Galoisova teorie nekonečných rozšíření

Radan Kučera, prosinec 2022

Nechť K/F je algebraické, normální a separabilní rozšíření. I když K/F je nekonečné rozšíření, máme jako u konečných rozšíření grupu $\mathrm{Aut}(K/F)$ a můžeme se ptát, jestli její všechny podgrupy odpovídají jednoznačně všem mezitělesům (tedy tělesům M splňujícím $F \subseteq M \subseteq K$). Následující příklad ukazuje, že obecně ne.

Příklad 1. Nechť $F = \mathbb{Q}$, za těleso K zvolme kompozitum všech kvadratických rozšíření tělesa racionálních čísel, tj. $K = \mathbb{Q}(\sqrt{a}; a \in \mathbb{Q}) = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \dots)$. Pak $\mathrm{Aut}(K/\mathbb{Q}) = \mathrm{Aut}(K)$. Libovolný $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ je určen svými obrazy na $\sqrt{-1}$ a $\sqrt{p}$ pro všechna prvočísla p, přitom $\sigma(\sqrt{-1}) = \pm\sqrt{-1}$ a $\sigma(\sqrt{p}) = \pm\sqrt{p}$ pro každé prvočíslo p. Je tedy $\sigma^2 = \mathrm{id}_K$. Proto je $\mathrm{Aut}(K)$ komutativní 2-elementární grupa, tedy vektorový prostor nad tělesem $\mathbb{F}_2$ o dvou prvcích. Evidentně je $\mathrm{Aut}(K)$ nekonečná grupa (z Kummerovy teorie plyne, že jsou-li $p_1, \dots, p_n$ různá prvočísla, pak $[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$), je to tedy nekonečně rozměrný vektorový prostor. Pak množina všech nenulových lineárních zobrazení $\mathrm{Aut}(K) \to \mathbb{F}_2$ je nespočetná (zvolíme-li libovolně bázi, pak nenulová lineární zobrazení jednoznačně odpovídají neprázdným podmnožinám báze, protože těleso skalárů má dva prvky). Tato lineární zobrazení jednoznačně odpovídají podgrupám grupy $\mathrm{Aut}(K)$ indexu 2 (každé odpovídá svému jádru). Proto je těchto podgrup více než kvadratických rozšíření $\mathbb{Q}$, kterých je jen spočetně mnoho (každé kvadratické rozšíření $\mathbb{Q}$ je Galoisovo, tedy cyklické, a protože $\pm 1 \in \mathbb{Q}$, je tvaru $\mathbb{Q}(\sqrt{a})$ pro nějaké $a \in \mathbb{Q}$). Ačkoli každému takovému kvadratickému rozšíření $\mathbb{Q}$ odpovídá jednoznačně určená podgrupa grupy $\mathrm{Aut}(K)$ indexu 2 a různým rozšířením odpovídají různé podgrupy, naopak to neplatí. Jen spočetně mnoha těmto podgrupám odpovídá rozšíření, kdežto pro nespočetně mnoho podgrup odpovídající rozšíření neexistuje. Cílem následujícího textu je vysvětlit proč; a také ukázat, čím se podgrupy odpovídající rozšířením odlišují od těch ostatních.

Poznámka 2. Připomeňme, že topologický prostor je libovolná množina spolu s topologií na ní. Topologie na množině X je libovolný systém podmnožin množiny X, kterým se říká otevřené (v této topologii), splňující: prázdná množina i celá množina X jsou otevřené, průnik libovolných dvou otevřených množin je otevřená množina a sjednocení libovolného systému otevřených množin je otevřená množina.

Největší topologií na množině X je tzv. diskrétní topologie, v níž je každá podmnožina množiny X otevřená. Naopak nejmenší topologií na množině X je tzv. indiskrétní topologie, v níž jsou otevřené pouze prázdná množina a množina X.

Topologii na množině X lze zadat pomocí nějaké její báze (resp. subbáze) otevřených množin, což je libovolný systém otevřených množin takový, že otevřenými množinami v X jsou právě sjednocení libovolně mnoha množin z báze (resp. množin, které jsou průniky konečně mnoha množin ze subbáze). Ze znalosti báze (resp. subbáze) snadno určíme celou topologii: pro libovolnou subbázi tvoří systém všech průniků konečně mnoha množin ze subbáze bázi; celou topologii pak dostaneme jako systém všech sjednocení množin báze.

Další možností, jak zadat topologii na množině X, je popsat pro každý bod $x \in X$ bázi (resp. subbázi) otevřených okolí bodu x, což je libovolný systém otevřených množin obsahujících bod x takových, že každá otevřená množina obsahující bod x nutně obsahuje i některou množinu z báze otevřených okolí bodu x (resp. průnik některých konečně mnoha množin z subbáze otevřených okolí bodu x). Máme-li pro každý bod dánu bázi (resp. subbázi) otevřených okolí tohoto bodu, jejich sjednocením dostaneme bázi (resp. subbázi) otevřených množin.

Topologický prostor X se nazývá Hausdorffův (neboli T_2), jestliže pro každé $x, y \in X$, $x \neq y$, existují disjunktní otevřené množiny A, $B \subseteq X$ tak, že $x \in A$, $y \in B$.

Z libovolného metrického prostoru (X, ρ) získáme Hausdorffův topologický prostor na X tak, že za bázi otevřených okolí libovolného bodu $x \in X$ zvolíme systém otevřených koulí se středem v bodě x s poloměry libovolně se blížícími nule, například $\{y \in X;\, \rho(x, y) < \frac{1}{n}\}$, $n \in \mathbb{N}$.

Množina $A \subseteq X$ se nazývá uzavřená (v této topologii), právě když je její doplněk $X - A$ otevřená množina.

Množina $A \subseteq X$ se nazývá kompaktní (v této topologii), právě když z libovolného jejího otevřeného pokrytí (tedy z libovolného systému otevřených množin, jejichž sjednocení je A podmnožinou) lze vybrat konečné podpokrytí. Topologický prostor X se nazývá kompaktní, je-li celá množina X kompaktní.

Zobrazení $X \to Y$ mezi topologickými prostory se nazývá spojité, jestliže pro každou otevřenou množinu $A \subseteq Y$ je množina $f^{-1}(A) \subseteq X$ otevřená.

Zobrazení $X \to Y$ mezi topologickými prostory se nazývá homeomorfismus (někdy též izomorfismus topologických prostorů), jestliže je f bijektivní a obě zobrazení f i f^{-1} jsou spojitá.

