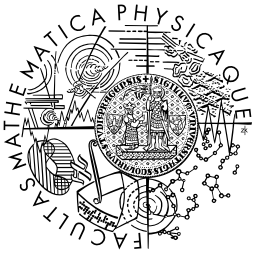

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Sára Tomášková

Elementární teorie grup lineárně lomených transformací

Katedra algebry

Vedoucí bakalářské práce: prof. RNDr. Aleš Drápal, CSc., DSc.
Studijní program: Obecná matematika
Studijní obor: MOMP

Praha 2023

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Děkuji svému vedoucímu prof. RNDr. Aleši Drápalovi, CSc,. DSc. za čas strávený nad mou prací, trpělivost a užitečné rady. Dále děkuji svým rodičům za umožnění vysokoškolského studia a podporu během něj. Za podporu děkuji také svým kočkám, byť v jejich případě obnášela jen to, že mi byly průběhu tvorby této práce velmi často nablízku.

Název práce: Elementární teorie grup lineárně lomených transformací

Autor: Sára Tomášková

Katedra: Katedra algebry

Vedoucí bakalářské práce: prof. RNDr. Aleš Drápal, CSc., DSc., Katedra algebry

Abstrakt: Práce popisuje vlastnosti obecné projektivní lineární grupy $PGL_2(\mathbb{F})$ a jejího působení na projektivní přímce $\mathbb{P}^1(\mathbb{F})$, a to jak pro konečné, tak i pro nekonečné těleso $\mathbb{F}$. K důkazům těchto vlastností jsou zde využívány pouze základní znalosti z bakalářského studia. Rozebrána je ostrá 3-tranzitivita zmíněné grupy. Poté jsou zkoumány podgrupy tvořené identitou a všemi prvky, jejichž množiny pevných bodů se shodují. Je rovněž popsáno, za jakých podmínek mají tyto podgrupy vlastnost, že každá jejich konečná podgrupa je cyklická. Následně se odvodí, že v případě, že je těleso $\mathbb{F}$ konečné, platí, že jsou cyklické všechny tyto grupy, právě když $\mathbb{F}$ je rovno $\mathbb{Z}_p$ pro nějaké prvočíslo p. Dále se práce soustředí na působení $PGL_2(\mathbb{F})$ konjugací na množině těchto svých podgrup. Nakonec je dokázána jednoduchost projektivní speciální lineární grupy $PSL_2(\mathbb{F})$.

Klíčová slova: obecná projektivní lineární grupa, grupa lineárních lomených transformací, grupa Möbiových transformací, lineární lomená transformace

Title: Elementary theory for groups of linear transformations

Author: Sára Tomášková

Department: Department of Algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc., Department of Algebra

Abstract: The thesis focuses on the properties of general projective linear group $PGL_2(\mathbb{F})$ and its action on the projective line $\mathbb{P}^1(\mathbb{F})$, both for a finite and an infinite field $\mathbb{F}$. Only the basic knowledge from the Bachelor studies is used to prove these properties. Sharp 3-transitivity of the said group is discussed. Then, we deal with the subgroups consisting of identity and all elements whose sets of fixed points coincide. Furthermore, we show under which conditions all these subgroups have the property that all their finite subgroups are cyclic. We deduce that for a finite field $\mathbb{F}$, it holds that all of these groups are cyclic if and only if $\mathbb{F}$ is equal to $\mathbb{Z}_p$ for a prime number p. The thesis then focuses on the action of $PGL_2(\mathbb{F})$ by conjugation on the set of these sungroups. Finally, it is shown that projective special linear group $PSL_2(\mathbb{F})$ is simple.

Keywords: general projective linear group, group of linear transformations, group of Möbius transformations, linear fractional transformation

Obsah

Úvod

Práce se zaměřuje na obecnou projektivní lineární grupu $PGL_2(\mathbb{F})$ a její působení na projektivní přímce $\mathbb{P}^1(\mathbb{F})$. Pro stručnost místo $PGL_2(\mathbb{F})$ píšeme $L(\mathbb{F})$, což je značení, které jsme zvolili pro grupu lineárních lomených transformací. Jak dokládá Lemma 21 a důkaz Tvrzení 22, zkoumat $PGL_2(\mathbb{F})$ a $L(\mathbb{F})$ je v zásadě totéž, neboť tyto dvě grupy jsou izomorfní a působení $PGL_2(\mathbb{F})$ na $\mathbb{P}^1(\mathbb{F})$ je ekvivalentní (Definice 5) s působením $L(\mathbb{F})$ na množině $\mathbb{F} \cup \{\infty\}$.

Většina vlastností grupy $L(\mathbb{F})$ je dobře známá. Mnoho z nich je možné dokázat pouze za použití nepříliš pokročilé matematiky, tedy základních znalostí z bakalářského studia. Například, k důkazu skutečnosti, že za předpokladu konečnosti tělesa $\mathbb{F}$ můžeme $L(\mathbb{F})$ zapsat jako sjednocení určitých cyklických grup právě tehdy, když $\mathbb{F} = \mathbb{Z}_p$ pro nějaké prvočíslo p (Důsledek 42), stačí znát polynomy a umět počítat modulo prvočíslo. K důkazu existence Singerových cyklů v $L(\mathbb{F})$ (Definice 16) se obvykle využívá kvadratických rozšíření těles; práce ukazuje, že jej lze provést pouze elementárními úvahami.

Zaměřuji se i na některé aspekty, které obvykle detailně rozebírány nebývají. Zde můžeme opět zmínit Singerův cyklus, který je v matematice často skloňovaným pojmem, ale málokdy je uveden explicitní předpis operace skládání v podobě, která by ozřejmila, že jde vlastně o grupovou operaci na projektivní přímce (o této skutečnosti pojednává Věta 26). Strategie důkazu cykličnosti Singerova cyklu použitá v práci je takováto: V první fázi se explicitně popíše operace abelovské grupy na projektivní přímce, která je izomorfní podgrupě prvků $PGL_2(\mathbb{F})$, jež tvoří Singerův cyklus. V této fázi se však ještě neví, že je to skutečně cyklus, čili že jde o cyklickou grupu. Poté se ukáže, že násobení prvků pomocí popsané operace indukuje určité polynomy a že řád prvků je možno vyšetřovat pomocí toho, zda se takový polynom rovná nule. Využitím kombinatorických čísel se pak ověří, že jistý koeficient takového polynomu musí být pro nižší mocniny nenulový, a odsud se odvodí, že v grupě skutečně existují prvky maximálního možného řádu.

Tato práce se věnuje i případům, kdy $\mathbb{F}$ je nekonečné. V případě nekonečného tělesa je obdoba Singerova cyklu tranzitivní abelovská grupa (taková grupa je nutně regulární). V práci se zabývám otázkou, kdy jsou takové dvě grupy konjugované. Pro konečné těleso jsou konjugované libovolné dva Singerovy cykly. V obecném případě platí, že každá z uvažovaných grup je asociovaná s nějakým kvadratickým ireducibilním polynomem. Ukáže se, že dvě uvažované grupy jsou konjugované právě tehdy, když rozkladová nadtělesa těchto kvadratických polynomů jsou izomorfní.

Text je rozdělen na dvě části. První z nich, nazvaná Obecné poznatky o grupách, obsahuje tvrzení týkající se permutačních grup a tělesových rozšíření. Tato tvrzení jsou později využita v části druhé, zabývající se samotnou grupou $L(\mathbb{F})$. Ta je rozčleněna do několika sekcí. V sekci 2.2 je dokázána ostrá 3-tranzitivita zmíněné grupy. Sekce 2.3 se věnuje podgrupám $L(\mathbb{F})$ tvořeným jednotkou a všemi prvky se shodnými množinami pevných bodů. Speciálně jsou v ní popsány ty z těchto podgrup, jejichž netriviální prvky mají pevný bod právě jeden; na tyto grupy totiž často narážíme v sekci 2.4. Hlavními výsledky sekce 2.4 jsou již zmíněný Důsledek 42 a důkaz existence Singerova cyklu v $L(\mathbb{F})$ (Tvrzení 43). Sekce

2.5 pojednává o působení $L(\mathbb{F})$ konjugací na množině podgrup ze sekce 2.3. Především je zde rozebráno, za jakých podmínek jsou dvě takové podgrupy konjugované (Tvrzení 46, Věty 49 a 54, Důsledek 56), jak vypadají jejich normalizátory (Tvrzení 57, 59, 60) a že jde o maximální abelovské podgrupy (Tvrzení 67). Poslední sekce se týká projektivní speciální lineární grupy $PSL_2(\mathbb{F})$. Konkrétně se soustředí na důkaz její jednoduchosti.

Místy jsem vycházela z knihy [1], inspirovala jsem se jí v Tvrzení 1, 2 a Lematu 72. Zbytek jsou má vlastní pozorování podnícená vedoucím práce.

1. Obecné poznatky o grupách

1.1 Základní definice a tvrzení

Nechť $\mathbb{F}$ je komutativní těleso a $n \in \mathbb{N}$.

Definice 1. Obecná lineární grupa $GL_n(\mathbb{F})$ *je množina všech regulárních matic nad* $\mathbb{F}$ *typu* $n \times n$ *spolu s operacemi maticového násobení, maticového invertování a jednotkovou maticí jako jednotkou.*

Tvrzení 1. *Platí*

$$Z(GL_n(\mathbb{F})) = \{\lambda I_n \mid \lambda \in \mathbb{F}^*\},$$

kde I_n *značí jednotkovou matici typu* $n \times n$*. Přitom* $M \in Z(GL_n(\mathbb{F}))$*, právě když každý vektor z* F^n *je vlastním vektorem matice* M*.*

Důkaz. Označme E_{ij} matici, jejíž prvek na pozici (i,j) je 1 a ostatní jsou rovny 0. Nechť $X_{ij} = I_n + E_{ij}$. Pro $i \neq j$ pak $\det(X_{ij}) = \det(I_n) = 1$, tj. $X_{ij} \in GL_n(\mathbb{F})$.

Předpokládejme, že $M = (m_{ij})_{i,j=1}^n \in Z(GL_n(\mathbb{F}))$. Uvažujme čísla $k, l \in \{1, \ldots, n\}$, $k \neq l$.

Prvek matice $X_{kl}M$, resp. MX_{kl}, na pozici (k,k) je $m_{kk} + m_{lk}$, resp. m_{kk}. Protože $M \in Z(GL_n(\mathbb{F}))$, platí $X_{kl}M = MX_{kl}$, tedy dostáváme $m_{kk} + m_{lk} = m_{kk}$, neboli $m_{lk} = 0$. Prvek matice $X_{kl}M$, resp. MX_{kl}, na pozici (k,l) je $m_{kl} + m_{ll}$, resp. $m_{kk} + m_{kl}$. Odsud $m_{ll} = m_{kk}$.

Každá matice v $Z(GL_n(\mathbb{F}))$ je tedy diagonální a všechny prvky na její diagonále jsou stejné, neboli je nenulovým násobkem I_n.

Naopak, každá matice λI_n, $\lambda \in \mathbb{F}^*$, je v $Z(GL_n(\mathbb{F}))$ zřejmě obsažena.

Každý vektor z $\mathbb{F}^n$ je zjevně vlastním vektorem matice λI_n příslušný vlastnímu číslu λ. Pokud je naopak každý vektor vlastním vektorem matice $M \in GL_n(\mathbb{F})$, je M diagonální, neboť $(1, 0, \ldots, 0)^T, (0, 1, 0, \ldots, 0)^T, \ldots, (0, \ldots, 0, 1)^T$ jsou vlastní, přičemž všechny hodnoty na diagonále jsou stejné, jelikož $(1, \ldots, 1)^T$ je vlastní. Tedy $M = \lambda I_n$ pro nějaké $\lambda \in \mathbb{F}^*$.

□

Definice 2. Projektivní obecná lineární grupa *je definována jako faktorgrupa* $GL_n(\mathbb{F})/Z(GL_n(\mathbb{F}))$ *a značíme ji* $PGL_n(\mathbb{F})$*.*

Definice 3. Speciální lineární grupa $SL_n(\mathbb{F})$ *je podgrupa grupy* $GL_n(\mathbb{F})$ *tvořená všemi maticemi s determinantem 1.*

Definice 4. Projektivní speciální lineární grupu *definujeme jako* $PSL_n(\mathbb{F}) = SL_n(\mathbb{F})/Z(SL_n(\mathbb{F}))$*.*

Tvrzení 2. *Grupa* $Z(SL_n(\mathbb{F}))$ *je tvořena právě násobky jednotkové matice* I_n *s determinantem 1, neboli platí* $Z(SL_n(\mathbb{F})) = SL_n(\mathbb{F}) \cap Z(GL_n(\mathbb{F}))$*.*

Důkaz. Matice X_{ij} z důkazu Tvrzení 1 mají pro $i \neq j$ determinant 1, tedy leží v $SL_n(\mathbb{F})$. Tentýž postup jako ve zmíněném důkazu tudíž můžeme použít i zde.

□

Na grupu $PSL_n(\mathbb{F})$ můžeme nahlížet jako na podgrupu $PGL_n(\mathbb{F})$. Podle 3. věty

o izomorfismu je totiž $SL_n(\mathbb{F})/Z(SL_n(\mathbb{F})) = SL_n(\mathbb{F})/(SL_n(\mathbb{F}) \cap Z(GL_n(\mathbb{F})))$ izomorfní $(SL_n(\mathbb{F})Z(GL_n(\mathbb{F})))/Z(GL_n(\mathbb{F}))$, což je podgrupa $GL_n(\mathbb{F})/Z(GL_n(\mathbb{F})) = PGL_n(\mathbb{F})$.

Tvrzení 3. *Označme $[A]$ rozkladovou třídu grupy $GL_n(\mathbb{F})$ podle $Z(GL_n(\mathbb{F}))$ reprezentovanou prvkem $A \in GL_n(\mathbb{F})$ (tj. prvek grupy $PGL_n(\mathbb{F})$) a $\langle \mathbf{v} \rangle$ lineární obal (řádkového) vektoru $\mathbf{v} \in \mathbb{F}^n$. Grupa $PGL_n(\mathbb{F})$ má věrné působení na projektivním prostoru $\mathbb{P}^{n-1}(\mathbb{F}) = \{\langle \mathbf{v} \rangle \mid \mathbf{0} \neq \mathbf{v} \in \mathbb{F}^n\}$ definované předpisem*

$$[A](\langle \mathbf{v} \rangle) = \langle (A\mathbf{v}^T)^T \rangle \ \forall [A] \in PGL_n(\mathbb{F}),\ \langle \mathbf{v} \rangle \in \mathbb{P}^{n-1}(\mathbb{F}),$$

kde $A\mathbf{v}^T$ je maticový součin.

Důkaz. Připomeňme, že působení grupy G na množině X je grupový homomorfismus $\pi\colon G \to S_X$, kde S_X značí grupu všech permutací množiny X.

Uvažujme

$$\pi\colon GL_n(\mathbb{F}) \to S_{\mathbb{P}^{n-1}(\mathbb{F})},$$

kde

$$\pi(A)\colon \langle \mathbf{v} \rangle \mapsto \langle (A\mathbf{v}^T)^T \rangle,\ \langle \mathbf{v} \rangle \in \mathbb{P}^{n-1}(\mathbb{F}).$$

Nechť $A \in GL_n(\mathbb{F})$. Zobrazení $\pi(A)$ má inverz $\pi(A^{-1})$, tudíž jde o permutaci. Tedy $\pi(A) \in S_{\mathbb{P}^{n-1}(\mathbb{F})}$ a π je tudíž dobře definované.

Pro $A, B \in GL_n(\mathbb{F})$ a $\langle \mathbf{v} \rangle \in \mathbb{P}^{n-1}(\mathbb{F})$ platí

$$\pi(A)\pi(B)(\langle \mathbf{v} \rangle) = \pi(A)(\langle (B\mathbf{v}^T)^T \rangle) = \langle (A(B\mathbf{v}^T))^T \rangle = \pi(AB)(\langle \mathbf{v} \rangle),$$

tj. π je homomorfismus. Grupa $GL_n(\mathbb{F})$ tedy působí na $\mathbb{P}^{n-1}(\mathbb{F})$.

Navíc

$$\begin{gathered}
\mathrm{Ker}(\pi) = \{A \in GL_n(\mathbb{F}) \mid \pi(A)(\langle \mathbf{v} \rangle) = \langle \mathbf{v} \rangle\ \forall \langle \mathbf{v} \rangle \in \mathbb{P}^{n-1}(\mathbb{F})\} = \\
= \{A \in GL_n(\mathbb{F}) \mid \forall \mathbf{0} \neq \mathbf{v} \in \mathbb{F}^n\ \exists \lambda_{\mathbf{v}} \in \mathbb{F}^*\colon (A\mathbf{v}^T)^T = (\lambda_{\mathbf{v}}\mathbf{v}^T)^T\} = \\
= \{A \in GL_n(\mathbb{F}) \mid \forall \mathbf{0} \neq \mathbf{v} \in \mathbb{F}^n\ \exists \lambda_{\mathbf{v}} \in \mathbb{F}^*\colon A\mathbf{v}^T = \lambda_{\mathbf{v}}\mathbf{v}^T\} = \\
= \{A \in GL_n(\mathbb{F}) \mid \mathbf{v}^T \text{ je vlastním vektorem matice } A\ \forall \mathbf{v} \in \mathbb{F}^n\} = \\
= Z(GL_n(\mathbb{F})).
\end{gathered}$$

$\Rightarrow$ Grupa $PGL_n(\mathbb{F}) = GL_n(\mathbb{F})/Z(GL_n(\mathbb{F}))$ působí na $\mathbb{P}^{n-1}(\mathbb{F})$ věrně.

□

Definice 5. *Řekneme, že působení grupy G na množině X je* ekvivalentní *s působením grupy H na množině Y, pokud existuje izomorfismus $\varphi\colon G \simeq H$ a bijekce $\alpha\colon X \to Y$ tak, že $\forall g \in G$ a x_1,$x_2 \in X$ splňující $g(x_1) = x_2$ platí*

$$(\varphi(g))(\alpha(x_1)) = \alpha(x_2).$$

Tvrzení 4. *Mějme grupu $G = (G, \cdot, ^{-1}, e)$ a množinu H, na které je definována binární operace $\circ\colon H \times H \to H$. Nechť $\varphi\colon G \to H$ je surjektivní zobrazení splňující*

$$\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)\ \forall a, b \in G.$$

Pak H je grupa (vzhledem k operaci $\circ$).

Důkaz. Ověříme grupové axiomy pro H.

Nechť $\alpha, \beta, \gamma \in H$. Zobrazení φ je na, tudíž existují $a, b, c \in G$ taková, že $\varphi(a) = \alpha$, $\varphi(b) = \beta$, $\varphi(c) = \gamma$. Potom

$$\alpha \circ (\beta \circ \gamma) = \varphi(a) \circ (\varphi(b) \circ \varphi(c)) = \varphi(a) \circ \varphi(b \cdot c) = \varphi(a \cdot (b \cdot c)) =$$
$$= \varphi((a \cdot b) \cdot c) = \varphi(a \cdot b) \circ \varphi(c) = (\varphi(a) \circ \varphi(b)) \circ \varphi(c) = (\alpha \circ \beta) \circ \gamma.$$

Obdobně se ukáže, že $\varphi(e) \circ \alpha = \alpha \circ \varphi(e) = \alpha \ \forall \alpha \in H$ a $\varphi(a^{-1}) \circ \alpha = \alpha \circ \varphi(a^{-1}) = \varphi(e)$ pro $\alpha = \varphi(a)$, tj. že $\varphi(e)$ je jednotka v H a $\varphi(a^{-1})$ je inverzní prvek k prvku α.

□

Definice 6. *Prvek řádu 2 v grupě G nazýváme* involuce.

1.2 k-tranzitivita a ostrá k-tranzitivita

Definice 7. *Nechť $k \in \mathbb{N}$. Řekneme, že permutační grupa G na množině X je* k-tranzitivní, *pokud $|X| \geq k$ a $\forall x_1, \ldots, x_k, y_1, \ldots, y_k \in X$ taková, že $x_i \neq x_j$, $y_i \neq y_j$ pro $i \neq j$, existuje $g \in G$ splňující $g(x_i) = y_i \ \forall i = 1, \ldots, k$. Grupu G nazýváme* ostře k-tranzitivní, *pokud takový prvek g existuje právě jeden.*

Poznámka. Místo „(ostře) 1-tranzitivní“ budeme psát zkráceně jen „(ostře) tranzitivní“.

Připomeňme, že každou abstraktní grupu G lze považovat za permutační grupu, neboť má věrné působení na své nosné množině (například působení levou translací). Toto působení je prostý homomorfismus $\pi \colon G \to S_G$, díky 1. větě o izomorfismu tudíž můžeme G ztotožnit s permutační grupou $\mathrm{Im}(\pi) \leq S_G$.

Neřekneme-li jinak, budeme v dalším textu grupou G vždy myslet nějakou grupu permutací množiny X, tedy podgrupu grupy S_X.

Definice 8. Stabilizátorem *bodů $x_1, \ldots, x_n \in X$ nazýváme množinu*

$$G_{x_1,\ldots,x_n} = \{g \in G \mid g(x_i) = x_i \ \forall i \in \{1, \ldots, n\}\}.$$

Poznámka. Uvedeme-li, že je stabilizátor bodů $x_1, \ldots, x_n \in X$ k-tranzitivní, automaticky se předpokládá, že je k-tranzitivní jako permutační grupa na množině $X \setminus \{x_1, \ldots, x_n\}$.

Lemma 5. *Mějme $k \in \mathbb{N}$, $k \geq 2$. Nechť je grupa G tranzitivní a nechť libovolný stabilizátor G_x bodu $x \in X$ je $(k-1)$-tranzitivní. Pak je G k-tranzitivní. Je-li navíc libovolný stabilizátor bodu ostře $(k-1)$-tranzitivní, pak je G ostře k-tranzitivní.*

Důkaz. Uvažujme $x_1, \ldots, x_k, y_1, \ldots, y_k \in X$ taková, že $x_i \neq x_j$, $y_i \neq y_j$ pro $i \neq j$. Grupa G je tranzitivní, a tedy existuje $g \in G$, že

$$g(x_1) = y_1.$$

Nechť G_{y_1} je stabilizátor bodu y_1. Z $(k-1)$-tranzitivity G_{y_1} dostáváme, že existuje $h \in G_{y_1}$ splňující

$$h(g(x_i)) = y_i \ \forall i = 2, \ldots, k$$

(body $g(x_1),\ldots,g(x_k)$ jsou po dvou různé, protože g permutuje množinu X, tj. přiřazení $x \mapsto g(x)$ je prosté). Navíc $h(y_1) = y_1$, neboť $h \in G_{y_1}$.

