Algebraliste võrrandite lahenduvus radikaalides
Magistritöö

Raido Paas
Juhendaja: Mart Abel

Tartu 2013

Sisukord

Sissejuhatus

Käesolev magistritöö on mõeldud kasutamiseks õppematerjalina üliõpilastele. Loomulikult, materjali ei ole keelatud lugeda ka teistel huvilistel. Antud töös uurime algebraliste võrrandite lahendamise võimalikkust radikaalides. See küsimus köitis matemaatikute tähelepanu sajandeid kui mitte aastatuhandeid. Nagu on praeguseks teada, mitte kõiki võrrandeid ei ole võimalik lahendada radikaalides. See sai lõplikult selgeks 19. sajandil ning seda küllaltki "uudsel" moel selles mõttes, et tõestamisel kasutati tolleks ajaks veel vähe teada olnud matemaatilist aparatuuri, millist aparatuuri kutsutakse tänapäeval rühmateooriaks ning mille areng hoogustuski just tänu võrrandite radikaalides lahenduvuse küsimuse lahendamisele. Vaadeldavale probleemile ammendava vastuse andis seejuures noor keskkoolist tulnud prantsuse kodanik – Évariste Galois, kelle sellekohane töö avastati maailma jaoks alles mõned aastad peale tema surma.

Lugedes selle probleemi lahendamisega seotud ajaloolist tausta ning Galois' elukäiku, tekkis töö autoril huvi vaadeldava probleemi ja eriti selle lahenduse vastu. See on ka põhjus, miks käesolev õppematerjal sai kirjutatud. Nagu varem juba öeldud, arenes selle probleemi lahendamise ideest välja praeguseks küllaltki oluline algebra haru – rühmateooria. Ühtlasi hakkas tekkima ka kaasaegne abstraktne matemaatika. Seepärast peab autor seda teemat omale väga hästi sobivaks.

Töö on jaotatud kolme suuremasse peatükki – rühmateooria elemente, korpuseteooria elemente, Galois' teooria. Peaeesmärgiks on anda kompleksarvuliste kordajatega algebralise võrrandi radikaalides lahenduvuse kriteerium ning näidata seda kriteeriumi kasutades, et leidub viienda astme võrrand, mis ei ole lahenduv radikaalides. Õppematerjali on sisse arvatud ka mõned harjutusülesanded koos vastustega, et lugeja võiks materjali paremini omandada. Töö alguses on toodud ka võrrandite lahendamise ajaloolist külge tutvustav sissejuhatav peatükk.

Esimene ja teine peatükk on "eeltöö" viimase kolmanda peatüki mõistmiseks. St, viimases peatükis on meil vaja teada mõningaid tulemusi rühmade ja korpuste kohta. Kuna kõiki vajaminevaid teadmisi mainitud algebraliste struktuuride kohta ei ole võimalik leida kasutusel olevatest eestikeelsetest al-

gebra õpikutest ning meie käsitlus on ka veidi erinev, siis oli mõistlik need kaks peatükki siia õppematerjali sisse arvata.

Viimases ning ühtlasi ka kõige pikemas peatükis arendame välja teooria võrrandite radikaalides lahenduvuse probleemi lahendamiseks. Selles peatükis anname kompleksarvuliste kordajatega algebralise võrrandi radikaalides lahenduvuse kriteeriumi ning näitame seda kriteeriumi kasutades, et viienda astme võrrand $x^5 - 6x + 3 = 0$ ei ole lahenduv radikaalides. Peatükki alustame teooria sissejuhatava osaga, kus tutvume Joseph Louis Lagrange'i ideega võrrandite lahendamiseks ning seejärel Galois' "edasiarendustega" Lagrange'i ideest. See annab meile hea ettevalmistuse teooria mõistmiseks.

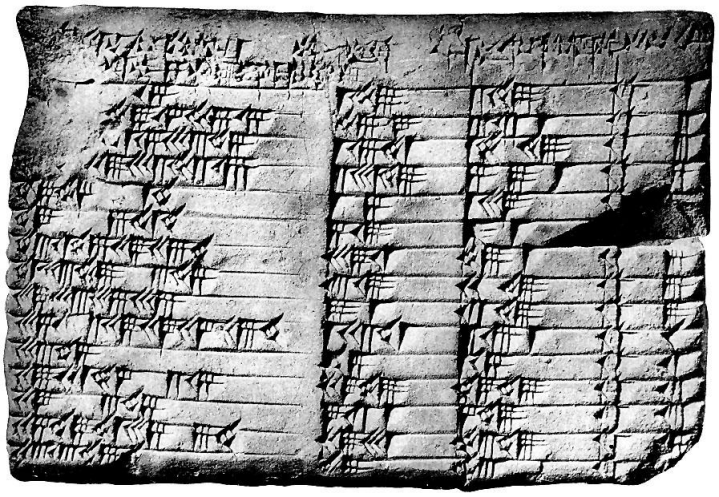
Peaaegu kogu töö ulatuses (välja arvatud punkt 3.1.1, kus vaatame võrrandeid abstraktsemalt) piirdume kompleksarvuliste kordajatega võrrandite vaatlemisega. See tähendab ühtlasi ka seda, et me töös enamasti ei maini, et K on korpuse $\mathbb{C}$ alamkorpus või, et R on ringi $\mathbb{C}$ alamring. Kirjutame lihtsalt, et K on korpus ning R on ring ja mõistame selle all, et K on korpuse $\mathbb{C}$ alamkorpus ning, et R on ringi $\mathbb{C}$ alamring.

Töö kirjutamisel on peamiselt tuginenud Coventry linnas (asub Suurbritannias Inglismaal) asuva Warwicki ülikooli professori Ian Stewarti õpikule [7]. Töös ei ole sellele õpikule eraldi viidanud (välja arvatud mõnes kohas, kus see tundus vajalikuna). Olgu siiski mainitud, et enamikud mainitud õpikus toodud tõestused on suurema selguse huvides käesolevas kraaditöös "lahti" kirjutatud ning mõnda tõestust on ka muudetud. Mainitud õpikust pärineb seejuures ka ajalooga seotud informatsioon ning enamik harjutusülesandeid (mõned harjutusülesanded pärinevad õpikust [1]). Professor Ian Stewart andis seejuures isikliku nõusoleku oma õpiku kasutamiseks antud töö kirjutamisel. Kasulikku abimaterjali on töö autor leidnud ka professor Kangro õpikust [1]. Mainitud õpikule tuginevad lausete 1.1.7, 2.1.5, 2.1.10 ning teoreemi 3.3.13 piisavuse osa tõestused. Ka viimatimainitud õpikule ei ole töös eraldi viidatud. Alapunkti 3.1.2 materjali koos tõestustega on töö autor aga ise tuletanud.

Ajalooline sissejuhatus

Erinevalt matemaatikast, mida võib enamikel juhtudel täiesti usaldada ning veel enam, ise veenduda teoreemide ja valemite korrektsuses, ei saa ajaloo üleskirjutust alati usaldada. See tähendab, tegelikke minevikus toimunud sündmusi võib olla varjatud ning kirja on pandud sündmusi moonutav tekst või hoopis midagi, mida ei ole toimunud. Ajaloolise tausta kaasamine käesolevasse töösse on siiski asjakohane, sest see aitab näha tekkinud probleeme algebraliste võrrandite lahendamise kohta. Nagu juba mainitud, ei saa siiski kõiges kirjapandus kindel olla, kuid kõik ei tohiks päris vale ka olla.

Algebraliste võrranditega (edaspidi kasutame algebralise võrrandi asemel lihtsalt sõna võrrand) tegeldi juba XVII sajandil e.Kr Babüloonias, kus mõned preestrid või matemaatikud töötasid välja, kuidas lahendada ruutvõrrandit. Nemad, või mõned nende õpilased, graveerisid selle savitahvlitele. Mõned sellised savitahvlid (lisaks savitahvlitele, milledel on näiteks maksukogumise andmed ja planeet Jupiteri liikumised üles tähendatud) on säilinud tänapäevani (vt Joonis 1).



Joonis 1: Babüloonia savitahvel Pythagorase arvudega.

On leitud Babüloonia savitahvel aastast umbes 1600 e.Kr, mis sisaldab

aritmeetilisi probleeme, mis taanduvad ruutvõrrandi lahendamisele. Tabel annab tunnistust, et babüloonlased omasid üldisi meetodeid ruutvõrrandite lahendamiseks, kuigi neil ei olnud mingit algebralist tähistusviisi, millega väljendada oma lahendusskeemi. Babüloonlased kasutasid arvude kuuekümnendsüsteemi nii, et näiteks sümbolid $7, 4, 0; 3, 11$ tähistasid arvu

$$7 \cdot 60^2 + 4 \cdot 60 + 0 \cdot 60 + 3 \cdot 60^{-1} + 11 \cdot 60^{-2} = 25440\frac{191}{3600} .$$

1930. aastal teatas teadusajaloolane Otto Neugebauer, et mõned kõige antiiksemad Babüloonia probleemtahvlid sisaldasid meetodeid ruutvõrrandi lahendamiseks (õigemini ühe reaalarvulise lahendi leidmiseks). Üks tabel sisaldas näiteks sellist probleemi: leida ruudu külg kui on teada, et ruudu pindala ja ühe külje vahe on $14, 30$. Arvestades, et arvule $14, 30$ vastab kümnendsüsteemis arv 870, võime selle probleemi formuleerida kui ruutvõrrandi

$$x^2 - x = 870$$

ühe positiivse lahendi leidmisena. Babüloonlaste lahendus oli järgmine:

> Võta 1-st pool, mis on $0; 30$, ning korruta arv $0; 30$ arvuga $0; 30$. Tulemuseks saad $0; 15$. Liida sellele $14, 30$, saad $14, 30; 15$. See on arvu $29; 30$ ruut. Nüüd liida $0; 30$ arvule $29; 30$. Saad 30, mis on ruudu külg.

Kuigi tegemist on ühe konkreetse näitega, on see esitatud nii, et võime selle üldistada üldisele juhule, mis oligi ilmselt Babüloonia "kirjatundja" eesmärk. Tänapäevast kirjapilti kasutades avaldub otsitav ruudu külje pikkus x kujul $x = \sqrt{a + 0.25} + 0.5$, mille asendamisel võrrandisse $x^2 - x = a$ saamegi samasuse. See valem on sarnane tänapäeval kasutatava ruutvõrrandi lahendamise valemiga ühe lahendi leidmiseks.

Antiikkreeklased seevastu lahendasid ruutvõrrandeid geomeetrilisi konstruktsioone kasutades. Kreeklastel olid samuti meetodid kuupvõrrandite lahendamiseks, mis sisaldasid koonuste lõikepunktide leidmist. Siiski, algebralisi lahendusmeetodeid kreeklastelt kuupvõrrandi jaoks ei ole teada.

Renessansiaja matemaatikud Bolognas Itaalias avastasid, et kuupvõrrandi saab taandada kolmele põhitüübile: $x^3 + px = q$, $x^3 = px + q$ ja $x^3 + q = px$, kus p ja q on positiivsed reaalarvud. Nad eristasid neid kolme põhitüüpi, sest nad ei tunnistanud negatiivseid arve. On arvatud (allikas [7], lk xix), et Scipio del Ferro lahendas ära kõik kolm tüüpi. Uudised sellest läksid liikvele ning teised proovisid samuti kuupvõrrandit ära lahendada. Kuupvõrrandi lahendusvalemid avastas uuesti Niccolo Fontana (hüüdnimega Tartaglia, "Kokutaja") 1535. aastal. 1545. aastal ilmus Girolamo Cardano teos "Ars Magna", kus on toodud põhjalik käsitlus Fontana

kuupvõrrandi lahendamise ideest. Teos sisaldas ka meetodit – tänu Cardano õpilasele Ludovico Ferrarile – 4. astme võrrandi lahendamiseks selle taandamisel kuupvõrrandile. Kõik leitud valemid sisaldasid üht huvipakkuvat tähelepanekut, mida võib illustreerida Fontana lahendivalemiga kuupvõrrandi $x^3 + px = q$ jaoks:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}\ .$$

Selline esitus, nimetatud "Cardano valemiks", esitub kordajate p ja q korduva liitmise, lahutamise, korrutamise, jagamise ning juurimise kaudu. Selline esitusviis sai tuntuks kui "lahendus radikaalides".

Kuna kõik võrrandid, mille aste on väiksem kui 5, said nüüd lahendatud, tekkis loomulik küsimus, kuidas lahendada 5. astme võrrandit radikaalides. Tuntud matemaatikul Leonhard Euleril ei õnnestunud lahendada 5. astme võrrandit, kuid ta leidis uued meetodid 4. astme võrrandi jaoks, millised leidis ka Etienne Bézout 1765. aastal. Joseph-Louis Lagrange astus suure sammu edasi oma aastail 1770-1771 esitatud töös "Réflexions sur la résolution algébrique des équations", kus ta ühendas kõik erinevad seni kasutatud meetodid võrrandite, mille aste on väiksem kui 5, lahendamiseks. Ta näitas, et nad kõik sõltuvad polünoomide leidmisest võrrandi lahenditest, mis jäävad muutumatuks teatavate võrrandi lahendite permuteerimisel. Lagrange näitas, et selline lähenemine ebaõnnestub kui vaadelda 5. astme võrrandit. See ei tõestanud veel, et 5. astme võrrand ei ole lahenduv radikaalides, sest teistsugused meetodid võivad õnnestuda. Kuid sellise üldise meetodi ebaõnnestumine oli huvipakkuv.

