KŪNŲ TEORIJA

2000 metų rudens paskaitos

1. Kūnų plėtiniai

2. Galua grupės

3. Polinomų Galua grupės

4. Mažos eilės grupių klasifikacija

5. Fundamentalioji teorema

Norint skaičiuoti sudėtingesnes Galua grupes reikia įrodyti pagrindinę Galua teorijos teoremą.

Teorema 5.1 (Fundamentalioji Galua teorijos teorema, I dalis) *Tegu F/K yra baigtinio laipsnio Galua plėtinys. Egzistuoja abipus vienareikšmė atitiktis tarp tarpinių kūnų aibės ir grupės* $\mathrm{Gal}(F/K)$ *pogrupių aibės, reiškiamos priskirimu $E \to E' <$ $\mathrm{Gal}(F/K)$ su visais tarpiniais kūnais E. Su visais tarpiniais kūnais $E \subseteq L$ teisinga $[L : E] = [E' : L']$.*

Pastebėsime, kad pagal Teoremą 2.4 , norint gauti norimą atitiktį, pakanka įrodyti, kad su kiekvienu tarpiniu kūnu E teisinga $[E'' : E] = 1$ ir su kiekvienu pogrupiu $H <$$\mathrm{Gal}(F/K)$ teisinga $[H'' : H] = 1$. Pradėsime nuo nelygybių tarp šių laipsnių.

Lema 5.2 *Tegu F/K yra baigtinio laipsnio Galua plėtinys. Su visais pogrupiais $H < J <$$\mathrm{Gal}(F/K)$ teisinga nelygybė $[H' : J'] \leq [J : H]$.*

Įrodymas. Tegu $n = [J : H]$ ir turime $n+1$ elementą $u_1, ..., u_{n+1} \in H'$. Norime parodyti, kad šie elementai yra tiesiškai priklausomi virš J'. Neapribojant bendrumo, galima tarti, kad $u_i \neq 0$ su visais $i = 1, ..., n+1$, nes priešingu atveju sistema $u_1, ..., u_{n+1}$ būtų tiesiškai priklausoma jau ir be įrodymo.

Tegu grupės J visi kairieji sluoksniai pogrupio H atžvilgiu yra: $H, \tau_2 H, ..., \tau_n H$ ir tegu $\tau_1 = \mathrm{id}_F$. Nagrinėkime n lygčių su $n+1$ nežinomaisiais homogeninę tiesinių lygčių sistemą

$$\begin{array}{c} \tau_1(u_1)x_1+\cdots+\tau_1(u_{n+1})x_{n+1}=0 \\ \tau_2(u_1)x_1+\cdots+\tau_2(u_{n+1})x_{n+1}=0 \\ \cdots \\ \tau_n(u_1)x_1+\cdots+\tau_n(u_{n+1})x_{n+1}=0 \end{array} \qquad (1)$$

Ši sistema visada turi nenulinį sprendinį kūne H'. Pastebėsime, kad norint įrodyti lemą, reikia parodyti, kad egzistuoja nenulinis sistemos sprendinys kūne J'. Tikrai, kiekvienas toks sprendinys $x_1=c_1,...,x_{n+1}=c_{n+1}$ tenktų pirmąją sistemos lygtį : $\tau_1(u_1)c_1+\cdots+\tau_1(u_{n+1})c_{n+1}=u_1c_1+\cdots+u_{n+1}c_{n+1}=0$, o tai ir reikštų, kad sistema $u_1,...,u_{n+1}$ yra tiesiškai priklausoma.

Tegu $x_1=c_1,...,x_{n+1}=c_{n+1}$ yra *mažiausiai* turintis nenulinių c_j nenulinis sistemos (1) sprendinys. Neapribojant bendrumo, galima tarti, kad $c_1,...,c_r$ yra nelygūs nuliui, o $c_{r+1}=\cdots=c_{n+1}=0$. Beto, tegu $c_1=1$.