Máme tedy

$$(hg)(x_1) = h(g(x_1)) = h(y_1) = y_1,$$
$$(hg)(x_i) = h(g(x_i)) = y_i,\ i = 2,\ldots,k,$$

což jsme přesně chtěli.

Je-li navíc libovolný stabilizátor bodu ostře $(k-1)$-tranzitivní, uvažujme prvek $\tilde{g} \in G$ takový, že $\tilde{g}(x_i) = y_i\ \forall i$. Platí $\tilde{g}^{-1}(hg) \in G_{x_1}$, neboť $(\tilde{g}^{-1}(hg))(x_1) = x_1$. Zároveň máme $1 \in G_{x_1}$. Jednotka ale také fixuje body $x_2,\ldots,x_n$, z ostré $(k-1)$-tranzitivity stabilizátoru G_{x_1} tedy plyne, že $\tilde{g}^{-1}(hg) = 1$, neboli $\tilde{g} = hg$, grupa G je tedy ostře k-tranzitivní.

□

Lemma 6. *Nechť je grupa G k-tranzitivní. Pak jsou každé dva stabilizátory k bodů konjugované.*

Důkaz. Označme G_1 stabilizátor po dvou různých bodů $x_1,\ldots,x_k \in X$, G_2 stabilizátor po dvou různých bodů $y_1,\ldots,y_k \in X$.

Z k-tranzitivity plyne, že existuje $g \in G$ takové, že $g(x_i) = y_i\ \forall i = 1,\ldots,k$.

Zobrazení

$$\varphi\colon G_2 \to G_1,\ h \mapsto g^{-1}hg,$$
$$\psi\colon G_1 \to G_2,\ h' \mapsto gh'g^{-1}$$

jsou poté vzájemně inverzní grupové homomorfismy. Jde tedy o izomorfismy grup G_1, G_2.

□

Důsledek 7. *Je-li grupa G tranzitivní a stabilizátor G_x bodu $x \in X$ je (ostře) k-tranzitivní, pak libovolný stabilizátor je (ostře) k-tranzitivní.*

Důkaz. Nechť G_y je stabilizátor bodu $y \in X$. Podle Lemmatu 6 nalezneme $g \in G$ takové, že $G_y = gG_xg^{-1}$, $g(x) = y$.

Uvažujme body $x_1,\ldots,x_k \in X\backslash\{y\}$ po dvou různé a $y_1,\ldots,y_k \in X\backslash\{y\}$ po dvou různé. Z k-tranzitivity G_x existuje $h \in G_x$, že $h(g^{-1}(x_i)) = g^{-1}(y_i)\ \forall i = 1,\ldots,k$.

Platí $(ghg^{-1})(x_i) = g(g^{-1}(y_i)) = y_i\ \forall i = 1,\ldots,k$, přičemž $ghg^{-1} \in G_y = gG_xg^{-1} \Rightarrow G_y$ je k-tranzitivní.

Nechť G_x je ostře k-tranzitivní. Předpokládejme, že pro $\tilde{g} \in G_y$ platí $\tilde{g}(x_i) = y_i\ \forall i = 1,\ldots,k$. Existuje $\tilde{h} \in G_x$ takové, že $\tilde{g} = g\tilde{h}g^{-1}$. Máme $\tilde{h}(g^{-1}(x_i)) = g^{-1}(y_i)$. Z ostré k-tranzitivity stabilizátoru G_x tudíž dostáváme, že $h = \tilde{h}$, a tedy také $\tilde{g} = ghg^{-1}$. Odsud plyne, že i stabilizátor G_y je ostře k-tranzitivní.

□

Poznámka. G_x v důsledku výše je k-tranzitivní jako permutační grupa na množině $X\backslash\{x\}$. V důkazu by tedy mohl nastat problém, kdyby $g^{-1}(x_i) = x$ nebo $g^{-1}(y_i) = x$ pro nějaké $i \in \{1,\ldots,k\}$. Tato možnost je ale vyloučena, neboť $g(x) = y$ a $x_i \neq y, y_i \neq y\ \forall i$.

Lemma 8. *Buď $x \in X$ a nechť pro každé $y \in X$ existuje $g_y \in G$ takové, že $g_y(y) = x$. Pak je grupa G tranzitivní.*

Důkaz. Pro libovolná $y_1, y_2 \in X$ platí

$$(g_{y_2}^{-1} g_{y_1})(y_1) = g_{y_2}^{-1}(x) = y_2.$$

□

Lemma 9. *Buď G permutační grupa na množině X a nechť g,$h \in G$. Prvky h a ghg^{-1} mají stejný počet pevných bodů.*

Důkaz. Buď $x \in X$. Platí

$$ghg^{-1}(x) = x \;\Leftrightarrow\; hg^{-1}(x) = g^{-1}(x),$$

tj. x je pevným bodem ghg^{-1} právě tehdy, když je $g^{-1}(x)$ pevným bodem h.

□

Lemma 10. *Buď H tranzitivní podgrupa grupy G, $g \in G$, $x \in X$. Pak existuje $a \in G_x$ takové, že $gHg^{-1} = aHa^{-1}$.*

Důkaz. Označme $g(y) = x$. Z tranzitivity grupy H plyne, že existuje $b \in H$ splňující $b(y) = x$. Potom $g = gb^{-1}b$, kde $gb^{-1} \in G_x$. Prvek gb^{-1} označme jako a. Pak

$$gHg^{-1} = (ab)H(ab)^{-1} = abHb^{-1}a^{-1} = aHa^{-1},$$

neboť $b \in H$.

□

Lemma 11. *Mějme abelovskou grupu $G \leq S_X$ a $O \subset X$ ať je orbita působení G na X. Nechť $g \in G$. Předpokládejme, že pro $x \in O$ platí $g(x) = x$. Pak $g(y) = y$ pro každé $y \in O$. Speciálně tedy máme, že je-li G tranzitivní a $g(x) = x$ pro $x \in X$, pak $g = 1$.*

Důkaz. Uvažujme prvek $y \in O$. Existuje $h \in G$ takové, že $h(x) = y$. Potom $(hg)(x) = y$. Protože G je abelovská, musí platit také $(gh)(x) = y$. Ale $(gh)(x) = g(h(x)) = g(y)$, takže $g(y) = y$.

□

Lemma 12. *Nechť $G \leq S_X$ a H je abelovská tranzitivní podgrupa G. Pak H je maximální abelovská podgrupa G, neboli neexistuje vlastní abelovská podgrupa $\tilde{H}$ grupy G taková, že H je ostře obsažena v $\tilde{H}$.*

Důkaz. Ať $\tilde{H} \subset G$ je maximální abelovská podgrupa G taková, že $H \subseteq \tilde{H}$. Nechť $g \in G$. Zvolme $x \in X$ a označme $g(x) = y$. Protože je grupa H tranzitivní, existuje $h \in H$ splňující $h(y) = x$. Pak $(hg)(x) = h(y) = x$. Použijeme-li tedy předchozí lemma pro abelovskou tranzitivní grupu $\tilde{H}$, dostaneme, že $hg = 1$, a tudíž $g = h^{-1} \in H$. Dokázali jsme tak, že $\tilde{H} = H$.

□

Definice 9. *Grupu G nazveme* regulární*, pokud je tranzitivní a každý stabilizátor bodu je triviální.*

1.3 Iwasawovo kritérium

Definice 10. *Grupa G je* jednoduchá*, pokud je netriviální a nemá vlastní podgrupu.*

Definice 11. Derivovanou podgrupu *grupy G definujeme jako*

$$G' = \langle ghg^{-1}h^{-1} \mid g,h \in G \rangle.$$

Označme $G' = G^{(1)}$ a pro $n > 1$ položme $G^{(n)} = (G^{(n-1)})'$.

Definice 12. *Grupa G je* řešitelná*, pokud existuje $n \in \mathbb{N}$ takové, že $G^{(n)}$ je triviální.*

Definice 13. *Podmnožinu $Y \subseteq X$ nazveme* blok *působení grupy G na množině X, jestliže $Y \neq \emptyset$ a pro každé $g \in G$ platí $g(Y) = Y$ nebo $g(Y) \cap Y = \emptyset$. Řekneme, že blok Y je* vlastní*, pokud $|Y| > 1$ a $Y \neq X$.*

Grupa $G \leq S_X$ je primitivní*, pokud její působení na X nemá vlastní bloky a $|X| > 1$.*

Poznámka. Je-li $|Y| = 1$ nebo $Y = X$, zřejmě jde vždy o blok.

Tvrzení 13. *Každá 2-tranzitivní grupa je primitivní.*

Důkaz. Ať G je 2-tranzitivní grupa. Nechť $Y \subset X$, $Y \neq X$, $|Y| > 1$. Uvažujme body $x_1, x_1' \in Y$, $x_1 \neq x_1'$. Dále zvolme libovolně $x_2 \in Y$ a $x_2' \in X \setminus Y \neq \emptyset$. Grupa G je 2-tranzitivní, tudíž existuje $g \in G$ takové, že $g(x_1) = x_2$, $g(x_1') = x_2'$. Tedy máme $x_2 \in g(Y) \cap Y$, $x_2' \in g(Y) \cap (X \setminus Y)$. Tj. platí $g(Y) \cap Y \neq \emptyset$ a zároveň $g(Y) \neq Y$. Množina Y tudíž není blok a G je tím pádem primitivní.

□

Lemma 14 (Iwasawovo kritérium)**.** *Buď $G \leq S_X$ primitivní permutační grupa taková, že $G' = G$. Ať $x \in X$, a nechť existuje podgrupa H grupy G splňující:*

1. *H je normální podgrupa grupy G_x,*
2. *H je řešitelná,*
3. *množina $\{ghg^{-1} \mid g \in G, h \in H\}$ generuje grupu G.*

Pak je G jednoduchá grupa.

Důkaz. Viz [2, Lemma 13.10].

□

1.4 Tělesová rozšíření

Lemma 15. *Předpokládejme, že charakteristika tělesa $\mathbb{F}$ je různá od 2. Pak každé rozšíření $\mathbb{G}$ tělesa $\mathbb{F}$ stupně 2 lze chápat jako rozkladové nadtěleso polynomu $x^2 - a \in \mathbb{F}[x]$. Ekvivalentně, existuje prvek $\delta \in \mathbb{G}$ takový, že $\mathbb{G} = \mathbb{F}[\delta]$ a $\delta^2 \in \mathbb{F}$.*

Důkaz. Jestliže je $\mathbb{G}$ rozšíření $\mathbb{F}$ stupně 2, lze na něj nahlížet jako na vektorový prostor nad $\mathbb{F}$ s bází $\{1,\varepsilon\}$. Pak $\mathbb{G} = \mathbb{F}[\varepsilon]$.

Označme $p(x) = x^2 + bx + c$ minimální polynom prvku ε, a přepišme jej do tvaru $p(x) = \left(x + \frac{b}{2}\right)^2 + c - \frac{b^2}{4}$. Platí

$$0 = p(\varepsilon) = \left(\varepsilon + \frac{b}{2}\right)^2 + c - \frac{b^2}{4},$$

tj. $\left(\varepsilon + \frac{b}{2}\right)^2 = \frac{b^2}{4} - c \in \mathbb{F}$. Tedy můžeme vzít $\delta = \varepsilon + \frac{b}{2}$. Zřejmě $\mathbb{F}[\varepsilon] = \mathbb{F}[\delta]$, a $\mathbb{G}$ je rozkladovým nadtělesem polynomu $x^2 - \delta^2 \in \mathbb{F}[x]$.

□

Lemma 16. *Je-li $|\mathbb{F}| < \infty$, jsou každá dvě rozšíření tělesa $\mathbb{F}$ stupně $k \in \mathbb{N}$ $\mathbb{F}$-izomorfní.*

Důkaz. Označme $|\mathbb{F}|^k = q$. Nechť $\mathbb{G}_1$, $\mathbb{G}_2$ jsou rozšíření tělesa $\mathbb{F}$ stupně k. Pak $|\mathbb{G}_1| = q = |\mathbb{G}_2|$. Pro libovolné $\delta \in \mathbb{G}_1^*$ platí $\delta^{q-1} = 1$, neboť $|\mathbb{G}_1^*| = q - 1$. Pro každé $\delta \in \mathbb{G}_1$ (včetně $\delta = 0$) tedy máme $\delta^q - \delta = 0$. Těleso $\mathbb{G}_1$ je tudíž tvořeno právě všemi kořeny polynomu $x^q - x \in \mathbb{F}[x]$. Je tedy rozkladovým nadtělesem tohoto polynomu. Obdobně je jeho rozkladovým nadtělesem také $\mathbb{G}_2$, neboť $\varepsilon^q - \varepsilon = 0$ $\forall \varepsilon \in \mathbb{G}_2$. Protože rozkladové nadtěleso je určeno jednoznačně až na $\mathbb{F}$-izomorfismus, dostáváme, co jsme chtěli.

□

Lemma 17. *Nechť $\mathbb{G}_1$, resp. $\mathbb{G}_2$, je rozkladové nadtěleso polynomu $p(x)$, resp. $q(x) \in \mathbb{F}[x]$, a platí $\mathbb{G}_1$,$\mathbb{G}_2 \subset \overline{\mathbb{F}}$. Pak $\mathbb{G}_1$ a $\mathbb{G}_2$ jsou $\mathbb{F}$-izomorfní, právě když $\mathbb{G}_1 = \mathbb{G}_2$.*

Důkaz. Nechť $\varphi\colon \mathbb{G}_1 \to \mathbb{G}_2$ je $\mathbb{F}$-izomorfismus. Označme $a_1, \ldots, a_n$ všechny kořeny polynomu $p(x)$ v $\overline{\mathbb{F}}$. Pak $\mathbb{G}_1 = \mathbb{F}[a_1, \ldots, a_n]$ a libovolný prvek $u \in \mathbb{G}_1$ lze (ne nutně jednoznačně) zapsat jako

$$u = \sum f_{i_1,\ldots,i_n} a_1^{i_1} \cdots a_n^{i_n}$$

pro nějaká $f_{i_1,\ldots,i_n} \in \mathbb{F}$. Pak máme

$$\varphi(u) = \sum f_{i_1,\ldots,i_n} \varphi(a_1)^{i_1} \cdots \varphi(a_n)^{i_n}.$$

Zobrazení φ permutuje množinu $\{a_1, \ldots, a_n\}$. Pro každé $i \in \{1, \ldots, n\}$ tedy existuje $j \in \{1, \ldots, n\}$ takové, že $\varphi(a_i) = a_j$. Tudíž $\varphi(u) \in \mathbb{G}_1$, neboli $\mathbb{G}_2 = \varphi(\mathbb{G}_1) \subset \mathbb{G}_1$.

Budeme-li uvažovat zobrazení $\varphi^{-1}\colon \mathbb{G}_2 \to \mathbb{G}_1$, které je opět $\mathbb{F}$-izomorfismem, obdobně dostaneme $\mathbb{G}_1 = \varphi^{-1}(\mathbb{G}_2) \subset \mathbb{G}_2$.

Dohromady tedy $\mathbb{G}_1 = \mathbb{G}_2$.

□

Lemma 18. *Nechť $\mathrm{char}(\mathbb{F}) \neq 2$ a a,$b \in \mathbb{F}^*$. Rozkladová nadtělesa polynomů $p(x) = x^2 - a$, $q(x) = x^2 - b \in \mathbb{F}[x]$ jsou $\mathbb{F}$-izomorfní, právě když existuje $c \in \mathbb{F}$ takové, že $ba^{-1} = c^2$.*

Důkaz. Předpokládejme, že jsou rozkladová nadtělesa polynomů $p(x)$, $q(x)$ $\mathbb{F}$-izomorfní. Rozlišíme dva případy.

1. Polynomy $p(x)$, $q(x)$ jsou reducibilní, tj. existují $s,t \in \mathbb{F}$ tak, že $a = s^2$, $b = t^2$. Pak $ba^{-1} = t^2 s^{-2} = (ts^{-1})^2$.

2. Polynomy $p(x)$, $q(x)$ jsou ireducibilní.

   Zafixujme $\overline{\mathbb{F}}$. Označme α, resp. β, kořen $p(x)$, resp. $q(x)$, v $\overline{\mathbb{F}}$. Máme $\mathbb{F} \subset \mathbb{F}[\alpha], \mathbb{F}[\beta] \subset \overline{\mathbb{F}}$. Z předchozího lemmatu víme, že $\mathbb{F}[\alpha] = \mathbb{F}[\beta]$. Existují tedy $e,f \in \mathbb{F}$ tak, že $\beta = e + f\alpha$. Potom také

   $$e^2 + 2ef\alpha + f^2\alpha^2 = (e + f\alpha)^2 = \beta^2 = b \in \mathbb{F}.$$

   Protože $e^2 + f^2\alpha^2 = e^2 + f^2 a \in \mathbb{F}$, musí platit $2ef\alpha \in \mathbb{F}$. Tedy $ef = 0$. Jinak by totiž prvek α ležel v $\mathbb{F}$, což neplatí, neboť $p(x)$ v $\mathbb{F}$ nemá kořen. Dále $f \neq 0$, jelikož $\beta \notin \mathbb{F}$. Nutně tudíž $e = 0$. Dostáváme tedy $f^2 a = f^2\alpha^2 = \beta^2 = b$, neboli $ba^{-1} = f^2$.

Nechť naopak platí $ba^{-1} = c^2$ pro nějaké $c \in \mathbb{F}$. Označme jako α kořen polynomu $p(x)$ (může být i $\alpha \in \mathbb{F}$). Rozkladovým nadtělesem $p(x)$ je pak $\mathbb{F}[\alpha]$. Z rovnosti $b = c^2 a = c^2\alpha^2$ plyne, že $q(x) = (x + c\alpha)(x - c\alpha)$, tj. $\mathbb{F}[c\alpha] = \mathbb{F}[\alpha]$ je zároveň rozkladovým nadtělesem polynomu $q(x)$.

□

Lemma 19. *Nechť $p(x)$, $q(x) \in \mathbb{F}[x]$ jsou ireducibilní polynomy, které mají $\mathbb{F}$-izomorfní rozkladová nadtělesa. Platí, že $p(x)$ nemá násobný kořen v $\overline{\mathbb{F}}$ právě tehdy, když nemá $q(x)$ násobný kořen v $\overline{\mathbb{F}}$.*

Důkaz. Označme $\mathbb{G}_1$, resp. $\mathbb{G}_2$, rozkladová nadtělesa polynomů $p(x)$, resp. $q(x)$.

Nechť $p(x)$ nemá násobný kořen v $\overline{\mathbb{F}}$, tj. je separabilní. Protože $\mathbb{G}_1$ a $\mathbb{G}_2$ jsou $\mathbb{F}$-izomorfní, je $\mathbb{G}_1$ zároveň také rozkladovým nadtělesem $q(x)$. Těleso $\mathbb{G}_1$ je separabilním rozšířením tělesa $\mathbb{F}$, neboť $p(x)$ je separabilní (viz [4, Tvrzení 2.21b)]). Každý kořen $q(x)$ je tedy separabilní prvek, a protože $q(x)$ je až na nenulový násobek minimálním polynomem každého ze svých kořenů (jelikož je ireducibilní nad $\mathbb{F}$), jde o separabilní polynom.

Obdobně, je-li $q(x)$ separabilní, pak je separabilní i $p(x)$.

□

2. Grupa lineárních lomených zobrazení

2.1 Definice

Buď $\mathbb{F}$ komutativní těleso a označme $M = \{ax + b \mid a,b \in \mathbb{F}\}$. Na $M \times M$ definujme relaci $\sim$ následovně:

$$(ax+b, cx+d) \sim (a'x+b', c'x+d') \Leftrightarrow \exists\lambda \in \mathbb{F}^*\colon\ a = \lambda a', b = \lambda b', c = \lambda c', d = \lambda d'.$$

Relace $\sim$ je zřejmě reflexivní, symetrická a tranzitivní, jedná se tedy o ekvivalenci. Třídu této ekvivalence reprezentovanou prvkem $(ax + b, cx + d)$ budeme značit $\frac{ax+b}{cx+d}$ a položíme

$$L(\mathbb{F}) = \left\{ \frac{ax + b}{cx + d} \mid ad - bc \neq 0 \right\}.$$

Výraz $\frac{ax+b}{0x+d} \in L(\mathbb{F})$ budeme někdy zapisovat také jako $ad^{-1}x + bd^{-1}$. Poznamenejme, že prvky M jsou pouze formální výrazy.

Lemma 20. *Na množině $L(\mathbb{F})$ definujme operaci $\circ\colon L(\mathbb{F}) \times L(\mathbb{F}) \to L(\mathbb{F})$ předpisem*

$$\frac{ax + b}{cx + d} \circ \frac{ex + f}{gx + h} = \frac{(ae + bg)x + (af + bh)}{(ce + dg)x + (cf + dh)}. \tag{2.1}$$

Tato definice je korektní, tedy nezávisí na volbě reprezentantů prvků $L(\mathbb{F})$.

