Korpused

Sven Laur

Sisukord

Peatükk 1

Korpuste laiendamine

1.1 Korpused ja nende laiendid

Definitsioon 1.1.1. *Korpuse K karakteristikaks* $\operatorname{kar} K$ *nimetatakse ühikelemendi poolt genereeritud alamkorpuse elementide arvu, kui* $\langle 1 \rangle$ *on lõplik ja 0 vastasel korral.*

Järeldus 1.1.1.1. *Kui korpuse K karakteristika on* $\operatorname{kar} K = 0$*, siis leidub injektsioon Ψ korpus* $\mathbb{Q} \overset{\Psi}{\hookrightarrow} K$

Järeldus 1.1.1.2. *Kui korpus K ei sisalda ratsionaalarvude korpust $\mathbb{Q}$, siis* $\operatorname{kar} K \in \mathbb{P}$.

Definitsioon 1.1.2. *Olgu meil korpused $K \subseteq L$, siis korpust L nimetatakse korpuse K laiendiks ja seda tähistatakse $L : K$. Korpus L loomulikul viisil vektorruum üle K. Vektoruumi mõõdet $[L : K] := \dim L : K$ nimetatakse laiendi astmeks.*

Definitsioon 1.1.3. *Korpuste laiendi $L : K$ elementi α nimetatakse transtsendentseks kui elementide süsteem $(\alpha^i)_{i=0}^{\infty}$ on lineaarselt sõltumatu. Elementi α nimetatakse algebraliseks, kui leidub polünoom $f \in K[X] \setminus \{0\}$ nii, et $f(\alpha) = 0$.*

Teoreem 1.1.1 (Dimensiooni teoreem)**.** *Olgu meil korpuste laiendid $K : L$ ja $F : L$, siis laiendi $F : K$ mõõde avaldub $[F : K] = [F : L] \cdot [L : K]$.*

Tõestus. Kui ühe laiendi mõõde on lõpmatu, siis peab seda olema ka laiendi $F : K$ mõõde, seega on tarvis vaadata vaid lõplikke laiendeid. Olgu L baas K suhtes $(\alpha_i)_{i=1}^n$ ja F baas L suhtes $(\beta_j)_{j=1}^m$. Vaatleme nüüd vektorite süsteemi $\delta_{i,j} = \alpha_i \beta_j$. Olgu meil lineaarkombimatsioon $\sum_{i=1}^n \sum_{j=1}^m \kappa_{i,j} \delta_{i,j} = 0$, siis saame avaldada

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} \kappa_{i,j} \alpha_i \right) \beta_j = 0 \qquad \Rightarrow \qquad \sum_{i=1}^{n} \kappa_{i,j} \alpha_i = 0, \qquad j = 1, 2, \ldots, m.$$

Kuna $(\alpha_i)_{i=1}^n$ on lineaarselt sõltumatud, siis $\kappa_{i,j} = 0$. Seega süsteem $(\delta_{i,j})_{i=1}^n{}_{j=1}^m$ on vektorrumi F baas K suhtes, kuna see on moodustajate süsteem.

Definitsioon 1.1.4. *Olgu meil korpuste laiend $L : K$ ja $\alpha \in L$, siis elemendi α adjugeerimisel korpusele K saadakse korpus $K(\alpha)$, mis on vähim korpus, mis sisaldab endas korpust K ja elementi α.*

Lause 1.1.2. *Elementide adjugeerimine korpusele K on assotsiatiivne ning kommutatiivne.*

Definitsioon 1.1.5. *Korpuse K ja transtsendentse elemendi t ratsionaalavaldiste korpuseks nimetatakse hulka*

$$K(t) = \left\{ \frac{p(t)}{q(t)} \,\middle|\, p, q \in K[X] \text{ ja } q \neq 0 \right\},$$

millel korrutamine ja jagamine on defineeritud analoogselt murdudega st. tehted on defineeritud ekvivalentsi klassidel.

Tõestus. Definitsioon on korrektne.

Definitsioon 1.1.6. *Korpuste laiendit $L : K$ nimetatakse lihtsaks parajasti siis, kui leidub $\alpha \in L$ nii, et $L = K(\alpha)$.*

Lause 1.1.3. *Kui korpuste laiendi $L : K$ aste on lõplik, siis kõik elemendid on algebralised üle K.*

Definitsioon 1.1.7. *Korpuste laiendit $L : K$ nimetatakse algebraliseks parajasti siis, kui kõik L elemendid on algebralised üle K.*

Definitsioon 1.1.8. *Korpuste laiendid $L_1 : K$ ja $L_2 : K$ on isomorfsed parajasti siis, kui leidub bijektiivne homomorfism $\Phi : L_1 \to L_2$, mille ahend $\Phi|_K = I_K$.*

Teoreem 1.1.4. *Kui s ja t on transtsendentsed elemendid üle K, siis ratsionaalavaldiste korpused $K(s)$ ja $K(t)$ on isomorfsed.*

Tõestus. Defineerime isomorfismi $\Phi : K(s) \to K(t)$ järgnevalt $\Phi\left(\frac{p(s)}{q(s)}\right) = \frac{p(t)}{q(t)}$. Definitsioon on korrektne, sest kui

$$\frac{p_1(s)}{q_1(s)} = \frac{p_1(s)}{q_1(s)} \qquad \Leftrightarrow \qquad p_1 q_2 = p_2 q_1 \qquad \Leftrightarrow \qquad \frac{p_1(t)}{q_1(t)} = \frac{p_1(t)}{q_1(t)}.$$

On ilmne, et Φ on sürjektiivne homomorfism. Olgu $\Phi\left(\frac{p(s)}{q(s)}\right) = 0$, siis $p1 = 0q = 0$ ja seega $p = 0$, millest $\frac{p(s)}{q(s)} = 0$. Seega on Φ injektiivne.

1.2 Lihtsad algebralised laiendid

Definitsioon 1.2.1. *Korpuste laiendi $L : K$ algebralise elemendi $\alpha \in L$ miinimaalseks polünoomiks nimetatakse vähima astmega unitaarset polünoomi $m_\alpha \in K[X] \setminus \{0\}$, mille korral $m_\alpha(\alpha) = 0$.*

Lause 1.2.1. *Korpuste laiendi $L : K$ algebralise elemendi $\alpha \in L$ minimaalne polünoom on üheselt määratud kui unitaarne taandumatu polünoom üle korpuse K, mille juureks on α. Iga polünoom $f \in K[X]$ mille juureks on α jagub elemendi α minimaalse polünoomiga.*

TÕESTUS. Olgu meil polünoom $f \in K[X]$, mille juureks on element α, siis jagades seda minimaalse polünoomiga saame $f = qm_\alpha + r$, seega

$$0 = f(\alpha) = q(\alpha)m_\alpha(\alpha) + r(\alpha) = r(\alpha).$$

Kuna minimaalne polünoom on vähima astmega nullist erinev polünoom, siis $r = 0$. Kui m_α oleks taandumatu polünoom, siis nullitegurite puudumise tõttu polünoomide ringis $K[X]$ poleks ta vähima astmega polünoom. Kui elemendil oleks kaks minimaalset polünoomi m_α ja m'_α, siis $m_\alpha \mid m'_\alpha$ ja $m'_\alpha \mid m_\alpha$. Kui arvestada polünoomi unitaarsust, siis $m_\alpha = m'_\alpha$.

Teoreem 1.2.2 (Kroneckeri teoreem)**.** *Kui $m \in K[X]$ on taandumatu unitaarne polünoom, siis faktorring $L = K[X]/(m)$ korpus ja polünoom m omab vähemalt ühte juurt korpuses L ja leidub loomulik sisestus $K \hookrightarrow L$.*

TÕESTUS.
A. Polünoomi m on esimese astme polünoom, siis $L = K$.
B. Polünoomi aste $\deg m > 1$. Näitame, et kommutatiivne ring $L = K[X]/(m)$ on korpus. Selleks paneme tähele $\gcd(m, g) = 1$ kui $f \nmid g \Leftrightarrow \overline{g} \neq 0$. Laiendatud Eukleidese algoritm annab polünoomid $u, v \in K[X]$ nii, et $um + vg = 1 \Leftrightarrow \overline{v} \cdot \overline{g} = 1$ ja seega $\overline{v} = (\overline{g})^{-1}$. Teisalt $f(\overline{x}) = \overline{f(x)} = 0$ ja seega $\overline{x}$ polünoomi f juur. Loomulik projektsioon $\pi : K \hookrightarrow K[X]/(f)$ on injektiivne homomorfism.

Järeldus 1.2.2.1. *Olgu meil korpuste laiend $L : K$. Kui polünoom $m \in K[X]$ on taandumatu ja unitaarne ning element $\alpha \in L$ on polünoomi m juur, siis korpused $K[X]/(m)$ ja $K(\alpha)$ on isomorfsed(kui samastada K elementide klassid K elementidega korpuses $K[X]/(m)$) ja m on elemendi α minimaalne polünoom.*

TÕESTUS. Olgu $\Phi : K[X]/(m) \to K(\alpha)$ defineeritud järgnevalt $\Phi(\overline{p}) = p(\alpha)$. Definitsioon on korrektne, sest $m(\alpha) = 0$ ja seega teisenduvad erinevad esindajad üheks elemendiks. Olgu m_α elemendi α minimaalne polünoom, siis $m_\alpha \mid m$. Kuna m on taandumatu unitaarne polünoom, siis $m = m_\alpha$. Nüüd on lihtne on veenduda $\operatorname{Ker}\Phi = 0$ ja seega Φ injektsioon. Kuna Φ on sürjektsioon ja kooskõlas korpuse tehetega, siis on Φ isomorfism.

Järeldus 1.2.2.2 (Lihtsa laiendi ehitus)**.** *Korpuste laiendi $L : K$ algebralise elemendi α poolt mooduatatud lihtse laiendi $K(\alpha)$ mõõde $[K(\alpha) : K] = \deg m_\alpha$, kus m_α on elemedi α minimaalne polünoom. Iga element $\beta \in K(\alpha)$ avaldub üheselt polünoomi $f \in K[X]$ väärtustusena $f(\alpha)$, kus $\deg f < \deg m_\alpha$.*

TÕESTUS. Eelmisest teoreemist 1.2.2.1 teame $K(\alpha) \cong K[X]/(m_\alpha)$. Olgu $n = \deg m_\alpha$, siis korpuse $K[X]/(m_\alpha)$ iga klassil leidub esindaja, mille aste on väiksem n ja seega isomorfism Φ kujutab

$$K(\alpha) = \Phi\Big[K[X]/(m_\alpha)\Big] = \{f(\alpha) \mid f \in K[X], \deg f < n\}$$

Selle vektoruumi baasiks sobib $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. Süsteem on üle K lineaarselt sõltumatu, muidu poleks m_α minimaalne polünoom.

Järeldus 1.2.2.3. *Olgu meil korpuse K kaks lihtsat laiendit $K(\alpha)$ ja $K(\beta)$, siis järgnevad väited on samaväärsed:*

1. *leidub laiendite isomorfism ψ nii, et $\psi(\alpha) = \beta$;*

2. *elementide α ja β minimaalsed polünoomid on võrdsed.*

Tõestus.
$1 \Rightarrow 2$
Lihtne on veenduda $0 = \psi(m_\alpha(\alpha)) = m_\alpha(\psi(\alpha)) = m_\alpha(\beta)$, kus m_α on elemendi α minimaalne polünoom. Kuna polünoom m_α on taandumatu unitaarne polünoom, siis on see ka elemendi β minimaalne polünoom vastavalt lausele 1.2.1.
$2 \Rightarrow 1$
Siis on $K(\alpha) \cong K[X]/(m_\alpha) \cong K(\beta)$, kus m_α on α minimaalne polünoom.

1.3 Korpuste algebralised laiendid

Definitsioon 1.3.1. *Polünoomi $f \in K[X]$ lahutuskorpuseks nimetatakse korpuse K sellist laiendit, milles polünoom f lahutub lineaarteguriteks. Kitsamas mõttes on polünoomi lahutuskorpus minimaalne korpuse K laiend, milles polünoom f lahutub lineaarteguriteks*[1].

Lause 1.3.1. *Olgu $L : K$ polünoomi $f \in K[X]$ lahutuskorpus ja $(\xi_i)_{i=1}^n \subseteq L$ polünoomi kõik juured, siis minimaalne lahutuskorpus $M = K(\xi_1, \xi_2, \ldots, \xi_n)$.*

Teoreem 1.3.2. *Iga mittekonstantse polünoomil $f \in K[X]$ leidub lahutuskorpus $L : K$. Minimaalne lahutuskorpus on määratud üheselt isomorfismi täpsuseni.*

Tõestus. Lahutuskorpuse olemasolu on selge tänu teoreemile 1.2.2, kuna polünoomi juurte arv on tõkestatud polünoomi astmega.

Minimaalse lahutuskorpuse ühesuseks vaatame kahte minimaalset lahutuskorpust L ja L'. Teeme induktsiooni üle polünoomi astme. Lahutugu polünoom $f = f_1 f_2 \cdots f_r$ taandumatuteks teguriteks f_k. Kuna tegutite f_k pealiikmete kordajatega saab läbi jagada, siis võib üldsust kitsendamata eeldada, et f_k ja f on unitaarsed polünoomid. Olgu polünoomi juured kordsusi arvestades esimeses korpuses $(\xi_i)_{i=1}^n \subseteq L$ ja teises korpuses $(\zeta_j)_{j=1}^n \subseteq L'$. Olgu taandumatu tegurile f_k juured ξ_i ja ζ_j. Nüüd korpused on $K(\xi_i)$ ja $K(\zeta_j)$ on järelduse 1.2.2.1 isomorfsed

$$K(\xi_i) \cong K[X]/(f_k) \cong K(\zeta_j).$$

[1] Järgnevates peatükkides ning paragrafides mõistame polünoomi lahutuskorpust kitsamas mõttes.

Seega leidub laiendite isomorfism $\Phi : K(\xi_i) \to K(\zeta_j)$, kusjuures $\Phi(\xi_i) = \zeta_j$. Konstrueerime formaalselt korpuse L'' kui korpuse $K(\zeta_j)$ laiendi. Selleks paneme tähele, et $K(\xi_1, \xi_2, \ldots, \xi_n)$ on vektorruum üle $K(\xi_i)$. Muudame vektorite süsteemi $\xi_1, \xi_2 \ldots, \xi_n$ lineaarselt sõltumatuks arvates välja teiste kaudu avaldatavad vektorid ning täiendame siis vektorruumi baasiks $\alpha_1, \alpha_2, \ldots, \alpha_s$. See on võimalik lisades vaid juurte $\xi_{i'}$ astmeid, sest L on lõplik laiend. Definerime L'' kui vektorruumi üle $K(\zeta_j)$ võttes formaalselt vektoruumi baasiks süsteemi $\alpha_1, \alpha_2, \ldots, \alpha_s$. Defineerime nüüd vektorrumide vahelise kujutuse $\Psi : L \to L''$ järgnevalt

$$\Psi\left(\sum_{l=1}^{s} p_l \alpha_l\right) = \sum_{l=1}^{s} \Phi(p_l)\alpha_l, \text{ kus } p_l \in K(\xi_i).$$

On lihtne veenduda, et tegu on vektorruumide bijektiivse lineaarteisendusega üle korpuse K. Nüüd definerime vektorrumis L'' korrutamise järgneval viisil $a \cdot b = \Psi(\Psi^{-1}(a) \cdot \Psi^{-1}(b))$. Lihtne on veenduda, et tehe on assotsiatiivne ja kommutatiivne ning rahuldab distributiivsuse võrrandeid. Ja seega on L'' ring. Kui $a \in L''^*$, siis $\Psi^{-1}(a) \neq 0$ ja seega leidub $b \in L$ nii, et $\Psi(a)b = 1$ ja seega

$$\Psi(b)a = \Psi(\Psi^{-1}(\Psi(b))\Psi^{-1}(a)) = \Psi(b\Psi(a)) = \Psi(1) = 1.$$

Seega oleme näidanud, et L'' on korpus ja $\Psi : L \to L''$ on konstruktsiooni tõttu laiendite isomorfism. Kuna korpus L on polünoomi f lahutuskorpus, siis $f = \prod_{i'=1}^{n}(X - \xi_{i'})$, rakendades polünoomile isomorfismi Ψ saame lahutuse $f = \prod_{i'=1}^{n}\big(X - \Psi(\xi_{i'})\big)$ ning seega on L'' lahutuskorpus. Kui oletatada vastuväiteliselt, et leidub L'' pärisalamkorpus L''', mis sisaldab kõik polünoomi f juured, siis peab $\Psi^{-1}(L''') \subsetneq L$, mis on ilmne vastuolu L minimaalsusega. Kuna korpuses $K(\zeta_j)$ jagab polünoom $X - \zeta_j$ polünoomi f, siis $f = (X - \zeta_j)f'$. Et L' ja L'' on minimaalsed f' lahutuskorpused üle $K(\zeta_j)$, siis induktsiooni eelduse tõttu peavad L'' ja L' olema isomorfsed kui f' lahutuskorpused. Seega üle korpuse K oleme saanud laiendit isomorfismide jada $L \cong L'' \cong L'$.

Teoreem 1.3.3. *Olgu meil korpuste laiend $L : K$ ja algebraliste elementide süsteem $(\alpha_i)_{i=1}^n \subseteq L$. Elementide adjugeerimisel saadud korpus $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ on lõplikumõõtmeline korpuse K laiend*

Tõestus. Olgu elementidele $(\alpha_i)_{i=1}^n$ vastavate minimaalsete polünoomide astmed k_i. Siis dimensioonide teoreemist saame

$$[K(\alpha_1, \alpha_2, \ldots, \alpha_n) : K] = [K(\alpha_1) : K] \prod_{i=2}^{n} [K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})],$$

$$[K(\alpha_1, \alpha_2, \ldots, \alpha_n) : K] \leq \prod_{i=1}^{n} k_i \in \mathbb{N}.$$

Järeldus 1.3.3.1. *Olgu meil korpuste laiend $L : K$ ja algebraliste elementide süsteem $(\alpha_i \mid i \in I)$. Elementide adjugeerimisel saadud korpus $K(\alpha_i \mid i \in I)$ on algebraline korpuse K laiend.*

TÕESTUS. Olgu $\alpha \in K(\alpha_i \mid i \in I)$, siis on kerge veenduda, et leidub arv $n \in \mathbb{N}$ esindajat süsteemist $(\alpha_i \mid i \in I)$ nii, et $\alpha = f(\alpha_1, \alpha_2, \ldots, \alpha_n)$, kus polünoom $f \in K[X_1, X_2, \ldots, X_n]$. Sest iga α_i lineaarselt sõltumatute astmete arv on tõkestatud minimaalse polünoomi astmega ja iga element peab avalduma lõpliku summana vektoruumi $K(\alpha_i \mid i \in I)$ baasi elementidest. Nüüd on ilmne, et element $\alpha \in K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, mis on lõplik laiend ja seega on α algebraline.