Su kiekvienu $\sigma\in J$ turime, kad kairieji sluoksniai $\sigma\tau_1H,\sigma\,\tau_2H,...,\sigma\tau_nH$ sudaro visų kairiųjų sluoksnių sistemą, nes jeigu $\sigma\tau_iH=\sigma\,\tau_jH$, tai $\sigma\tau_i=\sigma\,\tau_jh\Rightarrow\tau_i=\tau_jh$ ir todėl būtų $\tau_iH=\tau_jH$. Bet tai yra teisinga tik tada, kai $i=j$. Taigi, $\{H,\tau_2H,...,\tau_nH\}=\{\sigma\tau_1H,\sigma\tau_2H,...,\sigma\tau_nH\}$ su kiekvienu $\sigma\in J$. Todėl su kiekvienu $1\leq i\leq n$ egzistuoja toks $1\leq k_i\leq n$, kad $\sigma\tau_iH=\tau_{k_i}H$, t.y. $\sigma\tau_i\in\tau_{k_i}H$. Gavome, kad su kiekvienu $1\leq j\leq n+1$ ir $u_j\in H'$ turime $\sigma\tau_i(u_j)=\tau_{k_i}h(u_j)=\tau_{k_i}(u_j)$, čia $h\in H$.

Su kiekvienu $1\leq i\leq n$ iš sistemos (1) turime, kad

$0=\sigma(\tau_i(u_1)c_1+\cdots+\tau_i(u_{n+1})c_{n+1})=\sigma\tau_i(u_1)\sigma(c_1)+\cdots+\sigma\tau_i(u_{n+1})\sigma(c_{n+1})$.
Gavome, kad elementai $x_1=\sigma(c_1)=\sigma(1)=1,x_2=\sigma(c_2),...,x_{n+1}=\sigma(c_{n+1})$

yra sistemos

$$\begin{array}{c} \tau_{k_1}(u_1)x_1+\cdots+\tau_{k_1}(u_{n+1})x_{n+1}=0 \\ \tau_{k_2}(u_1)x_1+\cdots+\tau_{k_2}(u_{n+1})x_{n+1}=0 \\ \cdots \\ \tau_{k_n}(u_1)x_1+\cdots+\tau_{k_n}(u_{n+1})x_{n+1}=0 \end{array} \qquad (2)$$

sprendinys.

Kadangi $\{\tau_{k_1},...,\tau_{k_n}\}$ yra pilnoji kairiųjų sluoksnių H atžvilgiu sistema, t.y. $\{\tau_{k_1}H,...,\tau_{k_n}H\}=\{\tau_1H,\tau_2H,...,\tau_nH\}$, tai $\{\tau_{k_1},...,\tau_{k_n}\}=\{\tau_1,\tau_2,...,\tau_n\}$. Tai reiškia, kad sistemos (1) ir (2) sutampa ir $x_1=\sigma(c_1)=\sigma(1)=1,x_2=\sigma(c_2),...,x_{n+1}=\sigma(c_{n+1})$ yra (1) sistemos sprendinys.

Homogeninės sistemos (1) sprendiniu bus taip pat ir $x_1=c_1\Leftrightarrow\sigma(c_1)=0,x_2=c_2\Leftrightarrow\sigma(c_2),...,x_r=c_r\Leftrightarrow\sigma(c_r),x_{r+1}=c_{r+1}\Leftrightarrow\sigma(c_{r+1})=0,...,x_n=c_n\Leftrightarrow\sigma(c_n)=0$. Šiame sprendinyje yra mažiau negu r nenulinių skaičių, todėl jis turėtų būti nuliniu

sprendiniu: $x_1 = \cdots = x_n = 0$, t.y. su visais $1 \leq i \leq n+1$ teisinga $\sigma(c_i) = c_i$. Kitais žodžiais sakant, $c_1, ..., c_{n+1} \in J'$ ir todėl sistema $\{u_1, ..., u_{n+1}\}$ yra tiesiškai priklausoma virš J'.

Įrodyta.

