$ jest $\mathbb{Z}_2$-modułem, a G jest 2-grupą, dla której dane jest działanie $\phi : G \to \mathrm{Aut}(M, +)$. Wtedy $M^G \neq \{0\}$.*

Dowód. G jest 2-grupą, a więc z definicji $|G| = 2^n$, przy czym $n > 0$. Przeprowadzimy indukcję względem n.

Niech $n = 1$, tj. $G = \langle\sigma\rangle$, gdzie σ jest rzędu 2. Ustalmy dowolne $0 \neq m \in M$. Załóżmy, że $m \notin M^G$. Wtedy $\sigma \cdot_\phi m \neq m$, zatem $\sigma \cdot_\phi (\sigma \cdot_\phi m + m) = m + \sigma \cdot_\phi m = \sigma \cdot_\phi m - m \neq 0$.

Pokazaliśmy zatem, że $0 \neq \sigma \cdot_\phi m + m \in M^G$ to znaczy lemat zachodzi dla $n = 1$. Załóżmy teraz, że $n > 1$ i lemat jest prawdziwy dla $k < n$. G jest 2-grupą, a więc istnieje jej właściwy, nietrywialny dzielnik normalny $H \trianglelefteq G$. Wtedy z założenia indukcyjnego M^H jest nietrywialny.

Zauważmy, że również G/H jest 2-grupą. Ustalmy dowolne $\sigma_1, \sigma_2 \in G, m \in M^H$. Załóżmy, że $\sigma_1 H = \sigma_2 H$, wtedy $\sigma_1 = \sigma_2\tau$ dla pewnego $\tau \in H$ i $\sigma_1 \cdot_\phi m = \sigma_2\tau \cdot_\phi m = \sigma_2 \cdot_\phi m$, czyli możemy zdefiniować działanie φ indukowane przez ϕ następująco:

$$\begin{aligned} \varphi\colon G/H &\to \mathrm{Aut}(M^H, +) \\ \sigma H &\mapsto \phi(\sigma). \end{aligned}$$

Z założenia indukcyjnego $(M^H)^{G/H} \neq \{0\}$.

Pokażemy, że $(M^H)^{G/H} = M^G$. Jeśli $m \in M^G$, to oczywiście $m \in M^H$ i dla dowolnego $gH \in G/H$, $gH \cdot_\varphi m = g \cdot_\phi m = m$, czyli $m \in (M^H)^{G/H}$. W drugą stronę, jeśli $m \in (M^H)^{G/H}$, to dla dowolnego $g \in G$, $g \cdot_\phi m = gH \cdot_\varphi m = m$, stąd $m \in M^G$, zatem $M^G = (M^H)^{G/H} \neq \{0\}$. □

W dalszej części rozdziału, dla dowolnego ciała K przez K^2 będziemy oznaczać zbiór kwadratów w K.

Lemat 8.16. *Dla każdego $n < \omega$, $[K_{n+1} : K_n] = 2^{2^n} \iff c_{n+1} \notin K_n^2$.*

Dowód. Ustalmy dowolny $n < \omega$. Niech $a_0, ..., a_{2^n} - 1 \in K_n$ będą parami różnymi pierwiastkami f_n. Wówczas $c_{n+1} = f_n(2) = \prod_{i=0}^{2^n-1}(2 - a_i)$.
$\Longleftarrow$: Załóżmy, że $c_{n+1} \notin K_n^2$. Ponieważ $K_{n+1} = K_n(\sqrt{a_0 - 2}, \ldots, \sqrt{a_{2^n-1} - 2})$, na mocy lematu 4.6., wystarczy pokazać, że $a_0 - 2, ..., a_{2^n-1} - 2$ są 2-niezależne w K_n.

Zauważmy, że $\prod_{i=0}^{2^n-1}\mathbb{Z}_2$ jest $\mathbb{Z}_2$-modułem przy mnożeniu przez elementy pierścienia zdefiniowanym jako:

$$\epsilon \cdot (d_0, \ldots, d_{2^n-1}) = (\epsilon \cdot_2 d_0, \ldots, \epsilon \cdot_2 d_{2^n-1}).$$

Rozważmy zbiór:

$$V = \{(d_0, ..., d_{2^n-1}) \in \prod_{i=0}^{2^n-1}\mathbb{Z}_2 : \prod_{i=0}^{2^n-1}(a_i - 2)^{d_i} \in K_n^2\}.$$