Je-li X topologický prostor a $Y \subseteq X$ jeho libovolná podmnožina, můžeme na Y definovat topologii tak, že otevřenými množinami v topologii na Y jsou právě průniky množiny Y postupně se všemi otevřenými množinami na X. Tomuto topologickému prostoru Y se říká podprostor topologického prostoru X. (Jedná se tedy o nejmenší topologii na Y, v níž je zobrazení inkluze $Y \to X$ spojité.)

Jsou-li X_i, $i \in I$, topologické prostory, na součinu množin $X = \prod_{i \in I} X_i$ definujeme topologii takto: je to nejmenší topologie, v níž jsou všechny projekce $\pi_i : X \to X_i$ spojité. Tomuto topologickému prostoru X pak říkáme součin topologických prostorů X_i, $i \in I$. (Znamená to, že subbází otevřených množin v X je systém množin $\pi_i^{-1}(A)$, kde $i \in I$ a $A \subseteq X_i$ je otevřená množina v topologii prostoru X_i.)

Platí Tichonovova věta: Součinem libovolného systému kompaktních topologických prostorů je kompaktní topologický prostor.

Podmnožina topologického prostoru se nazývá obojetná, právě když je současně otevřená i uzavřená. Topologický prostor se nazývá souvislý, jestliže jeho jediné obojetné množiny jsou prázdná množina a celý prostor. Podmnožina Y topologického prostoru X se nazývá souvislá, jestliže tvoří v topologii podprostoru (zmiňované výše) souvislý topologický prostor. Jinými slovy: podmnožina Y topologického prostoru X není souvislá, právě když existují otevřené množiny A, B topologického prostoru X takové, že $A \cap Y$ a $B \cap Y$ jsou neprázdné disjunktní množiny, jejichž sjednocením je Y.

Topologický prostor se nazývá totálně nesouvislý (anglicky totally disconnected), jestliže nemá žádnou alespoň dvouprvkovou souvislou podmnožinu.

Topologické prostory, pro jejichž každé dva různé body existuje obojetná množina, která obsahuje právě jeden z nich, se nazývají totálně separované (anglicky totally separated). Každý takový prostor je totálně nesouvislý (opačná implikace však neplatí).

Definice 3. Nechť $(G, \cdot)$ je grupa taková, že její nosná množina je současně topologický prostor. Pak i součin $G \times G$ je topologický prostor (s topologií součinu). Jestliže obě zobrazení $G \to G$, $x \mapsto x^{-1}$, a $G \times G \to G$, $(x, y) \mapsto x \cdot y$, jsou spojitá, říkáme, že G je topologická grupa.

Příklad 4.

- Libovolná grupa spolu s diskrétní nebo indiskrétní topologií je topologická grupa.
- Grupy $(\mathbb{R}, +)$ a $(\mathbb{R}^*, \cdot)$ vzhledem k obvyklé topologii dané metrikou absolutní hodnoty jsou topologické.

- Pro libovolné $n \in \mathbb{N}$ je $(\mathbb{R}^n, +)$ spolu s topologií danou euklidovskou metrikou také topologická grupa.
- Grupa $(\mathbb{F}_2, +)$ spolu s topologií, v níž jsou otevřené právě množiny $\mathbb{F}_2, \{[0]_2\}, \emptyset$, není topologická, protože zobrazení $+ : \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$ není spojité (promyslete si, které podmnožiny jsou v topologickém prostoru $\mathbb{F}_2 \times \mathbb{F}_2$ otevřené).

Poznámka 5. Nechť $(G, \cdot)$ je topologická grupa. Zobrazení $G \times G \to G$, $(x, y) \mapsto x \cdot y$, je spojité, a tedy pro každé $g \in G$ je posunutí $\rho_g \colon G \to G$, $\rho_g(x) = g \cdot x$, spojité. Přitom jde o bijekci, jejíž inverzí je $\rho_{g^{-1}}$. Je tedy ρ_g homeomorfismus. Proto lze topologii topologické grupy zadat nějakou bází (resp. subbází) otevřených okolí neutrálního prvku $1 \in G$.

Tvrzení 6. *Je-li I množina a pro každé $i \in I$ je dána topologická grupa G_i, pak součin grup $\prod_{i \in I} G_i$ spolu s topologií součinu tvoří topologickou grupu.*

Definice 7. Relace $\preceq$ na množině I se nazývá předuspořádání, jestliže je reflexivní a tranzitivní. Řekneme, že $(I, \preceq)$ je usměrněná množina, jestliže $\preceq$ je předuspořádání, v němž má každá konečná podmnožina horní závoru, jinými slovy pro každé $i, j \in I$ existuje $k \in I$ tak, že $i \preceq k$, $j \preceq k$.

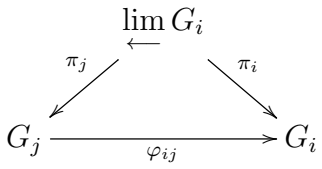
Definice 8. Nechť $(I, \preceq)$ je usměrněná množina taková, že pro každé $i \in I$ je dána množina G_i a pro každá $i, j \in I$, $i \preceq j$, je dáno zobrazení $\varphi_{ij} : G_j \to G_i$, přičemž platí

- $\forall i \in I : \ \varphi_{ii} = \mathrm{id}_{G_i}$,
- $\forall i, j, k \in I : \ i \preceq j \preceq k \implies \varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$.

Pak G_i, $i \in I$, nazveme projektivním (nebo též inverzním) systémem množin. Jeho projektivní (nebo též inverzní) limitou rozumíme

$$\varprojlim G_i = \Big\{ \chi \in \prod_{i \in I} G_i; \ \ \forall i, j \in I \colon \ i \preceq j \implies \varphi_{ij}\big(\chi(j)\big) = \chi(i) \Big\}.$$

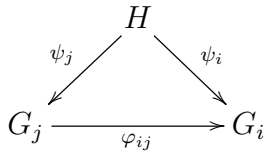
Pro každé $j \in I$ pak dostáváme projekci $\pi_j \colon \varprojlim G_i \to G_j$ (stačí zúžit projekce ze součinu). Tyto projekce zřejmě pro každé $i, j \in I$, $i \preceq j$, tvoří komutativní diagram



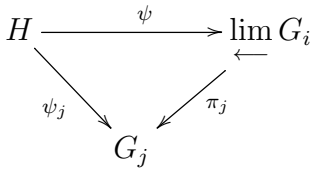
Je-li navíc každé G_i grupa (resp. okruh, resp. topologický prostor, resp. topologická grupa) a je-li každé φ_{ij} homomorfismus grup (resp. homomorfismus okruhů, resp. spojité zobrazení, resp. spojitý homomorfismus grup), hovoříme o projektivním (nebo též inverzním) systému grup (resp. okruhů, resp. topologických prostorů, resp. topologických grup).