Teoremos 5.1 įrodymas. Norint gauti abipus vienareikšmę atitiktį tarp tarpinių kūnų ir grupės $\mathrm{Gal}(F/K)$ pogrupių pagal Teoremą 2.4 pakanka parodyti, kad visi tarpiniai kūnai ir visi pogrupiai yra uždari.

Tegu E yra tarpinis kūnas. Pagal Teiginį (6) turime, kad $E \subseteq E''$. Bet plėtinys F/K yra Galua plėtinys, $K = K''$, todėl pagal Lemas 3.4 ir 5.2 turime, kad $[E'' : K] \geq [E : K] \geq [K' : E'] \geq [E'' : K''] = [E'' : K]$. Iš čia pagal Teoremą 1.8 turime $[E'' : E] = \dfrac{[E'' : K]}{[E : K]} = 1$ ir todėl $E'' = E$, t.y. E yra uždaras.

Tegu dabar $H < \mathrm{Gal}(F/K)$. Iš Teiginių (1), (3) ir (6) turime, kad $\langle \mathrm{id}_F \rangle$ yra uždaras ir $H < H''$. Pagal Lemas 3.4 ir 5.2 turime, kad $[H'' : \langle \mathrm{id}_F \rangle] \geq [H : \langle \mathrm{id}_F \rangle] \geq \left[\langle \mathrm{id}_F \rangle' : H'\right] \geq \left[H'' : \langle \mathrm{id}_F \rangle''\right] = [H'' : \langle \mathrm{id}_F \rangle]$. Iš čia pagal Lagranžo teoremą turime $[H'' : H] = \dfrac{[H'' : \langle \mathrm{id}_F \rangle]}{[H : \langle \mathrm{id}_F \rangle]} = 1$ ir todėl $H'' = H$, t.y. H yra uždaras.

Pagaliau, su bet kuriais tarpiniais kūnais $L \subseteq E$ turime, kad $[E : L] \geq [L' : E'] \geq [E'' : L''] = [E : L]$ ir todėl $[E : L] = [L' : E']$.

Įrodyta.

Iš teoremos mes matome, kad, norint tirti Galua plėtinio Galua grupę, reikia mokėti kiekvienam tarpiniam kūnui priskirti plėtinio Galua grupės pogrupį. Šis priskirimas palengvina taip pat ir polinomo Galua grupės radimą.

Pavyzdys. Rasime kūno $F = \mathbf{Q}\left(i, \sqrt{2}\right)$ Galua grupę virš $\mathbf{Q}$ ir visus plėtinio $F/\mathbf{Q}$ tarpinius kūnus. Aišku, kad $x^2 + 1$ yra minimalusis i polinomas, o $x^2 \Leftrightarrow 2$ yra minimalusis $\sqrt{2}$ polinomas. Iš čia turime, kad kūnas F yra polinomo $f(x) = (x^2 + 1)(x^2 \Leftrightarrow 2) = x^4 \Leftrightarrow x^2 \Leftrightarrow 2$ skaidymo kūnas ir todėl $\mathrm{Gal}(F/\mathbf{Q})$ yra polinomo $f(x)$ Galua grupė.

Kiekvienas grupės $\mathrm{Gal}(F/\mathbf{Q})$ elementas Θ yra kūno F automorfizmas virš $\mathbf{Q}$ ir todėl yra polinomo $f(x)$ šaknų $\sqrt{2}, \Leftrightarrow\sqrt{2}, i$ ir $\Leftrightarrow i$ keitinys. Galimi 4 variantai: $\Theta\left(\sqrt{2}\right) = \pm\sqrt{2}$; $\Theta(i) = \pm i$.

1) $\Theta_1\left(\sqrt{2}\right) = \sqrt{2}$; $\Theta_1(i) = i$.

2) $\Theta_2\left(\sqrt{2}\right) = \sqrt{2}$; $\Theta_2(i) = \Leftrightarrow i$.

3) $\Theta_3\left(\sqrt{2}\right) = \Leftrightarrow\sqrt{2}$; $\Theta_3(i) = i$.