Sprawdzimy, że $(V, +)$ jest podgrupą $\prod_{i=0}^{2^n-1}\mathbb{Z}_2$. Oczywiście $(0, \ldots, 0) \in V$, ponieważ $(0, \ldots, 0) \in \prod_{i=0}^{2^n-1}\mathbb{Z}_2$ oraz $1 \in K_n^2$. Ustalmy dowolne $(d_0, \ldots, d_{2^n-1}), (c_0, \ldots, c_{2^n-1}) \in V$, wtedy $(d_0 - c_0, \ldots, d_{2^n-1} - c_{2^n-1}) \in \prod_{i=0}^{2^n-1}\mathbb{Z}_2$. Ponadto jeśli $\prod_{i=0}^{2^n-1}(a_i - 2)^{d_i} = k_1^2$ oraz $\prod_{i=0}^{2^n-1}(a_i - 2)^{c_i} = k_2^2$ dla pewnych $k_1, k_2 \in K_n$, to $\prod_{i=0}^{2^n-1}(a_i - 2)^{d_i - c_i} = (k_1 k_2^{-1})^2 \in K_n^2$. Zatem $(d_0, \ldots, d_{2^n-1}) - (c_0, \ldots, c_{2^n-1}) \in V$. Pokazaliśmy więc że $(V, +)$ jest podgrupą $\prod_{i=0}^{2^n-1}\mathbb{Z}_2$. Dodatkowo zauważmy, że dla dowolnych $\epsilon \in \mathbb{Z}_2, \bar{d} \in V$, $\epsilon \cdot \bar{d} \in V$, zatem $(V, +)$ jest w szczególności $\mathbb{Z}_2$-modułem.
Załóżmy nie wprost, że V jest nietrywialny. Zauważmy, że na mocy twierdzenia 8.13. $\mathrm{Gal}(K_n/\mathbb{Q})$ zanurza się w 2-grupie. Ponadto permutacje współrzędnych $\bar{d} \in V$ zadane przez działanie $\mathrm{Gal}(K_n/\mathbb{Q})$ na zbiorze $\{0, \ldots, 2^n - 1\}$ indukują działanie $\phi : \mathrm{Gal}(K_n/\mathbb{Q}) \to \mathrm{Aut}(V, +)$. Z lematu 8.15. otrzymujemy, że $V^{\mathrm{Gal}(K_n/\mathbb{Q})}$ jest nietrywialny, to znaczy istnieje pewien $(0, \ldots, 0) \neq (d_0, \cdots, d_{2^n-1}) \in V$, taki że dla każdego $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q}), (d_{\sigma 0}, \ldots, d_{\sigma 2^n-1}) = (d_0, \ldots, d_{2^n-1})$. Wtedy dla każdego $0 \leqslant i < j \leqslant 2^n - 1$, $d_i = d_j$, czyli $(d_0, \ldots, d_{2^n-1}) = (1, \ldots, 1)$. Z definicji V oznacza to, że $c_{n+1} = \prod_{i=0}^{2^n-1}(a_i - 2)$ należy do K_n^2, co daje sprzeczość z założeniem, że $c_{n+1} \notin K_n^2$. Wobec tego V jest trywialny, czyli $a_0 - 2 \ldots, a_{2^n-1} - 2$ są 2-niezależne w K_n, zatem z lematu 4.6. $[K_{n+1} : K_n] = 2^{2^n}$.
$\Longrightarrow$: Mamy, że $K_{n+1} = K_n(\sqrt{a_0 - 2}, \ldots, \sqrt{a_{2^n-1} - 2})$ oraz dla każdego $0 \leqslant i \leqslant 2^n - 1$, $a_i - 2 \in K_n$, czyli $[K_{n+1} : K_n] \leqslant 2^{2^n}$.

Załóżmy nie wprost, że $c_{n+1} \in K_n^2$. Wtedy $\sqrt{a_0 - 2} = \sqrt{c_{n+1}}\prod_{i=1}^{2^n-1}(\sqrt{a_i - 2})^{-1}$ należy do $K_n(\sqrt{a_1 - 2}, \ldots, \sqrt{a_{2^n-1} - 2})$. Wówczas $K_{n+1} = K_n(\sqrt{a_1 - 2}, \ldots, \sqrt{a_{2^n-1} - 2})$, to znaczy $[K_{n+1} : K_n] < 2^{2^n}$, sprzeczność. □

Lemat 8.17. *Niech* $\mathrm{Gal}(K_n/\mathbb{Q}) \cong G_n$, *a* $c_1, ..., c_n$ *będą 2-niezależne w* $\mathbb{Q}$. *Wówczas dla każdego* $q \in \mathbb{Q}$ *jeśli* $q, c_1, ..., c_n$ *są 2-niezależne w* $\mathbb{Q}$, *to* $q \notin K_n^2$.

Dowód. Z założenia i na mocy lematu 8.11., $\mathrm{Gal}(K_n/\mathbb{Q})^{ab} \cong \prod_{i=1}^{n} \mathbb{Z}_2$. Niech L będzie największym rozszerzeniem abelowym $\mathbb{Q}$ wewnątrz K_n. Z uwagi 6.4. wiemy, że $\mathrm{Gal}(K_n/\mathbb{Q})^{ab}$ jest izomorficzna z $\mathrm{Gal}(L/\mathbb{Q})$, a więc największe rozszerzenie abelowe $\mathbb{Q} \subseteq L$ w K_n jest stopnia 2^n (lemat 3.11.).