Üldine arvamus, et 5. astme võrrand ei ole lahenduv radikaalides, oli nüüd õhus. Paolo Ruffini esitas 18. sajandi lõpul ja 19. sajandi algul töid (mis olid seejuures küllaltki mahukad), milledes tal lõpuks õnnestus näidata, et üldine 5. astme võrrand (vt definitsioon 3.1.1 leheküljel 54) ei ole lahenduv radikaalides. Tõestus ei olnud siiski piisavalt täielik, st, sisaldas üht puudust. Selle puuduse suutis 1824. aastal kõrvaldada Niels Henrik Abel. Abeli töö oli pikk ja sisaldas väikest viga, mis küll ei tühistanud ta tõestust.

Üldine 5. astme võrrand oli seega radikaalides mittelahenduv, kuid mõned konkreetsed 5. astme võrrandid võisid siiski olla lahenduvad. Abelil õnnestus leida mitmesuguseid meetodeid teatud kujul olevate 5. astme võrrandite lahendamiseks – iga võrrandi kuju jaoks erinev lahendivalem. Uus küsimus oli nüüd seega õhus: otsustada, kas mõni konkreetne 5. astme võrrand on radikaalides lahenduv. Abel töötas selle küsimuse kallal just enne seda kui ta suri tuberkuloosi 1829. aastal.

1832. aastal tapeti noor (20 aastane) prantsuse matemaatik Évariste Galois duellil. Ta oli tegelenud võrrandite radikaalides lahenduvuse küsimusega,

olles seejuures esitanud 3 tööd Pariisi Teaduste Akadeemiale oma sellekohaste uurimuste kohta. Need tööd tema eluajal teatud põhjustel küll tunnustust ei leidnud ning Galois' uurimused tundusid olevat maailmale kadunud. Siiski, 4. juulil 1843, pöördus Joseph Liouville Akadeemia poole. Ta alustas järgnevate sõnadega:

> *"Ma loodan pöörata Akadeemia tähelepanu tõsiasjale, et Évariste Galois' tööde seas olen ma leidnud lahenduse, nii täpse kui olla saab, sellisele ilusale probleemile: kas leidub või mitte lahendus radikaalides..."*

Peatükk 1

Rühmateooria elemente

Algebraliste võrrandite radikaalides lahendamise uurimisel on meile abiks rühmateooria "vahendid". Rühmateooria, kui üks algebra valdkond, saigi tegelikult alguse seoses algebraliste võrrandite lahendamise küsimuse uurimisega. Seepärast on meil enne kõrgema astme võrrandite radikaalides lahenduvuse küsimuse uurimist vajalik teada mõningaid tulemusi rühmateooria valdkonnast.

Eeldame järgnevas, et lugeja on tuttav põhiliste rühmade kohta käivate mõistete ja tulemustega nagu näiteks rühm, alamrühm, rühma järk, rühma elemendi järk, faktorrühm, isomorfism, homomorfism, normaaljagaja ehk normaalne alamrühm, Lagrange'i teoreem ja rühmade homomorfismiteoreem. Samuti eeldame arvuteooria põhiliste tulemuste tundmist. Loetletud mõistetega võib tutvuda näiteks nii õpikute [2], [4], [5] kui ka loengukonspekti [6] abil.

1.1 Substitutsioonide rühmad

Meenutame, et substitutsiooniks n-elemendilisel ($n \in \mathbb{N}$) hulgal nimetatakse mistahes bijektiivset kujutust sellel hulgal (vt [5], lk 122, definitsioon 4.3.9). Tähistades vaadeldava hulga elemente vastavalt arvudega 1, 2, ..., n, võime substitutsiooni s esitada kujul

$$s = \begin{pmatrix} 1 & 2 & \dots & n \\ s_1 & s_2 & \dots & s_n \end{pmatrix}, \tag{1.1}$$

kus

$$s_1 \;\; s_2 \;\; \dots \;\; s_n$$

on arvude 1, 2, ..., n teatav ümberjärjestus ehk permutatsioon. Sellise tähistusviisi korral loeme, et näiteks element, mis on tähistatud arvuga 1, teiseneb

substitutsiooni s toimel elemendiks, mis on tähistatud arvuga s_1. Kõigi substitutsioonide hulka n elemendist (n-elemendilisel hulgal) tähistame järgnevalt sümboliga $\mathbb{S}_n$.

Märgime, et substitutsiooni 1.1 võime esitada ka teisiti, st selliselt, kus tema esimese rea elemendid 1, 2, ..., n on esitatud mingis teises järjekorras. Tingimuseks aga jääb siiski, et arvule 1 vastab alumises reas samal kohal arv s_1, arvule 2 vastab alumises reas samal kohal arv s_2 jne.

Näide 1.1.1. Substitutsioonide hulk $\mathbb{S}_3$ koosneb järgnevatest elementidest:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \quad \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \quad \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$
$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \quad \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \quad \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

Seejuures, vastavalt eelöeldule,

$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&3&2\\3&2&1\end{pmatrix} = \begin{pmatrix}2&1&3\\1&3&2\end{pmatrix} =$$
$$= \begin{pmatrix}2&3&1\\1&2&3\end{pmatrix} = \begin{pmatrix}3&1&2\\2&3&1\end{pmatrix} = \begin{pmatrix}3&2&1\\2&1&3\end{pmatrix}.$$

Definitsioon 1.1.2. *Substitutsioonide* $r, s \in \mathbb{S}_n$, kus

$$r = \begin{pmatrix}s_1&s_2&\dots&s_n\\r_{s_1}&r_{s_2}&\dots&r_{s_n}\end{pmatrix}, \qquad s = \begin{pmatrix}1&2&\dots&n\\s_1&s_2&\dots&s_n\end{pmatrix}, \tag{1.2}$$

korrutiseks nimetame substitutsiooni

$$rs = \begin{pmatrix}1&2&\dots&n\\r_{s_1}&r_{s_2}&\dots&r_{s_n}\end{pmatrix}. \tag{1.3}$$

Lause 1.1.3. *Substitutsioonide hulk* $\mathbb{S}_n$ *osutub substitutsioonide korrutamise suhtes rühmaks.*

Tõestus. Definitsiooni 1.1.2 põhjal on kahe substitutsiooni $r, s \in \mathbb{S}_n$, millised on antud kujul (1.2), korrutis (1.3) tõepoolest substitutsioon, sest kuna $r \in \mathbb{S}_n$, siis on arvud r_{s_1}, r_{s_2}, ..., r_{s_n} paarikaupa erinevad arvud hulgast $\{1, 2, ..., n\}$.

Olgu nüüd $r, s, t \in \mathbb{S}_n$ suvalised substitutsioonid kujul

$$r = \begin{pmatrix}s_{t_1}&s_{t_2}&\dots&s_{t_n}\\r_{s_{t_1}}&r_{s_{t_2}}&\dots&r_{s_{t_n}}\end{pmatrix}, \qquad s = \begin{pmatrix}t_1&t_2&\dots&t_n\\s_{t_1}&s_{t_2}&\dots&s_{t_n}\end{pmatrix},$$
$$t = \begin{pmatrix}1&2&\dots&n\\t_1&t_2&\dots&t_n\end{pmatrix}.$$

Siis, ühelt poolt,

$$(rs)t = \left[\begin{pmatrix} s_{t_1} & s_{t_2} & \dots & s_{t_n} \\ r_{s_{t_1}} & r_{s_{t_2}} & \dots & r_{s_{t_n}} \end{pmatrix} \begin{pmatrix} t_1 & t_2 & \dots & t_n \\ s_{t_1} & s_{t_2} & \dots & s_{t_n} \end{pmatrix}\right] \begin{pmatrix} 1 & 2 & \dots & n \\ t_1 & t_2 & \dots & t_n \end{pmatrix} =$$
$$= \begin{pmatrix} t_1 & t_2 & \dots & t_n \\ r_{s_{t_1}} & r_{s_{t_2}} & \dots & r_{s_{t_n}} \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ t_1 & t_2 & \dots & t_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ r_{s_{t_1}} & r_{s_{t_2}} & \dots & r_{s_{t_n}} \end{pmatrix}.$$

Teiselt poolt aga

$$r(st) = \begin{pmatrix} s_{t_1} & s_{t_2} & \dots & s_{t_n} \\ r_{s_{t_1}} & r_{s_{t_2}} & \dots & r_{s_{t_n}} \end{pmatrix} \left[\begin{pmatrix} t_1 & t_2 & \dots & t_n \\ s_{t_1} & s_{t_2} & \dots & s_{t_n} \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ t_1 & t_2 & \dots & t_n \end{pmatrix}\right] =$$
$$= \begin{pmatrix} s_{t_1} & s_{t_2} & \dots & s_{t_n} \\ r_{s_{t_1}} & r_{s_{t_2}} & \dots & r_{s_{t_n}} \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ s_{t_1} & s_{t_2} & \dots & s_{t_n} \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ r_{s_{t_1}} & r_{s_{t_2}} & \dots & r_{s_{t_n}} \end{pmatrix}.$$

Seega $(rs)t = r(st)$, mistõttu substitutsioonide korrutamine on assotsiatiivne.

Ühikelemendiks substitutsioonide korrutamise suhtes on substitutsioon (ühiksubstitutsioon)

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

ning substitutsiooni

$$s = \begin{pmatrix} 1 & 2 & \dots & n \\ s_1 & s_2 & \dots & s_n \end{pmatrix}$$

pöördsubstitutsioon on

$$s^{-1} = \begin{pmatrix} s_1 & s_2 & \dots & s_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Seega on tõepoolest tegemist rühmaga. □

Definitsioon 1.1.4. Rühma $\mathbb{S}_n$, mis on moodustatud kõigi n-elemendiliste substitutsioonide poolt ($n \in \mathbb{N}$), nimetame *substitutsioonide rühmaks* (n *elemendist*).

Osutub, et iga lõplik rühm on isomorfne teatava substitutsioonide rühma alamrühmaga (vt [5], lk 175, teoreem 6.4.1). Seepärast on meil oluline tunda just substitutsioonide rühmi.

Definitsioon 1.1.5. Substitutsiooni nimetame *tsükliks*, kui ta paigutab teatud elemente tsükliliselt ümber, ülejäänud elemendid jätab aga paigale. Tsüklit, mis viib elemendi s_1 elemendiks s_2, elemendi s_2 elemendiks s_3, ..., elemendi s_k elemendiks s_1, tähistame

$$(s_1 s_2 \dots s_k),$$

ning nimetame seda seejuures *k-tsükliks*.

Paneme tähele, et tsükkel on kuni järjekorra täpsuseni üheselt määratud.

Näide 1.1.6. Substitutsioon

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

on tsükkel, mille võime esitada ka samaväärsel kujul

$$(124)\,.$$

Lause 1.1.7. *Mistahes substitutsiooni rühmast $\mathbb{S}_n$ saab esitada sõltumatute tsüklite korrutisena, st, selliste tsüklite korrutisena, mille üleskirjutises ei ole ühiseid elemente. Seejuures sellises korrutises ei ole sõltumatute tsüklite järjekord oluline.*

Tõestus. Olgu

$$s = \begin{pmatrix} 1 & 2 & \dots & n \\ s_1 & s_2 & \dots & s_n \end{pmatrix} \tag{1.4}$$

suvaline substitutsioon rühmast $\mathbb{S}_n$. Tõestuseks tuleb näidata, et substitutsiooni s saab esitada tsüklite korrutisena nii, et iga arv 1, 2, ..., n esineb parajasti ühes tsüklis.

Paneme tähele, et arv 1 teiseneb substitutsiooni s toimel arvuks s_1, arv s_1 omakorda arvuks s_{s_1} jne kuni mingil sammul jõuame arvuni, mis teiseneb s toimel arvuks 1 (sest n on lõplik arv ning substitutsiooni 1.4 alumine rida koosneb paarikaupa erinevatest arvudest hulgast $\{1, 2, ..., n\}$). Sel teel saame tsükli

$$\begin{pmatrix} 1 & s_1 & s_{s_1} & \dots \\ s_1 & s_{s_1} & \dots & 1 \end{pmatrix} = (1 s_1 s_{s_1} \dots)\,. \tag{1.5}$$

Otsime nüüd substitutsiooni s ülemises reas sellist arvu a, mis ei esine eraldatud tsüklis (1.5). Kui sellist arvu ei leidu, siis on väide tõestatud. Kui selline arv a aga leidub, siis ta teiseneb s toimel arvuks s_a, arv s_a omakorda arvuks s_{s_a} jne kuni mingil sammul jõuame arvuni, mis teiseneb s toimel arvuks a. Sel teel saame tsükli

$$\begin{pmatrix} a & s_a & s_{s_a} & \dots \\ s_a & s_{s_a} & \dots & a \end{pmatrix} = (a s_a s_{s_a} \dots)\,. \tag{1.6}$$

Kui oletada, et arvude a, s_a, s_{s_a}, ... ja arvude 1, s_1, s_{s_1}, ... seas leidub võrdseid, siis olgu $i, j \in \{1, 2, ..., n\}$ sellised indeksid, et $s_i = s_j$, kus s_i kuulub tsüklisse (1.5) ja s_j kuulub tsüklisse (1.6). Siit järelduks nüüd, et $s_{s_i} = s_{s_j}$, kus s_{s_i} kuulub tsüklisse (1.5) ja s_{s_j} kuulub tsüklisse (1.6) ning nii edasi liikudes saaksime, et a võrdub mingi arvuga tsüklist (1.5), mis on vastuolus a valikuga.