Důkaz. Nechť $\frac{ax+b}{cx+d} = \frac{a'x+b'}{c'x+d'}$, $\frac{ex+f}{gx+h} = \frac{e'x+f'}{g'x+h'}$, tj. $a' = \lambda_1 a$, $b' = \lambda_1 b$, $c' = \lambda_1 c$, $d' = \lambda_1 d$, $e' = \lambda_2 e$, $f' = \lambda_2 f$, $g' = \lambda_2 g$, $h' = \lambda_2 h$ pro nějaká $\lambda_1,\lambda_2 \in \mathbb{F}^*$. Máme

$$\frac{a'x + b'}{c'x + d'} \circ \frac{e'x + f'}{g'x + h'} = \frac{(\lambda_1 a\lambda_2 e + \lambda_1 b\lambda_2 g)x + (\lambda_1 a\lambda_2 f + \lambda_1 b\lambda_2 h)}{(\lambda_1 c\lambda_2 e + \lambda_1 d\lambda_2 g)x + (\lambda_1 c\lambda_2 f + \lambda_1 d\lambda_2 h)} =$$
$$= \frac{\lambda_1\lambda_2((ae + bg)x + (af + bh))}{\lambda_1\lambda_2((ce + dg)x + (cf + dh))} = \frac{(ae + bg)x + (af + bh)}{(ce + dg)x + (cf + dh)} = \frac{ax + b}{cx + d} \circ \frac{ex + f}{gx + h}.$$

□

Lemma 21. *Množina $L(\mathbb{F})$ spolu s operací $\circ$ definovanou vztahem 2.1 je grupa izomorfní grupě $PGL_2(\mathbb{F})$.*

Důkaz. Uvažujme zobrazení

$$\Phi\colon GL_2(\mathbb{F}) \to L(\mathbb{F}),\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{ax + b}{cx + d}.$$

Z definice operace $\circ$ je ihned vidět, že $\forall A, B \in GL_2(\mathbb{F})$ platí

$$\Phi(AB) = \Phi(A) \circ \Phi(B).$$

Z Tvrzení 4 tedy plyne, že $\mathrm{Im}(\Phi)$ je grupa. Navíc

$$\mathrm{Im}(\Phi) = \left\{ \frac{ax+b}{cx+d} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}) \right\} =$$
$$= \left\{ \frac{ax+b}{cx+d} \mid a,b,c,d \in \mathbb{F},\ \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0 \right\} =$$
$$= \left\{ \frac{ax+b}{cx+d} \mid a,b,c,d \in \mathbb{F},\ ad-bc \neq 0 \right\} = L(\mathbb{F}).$$

Pro $\mathrm{Ker}(\Phi)$ platí

$$\mathrm{Ker}(\Phi) = \{A \in GL_2(\mathbb{F}) \mid \Phi(A) = x\} =$$
$$= \left\{ A \in GL_2(\mathbb{F}) \mid \Phi(A) = \frac{\lambda x + 0}{0x + \lambda},\ \lambda \in \mathbb{F}^* \right\} = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \mid \lambda \in \mathbb{F}^* \right\} =$$
$$= Z(GL_2(\mathbb{F})).$$

Z 1. věty o izomorfismu tedy plyne, že

$$L(\mathbb{F}) = \mathrm{Im}(\Phi) \simeq GL_2(\mathbb{F})/\mathrm{Ker}(\Phi) = GL_2(\mathbb{F})/Z(GL_2(\mathbb{F})) = PGL_2(\mathbb{F}).$$

□

Definice 14. *Grupu $(L(\mathbb{F}), \circ)$ z předchozího lemmatu nazýváme* grupa lineárních lomených zobrazení *(případně* lineárně lomená grupa *či* grupa Möbiových transformací*) a značíme opět $L(\mathbb{F})$. Z definice $\circ$ plyne, že unární operace $^{-1}$ v $L(\mathbb{F})$ má předpis*

$$\left(\frac{ax+b}{cx+d} \right)^{-1} = \frac{dx-b}{-cx+a}$$

a jednotkou je $\frac{1x+0}{0x+1}$.

Jednotku $\frac{1x+0}{0x+1}$ budeme dále zapisovat jen jako x.

2.2 Ostrá 3-tranzitivita

Položme $\frac{y}{0} = \infty$ pro $y \in \mathbb{F}^*$. Výraz $\frac{0}{0}$ nedefinujeme.

Množinu $\mathbb{F} \cup \{\infty\}$ můžeme ztotožnit s projektivní přímkou $\mathbb{P}^1(\mathbb{F})$. Nyní ukážeme, že grupa $L(\mathbb{F})$ má působení na $\mathbb{F} \cup \{\infty\}$, které je ekvivalentní s působením $PGL_2(\mathbb{F})$ na $\mathbb{P}^1(\mathbb{F})$.

Tvrzení 22. *Grupa $L(\mathbb{F})$ má na $\mathbb{F} \cup \{\infty\}$ věrné působení definované následovně:*

$$\left(\frac{ax+b}{cx+d} \right)(f) = \frac{af+b}{cf+d},\ f \in \mathbb{F};$$
$$\left(\frac{ax+b}{cx+d} \right)(\infty) = \frac{a}{c}.$$

Důkaz. Nejprve poznamenejme, že jde o korektní definici, neboli že na pravé straně nemůžeme dostat $\frac{0}{0}$. Případ $a = 0 = c$ je vyloučen podmínkou $ad - bc \neq 0$. Pokud $af + b = cf + d = 0$, $a \neq 0$ a $c \neq 0$, pak máme

$$af = -b,\, cf = -d \Rightarrow -a^{-1}b = f = -c^{-1}d \Rightarrow bc = ad,$$

ale poslední rovnost nenastává z definice $L(\mathbb{F})$. Je-li $a = 0$ a $af + b = 0$, potom nutně $b = 0$, a obdobně z $c = 0$ a $cf + d = 0$ plyne $d = 0$ a v obou případech tak opět dostáváme $bc = ad$.

Uvažujme značení jako v Tvrzení 3. Již víme, že $L(\mathbb{F}) \simeq PGL_2(\mathbb{F})$ a že $PGL_2(\mathbb{F})$ působí věrně na projektivní přímce $\mathbb{P}^1(\mathbb{F}) = \{\langle \mathbf{v} \rangle \mid \mathbf{0} \neq \mathbf{v} \in \mathbb{F}^2\}$. Navíc máme bijekci

$$\alpha \colon \mathbb{P}^1(\mathbb{F}) \to \mathbb{F} \cup \{\infty\};\ \alpha(\langle \mathbf{v} \rangle) = \frac{v_1}{v_2} \text{ pro } \mathbf{v} = (v_1,\, v_2)$$

(snadno lze nahlédnout, že zobrazení α je dobře definované).

Pro $a, b, c, d, f_1, f_2 \in \mathbb{F}$, $ad - bc \neq 0$, platí

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \langle (f_1,\, f_2) \rangle = \langle (af_1 + bf_2,\, cf_1 + df_2) \rangle\,,$$

$$\left(\frac{ax+b}{cx+d}\right)(\alpha\,(\langle (f_1,\, f_2) \rangle)) = \frac{a\frac{f_1}{f_2} + b}{c\frac{f_1}{f_2} + d} = \frac{af_1 + bf_2}{cf_1 + df_2} = \alpha\,(\langle (af_1 + bf_2,\, cf_1 + df_2) \rangle)$$

(předposlední rovnost je splněna i pro $f_2 = 0$).

Působení $L(\mathbb{F})$ na $\mathbb{F} \cup \{\infty\}$ je tedy také dobře definované a věrné, neboť je ekvivalentní s působením $PGL_2(\mathbb{F})$ na $\mathbb{P}^1(\mathbb{F})$.

□

Odteď tedy budeme $L(\mathbb{F})$ chápat jako podgrupu permutační grupy množiny $\mathbb{F} \cup \{\infty\}$.

Lemma 23. *Pro stabilizátory $L(\mathbb{F})_\infty$ a $L(\mathbb{F})_{\infty,0}$ platí, že $L(\mathbb{F})_\infty$ je ostře 2-tranzitivní a*

$$L(\mathbb{F})_\infty = \{ax + b \mid a \in \mathbb{F}^*,\, b \in \mathbb{F}\},\ L(\mathbb{F})_{\infty,0} = \{ax \mid a \in \mathbb{F}^*\}.$$

Důkaz. Přímým výpočtem dostaneme

$$L(\mathbb{F})_\infty = \left\{\frac{ax+b}{cx+d} \in L(\mathbb{F}) \mid \frac{a}{c} = \infty\right\} = \left\{\frac{ax+b}{cx+d} \in L(\mathbb{F}) \mid c = 0\right\} =$$
$$= \{a'x + b' \mid a' \in \mathbb{F}^*,\, b' \in \mathbb{F}\},$$

$$L(\mathbb{F})_{\infty,0} = \{a'x + b' \mid a' \in \mathbb{F}^*,\, b' = 0\} = \{a'x \mid a' \in \mathbb{F}^*\}.$$

Lemma 8 dává, že $L(\mathbb{F})_\infty$ je tranzitivní permutační grupa množiny $\mathbb{F}$, neboť pro každé $f \in \mathbb{F}$ existuje $L_f \in L(\mathbb{F})_\infty$, že $L_f(f) = 0$; můžeme položit $L_f = x + (-f)$.

Grupa $L(\mathbb{F})_{\infty,0}$ je stabilizátorem bodu 0 při působení $L(\mathbb{F})_\infty$ na $\mathbb{F}$. Jde o ostře tranzitivní permutační grupu množiny $\mathbb{F}^*$, neboť pro libovolná $f_1, f_2 \in \mathbb{F}^*$ platí

$$(f_2 f_1^{-1} x)(f_1) = f_2,$$

a naopak platí-li $ax(f_1) = f_2$, pak nutně $a = f_2 f_1^{-1}$. Z Důsledku 7 tedy dostáváme, že je ostře tranzitivní libovolný stabilizátor.

Ostrá 2-tranzitivita $L(\mathbb{F})_\infty$ nyní plyne z Lemmatu 5.

□

Tvrzení 24. *Grupa $L(\mathbb{F})$ je ostře 3-tranzitivní.*

Důkaz. Pro $f \in \mathbb{F} \cup \{\infty\}$ existuje $L_f \in L(\mathbb{F})$ takové, že $L_f(f) = 0$; pro $f \in \mathbb{F}$ to již bylo konstatováno v důkazu Lemmatu 23 a pro $f = \infty$ můžeme vzít $L_f = \frac{1}{x}$. Podle Lemmatu 8 je tudíž $L(\mathbb{F})$ tranzitivní.

Z Důsledku 7 a Lemmatu 23 plyne, že libovolný stabilizátor v $L(\mathbb{F})$ je ostře 2-tranzitivní.

$\Rightarrow$ Grupa $L(\mathbb{F})$ je ostře 3-tranzitivní díky Lemmatu 5.

□

2.3 Podgrupy podle pevných bodů

Jak vzápětí dokážeme, prvky $L(\mathbb{F})$, jejichž množiny pevných bodů se shodují, tvoří spolu s jednotkou podgrupu grupy $L(\mathbb{F})$. V této sekci se budeme zabývat vlastnostmi takových podgrup.

Tvrzení 25. *Bod f je pevným bodem prvku $\frac{ax+b}{cx+d} \in L(\mathbb{F})$ právě tehdy, když platí jedna z následujících podmínek:*

a) f je prvkem tělesa $\mathbb{F}$ a je kořenem polynomu $cx^2 + (d-a)x - b$,

b) $f = \infty$ a $c = 0$.

Důkaz. Nejprve předpokládejme, že $f \in \mathbb{F}$. Prvek $\frac{ax+b}{cx+d}$ fixuje bod f právě tehdy, když platí

$$\frac{af+b}{cf+d} = f.$$

To nastane, právě když

$$0 = cf^2 + (d-a)f - b.$$

Pokud $f = \infty$, z definice působení $L(\mathbb{F})$ na $\mathbb{F} \cup \{\infty\}$ ihned vidíme, že f je pevným bodem $\frac{ax+b}{cx+d}$ právě tehdy, když $c = 0$.

□

Věta 26. *Nechť $\alpha, \beta, \gamma \in \mathbb{F}$, $(\alpha,\beta,\gamma) \neq (0,0,0)$. Označme*

$$\hat{A} = \hat{A}_{\alpha,\beta,\gamma} =$$

$$= \left\{ \frac{ax+b}{cx+d} \in L(\mathbb{F}) \mid \exists \lambda \in \mathbb{F}^* \colon cx^2 + (d-a)x - b = \lambda(\alpha x^2 + \beta x + \gamma) \right\},$$

$$A = A_{\alpha,\beta,\gamma} = \hat{A} \cup \{x\}.$$

Dále definujme pro $t \in \mathbb{F}$:

$$L_t = \frac{tx - \gamma}{\alpha x + \beta + t}.$$

Množina A je podgrupou grupy $L(\mathbb{F})$ a platí

$$\hat{A} = \{L_t \mid t \in \mathbb{F},\, t^2 + \beta t + \alpha\gamma \neq 0\}.$$

Grupa A je izomorfní grupě $(S, *)$, kde $S = S_{\beta,\alpha\gamma} = \{t \in \mathbb{F} \mid t^2 + \beta t + \alpha\gamma \neq 0\} \cup \{\infty\}$ a operace $*$ je definovaná předpisem

$$s * t = \frac{st - \alpha\gamma}{s + t + \beta},\ s,t \in S,\ s,t \neq \infty,$$
$$s * \infty = \infty * s = s\ \forall s \in S.$$

Izomorfismus $\varphi\colon S \to A$ lze zvolit takto:

$$\varphi(t) = \begin{cases} L_t,\ \textit{pokud } t \in S,\ t \neq \infty, \\ x,\ \textit{pokud } f = \infty. \end{cases}$$

Důkaz. Platí

$$\hat{A} = \left\{ \frac{ax+b}{cx+d} \in L(\mathbb{F}) \mid \exists \lambda \in \mathbb{F}^*\colon c = \lambda\alpha,\, d - a = \lambda\beta,\, -b = \lambda\gamma \right\} =$$
$$= \left\{ \frac{ax - \lambda\gamma}{\lambda\alpha x + \lambda\beta + a} \mid \lambda \in \mathbb{F}^*,\, a(\lambda\beta + a) + \lambda^2\alpha\gamma \neq 0 \right\} =$$
$$= \left\{ \frac{\frac{a}{\lambda}x - \gamma}{\alpha x + \beta + \frac{a}{\lambda}} \mid \lambda \in \mathbb{F}^*,\, \frac{a}{\lambda}(\beta + \frac{a}{\lambda}) + \alpha\gamma \neq 0 \right\} =$$
$$= \left\{ \frac{tx - \gamma}{\alpha x + \beta + t} \mid t \in \mathbb{F},\, t(\beta + t) + \alpha\gamma \neq 0 \right\} = \{L_t \mid t \in \mathbb{F},\, t^2 + \beta t + \alpha\gamma \neq 0\}.$$

Odsud zároveň plyne i uzavřenost na $\circ$ a $^{-1}$. Pro prvky $L_s, L_t \in \hat{A}$ totiž dostáváme

$$L_s \circ L_t = \frac{(st - \alpha\gamma)x - \gamma(s + t + \beta)}{\alpha(s + t + \beta)x + \beta(s + t + \beta) + st - \alpha\gamma} =$$
$$= \begin{cases} \frac{\frac{st-\alpha\gamma}{s+t+\beta}x - \gamma}{\alpha x + \beta + \frac{st-\alpha\gamma}{s+t+\beta}},\ s + t + \beta \neq 0, \\ \frac{1x+0}{0x+1} = x,\ s + t + \beta = 0, \end{cases}$$
$$L_t^{-1} = \frac{-(\beta + t)x - \gamma}{\alpha x - t} = \frac{-(\beta + t)x - \gamma}{\alpha x + \beta + (-(\beta + t))},$$

v každém případě tedy $L_s \circ L_t, L_t^{-1} \in A$ (že $\frac{st-\alpha\gamma}{s+t+\beta}$ ani $-(\beta + t)$ nejsou kořeny polynomu $\lambda^2 + \beta\lambda + \alpha\gamma \in \mathbb{F}[\lambda]$ vyplývá z podmínky $ad - bc \neq 0\ \forall \frac{ax+b}{cx+d} \in L(\mathbb{F})$). Jednotka leží v A přímo z definice. Množina A je tedy uzavřená na grupové operace.

K důkazu poslední části tvrzení uvažujme zobrazení

$$\varphi\colon S \to A,\ \varphi(t) = \begin{cases} L_t, \text{ pokud } t \in S,\ t \neq \infty, \\ x, \text{ pokud } f = \infty. \end{cases}$$

Protože pro všechna $s,t \in S$ platí vztah

$$\varphi(s * t) = L_{s*t} = L_s \circ L_t = \varphi(s) \circ \varphi(t),$$

jde o homomorfismus. Množina S s operací $*$ je tedy skutečně grupa podle Tvrzení 4. Zobrazení φ je navíc zřejmě prosté i na, a tedy je izomorfismem mezi grupami S a A.

□

Definice 15. *Označme*

$$\mathcal{A}(\mathbb{F}) = \{A_{\alpha,\beta,\gamma} \mid \alpha,\beta,\gamma \in \mathbb{F},\ A_{\alpha,\beta,\gamma} \neq \{x\}\}$$

a dále pro $A \in \mathcal{A}(\mathbb{F})$,

$$\mathrm{Fix}(A) = \{f \in \mathbb{F} \cup \{\infty\} \mid L(f) = f\ \forall L \in A\},$$

$$\mathcal{A}_i(\mathbb{F}) = \{A \in \mathcal{A}(\mathbb{F}) \mid |\mathrm{Fix}(A)| = i\},$$

$i = 0,1,2$.

Z Tvrzení 25 plyne, že $\forall\ A \in \mathcal{A}(\mathbb{F})$ mají každé dva netriviální prvky grupy A stejné pevné body. Právě tyto body tvoří množinu $\mathrm{Fix}(A)$.

Protože je $L(\mathbb{F})$ ostře 3-tranzitivní, jediným prvkem fixujícím 3 a více bodů je jednotka. Každá grupa $A_{\alpha,\beta,\gamma}$ je netriviální, a tedy $|\mathrm{Fix}(A)| \leq 2\ \forall A \in \mathcal{A}(\mathbb{F})$. Odsud

$$\mathcal{A}(\mathbb{F}) = \mathcal{A}_0(\mathbb{F}) \cup \mathcal{A}_1(\mathbb{F}) \cup \mathcal{A}_2(\mathbb{F}).$$

Tvrzení 27. *Ať* $A \in \mathcal{A}_1(\mathbb{F}) \cup \mathcal{A}_2(\mathbb{F})$. *Potom* $L \in A \setminus \{x\}$, *právě když množina pevných bodů* L *je rovna* $\mathrm{Fix}(A)$.

Důkaz. Výše již bylo řečeno, že množiny pevných bodů dvou netriviálních prvků téže grupy $A \in \mathcal{A}(\mathbb{F})$ se shodují.

Nyní přistupme k opačné implikaci. Nechť má prvek $L \neq x$ pevné body e,f (může být i $e = f$). Víme, že $L \in A_{\alpha,\beta,\gamma}$ pro nějaká $\alpha,\beta,\gamma \in \mathbb{F}$. Podle Tvrzení 25 je ∞ pevným bodem L, právě když $\alpha = 0$, a element tělesa $\mathbb{F}$ je pevným bodem L, právě když je to kořen polynomu $\alpha x^2 + \beta x + \gamma$.

- Ať ∞ není pevným bodem L. Potom $\alpha \neq 0$. Platí tedy $\alpha x^2 + \beta x + \gamma = \alpha(x - e)(x - f)$, a tudíž $A_{\alpha,\beta,\gamma} = A_{1,-(e+f),ef}$.
- Ať ∞ je pevným bodem L. Pak $\alpha = 0$.

  Je-li ∞ jediným pevným bodem prvku L, nemá polynom $\beta x + \gamma$ kořen v $\mathbb{F}$, a tedy musí být $\beta = 0$, $\gamma \neq 0$. Tj. $L \in A_{0,0,1}$.

  Pokud je také $f \in \mathbb{F}$ pevným bodem L, je to kořen $\beta x + \gamma$. Tento polynom je nenulový, protože kdyby nebyl, pak $A_{\alpha,\beta,\gamma} = A_{0,0,0} = \{x\}$. Tedy $\beta x + \gamma = \beta(x - f)$, kde $\beta \neq 0$. Odsud $A_{\alpha,\beta,\gamma} = A_{0,1,-f}$.

Vidíme tedy, že grupa $A_{\alpha,\beta,\gamma}$ je jednoznačně určena pevnými body prvku L.

□

Lemma 28. *Grupa* $A = A_{\alpha,\beta,\gamma}$ *je tranzitivní permutační grupou na množině* $(\mathbb{F} \cup \{\infty\}) \setminus \mathrm{Fix}(A)$.

Důkaz. Uvažujme body $e, f \in (\mathbb{F} \cup \{\infty\}) \backslash \mathrm{Fix}(A)$. Pokud $e = f$, máme hotovo, neboť $x \in A$. Předpokládejme tedy, že $e \neq f$.

Každý netriviální prvek grupy A je tvaru $L_t = \frac{tx-\gamma}{\alpha x+\beta+t}$. Chceme-li, aby platilo $\frac{te-\gamma}{\alpha e+\beta+t} = f$, dostáváme

$$t = \frac{\alpha ef + \beta f + \gamma}{e - f}.$$

Zbývá ověřit, že pro takto definované t je L_t skutečně prvkem grupy A, tj. že $t^2 + \beta t + \alpha\gamma \neq 0$. To je ekvivalentní s podmínkou

$$(\alpha ef + \beta f + \gamma)^2 + \beta(\alpha ef + \beta f + \gamma)(e - f) + \alpha\gamma(e - f)^2 \neq 0.$$

Výraz na levé straně je roven $(\alpha e^2 + \beta e + \gamma)(\alpha f^2 + \beta f + \gamma)$, přičemž e ani f není kořenem polynomu $\alpha x^2 + \beta x + \gamma$ z definice množiny $\mathrm{Fix}(A)$. Máme tedy, co jsme chtěli.

□

2.3.1 Podgrupy s právě jedním pevným bodem

Tvrzení 29. *Nechť* $\mathrm{char}(\mathbb{F}) \neq 2$, $\alpha,\beta,\gamma \in \mathbb{F}$, $(\alpha,\beta,\gamma) \neq (0,0,0)$. *Pak*

$$|\mathrm{Fix}(A_{\alpha,\beta,\gamma})| = 1 \;\Leftrightarrow\; \beta^2 = 4\alpha\gamma.$$

Důkaz. Předpokládejme, že $\beta^2 = 4\alpha\gamma$. Mohou nastat dvě možnosti.

- $\alpha = 0$. Potom $\beta = 0$, a tedy $\gamma \neq 0$. Podle Tvrzení 25 platí $\mathrm{Fix}(A_{\alpha,\beta,\gamma}) = \{\infty\}$.
- $\alpha \neq 0$. Bez újmy na obecnosti nechť $\alpha = 1$. Existuje $\delta \in \mathbb{F}$ takové, že $\gamma = \alpha\gamma = \delta^2$, $\beta = 2\delta$. Pak $t^2 + \beta t + \gamma = (t + \delta)^2$. Z Tvrzení 25 tudíž plyne, že $\mathrm{Fix}(A_{\alpha,\beta,\gamma}) = \{-\delta\}$.

Odsud dostáváme i opačnou implikaci, neboť výše jsme získali všechny grupy $A_{\alpha,\beta,\gamma}$ takové, že $|\mathrm{Fix}(A_{\alpha,\beta,\gamma})| = 1$. Pro každou z těchto grup tedy platí $\beta^2 = 4\alpha\gamma$, jelikož trojice (α,β,γ), která danou grupu definuje, je určena jednoznačně až na nenulový násobek.

□

Jestliže má $\mathbb{F}$ charakteristiku 2, implikace $\Leftarrow$ obecně neplatí. Pokud však přidáme předpoklad, že $\mathbb{F}$ je perfektní, pak ano.