Projektivní limita spolu s projekcemi má následující univerzální vlastnost, která ji jednoznačně určuje až na izomorfismus:

Tvrzení 9. *Nechť G_i, $i \in I$, je projektivní systém množin a nechť je dána množina H a pro každé $i \in I$ zobrazení $\psi_i\colon H \to G_i$ takové, že pro každé $i, j \in I$, $i \preceq j$, komutuje diagram*



Pak existuje jediné zobrazení $\psi\colon H \to \varprojlim G_i$ tak, že pro každé $j \in I$ komutuje diagram



Tvrzení 10. *Je-li G_i, $i \in I$, projektivní systém grup (resp. okruhů), pak je $\varprojlim G_i$ podgrupou (resp. podokruhem) součinu $\prod_{i\in I} G_i$.*

Příklad 11.

- Nechť p je prvočíslo. Zřejmě $(\mathbb{N}, \leq)$ je usměrněná množina. Pro každé $i, j \in \mathbb{N}$ takové, že $i \leq j$, máme jediný homomorfismus okruhů $\varphi_{ij}\colon \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ (platí $\varphi_{ij}([a]_{p^j}) = [a]_{p^i}$ pro každé $a \in \mathbb{Z}$). Tyto homomorfismy tvoří projektivní systém okruhů (to plyne okamžitě už z toho, že to jsou jediné homomorfismy mezi uvedenými okruhy). Jako inverzní limitu dostáváme okruh $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$, který se nazývá okruh celých p-adických čísel.

- Zřejmě $(\mathbb{N}, |)$ je usměrněná množina. Pro každé $m, n \in \mathbb{N}$ takové, že $m \mid n$, máme jediný homomorfismus okruhů $\varphi_{mn}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

(platí $\varphi_{mn}([a]_n) = [a]_m$ pro každé $a \in \mathbb{Z}$). Tím opět dostáváme projektivní systém okruhů, jehož inverzní limitou je okruh $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$.

Je možné ukázat, že $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$, kde p probíhá všechna prvočísla a $\mathbb{Z}_p$ je výše zmíněný okruh celých p-adických čísel.

Věta 12. *Nechť G_i, $i \in I$, je projektivní systém Hausdorffových topologických prostorů. Pak projektivní limita $\varprojlim G_i$ je uzavřená podmnožina topologického prostoru $\prod_{i\in I} G_i$.*

Důkaz. Ukážeme, že doplněk $\prod_{i\in I} G_i - \varprojlim G_i$ je otevřená množina. Nechť $\chi \in \prod_{i\in I} G_i$, $\chi \notin \varprojlim G_i$. Pak existují $i, j \in I$, $i \preceq j$, tak, že $\varphi_{ij}\big(\chi(j)\big) \neq \chi(i)$. Protože G_i je Hausdorffův, existují disjunktní otevřené množiny U, $V \subseteq G_i$ tak, že $\chi(i) \in U$, $\varphi_{ij}\big(\chi(j)\big) \in V$. Označme pro $k \in I$

$$T_k = \begin{cases} U & \text{pro } k = i, \\ \varphi_{ij}^{-1}(V) & \text{pro } k = j, \\ G_k & \text{jinak.} \end{cases}$$

Pak $\prod_{k\in I} T_k$ je otevřená množina v $\prod_{k\in I} G_k$, která je disjunktní s $\varprojlim G_i$ a obsahuje χ.

Definice 13. Prokonečnou grupou máme na mysli topologickou grupu, která je izomorfní (tj. existuje mezi nimi izomorfismus grup, který je současně i homeomorfismem) s projektivní limitou konečných grup s diskrétní topologií.

Poznámka 14. Abychom lépe porozuměli topologii prokonečné grupy, popišme nějakou bázi otevřených okolí neutrálního prvku. Nechť G_i, $i \in I$, je projektivní systém konečných diskrétních grup. Pak projektivní limita $\varprojlim G_i$ má nejmenší topologii takovou, že všechny projekce $\pi_j\colon \varprojlim G_i \to G_j$ jsou spojité. Proto množiny $\pi_j^{-1}(\{1\})$, $j \in I$, tvoří subbázi otevřených okolí neutrálního prvku. Protože $(I, \preceq)$ je usměrněná, pro libovolnou konečnou podmnožinu $\{i_1, \ldots, i_n\} \subseteq I$ existuje $j \in I$ tak, že $i_1 \preceq j$, …, $i_n \preceq j$. Protože $\varphi_{i_k j}$ jsou homomorfismy, je $\varphi_{i_k j}(1) = 1$, a tedy

$$\pi_j^{-1}(\{1\}) \subseteq \bigcap_{k=1}^{n} \pi_{i_k}^{-1}(\{1\}).$$

Proto množiny $\pi_j^{-1}(\{1\})$, $j \in I$, tvoří dokonce bázi otevřených okolí neutrálního prvku.

Věta 15. *Každá prokonečná grupa je kompaktní.*

Důkaz. Každý konečný topologický prostor je kompaktní. Z Tichonovovy věty je součin kompaktních prostorů kompaktní. Podle věty 12 je prokonečná grupa uzavřenou podmnožinou v kompaktním prostoru, a tedy kompaktní.

Lemma 16. *Nechť G je topologická grupa, H otevřená podgrupa grupy G. Pak H je uzavřená (a tedy obojetná) množina.*

Důkaz. Pro libovolné $g \in G$ je levá třída $g \cdot H$ obrazem podgrupy H v posunutí ρ_g. Proto je každá levá třída otevřená. Protože levé třídy tvoří rozklad na G a jednou z nich je podgrupa H, je H doplňkem sjednocení ostatních levých tříd. Toto sjednocení otevřených množin je otevřená množina, tedy H je uzavřená.

Věta 17. *Každá prokonečná grupa je totálně nesouvislá.*

Důkaz. Nechť tedy G_i, $i \in I$, je projektivní systém konečných diskrétních grup, $G = \varprojlim G_i$ jeho projektivní limita. Vzhledem k tomu, že posunutí je homeomorfismus, stačí ukázat, že pro libovolné $g \in G$, $g \neq 1$, existuje obojetná množina obsahující 1 a neobsahující g. Protože $g \neq 1$, existuje $j \in I$ tak, že $\pi_j(g) \neq 1$. Pak $\pi_j^{-1}(\{1\})$ je otevřená podgrupa grupy G neobsahující g. Stačí užít lemma 16.

Pro zajímavost uveďme následující topologickou charakterizaci prokonečných grup.

Věta 18. *Topologická grupa je prokonečná, právě když je kompaktní a totálně nesouvislá.*

Důkaz. V případě zájmu lze šestistránkový důkaz nalézt v [1], str. 25-31.