Kirjeldatud tsüklite eraldamise protsessi jätkame seni, kuni ei leidu enam arvu $b \in \{1, 2, ..., n\}$, mis ei kuuluks ühessegi meie poolt eraldatud tsüklisse.

Nüüd paneme aga tähele, et

$$s = \dots (a s_a s_{s_a} \dots)(1 s_1 s_{s_1} \dots) ,$$

seejuures antud korrutises ei ole tsüklite korrutamise järjekord oluline, sest iga arv 1, 2, ..., n esineb parajasti ühes tsüklis. □

Näide 1.1.8. Esitame substititsiooni

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 8 & 9 & 2 & 4 & 7 & 3 & 6 \end{pmatrix}$$

sõltumatute tsüklite korrutisena.

Paneme tähele, et substitutsiooni s toimel arv 1 teiseneb arvuks 5, arv 5 teiseneb arvuks 2, arv 2 teiseneb arvuks 1, millega sulgub esimene tsükkel (152). Teise tsükli koostamist alustame arvuga 3. Nüüd 3 teiseneb arvuks 8, arv 8 arvuks 3, millega sulgub teine tsükkel (38). Kolmandat tsüklit alustame arvuga 4. Arv 4 teiseneb arvuks 9, arv 9 arvuks 6 ja arv 6 teiseneb arvuks 4, millega sulgeb kolmas tsükkel (496). Järelejäänud arv 7 moodustab omaette tsükli, mille me võime kirjutamata jätta. Seega

$$s = (496)(38)(152) .$$

Lause 1.1.9. *Iga k-tsükli $(s_1 s_2 \dots s_k) \in \mathbb{S}_n$ järk substitutsioonide rühmas $\mathbb{S}_n$ on k.*

Tõestus. Kui $k = 1$ või kui $k = 2$, siis on väide selge. Eeldame seega järgnevas, et $k > 2$. Olgu s_i, $i \in \{1, 2, ..., k\}$, mingi element k-tsüklis $t = (s_1 s_2 \dots s_k)$.

Paneme tähele, et substitutsioon t^j, kus $j < k$ ning $j > 0$, viib elemendi s_i elemendiks $s_{\overline{i+j}}$, kus

$$\overline{i+j} = \begin{cases} \text{arvu } i+j \text{ jääk jagamisel arvuga } k & \text{kui } i+j > k , \\ i+j & \text{muul juhul.} \end{cases}$$

Veendume, et sellisel juhul t^j ei ole ühiksubstitutsioon. Selleks piisab näidata, et $s_{\overline{i+j}} \neq s_i$, st, et $\overline{i+j} \neq i$. Vaatame kahte juhtu, sõltuvalt sellest, kas $i + j > k$ või $i + j \leq k$.

Juhul, kui $i + j > k$, siis tingimuse $j < k$ tõttu $\overline{i+j} \neq i$, sest vastasel juhul peaks $i + j = k + i$ (arvestame, et $i \leq k$ ja $j < k$ tõttu $i + j < 2k$) ehk $j = k$, mis oleks vastuolus arvu j valikuga.

Kui $i + j \leq k$, siis $\overline{i+j} = i + j$ ning tingimuse $j > 0$ tõttu $i + j \neq i$. St $\overline{i+j} \neq i$.

Seevastu substitutsioon t^k viib elemendi s_i selleks samaks elemendiks s_i ning on seetõttu ühiksubstitutsioon.

Sellega oleme näidanud, et k-tsükli t järk rühmas $\mathbb{S}_n$ on k. □

Järeldus 1.1.10. *Olgu p algarv. Siis ainsad elemendid rühmas $\mathbb{S}_p$ järguga p on p-tsüklid.*

Tõestus. Lause 1.1.9 põhjal on iga p-tsükli järk rühmas $\mathbb{S}_p$ arv p. Olgu $s \in \mathbb{S}_p$ substitutsioon, mis ei ole p-tsükkel ega ühiksubstitutsioon. Lause 1.1.7 põhjal võime ta esitada sõltumatute tsüklite korrutisena

$$s = t_r t_{r-1} \dots t_1 \, .$$

Seejuures paneme tähele, et igas tsüklis t_i, $i \in \{1, 2, ..., r\}$, on elemente vähem kui p (sest vastasel juhul oleks s ju p-tsükkel). Teisisõnu, t_i on k_i-tsükkel, kus $k_i < p$ ($i \in \{1, 2, ..., r\}$). Lause 1.1.9 põhjal on iga k_i-tsükli t_i järk k_i, $i \in \{1, 2, ..., r\}$. Oletame, et $s^p = e$, kus e on ühiksubstitutsioon. Kuna s ei ole ühiksubstitutsioon, siis leidub k_i-tsükkel s_i, mille järk ei ole 1 ($i \in \{1, 2, ..., r\}$). Meie oletuse $s^p = e$ tõttu ning kuna sõltumatute tsüklite t_1, t_2, ..., t_r omavaheline korrutamine on kommutatiivne, siis ka $t_i^p = e$ (arvestame, et ka tsüklid t_j^p, $j \in \{1, 2, ..., r\}$, on sõltumatud). See aga tähendab, et $k_i \mid p$ (vt [6], lk 28, lemma 7.3), mis on vastuoluline, sest p on algarv ning $1 < k_i < p$. Seega substitutsiooni s järk ei saa olla p. □

Definitsioon 1.1.11. Substitutsiooni $s \in \mathbb{S}_n$ nimetame *transpositsiooniks*, kui ta esitub sõltumatute tsüklite korrutisena kujul

$$s = (ij) \, ,$$

kus $i, j \in \{1, 2, ..., n\}$, $i \neq j$.

Definitsioon 1.1.12. Olgu permutatsioonis

$$s_1 \;\; s_2 \;\; \dots \;\; s_j \;\; \dots \;\; s_i \;\; \dots \;\; s_n$$

arv s_j suurem arvust s_i. Sellisel juhul ütleme, et arvud s_i ja s_j moodustavad vaadeldavas permutatsioonis *inversiooni*.

Kui inversioonide koguarv permutatsioonis on paarisarv, siis nimetame permutatsiooni *paarispermutatsiooniks*. Vastasel juhul nimetame permutatsiooni *paarituks permutatsiooniks*.

Definitsioon 1.1.13. Substitutsiooni $s \in \mathbb{S}_n$, mis on antud kujul

$$s = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ s_{a_1} & s_{a_2} & \dots & s_{a_n} \end{pmatrix} ,$$

nimetame *paarissubstitutsiooniks*, kui permutatsioonid

$$a_1 \;\; a_2 \;\; \ldots \;\; a_n \qquad \text{ja} \qquad s_{a_1} \;\; s_{a_2} \;\; \ldots \;\; s_{a_n}$$

on ühesuguse paarsusega. Vastasel juhul nimetame substitutsiooni s *paarituks substitutsiooniks*.

Märgime, et toodud definitsioon on korrektne, sest ühe ja sama substitutsiooni erinevad esitused on teineteisest saadavad veergude teatava arvu ümberpaigutamiste abil. Kahe veeru ümberpaigutamine tähendab aga transpositsiooni teostamist substitutsiooni esituse mõlemas permutatsioonis. Transpositsioon aga muudab permutatsiooni paarsust (vt [5], lk 121, lause 4.3.7).

Esitame nüüd veel mõned tulemused substitutsioonide rühmade kohta, milledest enamikud toome tõestuseta (tõestused võib leida näiteks õpikust [5], lehekülgedelt 123 - 125).

Lause 1.1.14. *Substitutsoonide rühma $\mathbb{S}_n$ järk on $n!$.*

Lause 1.1.15. *Kui $n \geq 2$, siis rühmas $\mathbb{S}_n$ on paaris ja paarituid substitutsioone ühepalju.*

Lause 1.1.16. *Iga transpositsioon on paaritu substitutsioon.*

Teoreem 1.1.17. *Rühma $\mathbb{S}_n$ $(n \geq 2)$ iga substitutsioon on esitatav transpositsioonide korrutisena.*

Lause 1.1.18. *Tegurite arv substitutsiooni esituses transpositsioonide korrutisena on sama paarsusega kui substitutsioon ise.*

Lause 1.1.19. *Rühma $\mathbb{S}_n$ alamhulk, mis koosneb kõigist paarissubstitutsioonidest, on rühma $\mathbb{S}_n$ alamrühm.*

Tõestus. Olgu s ja t kaks paarissubstitutsiooni. Lause 1.1.18 põhjal on s ja t esituses transpositsioonide korrutisena transpositsioone paarisarv. Siis aga ka korrutis st sisaldab paarisarvu transpositsioone ning on seetõttu paarissubstitutsioon. Veendume nüüd, et suvalise paarissubstitutsiooni s pöördsubstitutsioon s^{-1} on paarissubstitutsioon. Oletame, et s^{-1} on paaritu substitutsioon. Olgu s ja s^{-1} esitatud transpositsioonide korrutisena. Siis s esituses on transpositsioone paarisarv ja s^{-1} esituses paaritu arv. Korrutis ss^{-1} sisaldab seega paaritu arv transpositsioone ning seepärast peaks ühiksubstitutsioon e olema paaritu substitutsioon. See oleks vastuoluline, mistõttu s^{-1} peab olema paarissubstitutsioon. □

Definitsioon 1.1.20. Rühma $\mathbb{S}_n$ alamrühma, mis koosneb kõigist paarissubstitutsioonidest, nimetame *n-astme alterneeruvaks rühmaks* ning tähistame $\mathbb{A}_n$.

Lause 1.1.21. *Rühma $\mathbb{A}_n$ järk on $\frac{n!}{2}$.*

Tõestus. Järeldub vahetult lausetest 1.1.14 ja 1.1.15. □

1.2 Lahenduvad ja lihtsad rühmad

Selles punktis teeme kõigepealt tutvust lahenduvate rühmadega ning tõestame mõned üldtulemused nende rühmade kohta. Lahenduvad rühmad mängivad olulist rolli võrrandite radikaalides lahenduvuse teoorias. Tutvume ka lihtsate rühmadega. Näitame, et alterneeruv rühm $\mathbb{A}_n$ on juhul $n \geq 5$ lihtne ning seda tulemust kasutades näitame, et substitutsioonide rühm $\mathbb{S}_n$ ei ole juhul $n \geq 5$ lahenduv. Just viimasele faktile tugineme hiljem, kui näitame, et kõik 5. astme võrrandid ei ole lahenduvad radikaalides.

Kui G on rühm ning H on tema normaalne alamrühm ehk normaaljagaja, siis tähistame seda järgnevalt $H \trianglelefteq G$. Rühma G ühikelementi tähistame sümboliga 1_G või ka lihtsalt sümboliga 1, kui kontekstist on selge, millise rühma ühikelementi me silmas peame.

Definitsioon 1.2.1. Rühma G lõplikku alamrühmade jada

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n = G\,,$$

milles sisalduvused on ranged ning $G_i \trianglelefteq G_{i+1}$ iga $i \in \{0, 1, ..., n-1\}$ korral, nimetame rühma G *normaaljadaks*. Kui G on üheelemendiline, siis sellisel juhul ka üheelemendilist jada $\{1\} = G$ nimetame rühma G *normaaljadaks*.

On lihtsasti mõistetav, et igas rühmas G leidub normaaljada - näiteks jada $\{1\} \subseteq G$. Rühmas G võib leiduda ka mitu normaaljada. Abeli rühma iga alamrühmade jada on ju normaaljada.

Definitsioon 1.2.2. Ütleme, et *rühma G normaaljada on saadud teise normaaljada tihendamisel*, kui esimene normaaljada on tekkinud nii, et teise normaaljadasse kuuluvate alamrühmade vahele on paigutatud täiendavaid alamrühmi.

Definitsioon 1.2.3. Rühma G normaaljada nimetame *kompositsioonijadaks*, kui teda ei ole võimalik nii tihendada, et tulemuseks on uus normaaljada.

Definitsioon 1.2.4. Olgu $\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$ rühma G normaaljada. Faktorrühmi

$$G_{i+1}/G_i\,,$$

$i \in \{1, 2, ..., n-1\}$, nimetame selle *normaaljada faktoriteks*.