Tvrzení 30. *Nechť* $\mathbb{F}$ *je perfektní a* $(\alpha,\beta,\gamma) \neq (0,0,0)$. *Pak*

$$|\mathrm{Fix}(A_{\alpha,\beta,\gamma})| = 1 \;\Leftrightarrow\; \beta^2 = 4\alpha\gamma.$$

Důkaz. Případ, kdy $\mathrm{char}(\mathbb{F}) \neq 2$, byl již rozebrán v předchozím tvrzení.

Předpokládejme tedy $\mathrm{char}(\mathbb{F}) = 2$. Potom máme $4\alpha\gamma = 0$.

Pokud $|\mathrm{Fix}(A_{\alpha,\beta,\gamma})| = 1$, pak je buďto společným pevným bodem ∞, tj. $\alpha = 0 = \beta$ (neboť kdyby $\beta \neq 0$, dostali bychom $\beta^{-1}\gamma \in \mathrm{Fix}(A_{\alpha,\beta,\gamma})$), nebo je jím $\delta \in \mathbb{F}$

a $\alpha t^2 + \beta t + \gamma = \alpha(t+\delta)^2 = \alpha(t^2+\delta^2)$, tudíž opět $\beta = 0$. Rovnost $\beta^2 = 0$ je tak v obou případech splněna.

Buď $\beta^2 = 0$ (neboli $\beta = 0$). Jestliže také $\alpha = 0$, pak $\gamma \neq 0$ a $\mathrm{Fix}(A_{\alpha,\beta,\gamma}) = \{\infty\}$. Je-li $\alpha = 1$ (tj. $\alpha t^2 + \beta t + \gamma = t^2 + \gamma$), platí

$$\mathrm{Fix}(A_{\alpha,\beta,\gamma}) = \begin{cases} \{\delta\}, \text{ pokud existuje } \delta \in \mathbb{F} \text{ t. ž. } \delta^2 = -\gamma, \\ \emptyset, \text{ pokud takové } \delta \in \mathbb{F} \text{ neexistuje.} \end{cases}$$

Jestliže platí druhá možnost, je $x^2 + \gamma$ ireducibilní neseparabilní polynom. Takové polynomy však nad perfektním tělesem neexistují. Druhá možnost tedy nenastane.

□

Lemma 31. *Nechť je charakteristika tělesa $\mathbb{F}$ rovna lichému prvočíslu p, a $\beta^2 = 4\alpha\gamma$. Pak pro každé $L \in A_{\alpha,\beta,\gamma}$ platí $L^p = x$.*

Důkaz. Nejprve rozebereme případ, kdy $(\alpha,\beta,\gamma) = (0,0,1)$. Podle Tvrzení 25 máme

$$A_{0,0,1} = \left\{ \frac{tx-1}{t} \mid t^2 \neq 0 \right\} \cup \{x\} = \left\{ x - \frac{1}{t} \mid t \neq 0 \right\} \cup \{x\} = \{x + s \mid s \in \mathbb{F}\}.$$

Pro libovolné $s \in \mathbb{F}$ zřejmě platí $(x+s)^p = x + ps = x$.

Později (v Tvrzení 46) dokážeme, že každé dvě grupy splňující ekvivalentní podmínky z Tvrzení 29 jsou konjugované. Speciálně je tedy každá grupa $A_{\alpha,\beta,\gamma}$, kde $\beta^2 = 4\alpha\gamma$, konjugovaná s $A_{0,0,1}$, neboli pro $L \in A_{\alpha,\beta,\gamma}$ existují $K \in L(\mathbb{F})$ a $N \in A_{0,0,1}$ tak, že $L = KNK^{-1}$. Potom

$$L^p = (KNK^{-1})^p = KN^pK^{-1} = KxK^{-1} = x.$$

□

Tvrzení 32. *Nechť $|\mathbb{F}| < \infty$ a $A \in \mathcal{A}(\mathbb{F})$. Platí*

$$|A| = \begin{cases} |\mathbb{F}| + 1, \text{ pokud } A \in \mathcal{A}_0(\mathbb{F}), \\ |\mathbb{F}|, \text{ pokud } A \in \mathcal{A}_1(\mathbb{F}), \\ |\mathbb{F}| - 1, \text{ pokud } A \in \mathcal{A}_2(\mathbb{F}). \end{cases}$$

Důkaz. Podle Věty 26 platí pro $A = A_{\alpha,\beta,\gamma} \in \mathcal{A}(\mathbb{F})$:

$$|A| = |\{t \in \mathbb{F} \mid t^2 + \beta t + \alpha\gamma \neq 0\}| + 1.$$

Nejprve nechť $\infty \notin \mathrm{Fix}(A)$. Pak můžeme předpokládat, že $\alpha = 1$. Máme tedy, že

$$\alpha t^2 + \beta t + \gamma = t^2 + \beta t + \alpha\gamma,$$

tj. $t^2 + \beta t + \alpha\gamma = 0$, právě když $t \in \mathrm{Fix}(A)$. Odsud

$$|A| = \begin{cases} |\mathbb{F}| + 1, \text{ pokud } |\mathrm{Fix}(A)| = 0, \\ |\mathbb{F}|, \text{ pokud } |\mathrm{Fix}(A)| = 1, \\ |\mathbb{F}| - 1, \text{ pokud } |\mathrm{Fix}(A)| = 2. \end{cases}$$

Nyní ať $\infty \in \mathrm{Fix}(A)$, neboli $\alpha = 0$. Potom

$$t^2 + \beta t + \alpha\gamma = t(t + \beta),$$

a tudíž

$$|A| = \begin{cases} |\mathbb{F}|, \text{ pokud } \beta = 0, \\ |\mathbb{F}| - 1, \text{ pokud } \beta \neq 0. \end{cases}$$

Navíc zde platí, že $\beta \neq 0$, právě když $\mathrm{Fix}(A) = \{\infty, -\beta^{-1}\gamma\}$, a $\beta = 0$, právě když $\mathrm{Fix}(A) = \{\infty\}$.

Tím je důkaz proveden.

□

Tvrzení 33. *Nechť $|\mathbb{F}| < \infty$ a $\mathrm{char}(\mathbb{F}) = p \neq 2$. Pak prvky řádu p v $L(\mathbb{F})$ jsou právě prvky mající právě jeden pevný bod.*

Důkaz. Je-li $\mathbb{F}$ konečné těleso charakteristiky p, pak $|\mathbb{F}| = p^k$ a pro $A_{\alpha,\beta,\gamma} \in \mathcal{A}(\mathbb{F})$ platí, že $|A_{\alpha,\beta,\gamma}| \in \{|\mathbb{F}| - 1, |\mathbb{F}|, |\mathbb{F}| + 1\}$.

Pokud $|A_{\alpha,\beta,\gamma}| = |\mathbb{F}| \pm 1$, $A_{\alpha,\beta,\gamma}$ neobsahuje prvek řádu p, neboť p nedělí $p^k \pm 1$. Případ $|A_{\alpha,\beta,\gamma}| = |\mathbb{F}|$ nastává právě tehdy, když $t^2 + \beta t + \alpha\gamma$ má právě jeden kořen, tedy právě když $t^2 + \beta t + \alpha\gamma = (t + \delta)^2 = t^2 + 2\delta t + \delta^2$ pro nějaké $\delta \in \mathbb{F}$, neboli $\beta = 2\delta$, $\alpha\gamma = \delta^2$. To je ekvivalentní s $\beta^2 = 4\alpha\gamma$. Jestliže tedy $A_{\alpha,\beta,\gamma}$ obsahuje prvek řádu p, podle Tvrzení 29 musí být $|\mathrm{Fix}(A_{\alpha,\beta,\gamma})| = 1$.

Naopak, pokud $|\mathrm{Fix}(A_{\alpha,\beta,\gamma})| = 1$ (tj. $\beta^2 = 4\alpha\gamma$), je každý netriviální prvek grupy $A_{\alpha,\beta,\gamma}$ řádu p; to plyne z Lemmatu 31. Máme tedy, že každý prvek $L(\mathbb{F})$ s právě jedním pevným bodem je řádu p.

□

2.4 Disjunktní rozklady

Následující tvrzení dokládá, že množina všech netriviálních prvků grupy $L(\mathbb{F})$ je disjunktním sjednocením systému abelovských podgrup, z nichž z každé je vyjmuta jednotka. Připomeňme, že jednotku v $L(\mathbb{F})$ značíme x.

Tvrzení 34. *Pro každé $A \in \mathcal{A}(\mathbb{F})$ je A abelovská grupa regulární na množině $(\mathbb{F} \cup \{\infty\}) \setminus \mathrm{Fix}(A)$ a $L(\mathbb{F}) \setminus \{x\}$ lze zapsat jako* disjunktní *sjednocení*

$$L(\mathbb{F}) \setminus \{x\} = \bigcup_{A \in \mathcal{A}(\mathbb{F})} A \setminus \{x\}.$$

Důkaz. Mějme grupu $A \in \mathcal{A}(\mathbb{F})$.

Z Věty 26 dostáváme, že A je abelovská.

Pokud pro $L \in A$ a $f \in (\mathbb{F} \cup \{\infty\}) \setminus \mathrm{Fix}(A)$ je $L(f) = f$, pak $L \notin A \setminus \{x\}$, a tedy $L = x$. Libovolný stabilizátor bodu v A je tudíž triviální. Tranzitivitu A jsme dokázali v Lemmatu 28. Grupa A je tedy regulární.

Nechť $A = A_{\alpha,\beta,\gamma}$, $B = A_{\rho,\sigma,\tau}$ a $x \neq L \in A \cap B$, tj.

$$L = \frac{tx - \gamma}{\alpha x + \beta + t} = \frac{sx - \tau}{\rho x + \sigma + s}$$

pro nějaká s, t. Pak existuje $\lambda \in \mathbb{F}^*$ takové, že $t = \lambda s$, $\gamma = \lambda\tau$, $\alpha = \lambda\rho$, $\beta = \lambda\sigma$. Potom $\alpha x^2 + \beta x + \gamma = \lambda(\rho x^2 + \sigma x + \tau)$, takže podle Věty 26 máme $A = B$. Pro $A \neq B$ tudíž platí $A \cap B = \{x\}$.

□

Nyní se vraťme ke grupám $S_{\beta,\delta}$ z Věty 26.

Lemma 35. *Nechť β,$\delta \in \mathbb{F}$. Definujme polynomy $u_k(x), v_k(x) \in \mathbb{F}[x]$:*

$$u_1(x) = x,\ v_1(x) = 1,$$
$$u_k(x) = xu_{k-1}(x) - \delta v_{k-1}(x),$$
$$v_k(x) = u_{k-1}(x) + (x+\beta)v_{k-1}(x).$$

Potom pro každé $t \in \mathbb{F} \cap S_{\beta,\delta}$ a $k \geq 1$ platí $t^{[k]} = \frac{u_k(t)}{v_k(t)}$, kde $t^{[k]} =: \underbrace{t * \cdots * t}_{k\text{-krát}}$. Navíc $u_k(x)$ je monický polynom stupně k a $v_k(x)$ je polynom stupně nejvýše $k-1$.

Důkaz. Tvrzení dokážeme indukcí podle k.

Pro $k = 1$ máme

$$t^{[1]} = t = \frac{t}{1} = \frac{u_1(t)}{v_1(t)}.$$

Také vidíme, že $u_1(x) = x$ je monický polynom stupně 1 a $v_1(x) = 1$ je polynom stupně 0.

Nechť tvrzení platí pro $k \geq 1$. Pak dostáváme

$$t^{[k+1]} = t * t^{[k]} = \begin{cases} t * \frac{u_k(t)}{v_k(t)} = \frac{t\frac{u_k(t)}{v_k(t)} - \delta}{t + \frac{u_k(t)}{v_k(t)} + \beta} = \frac{tu_k(t) - \delta v_k(t)}{u_k(t) + (t+\beta)v_k(t)}, \text{ pokud } v_k(t) \neq 0, \\ t = \frac{tu_k(t) - \delta v_k(t)}{u_k(t) + (t+\beta)v_k(t)}, \text{ pokud } v_k(t) = 0 \text{ (tj. } t^{[k]} = \infty). \end{cases}$$

Navíc byl-li $u_k(x)$ monický polynom stupně k a $v_k(x)$ polynom stupně nejvýše $k-1$, je $u_{k+1}(x) = xu_k(x) - \delta v_k(x)$ monický polynom stupně $k+1$ a $v_{k+1}(x) = u_k(x) + (x+\beta)v_k(x)$ polynom stupně nejvýše k.

□

Poznámka. Polynom $v_k(x)$ je v některých případech možné určit rovnou, aniž bychom museli využívat rekurentního vzorce z Lemmatu 35:

Nechť β,$\delta \in \mathbb{F}$ a označme $p(x) = x^2 + \beta x + \delta$.

Předpokládejme, že β,δ jsou taková, že $p(x)$ nemá kořen v $\mathbb{F}$. Potom $S := S_{\beta,\delta} = \mathbb{F} \cup \{\infty\}$. Hodnoty β a δ určují násobení v grupě S a polynomy $u_k(x)$, $v_k(x)$. Přestože však figurují v rekurentních vztazích v Lemmatu 35, pro $k = |S| = |\mathbb{F}|+1$ na nich koeficienty polynomu $v_k(x)$ nezávisejí. Pak totiž $\forall t \in \mathbb{F}$ platí, že $\mathrm{ord}_S(t)$ dělí $|S|$, a tedy $t^{[|S|]} = \infty$. To podle Lemmatu 35 znamená, že $v_{|S|}(t) = 0\ \forall t \in \mathbb{F}$. Polynom $v_{|S|}(x)$ je stupně nejvýše $|S| - 1 = |\mathbb{F}|$, každé $t \in \mathbb{F}$ je tedy kořenem násobnosti 1 a dostáváme rozklad

$$v_{|S|}(x) = \prod_{t \in \mathbb{F}} (x - t).$$

Polynom $v_{|S|}(x)$ jsme tudíž schopni určit ihned, a to i bez znalosti β, δ.

Obdobně je možné spočítat koeficienty polynomu $v_{|S|}(x)$ i pro β, δ taková, že $p(x)$ není ireducibilní. V tomto případě je $|S| = |\mathbb{F}|$ (má-li $p(x)$ jeden dvojnásobný kořen) nebo $|S| = |\mathbb{F}| - 1$ (má-li $p(x)$ dva různé kořeny). Dostaneme

$$v_{|S|}(x) = \prod_{t \in \mathbb{F}:\ p(t) \neq 0} (x - t).$$

Polynom $v_{|S|}(x)$ tudíž závisí jen na kořenech $p(x)$. Hodnoty těchto kořenů jednoznačně určují β a δ a naopak. Opět tedy můžeme $v_{|S|}(x)$ určit rovnou. Ale zatímco výše nám k tomu stačilo vědět, že $p(x)$ je ireducibilní, zde musíme znát β a δ.

Lemma 36. *Buď $\mathbb{F}$ těleso prvočíselné charakteristiky p, $k \leq p$. Potom polynom $u_k(x)$, resp. $v_k(x)$, má koeficient u x^i roven $\binom{k}{i}\delta^u_{i,k}$, resp. $\binom{k}{i}\delta^v_{i,k}$, pro nějaká $\delta^u_{i,k}$,$\delta^v_{i,k} \in \mathbb{F}$, $i \in \{0,\ldots,k\}$.*

Speciálně tedy platí, že polynom $v_p(x)$ je konstantní.

Důkaz. Dokážeme silnější tvrzení, a sice že platí lemma a zároveň jsou pro každé $i \in \{1,\ldots,k\}$ splněny rovnosti

$$\delta^u_{i-1,k} = -\alpha\gamma\delta^v_{i,k},$$
$$\delta^u_{i,k} + \beta\delta^v_{i,k} = \delta^v_{i-1,k}.$$

Důkaz provedeme indukcí podle k.

Protože $u_1(x) = x = \binom{1}{1}\cdot 1\cdot x + \binom{1}{0}\cdot 0$, $v_1(x) = 1 = \binom{1}{1}\cdot 0\cdot x + \binom{1}{0}\cdot 1$, je vidno, že pro $k = 1$ naše tvrzení platí.

Nechť $k \geq 2$ a předpokládejme platnost pro $k-1$. Z rovnosti $u_k(x) = xu_{k-1}(x) - \alpha\gamma v_{k-1}(x)$ potom plyne, že koeficient $u_k(x)$ u x^i má tvar

$$\begin{aligned}
&\binom{k-1}{i-1}\delta^u_{i-1,k-1} - \alpha\gamma\binom{k-1}{i}\delta^v_{i,k-1} = \\
&= \binom{k-1}{i-1}(-\alpha\gamma)\delta^v_{i,k-1} - \alpha\gamma\binom{k-1}{i}\delta^v_{i,k-1} = \\
&= -\left(\binom{k-1}{i-1} + \binom{k-1}{i}\right)\alpha\gamma\delta^v_{i,k-1} = \binom{k}{i}(-\alpha\gamma\delta^v_{i,k-1}).
\end{aligned}$$

Podobně dostáváme z rovnosti $v_k(x) = u_{k-1}(x) + (x+\beta)v_{k-1}(x)$ a indukčního předpokladu tvar koeficientu $v_k(x)$ u x^i:

$$\begin{aligned}
&\binom{k-1}{i}\delta^u_{i,k-1} + \binom{k-1}{i-1}\delta^v_{i-1,k-1} + \beta\binom{k-1}{i}\delta^v_{i,k-1} = \\
&= \binom{k-1}{i}(\delta^u_{i,k-1} + \beta\delta^v_{i,k-1}) + \binom{k-1}{i-1}\delta^v_{i-1,k-1} = \\
&= \binom{k-1}{i}\delta^v_{i-1,k-1} + \binom{k-1}{i-1}\delta^v_{i-1,k-1} = \binom{k}{i}\delta^v_{i-1,k-1}.
\end{aligned}$$

Zároveň si všimněme, že tudíž platí

$$\delta^u_{i-1,k} = -\alpha\gamma\delta^v_{i-1,k-1} = -\alpha\gamma\delta^v_{i,k}$$

a také

$$\begin{aligned}
\delta^u_{i,k} + \beta\delta^v_{i,k} = -\alpha\gamma\delta^v_{i,k-1} + \beta\delta^v_{i-1,k-1} = \delta^u_{i-1,k-1} + \beta\delta^v_{i-1,k-1} = \\
= \delta^v_{i-2,k-1} = \delta^v_{i-1,k},
\end{aligned}$$

kde první a poslední rovnost plyne z předchozích výpočtů a druhá a třetí rovnost z indukčního předpokladu.

Polynom $v_p(x)$ je konstantní, neboť má stupeň nejvýše $p-1$, přičemž p dělí $\binom{p}{i}$ pro každé $i \in \{1,\dots,p-1\}$, takže koeficient $v_p(x)$ u x^i je nulový pro všechna $i \in \{1,\dots,p-1\}$.

□

Označme $v_k(0) = a_k$ pro $k \in \mathbb{N}$.

Lemma 37. *Buď $\mathbb{F}$ těleso charakteristiky $p > 2$. Pak pro $k \leq p$ platí*

$$a_k = \sum_{i=0}^{N_k} \binom{k-1-i}{i} \beta^{k-1-2i} (-\delta)^i,$$

kde $N_k = \begin{cases} \frac{k-2}{2} \text{ pro } k \text{ sudé,} \\ \frac{k-1}{2} \text{ pro } k \text{ liché.} \end{cases}$

Důkaz. Lemma dokážeme indukcí podle k.

Pro $k = 1, 2$ máme

$$\sum_{i=0}^{\frac{1-1}{2}} \binom{1-1-i}{i} \beta^{1-1-2i} (-\delta)^i = \binom{0}{0} \beta^0 (-\delta)^0 = 1 = a_1,$$
$$\sum_{i=0}^{\frac{2-2}{2}} \binom{2-1-i}{i} \beta^{2-1-2i} (-\delta)^i = \binom{1}{0} \beta^1 (-\delta)^0 = \beta = a_2.$$

Nyní nechť $k \geq 3$. Z definice polynomů $u_k(x)$, $v_k(x)$ lze vyvodit rekurentní předpis pro absolutní členy: $a_k = \beta a_{k-1} - \delta a_{k-2}$. Odsud a z indukčního předpokladu plyne

$$a_k = \beta \sum_{i=0}^{N_{k-1}} \binom{k-2-i}{i} \beta^{k-2-2i} (-\delta)^i - \delta \sum_{i=0}^{N_{k-2}} \binom{k-3-i}{i} \beta^{k-3-2i} (-\delta)^i.$$

Je-li k sudé (a tedy $k-1$ je liché a $k-2$ je sudé), pak $N_{k-1} = \frac{k-2}{2}$, $N_{k-2} = \frac{k-4}{2}$ a výraz výše je roven

$$\sum_{i=0}^{\frac{k-2}{2}} \binom{k-2-i}{i} \beta^{k-1-2i} (-\delta)^i + \sum_{i=0}^{\frac{k-4}{2}} \binom{k-3-i}{i} \beta^{k-3-2i} (-\delta)^{i+1} =$$
$$= \sum_{i=0}^{\frac{k-2}{2}} \binom{k-2-i}{i} \beta^{k-1-2i} (-\delta)^i + \sum_{i=1}^{\frac{k-2}{2}} \binom{k-2-i}{i-1} \beta^{k-1-2i} (-\delta)^i =$$
$$= \sum_{i=1}^{\frac{k-2}{2}} \left(\binom{k-2-i}{i} \beta^{k-1-2i} (-\delta)^i + \binom{k-2-i}{i-1} \beta^{k-1-2i} (-\delta)^i \right) +$$
$$+ \binom{k-2}{0} \beta^{k-1} = \sum_{i=0}^{\frac{k-2}{2}} \binom{k-1-i}{i} \beta^{k-1-2i} (-\delta)^i.$$

Poslední rovnost platí proto, že $\binom{k-2}{0} = 1 = \binom{k-1}{0} = \binom{k-1-0}{0}$.