Poznámka 19. Nechť K/F je algebraické, normální a separabilní rozšíření. Označme $\mathcal{L}$ množinu všech mezitěles L (tj. L je těleso splňující $F \subseteq L \subseteq K$) takových, že L/F je konečné a normální. Zřejmě je pro každé $L \in \mathcal{L}$ také L/F separabilní, a tedy Galoisovo, a máme konečnou Galoisovu grupu $\mathrm{Gal}(L/F)$. Navíc je $(\mathcal{L}, \subseteq)$ usměrněná množina, neboť pro $L_1, L_2 \in \mathcal{L}$ je také jejich kompozitum $L_1 L_2 \in \mathcal{L}$. Jsou-li $L_1, L_2 \in \mathcal{L}$, $L_1 \subseteq L_2$, pak restrikce

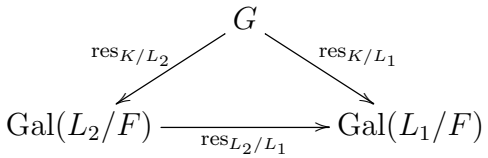
$$\mathrm{res}_{L_2/L_1} : \mathrm{Gal}(L_2/F) \to \mathrm{Gal}(L_1/F)$$

je homomorfismus grup. Grupy $\mathrm{Gal}(L/F)$ jsou konečné, jestliže je vezmeme s diskrétní topologií, dostáváme jako inverzní limitu tohoto projektivního systému topologických grup prokonečnou grupu $\varprojlim \mathrm{Gal}(L/F)$, přičemž L v limitě probíhá usměrněnou množinu $\mathcal{L}$.

Označme $G = \mathrm{Aut}(K/F)$. Pak pro každé $L \in \mathcal{L}$ máme restrikci

$$\mathrm{res}_{K/L} : G \to \mathrm{Gal}(L/F),$$

která je homomorfismem grup. Pro každé $L_1, L_2 \in \mathcal{L}$, $L_1 \subseteq L_2$, máme komutativní diagram



Stejně jako v tvrzení 9 tím dostáváme zobrazení $\rho: G \to \varprojlim \mathrm{Gal}(L/F)$, ve kterém se $\sigma \in G$ zobrazí na prvek, v jehož L-té komponentě je $\mathrm{res}_{K/L}(\sigma)$.

Zřejmě je ρ homomorfismus grup. Předpokládejme, že existuje $\sigma \in \ker \rho$, $\sigma \neq \mathrm{id}_K$. Pak existuje $\alpha \in K$ tak, že $\sigma(\alpha) \neq \alpha$. Přitom toto α je algebraické nad F (vždyť K/F je algebraické) a jeho minimální polynom f nad F nemá násobné kořeny (vždyť K/F je separabilní) a všechny kořeny f leží v K (vždyť K/F je normální). Proto rozkladové těleso L polynomu f nad F splňuje $L \subseteq K$, a tedy $L \in \mathcal{L}$. Protože $\sigma \in \ker \rho$, platí $\mathrm{res}_{K/L}(\sigma) = \mathrm{id}_L$. Navíc $\alpha \in L$, a tedy

$$\alpha \neq \sigma(\alpha) = (\mathrm{res}_{K/L}(\sigma))(\alpha) = \mathrm{id}_L(\alpha) = \alpha,$$

spor. Je tedy ρ injektivní.

Ukažme, že je ρ také surjektivní. Zvolme $\chi \in \varprojlim \mathrm{Gal}(L/F)$ libovolně, ale pevně. Konstruujme $\sigma: K \to K$ takto: už víme, že pro libovolné $\alpha \in K$ existuje $L \in \mathcal{L}$ tak, že $\alpha \in L$; položme $\sigma(\alpha) = (\chi(L))(\alpha)$. Tato definice je korektní, neboť jsou-li $L_1, L_2 \in \mathcal{L}$ takové, že $\alpha \in L_1$ a $\alpha \in L_2$, pak také jejich kompozitum $L_1 L_2 \in \mathcal{L}$ a z $\chi \in \varprojlim \mathrm{Gal}(L/F)$ plyne

$$\mathrm{res}_{L_1 L_2/L_1}\, \chi(L_1 L_2) = \chi(L_1),$$
$$\mathrm{res}_{L_1 L_2/L_2}\, \chi(L_1 L_2) = \chi(L_2),$$

a tedy $(\chi(L_1))(\alpha) = (\chi(L_1 L_2))(\alpha) = (\chi(L_2))(\alpha)$. Je tedy σ definováno korektně. Snadno se ukáže, že je σ automorfismus: pro libovolné $\alpha, \beta \in K$

existuje $L \in \mathcal{L}$, $\alpha, \beta \in L$, a $\chi(L)$ je automorfismus tělesa L. Tedy σ je homomorfismus okruhů. Zřejmě $\sigma(\alpha) = \alpha$ pro každé $\alpha \in F$. Protože K je těleso, je σ injektivní. A protože libovolné $\alpha \in K$ je kořenem svého minimálního polynomu f nad F a σ permutuje kořeny polynomu f, je σ surjektivní. Tedy $\sigma \in G$. Dokázali jsme, že

$$\rho\colon G \to \varprojlim \mathrm{Gal}(L/F)$$

je izomorfismus grup. Protože grupa vpravo je prokonečná, lze izomorfismem ρ přenést topologii prokonečné grupy na G. Tato topologie na $G = \mathrm{Aut}(K/F)$ se nazývá Krullova.

Z poznámky 14 dostáváme popis báze otevřených okolí neutrálního prvku id_K grupy G. Pro každé $L \in \mathcal{L}$ je $\pi_L \circ \rho = \mathrm{res}_{K/L}$, a platí $(\pi_L \circ \rho)^{-1}(\{\mathrm{id}_L\}) = \mathrm{Aut}(K/L)$. Proto $\mathrm{Aut}(K/L)$, $L \in \mathcal{L}$, tvoří bázi otevřených okolí neutrálního prvku id_K grupy G.