Definitsioon 1.2.5. Rühma G nimetame *lahenduvaks*, kui temas leidub normaaljada, mille faktorid on Abeli rühmad. Teisisõnu, rühm G on *lahenduv*, kui leidub lõplik arv selliseid alamrühmi

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n = G\,, \tag{1.7}$$

et kehtib

1. $G_i \trianglelefteq G_{i+1}$ iga $i \in \{0, 1, ..., n-1\}$ korral.

2. Faktorrühm G_{i+1}/G_i on Abeli rühm iga $i \in \{0, 1, ..., n-1\}$ korral.

Näide 1.2.6.

1. Iga Abeli rühm G on lahenduv, sest jada $\{1\} \subseteq G$ rahuldab definitsiooni 1.2.5 tingimusi.

2. Substitutsioonide rühm $\mathbb{S}_3$ on lahenduv. Temas leidub alamrühmade jada
$$\{e\} \subset \langle (123) \rangle \subset \mathbb{S}_3 \,,$$
kus e on ühiksubstitutsioon ning $\langle (123) \rangle$ on rühma $\mathbb{S}_3$ tsükliline alamrühm moodustajaga (123). Võib veenduda, et $\langle (123) \rangle \trianglelefteq \mathbb{S}_3$ ning, et rühma $\langle (123) \rangle$ järk on 3. Kuna rühma $\mathbb{S}_3$ järk on lause 1.1.14 põhjal $3! = 6$, siis faktorrühma $\mathbb{S}_3/\langle (123) \rangle$ järk on $6 : 3 = 2$ ning $\mathbb{S}_3/\langle (123) \rangle$ on seega Abeli rühm.

3. Substitutsioonide rühm $\mathbb{S}_4$ on samuti lahenduv. Temas leidub alamrühmade jada
$$\{e\} \subset \mathbb{V} \subset \mathbb{A}_4 \subset \mathbb{S}_4 \,,$$
kus e on ühiksubstitutsioon, $\mathbb{V} = \{e, (34)(12), (24)(13), (23)(14)\}$ (tuntud kui "Kleini neljarühm"). Võib veenduda, et $\{e\} \trianglelefteq \mathbb{V}$, $\mathbb{V} \trianglelefteq \mathbb{A}_4$ ning $\mathbb{A}_4 \trianglelefteq \mathbb{S}_4$. Lausete 1.1.14 ja 1.1.21 põhjal ning sellest, et rühmas $\mathbb{V}$ on 4 elementi, järeldub, et faktorrühmade $\mathbb{S}_4/\mathbb{A}_4$ ja $\mathbb{A}_4/\mathbb{V}$ järgud on vastavalt 2 ja 3. Seega kehtivad[1]
$$\begin{aligned} \mathbb{V}/\{e\} &\cong \mathbb{V} \,, \\ \mathbb{A}_4/\mathbb{V} &\cong \mathbb{Z}_3 \,, \\ \mathbb{S}_4/\mathbb{A}_4 &\cong \mathbb{Z}_2 \,. \end{aligned}$$
Rühmad $\mathbb{V}$, $\mathbb{Z}_3$, $\mathbb{Z}_2$ on aga Abeli rühmad.

Tõestame siinkohal ühe elementaarse lause.

Lause 1.2.7. *Olgu G lahenduv rühm ning olgu rühm H isomorfne rühmaga G. Siis H on lahenduv rühm.*

Tõestus. Olgu
$$\{1_G\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

[1] Vt näiteks [5], lk 168, definitsioon 6.1.24, kus on defineeritud jäägiklassirühm $\mathbb{Z}_n$ ($n \in \mathbb{N}$).

rühma G normaaljada, mille faktorid on Abeli rühmad ($n \in \mathbb{N}$). Olgu $\phi : G \to H$ isomorfism. Siis on kujutised $H_i = \phi(G_i)$, $i \in \{0, 1, ..., n\}$ rühma H alamrühmad (vt [5], lk 74, lause 2.5.29) ning meil on rühma H alamrühmade jada

$$\{1_H\} = H_0 \subset H_1 \subset \ldots \subset H_n = H\,.$$

Olgu $i \in \{0, 1, ..., n-1\}$ suvaline.

Veendume, et $H_i \trianglelefteq H_{i+1}$. Selleks olgu $h_i \in H_i$ ja $h_{i+1} \in H_{i+1}$ suvalised ning näitame, et $h_{i+1}^{-1} h_i h_{i+1} \in H_i$. Olgu $g_i \in G_i$ ja $g_{i+1} \in G_{i+1}$ sellised, et $\phi(g_i) = h_i$ ja $\phi(g_{i+1}) = h_{i+1}$. Siis

$$h_{i+1}^{-1} h_i h_{i+1} = (\phi(g_{i+1}))^{-1} \phi(g_i)\phi(g_{i+1}) = \phi(g_{i+1}^{-1})\phi(g_i)\phi(g_{i+1}) = \\ = \phi(g_{i+1}^{-1} g_i g_{i+1}) \in \phi(G_i) = H_i\,,$$

sest $g_{i+1}^{-1} g_i g_{i+1} \in G_i$.

Veendume nüüd, et H_{i+1}/H_i on Abeli rühm. Selleks piisab näidata, et suvaliste $h_1, h_2 \in H_{i+1}$ korral $h_1 h_2 H_i = h_2 h_1 H_i$ (see on faktorrühma elementide korrutamise eeskiri, vt [5], lk 166, lause 6.1.11). Olgu $g_1, g_2 \in G_{i+1}$ sellised, et $\phi(g_1) = h_1$ ning $\phi(g_2) = h_2$. Siis

$$h_1 h_2 H_i = \phi(g_1)\phi(g_2)\phi(G_i) = \phi(g_1 g_2 G_i) = \\ = \phi(g_2 g_1 G_i) = \phi(g_2)\phi(g_1)\phi(G_i) = h_2 h_1 H_i\,,$$

sest G_{i+1}/G_i on eelduse põhjal Abeli rühm. □

Järgnevad tulemused (teoreemid 1.2.8 kuni 1.2.12) koos tõestustega on leitavad eestikeelsest õpikust [4] lehekülgedelt 13-14 ning 21-22.

Teoreem 1.2.8 (Esimene isomorfismiteoreem)**.** *Olgu G, H ja K rühmad. Kui $K \trianglelefteq G$ ning $H \subseteq G$, siis $H \cap K \trianglelefteq H$, $K \trianglelefteq HK$ ning kehtib*

$$HK/K \cong H/(H \cap K)\,.$$

Teoreem 1.2.9 (Teine isomorfismiteoreem)**.** *Olgu G, H ja K rühmad. Kui $K \trianglelefteq G$, $K \subseteq H$ ning $H \trianglelefteq G$, siis $K \trianglelefteq H$, $H/K \trianglelefteq G/K$ ning kehtib*

$$(G/K)/(H/K) \cong G/H\,.$$

Teoreem 1.2.10 (Kolmas isomorfismiteoreem)**.** *Olgu G rühm, H tema normaaljagaja, $\pi : G \to G/H$ loomulik projektsioon, $N \trianglelefteq G/H$ ning $M = \pi^{-1}(N)$. Siis $H \trianglelefteq M \trianglelefteq G$ ning kehtib*

$$G/M \cong (G/H)/N\,.$$

Teoreem 1.2.11. *Kui G on lahenduv rühm ning H on tema alamrühm, siis on ka H lahenduv rühm.*

Teoreem 1.2.12. *Kui G on lahenduv rühm ning $N \trianglelefteq G$, siis on ka G/N lahenduv rühm.*

Teoreem 1.2.13. *Olgu G rühm ning olgu $N \trianglelefteq G$. Kui rühmad N ja G/N on lahenduvad, siis on ka rühm G lahenduv.*

Tõestus. Veendume kõigepealt, et kui H on rühma G/N alamrühm, siis hulk

$$G_H = \{g \in G \,\big|\, gN \in H\}$$

on rühma G alamrühm. Olgu $g_1, g_2 \in G_H$ suvalised. Siis $g_1N, g_2N \in H$ ning, kuna H on rühm, siis $g_1g_2N = g_1Ng_2N \in H$. Seega ka $g_1g_2 \in G_H$. Olgu nüüd $g \in G_H$ suvaline. Siis $gN \in H$, mistõttu $g^{-1}N = (gN)^{-1} \in H$. Seega $g^{-1} \in G_H$. Sellega oleme näidanud, et G_H on rühma G alamrühm. Paneme veel tähele, et $N \subseteq G_H$ ning, kuna $N \trianglelefteq G$, siis ka $N \trianglelefteq G_H$ ning seejuures $H = G_H/N$.

Nüüd eelduse põhjal leiduvad jadad[2]

$$\{1_G\} = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_r = N\,,$$
$$\{1_{G/N}\} = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_s = G/N\,,$$

kus faktorrühmad N_{i+1}/N_i, H_{j+1}/H_j ($i \in \{0, 1, ..., r-1\}$, $j \in \{0, 1, ..., s-1\}$) on Abeli rühmad. Eelöeldu tõttu $H_j = G_j/N$, kus G_j on teatav rühma G alamrühm, $j \in \{0, 1, ..., s\}$. Seejuures, kuna H_0 on üheelemendiline, siis $H_0 = N/N$.

Veendume nüüd, et $G_j \trianglelefteq G_{j+1}$, $j \in \{0, 1, ..., s-1\}$. Olgu $g \in G_j$ ja $x \in G_{j+1}$ suvalised. Kuna kehtib võrdus

$$(xN)^{-1}(gN)(xN) = (x^{-1}N)(gN)(xN) = x^{-1}gxN$$

ning kuna $G_j/N \trianglelefteq G_{j+1}/N$, siis $x^{-1}gxN \in G_j/N$. See tähendab, et $x^{-1}gx \in G_j$ ning ühtlasi ka, et $G_j \trianglelefteq G_{j+1}$.

Nüüd saame moodustada jada

$$\{1_G\} = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_r = N = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_s = G\,. \qquad (1.8)$$

Paneme tähele, et faktorrühm N_{i+1}/N_i on eelduse põhjal Abeli rühm iga $i \in \{0, 1, ..., r-1\}$ korral. Faktorrühm G_{j+1}/G_j on aga iga $j \in \{0, 1, ..., s-1\}$ korral teoreemi 1.2.9 põhjal isomorfne Abeli rühmaga

$$(G_{j+1}/N)/(G_j/N)\,,$$

[2]Rühma G ühikelement 1_G on ühtlasi ka alamrühma N ühikelemendiks, mistõttu tähistame ka rühma N ühikelementi sümboliga 1_G.

mistõttu on ka ise Abeli rühm. "Korrastades" nüüd jada (1.8) nii, et sisalduvused oleksid ranged, saame kommutatiivsete faktoritega rühma G normaaljada. □

Definitsioon 1.2.14. Rühma G nimetame *lihtsaks* kui tema ainsad normaalsed alamrühmad on $\{1\}$ ja G. Viimaseid normaalseid alamrühmi me nimetame seejuures rühma G *triviaalseteks normaaljagajateks.*

Näide 1.2.15. Kui p on algarv, siis jäägiklassirühm $\mathbb{Z}_p$ on lihtne, sest Lagrange'i teoreemist (vt [5], lk 164, teoreem 6.1.5) ning sellest, et p on algarv, järeldub, et selle rühma ainsad alamrühmad (ning seega ka ainsad normaalsed alamrühmad) on $\{\overline{0}\}$ ja ta ise.

Olgu G lahenduv rühm normaaljadaga

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n = G\,, \tag{1.9}$$

mille faktorid on Abeli rühmad. Olgu M selline rühma G alamrühm, et $M \neq G_i$ ning $M \neq G_{i+1}$, kuid $G_i \trianglelefteq M \trianglelefteq G_{i+1}$. Teise isomorfismiteoreemi 1.2.9 põhjal kehtib siis

$$(G_{i+1}/G_i)/(M/G_i) \cong G_{i+1}/M\,. \tag{1.10}$$

Kuna G_{i+1}/G_i on Abeli rühm, siis on ka tema faktorrühm $(G_{i+1}/G_i)/(M/G_i)$ Abeli rühm ning seega isomorfismi (1.10) tõttu on ka G_{i+1}/M Abeli rühm. Samuti, sisalduvuse $M \subset G_{i+1}$ tõttu, on ka rühm M/G_i Abeli rühm. Seega, tihendades lahenduva rühma G normaaljada (1.9), siis saadavad faktorid on ikka Abeli rühmad. See lubab meil lahenduva rühma G korral rääkida tema kompositsioonijadast, mille faktorid on Abeli rühmad. Kehtib järgmine lause.

Lause 1.2.16. *Lahenduva rühma G kompositsioonijada faktorid on lihtsad tsüklilised rühmad ning nende järk on algarv.*

Tõestus. Olgu

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n = G \tag{1.11}$$

lahenduva rühma G kompositsioonijada, mille faktorid on Abeli rühmad. Oletame vastuväiteliselt, et mingi indeksi $i \in \{0, 1, ..., n-1\}$ korral faktorrühmal G_{i+1}/G_i leidub mittetriviaalne normaaljagaja N. Olgu $\pi : G_{i+1} \to G_{i+1}/G_i$ loomulik projektsioon. Teoreemi 1.2.10 põhjal on $M = \pi^{-1}(N)$ rühma G_{i+1} normaalne alamrühm ning

$$G_{i+1}/M \cong (G_{i+1}/G_i)/N\,. \tag{1.12}$$

Paneme tähele, et kuna $G_i \subseteq M \subseteq G_{i+1}$ ning $G_i \trianglelefteq G_{i+1}$, siis $G_i \trianglelefteq M$.