V případě, že je k liché (tj. $k-1$ je sudé a $k-2$ je liché), máme $N_{k-1} = \frac{k-3}{2} = N_{k-2}$, a výraz je tedy roven

$$\sum_{i=0}^{\frac{k-3}{2}} \binom{k-2-i}{i} \beta^{k-1-2i}(-\delta)^i + \sum_{i=0}^{\frac{k-3}{2}} \binom{k-3-i}{i} \beta^{k-3-2i}(-\delta)^{i+1} =$$
$$= \sum_{i=0}^{\frac{k-3}{2}} \binom{k-2-i}{i} \beta^{k-1-2i}(-\delta)^i + \sum_{i=1}^{\frac{k-1}{2}} \binom{k-2-i}{i-1} \beta^{k-1-2i}(-\delta)^i =$$
$$= \binom{\frac{k-3}{2}}{\frac{k-3}{2}} \beta^0 (-\delta)^{\frac{k-1}{2}} + \sum_{i=1}^{\frac{k-3}{2}} \left(\binom{k-2-i}{i} + \binom{k-2-i}{i-1} \right) \beta^{k-1-2i}(-\delta)^i +$$
$$+ \binom{k-2}{0} \beta^{k-1} = \sum_{i=0}^{\frac{k-1}{2}} \binom{k-1-i}{i} \beta^{k-1-2i}(-\delta)^i,$$

neboť $\binom{\frac{k-3}{2}}{\frac{k-3}{2}} = 1 = \binom{\frac{k-1}{2}}{\frac{k-1}{2}} = \binom{k-1-\frac{k-1}{2}}{\frac{k-1}{2}}$.

□

Poznámka. Kombinační čísla $\binom{k-1-i}{i} = \frac{(k-1-i)!}{i!(k-1-2i)!}$ pro $i \in \{0, \ldots, k\}$ nad tělesem charakteristiky p můžeme v předchozím lemmatu uvažovat proto, že dle předpokladu je $k \leq p$ a $i \leq \left\lfloor \frac{k-1}{2} \right\rfloor$, a tudíž se ve výrazu $i!(k-1-2i)!$ vyskytují pouze čísla mezi 1 a $p-1$ (připomeňme, že $0! = 1$), tedy je nenulový a zlomek výše je dobře definován. Ze stejného důvodu je také korektní uvažovat kombinační čísla v Lemmatu 36.

Lemma 38. *Buď $\mathbb{F}$ těleso charakteristiky $p > 2$, $i \in \{0, \ldots, \frac{p-1}{2}\}$. Pak*

$$\binom{p-1-i}{i} = 4^i \binom{\frac{p-1}{2}}{i}.$$

Důkaz. Poznamenejme, že p je liché prvočíslo, a tedy $(-1)^{p-1} = 1$, a pišme

$$(p-1-i)! = (p-1-i)(p-1-i-1)\cdots(p-1-i-(p-2-i)) =$$
$$= (-1-i)(-2-i)\cdots(1-p) = (-1)^{p-1-i}(i+1)(i+2)\cdots(p-1) =$$
$$= (-1)^i \frac{(p-1)!}{i!},$$
$$(p-1-2i)! = (p-1-2i)(p-1-2i-1)\cdots(p-1-2i-(p-2-2i)) =$$
$$= (-1)^{p-1-2i}(1+2i)(2+2i)\cdots(p-1) = \frac{(p-1)!}{(2i)!},$$
$$(p-1)! = (p-1)(p-2)\cdots(p-\frac{p-1}{2})\frac{p-1}{2}\cdots 1 = (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}! \right) \right)^2,$$
$$\frac{p-1}{2}! = \frac{p-1}{2} \cdot \frac{p-3}{2} \cdots \frac{p-1-2(i-1)}{2} \cdot \left(\frac{p-1}{2} - i \right)! =$$
$$= 2^{-i}(-1)(-3)\cdots(2i-1) \left(\frac{p-1}{2} - i \right)! = (-2)^{-i}(2i-1)!! \left(\frac{p-1}{2} - i \right)!,$$
$$(2i)! = 2i(2i-2)\cdots 2(2i-1)(2i-3)\cdots 1 = 2^i i!(2i-1)!!.$$

Dohromady tedy

$$\binom{p-1-i}{i} = \frac{(p-1-i)!}{i!(p-1-2i)!} = \frac{(-1)^i(p-1)!(2i)!}{(p-1)!i!i!} = \frac{(-1)^i\frac{p-1}{2}!(2i)!}{\frac{p-1}{2}!i!i!} =$$
$$= \frac{(-1)^i\frac{p-1}{2}!2^i i!(2i-1)!!}{(-2)^{-i}(2i-1)!!\left(\frac{p-1}{2}-i\right)!i!i!} = 4^i\frac{\frac{p-1}{2}!}{\left(\frac{p-1}{2}-i\right)!i!} = 4^i\binom{\frac{p-1}{2}}{i}.$$

□

Lemma 39. *Buď $\mathbb{F}$ těleso charakteristiky p, $|S_{\beta,\delta}| > p$. Potom $v_p(x) = 0$ právě tehdy, když $\beta^2 = 4\delta$.*

Důkaz. Z Lemmatu 36 plyne, že nad tělesem charakteristiky p je polynom $v_p(x)$ konstantní, neboť p dělí $\binom{p}{i}$ pro každé $i \in \{1,\ldots,p-1\}$. Zbývá tedy určit, kdy je nulový absolutní člen a_p.

Pro $p > 2$ z Lemmat 37 a 38 ihned dostáváme, že

$$a_p = \sum_{i=0}^{\frac{p-1}{2}} \binom{p-1-i}{i} \beta^{p-1-2i}(-\delta)^i = \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i} (\beta^2)^{\frac{p-1}{2}-i}(-4\delta)^i =$$
$$= (\beta^2 - 4\delta)^{\frac{p-1}{2}}.$$

Poslední výraz je roven 0 právě tehdy, když $\beta^2 = 4\alpha\gamma$.

Nad tělesem charakteristiky 2 platí $v_2(x) = 2x + \beta = \beta$, tj. $v_2(x) = 0 \Leftrightarrow \beta = 0 \Leftrightarrow \beta^2 = 0$, přičemž $4\delta = 0$.

□

Lemma 40. *Je-li $\mathbb{F}$ těleso charakteristiky 0, pro každé $k \in \mathbb{N}$ existuje v grupě $(S_{\beta,\delta}, *)$ nejvýše k prvků t takových, že $t^{[k]} = \infty$. Je-li $\mathbb{F}$ těleso prvočíselné charakteristiky p, splňuje grupa $(S_{\beta,\delta}, *)$ tuto vlastnost právě tehdy, když $\beta^2 \neq 4\delta$ nebo $|S_{\beta,\delta}| \leq p$.*

Důkaz. Jak již bylo řečeno v důkazu Lemmatu 39, $t^{[k]} = \infty$ právě tehdy, když je t kořenem polynomu $v_k(x) \in \mathbb{F}[x]$.

Polynom $v_k(x)$ je stupně nejvýše $k-1$. Je-li tedy nenulový, má v tělese $\mathbb{F}$ maximálně $k-1$ kořenů. Rovnost $t^{[k]} = \infty$ tak splňuje nejvýše $k-1$ prvků $t \in \mathbb{F}$. Protože platí $\infty^{[k]} = \infty$, dohromady dostaneme, že existuje nejvýše k prvků $S_{\beta,\delta}$, jejichž k-tá mocnina je rovna ∞. Tj. jestliže je $v_k(x)$ nenulový, podmínka z lemmatu je pro dané k splněna.

Je-li charakteristika tělesa $\mathbb{F}$ nulová, x^{k-1} se ve $v_k(x)$ vyskytuje s koeficientem $k \neq 0$. Tedy $v_k(x) \neq 0$.

Nyní předpokládejme, že je charakteristika $\mathbb{F}$ rovna prvočíslu p.

V tomto případě máme nenulovost $v_k(x)$ zaručenou pro každé k, které není násobkem p, neboť vedoucí koeficient polynomu $v_k(x)$ je roven $k \bmod p$.

Z Lemmatu 39 víme, že pokud $\beta^2 = 4\delta$ a $|S_{\beta,\delta}| > p$, podmínka z tvrzení splněna není (neboť $t^{[p]} = \infty\ \forall t \in S_{\beta,\delta}$). Pokud $|S_{\beta,\delta}| \leq p$, je zřejmě splněna pro každé $k \geq p$. Je tedy splněna pro každé $k \in \mathbb{N}$, neboť pro $k < p$ je splněna vždy.

Nechť $\beta^2 \neq 4\delta$ a $t^{[kp^n]} = \infty$ pro $t \in S_{\beta,\delta}$, $n \in \mathbb{N}$, p nedělí k. Pak $t^{[kp^{n-1}]} = \infty$, neboť $\left(t^{[kp^{n-1}]}\right)^{[p]} = \infty$ a polynom $v_p(x)$ je konstantní a nenulový. Opakováním

této úvahy dostaneme $t^{[kp^{n-2}]} = t^{[kp^{n-3}]} = \cdots = t^{[k]} = \infty$. Prvků splňujících $t^{[k]} = \infty$ existuje nejvýše k, neboť p nedělí k. Tedy existuje maximálně $k < kp^n$ prvků takových, že $t^{[kp^n]} = \infty$.

□

Tvrzení 41. *Platí-li jedna z následujících podmínek, je každá konečná podgrupa grupy $A_{\alpha,\beta,\gamma} \in \mathcal{A}(\mathbb{F})$ cyklická:*

a) $\mathbb{F}$ je těleso charakteristiky 0,

b) $\mathbb{F}$ je těleso prvočíselné charakteristiky p a $\beta^2 \neq 4\alpha\gamma$ nebo $|\mathbb{F}| = p$.

Důkaz. Protože $A_{\alpha,\beta,\gamma} \simeq S_{\beta,\alpha\gamma} = S$, stačí dokázat, že je cyklická každá konečná podgrupa grupy S.

Operace $*$ je komutativní, z klasifikace konečných abelovských grup tedy víme, že konečná podgrupa S' grupy S je izomorfní $\mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}$ pro nějaká $m \geq 0$, $k_i \geq 1$ a prvočísla p_i.

Je-li $|\mathbb{F}| = p$ a $\beta^2 = 4\alpha\gamma$, Věta 26 dává, že $|A_{\alpha,\beta,\gamma}| = p$. Z Lemmatu 40 tedy plyne, že pokud platí a) nebo b), jsou prvočísla p_i po dvou různá. Kdyby totiž $p_i = p_j$ pro $i \neq j$, pak by $\mathbb{Z}_{p_i^{k_i}} \times \mathbb{Z}_{p_j^{k_j}}$ obsahovala $p_i^{k_i+k_j}$ prvků, jejichž řád dělí $p_i^{\max\{k_i,k_j\}}$. Ale $p_i^{k_i+k_j} > p_i^{\max\{k_i,k_j\}}$, dostáváme tedy spor s Lemmatem 40, neboť grupa $\mathbb{Z}_{p_i^{k_i}} \times \mathbb{Z}_{p_j^{k_j}}$ je izomorfní nějaké podgrupě grupy S. Grupa S' je tedy cyklická, neboť je izomorfní $\mathbb{Z}_{p_1^{k_1} \ldots p_m^{k_m}}$.

Cykličnost S' lze pomocí Lemmatu 40 dokázat též bez znalosti oné klasifikace, viz [3, sekce 16.2].

□

Nyní můžeme dokázat následující důsledek, který je rozšířením Tvrzení 34.

Důsledek 42. *Předpokládejme, že je $L(\mathbb{F})$ konečná. Pak jsou následující dvě tvrzení ekvivalentní:*

1) Grupu $L(\mathbb{F})$ lze zapsat jako sjednocení

$$L(\mathbb{F}) = \bigcup_{A \in \mathcal{A}(\mathbb{F})} A,$$

kde pro každé $A \in \mathcal{A}(\mathbb{F})$ je A cyklická *grupa regulární na množině $(\mathbb{F} \cup \{\infty\}) \setminus \mathrm{Fix}(A)$, a pro $A, B \in \mathcal{A}(\mathbb{F})$ taková, že $A \neq B$, platí $A \cap B = \{x\}$,*

2) $\mathbb{F} = \mathbb{Z}_p$ pro nějaké prvočíslo p.

Důkaz. Má-li $\mathbb{F}$ charakteristiku 0, obsahuje $\mathbb{Z}$ jako podobor, a tedy je nekonečné. Grupa $L(\mathbb{F})$ je tudíž také nekonečná, neboť v ní leží každý z prvků nekonečné množiny $\left\{ax = \frac{ax+0}{0x+1} \mid a \in \mathbb{F}^*\right\}$. Je-li tedy $L(\mathbb{F})$ konečná, charakteristika $\mathbb{F}$ musí být rovna nějakému prvočíslu p.

Za předpokladu konečnosti $L(\mathbb{F})$ nám Tvrzení 41 zaručuje cykličnost těch grup $A_{\alpha,\beta,\gamma}$, kde $\beta^2 \neq 4\alpha\gamma$.

Nechť platí 1). Jestliže $\beta^2 = \alpha\gamma$, podle Věty 26 je $|A_{\alpha,\beta,\gamma}| = |\mathbb{F}|$ (jako v důkazu Tvrzení 33). Pro spor nechť $|A_{\alpha,\beta,\gamma}| > p$. Z Důsledku 39 víme, že $v_p(x) = 0$, tj. $t^p = \infty\ \forall t \in A_{\alpha,\beta,\gamma}$. Pokud tedy $|\mathbb{F}| = |A_{\alpha,\beta,\gamma}| > p$, žádný z prvků $A_{\alpha,\beta,\gamma}$ celou grupu nenageneruje, neboli není cyklická. Musí tudíž být $|\mathbb{F}| \leq p$. Protože velikost

tělesa charakteristiky p je rovna nenulové mocnině p, dostáváme $|\mathbb{F}| = p$, tedy $\mathbb{F} = \mathbb{Z}_p$.

Naopak, jestliže $\mathbb{F} = \mathbb{Z}_p$, pak $|\mathbb{F}| = p$. Každá grupa $A_{\alpha,\beta,\gamma}$ splňuje $\beta^2 \neq 4\alpha\gamma$ nebo $|A_{\alpha,\beta,\gamma}| = p$. Z Tvrzení 34 a Tvrzení 41 tedy vyplývá, že podmínka 1) platí. □

Definice 16. *Předpokládejme, že $|\mathbb{F}| < \infty$. Singerův cyklus v $L(\mathbb{F})$ je regulární cyklická podgrupa grupy $L(\mathbb{F})$, jejíž každý netriviální prvek nemá pevný bod.*

Tvrzení 43. *Nechť $|\mathbb{F}| = q < \infty$. Platí $\mathcal{A}_0(\mathbb{F}) \neq \emptyset$. Přesněji řečeno, máme, že*

$$|\mathcal{A}_0(\mathbb{F})| = \frac{q(q-1)}{2}.$$

Speciálně tedy v $L(\mathbb{F})$ existuje Singerův cyklus.

Důkaz. Z Tvrzení 34 dostáváme, že

$$|L(\mathbb{F}) \setminus \{x\}| = \left|\bigcup_{A\in\mathcal{A}_2(\mathbb{F})} A \setminus \{x\}\right| + \left|\bigcup_{A\in\mathcal{A}_1(\mathbb{F})} A \setminus \{x\}\right| + \left|\bigcup_{A\in\mathcal{A}_0(\mathbb{F})} A \setminus \{x\}\right|.$$

Grupa $L(\mathbb{F})$ je ostře 3-tranzitivní, takže každý z jejích prvků je jednoznačně určen svými hodnotami na libovolné trojici bodů. Z toho vyplývá, že

$$|L(\mathbb{F})| = (q+1)q(q-1),$$

tj. $|L(\mathbb{F}) \setminus \{x\}| = (q+1)q(q-1) - 1$.

Snadno lze také nahlédnout, že $|\mathcal{A}_1(\mathbb{F})| = |\mathbb{F} \cup \{\infty\}| = q+1$ a $|\mathcal{A}_2(\mathbb{F})| = \binom{q+1}{2} = \frac{(q+1)q}{2}$. Za použití Tvrzení 32 tudíž obdržíme

$$\left|\bigcup_{A\in\mathcal{A}_1(\mathbb{F})} A \setminus \{x\}\right| = (q+1)(q-1), \quad \left|\bigcup_{A\in\mathcal{A}_2(\mathbb{F})} A \setminus \{x\}\right| = \frac{(q+1)q(q-2)}{2}.$$

Dostáváme tedy

$$\left|\bigcup_{A\in\mathcal{A}_0(\mathbb{F})} A \setminus \{x\}\right| = (q+1)q(q-1) - 1 - (q+1)(q-1) - \frac{(q+1)q(q-2)}{2} =$$

$$= \frac{q^2(q-1)}{2}.$$

Podle Tvrzení 32 je $|A \setminus \{x\}| = q$ pro $A \in \mathcal{A}_0(\mathbb{F})$, takže z předchozího výpočtu plyne, že $|\mathcal{A}_0(\mathbb{F})| = \frac{q(q-1)}{2}$.

Z Tvrzení 34 víme, že každá grupa $A \in \mathcal{A}_0(\mathbb{F})$ je regulární. Těleso $\mathbb{F}$ je konečné, tedy je perfektní. Podle Tvrzení 30 a 41 je tudíž každá $A \in \mathcal{A}_0(\mathbb{F})$ cyklická. Je to tedy Singerův cyklus.

□

Poznámka. Rovnost $|\mathcal{A}_0(\mathbb{F})| = \frac{q(q-1)}{2}$ lze dokázat i následovně.

Grupa $A = A_{\alpha,\beta,\gamma}$ je bez pevného bodu (tj. $A \in \mathcal{A}_0(\mathbb{F})$), právě když $\alpha \neq 0$ a polynom $\alpha t^2 + \beta t + \gamma$ nemá kořen v $\mathbb{F}$. Pro $(\beta,\gamma) \neq (\sigma,\tau)$ dostáváme dvě různé grupy $A_{1,\beta,\gamma}$ a $A_{1,\sigma,\tau}$. Velikost množiny $\mathcal{A}_0(\mathbb{F})$ je tedy rovna počtu ireducibilních monických polynomů stupně 2 nad $\mathbb{F}$. Monických polynomů stupně 2 nad $\mathbb{F}$ (tj. polynomů tvaru $t^2 + \beta t + \gamma$, kde $\beta,\gamma \in \mathbb{F}$) je q^2. Z toho je reducibilních právě tolik, kolik existuje výrazů typu $(t-e)(t-f)$ pro $e,f \in \mathbb{F}$. Takových výrazů je $\frac{q(q-1)}{2} + q = \frac{q(q+1)}{2}$. Neboli, $|\mathcal{A}_0(\mathbb{F})| = q^2 - \frac{q(q+1)}{2} = \frac{q(q-1)}{2}$.

2.5 Působení konjugací

Grupa $L(\mathbb{F})$ působí konjugací na množině všech svých podgrup. V Tvrzení 45 dokážeme, že $\mathcal{A}(\mathbb{F})$ je orbitou tohoto působení, a tedy $L(\mathbb{F})$ působí konjugací na $\mathcal{A}(\mathbb{F})$.

Pro zjednodušení notace budeme pro L,$K \in L(\mathbb{F})$ psát pouze LK místo $L \circ K$.

Lemma 44. *Mějme $N = ax + b \in L(\mathbb{F})_\infty$ a $A = A_{1,\beta,\gamma} \in \mathcal{A}(\mathbb{F})$. Pak platí*

$$NAN^{-1} = A_{1,\mu,\nu},$$

kde $\mu = a\beta - 2b$, $\nu = b^2 + a^2\gamma - ab\beta$.

Důkaz. Buď $L \in A$ netriviální. Máme, že $L = \frac{tx-\gamma}{x+\beta+t}$ pro nějaké $t \in \mathbb{F}$. Potom

$$NLN^{-1} = (ax+b)\left(\frac{tx-\gamma}{x+\beta+t}\right)(a^{-1}x - a^{-1}b) =$$
$$= \frac{(at+b)x - b(at+b) - a^2\gamma + ab(\beta+t)}{x - b + a(\beta+t)} = \frac{(at+b)x - (b^2 + a^2\gamma - ab\beta)}{x + (a\beta - 2b) + (at+b)}.$$

Vidíme tedy, že $NLN^{-1} = \frac{sx-\nu}{x+\mu+s}$ pro

$$s = at + b,\ \mu = a\beta - 2b,\ \nu = b^2 + a^2\gamma - ab\beta.$$

Protože výše uvedené vztahy pro μ a ν závisí pouze na hodnotách β, γ, a, b (nikoliv na t), platí $NKN^{-1} \in A_{1,\mu,\nu}$ pro každé $K \in A$. Tedy $NAN^{-1} \subset A_{1,\mu,\nu}$.

Zároveň platí i inkluze $A_{1,\mu,\nu} \subset NAN^{-1}$, neboť libovolný prvek $\frac{sx-\nu}{x+\mu+s}$ dostaneme jako NMN^{-1} volbou $t = \frac{s-b}{a}$ (kdyby $a = 0$, platilo by $a \cdot 1 - b \cdot 0 = 0 - 0 = 0$ a N by tudíž nebyl prvkem $L(\mathbb{F})$).

Dohromady $NAN^{-1} = A_{1,\mu,\nu}$.

□

Tvrzení 45. *Grupa $L(\mathbb{F})$ působí konjugací na množině $\mathcal{A}(\mathbb{F})$. Speciálně působí konjugací na každé z množin $\mathcal{A}_i(\mathbb{F})$, $i = 0,1,2$.*

Důkaz. Potřebujeme ukázat, že je-li $A = A_{\alpha,\beta,\gamma} \in \mathcal{A}(\mathbb{F})$ a $L \in L(\mathbb{F})$, pak $LAL^{-1} \in \mathcal{A}(\mathbb{F})$.

Nejprve nechť $|\mathrm{Fix}(A)| > 0$. Uvažujme $K \in LAL^{-1}$. Pak $K = LML^{-1}$ pro nějaké $M \in A$. Zřejmě platí, že $f \in \mathbb{F} \cup \{\infty\}$ je pevným bodem M, právě když je $L(f)$ pevným bodem K. Neboli, LAL^{-1} je rovna grupě $B \in \mathcal{A}(\mathbb{F})$ takové, že $\mathrm{Fix}(B) = L(\mathrm{Fix}(A))$.

V případě, kdy $|\mathrm{Fix}(A)| = 0$, předchozí argument nefunguje, neboť dva různé prvky bez pevného bodu ještě nemusí ležet v téže grupě z $\mathcal{A}(\mathbb{F})$. Buď tedy $|\mathrm{Fix}(A)| = 0$. Protože $\infty \in \mathrm{Fix}(A) \Leftrightarrow \alpha = 0$, platí $\alpha \neq 0$. Můžeme tedy bez újmy na obecnosti předpokládat, že $\alpha = 1$. Podle Lemmatu 10 existuje $N \in L(\mathbb{F})_\infty$ takové, že $LAL^{-1} = NAN^{-1}$, neboť A je tranzitivní na množině $\mathbb{F} \cup \{\infty\}$ (plyne z Lemmatu 28 a z toho, že $|\mathrm{Fix}(A)| = 0$). Lemma 44 pak dává, že $LAL^{-1} = NAN^{-1} = A_{1,\mu,\nu} \in \mathcal{A}(\mathbb{F})$.