Teoreem 1.3.4. *Korpuste laiendi $L : K$ jaoks leidub suurim vahepealne korpus $L \subseteq M \subseteq L$, mis on algebraline üle K.*

TÕESTUS. Võtame elemenditde $(\alpha_i \mid i \in I) \subseteq L$ süsteemiks kõigi algebraliste elementide hulga korpuses L, siis $M = K(\alpha_i \mid i \in I)$ on korpuse K algebraline laiend. Konstruktsiooonist tulenevalt peab see olema suurim.

1.4 Korpuse algebraline sulund

Definitsioon 1.4.1. *Korpust K nimetatakse algebraliselt kinniseks parajasti siis, kui iga mittekonstantse polünoomi $f \in K[X]$ leidub polünoomil vähemalt üks juur.*

Järeldus 1.4.0.1. *Algebraliselt kinnises korpuses lahutub iga mittekonstantne polünoom lineaartegurite korrutiseks.*

Lemma 1.4.1. *Olgu $I \subsetneq R$ kahepoolne ideaal ringis R, siis leidub maksimaalne ideaal $J \subsetneq R$ nii, et $I \subseteq J$.*

TÕESTUS. Olgu meil $\mathcal{P} = \{M \subsetneq R \mid i \subseteq M,\ M \text{ on kahepoolne ideaal}\}$ osaliselt järjestatud sisalduvusseose suhtes. Siis $I \in \mathcal{P} \neq \emptyset$ ja igal täielikult järjestatud alamhulgal $(M_\alpha \mid \alpha \in I)$ on olemas ülemine tõke $N = \bigcup_{\alpha \in I} M_\alpha$. On ilmne, et hulk N on ideaal, kuna ideaal on defineeritud lõpliku hulga elementide abil. Teisalt $N = R$, siis $1 \in N$ ja seega peaks leiduma $\alpha \in I$ nii, et $1 \in M_\alpha \neq R$, mis on ilmne vastuolu. Seega on $N \in \mathcal{P}$ ning on täidetud Zorni lemma eeldused, mistõttu peab leiduma maksimaalne ideaal J.

Teoreem 1.4.2. *Igal korpusel K on olemas laiend L, milles iga mittekonstantne polünoom $f \in K[X]$ omab juurt.*

TÕESTUS. Vaatleme kõikide mittekonstantsete polünoomide hulka $\{f_i \mid i \in I\}$. Võtame nüüd sama võimsusega muutujate hulga $S = \{X_i \mid i \in I\}$. Vaatleme nüüd polünoomide ringi $K[S]$ ideaali $I = \big(f_i(X_i) \mid i \in I\big)$. Näitame $I \neq K[S]$. Kui $I = K[S]$, siis peaks leiduma mittetriviaalne lõplik lineaarkombinatsioon

$$f_{i_1}(X_{i_1})g_1 + f_{i_2}(X_{i_2})g_2 + \cdots + f_{i_n}(X_{i_n})g_n = 1,$$

kus $g_i \in K[S]$. Kuna meil on lõplik arv polünoome, siis leidub korpuse K laiend L, milles iga f_{i_k} omab juurt α_{i_k}, seega väärtustades $X_{i_k} = \alpha_{i_k}$ saame vastuolu

$$0 = f_{i_1}(\alpha_{i_1})g_1 + f_{i_2}(\alpha_{i_2})g_2 + \cdots + f_{i_n}(\alpha_{i_n})g_n = 1.$$

Eelnevast lemmast 1.4.1 saame, et leidub maksimmalne ideaal $I \subseteq J \subsetneq K[S]$. Paneme tähele, et faktorringis $F = K[S]/J$ leidub igal polünoomil $f_i \in K[X]$ juur $\overline{X_i}$. Selge on, et loomulik sisestus $\pi : K \hookrightarrow F$ on injektsioon, sest $J \bigcap K = \{0\}$. Tõestame F on korpus. Olgu $\overline{f} \neq 0 \Leftrightarrow f \notin J$, siis ideaali J maksimaalsusest $J + (f) = K[S]$ ja seega leidub $u, v \in K[S]$ ja $g \in J$ nii, et $ug + vf = 1$ ja seega $\overline{v} \cdot \overline{f} = \overline{1}$.

Teoreem 1.4.3. *Igal korpusel K leidub algebraliselt kinnine laiend.*

TÕESTUS. Olgu $K_0 = K$, vastavalt eelnevale teoreemile1.4.2 leidub laiend K_1, milles iga mittekonstantne polünoom $f \in K_0[X]$ omab juurt. Olgu K_i korpuse K_{i-1} selline laiend, milles iga mittekonstantne polünoom $f \in K_{i-1}[X]$ omab juurt. Nüüd saab defineerida $F = \bigcup_{i=0}^{\infty} K_i$. On lihtne veenduda, et tegu on korpusega. Teisalt iga mittekonstantne polünoom üle F peab olema polünoom üle mingi K_i ja seega omama juurt.

Järeldus 1.4.3.1. *Igal korpusel leidub algebraline algebraliselt kinnine laiend.*

TÕESTUS. Pannes kokku teoreemide 1.4.3 ja 1.3.4 konstruktsioonid, saame korpuste jada $K \subseteq \overline{K} \subseteq F$, kus F on algebraliselt kinnine ja $\overline{K}$ on suurim algebraline F alamkorpus. Oletame, et $\overline{K}$ pole algebraliselt kinnine, siis leidub polünoom $f \in \overline{K}[X]$, mis ei oma juurt ξ korpuses $\overline{K}$. Kuna Iga $\overline{K}$ element on lõplik summa algebralistest elementidest üle K, siis ξ on algebraline üle lõplikumõõtmelise laiendi $K(a_1, a_2, \ldots, a_n)$ ja seega peab dimensioonide teoreemist $K(a_1, a_2, \ldots, a_n, \xi)$ olema lõplikumõõtmeline laiend ja ξ peab seega olema algebraline üle K, mis annab vastuolu $\overline{K}$ konstruktsiooniga.

Definitsioon 1.4.2. *Korpuse K minimaalset algebralist laiendit $\overline{K}$, mis sisaldab endas laiendite isomorfismi täpsuseni kõiki algebralisi laiendeid nimetatakse korpuse K algebraliseks sulundiks.*

Teoreem 1.4.4. *Igal korpusel leidub algebraline sulund ning see on isomorfismi täpsuseni üheselt määratud.*

TÕESTUS. Tõestuseks näitame, et algebraline algebraliselt kinnine laiend $\overline{K}$ sisaldab isomorfismi täpsuseni kõiki algebralisi laiendeid. Olgu F suvaline algebraline laiend. Moodustame osaliselt järjestatud hulga

$$\mathcal{P} = \left\{(L, \varphi) \mid K \subseteq L \subseteq F,\ \varphi : L \to \overline{K},\ \varphi \text{ on sisestus},\ \varphi|_K = I_K\right\},$$

kus

$$(L_1, \varphi_1) \preceq (L_2, \varphi_2) \Leftrightarrow L_1 \subseteq L_2,\ \varphi_2|_{L_1} = \varphi_1.$$

Paneme tähele $\mathcal{P} \neq \emptyset$, sest paar $(K, I_K) \in \mathcal{P}$. Näitame, et igal osaliselt järjestatud ahelal $\big((L_\alpha, \varphi_\alpha) \mid \alpha \in I\big) \subseteq \mathcal{P}$ leidub ülemine tõke hulgas $\mathcal{P}$. Võtame traditsiooniliselt $L = \bigcup_{\alpha \in I} L_\alpha$ ja $\varphi(x) = \varphi_\alpha(x)$, kui $x \in L_\alpha$. Lihtne on veenduda φ definitsioon on korrektne ja $(L, \varphi) \in \mathcal{P}$. Kuna on täidetut Zorni lemma eeldused, siis leidub maksimaalne element (M, φ) hulgas $\mathcal{P}$. Oletame vastuväiteliselt,

et $M \neq F$, siis leidub element $\alpha \in F \setminus M$. Vaatleme laiendit $K(\alpha)$. Kuna α on algebraline, siis leiduvad minimaalse polünoomid $m_\alpha \in K[X]$ ja $n_\alpha \in M[X]$. Paneme tähele, et vastavalt minimaalsete polünomomide omadustele $n_\alpha \mid m_\alpha$. Tähistame $m'_\alpha = \varphi(n_\alpha) \in M'[X] \subseteq \overline{K}[X]$, kus $M' = \varphi[M]$. Sisestus φ säilitab polünoomide jagumise ja seega $m'_\alpha \mid m_\alpha$, sest $m_\alpha \in K[X]$. Korpuse $\overline{K}$ algebralisest kinnisusest saame, et polünoom m'_α omab juurt $\alpha' \in \overline{K}$, mis on ühtlasi juureks polünoomile m_α. Polünoom m'_α peab olema elemendi α' minimaalne polünoom üle korpuse M', sest vastasel korral saaks isomorfismi φ^{-1} abil polünoomi n_α tegurdada, mis oleks vastuolus n_α valikuga. Nüüd saab moodustada kaks korpuste jada $K \subseteq M' \subseteq M'(\alpha') \subseteq \overline{K}$ ja $K \subseteq M \subsetneq M(\alpha) \subseteq F$. Olgu $r = \deg n_\alpha$, siis vektorite süsteem $1, \alpha, \alpha^2, \ldots, \alpha^{r-1}$ on vektoruumi $M(\alpha)$ baas ja $1, \alpha', (\alpha')^2, \ldots, (\alpha')^{r-1}$ on baas vektorruumis $M'(\alpha')$. Nüüd saab defineerida bijektiivse lineaarkujutuse $\Psi : M(\alpha) \to M'(\alpha')$ järgnevalt

$$\Psi\left(\sum_{i=0}^{r-1} m_i \alpha^i\right) = \sum_{i=0}^{r-1} \varphi(m_i)(\alpha')^i$$

On lihtne veenduda, et Ψ on kooskõlas korrutamise ja pöördelemendi võtmisega, ning seega tekib sisestus $M(\alpha) \overset{\Psi}{\hookrightarrow} \overline{K}$, mille ahend $\Psi|_M = \psi$, mis on vastuolus paari (M, ψ) maksimaalsusega, mistõttu peab $M = F$.

Kuna $\overline{K}$ on ise algebraline, siis peab see isomorfismi täpsuseni sisalduma korpuse K algebralises sulundis. Sulundi minimaalsuse tõttu peab see langema kokku $\overline{K}$, sest $\overline{K}$ sisaldab isomorfismi täpsuseni kõik korpuse K algebralised laiendid.

1.5 Lõplikud korpused

Definitsioon 1.5.1. *Korpust, milles on lõplik arv elemente, nimetatakse lõplikuks korpuseks.*

Teoreem 1.5.1. *Iga lõplik kaldkorpus on korpus.*

Tõestus. Vaata Mati Kilp *Algebra II* lk. 8-10.

Teoreem 1.5.2. *Iga lõplik korpus sisaldab p^n elementi.*

Tõestus. Olgu K lõplik korpus, siis ühikelemendi poolt moodustatud aditiivset tsükliline rühm $\langle 1 \rangle \cong \mathbb{Z}_p$. Lihtne on veenduda $\mathbb{Z}_p$ kui korpus on K alamkorpus. Võttes vektorruumis K suvalise baasi $a_1, a_2, \ldots, a_n$ üle $\mathbb{Z}_p$, peab see olema lõplik, sest korpus K on sise lõplik. Nüüd saame $K \cong \mathbb{Z}_p^n$ kui vektoruumid üle $\mathbb{Z}_p$ ja siit $|K| = p^n$.

Teoreem 1.5.3 (Korpuste ühesuse teoreem)**.** *Iga algarvu p ja naturaalarvu n korral leidub isomorfismi täpsuseni üks korpus, milles on p^n elementi.*

Tõestus. Vaatlen polünoomi $f(x) = X^{p^n} - X \in \mathbb{Z}_p[X]$ lahutuskorpust L. Olgu hulk $S = \{x \in L \mid f(x) = 0\}$, siis hulgas S on p^n elementi, kuna $f'(x) =$

$p^n x^{p^n-1} - 1 = -1 \neq 0$ ja seega pole polünoomil kordseid juuri. Näitame, et S on alamkorpus. Kui $a, b \in S$, siis

$$(a+b)^{p^n} = \left(\sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}\right)^{p^{n-1}} = (a^p + b^p)^{p^{n-1}} = \ldots = a^{p^n} + b^{p^n},$$

sest $p1 = 0$. Kui $p = 2$, siis $-a = a$, ja kui $p > 2$, siis $(-1)^{p^n} = -1$, mistõttu saame

$$\begin{aligned}
f(a+b) &= (a+b)^{p^n} - (a+b) = a^{p^n} + b^{p^n} - a - b = f(a) + f(b) = 0\\
f(-a) &= (-a)^{p^n} - (-a) = a - a^{p^n} = -f(a) = 0\\
f(ab) &= ab^{p^n} - ab = \big((ab)^{p^n} - ab\big) - b\big(a^{p^n} - a\big) - a\big(b^{p^n} - b\big)\\
&= (a^{p^n} - a)(b^{p^n} - b) = f(a)f(b) = 0\\
f(a^{-1}) &= (a^{-1})^{p^n} - a^{-1} = a^{-p^n-1}(a - a^{p^n}) = a^{-p^n-1} f(a) = 0
\end{aligned}$$

Seega on S korpuse L alamkorpus ja lahutuskorpuse minimaalsusest $S = L$. Seega leidub alati korpus, milles on p^n elementi.

Olgu meil korpus L', milles on p^n elementi, siis iga nullist erineva elemendi multiplikatiivne järk jagab Lagrange' teoreemi tõttu $p^n - 1$ ja seega on iga element polünoomi $f = X^{p^n} - X \in \mathbb{Z}_p[X]$ juur. Element 0 sammuti polünoomi f juur ning seetõttu on korpus L' polünoomi f lahutuskorpus. Lahutuskorpuste ühesuse tõttu $L \cong L'$.

Definitsioon 1.5.2. *Korpust, milles on p^n elementi, tähistatakse $\mathbb{F}_{p^q}$.*

Järeldus 1.5.3.1. *Taandumatu n-astme polünoomi $f \in \mathbb{Z}_p[X]$ lahutuskorpus L on isomorfne $\mathbb{F}_{p^n}$.*

Tõestus. Olgu polünoomi f juur $\alpha \in L$. Kui jagada polünoom f pealiikme kordajaga, siis saame taandumatu unitaarse polünoomi f', mistõttu polünoom f' on elemendi α minimaalne polünoom. Lihtsa laiendi ehitusest saame mõõtmeks $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = n$ ja seega $\mathbb{Z}_p(\alpha) \cong \mathbb{F}_{p^n}$, mistõttu võime eeldada $\mathbb{F}_{p^n} \subseteq L$. Eelnevast saime teda, et iga juure $\beta \in L$ poolt moodustatud laiend $\mathbb{Z}_p(\beta) \cong \mathbb{F}_{p^n}$, mistõttu on β polünoomi $g = X^{p^n} - X$ juur. Kuna $\mathbb{F}_{p^n}$ on polünoomi g lahutuskorpus, siis $\beta \in \mathbb{F}_{p^n}$ ja $L = \mathbb{F}_{p^n}$.

Lemma 1.5.4. *Kui kommutatiivses rühmas G on elemendid järkudega n ja m, siis rühmas G leidub element järguga $k = \operatorname{lcm}(m, n)$.*

Tõestus. Vaatlen, esmalt juhtu, kus $\gcd(m, n) = 1$. Olgu elemendid a ja b, nii et $ord(a) = m$ ja $ord(b) = n$. Siis $(ab)^{mn} = a^{mn}b^{mn} = 1$. Teisalt kui $1 = (ab)^l = a^l b^l$, millest $a^l = b^{-l}$. Seega $a^l = b^{-l} \in \langle b \rangle$, siis $ord(a^l) \mid ord(b)$ ja samas $ord(a^l) \mid ord(a)$. Kuna $\gcd(m, n) = 1$, siis $ord(a^l) = 1$, millest $a^l = 1$. Seega kui $(ab)^l = 1$, siis $a^l = 1$ ja $m \mid l$. Analoogselt tõestades $n \mid l$. Siit on selge $ord(ab) = \operatorname{lcm}(m, n)$.

Vaatlen üldist juhtu, kus $\gcd(m, n) = k$. Olgu elemendid a ja b, nii et $ord(a) = m$ ja $ord(b) = n$. Nüüd vaatlen elementi a^k, siis $ord(a^k) = \frac{m}{k} =$

m_1. Siit on selge, et $\gcd(m_1, n) = 1$ ja seega leidub element, mille järk on $\mathrm{lcm}(m_1, n) = \mathrm{lcm}(m, n)$.

Teoreem 1.5.5. *Lõpliku korpuse K multiplikatiivne rühm on tsükliline.*

Tõestus. Eelneva teoreemi põhjal leidub rühma K^* element a, mille järku jagavad kõik teised elemendid st. leidub maksimaalse järguga element. Olgu meil multiplikatiivses rühmas n elementi ja olgu a järk m. Siis on polünoomil $X^m - 1 =\in \mathbb{Z}_p[X]$ on kopruses K täpselt n lahendit, sest iga $g \in K^*$ korral $ord(g) \mid m \Rightarrow g^m = 1$. Siit on selge $m \geq n$, teisalt elemendi a järk peab olema väiksem kui n ja siit $m = n$. Ühesõnaga a on korpuse tsüklilise rühma moodustaja.

Järeldus 1.5.5.1. *Korpus $\mathbb{F}_{p^k}$ on korpuse $\mathbb{F}_{p^n}$ alamkorpus parajasti siis, kui k jagab n.*

Tõestus. Kui korpus $\mathbb{F}_{p^k}$ on korpuse $\mathbb{F}_{p^n}$ alamkorpus, siis $p^k - 1 \mid p^n - 1$, sest alamkorpuse tsüklilise rühma moodustaja järk peab jagama korpuse tsüklilise rühma järku. Kuid see tingimus on ka piisav. Olgu korpuse $\mathbb{F}_{p^n}$ moodustaja α ja $v(p^k - 1) = p^n - 1$, siis leidub element $\beta = \alpha^v$, mille järk on $p^k - 1$. Nüüd tsüklilises rühma $\langle\beta\rangle$ iga element on polünoomi $X^{p^k} - X \in \mathbb{Z}_p[X]$ juur, sest $\beta^{p^k} = \alpha^{vp^k} = \alpha^v = \beta$. Lisades hulgale $\langle b\rangle$ elemendi 0, saame polünoomi $X^{p^k} - X$ lahutuskorpuse, mis on isomorfne $\mathbb{F}_{p^k}$.