Kui nüüd M võrduks rühmaga G_{i+1}, siis (1.12) vasakul pool oleks ühikrühm, mistõttu peaks ka (1.12) paremal pool olema ühikrühm. Kuna aga $N \neq G_{i+1}/G_i$, siis (1.12) parem pool ei ole ühikrühm. Kui aga M võrduks rühmaga G_i, siis (1.12) tõttu peaks N võrduma faktorrühma G_{i+1}/G_i ühikrühmaga $\{G_i\}$. Jällegi vastuolu eeldusega. Seega peab M olema erinev rühmadest G_{i+1} ja G_i. See on aga vastuoluline, sest sellisel juhul saaksime normaaljada (1.11) tihendada alamrühmaga M, mistõttu ei oleks jada (1.11) rühma G kompositsioonijada. Seega peavad kompositsioonijada (1.11) faktorid olema lihtsad rühmad.

Olgu $i \in \{0, 1, ..., n-1\}$ suvaline ning veendume, et faktorrühm G_{i+1}/G_i on algarvulist järku tsükliline rühm. Olgu $\overline{a} \in G_{i+1}/G_i$ mingi element, mis ei võrdu selle rühma ühikelemendiga $\overline{e} = \{G_i\}$. Vaatame rühma G_{i+1}/G_i alamrühma

$$\langle \overline{a} \rangle = \left\{ \overline{e}, \overline{a}, \overline{a}^2, \ldots, \overline{a}^{m-1} \right\} .$$

Kuna G_{i+1}/G_i on kompositsioonijada (1.11) faktor, siis on ta Abeli rühm. Abeli rühma iga alamrühm on aga selle rühma normaaljagaja, mistõttu on rühm $\langle \overline{a} \rangle$ lihtsa rühma G_{i+1}/G_i normaaljagaja. Seega, kas $\langle \overline{a} \rangle = G_{i+1}/G_i$, või $\langle \overline{a} \rangle = \{\overline{e}\}$. Kuna meie valiku tõttu $\overline{a} \neq \overline{e}$, siis peab $\langle \overline{a} \rangle = G_{i+1}/G_i$, mis tähendab ühtlasi, et rühm G_{i+1}/G_i on tsükliline ning järku m. Oletame, et m ei ole algarv, st, $m = pq$, kus $1 < p < m$. Sellisel juhul on

$$\langle \overline{a}^q \rangle = \left\{ \overline{e}, \overline{a}^q, \overline{a}^{2q}, \ldots, \overline{a}^{(p-1)q} \right\}$$

rühma G_{i+1}/G_i alamrühm, mille järk on p. See aga tähendab ühtlasi, et $\langle \overline{a}^q \rangle$ on rühma G_{i+1}/G_i mittetriviaalne normaaljagaja. See on vastuoluline, sest G_{i+1}/G_i on lihtne rühm. □

Teoreem 1.2.17. *Lahenduv rühm G on lihtne siis ja ainult siis kui G on tsükliline ning tema järk on algarv.*

Tõestus. Tarvilikkus. Olgu lahenduv rühm G lihtne. Kuna G on lahenduv, siis leidub normaaljada

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n = G\,, \tag{1.13}$$

mille faktorid on Abeli rühmad. Kuna G on lihtne, siis peab $G_{n-1} = \{1\}$. Paneme tähele, et sellisel juhul

$$G \cong G/\{1\} = G_n/G_{n-1}\,. \tag{1.14}$$

Faktorrühm G_n/G_{n-1} on aga Abeli rühm, mistõttu peab siis (1.14) tõttu ka G olema Abeli rühm. Paneme nüüd tähele, et kuna G on Abeli rühm, siis iga tema alamrühm on ühtlasi ka normaaljagaja. Seega, kuna G on lihtne, siis ei saa rühmas G leiduda mittetriviaalseid alamrühmi.

Olgu $1 \neq g \in G$ suvaline. Siis $\langle g \rangle \neq \{1\}$ ning seega peab $\langle g \rangle = G$ (sest vastasel juhul oleks $\langle g \rangle$ rühma G mittetriviaalne alamrühm). Sellega oleme näidanud, et G on tsükliline.

Veendume, et G järk on algarv. Oletame, et rühma $G = \langle g \rangle$ järk p ei ole algarv, st $p = kl$, kus $k > 1$, $l > 1$. Siis element $g^k \neq 1$ ei ole rühma G moodustaja (vt [5], lk 173, lause 6.3.8) ning seega $\langle g^k \rangle$ oleks rühma G mittetriviaalne alamrühm.

Piisavus. Kui rühma G järk on algarv, siis, kuna lõpliku rühma alamrühma järk on rühma järgu jagaja (vt [5], lk 164, teoreem 6.1.5), ei saa sel rühmal olla mittetriviaalseid alamrühmi ning seega ka mittetriviaalseid normaalseid alamrühmi. Seega peab G olema lihtne. □

Teoreem 1.2.18. *Kui $n \geq 5$, siis n-astme alterneeruv rühm $\mathbb{A}_n$ on lihtne.*

Tõestus. Olgu $N \trianglelefteq \mathbb{A}_n$, $N \neq \{e\}$.

Veendume kõigepealt, et kui N sisaldab mingit 3-tsüklit, siis $N = \mathbb{A}_n$. Üldisust kitsendamata võime eeldada, et $(123) \in N$ (sest me võime substitutsiooni arvud alati meile sobivalt ümber järjestada). Paneme tähele, et $(12k) = (1k)(12)$, kus $k > 3$. Lause 1.1.18 põhjal seega $(12k) \in \mathbb{A}_n$ $(k > 3)$. Kuna $N \trianglelefteq \mathbb{A}_n$, siis $k > 3$ korral

$$(12k)(123)(12k)^{-1} = (12k)(123)(k21) = (k32) \in N\,. \tag{1.15}$$

Nüüd aga $(123)(k32) = (k12) = (12k) \in N$ $(k > 3)$. Seega

$$(12k) \in N \;\; \forall k \in \{3, 4, \ldots, n\}\,. \tag{1.16}$$

Olgu $x \in \mathbb{A}_n$ suvaline ning olgu ta esitatud sõltumatute tsüklite korrutisena (vt lause 1.1.7)

$$x = \ldots \cdot c \cdot b \cdot a\,. \tag{1.17}$$

Paneme tähele, et k-tsükli a võime esitada kujul

$$a = (a_1 a_2 \ldots a_k) = (a_1 a_k) \ldots (a_1 a_3)(a_1 a_2)\,. \tag{1.18}$$

Lisaks märkame, et

$$(a_1 a_i) = (1a_1)(1a_i)(1a_1)\,, \;\; i \in \{2, 3, \ldots, k\}\,. \tag{1.19}$$

Võrdustest (1.18) ja (1.19) järeldame, et k-tsükli a võime esitada kujul $(1i)$, $i \in \{2, 3, ..., n\}$, olevate transpositsioonide korrutisena. Sarnaselt võime veenduda, et ka tsüklid $b, c, ...$ substitutsiooni x esitusest kujul (1.17) ning seega ka substitutsiooni x võime esitada kujul $(1i)$, $i \in \{2, 3, ..., n\}$, olevate transpositsioonide korrutisena. Kuna $x \in \mathbb{A}_n$ oli suvaline, siis iga substitutsiooni

rühmast $\mathbb{A}_n$ võime esitada kujul $(1i)$, $i \in \{2,3,...,n\}$, olevate transpositsioonide korrutisena, kusjuures neid transpositsioone peab lause 1.1.18 põhjal olema paarisarv. Seega

$$\mathbb{A}_n = \langle \{(1j)(1i) \,|\, i,j \in \{2,3,\ldots,n\}\} \rangle \,, \tag{1.20}$$

st, rühm $\mathbb{A}_n$ on moodustatud hulga poolt, mille elementideks on substitutsioonid $(1j)(1i)$, $i,j \in \{2,3,...,n\}$ (selle kohta ütleme ka, et rühm $\mathbb{A}_n$ on *tekitatud* kujul $(1j)(1i)$, $i,j \in \{2,3,...,n\}$, olevate substitutsioonide poolt).

Veendume nüüd, et iga substitutsiooni kujul $(1j)(1i)$ $(i,j \in \{2,3,...,n\})$ on võimalik esitada rühma N kuuluvate substitutsioonide kaudu. Siis võrdusest (1.20) järeldub, et $\mathbb{A}_n = N$. Juhul kui $i = j$, siis väide kehtib, sest $(1j)(1i) = I \in N$. Eeldame nüüd, et $i \neq j$. Paneme esiteks tähele, et sellisel juhul $(1j)(1i) = (1ij)$. Nüüd juhul, kui $i \neq 2$ ja $j \neq 2$, saame tingimust (1.16) arvestades, et

$$(1ij) = (12j)(12j)(12i)(12j) \in N \,.$$

Juhul, kui $i > 3$ ja $j = 2$, siis tingimuse (1.15) tõttu

$$(1ij) = (1i2) = (32i)(123)(i23) = (32i)(123)(32i)^{-1} \in N \,.$$

Kui $i = 3$ ja $j = 2$, siis tingimuse (1.16) tõttu

$$(1ij) = (132) = (123)^{-1} \in N \,.$$

Juhul, kui $i = 2$ ja $j > 2$, järeldub tingimusest (1.16), et

$$(1ij) = (12j) \in N \,.$$

Sellega oleme näidanud, et kui N sisaldab mingit 3-tsüklit, siis $N = \mathbb{A}_n$.

Näitame nüüd, et N sisaldab mingit 3-tsüklit. Olgu $x \in N$ mingi suvaline ühiksubstitutsioonist erinev substitutsioon. Olgu x esitatud sõltumatute tsüklite a, b, c, ... korrutisena

$$x = \ldots \cdot c \cdot b \cdot a \,. \tag{1.21}$$

Vaatleme nüüd kõikvõimalikke juhte, mis võivad esineda x esituses sõltumatute tsüklite korrutisena.

1. Substitutsioon x sisaldab tsüklit, milles on rohkem kui 3 elementi. Üldisust kitsendamata võime eeldada, et selliseks tsükliks on a, sest korrutises (1.21) ei ole korrutatavate järjekord oluline (vt lause 1.1.7). Seega $a = (a_1 a_2 \ldots a_k)$, kus $k \geq 4$. Olgu

$$t = (a_1 a_2 a_3) = (a_1 a_3)(a_1 a_2) \in \mathbb{A}_n \,.$$

Nüüd, kuna tsüklid b, c, ... on sõltumatud ning kuna $N \trianglelefteq \mathbb{A}_n$, siis kehtib

$$txt^{-1} = t(\ldots cba)t^{-1} = \ldots cb(tat^{-1}) = z \in N\,.$$

Nüüd aga

$$\begin{aligned} x^{-1}z &= (a^{-1}b^{-1}c^{-1}\ldots)(\ldots cb(tat^{-1})) = a^{-1}tat^{-1} = \\ &= (a_k \ldots a_2a_1)(a_1a_2a_3)(a_1a_2 \ldots a_k)(a_3a_2a_1) = (a_3a_ka_1) \in N\,. \end{aligned}$$

2. Substitutsiooni x esituses sõltumatute tsüklite korrutisena on vähemalt kaks 3-tsüklit, st
$$x = y(a_4a_5a_6)(a_1a_2a_3)\,,$$
kus y on substitutsioon, mis jätab elemendid a_1, a_2, ..., a_6 muutumatuks. Olgu
$$t = (a_2a_3a_4) = (a_2a_4)(a_2a_3) \in \mathbb{A}_n\,.$$
Nüüd
$$\begin{aligned} &x^{-1}(txt^{-1}) = \\ &\quad = (a_3a_2a_1)(a_6a_5a_4)y^{-1}(a_2a_3a_4)\,y\,(a_4a_5a_6)(a_1a_2a_3)(a_4a_3a_2) = \\ &\qquad\qquad = (a_4a_3a_6a_1a_2) \in N \end{aligned}$$
ning olukord taandub juhule 1.