4) $\Theta_4\left(\sqrt{2}\right) = \Leftrightarrow\sqrt{2}$; $\Theta_4(i) = \Leftrightarrow i$. Pastebėsime, kad $\Theta_4 = \Theta_3\Theta_2$.

Taigi, grupės $\mathrm{Gal}(F/\mathbf{Q})$ veiksmų lentelė yra

$\circ$	Θ_1	Θ_2	Θ_3	Θ_4
Θ_1	Θ_1	Θ_2	Θ_3	Θ_4
Θ_2	Θ_2	Θ_1	Θ_4	Θ_3
Θ_3	Θ_3	Θ_4	Θ_1	Θ_2
Θ_4	Θ_4	Θ_3	Θ_2	Θ_1

Matome, kad ši lentelė sutampa su grupės $\mathbf{Z}_2 \times \mathbf{Z}_2$ veiksmų lentele:

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,0)$	$(1,0)$	$(0,1)$	$(0,0)$

Taigi $\mathrm{Gal}(F/\mathbf{Q}) \approx \mathbf{Z}_2 \times \mathbf{Z}_2$. Grupėje $\mathrm{Gal}(F/\mathbf{Q})$ yra trys netrivialūs pogrupiai: $A = \{\Theta_1, \Theta_2\} = \langle\Theta_2\rangle$, $B = \{\Theta_1, \Theta_3\} = \langle\Theta_3\rangle$ ir $C = \{\Theta_1, \Theta_4\} = \langle\Theta_4\rangle$ ir todėl $A' = \mathbf{Q}\left(\sqrt{2}\right)$, $B' = \mathbf{Q}(i)$ ir $C' = \mathbf{Q}\left(\sqrt{2}\cdot i\right)$. Pagal Fundamentaliosios teoremos I dalį tai ir yra visi plėtinio $\mathbf{Q}\left(i, \sqrt{2}\right)/\mathbf{Q}$ tarpiniai kūnai. Visi šie tarpiniai kūnai yra Galua kūnai virš $\mathbf{Q}$: $A'' = \left(\mathbf{Q}\left(\sqrt{2}\right)\right)' = \mathrm{Gal}\left(\mathbf{Q}\left(\sqrt{2}\right)/\mathbf{Q}\right) = A$, $B'' = (\mathbf{Q}(i))' = \mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q}) = B$ ir $C'' = \left(\mathbf{Q}\left(\sqrt{2}\cdot i\right)\right)' = \mathrm{Gal}\left(\mathbf{Q}\left(\sqrt{2}\cdot i\right)/\mathbf{Q}\right) = C$. Pastebėsime, kad visos grupės A, B, C yra izomorfinės vienintėlei grupei iš 2 elementų $\mathbf{Z}_2$.

Kita išvada yra ta, kad su kiekvienu Galua plėtiniu F/K ir kiekvienu tarpiniu kūnu E teisinga $E = \mathrm{Gal}(F/E)'$. Bet ką galėtume pasakyti apie $\mathrm{Gal}(E/K)$? Sunkumai kyla jau ir todėl, kad kūnas E gali nebūti kūno K Galua plėtinys. Pavyzdžiui, nagrinėjant kūnų grandinę $\mathbf{Q} \subset \mathbf{Q}\left(\sqrt[3]{5}\right) \subset F$, čia $F \Leftrightarrow$ polinomo $x^3 \Leftrightarrow 5 \in \mathbf{Q}[x]$ skaidymo kūnas, matome, kad $\mathbf{Q}\left(\sqrt[3]{5}\right)/\mathbf{Q}$ nėra Galua plėtinys, nes $\left(\mathrm{Gal}\left(\mathbf{Q}\left(\sqrt[3]{5}\right)/\mathbf{Q}\right)\right)' = \left(\langle\ \mathrm{id}_{\mathbf{Q}\left(\sqrt[3]{5}\right)}\ \rangle\right)' = \mathbf{Q}\left(\sqrt[3]{5}\right) \neq \mathbf{Q}$. Antroji Fundamentaliosios teoremos dalis yra skirta kaip tik šiai problemai spręsti.