Lemma 20. *Pro každé $L \in \mathcal{L}$ platí, že $\mathrm{res}_{K/L} : G \to \mathrm{Gal}(L/F)$ je surjektivní.*

Důkaz. Nechť $\sigma \in \mathrm{Gal}(L/F)$ je libovolné. Označme $\mathcal{M}$ množinu všech uspořádaných dvojic (M, τ), kde těleso M splňuje $L \subseteq M \subseteq K$ a pro automorfismus $\tau\colon M \to M$ platí $\mathrm{res}_{M/L}(\tau) = \sigma$. Zřejmě $(L, \sigma) \in \mathcal{M}$, a tedy $\mathcal{M}$ je neprázdná. Na $\mathcal{M}$ zavedeme uspořádání $\leq$ takto: $(M_1, \tau_1) \leq (M_2, \tau_2)$, právě když $M_1 \subseteq M_2$ a $\mathrm{res}_{M_2/M_1}(\tau_2) = \tau_1$. Zřejmě libovolná lineárně uspořádaná podmnožina $\mathcal{M}$ má v $\mathcal{M}$ horní závoru. Podle Zornova lemmatu existuje maximální prvek (M_0, τ_0) množiny $\mathcal{M}$. Předpokládejme na okamžik, že existuje $\alpha \in K$, $\alpha \notin M_0$. Označme f minimální polynom prvku α nad F, nechť R je rozkladové těleso polynomu f nad M_0. Automorfismus τ_0 nechává koeficienty polynomu f na místě. Z věty o jednoznačnosti rozkladových těles víme, že existuje automorfismus τ_1 tělesa R, jehož restrikcí na M_0 je τ_0. Pak $(R, \tau_1) > (M_0, \tau_0)$, spor. Je tedy $M_0 = K$.

Důsledek 21. *Pro libovolné $\alpha \in K$ platí: $\alpha \in F$, právě když pro každé $\tau \in G$ je $\tau(\alpha) = \alpha$.*

Důkaz. Jeden směr plyne ihned z definice G. Naopak, předpokládejme, že $\alpha \in K$, $\alpha \notin F$. Pak existuje $L \in \mathcal{L}$ tak, že $\alpha \in L$. Protože $\alpha \notin F$, existuje $\sigma \in \mathrm{Gal}(L/F)$ tak, že $\sigma(\alpha) \neq \alpha$. Předchozí lemma zaručuje, že σ je restrikcí vhodného $\tau \in G$.

Lemma 22. *Nechť M je libovolné mezitěleso rozšíření K/F, tj. pro těleso M platí $F \subseteq M \subseteq K$. Pak* $\mathrm{Aut}(K/M)$ *je normální podgrupa grupy G, právě když pro každé $\tau \in G$ platí* $\mathrm{Aut}(K/M) = \mathrm{Aut}(K/\tau(M))$. *Tato podmínka je splněna, je-li M/F normální rozšíření.*

Důkaz. Zvolme $\tau \in G$ libovolně, ale pevně. Podle definice je $\mathrm{Aut}(K/M)$ množina všech prvků $\sigma \in G$, které splňují $\sigma(\alpha) = \alpha$ pro každé $\alpha \in M$, což je ekvivalentní s tím, že $(\tau \circ \sigma \circ \tau^{-1})(\beta) = \beta$ pro každé $\beta \in \tau(M)$, tedy s tím, že $\tau \circ \sigma \circ \tau^{-1} \in \mathrm{Aut}(K/\tau(M))$. Je tedy $\mathrm{Aut}(K/M)$ normální podgrupa grupy G, právě když pro každé $\tau \in G$ platí $\mathrm{Aut}(K/M) = \mathrm{Aut}(K/\tau(M))$.

Je-li M/F normální rozšíření, pak M s každým prvkem $\alpha \in M$ obsahuje všechny kořeny minimálního polynomu f prvku α nad F, tedy pro každé $\tau \in G$ platí $\tau(M) \subseteq M$ a také $\tau^{-1}(M) \subseteq M$, tj. $M \subseteq \tau(M)$, dohromady $\tau(M) = M$.

Důsledek 23. *Pro každé $L \in \mathcal{L}$ platí, že* $\mathrm{Aut}(K/L)$ *je normální podgrupa grupy G.*

Důkaz. Z definice L/F je Galoisovo, a tedy normální.

Věta 24. *Uzavřené podgrupy grupy G v Krullově topologii jsou právě průniky (libovolných systémů) otevřených podgrup. Přesněji: je-li H uzavřená podgrupa grupy G, pak platí*

$$H = \bigcap_{L \in \mathcal{L}} H \circ \mathrm{Aut}(K/L).$$

Důkaz. Podle lemma 16 je každá otevřená podgrupa také uzavřená. Zřejmě průnik libovolného systému uzavřených podgrup je uzavřená podgrupa.

Pro libovolnou podgrupu H grupy G je podle důsledku 23 množina

$$H \circ \mathrm{Aut}(K/L) = \{\tau \circ \sigma;\ \tau \in H,\ \sigma \in \mathrm{Aut}(K/L)\} = \bigcup_{\tau \in H} \tau \circ \mathrm{Aut}(K/L)$$

podgrupou grupy G a také sjednocením otevřených množin, tedy otevřenou podgrupou grupy G. Stačí tedy ukázat, že je-li H uzavřená, platí rovnost uvedená ve znění věty. Jedna inkluze je zřejmá, předpokládejme, že druhá inkluze neplatí, tj. existuje $x \in \bigcap_{L \in \mathcal{L}} H \circ \mathrm{Aut}(K/L)$, $x \notin H$. Protože H je uzavřená, je $G - H$ otevřená. Bází otevřených okolí bodu x je systém

$x \circ \mathrm{Aut}(K/L)$, $L \in \mathcal{L}$. Existuje tedy $L_0 \in \mathcal{L}$ tak, že $x \circ \mathrm{Aut}(K/L_0) \subseteq G - H$. Protože $x \in \bigcap_{L\in\mathcal{L}} H \circ \mathrm{Aut}(K/L)$, platí také $x \in H \circ \mathrm{Aut}(K/L_0)$, odkud

$$x \circ \mathrm{Aut}(K/L_0) \in (H \circ \mathrm{Aut}(K/L_0))/\mathrm{Aut}(K/L_0) = \{h \circ \mathrm{Aut}(K/L_0);\ h \in H\}.$$

Existuje tedy $h_0 \in H$ tak, že

$$x \circ \mathrm{Aut}(K/L_0) = h_0 \circ \mathrm{Aut}(K/L_0),$$

tedy $h_0 \in x \circ \mathrm{Aut}(K/L_0) \subseteq G - H$, spor.

Nyní už můžeme formulovat zobecnění základní věty Galoisovy teorie na nekonečná algebraická, normální a separabilní rozšíření.