Näitan tingimuseks $p^k - 1 \mid p^n - 1$ on tarvilik ja piisav $k \mid n$. Piisavus on ilmne, sest $p^n - 1 = (p^k)^l - 1 = (p^k - 1)(1 + p^k + p^{2k} + \cdots + p^{(l-1)k})$. Tarvilikkuse tõestame induktsiooniga n järgi. Kui $n = 1$ on väide triviaalne. Kui väide on õige juhul $n < n_0$, siis $p^{n_0} - 1 = v(p^k - 1) \Leftrightarrow p^{n_0} = vp^k + (1 - v)$. Siit omakorda $p^k \mid v - 1$, millest $v = p^k v_1 + 1$. Siit saame $p^{n_0 - k} - 1 = v_1(p^k - 1)$, mis saab olla täidetud vaid siis, kui $k \mid n_0 - k$ ja seega $k \mid n_0$.

1.6 Sirkli ja joonlaua konstruktsioonid

Definitsioon 1.6.1. *Sirkli ja joonlaua konstruktsioon on geomeetriline konstruktsioon, mida saab teha järgnevate reeglite kohaselt:*

1. *On antud suvaline algkonstruktsioon, mis koosneb ainult lõplikust arvust sirglõikudest ja ringjoontest. Lisaks on antud ühikringjoon ja selle keskpunkti läbiv sirge.*

2. *Punkte saab konstrueerida vaid eelnevat konstrueeritud sirge lõikamisel konstrueeritava sirge või ringjoonega või eelnevalt konstrueritud ringjoone lõikamisel konstrueeritava sirge või ringjoonega.*

3. *Konstruktsiooni võib lisada sirge tõmmates selle läbi eelnevalt konstrueeritud punktide.*

4. *Konstruktsiooni võib lisada sirglõigu ühendades varem konstrueeritud punktid.*

5. *Konstruktsiooni võib lisada ringjoone mis on tõmmatud läbi kahe eelnevalt konstrueeritud punkti, millest üks on keskpunkt ja teist läbib ringjoon.*

Harilikult vaatame konstruktsioone komplekstasandil, st. konstrueeritakse kompleksvektoreid.

Järeldus 1.6.0.2. *Iga algkonstruktsiooni korral on lubatavad järgmised konstruktsioonid:*

1. *Läbi eelnevalt konstrueeritud punkti sirge tõmbamine, mis on parallelne eelnevalt konstrueeritud sirgega.*
2. *Läbi eelnevalt konstrueeritud punkti sirge tõmbamine, mis on risti eelnevalt konstrueeritud sirgega.*
3. *Eelnevalt konstrueeritud nurga poolitamine sirgega.*
4. *Lõigu keskristsirge konstrueerimine.*
5. *Täisnurkse kolmnurga konstrueerimine kaatetite järgi.*
6. *Täisnurkse kolmnurga konstrueerimine kaateti ja hüpotenuusi järgi.*
7. *Konstruktsiooni nihutamine fikseeritud punkti.*
8. *Konstruktsiooni pöötamine eelnevalt konstrueeritud nurga võrra.*

TÕESTUS. Lihtsate geomeetriliste konstruktsioonide järjekindel läbivaatus. Viimase kahe väite korral induktsioon konstruktsioonielementide arvu järgi.

Lemma 1.6.1. *Iga algkonstruktsiooni korral saab sirkli ja joonlauaga konstrueerida iga positiivse ratsionaalarvu $q \in \mathbb{Q}^+$ pikkuse lõigu. Ja seega on komplekstasandi kõik ratsionaalarvuliste komponentidega vektorid konstrueeritavad.*

TÕESTUS. Selleks võib kasutatada kiirte teoreemile vastavat konstruktsiooni.

Lemma 1.6.2. *Iga algkonstruktsiooni korral ja iga naturaalarvu $n \in N$ korral on võimalik konstrueerida lõik pikkusega $\sqrt{n}$.*

TÕESTUS. Kasutada saab Pütagorase teoreemil põhinevat iteratiivset konstruktsiooni kasutades lõiku pikkusega $\sqrt{n-1}$ lõigu $\sqrt{n}$ konstrueerimiseks.

Lemma 1.6.3. *Iga algkonstruktsiooni korral on sirkli ja joonlauaga konstrueeritavad lõigu pikkused kinnised liitmise, lahutamise*, korrutamise ja jagamise suhtes.*

Järeldus 1.6.3.1. *Iga algkonstruktsiooni korral moodustab sirkli ja joonlauaga konstrueeriavate kompleksvektorite hulk korpuse.*

Järeldus 1.6.3.2. *Iga algkonstruktsiooni korral saab sirkli ja joonlauaga saab konstrueerida kõik ratsionaalarvuliste kordajatega ruutvõrrandite lahendid.*

TÕESTUS. See tuleneb ratsionaalarvuliste ruutjuurte konstrueerimise võimalikkusest tänu lemmale 1.6.2 ja ruutvõrrandi avaldumisest radikaalides.

Järeldus 1.6.3.3. *Iga algkonstruktsiooni korral saab sirkli ja joonlauaga konstrueerida vaid algkonstruktsiooni punkte või ruutvõrrandite lahendeid, mille kordajad on eelnevalt konstrueeritud.*

TÕESTUS. Induktsioon üle konstruktsiooni elementide.
Baas. Algkonstruktsioon on algkonstruktsioon.
Induktsiooni samm
Olgu eelnevalt konstrueeritud komplekstasandi vektorid $a_1, a_2, \ldots, a_n$, siis vastavalt definitsioonile on võimalik. A. Konstrueerida kahe sirge lõikepunkt. Olgu neli sirgeid fikseerivat punkti a_1, a_2, a_3 ja a_4. Sellele vastab võrrandisüsteem

$$\frac{x-x_1}{y-y_1} = \frac{x_2-x_1}{y_2-y_1}, \qquad \frac{x-x_3}{y-y_3} = \frac{x_4-x_3}{y_4-y_3}.$$

Kuna kõik lineaarvõrrnadisüsteemi konstandid on sirkli ja joonlauaga konstrueeritavad, siis on seda ka lahend.
B. Konstrueerida sirge ja ringjoone lõikepunkt. Olgu meil neli konstruktsiooni fikseerivat punkti a_1, a_2, a_3 ja a_4. Sellele vastab võrrandisüsteem

$$\frac{x-x_1}{y-y_1} = \frac{x_2-x_1}{y_2-y_1}, \qquad (x-x_3)^2+(y-y_3)^2 = (x_4-x_3)^2+(y_4-y_3)^2.$$

Asendades esimese võrrandi teise on ilmne, et kõik arvulised kordajad, mis tekivad, on konstrueeritavd, sest esialgseid kordajaid tuleb liita, lahutada ja korrutada.
C. Konstrueerida sirge ja ringjoone lõikepunkt. Olgu meil neli konstruktsiooni fikseerivat punkti a_1, a_2, a_3 ja a_4. Sellele vastab võrrandisüsteem

$$\begin{aligned}(x-x_1)^2+(y-y_1)^2 &= (x_2-x_1)^2+(y_2-y_1)^2,\\ (x-x_3)^2+(y-y_3)^2 &= (x_4-x_3)^2+(y_4-y_3)^2.\end{aligned}$$

Lahutades esimesest võrrandist teise, saame konstrueeritavate kordajatega lineaarvõrrandi ja oleme seega taandanud tõestuse juhule B.

Teoreem 1.6.4 (Eisestani kriteerium)**.** *Olgu meil polünoom $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in Z[X]$ ja leidub algatv p nii, et $p \mid a_i$, kui $i = 0, 1, \ldots n-1$, $p \nmid a_n$ ning $p^2 \nmid a_0$, siis f on taandumatu polünoom üle $\mathbb{Q}$.*

Definitsioon 1.6.2. *Kuubi kahekordistamise probleemiks nimetatakse tühja algkonstruktsiooniga sirkli ja joonlaua ülesannet ja ülesandeks on konstrueerida kuubi ruumalaga 2 serv.*

Teoreem 1.6.5. *Kuubi kahekordistamise probleem on lahendumatu.*

TÕESTUS. Kogu ülesanne taandub polünoomi $f = X^3 - 2 \in \mathbb{Q}[X]$ lahutuskorpuse leidmisele. Kuna polünoom on taandumatu üle $\mathbb{Q}$. Tõestus on vastuoluline. Olgu taandumatu murd $\frac{m}{n}$ polünoomi f juureks, siis $2 \mid m^3$, millest

$2 \mid m$. Seetõttu peab $4 \mid n^3 \Rightarrow 2 \mid n$ ja seega pole murd $\frac{m}{n}$ taandumatu. Olgu polünoomi lahutuskorpus L, siis teoreemi 1.2.2.2 tõttu $[L : \mathbb{Q}] = 3$. Järelduse 1.6.3.3 tõttu saab konstrueerida, vaid ruutõrrandite laendeid, mistõttu suvalise konsrueeritud laiendi K mõõde on $[K : \mathbb{Q}] = 2^k$. Kuna $3 \nmid 2^k \ k \in \mathbb{N}$, siis pole $\sqrt[3]{2}$ sirkli ja joonlauaga konstrueeritav.

Definitsioon 1.6.3. *Nurga trisektsiooni probleemiks nimetatakse sirkli ja joonlaua konstruktsiooniprobleemi, kus algkonstruktsiooniks on ringjoone kaar koos kahe otspunktiga. Ülesanne on kaar kolmeks võrdse pikkusega osaks.*

Lemma 1.6.6. *Nurga trisektsiooni probleem on samaväärne lihtsa kuupvõrrandi $4x^3 - 3x = C$ lahendamisega, kus $C = \cos\varphi$ on ette antud.*

Tõestus. Tuleneb nurga ja nurgale vastava koosinuse konstrueerimise samaväärsusest ja trigonomeetrilistest lihtsustusvalemitest.

Teoreem 1.6.7. *Nurgatrisektsiooni probleem on üldjuhul lahendamatu.*

Tõestus. Võtame ühikringjoone kaare pikkusega $\frac{\pi}{3}$, siis sellele vastav kuupvõrrand on $8X^3 - 6X - 1 = 0$. Tehes asenduse $2X = Y$, saame samaväärse võrrandi $Y^3 - 3Y - 1 = 0$. Tehes asenduse $Y = Z + 1$, saame samaväärse võrrandi $Z^3 + 3Z^2 - 3 = 0$. Kuna polünoom $f = Z^3 - 3Z^2 - 3 \in \mathbb{Q}[Z]$ on Eisestaini kriteeriumi tõttu taandumatu, siis analoogselt kuubi kahekordistamisega on ülesanne lahendamatu.

Definitsioon 1.6.4. *Ringi kvadratuuri probleemiks nimetatakse sirkli ja joonlaua ülesannet, mille algkonstruktsiooniks on ühikringjoon ning ülesandeks on konstrueerida pindvõrdne ruut.*

Teoreem 1.6.8. *Ringi kavadratuur on lahendumatu.*

Tõestus. Teoreemi ?? tõttu on π transtendentne ja kui õnnestuks konstrueerida lõik pikkusega $\sqrt{\pi}$, siis õnnestuks konstrueerida ka lõik pikkusega π. Kuna sirkli ja joonlauaga, saab konstrueerida vaid lõplikumõõtmelisi $\mathbb{Q}$ laiendeid, siis oleme saanud vastuolu.

Peatükk 2

Galois' teooria alused

2.1 Laiendi Galois' rühm ja Galois' vastavus

Definitsioon 2.1.1. *Olgu meil korpuse K laiend L, siis laiendi automorfismiks α nimetetakse kujutust, mis on kooskõlas korpuse tehetega ja mille ahend $\alpha|_K$ on ühiktesisendus I_K. Laiendi $L : K$ automorfismide rühma tähistatakse* $\mathrm{Gal}(L : K)$.

Definitsioon 2.1.2. *Olgu meil korpuste laiend $L : K$. Rühma* $\mathrm{Gal}(F : K)$ *alamrühmale G vastavat maksimaalset alamkorpust* $\mathrm{Inv}\, G$*, mille kõik elemendid on teisenduste $\alpha \in G$ püsipunktideks, nimetatakse rühmale G vastavaks laiendiks.*

Definitsioon 2.1.3. *Olgu meil korpuste laiend $L : K$. Tähistagu P kõigi korpuse L alamkorpuste hulka, mis on laiendid üle K, ning olgu Q automorfismirühma* $\mathrm{Gal}(L : K)$ *kõigi alamrühmade hulk. Vastavust hulkade P ja Q elementide vahel, mis tekib operaatorite* $\mathrm{Gal}(F : -)$ *ja* Inv *rakendamisel, nimetatakse Galois' vastavuseks.*

Lause 2.1.1. *Galois' vastavus on antimonotoone.*

Definitsioon 2.1.4. *Üldiseks Galois' vastavuseks kahe osaliselt järjestatud hulga P ja Q vahel nimetatakse kahte antimonotoonset teisendust $T_1 : P \to Q$ ja $T_2 : Q \to P$, mille korral on täidetud tingimused*

$$\forall x \in P \; x \preceq T_2T_1(x), \qquad \forall y \in Q \; y \preceq T_1T_2(y).$$

Harilikult tähistatakse $T_1(x) = x'$ ja $T_2(y) = y'$.

Definitsioon 2.1.5. *Olgu P osaliselt järjestatud hulk. Monotoonset teisendust $\varphi : P \to P$ nimetatakse sulundioperaatoriks, parajasti siis kui on täidetud kaks tingimust*

$$\forall x \in P \; x \preceq \varphi(x), \qquad \varphi^2 = \varphi.$$

Hulga P elemente, mis on sulundioperaatori püsipunktideks, nimetatakse kinnisteks elementideks.

Lause 2.1.2. *Olgu osaliselt järjestatud hulkade P ja Q vahel üldine Galois' vastavus, siis operaatorid $\varphi_P : P \to P$ ja $\varphi_Q : Q \to Q$, mis on defineeritud järgnevalt*

$$\varphi_P(x) = x'', \qquad \varphi_Q(y) = y''$$

on sulundioperaatorid.

Tõestus. On ilmne $x_1 \preceq x_2$, siis $x_1' \succeq x_2'$ ja $x_1'' \preceq x_2''$ ja seega on teisendused φ_P ja φ_Q monotoonsed. Tingimus $x \preceq x''$ tuleneb Galois' vastavuse definitsioonist. Kolmas tingimus $x'' = x''''$ tuleneb kahest võrdusest $x \preceq x'' \Rightarrow x'' \preceq x''''$ ja $x' \preceq (x')'' \Rightarrow x'' \succeq (x')''' = x''''$.

Lemma 2.1.3. *Hulga P element on x kinnine parajasti siis, kui leidub $y \in Q$ nii, et $y' = x$.*

Tõestus. Tarvilikkus. Olgu element $x = x''$, siis $x = (x')'$. Piisavus $x = y'$, siis $x'' = y'''$. Kuna $y' \preceq (y')'' = y'''$ ja $y \preceq y'' \Rightarrow y' \succeq y'''$, mistõttu $y''' = y' = x$.

Teoreem 2.1.4. *Olgu P ja Q osaliselt järjestatud hulgad, mille vahel on üldine Galois' vastavus, siis hulkade P ja Q kinniste elementide vahel on üksühene vastavus $x \leftrightarrow x'$.*

Tõestus. Eelneva lemma tõttu on x' kinnised elemendid ja kõikidel kinnistel elementidel y leidub originaal x nii, et $y = x'$.

2.2 Laiendite automorfismide omadused

Lemma 2.2.1. *Olgu korpuse laiend $F : K$ polünoomi $f \in K[X]$ lahutuskorpus. Laiendi $F : K$ suvaline automorfism $\alpha \in \mathrm{Gal}(F : K)$ on üheselt määratud oma väärtustega polünoomi f juurtel $(c_i)_{i=1}^n$, kusjuures polünoomi juured peavad kujutuma polünoomi juurteks ja iga juure c_i korral peab leiduma juur c_j, mis kujutub selleks, st. $\alpha(c_j) = c_i$.*

Tõestus. Üheselt määratlus on ilmne, sest polünoomi juurte $(c_i)_{i=1}^n$ omavahelised korrutised moodustavad laiendi(kui vektoruumi) baasi. Teisalt $f(\alpha(c_j)) = \alpha(f(c_j)) = f(0) = 0$, seega peab polünoomi juur kujutuma juureks. Teisalt peab automorfism olema pealekujutus, seega peab leiduma element $c \in L$ $\alpha(c) = c_i$, siis $\alpha(f(c)) = f(\alpha(c)) = 0$. Kujutise injektiivsusest saame $f(c) = 0$ ja seega on c polünoomi juur.

Lemma 2.2.2. *Olgu meil korpuste (laiendite) isomorfism $\varphi : K \to K'$ ja taandumatu polünoom $m \in K[X]$, siis $\varphi : K[X]/(m) \to K'[X]/(m')$ on isomorfism, kusjuures $m' = \varphi(m)$ on sama astme taandumatu polünoom üle K' .*

TÕESTUS. Polünoom m' peab olema sama astme polünoomi kui m, sest m kujutamisel pealiikme kordaja ei saa kujutuda nulliks. Polünoom m' peab olema taandumatu, sest vastasel korral indutseerib lahutus $m' = pq$ üle K' isomorfismi φ^{-1} abil mitteriviaalse teguriteks lahutuse $m = \varphi^{-1}(p)\varphi^{-1}(q)$ üle K. Kui $\overline{f} = \overline{g} \Leftrightarrow f = g + qm$, siis isomorfismi φ tõttu $f' = g' + p'm' \Leftrightarrow \overline{f'} = \overline{g'}$, kus $'$ on tähistatud φ rakendamist. Konstruktsiooni sümmetrilisusest $\overline{f} = \overline{g} \Leftrightarrow \overline{f'} = \overline{g'}$ ja seega φ injektsioon. Kuna ilmselt $\varphi^{-1} : K'[X]/(m') \to K[X]/(m)$ on φ pöördkujutus, siis on φ isomorfism.