Tegu E yra plėtinio F/K tarpinis kūnas. Sakysime, kad E yra **stabilus** F/K atžvilgiu, jeigu su visais $\sigma \in \mathrm{Gal}(F/K)$ teisinga $\sigma(E) \subseteq E$. Tai tarp kitko reiškia ir tai, kad apribojus σ apibrėžimo sritį kūnu E gauname E automorfizmą, kurio atvirkštinis yra σ^{-1} siaurinys kūne E.

Lema 5.3 *Tegu F/K yra kūno plėtinys, o E - stabilus tarpinis kūnas. Egzistuoja homomorfizmas $\Psi : \mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K)$, kurio $\ker \Psi = E' = \mathrm{Gal}(F/E)$.*

Įrodymas. Su visais $\sigma \in \mathrm{Gal}(F/K)$ apibrėžkime $\Psi(\sigma) = \sigma|_E$. Kūnas E yra stabilus, todėl $\Psi(\sigma) \in \mathrm{Gal}(E/F)$. Aišku, kad taip apibrėžtas Ψ yra homomorfizmas(patikrinkit!). Pagaliau, $\sigma \in \ker(\Psi) \Leftrightarrow \sigma|_E = \mathrm{id}_E \Leftrightarrow \sigma \in E'$.

Įrodyta.

Lema 5.4 *Tegu F/K yra kūno plėtinys.*

1. Jeigu E yra stabilus tarpinis kūnas, tai E' yra normalusis $Gal(F/K)$ pogrupis $E' \lhd Gal(F/K)$.

2. Jeigu $H \lhd Gal(F/K)$, tai H' yra stabilus tarpinis kūnas.

Įrodimas. 1. Iš Lemos 5.3 mes žinome, kad $E' = \ker \Psi$, o kiekvieno homomorfizmo branduolys yra normalusis pogrupis.

2. Tegu $\sigma \in \mathrm{Gal}(F/K)$ ir $u \in H'$. Tada su visais $\tau \in H$ turime $\sigma^{-1}\tau\sigma \in H$ ir todėl $\sigma^{-1}\tau\sigma(u) = u$. Iš čia $\tau(\sigma(u)) = \sigma(u)$ ir todėl $\sigma(u) \in H'$, t.y. H' yra stabilus tarpinis kūnas.

Įrodyta.

Teorema 5.5 (Fundamentalioji Galua teorijos teorema, II dalis) *Tegu F/K yra baigtinio laipsnio Galua plėtinys. Tada F yra Galua kūnas virš bet kurio tarpinio kūno E. Savo ruožtu, kūnas E yra Galua kūnas virš K tada ir tik tada, kada $E' \lhd \mathrm{Gal}(F/K)$. Šiuo atveju $\mathrm{Gal}(E/K) \approx \mathrm{Gal}(F/K)/E'$.*

Įrodymas. Iš Fundamentaliosios Teoremos I dalies mes žinome, kad kiekvienas tarpinis kūnas E yra uždaras, todėl F yra Galua kūnas virš E. Jeigu $E' \lhd \mathrm{Gal}(F/K)$, tai $E = E''$ yra stabilus tarpinis kūnas(Lema 5.4, 2). Dabar belieka parodyti, kad grupės $\mathrm{Gal}(E/K)$ nekintantis kūnas yra K : $(\mathrm{Gal}(E/K))' = K$. Tegu $u \in E$ ir $u \notin K$. Tada egzistuoja toks $\sigma \in \mathrm{Gal}(F/K)$, kad $\sigma(u) \neq u$ ir todėl $\Psi(\sigma)(u) \neq u$, čia $\Psi : \mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K)$ homomorfizmas iš Lemos 5.3 ir $\Psi(\sigma) \in \mathrm{Gal}(E/K)$. Gavome, kad grupės $\mathrm{Gal}(E/K)$ nekintantis kūnas yra K

ir todėl E yra Galua kūnas virš K.