3. Substitutsiooni x esituses sõltumatute tsüklite korrutisena on täpselt üks 3-tsükkel ning mitte ühtegi k-tsüklit, kus $k \geq 4$. Siis $x = p(a_1a_2a_3)$, kus substitutsioon p jätab elemendid a_1, a_2 ja a_3 muutumatuks ning $p^2 = I$ (p on sõltumatute transpositsioonide korrutis). Siis aga
$$x^2 = p(a_1a_2a_3)p(a_1a_2a_3) = p^2(a_1a_2a_3)^2 = (a_1a_3a_2) \in N\,.$$

4. Kui substitutsiooni x esituses sõltumatute tsüklite korrutisena ei kehti ükski tingimustest 1., 2., 3., siis esitub x sõltumatute transpositsioonide korrutisena. Seejuures, meie valiku tõttu $x \neq e$ ning $x \in N \subseteq \mathbb{A}_n$, mistõttu peab x esituses sõltumatute transpositsioonide korrutisena transpositsioone olema vähemalt 2. St,
$$x = p(a_3a_4)(a_1a_2)\,,$$
kus substitutsioon p jätab elemendid a_1, a_2, a_3 ja a_4 muutumatuks. Olgu
$$t = (a_2a_3a_4) \in \mathbb{A}_n\,.$$

Paneme tähele, et

$$u = x^{-1}(txt^{-1}) = (a_1a_2)(a_3a_4)p^{-1}(a_2a_3a_4)p(a_3a_4)(a_1a_2)(a_4a_3a_2) = \\ = (a_4a_1)(a_3a_2) \in N\,.$$

Olgu $a_5 \in \{1, 2, ..., n\}$ mingi element, mis erineb elementidest a_1, a_2, a_3 ja a_4. Olgu

$$v = (a_1a_2a_5) = (a_1a_5)(a_1a_2) \in \mathbb{A}_n\,.$$

Nüüd

$$u(vuv^{-1}) = (a_4a_1)(a_3a_2)(a_1a_2a_5)(a_4a_1)(a_3a_2)(a_5a_2a_1) = \\ = (a_5a_2a_1a_4a_3) \in N$$

ning olukord taandub juhule 1.

Sellega oleme näidanud, et rühma $\mathbb{A}_n$ ainsad normaalsed alamrühmad on triviaalsed normaaljagajad, mistõttu rühm $\mathbb{A}_n$ on lihtne. □

Järeldus 1.2.19. *Substitutsioonide rühm $\mathbb{S}_n$ ei ole juhul $n \geq 5$ lahenduv.*

Tõestus. Kui rühm $\mathbb{S}_n$, $n \geq 5$, oleks lahenduv, siis teoreemi 1.2.11 põhjal peaks ka alamrühm $\mathbb{A}_n$ olema lahenduv. Teoreemi 1.2.18 põhjal on rühm $\mathbb{A}_n$, juhul kui $n \geq 5$, lihtne. Teoreemi 1.2.17 põhjal peaks siis $\mathbb{A}_n$ järk olema algarv. Lause 1.1.21 põhjal on rühma $\mathbb{A}_n$ järk $\frac{n!}{2}$, mis aga ei ole algarv kui $n \geq 5$.

Saadud vastuolu tõttu ei saa rühm $\mathbb{S}_n$ olla lahenduv kui $n \geq 5$. □

1.3 Cauchy teoreem

Selle punkti eesmärgiks on Cauchy teoreemi tõestus, milline teoreem väidab, et kui algarv p jagab lõpliku rühma järku, siis selles rühmas leidub element, mille järk on p. Selles punktis vaatlemegi vaid lõplikke rühmi. Eelnevalt läheb meil vaja aga mõningaid abitulemusi. Tõestuseta toodud tulemuste tõestused võib leida õpikust [4] lehekülgedelt 7 ja 8.

Rühma G järku ehk elementide arvu kui ka hulga G võimsust tähistame edaspidises järgnevalt: $|G|$.

Lause 1.3.1. *Olgu G rühm. Seos $\sim$, mis suvaliste $a, b \in G$ korral on defineeritud*

$$a \sim b \Leftrightarrow \exists g \in G :\ a = g^{-1}bg\,,$$

on ekvivalentsiseos rühmal G.

Definitsioon 1.3.2. Olgu G rühm ning $a, b \in G$. Ütleme, et element b on elemendi a *kaaselement* (*rühmas* G) kui leidub $g \in G$ nii, et

$$a = g^{-1}bg\,.$$

Kui $b \in G$ on elemendi $a \in G$ kaaselement rühmas G, siis lause 1.3.1 tõttu on ka element a elemendi b kaaselement ning seepärast nimetame elemente a ja b ka *teineteise kaaselementideks*.

Lause 1.3.1 väidab, et seos "a ja b on kaaselemendid rühmas G", on ekvivalentsiseos rühmal G. Rühm G jaguneb selle seose järgi ekvivalentsiklassideks, milliseid ekvivalentsiklasse me nimetame rühma G *kaaselementide klassideks*.

Kui rühma G kaaselementide klassid on K_1, K_2, ..., K_r, siis üks neist, ütleme, et K_1, sisaldab ainult rühma G ühikelementi. Seega $|K_1| = 1$. Kuna rühma G kaaselementide klassid ei lõiku ning katavad rühma G, siis

$$|G| = 1 + |K_2| + \ldots + |K_r|\,. \tag{1.22}$$

Elementi $a \in G$ sisaldavat rühma G kaaselemendi klassi tähistame $K(a)$.

Definitsioon 1.3.3. Olgu G rühm ning $x \in G$ mingi element. Siis elemendi x *tsentralisaatoriks* (*rühmas* G) nimetame hulka

$$C_G(x) = \{g \in G \,|\, gx = xg\}\,.$$

Lause 1.3.4. *Elemendi $x \in G$ tsentralisaator $C_G(x)$ rühmas G on rühm ning*

$$|K(x)| = \frac{|G|}{|C_G(x)|}\,, \tag{1.23}$$

st, elementi x sisaldava rühma G kaaselementide klassi $K(x)$ võimsus võrdub rühma G kõrvalklasside arvuga alamrühma $C_G(x)$ järgi.

Järeldus 1.3.5. *Elementide arv rühma G mistahes kaaselementide klassis on rühma G järgu jagaja.*

Tõestus. Väide järeldub vahetult võrdusest (1.23). □

Lause 1.3.6. *Olgu G ja H rühmad ning $\phi : G \to H$ homomorfism. Olgu elemendi $g \in G$ järk k ning elemendi $\phi(g) \in H$ järk olgu l. Siis $l \mid k$.*

Tõestus. Paneme tähele, et

$$(\phi(g))^k = \phi(g^k) = \phi(1) = 1\,. \tag{1.24}$$

Kuna elemendi $\phi(g)$ järk on l, siis võrduse (1.24) tõttu $l \mid k$ (vt [6], lk 28, lemma 7.3). □

Lause 1.3.7. *Olgu G rühm, mille järk ei ole algarv. Siis rühmas G leidub mittetriviaalne pärisalamrühm.*

Tõestus. Olgu $|A| = mn$, kus $m > 1$ ja $n > 1$. Olgu $a \in A$ mingi selline element, et $a \neq 1_G$. Kui elemendi a järk ei ole mn, siis väide kehtib (mittetriviaalseks pärisalamrühmaks on sel juhul $\langle a \rangle$). Kui elemendi a järk on mn, siis $A = \langle a \rangle$ ning rühm $\langle a^m \rangle = \{1_G, a^m, a^{2m}, ..., a^{(n-1)m}\}$ on rühma A mittetriviaalne alamrühm. □

Lause 1.3.8. *Olgu A Abeli rühm, mille järk jagub algarvuga p. Siis rühmas A leidub element, mille järk on p.*

Tõestus. Väite tõestame matemaatilise induktsiooni meetodit kasutades rühma A järgu $|A|$ järgi.

Induktsiooni baas. Olgu rühma A järk algarv p. Olgu $a \in A$ mingi selline element, et $a \neq 1_G$. Kuna p on algarv ning $|\langle a \rangle| \neq 1$, siis Lagrange'i teoreemist (vt [5], lk 164, teoreem 6.1.5) järeldub, et alamrühma $\langle a \rangle$ järk on p. Teisisõnu, elemendi $a \in A$ järk on p.

Induktsiooni samm. Eeldame nüüd, et väide kehtib iga Abeli rühma korral, mille järk on väiksem kui pk, kus $k > 1$, ning mille järk jagub algarvuga p. Olgu A Abeli rühm, mille järk on pk. Lause 1.3.7 põhjal leidub rühmas A mittetriviaalne pärisalamrühm. Olgu M rühma A selline pärisalamrühm, mille järk m on maksimaalne rühma A pärisalamrühmade järkude seast. Kui m jagub arvuga p, siis induktsiooni eelduse tõttu meie väide kehtib. Eeldame nüüd, et m ei jagu arvuga p. Olgu $b \in A \setminus M$ suvaline ning olgu $B = \langle b \rangle$. Paneme tähele, et kuna A on Abeli rühm, siis MB on rühma A alamrühm, mille järk on seejuures rangelt suurem kui rühmal M (sest $M \subseteq MB$, kuid $b \in MB$ ja $b \notin M$). Alamrühma M valiku tõttu seega $MB = A$. Kuna A on Abeli rühm, siis kõik tema alamrühmad on normaalsed ning teoreemi 1.2.8 kasutades saame, et

$$\frac{|MB|}{|B|} = \frac{|M|}{|M \cap B|}$$

ehk

$$|A| = \frac{|M|}{|M \cap B|}|B|\,. \tag{1.25}$$

Kuna p jagab võrduse (1.25) vasakut poolt, siis jagab p ka sama võrduse paremat poolt. Kuna seejuures $\frac{|M|}{|M \cap B|}$ ei jagu arvuga p, siis peab p jagama rühma B järku r. Kuna B on tsükliline rühm moodustajaga b, siis elemendi $b^{r/p}$ järk on p. □

Oleme nüüd valmis punkti põhiteoreemi – Cauchy teoreem – tõestamiseks.

Teoreem 1.3.9 (Cauchy teoreem)**.** *Olgu G rühm, mille järk jagub algarvuga p. Siis rühmas G leidub element, mille järk on p.*

Tõestus. Tõestame väite matemaatilise induktsiooni meetodit kasutades.

Induktsiooni baas. Olgu G rühm, mille järk on algarv p. Tõestus kordab lause 1.3.8 induktsiooni baasi osa tõestust.

Induktsiooni samm. Eeldame, et väide kehtib iga rühma G korral, mille järk on väiksem kui pk, kus $k > 1$, ning mille järk jagub algarvuga p.

Lause 1.3.8 põhjal kehtib teoreemi väide Abeli rühmade korral. Olgu G seega mittekommutatiivne rühm, mille järk on pk. Olgu G järk esitatud tema kaaselementide klasside võimsuste summana kujul (1.22). Eelduse põhjal $p \mid |G|$. Kui iga $i \in \{2, 3, ..., r\}$ korral $p \mid |K_i|$, siis järelduks võrdusest (1.22), et $p \mid 1$, mis oleks vastuoluline. Seega, $p \nmid |K_j|$ mingi $j \in \{2, 3, ..., r\}$ korral. Olgu $x \in K_j$ mingi element. Lause 1.3.4 põhjal kehtib

$$|K_j| = \frac{|G|}{|C_G(x)|}\,. \tag{1.26}$$

Kaaselementide klassi K_j valiku tõttu järeldub võrdusest (1.26), et $p \mid |C_G(x)|$.

Kui $C_G(x) \neq G$, siis induktsiooni eelduse tõttu sisaldab rühm $C_G(x)$ elementi, mille järk on p ning see element on ühtlasi ka rühma G element.

Eeldame nüüd, et $C_G(x) = G$. See tähendab aga seda, et element x kommuteerub rühma G iga elemendiga ehk $x \in C(G)$, kus $C(G)$ on rühma G tsenter. Kuna aga $x \neq 1_G$ (klass $K_j \neq \{1_G\}$), siis $C(G) \neq \{1_G\}$.

Nüüd on meil kaks võimalust, kas $p \mid |C(G)|$ või $p \nmid |C(G)|$. Rühm $C(G)$ on Abeli rühm, mistõttu esimesel juhul järelduks teoreemi väide lausest 1.3.8. Vaatame nüüd juhtu kui $p \nmid |C(G)|$. Meie eelduse tõttu $C(G) \neq G$ (sest G ei ole Abeli rühm). Paneme tähele, et faktorrühma $G/C(G)$ järk $\frac{|G|}{|C(G)|}$ jagub sellisel juhul arvuga p ning on rangelt väiksem kui rühma G järk. Induktsiooni eelduse põhjal leidub element $\overline{y} = yC(G) \in G/C(G)$, mille järk on p. St, leidub selline $y^p \in C(G)$, et $y \notin C(G)$. Olgu $Y = \langle y \rangle$. Paneme tähele, et $C(G)Y$ on Abeli rühm. Kuna loomulik projektsioon $\pi : G \to G/C(G)$ on homomorfism, siis lause 1.3.6 põhjal jagab algarv p elemendi y järku rühmas G. Teisisõnu, rühma Y järk jagub algarvuga p. Esimest isomorfismiteoreemi 1.2.8 kasutades saame, et

$$\frac{|C(G)Y|}{|C(G)|} = \frac{|Y|}{|C(G) \cap Y|}$$

ehk

$$|C(G)Y| = |Y|\frac{|C(G)|}{|C(G) \cap Y|}\,. \tag{1.27}$$

Meie eelduse $p \nmid |C(G)|$ tõttu ei jaga algarv p ka rühma $C(G)$ alamrühma $C(G) \cap Y$ järku. Kuna aga $p \mid |Y|$, siis peab p jagama võrduse (1.27) paremat poolt ning seega ka sama võrduse vasakut poolt ehk $p \mid |C(G)Y|$. Nüüd lause 1.3.8 põhjal leidub Abeli rühmas $C(G)Y$ element, mille järk on p. See element on ühtlasi ka rühma G element, mille järk on p. □

1.4 Ülesanded

1. Leida rühmaga $\{1, a, b \mid a^2 = b, b^2 = a, ab = ba = 1\}$, kus 1 tähendab vaadeldava rühma ühikelementi, isomorfne substitutsioonide rühma alamrühm.