Lemma 2.2.3. *Olgu meil korpuste lõplik laiend $F : K$ ja taandumatu polünoom $f \in K[X]$, mis lahutub korpuses F esimese astme juurteks. Olgu a_0 ja b_0 polünoomi f juured, siis leidub laiendi $F : K$ automorfism φ, mis kujutab $\varphi(a_0) = b_0$.*

TÕESTUS. Induktiivne konstruktsioon üle hõlmatud juurte.
Algsamm isomorfismi φ_0 on defineerimine.
Kuna elemendidel a_0 ja b_0 on sama minimaalme polünoom üle K, siis järelduse 1.2.2.3 tõttu leidub laiendite isomorfism $\varphi_0 : K(a_0) \to K(b_0)$ nii, et $\varphi_0(a_0) = b_0$.
Induktiivne samm
Olgu meil defineeritud isomorfism $\varphi_i : K(a_0, \ldots, a_i) \to K(b_0, \ldots, b_i)$ ja leidub polünoomi f hõlmamata juur $a_{i+1} \notin K(a_0, \ldots, a_i)$. Elemendi a_{i+1} minimaalne polünoom $m \in K(a_0, \ldots, a_i)[X]$ peab jagama f, seega polünoom $m' = \varphi_i(m)$ jagab $\varphi_i(f) = f$. Siit polünoomi $m' \in K(b_0, \ldots, b_i)[X]$ kõik juured on f juured. Eelnevast lemmast 2.2.2 teame m' on taandumatu ja unitaarne sama astme polünoom ning seega peab leiduma m' juur $b_{i+1} \in F$, kuna korpus F sisaldab kõiki polünoomi f juuri. Sama lemma tõttu on saab isomorfismi φ_i laiendada $\varphi_{i+1} : K(a_0, \ldots, a_{i+1}) \to K(b_0, \ldots, b_{i+1})$ järgnevalt

$$\varphi_{i+1}(p(a_{i+1})) = \varphi_i(p)(b_{i+1}), \text{ kus } p \in K(a_0, a_1, \ldots, a_i)[X],$$

sest

$$\begin{array}{lcl} K(a_0, \ldots, a_{i+1}) & \cong & K(a_0, \ldots, a_{i+1})[X]/(m) \\ K(a_0, \ldots, a_{i+1})[X]/(m) & \cong & K(b_0, \ldots, b_{i+1})[X]/(m') \\ K(b_0, \ldots, b_{i+1})[X]/(m') & \cong & K(b_0, \ldots, b_{i+1}) \end{array}$$

Lõppsamm
Kui kõik juured on hõlmatud, siis on kaks võimalust. Kui F on polünoomi f lahutuskorpus, peab $K(a_0, \ldots, a_r) = F = K(b_0, \ldots, b_r)$ ja φ_r ongi soovitud automorfism. Vastasel korral $F = K(a_0, \ldots, a_r)(c_1, \ldots, c_n)$ ja me saame kujutust φ_r laiendada üle kogu korpuse F

$$\varphi_{r+1}(p(c_1, \ldots, c_n)) = \varphi_r(p)(c_1, \ldots, c_n), \text{ kus } p \in K(a_0, \ldots, a_r)[X_1, \ldots, X_n],$$

sest korpuse F kõik elemendid on algebralised ja seetõttu on kõik elemendid polünoomiaalsel kujul.

Lemma 2.2.4. *Olgu meil $\varphi : K \to K_1$ korpuste isomorfism ning polünoomi $f \in K[X]$ lahutuskorpuseks on laiend $F : K$. Olgu F_1 korpuse K_1 laiend, milles polünoom $f' = \varphi(f) \in K_1[X]$ lahutub esimese astme tegurite korrutiseks, siis leidub korpuste sisestus $\psi : F \hookrightarrow F_1$ nii, et $\psi \mid_K = \varphi$.*

TÕESTUS. Induktsioon üle polünoomi f astme.
Baas. Kui $\deg f = 1$ või f on konstantne polünoom, siis polünoomi f' lahutuskorpuseks on K_1 ja seega sisestuseks ψ sobib φ.
Induktsiooni samm
Üldsust kitsendamata võib eeldada, et f omab teguriteks lahutust $f = f_1 f_2$, kus f_1 on taandumatu unitaarne polünoom. Seetõttu leidub korpuses F alamkorpus $K(a)$, kus a on polünoomi f_1 juur. Kuna F_1 sisaldab polünoomi f' kõiki juuri, siis leidub polünoomi $f_1' = \varphi(f_1)$ juur b. Lemmade 1.2.2.1 ja 2.2.2 tõttu on kujutus $\psi_0 : K(a) \to K_1(b)$, mis on defineeritud järgnevalt

$$\psi_0(p(a)) = \varphi(p)(b), \text{ kus } p \in K[X],$$

on isomorfism ning lihtne kontroll näitab, et ahend $\psi_0|_K = \varphi$. Nüüd polünoom $g = f/(X-a) \in K(a)[X]$ kujutub $g' = \psi(g) = f/(X-b) \in K_1(b)[X]$ ning on täidetud induktsiooni eeldused ja seega leidub sisestus $\psi : F \hookrightarrow F_1$ nii, et $\psi|_K = \psi_0|_K = \varphi$.

2.3 Korpuste normaalsed laiendid

Definitsioon 2.3.1. *Polünoomi $f \in K[X]$ nimetatakse separaabliks kui kõik polünoomi juured on ühekordsed. Korpuse K algebralise laiendi F elementi a nimetatakse separaabliks, parajasti siis kui elemendi a minimaalne polünoom on separaabel. Korpuse K algebraline laiend F on separaabel, parajasti siis kui iga laiendi element on separaabel.*

Lemma 2.3.1. *Olgu K korpus, mille karakteristika on 0. Kui $f \in K[X]$ on taandumatu, siis on ta ka separaabel.*

TÕESTUS. Kuna polünoom f on taandumatu, siis $\gcd(f, f') = 1$ ja seega puuduvad polünoomil kordsed juured.

Lemma 2.3.2. *Olgu meil lõpliku korpuse $\mathbb{F}_q$ laiend $F : \mathbb{F}_q$. Laiendi algebralise elemendi c minimaalne polünoom $m_c \in \mathbb{F}_q[X]$ on separaabel.*

TÕESTUS. Olgu elemendi c minimaalne polünoom $m_c = \sum_{i=0}^{n} m_i X^i$. Paneme tähele, et $\mathbb{F}_q(c)$ on separaabili polünoomi $X^{q^n} - X$ lahutuskorpus. Teisalt minimaalse polünoomi definitsiooni tõttu $m_c \mid X^{q^n} - X$ ja seega peab minimaalne polünoom olema separaabel.

Definitsioon 2.3.2. *Korpuste laiendit $F : K$ nimetatakse normaalseks, parajasti siis kui $K = \operatorname{Inv} \operatorname{Gal}(F : K)$.*

Teoreem 2.3.3. *Olgu meil korpuste lõplik laiend $F : K$, siis järgmised väited on samaväärsed:*

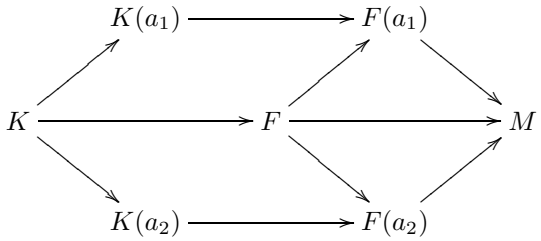
1. *korpuste lained $F : K$ on normaalne laiend;*

2. *iga elemendi $a \in F \setminus K$ korral leidub automorfism $\alpha \in \mathrm{Gal}(F : K)$, mille korral $\alpha(a) \neq a$;*

3. *Iga taandumatu polünoom $f \in K[X]$ omab laiendis F juurt parajasti siis, kui laiend F sisaldab endas polünoomi f lahutuskorpust ning F on separaabel;*

4. *laiend F on separaabel ja leidub polünoom $f \in K[X]$, mille lahutuskorpus on F.*

Tõestus.
(1) $\Leftrightarrow$ (2)
$F : K$ on normaalne $\Leftrightarrow$Iga $a \in F \setminus K$ korral a ei ole kõigi teisenduste $\mathrm{Gal}(F : K)$ püsipunkt$\Leftrightarrow$Iga elemendi $a \in F \setminus K$ korral leidub automorfism $\alpha \in \mathrm{Gal}(F : K)$, mille korral $\alpha(a) \neq a$.
(3) $\Rightarrow$ (4)
Et $F : K$ on lõplik, siis $F = K(c_1, c_2, \ldots, c_n)$. Olgu f_i elemendi c_i vastav minimaalne polünoom, kuna $F : K$ on lõplik, siis peab see alati leiduma. Erinevatele c_i võivad vastata ühesugused minimaalsed polünoomid. Olgu $f = f_{i_1} \cdot f_{i_2} \cdots f_{i_k}$, kus $i_1, i_2, \ldots, i_k$ on elementidele c_i vastavate polünoomide indeksid, nii et kõik polünoomid oleksid korrutises vaid üks kord. Eelduse tõttu on kõik f_{i_j} juured korpuses F. Nüüd on ilmne, et F on polünoomi f lahutuskorpus, kuna see on saadud K polünoomi juurte lisamise teel. Korpus F on separaabel eelduse tõttu.
(4) $\Rightarrow$ (3)
Olgu F polünoomi $g \in K[X]$ lahutuskorpus ning omagu taandumatu polünoom $f \in K[X]$ erinevaid juuri $a_1, a_2 \in M$, mis on polünoomi $fg \in K[X]$ lahutuskorpus. Selle tulemusena indutseerub järgmine diagramm



Paneme tähele $K(a_1) \cong K(a_2)$, sest mõlema elemendi minimaalne polünoom peab jagama taandumatut polünoomi f, millest kordaja täpsusega on f mõlema elemendi minimaalne polünoom ja seega $K(a_1) \cong K[X]/(f) \cong K(a_2)$. Kuna F on polünoomi g lahutuskorpus üle K, siis $F(a_1)$ ja $F(a_2)$ on vastalt polünoomi g lahutuskorpused üle $K(a_1)$ ja $K(a_2)$. Nüüd $F(a_1) \cong F(a_2)$, sest $F = K(b_1, b_2, \ldots, b_m)$ ja $K(a_1) \cong K(a_2)$ ning seega

$$F(a_1) = K(b_1, \ldots, b_m)(a_1) = K(a_1)(b_1, \ldots, b_m) \cong K(a_2)(b_1, \ldots, b_m) = F(a_2).$$

Kui $a_1 \in F$, siis $F(a_1) = F$ ja seetõttu $[F(a_2) : F] = [F(a_1) : F] = 1$, millest $F(a_2) = F$.
(3) $\Rightarrow$ (2)
Eelduse tõttu meil elemendi $a \in F \setminus K$ minimaalne polünoom m_a separaabel. Kuna a pole K element, siis on polünoomi aste vähemalt 2 ja seega leidub teine juur $b \neq a$. Nüüd lemma 2.2.3 tõttu on võimalik leida laiendite isomorfism φ, mis kujutab $\varphi(a) = b$.
(1) $\Rightarrow$ (3)
Olgu meil taandumatu polünoom $f \in K[X]$, mis omab juurt korpuses F, siis on tarvis näidata, et F sisaldab polünoomi kõiki juuri ja f on separaabel. Olgu $g(x) = (x - c_1)(x - c_2) \cdots (x - c_m)$, kus $c_1, \ldots, c_m$ on polünoomi f juured ilma kordsuseta korpuses F. On ilmne $g \mid f$ korpuses F. Võtame suvalise laiendite automorfismi $\alpha \in \mathrm{Gal}(F : K)$, siis juured peavad jääma üksühesesse vastavusse $\alpha(c_i) = c_j$. Viete' valemite põhjal on polünoomi g kordajad sümmetrilised polünoomid juurte suhtes seega on polünoomi g kordajad teisenduse α püsipunktideks. Et F on normaalne laiend, siis $g \in K[X]$, millest $f = g$ ja seega on f separaabel.

2.4 Dedekindi lemma. Galois' teoreem

Teoreem 2.4.1 (Dedekindi lemma)**.** *Olgu meil korpuste homomorfismide süsteem $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathrm{Hom}(K, L)$, siis süsteem $\alpha_1, \alpha_2, \ldots, \alpha_n$ on lineaarselt sõltumatu üle L parajasti siis, kui kõik homomorfismid on paarikaupa erinevad.*

Tõestus. Tarvilikkus on ilmne, tõestame piisavuse induktsiooniga üle n.
Baas $n = 2$
Olgu $\alpha_1 = \lambda\alpha_2$ ja $\lambda \in L$, siis iga $x, y \in K$ korral $\alpha_1(xy) = \lambda\alpha_2(x)\alpha_2(y)$. Võtame $y = 1$, siis $\alpha_1(x) = \lambda\alpha_2(x)$. Asendades selle esialgsesse seosesse saame $\alpha_1(x)\alpha_1(y) = \big(\lambda\alpha_2(x)\big)\alpha_2(y)$, millest $\alpha_1(y) = \alpha_2(y)$ iga $y \in K$.
Induktsiooni samm
Olgu meil minimaalse liidetavate arvuga mitteetriviaalne lineaarne kombinatsioon $\sum_{i=1}^{n} l_i\alpha_i \equiv 0$, $l_i \in L$, siis võib eeldada $l_i \neq 0$. Et $\alpha_1 \not\equiv \alpha_n$, siis leidub element $y \in K$ nii, et $\alpha_1(y) \neq \alpha_n(y)$. Lahutame kaks võrrandit

$$l_1\alpha_1(y)\alpha_1(x) + l_2\alpha_2(y)\alpha_2(x) + \cdots + l_n\alpha_n(y)\alpha_n(x) = 0$$
$$l_1\alpha_1(y)\alpha_1(x) + l_2\alpha_1(y)\alpha_2(x) + \cdots + l_n\alpha_1(y)\alpha_n(x) = 0$$

tulemuseks on võrrand

$$l_2\big(\alpha_2(y) - \alpha_1(y)\big)\alpha_2(x) + l_3\big(\alpha_3(y) - \alpha_1(y)\big)\alpha_3(x) + \cdots + l_n \underbrace{\big(\alpha_n(y) - \alpha_1(y)\big)}_{\neq 0} \alpha_n(x) = 0.$$

Kuna $x \in K$ on suvaline, siis oleme saanud uue $n - 1$ teisendust sisaldava lineaarselt sõltuva süsteemi, mille kordajad on induktsioonieelduse tõttu nullid. Siit $l_n = 0$ ja seega oleme saanud vastuolu minimaalsusega.

Lemma 2.4.2. *Korpuste lõpliku laiendi $L : K$ Galois' rühm* $\mathrm{Gal}(L : K)$ *on lõplik.*

TÕESTUS. Induktsiooni baas $[L : K] = 2$
Kui $[L : K] = 2$, siis $L = K(c)$, kus $c \in L$ on algebraline element. Olgu $m_c \in K[X]$ elemendi c minimaalne polünoom, siis lemma 2.2.1 põhjal peab automorfismide rühma $\mathrm{Gal}(K(c) : K)$ elementide arv olema väiksem või võrdne $\deg m_c$!.
Induktsiooni samm
Olgu laiendi mõõde $[F : K] = n$, üldsust kitsendamata leidub $c \in F \setminus K$ ja seega saame korpuste jada $K \subset K(c) \subseteq F$. Kõik automorfismide $\alpha \in \mathrm{Gal}(F : K)$ ahendid $\alpha \mid_{K(c)}$ laiendi $K(c) : K$ automorfismid, mida on tänu induktsiooni baasile lõplik arv. Seega saame me valida ülimalt $(\alpha_i)_{i=1}^n \in \mathrm{Gal}(F : K)$ nii, et nende ahendid $K(c)$ oleks kõik erinevad. Nüüd jagumeb hulk $\mathrm{Gal}(F : K)$ loomulikult lõplikuks hulgaks klassideks $C_i = \{\alpha \in \mathrm{Gal}(F : K) \mid \alpha \mid_{K(c)} \equiv \alpha_i \mid_{K(c)}\}$. Kui laiendi $F : K$ automorfism $\beta \in C_i$, siis ilmselt $(\alpha_i)^{-1}\beta \in \mathrm{Gal}(F : K(c))$. Paneme tähele, et tegu on injektiivse sisestusega $C_i \hookrightarrow \mathrm{Gal}(F : K(c))$, seega $|C_i| \leq |\mathrm{Gal}(F : K(c))|$, mille mõõde on väiksem kui n ja mis on seetõttu lõplik rühm. Kuna klasse on lõplik arv ja klassis on lõplik arv elemente, siis on hulk $\mathrm{Gal}(F : K)$ lõplik.

Teoreem 2.4.3. *Olgu G korpuse F lõplik automorfismirühm ja rühmateisenduste püsipunktide hulk $K = \mathrm{Inv}\, G = \{x \in F \mid \forall \alpha \in G\ \alpha(x) = x\}$, siis laiendi mõõde $[F : K] = |G|$.*

TÕESTUS. Olgu meil laiendi F baas $(a_i)_{i=1}^m$ üle K ja automorfismide rühm $G = (g_j)_{j=1}^n$. Näitame esmalt $m \geq n$. Moodustame väärtustuste maatriksi

$$M = \big(g_j(a_i)\big)_{i=1,j=1}^{m,n} \in \mathrm{Mat}_{m,n}(F).$$

Kui maatriksis oleks $m < n$, siis peaksid maatriksi veerud olema lineaarselt sõltuvad. Kuid kuna veergudes on teisenduse g_i väärtused baasielementidel, siis peaks $(g_j)_{j=1}^n$ süsteem olema lineaarselt sõltuv. Dedekindi lemma tõttu peaks $g_i \equiv g_j$, mis oleks vastuoluline.

Näitame veel $m \leq n$. Kui $m > n$, siis maatriksi M read peaksid olema lineaarselt sõltuvad, st. leiduks minimaalse arvu nullist erinevate elementidega mittetriviaalne jada $(b_i)_{i=1}^m \subseteq L$ nii, et

$$\sum_{i=1}^{m} b_i g_j(a_i) = 0, \qquad j = 1, 2, \ldots, m$$

Baasielemente a_i ümber järjestades saab tekitada olukorra, kus $b_i \neq 0$, kui $i \leq r$. Rakendades automorfismi rühma suvalist teisendust saame

$$\sum_{i=1}^{m} g(b_i) g_k(a_i) = 0, \qquad k = 1, 2, \ldots, m$$

Neist kahest võrdusest on lihtne saada

$$\begin{aligned} b_1 g(b_1) g_j(a_1) + b_2 g(b_1) g_j(a_2) + \cdots + b_r g(b_1) g_j(a_r) &= 0 \\ b_1 g(b_1) g_j(a_1) + b_1 g(b_2) g_j(a_2) + \cdots + b_1 g(b_r) g_j(a_r) &= 0 \\ g_j(a_2)\big(b_2 g(b_1) - b_1 g(b_2)\big) + \cdots + g_j(a_r)\big(b_r g(b_1) - b_1 g(b_r)\big) &= 0 \end{aligned}$$

Kuna esialgne kombinatisioon oli minimaalse arvu nullist erinevate elementidega, siis peab kehtima

$$b_i g(b_1) - b_1 g(b_i) = 0 \Leftrightarrow b_i b_1^{-1} = g(b_i d_1^{-1}), \qquad i = 2, 3, \ldots, r.$$

Kuna laiend $F : K$ on normaalne laiend, siis $b_i, b_1^{-1} \in K$. Seetõttu leiduvad $(c_i)_{i=1}^r \subseteq K$ ja element $d \in F^*$ nii, et $b_i = dc_i$ iga $i = 1, 2, \ldots, n$. Võtame $c_i = b_i b_1^{-1} \in K$ ja $d = b_1 \neq 0$, seetõttu saame võrduse

$$g_j(a_1)c_1 + g_j(a_2)c_2 + \cdots + g_j(a_r)c_r = 0.$$

Kuna g_j on automorfism, siis teisendab see vektoruumi baasi vektoruumi baasiks. Kuna $(c_i)_{i=1}^r \subseteq K$, siis $c_i = 0$ ja järelikult $1 = c_1 = 0$, mis on vastuolu.