Věta 25. *Nechť K/F je algebraické, normální a separabilní rozšíření, nechť $G = \mathrm{Aut}(K/F)$ je topologická grupa s Krullovou topologií. Označme $\mathcal{M}$ množinu všech mezitěles rozšíření K/F (tj. těles M, pro která $F \subseteq M \subseteq K$) a $\mathcal{H}$ množinu všech uzavřených podgrup grupy G. Pak zobrazení*

$$\begin{aligned} &\alpha\colon \mathcal{M} \to \mathcal{H}, && \alpha(M) = \mathrm{Aut}(K/M) \text{ pro každé } M \in \mathcal{M}, \\ &\beta\colon \mathcal{H} \to \mathcal{M}, && \beta(H) = \{x \in K;\ \forall \sigma \in H\colon \sigma(x) = x\} \text{ pro každou } H \in \mathcal{H}, \end{aligned}$$

tvoří dvojici navzájem inverzních bijekcí, přičemž

$$\begin{aligned} \alpha(M_1) \supseteq \alpha(M_2) \qquad &\text{pro každá } M_1, M_2 \in \mathcal{M},\ M_1 \subseteq M_2, \\ \beta(H_1) \supseteq \beta(H_2) \qquad &\text{pro každé } H_1, H_2 \in \mathcal{H},\ H_1 \subseteq H_2. \end{aligned}$$

Navíc pro každé $M \in \mathcal{M}$ platí

$$\begin{aligned} M/F \text{ je normální rozšíření} &\iff \alpha(M) \text{ je normální podgrupa grupy } G, \\ M/F \text{ je konečné rozšíření} &\iff \alpha(M) \text{ je otevřená podgrupa grupy } G, \\ M/F \text{ je konečné rozšíření} &\implies |G/\alpha(M)| = [M : F], \\ M/F \text{ je nekonečné rozšíření} &\implies |G/\alpha(M)| = \infty. \end{aligned}$$

Důkaz. Zřejmě pro libovolnou $H \in \mathcal{H}$ je $\{x \in K;\ \forall \sigma \in H\colon \sigma(x) = x\} \in \mathcal{M}$, je tedy β dobře definováno.

Abychom ukázali, že je dobře definováno i α, pro libovolnou $M \in \mathcal{M}$ ukažme, že $\mathrm{Aut}(K/M)$ je uzavřená podgrupa grupy G. Zřejmě jde o podgrupu, zbývá ukázat, že je uzavřená. Zvolme libovolně $\sigma \in G$, $\sigma \notin \mathrm{Aut}(K/M)$. Pak existuje $x \in M$ takové, že $\sigma(x) \neq x$. Pro toto x existuje $L \in \mathcal{L}$ tak, že

$x \in L$. Pro každé $\tau \in \mathrm{Aut}(K/L)$ platí $(\sigma \circ \tau)(x) = \sigma(\tau(x)) = \sigma(x) \neq x$, a tedy $\sigma \circ \mathrm{Aut}(K/L)$ je otevřená množina obsahující σ, která je disjunktní s $\mathrm{Aut}(K/M)$. Proto je $G - \mathrm{Aut}(K/M)$ otevřená množina.

Ihned z definic je jasné, že zobrazení α i β obracejí inkluze.

Nechť $M \in \mathcal{M}$ je libovolné. Důsledek 21 pro rozšíření K/M tvrdí, že libovolné $z \in K$ splňuje $z \in M$, právě když $\sigma(z) = z$ pro každé $\sigma \in \mathrm{Aut}(K/M)$, tj. právě když $z \in \beta(\alpha(M))$. Je proto $\beta \circ \alpha = \mathrm{id}_{\mathcal{M}}$.

Ukažme, že také $\alpha \circ \beta = \mathrm{id}_{\mathcal{H}}$. Z definic je vidět, že pro libovolnou $H \in \mathcal{H}$ platí $H \subseteq \alpha(\beta(H))$. Podle věty 24 platí

$$H = \bigcap_{L \in \mathcal{L}} H \circ \mathrm{Aut}(K/L),$$

a tedy

$$\beta(H) = \beta\Big(\bigcap_{L \in \mathcal{L}} H \circ \mathrm{Aut}(K/L)\Big) \supseteq \bigcup_{L \in \mathcal{L}} \beta\big(H \circ \mathrm{Aut}(K/L)\big),$$

odkud

$$\alpha(\beta(H)) \subseteq \alpha\Big(\bigcup_{L \in \mathcal{L}} \beta\big(H \circ \mathrm{Aut}(K/L)\big)\Big) \subseteq \bigcap_{L \in \mathcal{L}} \alpha\big(\beta\big(H \circ \mathrm{Aut}(K/L)\big)\big)\big).$$

Jestliže ukážeme, že $\alpha\big(\beta\big(H \circ \mathrm{Aut}(K/L)\big)\big)\big) = H \circ \mathrm{Aut}(K/L)$, průnik vpravo bude roven H a rovnost $(\alpha \circ \beta)(H) = H$ bude dokázána. Z definic plyne, že platí $H \circ \mathrm{Aut}(K/L) \subseteq \alpha\big(\beta\big(H \circ \mathrm{Aut}(K/L)\big)\big)\big)$. Zvolme libovolně, ale pevně $\sigma \in \alpha\big(\beta\big(H \circ \mathrm{Aut}(K/L)\big)\big)\big)$. Pak $\sigma \in \mathrm{Aut}(K/\beta(H \circ \mathrm{Aut}(K/L)))$, jinými slovy: $\sigma \in G$ je takové, že pro každé $z \in K$ platí, že

$$(1) \qquad \forall \tau \in H \circ \mathrm{Aut}(K/L)\colon \tau(z) = z \qquad \Longrightarrow \qquad \sigma(z) = z.$$

Potřebujeme ukázat, že $\sigma \in H \circ \mathrm{Aut}(K/L)$.

Udělejme to sporem, předpokládejme naopak, že $\sigma \notin H \circ \mathrm{Aut}(K/L)$. Restrikce $\mathrm{res}_{K/L} : G \to \mathrm{Gal}(L/F)$ je homomorfismus, který má jádro $\mathrm{Aut}(K/L)$. Kdyby $\mathrm{res}_{K/L}(\sigma) \in \mathrm{res}_{K/L}(H)$, existovalo by $\lambda \in H$ tak, že $\mathrm{res}_{K/L}(\lambda) = \mathrm{res}_{K/L}(\sigma)$, tedy $\lambda^{-1} \circ \sigma \in \mathrm{Aut}(K/L)$, odkud $\sigma \in H \circ \mathrm{Aut}(K/L)$. Proto $\mathrm{res}_{K/L}(\sigma) \notin \mathrm{res}_{K/L}(H)$. Ovšem L/F je konečné Galoisovo rozšíření, přičemž $\mathrm{res}_{K/L}(\sigma) \in \mathrm{Gal}(L/F)$ je automorfismus, který nepatří do podgrupy $\mathrm{res}_{K/L}(H)$ Galoisovy grupy $\mathrm{Gal}(L/F)$. Z hlavní věty Galoisovy teorie (pro konečná Galoisova rozšíření) plyne, že v tělese, které odpovídá podgrupě

$\mathrm{res}_{K/L}(H)$, existuje prvek z takový, že $(\mathrm{res}_{K/L}(\sigma))(z) \neq z$, tedy $\sigma(z) \neq z$. Pro libovolné $\tau \in H \circ \mathrm{Aut}(K/L)$ je $\mathrm{res}_{K/L}(\tau) \in \mathrm{res}_{K/L}(H)$, tedy $\tau(z) = (\mathrm{res}_{K/L}(\tau))(z) = z$. Toto z tedy nesplňuje implikaci (1), spor.