2. Lahutada substitutsioon

$$(21)(35)(56)(14)(27)(34)(25)$$

sõltumatute tsüklite korrutiseks.

3. Leida substitutsioonide rühma $\mathbb{S}_4$ kõik kolmandat järku tsüklilised alamrühmad.

4. Näidata, et seos "rühm A on rühma B normaaljagaja" ei ole transitiivne. (Näpunäide: Vaadata jada $G \trianglelefteq \mathbb{V} \trianglelefteq \mathbb{S}_4$, kus $G = \{e, (12)(34)\}$ ning $\mathbb{V}$ on Kleini neljarühm (vt näide 1.2.6(3) leheküljel 9).)

5. Näidata, et nn "üldine dieedri rühm"

$$\mathbb{D}_{2n} = \langle a, b \,|\, a^n = b^2 = 1,\, b^{-1}ab = a^{-1} \rangle$$

on lahenduv rühm. Siin a ja b on vaadeldava rühma moodustajad ning võrdused on seosed nende vahel.

6. Näidata, et rühma G elemendi x kõigil kaaselementidel on sama järk, mis elemendil x.

7. Lahutada rühm $\mathbb{S}_3$ kaaselementide klassideks ning veenduda, et $\langle (123) \rangle$ on tõepoolest rühma $\mathbb{S}_3$ normaaljagaja (nagu seda näites 1.2.6(2) väideti). Fikseerida igast kaaselementide klassist üks element ning leida tema tsentralisaator.

8. Olgu G rühm ning $x, g \in G$. Näidata, et $C_G(g^{-1}xg) = g^{-1}C_G(x)g$.

9. Näidata, et rühma $\mathbb{S}_n$ tsenter koosneb vaid ühest elemendist kui $n \geq 3$.

10. Märkida järgnevad kas "Tõene" (T) või "väär" (V).

    a. Kahe lahenduva rühma otsekorrutis on lahenduv rühm.

    b. Iga lihtne lahenduv rühm on tsükliline.

    c. Iga tsükliline rühm on lihtne.

    d. Substitutsioonide rühm S_n on lihtne kui $n \geq 5$.

    e. Rühma G mistahes elemendi x kaaselementide klass $K(x)$ on rühma G alamrühm.

Peatükk 2

Korpuseteooria elemente

Osutub, et polünoomide uurimisega on tihedalt seotud teatavad korpused. Selles peatükis me defineerime korpuse laiendid ning seletame nende seotust polünoomidega.

Polünoomi f muutujatest x_1, x_2, ..., x_n tähistame nii kujul f kui ka kujul $f(x_1, x_2, ..., x_n)$. Seda seepärast, et vahest osutub teine tähistusviis parema ülevaate saamiseks vajalikuks. Kui polünoom p on nullpolünoom, siis tähistame seda kujul $p = 0$.

2.1 Korpuse laiendid

Vaatleme 4. astme polünoomi

$$f = x^4 - 4x^2 - 5$$

üle korpuse $\mathbb{Q}$. Paneme tähele, et

$$f = (x^2 + 1)(x^2 - 5)\,,$$

millest ilmneb, et polünoomi f juured on $\pm i$ ja $\pm\sqrt{5}$, mis kuuluvad korpusesse $\mathbb{C}$. Osutub, et eksisteerib vaadeldavate juurtega seotud korpuse $\mathbb{C}$ vähim alamkorpus, mis on üheselt määratud ning sisaldab neid juuri. Seega, polünoomide üle korpuse $\mathbb{Q}$ uurimine viib meid teatud korpuse $\mathbb{C}$ alamkorpuse Σ uurimisele. Samal moel viib polünoomide uurimine üle korpuse $\mathbb{C}$ mingi alamkorpuse K meid $\mathbb{C}$ alamkorpuse Σ uurimisele, kusjuures $K \subseteq \Sigma$. Korpus Σ osutub korpuse K laiendiks. Anname aga korpuse laiendi mõistele üldisema definitsiooni.

Definitsioon 2.1.1. *Korpuse laiendiks* me nimetame monomorfismi (kui see eksisteerib)

$$\iota : K \to L\,,$$

kus K ja L on korpused.

Üldiselt, korpuse laiendi all me mõistame korpuste paari (K, L), kui on selge, millist monomorfismi (üksühest ehk injektiivset homomorfismi) me silmas peame. Kui $\iota : K \to L$ on korpuse laiend, siis me tavaliselt samastame K tema kujutisega $\iota(K)$, et võiksime vaadelda kujutust ι kui korpuse K sisestust korpusesse L ning korpust K kui korpuse L alamkorpust (st $\iota(k) = k$ iga $k \in K$ korral). Sellistel tingimustel me tähistame korpuse laiendit järgnevalt:

$$L : K\,,$$

ning ütleme, et L on korpuse K laiend. Edaspidises me samastame K ja $\iota(K)$ kõikjal, kus see on võimalik.

Näide 2.1.2. Sisestused $\iota_1 : \mathbb{Q} \to \mathbb{R}$, $\iota_2 : \mathbb{R} \to \mathbb{C}$, $\iota_3 : \mathbb{Q} \to \mathbb{C}$ on kõik korpuse laiendid.

Nagu sissejuhatuses mainitud, tegeleme korpuse $\mathbb{C}$ alamkorpuste vaatlemisega. Edasises läheb meil aga vaja teada ka ühemuutuja polünoomide ringi $K[x]$ jagatistekorpust $K(x)$ (vt [2], lk 160-166, või [5], lk 207-211). Seepärast nimetame ka sisestust $\iota : K \to K(x)$ *korpuse laiendiks* ning tähistame seda – analoogiliselt eelnevaga – $K(x) : K$.

Meil läheb vaja teada järgnevat triviaalset tulemust.

Lause 2.1.3. *Olgu L_i, $i \in I$, korpuse L alamkorpused. Siis korpuste L_i, $i \in I$, ühisosa $\cap_{i\in I} L_i$ on samuti korpuse L alamkorpus.*

Tõestus. Tähistame $L' = \cap_{i\in I} L_i$. Paneme tähele, et $L' \neq \emptyset$, sest iga korpus L_i, $i \in I$, (kui L alamkorpus) sisaldab nullelementi ja ühikelementi, mistõttu ka ühisosa $\cap_{i\in I} L_i$ sisaldab neid elemente.

Näitamaks, et L' on L alamkorpus, tuleb näidata, et L' on kinnine liitmise ja korrutamise tehete suhtes ning, et igal L' elemendil leidub liitmise suhtes vastandelement ning, et igal nullist erineval L' elemendil leidub korrutamise suhtes pöördelement. Näitame järgnevas, et L' on kinnine korrutamise tehte suhtes. Ülejäänud tingimuste täidetuses võib analoogiliselt veenduda.

Olgu seega $x, y \in L'$. Siis $x, y \in L_i$ iga $i \in I$ korral. Kuna L_i, $i \in I$, on korpused, siis $xy \in L_i$ iga $i \in I$ korral. Seega, $xy \in \cap_{i\in I} L_i = L'$. □

Asjaolu, et korpuse L alamkorpuste ühisosa on jällegi korpus, annab aluse järgnevale definitsioonile.

Definitsioon 2.1.4. Olgu X hulga $\mathbb{C}$ alamhulk. Siis kõigi hulka X sisaldavate korpuste ühisosa nimetame *hulga X poolt tekitatud korpuseks.*

Lause 2.1.5. *Olgu $X \subseteq \mathbb{C}$, $X \neq \emptyset$, $X \neq \{0\}$, ning olgu $\langle X \rangle$ hulga X poolt tekitatud korpus. Siis $\langle X \rangle$ on*

1. *Vähim ning üheselt määratud korpus, mis sisaldab hulka X. St, kui K on selline korpus, mis sisaldab hulka X, siis $\langle X\rangle \subseteq K$.*

2. *Kõigi selliste elementide hulk, millised võib saada hulga X elementidest lõpliku arvu korpuse tehete sooritamisel.*

Tõestus. Definitsiooni 2.1.4 põhjal

$$\langle X\rangle = \bigcap_{i\in I} K_i\,, \tag{2.1}$$

kus K_i $(i \in I)$ on kõik võimalikud korpused, mis sisaldavad hulka X.

1. Väide järeldub vahetult võrdusest (2.1).

2. Olgu K selline hulk, mis koosneb kõikidest sellistest elementidest, millised võime saada hulga X elementidest lõpliku arvu korpuse tehete sooritamisel. Siis K on korpus, mis sisaldab hulka X. Seega $K = K_i$ mingi indeksi $i \in I$ korral ning seetõttu $\langle X\rangle \subseteq K$. Teiselt poolt, iga korpus K_i, $i \in I$, sisaldades hulka X, sisaldab ka kõiki elemente, millised võime saada hulga X elementidest lõpliku arvu korpuse tehete sooritamisel. Seega $K \subseteq \cap_{i\in I} K_i = \langle X\rangle$. □

Lause 2.1.6. *Iga korpus sisaldab korpust $\mathbb{Q}$.*

Tõestus. Olgu K suvaline korpus. Korpuse definitsiooni (vt [5], lk 54, definitsioon 2.2.11) tõttu $0 \in K$ ja $1 \in K$, mistõttu $2 = 1 + 1 \in K$, $3 = 2 + 1 \in K$, ning induktiivselt jätkates, $n \in K$ iga naturaalarvu n korral. Kuna K on liitmise suhtes Abeli rühm, siis $-n \in K$ iga naturaalarvu n korral. Sellega oleme näidanud, et $\mathbb{Z} \subseteq K$. Nüüd aga ka suvaline ratsionaalarv p/q ($p \in \mathbb{Z}$, $q \in \mathbb{N}$) kuulub korpusesse K, sest kuna $q \neq 0$, siis $q^{-1} \in K$ ning seega $p/q = pq^{-1} \in K$.

Sellega oleme näidanud, et $\mathbb{Q} \subseteq K$. □

Näide 2.1.7. Leiame korpuse K, mis on tekitatud hulga $X = \{1, i\}$ poolt. Lause 2.1.6 põhjal $\mathbb{Q} \subseteq K$. Kuna K on kinnine arvude liitmise ja korrutamise tehete suhtes, siis $p+qi \in K$ mistahes ratsionaalarvude p ja q korral. Olgu M kõigi selliste arvude hulk. Veendume, et $M = K$. Võime vahetult kontrollida, et M on kinnine liitmise, vastandelementide võtmise ja korrutamise tehete suhtes. Paneme ka tähele, et

$$(p + qi)^{-1} = \frac{p}{p^2 + q^2} - \frac{q}{p^2 + q^2} i\,,$$

mis tähendab, et igal nullist erineval elemendil hulgast M leidub pöördelement hulgas M. Seega, M on korpus, mis sisaldab alamhulka X. Lause 2.1.5

esimeset väitest järeldub nüüd, et $K \subseteq M$. Teiselt poolt, korpuse M definitsiooni tõttu, $M \subseteq K$. Seega, hulga X poolt tekitatud korpus K on kirjeldatav järgnevalt:

$$K = \{p + qi \,|\, p, q \in \mathbb{Q}\}\,.$$

Definitsioon 2.1.8. Olgu $L : K$ korpuse laiend ning Y hulga L alamhulk ($L \subseteq \mathbb{C}$). Siis hulga $K \cup Y$ poolt tekitatud korpust tähistame $K(Y)$ ning ütleme, et $K(Y)$ *on saadud hulga* Y *adjungeerimisel korpusele* K.

Korpusele K mingi hulga $\{\xi_1, \xi_2, ..., \xi_n\}$ adjungeerimist tähistame lihtsalt $K(\xi_1, \xi_2, ..., \xi_n)$. Toome eelneva definitsiooni selgituseks paar näidet.

Näide 2.1.9. Korpus $\mathbb{C}$ on saadud korpusest $\mathbb{R}$ temale üheelemendilise hulga $\{i\}$ adjungeerimisel, st, $\mathbb{C} = \mathbb{R}(i)$. Samuti, võib veenduda, et korpuse $\mathbb{R}$ alamkorpus $P = \{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\}$ on võrdne korpusega $\mathbb{Q}(\sqrt{2})$.