Järeldus 2.4.3.1. *Olgu meil korpuste lõplik laiend $F : K$ ja automorfismide alamrühm $H \subseteq \mathrm{Gal}(F : K)$, siis korpuse laiendi $H' = \mathrm{Inv}\, H$ mõõde avaldub $[H' : K] = \frac{[F:K]}{|H|}$.*

Tõestus. On ilmne, et H peab olema lõplik. Eelmisest teoreemist $[F : H'] = |H|$ ja dimensioonide teoreemist $[F : H'][H' : K] = [F : K]$, millest järeldubki väide.

Lemma 2.4.4. *Olgu meil korpuste laiend $F : K$, siis iga vahepealse korpuse $K \subseteq L \subseteq F$ ja iga automorfismi $\alpha \in \mathrm{Gal}(F : K)$ korral $\big[\alpha(L)\big]' = \alpha L' \alpha^{-1}$.*

Tõestus. Tähistame $M = \alpha(L)$, siis ilmselt on $K \subseteq M \subseteq F$ alamkorpus. Võtame nüüd suvalise automorfismi $\gamma \in \mathrm{Gal}(F : L) = L'$ ja suvalise elemndi $c \in M$. Et $c \in M$, siis leidub $a \in L$ nii, et $\alpha(a) = c$, seega saame

$$(\alpha\gamma\alpha^{-1})(c) = (\alpha\gamma\alpha^{-1}\alpha)(a) = (\alpha\gamma)(a) = \alpha(a) = c.$$

See tähendab $\alpha L' \alpha^{-1} \subseteq M'$. Teisalt

$$M' \subseteq \alpha L' \alpha^{-1} \Leftrightarrow \alpha^{-1} M' \alpha \subseteq L'.$$

Selle näitamiseks võtame $\delta \in M'$ ja $a \in L$, seega saame

$$(\alpha^{-1}\delta\alpha)(a) = (\alpha^{-1}\delta(\alpha(a)) = (\alpha^{-1}\alpha)(a) = a,$$

mis tõestab kaa teistpidise sisestuse.

Galois' teoreem. *Olgu meil normaalne korpuste lõplik laiend $F : K$, mille mõõde on lõplik $[F : K] = n$. Tähistame $G = \mathrm{Gal}(F : K)$, siis kehtivad järgmised väited:*

1. *Galois' rühma elementide arv* $|G| = n$*;*
2. *kõik laiendi* $F : K$ *vahepealsed korpused on kinnised;*
3. *kõik rühma* G *alamrühmad on kinnised;*
4. *iga vahepealse korpuse* $K \subseteq L \subseteq F$ *korral kehtib* $[F : L] = |L'|$ *ja* $[L : K] = \frac{|G|}{|L'|}$*;*
5. *vahepealne korpuste laiend* $L : K$ *on normaalne parajasti siis, kui alamrühm* L' *on normaaljagaja* $L' \trianglelefteq G$*, siis* $\mathrm{Gal}(L : K) \cong G/L'$*.*

Tõestus.
(1)
Vastavalt lemmale 2.4.2 on rühm G lõplik. Teoreemi 2.4.3 tõttu saame kätte võrduse $n = |G| = [F : K]$, sest $K = \mathrm{Inv}\, G = \mathrm{Inv}(\mathrm{Gal}(F : K))$, kuna $F : K$ on normaalne.
(2)
Olgu meil vahepealne korpus $K \subseteq L \subseteq F$ näitame, et $L = \mathrm{Inv}(\mathrm{Gal}(L : K))$. Selleks paneme tähele, et normaalsus on samaväärne teoreemi 2.3.3 tõttu separaabi lahutuskorpuseks olemisega. Kui $F : K$ on polünoomi $f \in K[X]$ lahutuskorpus, siis on seda ka laiend $F : L$. Olgu meil element $c \in F \setminus L$ ning olgu $m_L \in L[X]$ elemendi minimaalne polünoom üle L ja $m_K \in K[X]$ elemendi c minimaalne polünoom üle K. On ilmne $m_K \in L[X]$, seega peab $m_L \mid m_K$ korpuses L ja kuna m_K ei sisalda kordseid juuri, siis ei saa neid sisaldada ka m_L. Seega on $F : L$ on polünoomi f separaabel lahutuskorpus.
(3)
Olgu meil alamrühm $H \subseteq G$ näitame, et see on kinnine. Galois' vastavuse põhiomaduse tõttu $H \subseteq H'' = \mathrm{Gal}(F : \mathrm{Inv}\, H)$. Teisalt on H lõplik ja tänu lemmale 2.4.2 ja lemmale 2.4.3 saame

$$|H''| = [F : \mathrm{Inv}\, H''] = [F : H'''] = [F : (H')''] = [F : H'] = |H|\,.$$

Kuna H ja H'' on lõplikud, siis $H = H''$.
(4)
Väite (2) tõestuses näitasime $F : L$ on normaalne laiend, kus $K \subseteq L \subseteq F$. Väitest (1) ilmneb $[F : L] = |\mathrm{Gal}(F : L)| = |L'|$. Tänu dimensioonide teoreemile

$$|G| = [F : K] = [F : L][L : K] = |L'|\,[L : K],$$

mis põhjendabki väite.
(5)
Olgu $L : K$ normaalne laiend. Siis peab L olema separaabel ja mingi polünoomi $f \in K[X]$ lahutuskorpus, seega $L = K(c_1, c_2, \ldots, c_n)$. Selleks, et näidata, et L' on normaaljagaja $L' \trianglelefteq G$ on tarvilik ja piisav iga $\alpha \in G$ saame sisalduvuse $\alpha L' \alpha^{-1} \subseteq L'$. Lemma 2.2.1 tõttu peab $\alpha(L) = L$, sest $\alpha|_L$ on kindlasti monomorfism ja seetõttu ei saa mitu juurt üheks kujutuda. Nüüd tänu lemmale 2.4.4 saame $L' = \big[\alpha(L)\big]' = \alpha L \alpha^{-1}$ ja seega peab L' olema normaaljagaja. Kui

meil on normaaljagaja $H \trianglelefteq G$ näitame $H' : K$ on normaalne laiend. Väite (3) tõttu $H'' = H$ ja seetõttu võime tähistada $L = H'$ ja $L' = H$. Võtame suvalise automorfismi $\alpha \in \mathrm{Gal}(F : K) = G$, nüüd normaaljagaja omadustest ja lemmast 2.4.4 saame

$$L' = \alpha L' \alpha^{-1} = \big[\alpha(L)\big]' \Rightarrow L = \alpha(L),$$

sest üldine Galois' vastavus on üksühene kinniste elementide korral ja L ja $\alpha(L)$ kui vahepealsed laiendid peavad olema kinnised. Selleks, et $L : K$ oleks normaalne on piisav näidata, et L on separaabel ja iga taandumatu polünoomi $f \in K[X]$ leidub juur $c \in L$ parajasti siis, kui L sisaldab kõiki juuri. Separaablus on ilmne, sest $F : K$ on separaabel. Oletame vastuväiteliselt $L : K$ korral leidub taandumatu polünoom $f \in K[X]$ nii, et leiduvad juured $c_1 \in L$ ja $c_2 \in F \setminus L$. Kuna $F : K$ on normaalne, siis lahutub f korpuses F esimese astme teguriteks. Vastavalt lemmale 2.2.3 leidub automorfism $\alpha \in \mathrm{Gal}(F : K)$ nii, et $\alpha(c_1) = c_2$, mis on ilmselt vastuolus $\alpha(L) = L$.

Nüüd on jäänud vaid näidata $\mathrm{Gal}(L : K) \cong G/L$. Vaatame lihtsalt teisendust $G \ni \alpha \xrightarrow{\psi} \alpha|_L \in \mathrm{Gal}(L : K)$. Esmalt veendume definitsiooni korrektsuses. Kuna $\alpha(L) = L$, siis on peab $\alpha|_L$ olema ilmselt L automorfism kui monomorfism, mis on sürjektiivne teisendus korpusesse L. Näitame ψ on sürjektiivne, selleks piisab kui veendume, et iga $\beta \in \mathrm{Gal}(L : K)$ saab laiendada $F : K$ automorfismiks. Kuna $L : K$ on normaalne, siis leidub polünoom $f \in K[X]$, mille lahutuskorpus on L. Lemma 2.2.3 tõestusest ilmneb, et selline jätkamine on võimalik. Rühmade homomorfismi teoreem kindlustab nüüd $\mathrm{Gal}(L : K) \cong G/\ker\psi$. Väide on tõestatud, kui $\ker\psi = L'$. See tuleneb otse definitsioonist $\ker\psi = \{\alpha \in \mathrm{Gal}(F : K) \mid \alpha|_L = I_L\} = L'$.

2.5 Näiteid Galois' vastavustest

Lause 2.5.1. *Olgu laiend $F : K$ lõplik polünoomi $f \in K[X]$ lahutuskorpus, siis on automorfismide rühm $\mathrm{Gal}(F : K) \hookrightarrow S_n$, kus $n = \deg f$ ja S_n on permutatsioonide rühm.*

Tõestus. Iga automorfism $\alpha \in \mathrm{Gal}(F : K)$ teisendab lemma 2.2.1 tõttu polünoomi f juured juurteks ja on üheselt määratud oma väärtustega juurtel. Olgu polünoomi f juured $(c_i)_{i=1}^n$, siis iga automorfism genereerib permutatsiooni hulgal $\{1, 2, \ldots, n\}$, sest see on injektiivne.

Laiendi $K : K$ automorfismi rühm $\mathrm{Gal}(K : K) = \{I_K\} \cong \mathbb{Z}_1$.

Kui laiendi $L : K$ mõõde on $[L : K] = 2$, siis on $\mathrm{Gal}(L : K) \cong S_2 \cong \{I, (1, 2)\} \cong \mathbb{Z}_2$. See on ilmne, sest peab leiduma element $c \in L \setminus K$ nii, et $k_2c^2 + k_1c + k_0 = 0$. Seega peab L olema elemendi c minimaalse polünoomi $m_c \in K[X]$ lahutuskorpus ning lemmade 2.2.1 ja 2.2.3 tõttu $\mathrm{Gal}(L : K) \cong S_2$. Näiteks $\mathbb{C} : \mathbb{R}$ ja $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$.

Kui laiendi $L : K$ mõõde $[L : K] = 3$, siis peab leiduma element $c \in L \setminus K$ nii, et minimaalse polünoomi $m_c \in K[X]$ aste oleks 3, kuna 3 on algarv. Nüüd on kaks võimalust. Esiteks võib $m_c = (X - c)g$, kus $g \in L[X]$ on taandumatu

üle L, siis ei ole laiend $L : K$ olla normaalne. Laiendi baasiks on $1, c, c^2$. Iga automorfism $\alpha \in \mathrm{Gal}(L : K)$ on üheselt määratud selle väärtustustega baasi elementidel. Kuna c on minimaalse polünoomi ainus juur korpuses L, siis $\alpha(c) = c$, teisalt $\alpha(1) = 1$. Nüüd $\alpha(c^2) = \alpha(c)\alpha(c) = c^2$. Seega moodustab automorfismi rühma $\mathrm{Gal}(L : K) = \{I\}$ ja $\mathrm{Inv}\, G = L$. Sellise laiendi näiteks $\mathbb{Q}\big(\sqrt[3]{2}\big) : \mathbb{Q}$, sest $\sqrt[3]{2}$ minimaalne polünoom avaldub kujul $X^3 - 2 = \big(X - \sqrt[3]{2}\big)\big(X^2 + \sqrt[3]{2}X + \sqrt[3]{4}\big)$, kus parempoolse polünoomi juurteks on $\left(-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i\right)\sqrt[3]{2} \notin \mathbb{Q}\big(\sqrt[3]{2}\big)$. Kui L on minimaalse polünoomi lahutuskorpus. Siis on kaks võimalust. Kui korpus L pole separaabel, siis minimaalne polünoom on kujul $m_c = (X - c)(X - d)^2$ ja analoogilistel põhjustel peab $\mathrm{Gal}(L : K) = \{I\}$. Kui lahutuskorpus L separaabel, siis on täidetud Galois' teoreemi eeldused ning $|\mathrm{Gal}(L : K)| = 3$. Lihtne on veenduda $\mathrm{Gal}(L : K) \cong \mathbb{Z}_3$. Näiteks sobib taandumatu polünoomi $f = X^3 + X + 1 \in \mathbb{Z}_2[X]$ lahutuskorpus $K(\alpha)$, kus $\alpha^3 + \alpha + 1 = 0$ ja mille minimaalne polünoom $X^3 + X + 1 = (X - \alpha)(X - \alpha^2)(X - \alpha^2 - \alpha)$.

Vaatame polünoomi $f = X^4 - 2 \in \mathbb{Q}[X]$ lahutuskorpust $\mathbb{Q}\big(\sqrt[4]{2}, i\big)$ automorfismide rühma $G = \mathrm{Gal}\left(\mathbb{Q}\big(\sqrt[4]{2}, i\big) : \mathbb{Q}\right)$. Lihtsuse mõttes tähistame $r = \sqrt[4]{2}$. Suvaline isomorfism $\alpha \in G$ on määratud väärtustustega $\alpha(r) \in \{\pm r, \pm ir\}$ ja $\alpha(i) = \pm i$, sest polünoomi juured peavad kujutuma polünoomide juurteks. Kokku on rühmas G vastavalt Galois' teoreemile kaheksa teisendust

α	$\alpha(r)$	$\alpha(i)$	α	$\alpha(r)$	$\alpha(i)$
I	r	i	τ	r	$-i$
σ	ir	i	$\sigma\tau$	ir	$-i$
σ^2	$-r$	i	$\sigma^2\tau$	$-r$	$-i$
σ^3	$-ir$	i	$\sigma^3\tau$	$-ir$	$-i$

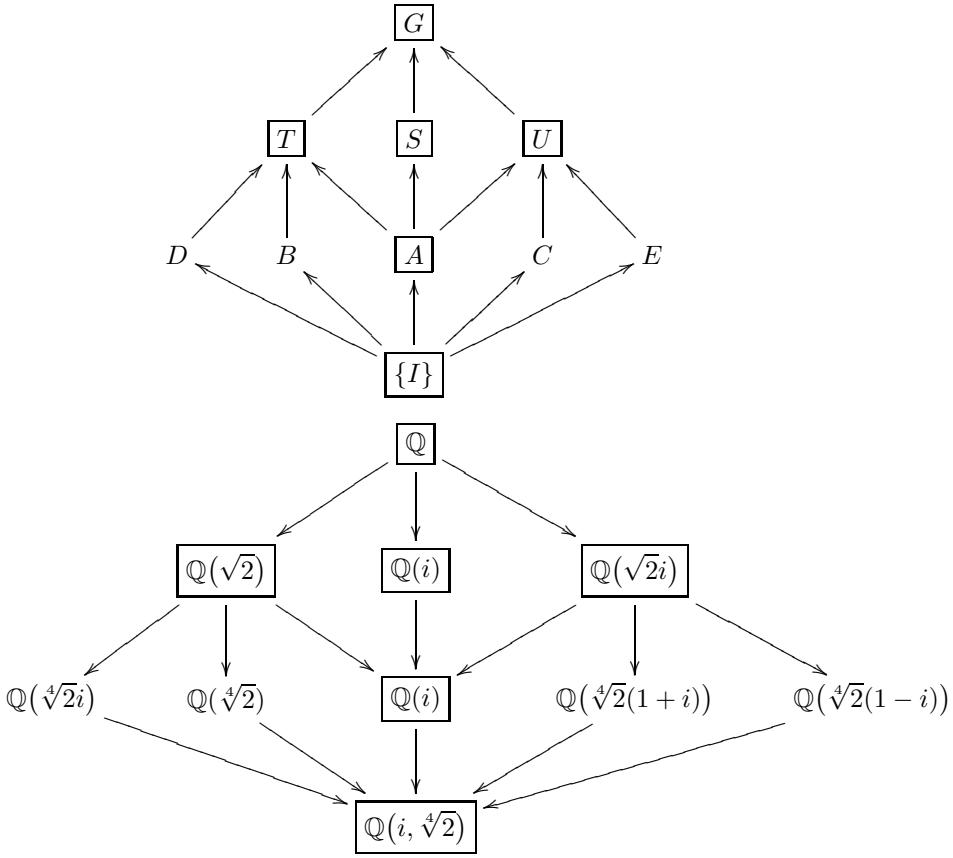
Seda rühm on isomorfne ruudu tippude sümmetriliste teisenduste rühmaga. Rühmad U ja T on omavahel isomorfsed ja selliseid rühmi nimetatakse nelirühmadeks ja tähistatakse $U \cong C_2 \times C_2 \cong V$. Arvestades, et $\tau\sigma = \sigma^3\tau$, saame rühma pärisalamrühmadeks

$$S = \big\{1, \sigma, \sigma^2, \sigma^3\big\} \qquad A = \big\{1, \sigma^2\big\} \qquad D = \big\{1, \sigma^2\tau\big\}$$
$$T = \big\{1, \sigma^2, \tau, \sigma^2\tau\big\} \qquad B = \{1, \tau\} \qquad E = \big\{1, \sigma^3\tau\big\}$$
$$U = \big\{1, \sigma^2, \sigma\tau, \sigma^3\tau\big\} \qquad C = \{1, \sigma\tau\}$$

Neist normaalsed alamrühmad on S, T, U, A. Leiame nüüd teisenduste püsipunktid

$$\mathrm{Inv}\, S = \mathbb{Q}(i) \qquad \mathrm{Inv}\, A = \mathbb{Q}\big(\sqrt{2}, i\big) \qquad \mathrm{Inv}\, D = \mathbb{Q}\big(\sqrt[4]{2}i\big)$$
$$\mathrm{Inv}\, T = \mathbb{Q}\big(\sqrt{2}\big) \qquad \mathrm{Inv}\, B = \mathbb{Q}\big(\sqrt[4]{2}\big) \qquad \mathrm{Inv}\, E = \mathbb{Q}\big(\sqrt[4]{2}(1 - i)\big)$$
$$\mathrm{Inv}\, U = \mathbb{Q}\big(\sqrt{2}i\big) \qquad \mathrm{Inv}\, C = \mathbb{Q}\big(\sqrt[4]{2}(1 + i)\big)$$

Sisalduvuseose järgi saame võred



2.6 Ühejuured ja neile vastavad Galois' rühmad

Lemma 2.6.1. *Olgu laiend $F : K$ separaabli polünoomi $X^n - 1$, kus $n \in \mathbb{N}$ lahutuskorpus, siis leidub primitiivne n-astme ühejuur ξ, mille poolt moodustatud multiplikatiivne rühm langeb kokku polünoomi $X^n - 1$ juurtega.*

Tõestus. Olgu meil polünoomi $X^n - 1$ mingi juur $\zeta \in F$ on ilmne ζ^i, $i \in \mathbb{Z}$ on samuti polünoomi juur, sest $(\zeta^i)^n = (\zeta^n)^i = 1$. Polünoomi $X^n - 1$ juured moodustavad rühma korrutamise suhtes, sest $(\zeta\eta)^n = \zeta^n\eta^n = 1$ ja kinnisus pöördelemendi võtmise suhtes on eelnevalt näidatud. Tähistame juurte multiplikatiivset rühma S. Kuna igas lõplikus rühmas leidub maksimaalse järguga element(jagamise suhtes). Olgu see element ξ. Lagrange' teoreemist saame $m = \operatorname{ord}\xi \mid |S|$. Seega on kõik rühma S elemendid juureks polünoomile $X^m - 1$. Polünoomi astme tõttu peab $|S| \leq m$ ja teisalt $m \leq |S|$ ja seega $m = |S|$. Kui polünoom $X^n - 1$ on separaabel, siis $|S| = n$ ja ξ on polünoomi $X^n - 1$ primitiivne ühejuur.