Atvirkščiai, jeigu E yra Galua kūnas virš K, tai pagal Lemą 5.4 pakanka parodyti, kad E yra stabilus. Tegu $u \in E$. Elementas u yra algebrinis, nes $[E:K]$ yra baigtinis (Teorema 1.7) ir tegu u minimalusis polinomas yra $p \in K[x]$. Tegu $u = u_1, u_2, ..., u_r$ yra skirtingos polinomo p šaknys kūne E. Aišku, kad $1 \leq r \leq n = \deg(p)$ ir pagal Teoremą 2.2 kiekvienas $\tau \in \mathrm{Gal}(E/K)$ yra šaknų $u_1, u_2, ..., u_r$ keitinys. Todėl unitaraus polinomo $g(x) = (x \Leftrightarrow u_1)(x \Leftrightarrow u_2) \cdots (x \Leftrightarrow u_r)$ koeficientai yra stabilūs su kiekvienu $\tau \in \mathrm{Gal}(E/K)$, taigi $g(x) \in K[x]$. Turime, kad $g(u) = 0 \Rightarrow g \in \ker(\phi_u) = \langle p \rangle$, taigi $\deg(g) \leq \deg(p)$. Bet abu polinomai yra unitarūs, todėl $g = p$ ir beto polinomo p visos šaknys yra skirtingos ir yra kūno E elementais. Iš čia aišku, kad su visais $\sigma \in \mathrm{Gal}(F/K)$ $\sigma(u)$ yra polinomo p šaknis, taigi $\sigma(u) \in E$. Tai ir rodo, kad E yra stabilus ir todėl $E' \lhd \mathrm{Gal}(F/K)$.

Pagaliau, jeigu E yra Galua kūnas virš K, tai parodysime, kad $\mathrm{Gal}(E/K) \approx \mathrm{Gal}(F/K)/E'$. Iš Lemos 5.3 ir Izomorfizmo Teoremos grupėms pakanka parodyti, kad Ψ yra siurjekcija. Iš Fundamentaliosios Teoremos I dalies mes žinome $|\mathrm{Gal}(F/K)/E'| = [\mathrm{Gal}(F/K) : E'] = [E:K] = |\mathrm{Gal}(E/K)|$, taigi $\mathrm{Im}(\Psi) = \mathrm{Gal}(E/K)$ ir todėl $\mathrm{Gal}(E/K) \approx \mathrm{Gal}(F/K)/E'$.

Įrodyta.

Išvada 5.6 *Tegu F/K yra baigtinis Galua plėtinys, o $p \in K[x]$ yra neredukuojamas polinomas. Jeigu kūne F yra nors viena polinomo p šaknis, tai visos polinomo p šaknys yra skirtingos ir yra kūne F.*

Ši išvada pateisina apibrėžimą.

Apibrėžimas 5.7 *Tegu K yra kūnas. Polinomas $f \in K[x]$ vadinamas* **separabiliuoju**, *jeigu visų jo neredukuojami daugikliai turi skirtingas šaknis, kurios yra polinomo f skaidymo kūne. Kūnas K vadinamas* **tobuluoju**, *jeigu visi žiedo $K[x]$ polinomai yra separabilieji. Algebrinis plėtinys F/K vadinamas* **separabiliuoju**, *jeigu visų kūno F elementų minimalieji polinomai yra separabilieji. Algebrinis plėtinys F/K vadinamas* **normaliuoju**, *jeigu su kiekvienu $u \in F$, kūne F yra elemento u minimalaus polinomo skaidymo kūnas.*

Taigi, jeigu $f \in K[x]$ yra neredukuojamas $n\Leftrightarrow$ojo laipsnio polinomas, turintis šaknį kūne F, tai

$$\left.\begin{array}{rcl} F/K \text{ - separabilusis} & \Rightarrow & f\text{šaknys yra skirtingos} \\ F/K \text{ - normalusis} & \Rightarrow & F \text{ yra } f \text{ skaidinio kūnas} \end{array}\right\} \Rightarrow \begin{array}{c} f \text{ turi } n \text{ skirtingų} \\ \text{šaknų} \end{array}.$$