Dokázali jsme, že α a β jsou navzájem inverzní bijekce.

Nechť $M \in \mathcal{M}$ je libovolné. Jestliže M/F je normální rozšíření, podle lemma 22 je $\alpha(M)$ normální podgrupa grupy G. Jestliže M/F není normální, existuje $z \in M$, jehož minimální polynom f nad F má kořen $y \notin M$. Existuje $L \in \mathcal{L}$ tak, že $z \in L$, a tedy i $y \in L$. Víme, že existuje $\sigma \in \mathrm{Gal}(L/F)$ tak, že $\sigma(z) = y$. Podle lemma 20 existuje $\tau \in G$ tak, že $\mathrm{res}_{K/L}(\tau) = \sigma$. Pro toto τ platí $\tau(z) = y$, a tedy $\tau(M) \neq M$. Protože α je bijekce, plyne odtud, že $\mathrm{Aut}(K/\tau(M)) = \alpha(\tau(M)) \neq \alpha(M) = \mathrm{Aut}(K/M)$. To podle lemma 22 znamená, že $\alpha(M)$ není normální podgrupa grupy G.

Je-li $M \in \mathcal{M}$ takové, že M/F je konečné rozšíření, pak existuje $L \in \mathcal{L}$ tak, že $M \subseteq L$ (za L můžeme vzít Galoisův uzávěr M/F v K). Víme, že $\mathrm{Aut}(K/L)$ je otevřená podgrupa grupy G (viz závěr poznámky 19). Protože $\mathrm{Aut}(K/L) \subseteq \mathrm{Aut}(K/M)$, je podgrupa

$$\alpha(M) = \mathrm{Aut}(K/M) = \bigcup_{\sigma \in \mathrm{Aut}(K/M)} \sigma \circ \mathrm{Aut}(K/L)$$

sjednocení otevřených množin, a tedy otevřená množina. Podle lemma 20 je $\mathrm{res}_{K/L}$ surjektivní. Protože $\ker(\mathrm{res}_{K/L}) = \mathrm{Aut}(K/L)$, existuje izomorfismus grup $\psi\colon G/\mathrm{Aut}(K/L) \to \mathrm{Gal}(L/F)$ tak, že komutuje diagram

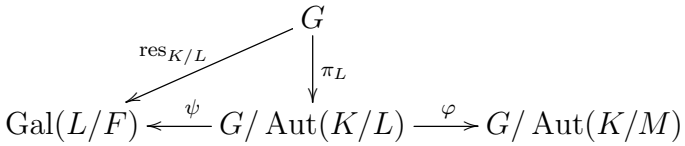
$$\begin{array}{ccc} & & G \\ & {\scriptstyle \mathrm{res}_{K/L}} \swarrow & \downarrow {\scriptstyle \pi_L} \\ \mathrm{Gal}(L/F) & \xleftarrow{\psi} & G/\mathrm{Aut}(K/L) \end{array}$$

kde π_L je projekce na faktorgrupu. Protože $\mathrm{Aut}(K/M)$ je podgrupou grupy G, máme rozklad $G/\mathrm{Aut}(K/M)$ na levé třídy rozkladu (vzhledem k tomu, že nepředpokládáme, že je M/F normální rozšíření, nemusí být podgrupa $\mathrm{Aut}(K/M)$ grupy G normální, a proto nelze hovořit o faktorgrupě, ale pouze o rozkladu). Sestrojíme zobrazení

$$\varphi\colon G/\mathrm{Aut}(K/L) \to G/\mathrm{Aut}(K/M)$$

předpisem $\varphi(\gamma \circ \mathrm{Aut}(K/L)) = \gamma \circ \mathrm{Aut}(K/M)$ pro libovolné $\gamma \in G$. Tato definice je korektní, neboť $\mathrm{Aut}(K/L) \subseteq \mathrm{Aut}(K/M)$: jestliže totiž pro nějaké

$\gamma, \delta \in G$ platí $\gamma \circ \mathrm{Aut}(K/L) = \delta \circ \mathrm{Aut}(K/L)$, pak $\delta^{-1} \circ \gamma \in \mathrm{Aut}(K/L) \subseteq \mathrm{Aut}(K/M)$, a tedy $\gamma \circ \mathrm{Aut}(K/M) = \delta \circ \mathrm{Aut}(K/M)$. Zřejmě je φ surjektivní. Protože ψ je bijekce, je také $\varphi \circ \psi^{-1}$ surjektivní zobrazení; přitom má následující předpis: pro dané $\sigma \in \mathrm{Gal}(L/F)$ zvolíme libovolné $\gamma \in G$ takové, že $\sigma = \mathrm{res}_{K/L}(\gamma)$, pak $(\varphi \circ \psi^{-1})(\sigma) = \gamma \circ \mathrm{Aut}(K/M)$.



Zvolme libovolně $\sigma, \tau \in \mathrm{Gal}(L/F)$ a najděme k nim vhodná $\gamma, \delta \in G$ tak, aby $\sigma = \mathrm{res}_{K/L}(\gamma)$, $\tau = \mathrm{res}_{K/L}(\delta)$. Následující podmínky jsou ekvivalentní:

- $(\varphi \circ \psi^{-1})(\sigma) = (\varphi \circ \psi^{-1})(\tau)$,
- $\gamma \circ \mathrm{Aut}(K/M) = \delta \circ \mathrm{Aut}(K/M)$,
- $\gamma^{-1} \circ \delta \in \mathrm{Aut}(K/M)$,
- $\forall\ z \in M$: $(\gamma^{-1} \circ \delta)(z) = z$,
- $\forall\ z \in M$: $\gamma(z) = \delta(z)$,
- $\forall\ z \in M$: $\sigma(z) = \tau(z)$,
- $\forall\ z \in M$: $(\tau^{-1} \circ \sigma)(z) = z$,
- $\tau^{-1} \circ \sigma \in \mathrm{Gal}(L/M)$,
- $\sigma \circ \mathrm{Gal}(L/M) = \tau \circ \mathrm{Gal}(L/M)$.