Järeldus 2.6.1.1. *Olgu korpuse K karakteristika* $\operatorname{kar} K = 0$ *korral leidub suvalise astme primitiivne ühejuur.*

TÕESTUS. Selleks veendume X^n-1 on separaabel kasutades tuletist $(X^n-1)' = nX^{n-1}$. Et tuletispolünoomi ainsaks juureks on 0, mis pole $X^n - 1$ juur, siis peavad kõik $X^n - 1$ juured olema ühekordsed.

Järeldus 2.6.1.2. *Olgu korpuse K karakteristika* $\operatorname{kar} K = p$. *Siis n-astme primitiivne ühejuur leidub parajasti siis, kui $p \nmid n$.*

TÕESTUS. Kui $p \nmid n$, siis $(X^n - 1)' = nX^{n-1} \neq 0$ ja seega on polünoom $X^n - 1$ separaabel, kuna tuletispolünoomi ainsaks juureks on 0. Kui $p \mid n$, siis leidub aste $k > 0$ $p^k d = n$ ja $p \nmid d$. Seega $X^n - 1 = (X^d - 1)^{p^k}$ ning seetõttu on polünoomi ühejuured moodustatud d-astme primitiivse ühejuure poolt ja iga juur on p^k kordne.

Lemma 2.6.2. *Olgu korpuse K karakteristika* $\operatorname{kar} K = 0$ *ja olgu laiend $F : K$ polünoomi $X^n - 1$ lahutuskorpus, siis on automorfimide rühm* $\operatorname{Gal}(F : K)$ *on Abeli rühm.*

TÕESTUS.

Vastavlt järeldusele 2.6.1.1 leidub meil primitiivne ühejuur $\xi \in F$ ja $F = K(\xi)$. Seetõttu on suvaline automorfism $\alpha \in \operatorname{Gal}(F : K)$ üheselt määratud väärtusega $\alpha(\xi) = \xi^k$. lihtne on veenduda $\alpha, \beta \in \operatorname{Gal}(F : K)$ kommuteeruvad kohal ξ, sest $\alpha\beta(\xi) = \alpha(\xi^l) = \alpha(\xi)^l = (\xi^k)^l = \xi^{kl}$.

Lemma 2.6.3. *Olgu korpuse K karakteristika* $\operatorname{kar} K = p$ *ja olgu laiend $F : K$ polünoomi $X^n - 1$ lahutuskorpus, siis on automorfimide rühm* $\operatorname{Gal}(F : K)$ *on Abeli rühm.*

TÕESTUS. Lemma 2.6.1 tõestusest ilmneb, et kõik ühejuured on mingi m-astme ühejuure $\xi \in F$ astmed, seega läheb eelnev tõestus läbi $F = K(\xi)$.

Lemma 2.6.4. *Olgu korpus K polünoomi $X^p - 1$, $p \in \mathbb{P}$ lahutuskorpus karakteristikaga* $\operatorname{kar} K = 0$ *ning laiend $F : K$ polünoomi $X^p - a$ lahutuskorpus, kus $a \in K$, siis automorfismirühm* $\operatorname{Gal}(F : K)$ *on Abeli rühm.*

TÕESTUS. Olgu $\xi \in K$ primitiivne p-astme ühejuur. Kui polünoomi $X^p - a$ kõik juured on korpuses K, siis on väide triviaalne, sest $\operatorname{Gal}(F : K) = 0$. Vastasel korral olgu $\zeta \in F \setminus K$ polünoomi $X^n - a$ juur. Tähistme nüüd $d = \xi\zeta$ ja seega $d^i = d^j$ ja $i, j < p$ parajasti siis, kui $\xi^{i-j} = \zeta^{j-i}$. Kui $r = j - i \neq 0$, siis peavad leiduma $u, v \in \mathbb{Z}$ nii, et $ru + pv = 1$. Aga siit saame vastuolu

$$\zeta = \zeta^{ru+nv} = \zeta^{ru}\zeta^{pv} = \xi^{-ru}a^v \in K$$

Seetõttu $F = K(d)$, kusjuures d on primitiivne juur ning eelnevatega analoogne tõestus läheb läbi.

Lemma 2.6.5. *Olgu korpus K polünoomi $X^p - 1$, $p \in \mathbb{P}$ lahutuskorpus karakteristikaga* $\operatorname{kar} K = q$ *ning laiend $F : K$ polünoomi $X^p - a$ lahutuskorpus, kus $a \in K$, siis automorfismirühm* $\operatorname{Gal}(F : K)$ *on Abeli rühm.*

TÕESTUS.
Juht $q \neq p$.
Lemma 2.6.1.2 tõttu leidub meil primitiivne p-astme ühejuur ja eelnevaga teoreemiga 2.6.4 analoogne tõestus läheb läbi.
Juht $q = p$.
Kui $b \in F$ on polünoomi $X^p - a$ juur, siis $X^p - a = X^p - b^p = (X - b)^p$. Seega $X^p - a$ ainus juur b. Tänu lemmale 2.2.1 iga $\alpha \in \mathrm{Gal}(F : K)$ korral $\alpha(b) = b$ ja seega on $\mathrm{Gal}(F : K) = 0$ ja teoreem on triviaalselt täidetud.

2.7 Radikaalsete laiendite Galois' rühmad

Definitsioon 2.7.1. *Rühma G nimetatakse lahenduvaks, kui temal leidub kommutatiivsete faktoritega normaaljada, st. $E = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_k = G$ ja H_i/H_{i-1} on kommutatiivne rühm.*

Lause 2.7.1. *Lõplik rühm on lahenduv parajasti siis, kui temal leidub tsükliste faktoritega normaaljada.*

TÕESTUS. Piisavus on ilmne. Tarvilikkuseks paneme tähele, et iga Abeli rühm laguneb tsükliliste Abeli rühmade otsesummaks. Kuna rühm G on lõplik, siis piisab vaid juhu $H_i/H_{i-1} = A_1 \oplus A_2$ läbi vaatmisest. Esmalt paneme tähele $A_1 \trianglelefteq A_1 \oplus A_2$, sest faktorrühm on kommutatiivne. Kolmandast isomorfismi teoreemist $H_i/M \cong (H_i/H_{i-1})/A_1 \cong A_2$, kus M on originaal loomuliku projektsiooni suhtes $M = \pi^{-1}(A_1)$. Teisalt $H_{i-1} = \pi^{-1}(0) \subsetneqq \pi^{-1}(A_1) = M \subseteq H_i$. Kuna $M \subsetneqq H_i$, siis ilmselt peab kehtima $0 \neq M/H_{i-1} \subsetneqq H_i/H_{i-1} = A_1 \oplus A_2$, mistõttu pole faktor triviaalne. Seega oleme lisanud normaaljadasse ühe mitteriviaalse normaaljagaja. Kuna rühm oli lõplik, siis peab mittetriviaalseid elementidest koosnev normaaljada olema lõplik, sest $|G| = \prod_i |H_i/H_{i-1}|$. Seetõttu antud protsess peatub ja me oleme saanud tsükliliste faktoritega normaaljada.

Lause 2.7.2. *Olgu rühma G normaaljagaja $H \trianglelefteq G$, siis rühm G on lahenduv parajasti siis, kui rühmad H ja G/H on lahenduvad.*

Definitsioon 2.7.2. *Korpuse laiendit $F : K$ nimetatakse radikaalseks kui leidub radikaalne jada $(c_i)_{i=1}^n \subseteq F$ ja naturaalarvud $(k_i)_{i=1}^n$ nii,et $F = K(c_1, c_2, \ldots, c_n)$ ja $c_i^{k_i} \in K(c_1, \ldots, c_{i-1})$, $i = 1, 2, \ldots, n$.*

Definitsioon 2.7.3. *Olgu meil korpuste (lõplik)laiend $F : K$, siis korpust $F \subseteq F_1$ nimetatakse laiendi $F : K$ normaalseks sulundiks üle K parajasti siis, kui laiend $F_1 : K$ on normaalne.*

Lemma 2.7.3. *Kui korpuse K karakteristika $\mathrm{kar}\, K = 0$ või K on lõplik korpus, siis leidub iga lõpliku laiendi $F : K$ korral leidub normaalne sulund üle K.*

TÕESTUS. Olgu $F = K(c_1, c_2, \ldots, c_n)$. Vaatme nüüd igale elemendile c_i vastavat minimaalset polünoomi $m_i \in K[X]$. Olgu $f = m_1 m_2 \cdots m_n \in K[X]$, siis laiendiks F_1 võtame polünoomi f lahutuskorpuse üle K. Kui $\mathrm{kar}\, K = 0$, siis on laiend F_1 automaatselt separaabel. Kui $K = \mathbb{F}_q$, siis $F_1 : F$ on lõplik laiend ja

seega on $F_1 : K$ samuti lõplik algebraline laiend. Lemma 2.3.2 on korpus F_1 separaabel kui lõpliku korpuse algebraline laiend.

Lemma 2.7.4. *Olgu korpuse K karakteristika $\operatorname{kar} K = 0$ või olgu K lõplik korpus. Kui $F : K$ on korpuste radikaalne laiend ning F_1 on F normaalne sulund üle K, siis laiend $F_1 : K$ on radikaalne.*

Tõestus. Teeme eelnevas lemmas 2.7.3 mainitud laienduskonstruktsiooni. Olgu $F = K(c_1, c_2, \ldots, c_n)$ ja $F_1 = K(c_1, c_2, \ldots, c_n, d_1, d_2, \ldots, d_m)$, kus elemendid $c_1, c_2, \ldots, c_n, d_1, d_2, \ldots, d_m$ on polünoomi $f = m_1 m_2 \cdots m_n \in K[X]$ kõik juured. Vastavalt lemmale 2.2.3 leidub automorfism $\alpha \in \operatorname{Gal}(F_1 : K)$ nii, et $\alpha(c_i) = d_j$, kui c_i ja d_j on minimaalse polünoomi m_i juurteks. Siis on lihtne veenduda, et korpus $\alpha(F)$ on radikaalne. Et F on radikaalne, siis $c_l^{k_l} \in K(c_1, \ldots, c_{l-1})$, kuid siis

$$\alpha(c_l)^{k_l} = \alpha(c_l^{k_l}) \subseteq \alpha(K(c_l \ldots, c_{l_1})) = K(\alpha(c_1), \ldots, \alpha(c_{l-1})).$$

Seega oleme näidanud d_j on avaldatav radikaalse jada $c_1, \ldots, c_n, \alpha(c_1), \ldots, \alpha(c_n)$. elemendina. Paneme tähele, et jada lõppu võib lisada teise d_k vastava radikaalse jada jne. Seega saame lõpuks radikaalse jada, mis sisaldab kõiki d_j ja seega on F_1 radikaalne.

Teoreem 2.7.5. *Olgu korpuse K karakteristika $\operatorname{kar} K = 0$ või olgu K lõplik korpus, siis normaalse radikaalse laiendi $F : K$ automorfismirühm $\operatorname{Gal}(F : K)$ on lahenduv.*

Tõestus. Induktsioon üle radikaalse jada pikkuse.
Olgu laiendit F moodustav radikaalne jada $(c_i)_{i=1}^n$. Üldsust kitsendamata võib eeldada $c_i^{p_i} \in K(c_1, \ldots, c_{i-1})$ ja $c_i \notin K(c_1, \ldots, c_{i-1})$ ning $p_i \in \mathbb{P}$.
Baas $n = 0$
Siis $F = K$ ja $\operatorname{Gal}(F : K) = 0$ ja väide on ilmne.
Induktsiooni samm
Olgu $m_c \in K[X]$ elemendi c_1 minimaalne polünoom. Kuna $c_1 \notin K$, siis peab minimaalne polünoomi aste $\deg m_c > 1$. Et F on normaalne ning separaabel, siis leidub minimaalse polünoomi m_c juur $d \neq c$. Seega leidub korpuse F element $a = cd^{-1} \neq 1$. Et $c_1^{p_1} = b \in K$, siis c polünoomi $f = X^{p_1} - b \in K[X]$ juur. Kuna m_c on minimaalne polünoom, siis $m_c \mid X^{p_1} - b$ ja seega on element d ka polünoomi f juur. Nüüd saame $a^{p_1} = 1$ mistõttu $\langle a \rangle$ on lõplik p_1 elemendiline rühm, kuna $p_1 \in \mathbb{P}$ ja $a \neq 1$. Vaatleme korpuse laiendit $K(a)$, siis on ilmne, et see on polünoomi $g = X^{p_1} - 1 \in K[X]$ lahutuskorpus. Laiend $K(a, c) : K$ on polünoomi f lahutuskorpus, kuna $(c_1 a^i)_{i=1}^n$ on polünoomi f ainsateks juureks. Teisalt on selge, et polünoomi f lahutuskorpus peab sisaldama kõiki polünoomi g juuri ja seega ka elementi a. Kuna teoreemi eelduste tõttu on kõik laiendid separaablid, siis laiendid $K(a) : K$ ja $K(a, c_1) : K$ on normaalsed. Galois teoreemist saame $\operatorname{Gal}(F : K(a, c_1)) \trianglelefteq \operatorname{Gal}(F : K)$ ja seega

$$\operatorname{Gal}(K(a, c_1) : K) \cong \operatorname{Gal}(F : K) / \operatorname{Gal}(F : K(a, c_1)).$$

Rühm $\mathrm{Gal}(F : K(a, c_1))$ on lahenduv induktsiooni eelduse põhjal, sest radikaalne jada on ühe võrra lühem. Näitame, et $\mathrm{Gal}(K(a, c_1) : K)$ on lahenduv, sest siis on seda ka faktoriseeritav rühm. Kuna laiendid $K(a) : K$ ja $K(a, c_1) : K$ on normaalsed, siis Galois' teoreemist saame

$$\mathrm{Gal}(K(a) : K) \cong \mathrm{Gal}(K(a, c_1) : K)/\,\mathrm{Gal}(K(a, c_1) : K(a)).$$

Rühmad $\mathrm{Gal}(K(a) : K)$ ja $\mathrm{Gal}(K(a, c_1) : K(a))$ on lemmade 2.6.2, 2.6.3, 2.6.4 ja 2.6.5 tõttu Abeli rühmad, mistõttu on $\mathrm{Gal}(K(a, c) : K)$ on lahenduv.

Järeldus 2.7.5.1. *Olgu korpuse K karakteristika $\mathrm{kar}\, K = 0$ või olgu K lõplik korpus. Siis radikaalse laiendi $F : K$ iga alamkorpuse $K \subseteq L \subseteq F$ automorfismirühm $\mathrm{Gal}(L : K)$ on lahenduv.*

Tõestus. Kuna F on radikaalne, siis laiend $F : K$ lõplik. Nüüd saame teha laiendite jada $K \subseteq K_1 \subseteq F \subseteq F_1$, kus $K_1 = \mathrm{Inv}\,\mathrm{Gal}(L : K)$ ja F_1 on tänu lemmadele 2.7.3 ja 2.7.4 radikaalse laiendi F normaalne radikaalne sulund üle K. On selge, et $\mathrm{Gal}(L : K) = \mathrm{Gal}(L : K_1)$ ja konstruktsiooni tõttu on laiend $L : K_1$ on normaalne. Galois' teoreemist järeldub $L' = \mathrm{Gal}(F_1 : L) \trianglelefteq \mathrm{Gal}(F_1 : K_1)$ ja $\mathrm{Gal}(L : K_1) \cong \mathrm{Gal}(F_1 : K_1)/\,\mathrm{Gal}(F_1 : L)$. Kuna laiend $F_1 : K_1$ on normaalne radikaalne laiend, siis eelneva teoreemi 2.7.5 tõttu on automorfimi rühm $\mathrm{Gal}(F_1 : K_1)$ lahenduv ja seega on seda ka faktorrühm $\mathrm{Gal}(L : K)$.

Järeldus 2.7.5.2. *Lõpliku korpuse iga laiendi automorfismirühm on lahenduv.*

Tõestus. Iga lõplik korpus on radikaalne kui polünoomi $X^{p^n} - 1 \in \mathbb{Z}_p[X]$ lahutuskorpus, siis järeldus 2.7.5.1 põhjendab väite.

2.8 Lahenduvate rühmadele vastavad laiendid

Definitsioon 2.8.1. *Olgu $L : K$ korpuste lõplik normaalne laiend, mille automorfimirühm $G = \mathrm{Gal}(L : K)$, siis suvalise elemendi $a \in L$ normiks $N(a)$ nimetatakse suurust $N(a) = \prod_{\alpha \in G} \alpha(a) \in K$*

Tõestus. Näitame, et definitsioon on korrektne. Olgu $\beta \in G$, siis

$$\beta\big(N(a)\big) = \prod_{\alpha \in G} \beta\alpha(a)) = \prod_{\alpha \in G} \alpha(a) = N(a).$$

Kuna $L : K$ on normaalne, siis $N(a) \in K$.