Z założenia $c_1, ..., c_n$ są 2-niezależne w $\mathbb{Q}$, a więc z lematu 4.6. $[\mathbb{Q}(\sqrt{c_1}, ..., \sqrt{c_n}) : \mathbb{Q}] = 2^n$. Dodatkowo $c_1, \ldots, c_n \in \mathbb{Q}$, więc $\mathrm{Gal}(\mathbb{Q}(\sqrt{c_1}, ..., \sqrt{c_n})/\mathbb{Q})$ jest izomorficzna z $\prod_{i=1}^{n} \mathbb{Z}_2$. Stąd $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{c_1}, ..., \sqrt{c_n})$ jest rozszerzeniem abelowym stopnia 2^n, zatem $\mathbb{Q}(\sqrt{c_1}, ..., \sqrt{c_n}) = L$.

Załóżmy a.a., że $q \in K_n^2$, to znaczy $\sqrt{q} \in K_n$. Wówczas $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{c_1}, ..., \sqrt{c_n})(\sqrt{q})$ jest rozszerzeniem abelowym zawartym w K_n i skoro $\mathbb{Q}(\sqrt{c_1}, ..., \sqrt{c_n})$ największe takie, to $\sqrt{q} \in \mathbb{Q}(\sqrt{c_1}, ..., \sqrt{c_n})$, czyli w szczególności $[\mathbb{Q}(\sqrt{c_1}, ..., \sqrt{c_n}, \sqrt{q}) : \mathbb{Q}] < 2^{n+1}$. Stąd na mocy lematu 4.6. $c_1, ..., c_n, q$ są 2-zależne w $\mathbb{Q}$, co jest sprzeczne z założeniem. □

Zanim przejdziemy dalej, przypomnijmy że funkcją Möbiusa nazywamy

$$\mu : \mathbb{N}^+ \to \{-1, 0, 1\},$$

$$\mu(n) = \begin{cases} 1, & \text{gdy } n = 1 \\ 0, & \text{gdy istnieje liczba pierwsza } p, \text{taka że } p^2 | n \\ (-1)^r, & \text{gdy } n \text{ jest iloczynem } r \text{ parami różnych liczb pierwszych.} \end{cases}$$

Poniżej sformułujemy podstawowe własności μ, które będziemy wykorzystywać.

Fakt 8.18. *Dla dowolnego $n \in \mathbb{N}^+$,*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \textit{gdy } n = 1 \\ 0, & \textit{w przeciwnym przypadku.} \end{cases}$$

Dowód. [9] 6.6. □

Fakt 8.19. *(Wzór Möbiusa) Załóżmy, że $f, g : \mathbb{N}^+ \to \mathbb{C}$. Wówczas*

$$f(n) = \prod_{d|n} g(d) \iff g(n) = \prod_{d|n} f(d)^{\mu(n/d)}.$$

Dowód. [8] 3.5. □

Lemat 8.20. *Istnieje ciąg liczb całkowitych parami względnie pierwszych $(b_n)_{n=1}^{\infty}$, taki że dla każdego $n < \omega$, $c_n = \prod_{d|n} b_d$.*

Dowód. Ustalmy dowolny $n < \omega$ i niech $b_n = \prod_{d|n} c_d^{\mu(n/d)}$, gdzie μ jest funkcją Möbiusa. Wówczas ze wzoru Möbiusa $c_n = \prod_{d|n} b_d$. Sprawdzimy, że $b_n \in \mathbb{Z}$, to znaczy pokażemy, że dla każdej liczby pierwszej p, $v_p(b_n) \geqslant 0$, gdzie v_p jest waluacją p-adyczną.

Ustalmy dowolną liczbę pierwszą p, dla której istnieje $s < \omega$, taki że p dzieli c_s. Niech l będzie najmniejszym takim indeksem i $e := v_p(c_l) > 0$. Zauważmy, że dla

dowolnego $k < \omega$, jeśli l dzieli k, to dla pewnego $d \in \mathbb{Z}$, mamy $r_{p^e}(c_k) = r_{p^e}(c_{ld}) = r_{p^e}(f_{ld}(0)) = r_{p^e}(f_{(d-1)l}(f_l(0))) = r_{p^e}(f_{(d-1)l}(c_l)) = r_{p^e}(f_{(d-1)l}(0)) = r_{p^e}(f_{(d-2)l}(c_l)) = ... = r_{p^e}(f_l(0)) = r_{p^e}(c_l) = 0$, a wtedy oczywiście p^e dzieli c_k. Ponadto p^{e+1} dzieli c_l^2 i dla każdego $n < \omega$, $f_n \in \mathbb{Q}[x^2]$. Zatem $r_{p^{e+1}}(c_k) = r_{p^{e+1}}(c_{ld}) = r_{p^{e+1}}(f_{ld}(0)) = r_{p^{e+1}}(f_{(d-1)l}(c_l)) = r_{p^{e+1}}(f_{(d-1)l}(0)) = r_{p^{e+1}}(f_{(d-2)l}(c_l)) = \cdots = r_{p^{e+1}}(c_l) \neq 0$.