Užijeme-li předchozí implikaci zdola nahoru, dostaneme, že předpis

$$\sigma \circ \mathrm{Gal}(L/M) \mapsto (\varphi \circ \psi^{-1})(\sigma) \qquad \text{pro libovolné } \sigma \in \mathrm{Gal}(L/F)$$

korektně definuje zobrazení $\mathrm{Gal}(L/F)/\mathrm{Gal}(L/M) \to G/\mathrm{Aut}(K/M)$. Tyto implikace shora dolů dávají, že je to injektivní zobrazení. A konečně ze surjektivity $\varphi \circ \psi^{-1}$ dostaneme, že je to také surjektivní zobrazení. Proto platí $|\mathrm{Gal}(L/F)/\mathrm{Gal}(L/M)| = |G/\mathrm{Aut}(K/M)|$, a tedy $|G/\mathrm{Aut}(K/M)| = [M : F]$.

Je-li naopak $M \in \mathcal{M}$ takové, že M/F je nekonečné rozšíření, pro libovolné $n \in \mathbb{N}$ existuje $N \in \mathcal{M}$ tak, že $N \subseteq M$ a N/F je konečné rozšíření stupně $[N : F] > n$. Pak $\mathrm{Aut}(K/M) \subseteq \mathrm{Aut}(K/N)$, a tedy

$$|G/\mathrm{Aut}(K/M)| \geq |G/\mathrm{Aut}(K/N)| = [N : F] > n.$$

Má tedy podgrupa $\alpha(M) = \mathrm{Aut}(K/M)$ v grupě G nekonečný index.

Nechť nakonec je $M \in \mathcal{M}$ takové, že $\alpha(M)$ je otevřená podgrupa grupy G. Rozklad $G/\alpha(M)$ je pak otevřené pokrytí kompaktní množiny G disjunktními množinami. Proto existuje jeho konečné podpokrytí. Ovšem vynecháním libovolné z těchto množin už nedostaneme pokrytí. Rozklad $G/\alpha(M)$ tedy má jen konečně mnoho tříd rozkladu, a proto $\alpha(M)$ má konečný index v G. Podle výše dokázaného je rozšíření M/F konečné.

Příklad 26. Nechť p je prvočíslo. Označme

$$K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{p^n}),$$

kde $\zeta_{p^n} = \cos\frac{2\pi}{p^n} + i\sin\frac{2\pi}{p^n}$ je primitivní p^n-tá odmocnina z jedné. Zřejmě je $K/\mathbb{Q}$ algebraické, normální a separabilní rozšíření. Nechť $G = \mathrm{Aut}(K/\mathbb{Q})$ je topologická grupa s Krullovou topologií. Pro každé $n \in \mathbb{N}$ platí

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times,$$

přičemž třídě $[a]_{p^n}$ odpovídá automorfismus tělesa $\mathbb{Q}(\zeta_{p^n})$ určený podmínkou $\zeta_{p^n} \mapsto \zeta_{p^n}^a$. Proto je G topologická grupa izomorfní (algebraicky a současně topologicky) s projektivní limitou grup $(\mathbb{Z}/p^n\mathbb{Z})^\times$ vůči homomorfismům určeným takto: pro každé $i, j \in \mathbb{N}$, $i \leq j$ je $\varphi_{ij}\colon (\mathbb{Z}/p^j\mathbb{Z})^\times \to (\mathbb{Z}/p^i\mathbb{Z})^\times$ (platí $\varphi_{ij}([a]_{p^j}) = [a]_{p^i}$ pro každé $a \in \mathbb{Z}$), tedy $G \cong \varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times$. Snadno je vidět, že tento projektivní systém grup dostáváme z prvního z příkladů 11 nahrazením okruhů jejich grupami jednotek, odkud dostáváme, že tato projektivní limita je grupou jednotek okruhu celých p-adických čísel $G \cong \mathbb{Z}_p^\times$.

Příklad 27. Nechť p je liché prvočíslo. Protože pro každé $n \in \mathbb{N}$ je grupa $(\mathbb{Z}/p^n\mathbb{Z})^\times$ cyklická řádu $(p-1)p^{n-1}$, má jedinou podgrupu řádu $p-1$ a vzniklá faktorgrupa je cyklická řádu p^{n-1}. Proto má těleso $\mathbb{Q}(\zeta_{p^n})$ jediné podtěleso stupně p^{n-1}, které označíme B_{n-1}. Je tedy $B_{n-1}/\mathbb{Q}$ cyklické rozšíření stupně p^{n-1}. Platí

$$\mathbb{Q} = B_0 \subset B_1 \subset B_2 \subset \ldots$$

Označme $K = \bigcup_{n=1}^{\infty} B_n$. Pak $K/\mathbb{Q}$ je algebraické, normální a separabilní rozšíření. Přitom restrikce dává pro libovolné $i, j \in \mathbb{N}$, $i \leq j$ surjektivni homomorfismus grup

$$\mathrm{Gal}(B_j/\mathbb{Q}) \to \mathrm{Gal}(B_i/\mathbb{Q}).$$

Protože $\mathrm{Gal}(B_j/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$, porovnáním s prvním z příkladů 11, v němž okruhy nahradíme jejich aditivními grupami, dostáváme, že platí (algebraicky a současně topologicky)

$$\mathrm{Aut}(K/\mathbb{Q}) \cong (\mathbb{Z}_p, +).$$

Poznámka 28. Algebraické, normální a separabilní rozšíření K/F takové, že $\mathrm{Aut}(K/F) \cong (\mathbb{Z}_p, +)$, se nazývá $\mathbb{Z}_p$-rozšíření. V případě, kdy $K \subseteq \mathbb{C}$ a F je konečné rozšíření $\mathbb{Q}$, jsou tato $\mathbb{Z}_p$-rozšíření studována v tzv. Iwasawově teorii.

Příklad 29. Nechť p je prvočíslo. Pro libovolné $n \in \mathbb{N}$ máme konečné těleso $\mathbb{F}_{p^n}$ o p^n prvcích, přičemž tato tělesa jsou volena tak, že pro každá $m, n \in \mathbb{N}$ taková, že $m \mid n$, platí $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. Víme, že Galoisova grupa $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ je cyklická, generována Frobeniovým automorfismem $x \mapsto x^p$, tedy

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}.$$

Porovnáním s druhým z příkladů 11, v němž okruhy nahradíme jejich aditivními grupami, dostáváme, že pro těleso $\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$, což je algebraický uzávěr tělesa $\mathbb{F}_p$, platí (algebraicky a současně topologicky)

$$\mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong (\widehat{\mathbb{Z}}, +).$$

Reference

[1] D. Ramakrishnan, R. V. Valenza, *Fourier Analysis on Number Fields*, Graduate Texts in Mathematics 186, Springer-Verlag, New York, 1999.