Teoreem 2.8.1 (Hilberti XC teoreem)**.** *Olgu $L : K$ korpuste lõplik normaalne laiend tsüklilise automorfismide rühmaga $G = \mathrm{Gal}(L : K)$, mille järk n ja moodustaja τ. Elemendi $a \in L$ korral $N(a) = 1$ parajasti siis, kui leidub $b \in L^*$ nii, et $a = b\tau(b)^{-1}$.*

Tõestus. Piisavus on ilmne, sest

$$N(a) = b\tau(b)^{-1}\tau(b)\tau^2(b)^{-1} \cdots \tau^{n-1}(b)\tau^n b^{-1}(b) = 1.$$

Tarvilikkus
Kui $1 = N(a) = a\tau(a)\tau^2(a)\cdots\tau^{n-1}(a)$ ja $a \neq 0$. Defineerime iga $c \in F$ elementide jada $(d_i)_{i=0}^{n-1}$ rekurentse seose $d_0 = ac$, $d_{i+1} = a\tau(d_i)$ abil. Lihtne arvutus näitab

$$\begin{aligned} d_i &= a\tau(a)\tau^2(a)\cdots\tau^i(a)\tau^i(c) \\ d_{n-1} &= \underbrace{a\tau(a)\tau^2(a)\cdots\tau^{n-1}(a)}_{N(a)=1}\tau^{n-1}(c) = \tau^{n-1}(c). \end{aligned}$$

Vaatleme nüüd summat $b = d_0 + d_1 + \cdots d_{n-1}$. Andes sellele nüüd teise kuju, saame

$$b = \lambda_0 c + \lambda_1\tau(c) + \cdots + \lambda_{n-1}\tau^{n-1}(c), \qquad \lambda_i \in L.$$

Kui iga $c \in F$ on $b = 0$, siis on $1, \tau, \cdots, \tau^{n-1}$ lineaarselt sõltuvad ja Dedekindi lemmast saame vastuolu, kuna $\tau^i \neq \tau^j$, kui $i \neq j$. Seega leidub $c \in F$, mille korral $b \neq 0$. Arvutame

$$\begin{aligned} b\tau(b)^{-1} =& (d_0 + d_1 + \cdots + d_{n-1})(aa^{-1})(\tau(d_0) + \tau(d_1) + \cdots + \tau(d_{n-1}))^{-1} \\ =& (d_0 + d_1 + \cdots + d_{n-1})(a\tau(d_0) + a\tau(d_1) + \cdots + a\tau(d_{n-1}))^{-1} \\ =& (d_0 + d_1 + \cdots + d_{n-1})(d_1 + d_2 + \cdots + d_{n-1} + d_0)^{-1} = a. \end{aligned}$$

Teoreem 2.8.2. *Sisaldagu korpus K polünoomi $p \in \mathbb{P}$ primitiivset ühejuurt. Kui $L : K$ korpuste lõplik normaalne laiend, mille automorfismi rühm $G = \mathrm{Gal}(L : K)$ on tsüliline ja $|G| = p$, siis $L = K(d)$, kus $d^p = a \in K$ ja polünoom $X^p - a$ on taandumatu üle K.*

Tõestus. Olgu primitiivne ühejuur $\xi \in K$, seega polünoomi $X^p - 1$ juured moodustavad tsüklilise rühma $\langle\xi\rangle$ ja $\mathrm{kar}\, K \neq p$. Elemendi ξ norm avaldub

$$N(\xi) = \prod_{i=0}^{p-1}\tau^i(\xi) = \prod_{i=0}^{p-1}\xi = \xi^p = 1.$$

Hilberti XC teoreemi põhjl leidub nüüd element $d \in L^*$ nii, et $\xi = d\tau(d)^{-1}$. Tähistame $a = d^p$, siis selleks, et näidata $a \in K$ piisab, kui näidata $\tau(a) = a$. Arvutame $\tau(a) = \tau(d^p) = \tau(d)^p = (d\xi^{-1})^p = d^p(\xi^p)^{-1} = d^p = a$. Kindlasti on meil ahel $K \subseteq K(d) \subseteq L$. Kuna $[L : K] = |G| = p$ on algarv, siis peab $K(d) = L$ või $d \in K$. Kuna ξ on primitiivne ühejuur $\xi \neq 1$ ja seega ei saa $d \in K$. Kui $X^p - a$ poleks taandumatu, siis leiduks väiksema astmega taandumatu polünoom, mille juured on $X^p - a$ juured. Selle lahutuskorpus indutseeriks korpuste K ja $K(d)$ vahele vahepealse laiendi, mis läheb vastuollu mõõtme p algarvulisusega.

Teoreem 2.8.3. *Olgu korpuse K karakteristika $\mathrm{kar}\, K = 0$ või K lõplik korpus. Kui korpuste lõplik laiend $L : K$ on normaalne ja automorfismide rühm $G = \mathrm{Gal}(L : K)$ on lahenduv, siis leidub korpuse L laiend F nii, et laiend $F : K$ on radikaalne.*

Tõestus. Kui K on lõplik korpus, siis iga normaalne laiend on lõplik korpus. Kuna kõik lõplikud korpused on polünoomi $X^{p^n} - 1 \in \mathbb{Z}_p[X]$ lahutuskorpused, siis on laiend L radikaalne.

Kui korpuse karakteristiska $\operatorname{kar} K = 0$, siis tõestame väite induktsiooniga üle automorfismi rühma G võimsuse.
Baas $G = \{I\}$
Eelduse kohaselt on $L : K$ normaalne ja seega $K = \operatorname{Inv} G = L$ ning teoreemi väide on triviaalne $F = K$.
Induktsiooni samm
Olgu G lahenduv rühm. Olgu H rühma G maksimaalne normaaljagaja, siis peab G/H olema ka lahenduv rühm. Teisalt on G/H konstruktsiooni tõttu lihtne rühm. Seetõttu peab $G/H \cong \mathbb{Z}_p$, kus $p \in \mathbb{P}$. Olgu nüüd laiend $K_1 : K$ polünoomi $X^p - 1$ lahutuskorpus üle K. Kuna laiend $L : K$ on normaalne, siis on see $f \in K[X]$ lahutuskorpus. Võtame nüüd laiendiks $L_1 : K$ polünoomi f lahutuskorpust üle K_1. Laiend $L_1 : K$ on normaalne laiend kui polünoomi $(X^p - 1)f \in K[X]$ separaabel lahutuskorpus. Galois' teoreemist tulenevalt on laiendid $L_1 : K_1$ ja $L_1 : L$ normaalsed. Paneme tähele, et automorfismi rühma $\operatorname{Gal}(L_1 : K_1)$ elemendi α ahend $\alpha|_K = (\alpha|_{K_1})|_K = I_K$ ja seega $\operatorname{Gal}(L_1 : K_1) \subseteq \operatorname{Gal}(L_1 : K)$. Kui $\alpha \in \operatorname{Gal}(L_1 : K_1)$, siis $\alpha(L) = L$, sest lemma 2.2.1 tõttu peavad polünoomi f juured peavad kujutuma üksüheselt f juurteks. Seega on selge $\alpha|_L$ on nii injektsioon kui sürjektisioon ja seega ahendusteisendus $\Phi : \operatorname{Gal}(L_1 : K_1) \to \operatorname{Gal}(L : K)$ on korrektne homomorfism. Olgu $\alpha \in \operatorname{Ker} \Phi$, siis $\alpha|_L = I_L$ ja definitsioonist $\alpha|_{K_1} = I_{K_1}$. Korpuse L_1 konstruktsiooni tõttu saame $\alpha = I_{L_1}$. Ja seega on Φ injektsioon. Tähistme $G_1 = \operatorname{Gal}(L_1 : K_1)$. Tekib sisestus $G_1 \overset{\Phi}{\hookrightarrow} G$. Nüüd on kaks võimalust.
A. Kui $|G_1| < |G|$, siis G_1 on lahenduv kui G alamrühm ja seega täidetud induktsiooni eeldus. Nüüd peab leiduma laiendi $L_1 : K_1$ radikaalne lahend F. Et laiend $K_1 : K$ on radikaalne, siis $F : K$ ka radikaalne. Teisalt $L \subseteq L_1 \subseteq F$.
B. Kui $|G_1| = |G|$, siis Φ on isomorfism ja $G_1 \cong G$. Olgu $H_1 = \Phi^{-1}(H) \trianglelefteq G_1$. Moodustame laiendi $M = \operatorname{Inv} H_1$, konstruktsiooni tõttu $K_1 \subseteq M \subseteq L_1$. Laiendid $L_1 : M$ ja $M : K_1$ on normaalsed, sest $H_1 \trianglelefteq G_1$. Galois' teoreemist saame $[M : K_1] = |G_1/H_1| = |\mathbb{Z}_p| = p$. Et korpuses K_1 leidub primitiivne p-astme ühejuur ning $|\operatorname{Gal}(M : K_1)| = [M : K_1] = p$, siis $M : K_1$ rahuldab teoreemi 2.8.2 eeldusi ja $M = K_1(d)$ on radikaalne laiend üle K. Kui $H_1 = \{I\}$, siis $M = L_1$ ja väide on tõestatud. Vastasel korral teame, et normaalse laiendi $L_1 : M$ automorfismi rühma H_1 elementide arv on väiksem G elementide arv ja seega on laiendil $L_1 : M$ radikaalne laiend $L \subseteq L_1 \subseteq F$ vastavalt induktsiooni eeldusele, mis on ka korpuse K radikaalne laiend.

2.9 Polünoomi juurte üldvõrrandid

Definitsioon 2.9.1. *Korpuste laiend $L : K$ on lõplikult moodustatud parjasti siis, kui leidub lõplik arv elemente $c_1, c_2, \ldots, c_n \in L$ nii, et $L = K(c_1, c_2, \ldots, c_n)$.*

Definitsioon 2.9.2. *Korpuste laiendi $L : K$ elementide $(c_i)_{i=1}^n \subseteq L$ süsteem on algebraliselt sõltuv parajasti siis, kui leidub unitaarne mitmemuutujapolünoom*

$f \in K[X_1, X_2, \ldots, X_n]$ nii, et $f(c_1, c_2, \ldots, c_n) = 0$.

Järeldus 2.9.0.1. *Kui korpuste laiendi $L : K$ elementide $(c_i)_{i=1}^n \subseteq L$ süsteem on algebraliselt sõltumatu, siis elemendid $(c_i)_{i=1}^n$ on transtsendentsed.*

Lemma 2.9.1. *Kui laiend $F : K$ on lõplikult moodustatud, siis leidub vahepealne korpus L nii, et*

1. *laiend $L = K(c_1, c_2, \ldots, c_n)$, kusjuures elemendid $c_1, c_2, \ldots, c_n$ on algebraliselt sõltumatud elemendid üle K;*

2. *laiend $F : L$ on lõplik.*

Tõestus. Induktsioon üle F moodustajate arvu.
Baas $F = K(a)$ on triviaalne.
Induktsiooni samm
Olgu korpus $F = K(a_1, a_2, \ldots, a_n)$. Kui elemendid $(a_i)_{i=1}^n$ on algebralised üle K, siis $L = K$ ja väide on tõestatud. Vastasel korral leidub element $c_1 = a_i$, mis on transtsendentne üle K. Ilmselt $F = K(c_1)(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$ kuna F on moodustajaid üle $K(c_1)$ on ühe võrra vähem, siis kehtib induktsioonieeldus ja leiduvad algebraliselt sõltumatute elemendide süsteem $(c_i)_{i=2}^n$ üle $K(c_1)$ ja laiend $F : K(c_1)(c_2, \ldots, c_n)$ on lõplik. Elemendide süsteem $(c_i)_{i=1}^n$ peab olema algebraliselt sõltumatu üle K, sest vastasel korral oleks elementide süsteem $(c_i)_{i=2}^n$ sõltumatu üle $K(c_1)$.

Teoreem 2.9.2 (Steinitzi teoreem)**.** *Olgu korpused L ja M laiendi $F : K$ vahepealsed korpused, kusjuures $F : L$ ja $F : M$ on lõplikud laiendid. Kui laiendid on kujul $L = K(c_1, c_2, \ldots, c_m)$ ja $M = K(d_1, d_2, \ldots, d_n)$, kus elementide süsteemid $(c_i)_{i=1}^m$ ja $(d_j)_{j=1}^n$ algebraliselt sõltumatud, siis $m = n$.*

Tõestus. Üldsust kitsendamata võime eeldada $m \leq n$. Väite tõestamiseks näitame, et kahe algebraliselt sõltumatu erineva süsteemi $(c_i)_{i=1}^m$ ja $(d_j)_{j=1}^n$ korral, mis rahuldavad teoreemi eeldusi leidub algebraliselt sõltumatute elementide süsteem $(d_{j_0}, c_1, \ldots, c_{i_0-1}, c_{i_0+1}, \ldots, c_m)$, kusjuures süsteemile vastav korpuste laiend $F : K(d_{j_0}, c_1, \ldots, c_{i_0-1}, c_{i_0+1}, \ldots, c_m)$ on lõplikumõõtmeline ja d_{j_0} erineb elementidest c_i. Nii saab järjestikku asendada kõik elemendid c_i elementidega d_i tulemuseks on algebraline süsteem $(d_i)_{i=1}^m$ nii, et laiend $F : K(d_1, \ldots, d_m)$ on lõplikumõõtmeline. Siit saame $n \leq m$, sest vastasel korral oleks element d_n algebraline üle $K(d_1, d_2, \ldots, d_m)$, mis on vastolus süsteemi $(d_j)_{j=1}^n$ algebralise sõltumatusega. Seega $m = n$ ja teoreem on tõestatud.

Kuna süsteemid $(c_i)_{i=1}^m$ ja $(d_j)_{j=1}^n$ erinevad, siis leidub d_{j_0} nii, et $d_{j_0} \neq c_i$. Samas $F : L$ on lõplikumõõtmeline laiend ja seega on element d_{j_0} algebraline üle L. See tähendab, et leidub unitaarne polünoom $f \in K[X_1, X_2, \ldots, X_m, X_{m+1}]$ nii, et $f(c_1, c_2 \ldots, c_m, d_1) = 0$. Oletame vastuväiteliselt, et ainsad nullist erineva kordajaga liikmed sisaldavad vaid c_i astmeid, mis kuuluvad ka süsteemi $(d_j)_{j=1}^n$. See tähendaks, et polünoomi f saab väärtustada $f(d_{i_1}, d_{i_2}, \ldots, d_{i_m}, d_{j_0}) = 0$ ja süsteem $(d_j)_{j=1}^n$ on algebraliselt sõltuv. Seega leidub c_{i_0} nii, et sellele vastab nullist erineva kordajaga monoom. Nüüd c_{i_0} on algebraline üle üle $L' =$

$K(d_{j_0}, c_1, \ldots, c_{i_0-1}, c_{i_0+1}, \ldots, c_m)$. Kuna laiendid $F : K(d_{i_0}, c_1, c_2, \ldots, c_n)$ ja $K(d_{j_0}, c_1, c_2, \ldots, c_m) : L'$ on lõplikumõõtmelised, siis on seda ka $F : L'$.

Definitsioon 2.9.3. *Lõplikult moodustatud laiendi $F : K$ transtsendentsuse astmeks nimetatakse maksimaalses algebraliselt sõltumatute elementide süsteemis olevate elementide arvu.*

Lause 2.9.3. *Sama arvu algebraliselt sõltumatute elementide lisamisel korpusele K saadud laiendid $K(c_1, c_2, \ldots, c_n)$ ja $K(d_1, d_2, \ldots, d_n)$ on isomorfsed.*

Lemma 2.9.4. *Olgu laiend $F : K$ lõplikult moodustatud algebraliselt sõltumatute elementide süsteemi $(X_i)_{i=1}^n$ poolt, siis automorfismi rühm $G = \mathrm{Gal}(F : K)$ sisaldab substitutsioonide rühmaga S_n isomorfset teisenduste rühma, mis teisendab omavahel elemente X_i . Olgu $L = \mathrm{Inv}\, S_n$, siis $L = K(s_1, s_2, \ldots, s_n)$, kus s_i on sümmetrilised põhipolünoomid.*

Tõestus. Lihtne on veenduda, et teisendus $\alpha : F \to F$, mis saadakse substitutsiooni $\pi \in S_n$ abil nii, et võrrandeid $\alpha(X_i) = X_{\pi(i)}$ laiendatakse kooskõlas liitmise ja korrutamisega on isomorfismid, mis jätavad K elemendid paigale, seega $S_n \hookrightarrow G$. Ka on selge $K(s_1, \ldots, s_n) \subseteq L$. Kuna $F : L$ on normaalne laiend, siis Galos' teoreemist saame $[F : L] = |S_n| = n!$. Kui õnnestub näidata $[F : K(s_1, \ldots, s_n)] \leq n!$, siis dimensioonide teoreemi tõttu $L = K(s_1, \ldots, s_n)$, sest

$$[F : K(s_1, \ldots, s_n)] = [F : L][L : K].$$

Näitame $[F : K(s_1, \ldots, s_n)] \leq n!$ induktsiooniga üle muutujate arvu n.
Baas $n = 1$ on triviaalne, sest $s_1 = X_1$.
Induktsiooni samm
Paneme tähele, et leidub lihtne seos muutujatest $X_1, \ldots, X_{n-1}$ sõltuvate põhipolünoomide $s'_1, s'_2, \ldots, s'_{n-1}$ ja põhipolünoomide $s_1, s_2, \ldots, s_n$ vahel

$$s_1 = X_n + s'_1 \qquad s_i = X_n s'_{i-1} + s'_i, \qquad i = 2, \ldots, n-1 \qquad s_n = X_n s'_{n-1}.$$

Seega saame sisalduvuse $K(s_1, \ldots, s_n, X_n) \subseteq K(s'_1, \ldots, s'_{n-1}, X_n)$ Kuna seosed on pööratavad

$$s'_1 = S_1 - X_n \qquad\qquad s'_i = s_i - X_n s'_{i-1}, \qquad j = 2, \ldots, n-1,$$

siis kehtib ka vastupidine sisalduvus $K(s'_1, \ldots, s'_{n-1}, X_n) \subseteq K(s_1, \ldots, s_n, X_n)$. Nüüd induktsiooni eelduse tõttu

$$[K(X_n)(X_1, \ldots, X_{n-1}) : K(X_n)(s'_1, \ldots, s'_{n-1})] \leq (n-1)!.$$

Laiendi $K(s_1, \ldots, s_n, X_n) : K(s_1, \ldots, s_n)$ mõõde peab olema väiksem võrdne n, sest X^n on unitaarse polünoomi $f = \prod_{i=1}^n (X - X_i)$ juureks ning Viete'i valemite põhjal avaldub

$$f = X^n - s_1 X^{n-1} + s_2 X^{n-1} - \cdots + (-1)^n s_n \in K(s_1, s_2, \ldots, s_n)[X]$$

Dimensioonide teoreemist saamegi $[K(X_1, \ldots, X_n) : K(s_1, \ldots, s_n)] \leq n!$, mis lõpetab teoreemi tõestuse.

Järeldus 2.9.4.1. *Sümmetrilised põhipolünoomid $s_1, s_2, \ldots, s_n$ on algebraliselt sõltumatud.*

TÕESTUS. Oletame vastuväiteliselt, et sümmetrilised polünoomid on algebraliselt sõltuvad, siis peab s_i olema alagebraline üle $K(s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$ seega laiend $K(X_1, \ldots, X_n) : K(s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$ on lõplikumõõtmeline. See on vastuolu, kuna laiendi $K(X_1, \ldots, X_n)$ transtsendentsuse aste on n.

Definitsioon 2.9.4. *Üldiseks n-nda astme polünoomiks üle korpuse K nimetatakse polünoomi*

$$f = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n.$$

kus s_1, s_2, s_n on algebraliselt sõltumatud elemendid.