První část tvrzení tedy platí. Zbytek pak plyne z Lemmatu 9.

□

Tvrzení 46. *Uvažujme grupy* $A = A_{\alpha,\beta,\gamma}$, $B = A_{\rho,\sigma,\tau}$. *Platí-li* $|\mathrm{Fix}(A)| = 1 = |\mathrm{Fix}(B)|$ *nebo* $|\mathrm{Fix}(A)| = 2 = |\mathrm{Fix}(B)|$, *pak jsou grupy* A *a* B *konjugované.*

Důkaz.

- $|\mathrm{Fix}(A)| = 2$:

  Netriviální prvek $L(\mathbb{F})$ může mít nejvýše dva pevné body. Každý prvek $L(\mathbb{F})$, který stabilizuje e i f, má tedy buďto právě dva pevné body, nebo jde o jednotku. Čili je A rovna stabilizátoru $L(\mathbb{F})_{e,f} = \{L \in L(\mathbb{F}) \mid L(e) = e,\ L(f) = f\}$ bodů e, f. Podobně je i B rovna stabilizátoru nějakých dvou bodů.

  Grupa $L(\mathbb{F})$ je 3-tranzitivní, je tedy také 2-tranzitivní. Lemma 6 tudíž dává, že každé dva stabilizátory dvou bodů jsou konjugované.

- $|\mathrm{Fix}(A)| = 1$:

  Označme $\mathrm{Fix}(A) = \{e\}$, $\mathrm{Fix}(B) = \{f\}$. Grupa A je zřejmě obsažena ve stabilizátoru $L(\mathbb{F})_e$ bodu e a B je obsažena ve stabilizátoru $L(\mathbb{F})_f$ bodu f. Grupa $L(\mathbb{F})$ je 3-tranzitivní, tedy je tranzitivní a z Lemmatu 6 plyne, že každé dva stabilizátory bodu jsou konjugované, tj. že existuje $L \in L(\mathbb{F})$ takové, že $L(\mathbb{F})_f = LL(\mathbb{F})_e L^{-1}$.

  Podle Lemmatu 9 konjugace zachovává počet pevných bodů, takže každý netriviální prvek grupy $LAL^{-1} \subset LL(\mathbb{F})_e L^{-1} = L(\mathbb{F})_f$ má pevný bod právě jeden. Všechny prvky $L(\mathbb{F})_f$, které mají právě jeden pevný bod, jsou obsaženy v B, tudíž $LAL^{-1} \subset B$.

  Naopak, pro každé $N \in B$ existuje $M \in L(\mathbb{F})_e$, že $N = LML^{-1}$. Toto M nutně leží v A, opět díky Lemmatu 9 a skutečnosti, že všechny prvky $L(\mathbb{F})_e$, které mají právě jeden pevný bod, jsou obsaženy v A. Tj. $B \subset LAL^{-1}$.

  Dohromady $B = LAL^{-1}$.

□

Dokážeme, že podobné tvrzení platí i pro případ, kdy $|\mathrm{Fix}(A)| = 0 = |\mathrm{Fix}(B)|$. Potřebujeme k tomu ale ještě jedno pomocné lemma.

Lemma 47. *Buď* $\mathrm{char}(\mathbb{F}) \neq 2$ *a nechť* $\mathbb{F}[\delta]$, *kde* $\delta^2 \in \mathbb{F}$, *je rozkladové nadtěleso polynomu* $x^2 + \beta x + \gamma \in \mathbb{F}[x]$ *ireducibilního nad* $\mathbb{F}$. *Pak platí, že grupy* $A_{1,\beta,\gamma}$ *a* $A_{1,0,-\delta^2}$ *jsou konjugované.*

Důkaz. Poznamenejme, že podle Lemmatu 15 skutečně takové $\delta \in \mathbb{F}$ existuje, neboť rozkladové nadtěleso polynomu $x^2 + \beta x + \gamma$ je rozšířením $\mathbb{F}$ stupně 2.

Řešme nad $\mathbb{F}$ soustavu rovnic o neznámých a, b:

$$\begin{aligned} 0 &= a\beta - 2b, \\ -\delta^2 &= b^2 + a^2\gamma - ab\beta. \end{aligned}$$

Dostáváme $b = \frac{a\beta}{2}$, $a^2 = \frac{-\delta^2}{\gamma - \frac{\beta^2}{4}}$. Abychom nahlédli, že takové a v $\mathbb{F}$ skutečně existuje, podíváme se blíže na hodnoty β, γ.

Polynom $x^2+\beta x+\gamma$ má kořeny $e+f\delta$, $g+h\delta$ pro nějaká e, f, g, $h \in \mathbb{F}$, tj.

$$x^2+\beta x+\gamma = (x-(e+f\delta))(x-(g+h\delta)) = \\ = x^2+(e+g+(f+h)\delta)x+(eg+(ef+gh)\delta+fh\delta^2).$$

Protože β, γ, $\delta^2 \in \mathbb{F}$ a $\delta \notin \mathbb{F}$, musí být $-f=h$, $ef=-gh$. Odsud pak $ef=gf$. Zkoumaný polynom nemá kořen v $\mathbb{F}$, tudíž $f \neq 0$, a tedy $e=g$. Nyní vidíme, že $\beta=2e$, $\gamma=e^2-f^2\delta^2$.

$\Rightarrow$ Máme $a^2=\frac{-\delta^2}{e^2-f^2\delta^2-\frac{4e^2}{4}}=f^{-2} \Rightarrow a=\pm f^{-1}$.

$\Rightarrow \; NA_{1,\beta,\gamma}N^{-1}=A_{1,0,-\delta^2}$ pro $N=\pm\left(f^{-1}x+\frac{\beta}{2f}\right)$.

□

Lemma 48. *Označme $A=A_{1,\beta,\gamma}$, $B=A_{1,\sigma,\tau}$. Nechť platí $|\mathrm{Fix}(A)|=0=|\mathrm{Fix}(B)|$. Jsou-li grupy A a B konjugované, mají polynomy $p(x)=x^2+\beta x+\gamma$ a $q(x)=x^2+\sigma x+\tau$ rozkladová nadtělesa, která jsou F-izomorfní.*

Důkaz. Tvrzení 25 a rovnost $|\mathrm{Fix}(A)|=0=|\mathrm{Fix}(B)|$ dávají, že $p(x)$ i $q(x)$ jsou ireducibilní nad $\mathbb{F}$.

Předpokládejme, že rozkladová nadtělesa polynomů $p(x)$ a $q(x)$ $\mathbb{F}$-izomorfní nejsou a nechť $K=NLN^{-1}$ pro $K \in B$, $L \in A$, $N \in L(\mathbb{F})$. Označme $\mathbb{G}$ rozkladové nadtěleso polynomu $p(x)$. Grupa $L(\mathbb{F})$ působí na $\mathbb{G}\cup\{\infty\}$ jako podgrupa $L(\mathbb{G})$, přičemž $\mathbb{F}\cup\{\infty\}$ je jednou z orbit tohoto působení a zúžení na tuto orbitu se shoduje s kanonickým působením $L(\mathbb{F})$. Prvky K, L, N lze tedy chápat jako elementy grupy $L(\mathbb{G})$.

Ať K má jako prvek $L(\mathbb{G})$ pevný bod. Onen bod je pak podle Tvrzení 25 kořenem polynomu $q(x)$. Tento polynom se tudíž v $\mathbb{G}[x]$ rozkládá na součin lineárních činitelů, tj. má rozkladové nadtěleso $\mathbb{G}_0$, které je obsaženo v tělese $\mathbb{G}$. Obě tělesa $\mathbb{G}_0$ a $\mathbb{G}$ jsou kvadratickými rozšířeními $\mathbb{F}$, neboť jde o rozkladová nadtělesa ireducibilních polynomů stupně 2. Odsud $\mathbb{G}_0=\mathbb{G}$, což je ve sporu s předpokladem, že rozkladová nadtělesa $p(x)$ a $q(x)$ nejsou $\mathbb{F}$-izomorfní. Prvek K tedy nemá pevný bod v $\mathbb{G}\cup\{\infty\}$.

Ale L jako prvek $L(\mathbb{G})$ pevný bod má, jelikož $p(x)$ má kořen v $\mathbb{G}$. Při tom rovnost $K=NLN^{-1}$ platí i v $L(\mathbb{G})$. Dostáváme tak spor s Lemmatem 9.

Grupy A a B tedy nejsou konjugované.

□

Věta 49. *Nechť $\mathrm{char}(\mathbb{F}) \neq 2$. Uvažujme grupy $A=A_{\alpha,\beta,\gamma}$, $B=A_{\rho,\sigma,\tau}$. Jestliže $|\mathrm{Fix}(A)|=0=|\mathrm{Fix}(B)|$, pak jsou ekvivalentní následující dvě podmínky:*

1) A a B jsou konjugované,

2) polynomy $\alpha x^2+\beta x+\gamma$ a $\rho x^2+\sigma x+\tau$ mají $\mathbb{F}$-izomorfní rozkladová nadtělesa.

Důkaz. Z podmínky $|\mathrm{Fix}(A)|=0=|\mathrm{Fix}(B)|$ plyne, že jsou oba polynomy ireducibilní nad $\mathbb{F}$. Proto můžeme předpokládat, že $\alpha=1=\rho$.

Nechť jsou rozkladová nadtělesa polynomů $x^2+\beta x+\gamma$ a $x^2+\sigma x+\tau$ $\mathbb{F}$-izomorfní $\mathbb{F}[\delta]$, kde $\delta^2 \in \mathbb{F}$. Z Lemmatu 15 víme, že takové $\delta \in \overline{\mathbb{F}}$ existuje. Lemma 47 dává, že existují $M, N \in L(\mathbb{F})$ splňující $MAM^{-1}=A_{1,0,-\delta^2}=NBN^{-1}$. Potom $(N^{-1}M)A(N^{-1}M)^{-1}=B$, tj. A a B jsou konjugované.

Opačná implikace je obsažena v Lemmatu 48.

□

Tvrzení 50. *Počet tříd konjugace ve Větě 49 je*

$$[\mathbb{F}^*\colon (\mathbb{F}^*)^2] - 1,$$

kde $(\mathbb{F}^*)^2 = \{c^2 \mid c \in \mathbb{F}^*\}$.

Důkaz. Na rozkladové nadtěleso libovolného polynomu $p(x) \in \mathbb{F}[x]$ stupně 2 můžeme nahlížet jako na rozkladové nadtěleso polynomu $x^2 - a \in \mathbb{F}[x]$. Je-li $p(x)$ ireducibilní, plyne tento fakt z Lemmatu 15. Je-li reducibilní, je jeho rozkladovým nadtělesem $\mathbb{F}$, které lze chápat jako rozkladové nadtěleso polynomu $x^2 - c^2$, kde $c \in \mathbb{F}$.

Nechť a,$b \in \mathbb{F}^*$. Podle Lemmatu 18 mají polynomy $x^2 - a$ a $x^2 - b$ $\mathbb{F}$-izomorfní rozkladová nadtělesa právě tehdy, když a a b reprezentují tutéž rozkladovou třídu grupy $(\mathbb{F}^*,\cdot)$ podle $(\mathbb{F}^*)^2$. Těchto rozkladových tříd je $[\mathbb{F}^*\colon (\mathbb{F}^*)^2]$. Počet tříd konjugace ve Větě 49 je tedy skutečně $[\mathbb{F}^*\colon (F^*)^2] - 1$. Jedničku odečítáme proto, že vylučujeme případ, kdy společným rozkladovým nadtělesem je $\mathbb{F}$, neboli kdy jde o reducibilní polynomy. Polynomy z Věty 49 jsou totiž právě všechny ireducibilní polynomy v $\mathbb{F}[x]$ stupně 2, neboť $|\mathrm{Fix}(A_{1,\beta,\gamma})| = 0 \Leftrightarrow x^2 + \beta x + \gamma$ nemá kořen v $\mathbb{F}$.

Poznamenejme ještě, že $(\mathbb{F}^*)^2$ je podgrupou $\mathbb{F}^*$ (a tedy je korektní uvažovat $[\mathbb{F}^*\colon (\mathbb{F}^*)^2]$). Zřejmě totiž $\forall c,d \in \mathbb{F}^*$ platí

$$1 = 1^2 \in (\mathbb{F}^*)^2,\ (c^2)^{-1} = (c^{-1})^2 \in (\mathbb{F}^*)^2,\ c^2d^2 = (cd)^2 \in (\mathbb{F}^*)^2.$$

□

Nad tělesem charakteristiky různé od 2 má každý ireducibilní polynom $p(x) \in \mathbb{F}[x]$ ve svém rozkladovém nadtělese dva různé kořeny, neboť kdyby pro $\delta \in \overline{\mathbb{F}}$ platilo $p(x) = (x+\delta)^2 = x^2 + 2\delta x + \delta^2$, měli bychom $2\delta \in \mathbb{F}$, a tedy $\delta \in \mathbb{F}$ (neboť $2 \neq 0$), což je spor s ireducibilitou $p(x)$. Nad tělesem charakteristiky 2 je situace jiná, jelikož vždy $2\delta = 0$.

Věta 49 nicméně platí i pro $\mathrm{char}(\mathbb{F}) = 2$. K důkazu ale bude potřeba dalších několik lemmat.

Lemma 51. *Předpokládejme, že* $\mathrm{char}(\mathbb{F}) = 2$. *Nechť* $p(x) = x^2 + \beta x + \gamma \in \mathbb{F}[x]$ *je ireducibilní polynom, který má v* $\overline{\mathbb{F}}$ *dva různé kořeny. Pak je grupa* $A_{1,\beta,\gamma}$ *konjugovaná s* $A_{1,1,\frac{\gamma}{\beta^2}}$. *Navíc platí* $\gamma = \delta(\beta+\delta)$, *kde* $\delta \in \overline{\mathbb{F}}$ *je jeden z kořenů* $p(x)$.

Důkaz. Označme jako δ kořen polynomu $p(x)$ v $\overline{\mathbb{F}}$. V $\mathbb{F}[\delta]$ potom platí

$$p(x) = (x+\delta)(x+(e+f\delta)) = x^2 + (e+(f+1)\delta)x + \delta(e+f\delta)$$

pro nějaká e,$f \in \mathbb{F}$. Protože $e+(f+1)\delta = \beta \in \mathbb{F}$ a $\delta \notin \mathbb{F}$ (neboť $p(x)$ je ireducibilní nad $\mathbb{F}$), musí být $f+1 = 0$, neboli $f = 1$. Z předpokladu, že kořeny $p(x)$ jsou různé, následně plyne, že $e \neq 0$. Máme tedy $\gamma = \delta(e+\delta)$, $\beta = e$ (speciálně tudíž $\beta \neq 0$) a $\frac{\gamma}{\beta^2} = \frac{\delta(\beta+\delta)}{\beta^2}$.

Podle Lemmatu 44 stačí k důkazu, že grupy $A_{1,\beta,\gamma}$ a $A_{1,1,\frac{\gamma}{\beta^2}}$ konjugované, nalézt $a, b \in \mathbb{F}$ taková, že

$$1 = a\beta,\ \frac{\gamma}{\beta^2} = b^2 + a^2\gamma + ab\beta.$$

Z první rovnice ihned dostáváme $a = \beta^{-1}$, druhá je pak zřejmě splněna pro $b = 0$. Pro $N = \beta^{-1}x$ tudíž platí $NA_{1,\beta,\gamma}N^{-1} = A_{1,1,\frac{\gamma}{\beta^2}}$.

□

Lemma 52. *Grupy $A, B \in \mathcal{A}_0(\mathbb{F})$ jsou konjugované, právě když existuje $N \in L(\mathbb{F})_\infty$ takové, že $B = NAN^{-1}$.*

Důkaz. Z definice jsou A a B konjugované $\Leftrightarrow$ existuje $L \in L(\mathbb{F})$ takové, že $A = LBL^{-1}$. Podle Lemmatu 10 toto nastane $\Leftrightarrow$ existuje $N \in L(\mathbb{F})_\infty$ splňující $A = NBN^{-1}$, neboť B je tranzitivní na množině $\mathbb{F} \cup \{\infty\}$ (plyne z Lemmatu 28 a z toho, že $|\mathrm{Fix}(B)| = 0$).

□

Lemma 53. *Buď $\mathrm{char}(\mathbb{F}) = 2$, $\mu,\nu \in \mathbb{F}$. Grupy $A = A_{1,1,\mu}$ a $B = A_{1,1,\nu}$ jsou konjugované právě tehdy, když existuje $b \in \mathbb{F}$ takové, že $b^2 + b = \mu + \nu$.*

Důkaz. Nejprve nechť $A, B \in \mathcal{A}_0(\mathbb{F})$. Lemma 44 dává, že $N \in L(\mathbb{F})_\infty$ splňující $B = NAN^{-1}$ je možné najít $\Leftrightarrow$ existují $a, b \in \mathbb{F}$ splňující

$$a = 1,\ \nu = b^2 + a^2\mu + ab.$$

Ta existují $\Leftrightarrow$ lze nalézt $b \in \mathbb{F}$ takové, že $\nu = b^2 + \mu + b$, tj. $b^2 + b = \mu + \nu$.

Nyní nechť $A, B \notin \mathcal{A}_0(\mathbb{F})$. Protože $|\mathrm{Fix}(A)| \neq 0$ a $\infty \notin \mathrm{Fix}(A)$, musí mít polynom $x^2 + x + \mu$ kořen v $\mathbb{F}$. Neboli, existují a,$b \in \mathbb{F}$ tak, že

$$x^2 + x + \mu = (x + a)(x + b) = x^2 + (a + b)x + ab.$$

Zřejmě musí platit $a + b = 1$, tj. $b = a + 1$, a tedy $\mu = a(a + 1)$. Podobně $\nu = c(c + 1)$ pro nějaké $c \in \mathbb{F}$. Tudíž

$$|\mathrm{Fix}(A)| = |\{a,a + 1\}| = 2 = |\{c,c + 1\}| = |\mathrm{Fix}(B)|.$$

Podle Tvrzení 46 jsou tedy grupy A a B konjugované. Zároveň

$$\mu + \nu = a(a + 1) + c(c + 1) = a^2 + c^2 + a + c = (a + c)^2 + a + c.$$

□

Věta 54. *Nechť $\mathrm{char}(\mathbb{F}) = 2$. Uvažujme grupy $A = A_{\alpha,\beta,\gamma}$, $B = A_{\rho,\sigma,\tau}$ a předpokládejme, že $|\mathrm{Fix}(A)| = 0 = |\mathrm{Fix}(B)|$. Pak jsou následující dvě podmínky ekvivalentní:*

1) A a B jsou konjugované,

2) polynomy $\alpha x^2+\beta x+\gamma$ a $\rho x^2+\sigma x+\tau$ mají $\mathbb{F}$-izomorfní rozkladová nadtělesa.

Důkaz. Stejně jako v důkazu Věty 49 můžeme předpokládat, že $\alpha = 1 = \rho$. Označme $x^2 + \beta x + \gamma = p(x)$, $x^2 + \sigma x + \tau = q(x)$.

Platí-li podmínka 1), pak musí být rozkladová nadtělesa polynomů $p(x)$, $q(x)$ $\mathbb{F}$-izomorfní podle Lemmatu 48.

Nechť platí 2).

Podle Lemmatu 19 mohou nastat pouze dvě možnosti; buďto mají oba polynomy $p(x)$, $q(x)$ dva různé kořeny v $\overline{\mathbb{F}}$, nebo má každý z nich jeden dvojnásobný kořen v $\overline{\mathbb{F}}$. Obě tyto možnosti rozebereme zvlášť.

- Nejprve předpokládejme, že mají polynomy $p(x)$, $q(x)$ dva různé kořeny v $\overline{\mathbb{F}}$.

  Z Lemmatu 51 víme, že existují $M, N \in L(\mathbb{F})$ taková, že $A = MA_{1,1,\frac{\gamma}{\beta^2}}M^{-1}$, $NBN^{-1} = A_{1,1,\frac{\tau}{\sigma^2}}$.

  Označme kořen polynomu $p(x)$ jako δ. Těleso $\mathbb{F}[\delta]$ je pak rozkladovým nadtělesem $p(x)$, je to tedy současně i rozkladové nadtěleso polynomu $q(x)$, a tudíž v něm má $q(x)$ kořen $\varepsilon = g + h\delta$ pro nějaká g,$h \in \mathbb{F}$. Lemma 51 říká, že $\gamma = \delta(\beta + \delta)$, $\tau = \varepsilon(\sigma + \varepsilon)$. Tudíž dostáváme

  $$\frac{\gamma}{\beta^2} + \frac{\tau}{\sigma^2} = \frac{\delta(\beta+\delta)}{\beta^2} + \frac{\varepsilon(\sigma+\varepsilon)}{\sigma^2} = \left(\frac{\delta^2}{\beta^2} + \frac{\varepsilon^2}{\sigma^2}\right) + \left(\frac{\delta}{\beta} + \frac{\varepsilon}{\sigma}\right) = b^2 + b$$

  pro $b = \frac{\delta}{\beta} + \frac{\varepsilon}{\sigma}$.

  Dokážeme, že $b \in \mathbb{F}$. Platí $\varepsilon(\sigma+\varepsilon) = (g+h\delta)(\sigma+g+h\delta) = \sigma g + g^2 + h^2(\sigma h^{-1}\delta + \delta^2) \in \mathbb{F}$, neboť $\varepsilon(\sigma+\varepsilon) = \tau$ a $\tau \in \mathbb{F}$. Tudíž $\sigma h^{-1}\delta + \delta^2 \in \mathbb{F}$, neboť $\sigma g + g^2 \in \mathbb{F}$ a $h^2 \in \mathbb{F}$ (poznamenejme, že ireducibilita polynomu $q(x)$ implikuje $h \neq 0$). Zároveň $\delta\beta + \delta^2 = \gamma \in \mathbb{F}$, a tedy $(\sigma h^{-1}\delta + \delta^2) + (\delta\beta + \delta^2) = (\sigma h^{-1} + \beta)\delta \in \mathbb{F}$. To znamená, že musí být $\sigma h^{-1} = \beta$. Máme tedy

  $$b = \frac{\delta}{\sigma h^{-1}} + \frac{\varepsilon}{\sigma} = \frac{\delta + (g+h\delta)h^{-1}}{\sigma h^{-1}} = \frac{gh^{-1}}{\sigma h^{-1}} = \frac{g}{\sigma} \in \mathbb{F}.$$

  Lemma 53 poté dává, že existuje $K \in L(\mathbb{F})$ splňující $A_{1,1,\frac{\gamma}{\beta^2}} = KA_{1,1,\frac{\tau}{\sigma^2}}K^{-1}$.