Z drugiej strony jeśli p dzieli c_k, to l dzieli k, ponieważ w przeciwnym przypadku $k = ls + r$ dla pewnych $s \geqslant 0, r > 0$, $r < l$ oraz $r_{p^e}(c_k) = r_{p^e}(f_k(0)) = r_{p^e}(f_{ls+r}(0)) = r_{p^e}(f_r(f_{ls}(0)))$ i powtarzając wcześniejsze rozumowanie otrzymamy, że $r_{p^e}(f_r(f_{ls}(0))) = r_{p^e}(c_r)$. Z minimalności l dostajemy, że $r_p(c_r) \neq 0$, a więc także $r_p(c_k) \neq 0$.

Pokazaliśmy zatem, że dla dowolnego $k < \omega$

$$v_p(c_k) = \begin{cases} e, & \text{gdy } l \text{ dzieli } k \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

Zauważmy, że wtedy z definicji b_n, $v_p(b_n) = v_p(\prod_{d|n} c^{\mu(n/d)}) = \sum_{d|n} v_p(c_d^{\mu(n/d)}) = \sum_{d|n} \mu(n/d) v_p(c_d) = \sum_{dl|n} \mu(n/dl) v_p(c_{dl}) = \sum_{dl|n} e\mu(n/dl) = e \sum_{dl|n} \mu(n/dl)$, a więc z 8.18. otrzymujemy

$$v_p(b_n) = \begin{cases} e, & \text{gdy } l = n \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

Zatem $v_p(b_n) \geqslant 0$ i dla każdego $b_i \neq b_l$, p nie dzieli b_i. Wobec dowolności p, $b_n \in \mathbb{Z}$ i dla każdego $i \neq n$, b_i, b_n są względnie pierwsze. □

Lemat 8.21. *Dla każdego $n < \omega$, jeśli zdefiniowane powyżej $b_1, ..., b_n \notin \mathbb{Q}^2$ oraz* $\mathrm{Gal}(K_{n-1}/\mathbb{Q}) \cong G_{n-1}$, *to* $\mathrm{Gal}(K_n/\mathbb{Q}) \cong G_n$.

Dowód. Pokażemy, że $c_1, ..., c_n$ są 2-niezależne w $\mathbb{Q}$. Załóżmy a.a., że $c_1, ..., c_n$ są 2-zależne w $\mathbb{Q}$. Niech $1 \leqslant j \leqslant n$ będzie najmniejszym indeksem, dla którego $c_1, ..., c_j$ są 2-zależne. Rozważmy dowolne $a_1, \ldots, a_j \in \mathbb{Z}$, $q \in \mathbb{Q}$ zaświadczające o 2-zależności $c_1, \ldots, c_j$ (w szczególności nie wszystkie a_i są parzyste). W przypadku, gdy $2|a_j$ zachodzi $c_1^{a_1} ... c_{j-1}^{a_{j-1}} = \frac{q^2}{(c_j^{a_j/2})^2} \in \mathbb{Q}^2$. Z minimalności j, dla każdego $1 \leqslant i \leqslant j-1$, 2 dzieli a_i, sprzeczność. Z drugiej strony, zauważmy, że $q^2 = b_1^{a_1} \prod_{d|2} b_d^{a_2} ... \prod_{d|j} b_d^{a_j} = b_j^{a_j} \prod_{\substack{i|j \\ i \neq j}} b_i^{a_i'}$ dla pewnych $a_i' \in \mathbb{Z}$. Przypomnijmy, że b_i są parami względnie pierwsze i $b \notin \mathbb{Q}^2$, a więc 2 dzieli a_j, sprzeczność. Zatem $c_1, ..., c_n$ są 2-niezależne w $\mathbb{Q}$, czyli z lematu 8.17. (z którego korzystamy tutaj dla $n-1$ w miejsce n oraz $q := c_n$) $c_n \notin K_n^2$, a więc z lematu 8.16. $[K_n : K_{n-1}] = 2^{2^{n-1}}$. Mamy więc, że $G_{n-1} \cong \mathrm{Gal}(K_{n-1}/\mathbb{Q})$ i $[K_n : K_{n-1}] = 2^{2^{n-1}}$, zatem z wniosku 8.14. $\mathrm{Gal}(K_n/\mathbb{Q}) \cong G_n$. □

Przejdziemy do pokazania, że dla każdego $n < \omega$, $\mathrm{Gal}(K_n/\mathbb{Q}) \cong G_n$. Na mocy powyższego lematu wystarczy sprawdzić, że żaden z b_i nie jest kwadratem w $\mathbb{Q}$.

Rozważmy ciąg wielomianów $(g_n)_{n<\omega}$ zdefiniowany rekurencyjnie w następujący sposób:

$$g_1(x) = 2x^2 + 1, g_{n+1}(x) = g_n(g_1(x))(= g_1(g_n(x))).$$

Niech dodatkowo $\gamma_n := g_n(0)$ oraz $m_n := \gamma_n + \gamma_{n+1}$.

Uwaga 8.22. Dla każdego $1 < n < \omega$, $r_8(\gamma_n) = 3$ i $r_8(m_n) = 6$.