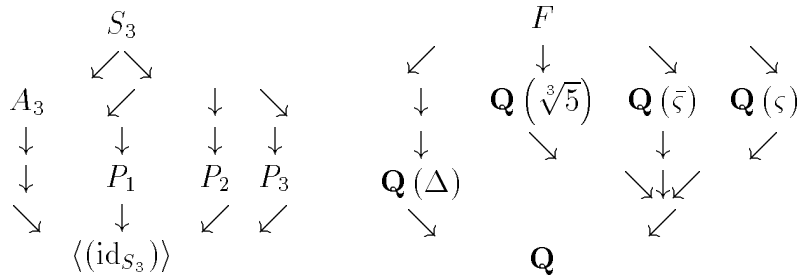
Pavyzdžiai. 1. Kūnas $\mathbf{Q}\left(\sqrt[3]{2}\right)$ yra separabilusis, bet ne normalusis virš $\mathbf{Q}$, nes $\mathbf{Q}\left(\sqrt[3]{2}\right)$ nėra polinomo $x^3 \Leftrightarrow 2$ skaidinio kūnas.

2. Kūnas $GF(p)(u)$ yra normalusis, bet ne separabilusis virš $GF(p)$, nes tai yra neseparabilaus polinomo $x^p \Leftrightarrow u^p$ skaidinio kūnas.

Dabar galime performuluoti Išvadą 5.6: *kiekvienas baigtinis Galua plėtinys yra normalusis separabilusis plėtinys.* Kitame skyrelyje mes parodysime, kad teisingas ir atvirkščias teiginys.

Baigdami šį skyrelį, grįžkime prie polinomo $x^3 \Leftrightarrow 5$ skaidymo kūno virš $\mathbf{Q}$.

Pavyzdys. Naudodamiesi Fundamentaliąja Galua teorijos teorema, mes aprašysime visus plėtinio $F/\mathbf{Q}$ tarpinius kūnus, čia $F \Leftrightarrow$ polinomo $x^3 \Leftrightarrow 5$ skaidymo kūnas. Naudosime aukščiau apibrėžtus žymenis. Išvardinsime visus grupės $S_3 = \langle \sigma, \tau \rangle$ pogrupius. Visų pirma tai alternuojanti grupė $A_3 = \langle \sigma \rangle$. Tai normalusis pogrupis, nes $\tau\sigma\tau^{-1} = \sigma^{-1} \in A_3$. Kiti grupės pogrupiai - tai 2 -osio eilės ciklinės grupės $P_1 = \langle \tau \rangle$, $P_2 = \langle \sigma\tau \rangle$ ir $P_3 = \langle \sigma^2\tau \rangle$. Pagal Fundamentaliąją Galua teorijos teoremą egzistuoja lygiai keturi tarpiniai kūnai, virš kurių šie pogrupiai yra pastovūs. Iš visų šių tarpinių kūnų tik A_3' yra Galua kūnas virš $\mathbf{Q}$ ir plėtinio $A_3'/\mathbf{Q}$ laipsnis turi būti lygus $[S_3 : A_3] = 2$. Grupės S_3 pogrupius ir juos atitinkančius tarpinius kūnus pavaizduosime diagramomis:



čia $\Delta = \left(\sqrt[3]{5} \Leftrightarrow \varsigma\right)\left(\sqrt[3]{5} \Leftrightarrow \bar{\varsigma}\right)(\varsigma \Leftrightarrow \bar{\varsigma})$. Iš visų tarpinių kūnų tik $\mathbf{Q}(\Delta)$ yra Galua kūnas virš $\mathbf{Q}$ ir $\mathrm{Gal}(\mathbf{Q}(\Delta)/\mathbf{Q}) = \left\langle \tau|_{\mathbf{Q}(\Delta)} \right\rangle \approx \mathbf{Z}_2$.