Teoreem 2.9.5. *Olgu f üldine n-nda astme polünoom üle K ja F olgu selle lahutuskorpus üle $K(s_1, s_2, \ldots, s_n)$, siis polünoomi f juured $(X_i)_{i=1}^n$ on algebraliselt sõltumatud üle K ja automorfismide rühm $Gal(F : K(s_1, s_2, \ldots, s_n)) \cong S_n$.*

TÕESTUS. Kuna $(X_i)_{i=1}^n$ polünoomi f juured, siis vastavalt Viete' valemitele on $(s_i)_{i=1}^n$ sümmetrilised põhipolünoomid ja $F = K(X_1, \ldots, X_n)$. Kuna $F : K(s_1, \ldots, s_n)$ on lõplikumõõtmeline laiend, ja $(s_i)_{i=1}^n$ on algebraliselt sõltumatu süsteem, siis laiendi $F : K$ transtsendentsuse aste peab olema n. Seega pole võimalik, et süsteem $(X_i)_{i=1}^n$ oleks algebraliselt sõltuv. Lemma 2.9.3 tõttu $K(s_1, \ldots, s_n) = \operatorname{Inv} S_n$ ja seega laiend $F : K(s_1, \ldots, s_n)$ on normaalne. Olgu laiendi automorfismi rühm $S_n \subseteq G$. Nüüd Galois' teoreemist saame

$$\operatorname{Gal}(F : K(s_1, \ldots, s_n)) = \operatorname{Gal}(F : \operatorname{Inv} S_n) = S_n'' = S_n,$$

kuna kõik G alamrühmad on kinnised.

Järeldus 2.9.5.1. *Kui $n \geq 5$, siis pole üldisel n-astme polünoomi juur radikaalides avalduv. Seega üldiselt pole võimalik avaldada n-nda astme polünoomi juurt radikaalides.*

Teoreem 2.9.6. *Üldise teise astme polünoomi f juured avalduvad kujul*

$$c_1 = \frac{s_1 + \sqrt{s_1^2 - 4s_2}}{2} \qquad c_2 = \frac{s_1 - \sqrt{s_1^2 - 4s_2}}{2},$$

kui korpuse karakteristika $\operatorname{kar} K \neq 2$.

TÕESTUS. Olgu üldise 2-astme polünoomi lahutuskorpuse automorfismi rühm $G \cong S_2$, siis avaldis $(X_1 - X_2)^2 \operatorname{Inv} G$ ja seega peab avalduma põhipolünoomide kaudu

$$(X_1 - X_2)^2 = (X_1 + X_2)^2 - 4X_1X_2 = s_1^2 - 4s_2.$$

Tekiv lineaarvõrrandite süsteemi

$$X_1 - X_2 = \sqrt{s_1^2 - 4s_2} \qquad X_1 + X_2 = s_1$$

lahendid ongi polünoomi juurteks.

Teoreem 2.9.7. *Üldise kolmanda astme polünoomi f juured avalduvad radikaalides, kui korpuse K karakteristika* $\operatorname{kar} K \neq 3$.

TÕESTUS. Olgu üldise 2-astme polünoomi lahutuskorpuse automorfismi rühm $G \cong S_3$, siis paarissubstitutsioonide rühm $A_3 = \{I, (2,3,1), (3,1,2)\}$ on S_3 normaaljagaja. Lisame korpusesse K 3-astme primitiivse ühejuure d ja vaatleme üldist võrrandit üle $K(d)$. Siis elemendi $y = X_1 + X_2 d + X_3 d^2$ mõjub teisenduste rühm A_3 järgmiselt

$$I(y) = y, \qquad (2,3,1)(y) = d^2 y, \qquad (3,1,2)(y) = dy$$

Seega element $y^3 = y(dy)(d^2y)$ on rühma A_3 püsipunkt. Analoognselt on elemendi $z = c_2 + dc_1 + d^2 c_3$ kuup $z^3 \in \operatorname{Inv} A_3$. Elemendid $z^3 + y^3, z^3 y^3$ on rühma S_3 püsipunktideks, kuna $z = (1,2)(y)$. Seetõttu vahetab paaritu substitutsioon π ära y ja z, sest $\pi(y) = \pi(1,2)(z)$ ja $\pi(z) = \pi(1,2)(y)$ ning $\pi(1,2) \in A_3$. Seega avalduvad

$$\begin{aligned} y^3 + z^3 =& 2s_1^3 - 9s_1 s_2 + 27 s_3 + (3s_1 s_2 - 9s_3)(1 + d + d^2) = 2s_1^3 - 9s_1 s_2 + 27 s_3 \\ y^3 z^3 =& s_1^6 - 9s_1^4 s_2 + 27 s_1^2 s_2^2 - 27 s_2^3 + (3s_1^4 s_2 - 9 s_1^2 s_2^2 + 9 s_2^3)(1 + d + d^2) = \\ & s_1^6 - 9s_1^4 s_2 + 27 s_1^2 s_2^2 - 27 s_2^3 \end{aligned}$$

Tekib ruutvõrrand y^3 ja y^3 suhtes, mis on radikaalides lahenduv eelneva teoreemi põhjal. Teisalt saab esialgsest võrrandisüsteemis y ja z kohta avaldada $X_1 = \frac{1}{3}(s_1 + y + d^2 z)$ ning seega oleme avaldanud X_1 polünoomi kordajate kaudu.

Teoreem 2.9.8. *Üldise neljanda astme polünoomi f juured avalduvad radikaalides, kui korpuse K karakteristika* $\operatorname{kar} K \neq 2$ *ja* $\operatorname{kar} K \neq 3$.

TÕESTUS. Olgu üldise neljanda astme polünoomi lahutuskorpuse automorfismi rühmas on lahenduv normaaljagajate jada $I \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4$ $G \cong S_2$. Kus neilkrühma moodustavad substitsoonid $V = \langle (2,1)(4,3), (1,4)(2,3) \rangle$. Paneme tähele, et suvalise automorfismi $\alpha \in S_n$ korral, elemendid

$$\begin{aligned} y_1 &= (X_1 + X_2)(X_3 + X_4) \\ y_2 &= (X_1 + X_3)(X_2 + X_4) \\ y_3 &= (X_1 + X_4)(X_2 + X_3) \end{aligned}$$

teisenevad teineteiseks, sest sulgudes on kõik neljaelemedilise hulga tükeldused $2+2$ elemendiks. Vaatkeme üldist kolmanda astme polünoomi $f = (Y - y_1)(Y - y_2)(Y - y_3)$ üle korpuse K. Et f on sümmetriline y_i suhtes ja $\alpha(y_i) = y_j$, siis $\alpha(f) = f$ ja seega polünoomi $f = X^3 - t_1 X^2 + t_2 X^2 - t_3$ kordajad $t_1, t_2, t_3 \in \operatorname{Inv} S_4$ ja avalduvad seega seega sümmetriliste põhipolünoomide $(s_i)_{i=1}^4$ kaudu. Kuna korpuse karakteristika $\operatorname{kar} K \neq 3$, siis leidub üldine lahendusvalem radikaalides ja y_1, y_2, y_3 saab avaldada üldkujul $(s_i)_{i=1}^4$ kaudu. Nüüd saab leida ruutvõrrandi üldlahendi valemi abil süsteemide

$$\begin{aligned} s_1 &= (X_1 + X_2) + (X_3 + X_4) & \qquad s_1 &= (X_1 + X_3) + (X_2 + X_4) \\ y_1 &= (X_1 + X_2)(X_3 + X_4) & \qquad y_2 &= (X_1 + X_3)(X_2 + X_4) \end{aligned}$$

$$s_1 = (X_1 + X_4) + (X_2 + X_3)$$
$$y_3 = (X_1 + X_4)(X_2 + X_3)$$

lahendid $A_{ij} = X_i + X_j$ ja seejärel avaldada $X_1 = \frac{1}{2}(A_{12} + A_{13} + A_{14} - s_1)$.

2.10 Polünoomid üle ratsionaalarvude korpuse

Lause 2.10.1. *Olgu p algarv ning $f \in \mathbb{Q}[X]$ taandumatu p-nda astme polünoom, mis omab täpselt ühe paari komplekseid juuri. Olgu F polünoomi f lahutuskorpus üle $\mathbb{Q}$, siis selle laiendi automorfismi rühm $G = \mathrm{Gal}(F : G) \cong S_p$.*

Tõestus. Et $F : \mathbb{Q}$ on lahutuskorpus, siis Galois' teoreemist saame $|G| = [F : \mathbb{Q}]$. Olgu $c \in F$ polünoomi f juur ja seega $[\mathbb{Q}(c) : Q] = p$ ja seega $p \mid |G|$. Kuna suvaline automorfism $\alpha \in G$ peab teisendama polünoomi f juuri omavahel, siis on ilmne $G \hookrightarrow S_p$. Zilovi teoreemi tõttu leidub rühmas G alamrühm järguga p. Kuna rühm, mis sisaldab algarvu elemete on tsükliline, siis peab G sisaldama tsüklit pikkusega p. Üldsus kitsendamata võib eeldada, et $\sigma = (2, 3 \ldots, p, 1) \in G$. Kuna polünoom, sisaldab täpselt ühe paari komplekseid juuri, siis isomorfism $\alpha(a + bi) = a - bi$ indutseerib vaid kahe elemendi trasposítsiooni. Üldsust kitsendamata võib eeldada, et see on $\tau = (1, i) \in G$. Nüüd on võimalik saada suvalist transpositsiooni $(1, ki) = \tau(\sigma^i\tau)^{k-1}$. Kuna $p \in \mathbb{P}$, siis saab teha transpositsioone $(1, k)$, kus k on suvaline, ja seega $\langle \sigma, \tau \rangle = S_n$.

Lemma 2.10.2. *Taandumatu kuuppolünoomi $f \in \mathbb{Q}[X]$ lahutuskorpuse F automorfismirühm $G = \mathrm{Gal}(F : \mathbb{Q}) \cong A_3$ parajasti siis, kui suurused $a = X_1^2X_2 + X_2^2X_3 + X_3^2X_1$ ja $b = X_2^2X_1 + X_3^2X_2 + X_1^2X_3$ on ratsionaalarvud, kusjuures $(X_i)_{i=1}^3$ on polünoomi juured.*

Tõestus. On ilmne, et $a, b \in \mathrm{Inv}\, A_3$ ja $a + b \in \mathrm{Inv}\, S_3$. Seega alati $a + b \in \mathbb{Q}$, mistõttu on a ja b samaegselt ratsionaalarvud. Tarvilikkus. Kui $G = A_3$, siis laiendi $F : \mathbb{Q}$ normaalsusest saame $\mathrm{Inv}\, A_3 = \mathbb{Q}$. Piisavus. Olgu vastuväiteliselt $a, b \in \mathbb{Q}$ ja $G \cong S_3$ nüüd $(1, 2)(a) = b$, millest $a = b$. Nüüd saame avaldada

$$0 = a - b = (X_2 - X_3)(X_1 - X_3)(X_1 - X_2),$$

millest polünoomi kaks juurt peab kokku langema. Tulemuseks on avastuolu, sest sellise polünoomi automorfismi rühm $G \hookrightarrow S_2$.

Teoreem 2.10.3. *Taandumatu kuuppolünoomi $f = X^3 - s_1X^2 + s_2X - s_3 \in \mathbb{Q}[X]$ lahutuskorpuse F automorfismirühm $\mathrm{Gal}(F : \mathbb{Q}) \cong A_3$ parajasti siis, kui suurus*

$$\Delta = s_1^2s_2^2 + 18s_1s_2s_3 - 27s_3^2 - 4s_1^3s_3 - 4s_2^2$$

on täisruut.

Tõestus. Ilmneb, et eelmisest lemmast olevad suurused a ja b saab avaldada sümmetriliste põhipolünoomide kaudu

$$a + b = s_1s_2 - 3s_3 \qquad ab = s_1^3s_3 + s_2^3 - 6s_1s_2s_3 + 9S3^2$$

Tulemuseks on ruutvõrrand, mille diskriminant on Δ. Kui Δ pole täisruut, siis $a \neq \mathbb{Q}$.

2.11 Korrapäraste hulknurkade konstrueerimine

Lemma 2.11.1. *Korrapärane n-nurk on sirkli ja joonlauaga konstrueeritav parajasti siis, kui nurk $\frac{2\pi}{n}$ on konstrueeritav.*

Lemma 2.11.2. *Olgu $n = n_1 \cdots n_k$, kus n_k on paarikaupa ühisteguriteta naturaalarvud. Korrapärane n-nurk on konstrueeritav parajasti siis, kui on konstrueeritavad korrapärased n_i-nurgad.*

Tõestus. Tarvilikkus on ilmne. Piisavus tuleb laiendatud Eukelidese algoritmist $\gcd(\frac{n}{n_i})_{i=1}^n = 1$ ja seega leidub $u_i \in \mathbb{Z}$ nii, et

$$\sum_{i=1}^{n} \frac{u_i n}{n_i} = 1 \qquad \Rightarrow \qquad \sum_{i=1}^{n} \frac{2\pi u_i}{n_i} = \frac{2\pi}{n}.$$

Lemma 2.11.3. *Kõik 2^n nurgad on konstrueeritavad.*

Tõestus. Nurga poolitamine.

Lemma 2.11.4. *Korrapärane n-nurk on sirkli ja joonlauaga konstrueeritav parajasti siis, kui nurga koosinus $a = \cos\frac{2\pi}{n} \in \mathbb{Q}(c_1, \ldots, c_n)$, kus $c_i^2 \in \mathbb{Q}(c_1, \ldots, c_{i-1})$.*

Tõestus. Nurk $\frac{2\pi}{n}$ on konstrueeritav parajasti siis, kui lõik pikkusega $\cos\frac{2\pi}{n}$ on konstrueritav. Järelduse 1.6.3.3 tõttu on väide ilmne.

Järeldus 2.11.4.1. *Korrapärane n-nurk on sirkli ja joonlauaga konstrueeritav parajasti siis, kui polünoomi primitiivne n-astme ühejuur on konstruueritav.*

Tõestus. Nurga koosinuse konstrueerimine on samaväärne nurga siinuse konstrueerimisega, järelikult on n-nurga konstrueerimine samaväärne $\xi = \cos\frac{2\pi}{n} + \sin\frac{2\pi}{n}i$ konstrueerimisega. Kuna ξ on primitiivne n-astme ühejuur, siis on väide tõestatud.

Lemma 2.11.5. *Primitiivse n-astme ühejuure ξ poolt moodustatud laiend $\mathbb{Q}(\xi) : \mathbb{Q}$ on sirkli ja joonlauaga konstrueeritav parajasti siis, kui $[\mathbb{Q}(\xi) : \mathbb{Q}] = 2^t$.*

Tõestus. Tarvilikkus tuleneb lemmast 2.11.4. Piisavuseks paneme tähele automorfismi rühm $G = \mathrm{Gal}(\mathbb{Q}(\xi) : \mathbb{Q})$ on lemma 2.6.2 tõttu Abeli rühm. Seetõttu peab $G \cong \mathbb{Z}_{2_1^n} \dot{+} \mathbb{Z}_{2_2^n} \dot{+} \cdots \dot{+} \mathbb{Z}_{2_k^n}$. Kuna iga $\mathbb{Z}_{2^i}$ korral leidub normaaljagajate $(H_i)_{i=0}^n$ jada $(2^i) \trianglelefteq (2^{i-1}) \trianglelefteq \cdots \trianglelefteq (2) \trianglelefteq (1) = \mathbb{Z}_{2^i}$ nii, et $H_k/H_{k-1} = (2^{i-k})/(2^{i-k+1}) = \{0, 1\}$. Galois' teoreemist saame, et leidub korpuste laiendite jada $(K_i)_{i=1}^n$ nii, et $[K_i : K_{i-1}] = 2$ ja $G_n = \mathbb{Q}(\xi)$. Seega iga vahepealne laiend on saadav eelnevast taandumatu ruutpolünoomi lahutuskorpusena. Ilmneb, et iga sellise ruutpolünoomi juur on konstruueritav sirkli ja joonlaua konstruktsiooniga ning teoreem on tõestatud.

Lemma 2.11.6. *Primitiivse p-astme ühejuure ξ poolt moodustatud laiendi mõõde $[\mathbb{Q}(\xi):\mathbb{Q}]=2^t$ ja $p\in\mathbb{P}$, siis $p=2^{2^s}+1$.*

TÕESTUS. Primitiivse ühejuure ξ minimaalne polünoom $m_\xi \mid f=1+X+X^2+\cdots+X^{p-1}$ üle $\mathbb{Q}$, sest $\xi\neq 1$. Olgu polünoom $g(Y)=f(1+Y)=\frac{(1+Y)^p-1}{Y}$, siis polünoomi f taandumatus on samaväärne g taandumatusega üle $\mathbb{Q}$, kuna f ja g on saadud pöötatava lineaarteisenduse abil. Et $g\equiv Y^{p-1} \mod p$ ja g vabaliige p, siis Eisestaini kriteeriumi kohaselt on g taandumatu. Järelikult $[\mathbb{Q}(\xi):\mathbb{Q}]=p-1$ ja seega $p=2^t+1$. Kui $t=uv$, kus u paaritu, siis $2^t+1=(1+2^v)(1-2^v+2^{2v}-\cdots+2^{v(u-1)})$, seega $p=2^{2^s}+1$.

Lemma 2.11.7. *Primitiivse p^2-astme ühejuure ξ poolt moodustatud laiendi mõõde $[\mathbb{Q}(\xi):\mathbb{Q}]\neq 2^t$, kui $p\in\mathbb{P}$ ja $p\neq 2$.*

TÕESTUS. Primitiivse ühejuure ξ minimaalne polünoom $m_\xi \mid f=1+X^p+X^{2p}+\cdots+X^{p(p-1)}$ üle $\mathbb{Q}$, sest $\xi^p\neq 1$. Olgu polünoom $g(Y)=f(1+Y)=\frac{(1+Y)^{p^2}-1}{(1+Y)^p-1}$, siis polünoomi f taandumatus on samaväärne g taandumatusega üle $\mathbb{Q}$, kuna f ja g on saadud pöötatava lineaarteisenduse abil. Et $g\equiv Y^{p(p-1)} \mod p$ ja g vabaliige p, siis Eisestaini kriteeriumi kohaselt on g taandumatu. Järelikult $[\mathbb{Q}(\xi):\mathbb{Q}]=p(p-1)$ ja seega $p(p-1)\neq 2^t$.

Gaussi teoreem. *Korrapärane n-nurk on konstrueeritav parajasti siis, kui $n=2^k p_1,p_2\cdots p_l$, kus p_i on paarikaupa erinevad algarvud, millel on kuju $p_i=2^{2^s_i}+1$ ja $s_i\in\mathbb{N}$.*

TÕESTUS. Lemmast 2.11.6 teame, et korrapärane p_i nurk on konstrueeritav. Lemma 2.11.7 tõttu pole võimalik konstrueerida p^k-nurka, kus $k>1$. Vastasel korral oleks p^2 konstrueeritav. Kuna korrapärane 2^k nurk on alati konstrueeritav, siis lemma 2.11.2 tõttu on teoreem tõestatud.

2.12 Arvude π ja e transtsententsus

Lindemanni teoreem (1882)**.** *Arv π on transtsendentne üle $\mathbb{Q}$.*

Hermite teoreem (1873)**.** *Arv e on transtsendentne üle $\mathbb{Q}$*