Dowód. Równość $r_8(m_n) = 6$ wynika natychmiast z pierwszej części uwagi. Dla $n = 2$ mamy $\gamma_n = 3$, załóżmy więc, że $n > 2$ i dla wszystkich $k < n$, $r_8(\gamma_k) = 3$. Obliczamy $r_8(\gamma_n) = r_8(2\gamma_{n-1}^2 + 1) = r_8(2\gamma_{n-1}^2) +_8 1 = 2 +_8 1 = 3$. □

Uwaga 8.23. Dla każdego $n < \omega$, $c_n = 2\gamma_n$.

Dowód. Dla $n = 1$ mamy $c_n = f_n(0) = 2 = 2g_n(0) = 2\gamma_n$. Załóżmy, że $n > 1$ oraz uwaga jest prawdziwa dla wszystkich $k < n$. Wówczas $c_n = f_1(f_{n-1}(0)) = f_1(c_{n-1}) = f_1(2\gamma_{n-1}) = (2\gamma_{n-1})^2 + 2 = 2(2\gamma_{n-1}^2 + 1) = 2\gamma_n$. □

Z powyższej uwagi otrzymujemy, że w szczególności dla każdego $n < \omega$, $\gamma_n > 0$. Definiujemy ciąg $(\beta_n)_{n<\omega}$ następująco:

$$\beta_n := \prod_{d|n} \gamma_d^{\mu(n/d)}.$$

Z uwagi 8.23. dostajemy dodatkowo, że dla każdego $k < \omega$,

$$b_k = \prod_{d|k} c_d^{\mu(k/d)} = \prod_{d|k} (2\gamma_k)^{\mu(k/d)} = \prod_{d|k} 2^{\mu(k/d)} \prod_{d|k} \gamma_k^{\mu(k/d)} = 2^{\sum_{d|k} \mu(k/d)} \beta_k = 2^0 \beta_k = \beta_k,$$

a więc z lematu 8.9. mamy, że $(\beta_n)_{n<\omega} \subseteq \mathbb{Z}$.

Lemat 8.24. *Dla każdej liczby pierwszej $p > 2$, $r_4(p) = 1$ wtedy i tylko wtedy, gdy istnieje $n \in \mathbb{Z}$, taka że p dzieli $n^2 + 1$.*

Dowód. [9] 5.5. □

Lemat 8.25. *Dla każdego $1 < n < \omega$, $\beta_n \notin \mathbb{Q}^2$.*

Dowód. Ustalmy dowolne $1 < n < \omega$. Niech $p_1^{e_1} \dots p_r^{e_r}$ będzie rozkładem n na czynniki pierwsze, $n' := p_1 \dots p_r$, $k := n/n'$.
Z definicji $g_i \in \mathbb{Z}[x^2]$, stąd $r_{m_k}(\gamma_{k+1}) = r_{m_k}(g_1(\gamma_k)) = r_{m_k}(g_1(-\gamma_{k+1})) = r_{m_k}(g_1(\gamma_{k+1})) = r_{m_k}(\gamma_{k+2}) = \dots = r_{m_k}(\gamma_{2k})$, to znaczy $r_{m_k}(\gamma_{2k}) = r_{m_k}(-\gamma_k)$. Ponadto dla dowolnego $1 < l < \omega$, $r_{m_k}(\gamma_{2k}) = r_{m_k}(g_k(\gamma_k)) = r_{m_k}(g_k(-\gamma_k)) = r_{m_k}(g_k(\gamma_{2k})) = r_{m_k}(\gamma_{3k}) = \dots = r_{m_k}(\gamma_{lk})$, czyli $r_{m_k}(\gamma_{lk}) = r_{m_k}(-\gamma_k)$.

Wówczas $\beta_n = \prod_{d|n} \gamma_d^{\mu(n/d)} = \prod_{d|n'} \gamma_{dk}^{\mu(n'/d)} = \gamma_k^{\mu(n')} \prod_{1<d,d|n'} \gamma_{dk}^{\mu(n'/d)}$. Wtedy $\beta_n = \frac{a}{b}$, gdzie:

$$a = \gamma_k^{\mu(n')} \prod_{d \in J_+} \gamma_{dk}^{\mu(n'/d)},\ b = \prod_{d \in J_-} \gamma_{dk}^{-\mu(n'/d)},$$

$$J_+ = \{d|n : 1 < d, \mu(n'/d) \geqslant 0\},\ J_- = \{d|n : 1 < d, \mu(n'/d) < 0\}.$$

W szczególności $\frac{a}{b} \in \mathbb{Z}$.

Z drugiej strony $-1 = -(-\gamma_k)^{\sum\limits_{d|n'} \mu(n'/d)} = -\prod\limits_{d|n'} (-\gamma_k)^{\mu(n'/d)} = -(-\gamma_k)^{\mu(n')}$.