  Dohromady

  $$A_{1,\beta,\gamma} = MA_{1,1,\frac{\gamma}{\beta^2}}M^{-1} = MKA_{1,1,\frac{\tau}{\sigma^2}}K^{-1}M^{-1} =$$
  $$= MKNA_{1,\sigma,\tau}N^{-1}K^{-1}M^{-1} = (MKN)A_{1,\sigma,\tau}(MKN)^{-1}.$$

- Nyní nechť má každý z polynomů $p(x)$, $q(x)$ jeden dvojnásobný kořen v $\overline{\mathbb{F}}$.

  Pak $p(x) = (x+\delta)^2 = x^2 + \delta^2$ pro $\delta \in \overline{\mathbb{F}}$, a protože $\mathbb{F}[\delta]$ je zároveň rozkladovým nadtělesem polynomu $q(x)$, tak také $q(x) = (x + (g + h\delta))^2 = x^2 + g^2 + h^2\delta^2$ pro nějaká g,$h \in \mathbb{F}$.

  Hledejme a,$b \in \mathbb{F}$ taková, že $\tau = b^2 + a^2\gamma$, neboli $g^2 + h^2\delta^2 = b^2 + a^2\delta$. Zvolme $a = h$, pak máme $g^2 = b^2$. Vyhovuje tedy třeba $b = g$. Podle Lemmatu 44 tudíž $A_{1,\sigma,\tau} = NA_{1,\beta,\gamma}N^{-1}$ pro $N = hx + g$ (protože $\beta = 0 = \sigma$, obě strany rovnice $\sigma = a\beta - 2b$ jsou nulové). Z ireducibility polynomu $q(x)$ opět plyne, že $h \neq 0$, takže je N skutečně prvkem $L(\mathbb{F})$.

□

Tvrzení 55. *Budˇ* $\mathrm{char}(\mathbb{F}) = 2$.

Počet tříd konjugace, na které se rozpadá množina $\mathcal{S} = \{A_{\alpha,\beta,\gamma} \in \mathcal{A}_0(\mathbb{F}) \mid \alpha x^2 + \beta x + \gamma$ je separabilní$\}$*, je*

$$[\mathbb{F}\colon H] - 1,$$

kde $H = \{b^2 + b \mid b \in \mathbb{F}\}$.

Existuje bijekce mezi třídami kojugace množiny $\mathcal{N} = \{A_{\alpha,\beta,\gamma} \in \mathcal{A}_0(\mathbb{F}) \mid \alpha x^2 + \beta x + \gamma$ není separabilní$\}$ *a množinou jednodimenzionálních podprostorů vektorového prostoru* $\mathbb{F}/\mathbb{F}^2 = \{f + \mathbb{F}^2 \mid f \in \mathbb{F}\}$ *nad* $\mathbb{F}^2 = \{f^2 \mid f \in \mathbb{F}\}$.

Důkaz. Podle Lemmatu 51 lze každou třídu konjugace množiny $\mathcal{S}$ reprezentovat grupou $A_{1,1,\mu}$ pro nějaké $\mu \in \mathbb{F}$.

Podle Lemmatu 53 jsou grupy $A_{1,1,\mu}$ a $A_{1,1,\nu}$ konjugované $\Leftrightarrow$ existuje $b \in \mathbb{F}$ takové, že $\mu + \nu = b^2 + b$. Celkový počet tříd konjugace, které lze takovou grupou reprezentovat, je tedy roven počtu rozkladových tříd grupy $(\mathbb{F},+)$ podle $H = \{b^2 + b \mid b \in \mathbb{F}\}$.

Množina $\mathcal{S}$ obsahuje právě prvky těch tříd konjugace, které jsou reprezentované grupou $A_{1,1,\mu}$ takovou, že $|\mathrm{Fix}(A_{1,1,\mu})| = 0$.

Z důkazu Lemmatu 53 víme, že platí-li $|\mathrm{Fix}(A_{1,1,\mu})|,|\mathrm{Fix}(A_{1,1,\nu})| \neq 0$, jsou $A_{1,1,\mu}$ a $A_{1,1,\nu}$ konjugované. Všechny takové grupy tedy reprezentují tutéž třídu konjugace.

Počet tříd konjugace ve Větě 54 je tudíž $[\mathbb{F}\colon H] - 1$.

Index $[\mathbb{F}\colon H]$ skutečně můžeme uvažovat, neboť H je podgrupou $\mathbb{F}$. Pro $b,c \in H$ totiž platí

$$0 = 0^2 + 0 \in H, \ -(b^2 + b) = b^2 + b \in H,$$
$$b^2 + b + c^2 + c = (b^2 + c^2) + (b + c) = (b + c)^2 + (b + c) \in H.$$

Nyní dokažme druhou část tvrzení.

Nechť $A = A_{\alpha,\beta,\gamma}, B = A_{\rho,\sigma,\tau} \in \mathcal{N}$. Potom $\beta = 0 = \sigma$, a můžeme předpokládat, že $\alpha = 1 = \rho$.

Podle Lemmat 52 a 44 jsou grupy A a B konjugované právě tehdy, když existují $a, b \in \mathbb{F}$ tak, že $\tau = b^2 + a^2\gamma$. Potom

$$\mathbb{F}^2\tau + \mathbb{F}^2 = \{c^2\tau + d^2 \mid c,d \in \mathbb{F}\} = \{c^2(a^2\gamma + b^2) + d^2 \mid c,d \in \mathbb{F}\} =$$
$$= \{(ca)^2\gamma + (cb + d)^2 \mid c,d \in \mathbb{F}\} = \{\tilde{c}^2\gamma + \tilde{d}^2 \mid \tilde{c},\tilde{d} \in \mathbb{F}\} = \mathbb{F}^2\gamma + \mathbb{F}^2,$$

kde předposlední rovnost platí díky tomu, že $a \neq 0$ (a tudíž $\{ca \mid c \in \mathbb{F}\} = \mathbb{F}$). To plyne ze skutečnosti, že polynom $x^2 + \tau$ je neseparabilní, a tedy $\tilde{b}^2 \neq \tau \ \forall \tilde{b} \in \mathbb{F}$.

Naopak, pokud $\mathbb{F}^2\tau + \mathbb{F}^2 = \mathbb{F}^2\gamma + \mathbb{F}^2$, potom zřejmě existují $a, b \in \mathbb{F}$ splňující $\tau = a^2\gamma + b^2$, neboť $\tau \in \mathbb{F}^2\tau + \mathbb{F}^2 = \mathbb{F}^2\gamma + \mathbb{F}^2$.

Máme tedy, že A a B jsou konjugované, právě když $\mathbb{F}^2\gamma + \mathbb{F}^2 = \mathbb{F}^2\tau + \mathbb{F}^2$.

Existuje tedy bijekce mezi třídami konjugace v $\mathcal{N}$ a množinou $\{\mathbb{F}^2\gamma + \mathbb{F}^2 \mid \gamma \in \mathbb{F} \setminus \mathbb{F}^2\} = \{(\gamma + \mathbb{F}^2)\mathbb{F}^2 \mid \gamma \in \mathbb{F} \setminus \mathbb{F}^2\} = \left\{\overline{\gamma}\mathbb{F}^2 \mid \overline{\gamma} \in (\mathbb{F}/\mathbb{F}^2)^*\right\}$, což je právě množina všech jednodimenzionálních podprostorů vektorového prostoru $\mathbb{F}/\mathbb{F}^2$ nad $\mathbb{F}^2$ (protože $\mathrm{char}(\mathbb{F}) = 2$, je $\mathbb{F}^2$ skutečně těleso; uzavřenost na inverzy a to, že $0,1 \in \mathbb{F}^2$, je zřejmé, a uzavřenost na sčítání a opačné prvky plyne z toho, že $(a+b)^2 = a^2 + b^2$, $-a^2 = a^2 \ \forall a, b \in \mathbb{F}$).

□

Důsledek 56. *Předpokládejme, že je $L(\mathbb{F})$ konečná. Pak jsou grupy $A,B \in \mathcal{A}(\mathbb{F})$ konjugované právě tehdy, když $|\mathrm{Fix}(A)| = |\mathrm{Fix}(B)|$.*

Důkaz. Jestliže $|L(\mathbb{F})| < \infty$, pak také $|\mathbb{F}| < \infty$. Z Tvrzení 46, Vět 49 a 54 a Lemmatu 16 tedy dostáváme, že platí-li $|\mathrm{Fix}(A)| = |\mathrm{Fix}(B)|$, jsou grupy A, B konjugované (neboť pokud $|\mathrm{Fix}(A)| = 0 = |\mathrm{Fix}(B)|$, jsou příslušné polynomy ireducibilní a jejich rozkladová nadtělesa jsou tudíž rozšířeními $\mathbb{F}$ stupně 2).

Opačná implikace plyne z Lemmatu 9.

□

2.5.1 Normalizátory

Pro $A \in \mathcal{A}(\mathbb{F})$ určíme *normalizátor* $N_{L(\mathbb{F})}(A)$ grupy A v $L(\mathbb{F})$, neboli množinu všech prvků $L \in L(\mathbb{F})$ takových, že $LAL^{-1} = A$.

Tvrzení 57. *Nechť $A \in \mathcal{A}_1(\mathbb{F})$, $\mathrm{Fix}(A) = \{f\}$. Pak*

$$N_{L(\mathbb{F})}(A) = A_{0,1,-f} \cup \bigcup_{e \in \mathbb{F}} A_{1,e+f,ef}.$$

Důkaz. Je-li $L \in A$, pak z důkazu Lemmatu 9 plyne, že f je pevným bodem KLK^{-1} právě tehdy, když $K(f) = f$. Normalizátor grupy A je tedy tvořen právě všemi grupami $B \in \mathcal{A}(\mathbb{F})$ takovými, že $f \in \mathrm{Fix}(B)$. Fixuje-li grupa B body f a ∞, pak $B = A_{0,1,-f}$. Fixuje-li body f a $e \in \mathbb{F}$, potom $B = A_{1,e+f,ef}$.

□

Lemma 58. *Označme $L = \frac{ax+b}{cx+d} \in L(\mathbb{F})$.*

Nechť $\mathrm{char}(\mathbb{F}) \neq 2$. Pak je prvek L involuce právě tehdy, když $d = -a$. Involuce jsou tedy právě všechny prvky $\frac{b}{x}$ pro $b \neq 0$ a $\frac{x+b}{cx-1}$, kde $bc + 1 \neq 0$.

Je-li char$(\mathbb{F}) = 2$, je L involuce právě tehdy, když $a = d$ a $(b,c) \neq (0,0)$. Involuce jsou tedy právě všechny prvky $\frac{b}{x}$ pro $b \neq 0$ a $\frac{x+b}{cx+1}$, kde $bc + 1 \neq 0$, $(b,c) \neq (0,0)$.

Důkaz. Hledáme prvky, jejichž druhá mocnina je x, a zároveň nejsou řádu 1. Máme

$$\left(\frac{ax+b}{cx+d}\right)^2 = \frac{(a^2+bc)x + b(a+d)}{c(a+d)x + (cb+d^2)}.$$

Požadujeme-li, aby byl poslední výraz roven x, dostáváme podmínky

$$a^2 + bc = cb + d^2,$$
$$b(a+d) = c(a+d) = 0.$$

Odsud $(a = \pm d) \wedge (b = c = 0 \vee a = -d)$.

Nechť $\mathrm{char}(\mathbb{F}) \neq 2$. Vyloučíme-li prvek řádu 1, neboli případ $a = d$, $b = c = 0$, ze všech podmínek dohromady vyjde $a = -d$. Množina všech involucí má tedy tvar

$$\left\{\frac{ax+b}{cx+d} \in L(\mathbb{F}) \mid d = -a\right\} =$$
$$= \left\{\frac{ax+b}{cx+d} \in L(\mathbb{F}) \mid d = -a,\, a = 1\right\} \cup \left\{\frac{ax+b}{cx+d} \in L(\mathbb{F}) \mid d = -a,\, a = 0\right\} =$$
$$= \left\{\frac{x+b}{cx-1} \mid -1 - bc \neq 0\right\} \cup \left\{\frac{b}{cx} \mid -bc \neq 0\right\} =$$
$$= \left\{\frac{x+b}{cx-1} \mid bc + 1 \neq 0\right\} \cup \left\{\frac{b}{x} \mid b \neq 0\right\}.$$

Jestliže $\mathrm{char}(\mathbb{F}) = 2$, podmínky $(a = \pm d) \wedge (b = c = 0 \vee a = -d)$ jsou ekvivalentní $a = d$. Vyloučit prvek řádu 1 zde tedy znamená požadovat navíc $(b,c) \neq (0,0)$.

□

Tvrzení 59. *Nechť $A \in \mathcal{A}_2(\mathbb{F})$. Pak libovolný prvek $N_{L(\mathbb{F})}(A)$ buďto leží v A, nebo jde o involuci.*

Důkaz. Označme $\mathrm{Fix}(A) = \{e,f\}$. Vidíme, že pro $L \in A$ a $K \in L(\mathbb{F})$ fixuje prvek KLK^{-1} body $K(e)$, $K(f)$, z čehož vyplývá, že

$$N_{L(\mathbb{F})}(A) = \{K \in L(\mathbb{F}) \mid K(e), K(f) \in \{e, f\}\}.$$

Uvažujme $K = \frac{ax+b}{cx+d} \in L(\mathbb{F})$ takové, že $K(e) = f$, $K(f) = e$.

Nejdříve předpokládejme, že $e, f \in \mathbb{F}$. Rovnost $\frac{ae+b}{ce+d} = f$, resp. $\frac{af+b}{cf+d} = e$, dává $b = cef + fd - ae$, resp. $b = cef + ed - af$. Máme tedy $fd - ae = ed - af \Rightarrow a(f-e) = d(e-f) \Rightarrow a = -d$, neboť $e \neq f$. Podle Lemmatu 58 je tudíž K involucí.

Nyní nechť $e = \infty$. Pak máme $K(f) = \frac{af+b}{cf+d} = \infty \Rightarrow cf + d = 0 \Rightarrow d = -cf$; $K(\infty) = \frac{a}{c} = f \Rightarrow a = cf$. Opět tedy $a = -d$.

□

Poznámka. Normalizátor z předchozího tvrzení můžeme určit přesněji. Nechť $K = \frac{ax+b}{cx+d} \in N_{L(\mathbb{F})}(A)$.

V důkazu jsme zjistili, že jestliže $e,f \in \mathbb{F}$, pak $K = \frac{ax+cef-a(f+e)}{cx-a}$. Rozlišíme dva případy.

- Je-li $a = 0$, pak $c \neq 0$ a dostáváme $K = \frac{cef}{cx} = \frac{ef}{x}$.

  Případ $a = 0$ může nastat pouze pokud $e,f \neq 0$, neboť $ad - bc \neq 0$.

- Je-li $a \neq 0$, potom bez újmy na obecnosti $a = 1$, a tudíž $K = \frac{x+cef-(e+f)}{cx-1}$.

  Zde je $c \in \mathbb{F}$ takové, že $0 \neq ad - bc = -1 - efc^2 + (e+f)c$. Pro $e,f \neq 0$ tedy $c \in \mathbb{F} \setminus \{e^{-1},f^{-1}\}$ a pro $e = 0$ bude $c \in \mathbb{F} \setminus \{f^{-1}\}$.

Nyní nechť $e = \infty$. Potom $d = -cf$, $a = cf$. Protože ∞ není pevným bodem prvku K (jelikož $f \neq \infty$ a $K(\infty) = f$), platí $c \neq 0$. Můžeme tudíž předpokládat $c = 1$. Pak $K = \frac{fx+b}{x-f}$, kde $b \in \mathbb{F} \setminus \{-f^2\}$.

Pro $N_{L(\mathbb{F})}(A)$ tedy máme následující možnosti:

- $N_{L(\mathbb{F})}(A) = A \cup \left\{\frac{fx+b}{x-f} \mid b \in \mathbb{F} \setminus \{-f^2\}\right\}$, pokud $e = \infty$,
- $N_{L(\mathbb{F})}(A) = A \cup \left\{\frac{x+cef-(e+f)}{cx-1} \mid c \in \mathbb{F} \setminus \{e^{-1},f^{-1}\}\right\} \cup \left\{\frac{ef}{x}\right\}$, pokud $\{e,f\} \cap \{\infty,0\} = \emptyset$,
- $N_{L(\mathbb{F})}(A) = A \cup \left\{\frac{x-f}{cx-1} \mid c \in \mathbb{F} \setminus \{f^{-1}\}\right\}$, pokud $e = 0$, $f \neq \infty$.

Tvrzení 60. *Nechť $A = A_{\alpha,\beta,\gamma} \in \mathcal{A}_0(\mathbb{F})$. Pak*

$$N_{L(\mathbb{F})}(A) = A \cup (-x - \beta)A,$$

kde $(-x-\beta)A = \{(-x-\beta)L \mid L \in A\}$.

Důkaz. Bez újmy na obecnosti předpokládejme, že $\alpha = 1$.

Nechť $L \in L(\mathbb{F})$. Použijeme Lemma 10 a nalezneme $N \in L(\mathbb{F})_\infty$ a $K \in A$ taková, že $L = NK$ a $LAL^{-1} = NAN^{-1}$. Uvažujme $M \in A$ a označme $M = \frac{tx-\gamma}{x+\beta+t}$, $N = ax + b$. Platí

$$NMN^{-1} = (ax+b)\left(\frac{tx-\gamma}{x+\beta+t}\right)(a^{-1}x - a^{-1}b) =$$
$$= \frac{(at+b)x - b(at+b) - a^2\gamma + ab(\beta+t)}{x - b + a(\beta+t)} = \frac{(at+b)x - (b^2 + a^2\gamma - ab\beta)}{x + (a\beta - 2b) + (at+b)}.$$

Tj. $NMN^{-1} \in A$ právě tehdy, když jsou splněny rovnosti

$$b^2 + a^2\gamma - ab\beta = \gamma,$$
$$a\beta - 2b = \beta.$$

Je-li char($\mathbb{F}$)$\neq 2$, z druhé rovnice dostáváme $b = \frac{\beta(a-1)}{2}$ a po dosazení do rovnice první poté vyjde $(4\gamma - \beta^2)a^2 = 4\gamma - \beta^2$. Kdyby $4\gamma - \beta^2 = 0$, neboli $\gamma = \frac{\beta^2}{4}$, měli bychom $\alpha x^2 + \beta x + \gamma = x^2 + \beta x + \frac{\beta^2}{4} = (x + \frac{\beta}{2})^2$, čili by $-\frac{\beta}{2}$ byl pevným bodem M, což je spor. Tudíž $a^2 = 1$, a tedy dostáváme dvě řešení:

$$(a,b) = (1,0),\ (a,b) = (-1,-\beta).$$

To znamená, že

$$N_{L(\mathbb{F})}(A) = A \cup (-x - \beta)A.$$

V případě, že char($\mathbb{F}$)$= 2$, má druhá rovnice tvar $\beta(a+1) = 0$. Pokud $\beta = 0$, první rovnice je tvaru $b^2 + a^2\gamma = \gamma$. Jestliže $a \neq 1$, dostáváme odsud $\gamma = \frac{b^2}{a^2+1} = \frac{b^2}{(a+1)^2}$, což je spor s ireducibilitou polynomu $x^2 + \beta x + \gamma$, který by měl za tohoto předpokladu dvojnásobný kořen $\frac{b}{a+1}$. Je-li tedy $\beta = 0$, musí platit $a = 1$, a tudíž $b^2 = \gamma \cdot 0 = 0 \Rightarrow b = 0$, tj. $(a,b) = (1,0) = (-1,\beta)$. Pokud $\beta \neq 0$, dostáváme z druhé rovnice, že $a = 1$. První rovnice potom dává $b(b+\beta) = 0$, tj. $b = 0$ nebo $b = -\beta = \beta$. Máme tedy stejný výsledek jako pro char($\mathbb{F}$)$\neq 2$.

□

Lemma 61. *Nechť $A \in \mathcal{A}_2(\mathbb{F})$. Pak je každý netriviální prvek centra grupy $N_{L(\mathbb{F})}(A)$ involuce.*

Důkaz. Z Tvrzení 59 víme, že je involuce libovolný prvek $N_{L(\mathbb{F})}(A) \setminus A$.

Předpokládejme, že existuje $L \in A \setminus \{x\}$ takové, že $LK = KL$ pro $K \in N_{L(\mathbb{F})}(A) \setminus A$. Označme Fix$(A) = \{e,f\}$. Podle důkazu Tvrzení 59 potom máme, že $K(e) = f$, $K(f) = e$. Díky 3-tranzitivitě grupy $L(\mathbb{F})$ můžeme dále požadovat, aby platilo $K(g) = L(g)$ pro nějaké $g \neq e,f$. Protože K je involuce, neboli $K^2 = x$, dostáváme $KL(g) = K^2(g) = g$. Vztah $LK = KL$ tedy implikuje $LK(g) = g$. Ale $LK(g) = L^2(g)$, což znamená, že L^2 fixuje po dvou různé body e,f,g a z ostré tranzitivity $L(\mathbb{F})$ je tudíž $L^2 = x$, tj. L je involuce.

□

Lemma 62. *Ať $A \in \mathcal{A}_2(\mathbb{F})$. Platí, že index A v $N_{L(\mathbb{F})}(A)$ je 2.*

Důkaz. Označme $\mathrm{Fix}(A) = \{e,f\}$. Položme

$$X = \{K \in L(\mathbb{F}) \mid K(e) = f,\, K(f) = e\}.$$

Potom $N_{L(\mathbb{F})}(A) = A \cup X$.

Buď $K \in X$, $L \in A$. Vidíme, že $KL(e) = K(e) = f$ a obdobně $KL(f) = e$, tj. $KL \in X$. Naopak, libovolný prvek $M \in X$ můžeme zapsat jako $M = K(KM)$ (X je podmnožinou $N_{L(\mathbb{F})}(A) \setminus A$, všechny prvky X jsou tedy involuce podle Tvrzení 59), kde $KM(e) = K(f) = e$, $KM(f) = K(e) = f$, neboli $KM \in A$. Dohromady tudíž $KA = X$.