$\prod\limits_{1<d,d|n'} (-\gamma_k)^{\mu(n'/d)} = \frac{a'}{b'}$, gdzie:

$$a' = \gamma_k^{\mu(n')} \prod_{d \in J_+} (-\gamma_k)^{\mu(n'/d)},\ b' = \prod_{d \in J_-} (-\gamma_k)^{-\mu(n'/d)}.$$

Powyżej pokazaliśmy, że dla dowolnego $1 < l < \omega$, $r_{m_k}(\gamma_{lk}) = r_{m_k}(-\gamma_k)$, a zatem $r_{m_k}(a) = r_{m_k}(a')$ oraz $r_{m_k}(b) = r_{m_k}(b')$. Ponadto $(b, m_k) = 1$ i $(b', m_k) = 1$, ponieważ skoro $m_k = \gamma_k + \gamma_{k+1}$ oraz $(\gamma_k, \gamma_{k+1}) = 1$, to $(\gamma_k, m_k) = 1$ i $(-\gamma_k, m_k) = 1$. Pokażemy, że $r_{m_k}(\frac{a}{b}) = r_{m_k}(\frac{a'}{b'})$.

Niech $\frac{a}{b} = sm_k + r$ oraz $\frac{a'}{b'} = s'm_k + r'$ dla pewnych $r, r', s, s' \in \mathbb{Z}$, takich że $0 \leqslant r, r' < m_k$. Wtedy $r_{m_k}(bsm_k + br) = r_{m_k}(a) = r_{m_k}(a') = r_{m_k}(b's'm_k + b'r')$, czyli $r_{m_k}(b) \cdot_{m_k} r_{m_k}(r) = r_{m_k}(b') \cdot_{m_k} r_{m_k}(r')$. Wiemy, że $r_{m_k}(b) = r_{m_k}(b')$ jest względnie pierwsze z m_k, a więc $r_{m_k}(r) = r_{m_k}(r')$, stąd $r_{m_k}(\frac{a}{b}) = r_{m_k}(\frac{a'}{b'})$.

Otrzymujemy zatem, że $r_{m_k}(-1) = r_{m_k}(\beta_n)$. Sprawdzimy, że -1 nie jest kwadratem w $\mathbb{Z}_{m_k}$, to znaczy pokażemy, że dla każdej $w \in \mathbb{Z}$, m_k nie dzieli $w^2 + 1$.

Z uwagi 8.22. $r_8(m_k) = 6$, tj. $m_k = 8t + 6$ dla pewnej $t \in \mathbb{Z}$. Zauważmy, że $4t + 3$ jest niepatrzysta, a więc $v_2(m_k) = 1$. Niech $p_1'^{e_1'} \dots p_s'^{e_s'}$ będzie rozkładem $4t + 3$ na czynniki pierwsze. Wówczas dla każdego $1 \leqslant i \leqslant s$, $r_4(p_i') \neq 0$ oraz $r_4(p_i') \neq 2$.

Załóżmy a.a., że istnieje $w \in \mathbb{Z}$, taka że m_k dzieli $w^2 + 1$. W szczególności oznacza to, że każda liczba pierwsza występująca w rozkładzie m_k na czynniki pierwsze dzieli $w^2 + 1$. Żeby dostać sprzeczność, na mocy lematu 8.24. wystarczy pokazać, że istnieje $1 \leqslant i \leqslant s$, taki że $r_4(p_i') = 3$. Zauważmy, że gdyby dla każdego $1 \leqslant i \leqslant s$, $r_4(p_i') = 1$, to w szczególności $r_4(p_1'^{e_1'} \dots p_s'^{e_s'}) = 1$, ale $r_4(p_1'^{e_1'} \dots p_s'^{e_s'}) = r_4(4t + 3) = 3$, sprzeczność. Otrzymujemy więc, że $r_{m_k}(\beta_n) = r_{m_k}(-1)$ nie jest kwadratem w $\mathbb{Z}_{m_k}$, zatem w szczególności $\beta_n \notin \mathbb{Q}^2$. □

Lemat 8.26. *Dla każdego $n < \omega$, $\mathrm{Gal}(K_n/\mathbb{Q}) \cong G_n$.*

Dowód. Dla $n = 1$ oczywiście $\mathrm{Gal}(K_n/\mathbb{Q}) \cong \mathbb{Z}_2 = G_n$, załóżmy więc że $n > 1$ i dla wszystkich $k < n$ lemat jest prawdziwy. Z lematu 8.25. otrzymujemy, że dla każdego $1 < k < \omega$, $b_k \notin \mathbb{Q}^2$. Ponadto $b_1 = 2 \notin \mathbb{Q}^2$. Dodatkowo z założenia indukcyjnego $\mathrm{Gal}(K_{n-1}/\mathbb{Q}) \cong G_{n-1}$. Wówczas z lematu 8.21. otrzymujemy, że $\mathrm{Gal}(K_n/\mathbb{Q}) \cong G_n$. □

Lemat 8.27. *Dla każdego $n < \omega$, G_n jest stopnia rozwiązalności n.*

Dowód. Przeprowadzimy indukcję względem n. Dla $n = 1$ $G_n = \mathbb{Z}_2$, więc jest stopnia rozwiązalności 1. Załóżmy więc, że $n > 1$ i lemat jest prawdziwy dla $k < n$. Zauważmy, że $|{}^{G_n}/_{G_{n-1} \rtimes \{0\}}| = 2$, stąd G_n jest rozwiązalna i $(G_n)' \leqslant G_{n-1} \rtimes \{0\}$.

Rozpatrzmy homomorfizm dany wzorem:

$$\Psi\colon G_n \to G_{n-1}$$
$$(g_0, g_1; \epsilon) \mapsto g_1.$$

Niech $\Psi' = \Psi|_{(G_n)'}$. Przypomnijmy, że dla każdego $g \in G_n$, $(g^{-1}, g; 0) \in (G_n)'$, ponieważ $(g^{-1}, g; 0) = (g^{-1}, e; 0)(e, e; 1)(g, e; 0)(e, e; 1) \in (G_n)'$. Widzimy więc, że Ψ' jest w szczególności epimorfizmem, ponieważ dla dowolnego $g \in G_{n-1}$, $(g^{-1}, g; 0) \in (G_n)'$ i $\Psi'((g^{-1}, g; 0)) = g$. Stąd i z założenia indukcyjnego mamy, że stopień rozwiązalności $(G_n)'$ jest równy co najmniej $n-1$. Z drugiej strony $(G_n)' \leqslant G_{n-1} \rtimes \{0\} \cong G_{n-1}$, więc stopień rozwiązalności $(G_n)'$ jest co najwyżej równy $n-1$. Stąd stopień rozwiązalności G_n jest równy n. □

Niech $K_\infty := \bigcup\limits_{n<\omega} K_n$.

Wniosek 8.28. *Nie istnieje maksymalne rozszerzenie rozwiązalne ciała* $\mathbb{Q}$.

Dowód. Zauważmy, że gdyby istniało maksymalne (rownoważnie największe, 8.1.) rozszerzenie rozwiązalne $\mathbb{Q}$, ozn. $\mathbb{Q}^{solv}$, to w szczególności dla każdego $n < \omega$, $K_n \subseteq \mathbb{Q}^{solv}$, a więc $K_\infty \subseteq \mathbb{Q}^{solv}$. Wówczas $\mathrm{Gal}(K_\infty/\mathbb{Q})$ byłaby rozwiązalna jako homomorficzny obraz grupy rozwiązalnej $\mathrm{Gal}(\mathbb{Q}^{solv}/\mathbb{Q})$. Wystarczy więc pokazać, że grupa $\mathrm{Gal}(K_\infty/\mathbb{Q})$ nie jest rozwiązalna.

Gdyby $\mathrm{Gal}(K_\infty/\mathbb{Q})$ była rozwiązalna stopnia r, to każda z grup G_n byłaby rozwiązalna stopnia co najwyżej r (jako obraz homomorficzny granicy odwrotnej). Z lematu 8.27. mamy jednak, że stopnie rozwiązalności G_n dążą do ∞, a więc otrzymujemy, że $\mathrm{Gal}(K_\infty/\mathbb{Q})$ nie jest rozwiązalna. □

Wniosek 8.29. $\mathrm{Gal}(K_\infty/\mathbb{Q}) \cong \varprojlim\limits_{n<\omega} \mathrm{G}_n$

Dowód. Przypomnijmy, że dla każdej grupy G_n istnieje izomorfizm w grupę $\mathbb{Z}_2 \wr G_{n-1}$ zachowujący działanie G_n na zbiorze $\{0, \ldots, 2^n - 1\}$. Z tego powodu w dalszej części będziemy utożsamiać (dla $n > 1$) G_n z $\mathbb{Z}_2 \wr G_{n-1}$. Rozważmy ciąg funkcji $(g_n)_{n=2}^{\infty}$ zdefiniowanych w następujący sposób:

$$g_n\colon \mathbb{Z}_2 \wr G_{n-1} \to G_{n-1}$$
$$(\epsilon, g_{n-1}) \mapsto g_{n-1},$$

Następnie, dla dowolnych $k \leqslant n < \omega$, definiujemy homomorfizm:

$$\varphi_{n,k} : G_n \to G_k$$

przez złożenie funkcji $g_{k+1}, \ldots, g_n$, to znaczy $\varphi_{n,k} = g_{k+1} \ldots g_n$.
Rozważmy zbiór $(G_n, \varphi_{n,k})_{k\leqslant n<\omega}$, gdzie zbiór indeksów rozważamy z naturalnym porządkiem. Zauważmy, że wprost z definicji $\varphi_{n,k}$, dla dowolnych $k \leqslant m \leqslant n < \omega$ zachodzi $\varphi_{n,k} = \varphi_{m,k}\varphi_{n,m}$, a zatem $(G_n, \varphi_{n,k})_{k\leqslant n<\omega}$ jest systemem odwrotnym.
Przypomnijmy, że na mocy twierdzenia 8.26., dla każdego $n < \omega$ istnieje izomorfizm

$$\theta_n : \mathrm{Gal}(K_n/\mathbb{Q}) \xrightarrow{\cong} G_n$$

zachowujący działanie grupy $\mathrm{Gal}(K_n/\mathbb{Q})$ na zbiorze $\{0,\dots,2^n-1\}$.