Dostáváme tak, že

$$[N_{L(\mathbb{F})}(A) \colon A] = |\{NA \mid N \in N_{L(\mathbb{F})}(A)\}| = |\{A,X\}| = 2.$$

□

Lemma 63. *Nechť $A,B \in \mathcal{A}(\mathbb{F})$. Ať $L \in A$ a $KLK^{-1} \in B$ pro $K \in L(\mathbb{F})$. Pak $KAK^{-1} = B$. Speciálně, platí-li $KL = LK$, potom $K \in N_{L(\mathbb{F})}(A)$.*

Důkaz. Rovnost $KAK^{-1} = B$ platí díky Tvrzení 45 a skutečnosti, že každý netriviální prvek $L(\mathbb{F})$ leží v právě jedné grupě z $\mathcal{A}(\mathbb{F})$.

Jestliže $KL = LK$, máme $KLK^{-1} = L$, a z předchozího tedy plyne, že $KAK^{-1} = A$, neboli $K \in N_{L(\mathbb{F})}(A)$.

□

Lemma 64. *Nechť $A = A_{\alpha,\beta,\gamma} \in \mathcal{A}_0(\mathbb{F})$.*

Jestliže $\mathrm{char}(\mathbb{F}) \neq 2$*, je každý netriviální prvek centra grupy $N_{L(\mathbb{F})}(A)$ involuce. Pokud* $\mathrm{char}(\mathbb{F}) = 2$*, je buďto každý netriviální prvek $Z(N_{L(\mathbb{F})}(A))$ involuce, nebo $Z(N_{L(\mathbb{F})}(A)) = N_{L(\mathbb{F})}(A) = A$.*

Důkaz. Označme $M = -x - \beta$. Pak $N_{L(\mathbb{F})}(A) = A \cup MA$ podle Tvrzení 60. Uvažujme $x \neq L \in Z(N_{L(\mathbb{F})}(A))$, existuje-li takové. Je-li $L = M$, máme hotovo, protože $M^2 = -(-x - \beta) - \beta = x$, tj. M je involuce. Dále tedy předpokládejme, že $L \neq M$.

Pro L speciálně platí $ML = LM$, neboť $M \in N_{L(\mathbb{F})}(A)$. Prvek M fixuje bod ∞. Rozebereme tři možné situace.

- ∞ je jediným pevným bodem M:

  Pro $L \in A$ zřejmě platí $L(\infty) \neq \infty$, jelikož $A \in \mathcal{A}_0(\mathbb{F})$. Pokud $L \in MA$, tj. $L = MK$ pro $K \in A$, pak opět $L(\infty) \neq \infty$, neboť $K(\infty) \neq \infty$.

  Máme tudíž $LM(\infty) = L(\infty)$, ale $ML(\infty) \neq L(\infty)$, protože $L(\infty) \neq \infty$ a M fixuje pouze ∞. Neplatí tedy $LM = ML$, takže dostáváme spor.

  Obdrželi jsme tak, že $Z(N_{L(\mathbb{F})}(A)) \subset \{x,M\}$. Pro tento případ tudíž dokazované tvrzení platí.

- M má právě dva pevné body ∞ a $f \in \mathbb{F}$:

  Označme B grupu z $\mathcal{A}_2(\mathbb{F})$ takovou, že $M \in B$.

  Lemma 63 dává, že $L \in N_{L(\mathbb{F})}(B)$.

Pokud $L \notin B$, podle Tvrzení 59 je L involuce.

Možnost $L \in B$ by mohla nastat pouze v případě, že $L \in MA$, neboť $A \neq B$. Ať $L = MK$, $K \in A$. Aby platilo, že L fixuje ∞ a f, musí být $K(\infty) = \infty$, $K(f) = f$. To je ovšem ve sporu s předpokladem, že K nemá pevný bod.

- $M = x$:

  Toto může nastat pouze za předpokladu, že $\mathrm{char}(\mathbb{F}) = 2$.

  Podle Tvrzení 60 je $N_{L(\mathbb{F})}(A) = A \cup A = A$, tudíž $Z(N_{L(\mathbb{F})}(A)) = N_{L(\mathbb{F})}(A)$, protože grupa A je abelovská.

□

Lemma 65. *Ať $A \in \mathcal{A}_0(\mathbb{F})$. Platí, že jestliže $\mathrm{char}(\mathbb{F}) \neq 2$, je index A v $N_{L(\mathbb{F})}(A)$ roven 2, a pokud $\mathrm{char}(\mathbb{F}) = 2$, je roven buďto 2, nebo 1.*

Důkaz. Plyne ihned z důkazu předchozího lemmatu a Tvrzení 60.

□

Tvrzení 66. *Platí-li $LK = KL$ pro L,$K \in L(\mathbb{F})$, pak buďto oba prvky L, K leží v téže grupě $A \in \mathcal{A}(\mathbb{F})$, nebo jsou oba involuce.*

Důkaz. Označme jako A grupu z $\mathcal{A}(\mathbb{F})$, v níž je obsažen prvek L. Protože $LK = KL$, díky Lemmatu 63 máme $K \in N_{L(\mathbb{F})}(A)$.

Ať $A \in \mathcal{A}_1(\mathbb{F})$, $\mathrm{Fix}(A) = \{f\}$. Předpokládejme, že $K \notin A$. Podle Tvrzení 57 má pak K právě dva pevné body e,f. Platí $L(e) \notin \{e,f\}$, tudíž $KL(e) \neq L(e) = LK(e)$. Nemůže tedy být $LK = KL$ a dostáváme tak spor. Z toho plyne, že musí platit $K \in A$.

Nyní nechť má každý z prvků L,K právě dva pevné body nebo nemá žádný pevný bod, přičemž $K \notin A$. Pak máme, že $K \in N_{L(\mathbb{F})}(A) \setminus A$. Protože platí $[N_{L(\mathbb{F})}(A) \colon A] = 2$, dostáváme

$$N_{L(\mathbb{F})}(A) = A \cup \{KM \mid M \in A\}.$$

Prvek L tudíž leží v centru $N_{L(\mathbb{F})}(A)$, neboť $L(KM) = KLM = (KM)L$ pro libovolné $M \in A$. Podle Lemmat 61 a 64 je tedy L involuce. Obdobně bychom dokázali, že také K je involuce.

□

Tvrzení 67. *Nechť $A \in \mathcal{A}(\mathbb{F})$. Je-li $\mathbb{F} \neq \mathbb{Z}_3$, pak A je maximální abelovská podgrupa $L(\mathbb{F})$. Pokud $\mathbb{F} = \mathbb{Z}_3$, je $A \in \mathcal{A}(\mathbb{F})$ maximální abelovská podgrupa $L(\mathbb{F})$ právě tehdy, když $A \in \mathcal{A}_0(\mathbb{F}) \cup \mathcal{A}_1(\mathbb{F})$.*

Důkaz. Pokud $|\mathrm{Fix}(A)| = 1$, pak pro netriviální prvek $L \in A$ a $K \in L(\mathbb{F})$ platí, že $LK = KL$, právě když $K \in A$. To bylo konstatováno v důkazu Tvrzení 66. Libovolná grupa $A \in \mathcal{A}_1(\mathbb{F})$ tedy skutečně je maximální abelovskou podgrupou $L(\mathbb{F})$.

Dále uvažujme $A \in \mathcal{A}_0(\mathbb{F}) \cup \mathcal{A}_2(\mathbb{F})$.

Označme $Y = (\mathbb{F} \cup \{\infty\}) \setminus \mathrm{Fix}(A)$. Víme, že A je tranzitivní permutační grupa množiny Y a že je abelovská.

Pokud $|\mathrm{Fix}(A)| = 0$, Lemma 12 ihned dává, že A je maximální abelovská podgrupa.

Nyní nechť $|\mathrm{Fix}(A)| = 2$ a $\mathbb{F} \neq \mathbb{Z}_3$. Označme $\mathrm{Fix}(A) = \{e,f\}$. Je-li $\tilde{A} \subset L(\mathbb{F})$ abelovská grupa a $A \subseteq \tilde{A}$, pak $\tilde{A} \subseteq N_{L(\mathbb{F})}(A)$. Pro $L \in N_{L(\mathbb{F})}(A)$ platí $L(e),L(f) \in \{e,f\}$, z čehož vyplývá, že $L(Y) = Y$; L tedy působí na množině $Y = (\mathbb{F} \cup \{\infty\}) \setminus \{e,f\}$ a na $\tilde{A}$ tak můžeme nahlížet jako na permutační grupu této množiny. Mějme $K \in \tilde{A}$. Grupa A je na Y tranzitivní, z důkazu Lemmatu 12 tedy plyne, že existuje $M \in A$ takové, že $K(a) = M(a)$ pro každé $a \in Y$. Je-li $|Y| \geq 3$, z ostré 3-tranzitivity grupy $L(\mathbb{F})$ dostáváme $K = M$, a tudíž $K \in A$, neboli máme, co jsme chtěli. Zbývá tak pouze vyřešit případ, kdy $|Y| \leq 2$, tj. $|\mathbb{F}| \leq 3$. Zde máme dvě možnosti; $\mathbb{F} = \mathbb{Z}_2$ nebo $\mathbb{F} = \mathbb{Z}_3$. Jestliže $\mathbb{F} = \mathbb{Z}_2$, pak $|\mathbb{F} \cup \{\infty\}| = 3$. Pokud nějaký prvek $L(\mathbb{Z}_2)$ fixuje dva body, fixuje i ten třetí a jedná se o identitu. Odsud plyne, že $\mathcal{A}_2(\mathbb{Z}_2) = \emptyset$, a tedy není co dokazovat.

Nakonec ať $|\mathrm{Fix}(A)| = 2$ a $\mathbb{F} = \mathbb{Z}_3$. Máme $|\mathbb{F} \cup \{\infty\}| = 4$. Fixuje-li prvek $L(\mathbb{Z}_3)$ dva body, buďto zbylé dva prohazuje, nebo jde o identitu. Grupa A je tudíž dvouprvková. Označme $A = \{x,M\}$. Libovolné $L \in L(Z_3)$ splňuje $LM = ML$, právě když $L \in N_{L(\mathbb{F})}(A)$. Podle Lemmatu 62 je index A v $N_{L(\mathbb{Z}_3)}(A)$ roven 2, což implikuje, že existuje prvek $K \in N_{L(\mathbb{Z}_3)}(A) \setminus A$. Grupa generovaná prvky M a K (označme ji $\tilde{A}$) je abelovská a A je její vlastní podgrupou. Zároveň $\tilde{A} \neq L(\mathbb{F})$, neboť kterékoliv L takové, že $L(e) \in Y$ pro $e \in \mathrm{Fix}(A)$, v $\tilde{A}$ neleží (jelikož M prvky $\mathrm{Fix}(A)$ fixuje a M je prohazuje). Grupa A tedy není maximální abelovská podgrupa $L(\mathbb{Z}_3)$.

□

2.6 Projektivní speciální lineární grupa

V této sekci se zaměříme na grupu $PSL_2(\mathbb{F})$. Protože $PGL_2(\mathbb{F}) \simeq L(\mathbb{F})$, lze $PSL_2(\mathbb{F})$ vnímat jako podgrupu $L(\mathbb{F})$.

Tvrzení 68. *Platí* $\frac{ax+b}{cx+d} \in PSL_2(\mathbb{F})$*, právě když* $ad - bc = \lambda^2$ *pro nějaké* $\lambda \in \mathbb{F}^*$.

Důkaz. Máme, že prvek $\frac{ax+b}{cx+d}$ leží v $PSL_2(\mathbb{F}) \simeq (SL_2(\mathbb{F})Z(GL_2(\mathbb{F})))/Z(GL_2(\mathbb{F}))$, právě když $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ leží v $SL_2(\mathbb{F})Z(GL_2(\mathbb{F}))$. To nastane právě tehdy, když

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

pro nějaké $\lambda \in \mathbb{F}^*$ a $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ takovou, že $\det \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = 1$. Pak

$$ad - bc = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \det \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \lambda^2.$$

Pokud naopak $ad - bc = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \lambda^2$ pro nějaké $\lambda \in \mathbb{F}^*$, potom

$$\det \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \right) = \lambda^2 \lambda^{-2} = 1,$$

a tedy

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a\lambda^{-1} & b\lambda^{-1} \\ c\lambda^{-1} & d\lambda^{-1} \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},$$

kde $\begin{pmatrix} a\lambda^{-1} & b\lambda^{-1} \\ c\lambda^{-1} & d\lambda^{-1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \in SL_2(\mathbb{F})$.

□

Lemma 69. *Stabilizátor $PSL_2(\mathbb{F})_\infty$ bodu ∞ je tranzitivní a platí*

$$PSL_2(\mathbb{F})_\infty = \{c^2x + b \mid c \in \mathbb{F}^*,\, b \in \mathbb{F}\}.$$

Důkaz. Máme

$$PSL_2(\mathbb{F})_\infty = L(\mathbb{F})_\infty \cap PSL_2(\mathbb{F}) = \{ax + b \mid a \in \mathbb{F}^*,\, b \in \mathbb{F}\} \cap PSL_2(\mathbb{F}) =$$
$$= \left\{\frac{ax+b}{0x+1} \mid a \in \mathbb{F}^*,\, b \in \mathbb{F}\right\} \cap PSL_2(\mathbb{F}) = \{ax + b \mid b \in \mathbb{F},\, a \in (\mathbb{F}^*)^2\} =$$
$$= \{c^2x + b \mid c \in \mathbb{F}^*,\, b \in \mathbb{F}\}.$$

Pro e,$f \in \mathbb{F}$ existuje $L_{e,f} \in PSL_2(\mathbb{F})_\infty$ takové, že $L_{e,f}(e) = f$, a to například $L_{e,f} = x + (f - e)$, tj. $PSL_2(\mathbb{F})_\infty$ je tranzitivní permutační grupou množiny $\mathbb{F}$.

□

Tvrzení 70. *Grupa $PSL_2(\mathbb{F})$ je 2-tranzitivní.*

Důkaz. Nejprve ukážeme, že je $PSL_2(\mathbb{F})$ tranzitivní. Podle Lemmatu 8 stačí dokázat, že pro každé $f \in \mathbb{F} \cup \{\infty\}$ existuje $L_f \in PSL_2(\mathbb{F})$ takové, že $L_f(f) = 0$.

Pro $f = \infty$ můžeme vzít $L_f = -\frac{1}{x} = \frac{0x-1}{1x+0}$. Platí $0 \cdot 0 - (-1) \cdot 1 = 1 = 1^2$, tudíž $-\frac{1}{x} \in PSL_2(\mathbb{F})$ podle Tvrzení 68.

Pro $f \in \mathbb{F}$ volme $L_f = x - f = \frac{x-f}{0x+1}$. Máme $x - f \in PSL_2(\mathbb{F})$, neboť $1 \cdot 1 - (-f) \cdot 0 = 1 = 1^2$.

Podle Lemmatu 69 a Důsledku 7 je libovolný stabilizátor bodu v $PSL_2(\mathbb{F})$ tranzitivní.

Grupa $PSL_2(\mathbb{F})$ je tedy 2-tranzitivní podle Lemmatu 5.

□

Tvrzení 71. *Grupa $PSL_2(\mathbb{F})$ je primitivní.*

Důkaz. Jde o přímočarý důsledek Tvrzení 70 a 13.

□

Lemma 72. *Množina $\left\{x + f,\, \frac{x}{fx+1} \mid f \in \mathbb{F}^*\right\}$ generuje grupu $PSL_2(\mathbb{F})$.*

Důkaz. Uvažujme prvek $\frac{ax+b}{cx+d} \in PSL_2(\mathbb{F})$.

- $a \neq 0$:

  Bez újmy na obecnosti $a = 1$. Platí $ad - bc = 1$, a tedy $d = a^{-1}(bc + 1) = bc + 1$. Máme

  $$\frac{x+b}{cx + (bc+1)} = \frac{x}{cx+1} \circ (x + b).$$

- $a = 0$:

  Potom b,$c \neq 0$, $-bc = 1$. Tudíž $c = -b^{-1}$.

  Platí

$$\frac{0x+b}{-b^{-1}x+d} = \begin{cases} (x+b) \circ \frac{x}{-b^{-1}x+1} \circ (x+b), \text{ pokud } d = 0, \\ (x+b) \circ \frac{x}{-b^{-1}x+1}, \text{ pokud } d = 1. \end{cases}$$

□

Tvrzení 73. *Jestliže $\mathbb{F} \neq \mathbb{Z}_2$,$\mathbb{Z}_3$, derivovanou podgrupou grupy $PSL_2(\mathbb{F})$ je opět $PSL_2(\mathbb{F})$.*

Důkaz. Pro $a \in \mathbb{F}^*$ a $b \in \mathbb{F}$ máme

$$a^2x \circ (x+b) \circ (a^2x)^{-1} \circ (x+b)^{-1} = x + (a^2-1)b.$$

Je-li $\mathbb{F} \neq \mathbb{Z}_2$,$\mathbb{Z}_3$, existuje $a \in \mathbb{F}^*$ takové, že $a^2 \neq 1$. Prvek $x + f$ pak dostaneme jako komutátor prvků a^2x a $x + b$, kde $b = f(a^2-1)^{-1}$.

Dále platí

$$a^{-2}x \circ \frac{x}{bx+1} \circ (a^{-2}x)^{-1} \circ \left(\frac{x}{bx+1}\right)^{-1} = \frac{x}{(a^2-1)bx+1}.$$

Pokud tedy opět $\mathbb{F} \neq \mathbb{Z}_2$,$\mathbb{Z}_3$, prvek $\frac{x}{fx+1}$ je roven komutátoru prvků $a^{-1}x$ a $\frac{x}{bx+1}$, kde $b = f(a^2-1)^{-1}$.

Každý prvek množiny z předchozího lemmatu tudíž můžeme vyjádřit jako komutátor prvků $PSL_2(\mathbb{F})$, a protože tato množina generuje $PSL_2(\mathbb{F})$, dostáváme, že $(PSL_2(\mathbb{F}))' = PSL_2(\mathbb{F})$.

□

Lemma 74. *Množina $\mathcal{M} = \{LML^{-1} \mid L \in PSL_2(\mathbb{F}), M \in PSL_2(\mathbb{F})_\infty\}$ generuje grupu $PSL_2(\mathbb{F})$.*

Důkaz. Dokážeme, že kterýkoliv prvek $PSL_2(\mathbb{F})$ lze vyjádřit jako součin prvků z $\mathcal{M}$.

Nechť K je prvek $PSL_2(\mathbb{F})$.

Nejdříve předpokládejme, že K má alespoň jeden pevný bod. Označme onen pevný bod jako f. Podle Lemmatu 6 jsou každé dva stabilizátory bodu v $PSL_2(\mathbb{F})$ konjugované. Nalezneme $L \in PSL_2(\mathbb{F})$ takové, že $PSL_2(\mathbb{F})_f = LPSL_2(\mathbb{F})_\infty L^{-1}$. Pak $K = LML^{-1}$ pro nějaké $M \in PSL_2(\mathbb{F})_\infty$.

Nyní uvažujme případ, kdy K nemá pevný bod. Zvolme $e \in \mathbb{F} \cup \{\infty\}$. Označme $K(e) = f$. Nechť N je prvek $PSL_2(\mathbb{F})$ s alespoň jedním pevným bodem takový, že $N(e) = f$ (takové N existuje, neboť $PSL_2(\mathbb{F})$ je 2-tranzitivní). Pak f je pevným bodem prvku KN^{-1}. Podle předchozího odstavce platí N,$KN^{-1} \in \mathcal{M}$. Tedy máme, co jsme chtěli, jelikož $K = (KN^{-1})N$.

□

Lemma 75. *Grupa $PSL_2(\mathbb{F})_\infty$ je řešitelná.*

Důkaz. Určíme komutátor prvků $c^2x + b$,$e^2x + f \in PSL_2(\mathbb{F})_\infty$:

$$(c^2x + b) \circ (e^2x + f) \circ (c^2x + b)^{-1} \circ (e^2x + f)^{-1} = x + (f - b)(e^2 - 1).$$

Prvky $(PSL_2(\mathbb{F})_\infty)'$ jsou tedy tvaru $x+d$. Grupa $\{x+d \mid d \in \mathbb{F}\}$ je abelovská, tudíž $(PSL_2(\mathbb{F})_\infty)'' = \{x\}$.

□

Tvrzení 76. *Ať $\mathbb{F} \neq \mathbb{Z}_2$,$\mathbb{Z}_3$. Pak je grupa $PSL_2(\mathbb{F})$ jednoduchá.*

Důkaz. Podle Tvrzení 71 a 73 můžeme použít Lemma 14 pro $G = PSL_2(\mathbb{F})$, $x = \infty$, $H = PSL_2(\mathbb{F})_\infty$. Platnost prvního bodu z Lemmatu 14 je triviální. Platnost zbylých dvou dávají Lemmata 74 a 75.

□

Závěr

Grupy $PGL_2(\mathbb{F})$ a $PSL_2(\mathbb{F})$ jsou frekventovaným matematickým objektem. Ke klasickým výsledkům patří úplný popis podgrup $PSL_2(\mathbb{F})$ pro konečné těleso $\mathbb{F}$ (uvedeno například v [5]). To by bylo jedním z možných pokračování této práce. Singerovy cykly existují v $PGL_n(\mathbb{F})$ pro každé $n \geq 2$ a konečné $\mathbb{F}$. Jejich existence se dokazuje pomocí rozšíření $\mathbb{F}$ na $\mathbb{F}^n$. Mohlo by být zajímavé zjistit, zda existenci Singerova cyklu v případě $n \geq 3$ je možno zjistit způsobem podobným tomu, který je v této práci uveden pro $n = 2$.

Seznam použité literatury

[1] Alperin, J. L.; Bell, Rowen B. *Graduate Texts in Mathematics: Groups and Representations*. Springer-Verlag, 1995. ISBN 0-387-94526-1.

[2] Drápal, Aleš; *Teorie grup — základní aspekty*. Karolinum, Praha 2009

[3] Stanovský, David; *Učební text algebra 2021/2022*. Online. Naposledy změněno 17. června 2022. Dostupné z: https://www2.karlin.mff.cuni.cz/ stanovsk/vyuka/2122/algebra22.pdf. [Citováno 2022-10-05].

[4] Kala, Vítězslav; *Úvod do komutativní algebry*. Online. Naposledy změněno 5. ledna 2023. Dostupné z: http://karlin.mff.cuni.cz/ kala/files/UKA22.pdf. [Citováno 2023-02-23].

[5] Huppert, Bertram. *Endliche Gruppen I*. Springer Berlin, Heidelberg, 2011. ISBN 978-3-642-64982-0.