Pokażemy, że $\mathrm{Gal}(K_\infty/\mathbb{Q}) \cong \varprojlim_{n<\omega} G_n$. Ustalmy dowolne $k \leqslant n < \omega$. Wystarczy sprawdzić, że poniższy diagram komutuje:

$$\begin{array}{ccc} \mathrm{Gal}(K_k/\mathbb{Q}) & \xleftarrow{\psi_{n,k}} & \mathrm{Gal}(K_n/\mathbb{Q}) \\ {\scriptstyle\theta_k}\downarrow & & \downarrow{\scriptstyle\theta_n} \\ G_k & \xleftarrow{\varphi_{n,k}} & G_n \end{array}$$

gdzie $\psi_{n,k}$ jest obcięciem automorfizmu do ciała K_k. Przez łatwą indukcję sprowadza się to do pokazania przemienności takich diagramów dla $k = n-1$.

Ustalmy dowolny $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$. Pokażemy, że $\theta_{n-1}\psi_{n,n-1}(\sigma) = \varphi_{n,n-1}\theta_n(\sigma)$. Zauważmy, że dla dowolnego $l < \omega$, skoro $\mathbb{Q} \subseteq K_l$ jest rozszerzeniem Galois oraz $\mathrm{Gal}(K_l/\mathbb{Q}) \cong G_l$ z zachowaniem działania na zbiorze $\{0,\dots,2^l-1\}$, to dla dowolnego $e \neq g \in G_l$ istnieje $a \in \{0,\dots,2^l-1\}$, taki że $ga \neq a$. Zatem dla dowolnych $g,h \in G_l$ jeśli dla każdego $a \in \{0,\dots,2^l-1\}$, $ga = ha$, to $g = h$, ponieważ w przeciwnym przypadku element $e \neq h^{-1}g$ stabilizowałby cały zbiór $\{0,\dots,2^l-1\}$. Stąd, aby pokazać że $\theta_{n-1}\psi_{n,n-1}(\sigma) = \varphi_{n,n-1}\theta_n(\sigma)$, wystarczy sprawdzić, że dla dowolnego $a \in \{0,\dots,2^{n-1}-1\}$, $\theta_{n-1}\psi_{n,n-1}(\sigma)a = \varphi_{n,n-1}\theta_n(\sigma)a$.
Weźmy dowolny $a \in \{0,\dots,2^{n-1}-1\}$. Zauważmy, że $\theta_{n-1}\psi_{n,n-1}(\sigma)a = \sigma|_{K_{n-1}}a$.
Z drugiej strony, zauważmy że $\theta_n(\sigma) \in G_n$ ma przedstawienie w postaci (f, g_{n-1}) dla pewnych $f \in \mathbb{Z}_2^{\{0,\dots,2^{n-1}-1\}}$ oraz $g_{n-1} \in G_{n-1}$.
Z twierdzenia 8.13. wynika, że dla dowolnego $a \in \{0,\dots,2^n-1\}$, któremu w sposób omówiony wcześniej odpowiada para $(\epsilon, j), \epsilon \in \mathbb{Z}_2, j \in \{0,\dots,2^{n-1}-1\}$, zachodzi:

$$(f, g_{n-1})(\epsilon, j) = (f(g_{n-1}j)\epsilon, g_{n-1}j) = (f(\theta_{n-1}(\sigma|_{K_{n-1}})j)\epsilon, \theta_{n-1}(\sigma|_{K_{n-1}})j) =$$

$$(f, \theta_{n-1}(\sigma|_{K_{n-1}}))(\epsilon, j),$$

czyli

$$\theta_{n-1}\psi_{n,n-1}(\sigma) = \theta_{n-1}(\sigma|_{K_{n-1}}) = g_{n-1} = \varphi_{n,n-1}\theta_n(\sigma).$$

Wobec dowolności $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$ otrzymujemy przemienność diagramu.

Z dowolności $k, n < \omega$, $\varprojlim_{n<\omega} \mathrm{Gal}(K_n/\mathbb{Q}) \cong \varprojlim_{n<\omega} \mathrm{G}_n$ (lemat 2.9.). Mamy więc, że również $\mathrm{Gal}(K_\infty/\mathbb{Q}) \cong \varprojlim_{n<\omega} \mathrm{G}_n$ (3.18.). □

Literatura

[1] Browkin J., *Teoria ciał*, PWN, 1978.

[2] Fried M.D., Jarden M., *Field arithmetic*, Springer, 2005.

[3] Ribes L., Zalesskii P., *Profinite Groups*, Springer, 2010.

[4] Wilson J.S., *Profinite groups*, Clarendon Press, 1998.

[5] Stoll M., *Galois groups over Q of some iterated polynomials*, Archiv der Mathematik vol. 59, 239-244, 1992.

[6] Shafarevich I.R., *Construction of fields of algebraic numbers with given solvable groups*, Izv. Akad. Nauk SSSR 18, 525-578, 1954.

[7] Weitraub S.H., *Galois theory*, Springer, 2006.

[8] Shapiro H.N., *Introduction to the Theory of Numbers*, Dover Publications, 2008.

[9] Burton D.M., *Elementary number theory*, McGraw-Hill, 2002.