Lause 2.1.10. *Olgu korpus* $K(X_1 \cup X_2 \cup ... \cup X_m)$, $m \in \mathbb{N}$, *saadud korpusest* K *hulga* $X_1 \cup X_2 \cup ... \cup X_m$ *adjungeerimisel. Siis*

$$K(X_1 \cup X_2 \cup \ldots \cup X_m) = K(X_1)(X_2)\ldots(X_m)\,.$$

See tähendab, et mingi hulga adjungeerimist korpusele K *võib teostada selle hulga alamhulkade järjestikuste adjungeerimistena.*

Tõestus. Tõestuseks piisab näidata, et mingi hulga Y adjungeerimist korpusele K võib teostada tema mingite alamhulkade Y_1 ja Y_2 järjestikuste adjungeerimistena, st

$$K(Y) = K(Y_1 \cup Y_2) = K(Y_1)(Y_2)\,.$$

Veendume seega kõigepealt, et $K(Y_1 \cup Y_2) \subseteq K(Y_1)(Y_2)$. Definitsioonide 2.1.8 ja 2.1.4 põhjal kehtivad

$$K \cup (Y_1 \cup Y_2) = (K \cup Y_1) \cup Y_2 \subseteq K(Y_1) \cup Y_2 \subseteq K(Y_1)(Y_2)\,.$$

See tähendab, et $K(Y_1)(Y_2)$ on korpus, mis sisaldab hulki K ja $Y_1 \cup Y_2$ ning definitsioonide 2.1.8 ja 2.1.4 põhjal seega $K(Y_1 \cup Y_2) \subseteq K(Y_1)(Y_2)$.

Veendume nüüd, et $K(Y_1)(Y_2) \subseteq K(Y_1 \cup Y_2)$. Hulk $K(Y_1 \cup Y_2)$ sisaldab peale korpuse K ka ühendit $Y_1 \cup Y_2$, mistõttu sisaldab mõlemat hulka Y_1 ja Y_2. Seega, kuna $K(Y_1 \cup Y_2)$ on korpus, mis sisaldab hulki K, Y_1 ja Y_2, siis sisaldab ta ka hulki $K(Y_1)$ ja Y_2 ning seega ka korpust $K(Y_1)(Y_2)$ (vt definitsioone 2.1.8 ja 2.1.4). □

2.1.1 Lihtlaiendid

Definitsioon 2.1.11. Korpuse K laiendit $K(\xi) : K$, kus $K(\xi)$ on saadud korpusest K üheainsa elemendi $\xi \in \mathbb{C}$ adjungeerimisel, nimetame *lihtlaiendiks*. Elementi ξ nimetame seejuures *lihtlaiendi moodustavaks elemendiks*.

Märgime jällegi, et ka laiendit $K(x) : K$, kus $K(x)$ on ringi $K[x]$ jagatistekorpus, nimetame *lihtlaiendiks* ning muutujat x selle laiendi *moodustavaks elemendiks*.

Lause 2.1.10 põhjal kehtib võrdus

$$K(\xi_1, \xi_2, \ldots, \xi_n) : K = K(\xi_1)(\xi_2) \ldots (\xi_n) : K\,,$$

kus $\xi_1, \xi_2, ..., \xi_n \in \mathbb{C}$ on mingid elemendid. Sel põhjusel tasub meil uurida just lihtlaiendeid.

Näide 2.1.12.

1. Laiendid $\mathbb{C} : \mathbb{R}$ ja $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ on mõlemad lihtlaiendid (vt näide 2.1.9).

2. Laiend võib osutuda lihtlaiendiks, olgugi, et esmapilgul see nii ei tundu. Vaatame laiendit $L : \mathbb{Q}$, kus $L = \mathbb{Q}(i, -i, \sqrt{2}, -\sqrt{2})$. Veendume, et $L = L'$, kus $L' = \mathbb{Q}(i + \sqrt{2})$. Selle näitamiseks piisab näidata, et $i \in L'$ ja $\sqrt{2} \in L'$, sest sellest järeldub, et $L \subseteq L'$, mis koos triviaalselt kehtiva sisalduvusega $L' \subseteq L$, annabki meile, et $L = L'$.

   Paneme tähele, et L' sisaldab elementi

   $$\left(i + \sqrt{2}\right)^2 = -1 + 2i\sqrt{2} + 2 = 1 + 2i\sqrt{2}\,.$$

   Nüüd L' sisaldab ka elementi

   $$\left(i + \sqrt{2}\right)\left(1 + 2i\sqrt{2}\right) = 5i - \sqrt{2}$$

   ning seega ka elementi

   $$\left(5i - \sqrt{2}\right) + \left(i + \sqrt{2}\right) = 6i\,,$$

   millest järeldub, et $i \in L'$. Nüüd aga ka $\left(i + \sqrt{2}\right) - i = \sqrt{2} \in L'$. Sellega oleme näidanud, et $L = L'$ ning laiend $L : \mathbb{Q}$ on seega lihtlaiend.

Definitsioon 2.1.13. *Isomorfismiks kahe korpuse laiendi $\iota : K \to L$ ja $j : K' \to L'$ vahel* nimetame isomorfismide $\lambda : K \to K'$ ja $\mu : L \to L'$ paari (λ, μ), mille korral iga $k \in K$ puhul kehtib võrdus

$$j(\lambda(k)) = \mu(\iota(k)) \tag{2.2}$$

ehk, piltlikult väljendudes, diagramm

$$\begin{array}{ccc} K & \stackrel{\iota}{\to} & L \\ \lambda\downarrow & & \downarrow\mu \\ K' & \underset{j}{\to} & L' \end{array}$$

on kommutatiivne. Ütleme ka, et laiendid (L, K) ja (L', K') on sellisel juhul isomorfsed.

Toodud definitsioonist saame teha paar järeldust. Kui me samastame K ja $\iota(K)$ ning K' ja $j(K')$, siis ι ja j on sisestused ning kommutatiivsuse tingimus saab kuju

$$\mu|_K = \lambda\,,$$

kus $\mu|_K$ tähistab kujutuse μ ahendit korpusele K. Teiste sõnadega, korpuste K ja K' vaheline isomorfism säilib sellisel juhul korpuste L ja L' vahelises isomorfismis. Isomorfismi μ nimetame sellisel juhul ka isomorfismi λ jätkuks. Kui me lisaks samastame korpused K ja K', siis kujutus λ on samasusteisendus, mistõttu ka $\mu|_K$ on samasusteisendus.

Võime eristada kahte tüüpi lihtlaiendeid – algebralisi ja transtsendentseid.

Definitsioon 2.1.14. Olgu K korpus ning olgu α mingi element (mis võib olla nii kompleksarv kui ka tundmatu muutuja kompleksarvude hulgas). Ütleme, et element α on *algebraline üle* K, kui leidub selline nullpolünoomist erinev polünoom p üle K, et $p(\alpha) = 0$. Vastavat lihtlaiendit $K(\alpha) : K$ nimetame sel juhul *algebraliseks lihtlaiendiks*. Kui aga ei leidu sellist nullpolünoomist erinevat polünoomi p üle K, et $p(\alpha) = 0$, siis nimetame elementi α *transtsendentseks üle* K ning vastavat lihtlaiendit $K(\alpha) : K$ *transtsendentseks lihtlaiendiks*.

Kui element α on algebraline üle $\mathbb{Q}$ siis ütleme selle asemel lihtsalt, et α on *algebraline* ning kui α on transtsendentne üle $\mathbb{Q}$, siis ütleme, et α on *transtsendentne*.

Näide 2.1.15. Arv $\sqrt{2}$ on algebraline, sest $\sqrt{2}$ rahuldab võrrandit $x^2 - 2 = 0$ ehk teisisõnu, $\sqrt{2}$ on polünoomi $x^2 - 2$ juur. Arv $\sqrt[3]{2}$ on samuti algebraline, sest ta rahuldab võrrandit $x^3 - 2 = 0$. Arv $\sqrt{\pi}$ on algebraline üle $\mathbb{Q}(\pi)$, sest ta rahuldab võrrandit $x^2 - \pi = 0$. On seejuures tõestatud, et arvud π ja e on transtsendentsed.

Algebra põhiteoreemi põhjal leidub igal n-astme polünoomil üle kompleksarvude korpuse $\mathbb{C}$ täpselt n juurt, mis kuuluvad hulka $\mathbb{C}$. Kompleksarvulist muutujat x me üldiselt ei loe ühegi nullpolünoomist erineva polünoomi (üle $\mathbb{C}$) juureks. Seepärast kehtib järgnev teoreem.

Teoreem 2.1.16. *Laiend $K(x) : K$, kus $K(x)$ on ringi $K[x]$ jagatistekorpus, on transtsendentne lihtlaiend.*

Olgu nüüd $K(\alpha) : K$ algebraline lihtlaiend. Siis leidub selline nullpolünoomist erinev polünoom p üle K, et $p(\alpha) = 0$. Seejuures võime eeldada, et p on normeeritud (võime polünoomi p alati pealiikme kordajaga läbi jagada). Seega, alati leidub vähemalt üks madalaima astmega nullpolünoomist erinev normeeritud polünoom, millele α on juureks. Me väidame, et selline polünoom p on üheselt määratud. Oletame, et p ja q on sellised polünoomid. Siis $p(\alpha) - q(\alpha) = 0$. Seega, juhul kui $p \neq q$, siis polünoomi $p - q$ mingi kordne on nullpolünoomist erinev, normeeritud ning madalama astme polünoom kui p. Seejuures paneme tähele, et α on selle polünoomi juur. Vastuolu, sest meie eelduse põhjal oli p selline madalaima astme polünoom. See asjaolu on aluseks järgnevale definitsioonile.

Definitsioon 2.1.17. Olgu $K(\alpha) : K$ algebraline lihtlaiend. Siis selle *laiendi määravaks polünoomiks* nimetame sellist nullpolünoomist erinevat madalaima astme normeeritud polünoomi üle K, millele α on juureks.

Definitsioon 2.1.18. Olgu $L : K$ korpuse laiend ning olgu element $\alpha \in L$ algebraline üle K. Siis laiendi $K(\alpha) : K$ määravat polünoomi nimetame *elemendi α minimaalseks polünoomiks* (*üle K*).

Näide 2.1.19. Imaginaararv $i \in \mathbb{C}$ on algebraline üle $\mathbb{R}$. Olgu $m = x^2 + 1$. Sellisel juhul $m(i) = 0$. Paneme tähele, et polünoom m on normeeritud. Ainsad nullist erinevad normeeritud polünoomid üle $\mathbb{R}$, mille aste on väiksem kui polünoomil m, on kujul $x + r$, kus $r \in \mathbb{R}$, või konstantne polünoom 1. Arv i aga ei ole ühegi sellise polünoomi juureks, sest vastasel korral kuuluks i hulka $\mathbb{R}$, mida ei saa aga olla. Seega, arvu i minimaalne polünoom üle $\mathbb{R}$ on $x^2 + 1$.

Lause 2.1.20. *Olgu α algebraline üle korpuse K. Siis α minimaalne polünoom üle K on taandumatu üle K ning jagab iga polünoomi üle K, millele α on juureks.*

Tõestus. Olgu m elemendi α minimaalne polünoom üle K. Oletame vastuväiteliselt, et m ei ole taandumatu, st, leiduvad madalama astme polünoomid f ja g üle K nii, et $m = fg$. Sellisel juhul, kuna m on normeeritud, peavad ka f ja g olema normeeritud. Kuna $m(\alpha) = 0$, siis $f(\alpha)g(\alpha) = 0$, mistõttu $f(\alpha) = 0$ või $g(\alpha) = 0$. See on aga vastuolus asjaoluga, et m on α minimaalne polünoom.

Oletame nüüd, et p on polünoom üle K, millele α on juureks, st $p(\alpha) = 0$. Kasutame polünoomide jäägiga jagamise teoreemi, mille põhjal leiduvad üheselt määratud polünoomid q ja r üle K nii, et $p = mq + r$, kusjuures

$\deg r < \deg m$ (vt [5], lk 197, teoreem 6.11.1). Sellisel juhul

$$0 = p(\alpha) = m(\alpha)q(\alpha) + r(\alpha) = 0 + r(\alpha) = r(\alpha)\,.$$

Kui $r \neq 0$, siis polünoomi r mingi K elemendi kordne on normeeritud polünoom, millele element α on juureks. Kuna aga $\deg r < \deg m$, siis ei saa m olla elemendi α minimaalne polünoom. Saadud vastuolu tõttu peab $r = 0$ ning m jagab seega polünoomi p. □

Lause 2.1.21. *Olgu K korpus ning olgu m taandumatu normeeritud polünoom üle K,* $\deg m > 0$. *Siis leidub $\alpha \in \mathbb{C}$, mis on algebraline üle K, nii et α minimaalne polünoom üle K on m.*

Tõestus. Olgu $\alpha \in \mathbb{C}$ polünoomi m mistahes juur. Siis $m(\alpha) = 0$ ning lause 2.1.20 põhjal α minimaalne polünoom f üle K jagab polünoomi m. Kuna aga m on taandumatu üle K ning nii f kui ka m on normeeritud, siis $f = m$. □

Järgnevalt on meil vaja aga teada mõningaid arvuteooria põhiliste tulemuste analoogiaid.

Definitsioon 2.1.22. Ütleme, et *polünoomid a ja b üle korpuse K on kongruentsed mooduli $m \in K[x]$ järgi* kui $m \mid a - b$ ringis $K[x]$. Asjaolu, et a ja b on kongruentsed mooduli m järgi, tähistame

$$a \equiv b \pmod{m}\,.$$

Lause 2.1.23. *Olgu* $a_1 \equiv a_2 \pmod{m}$ *ja* $b_1 \equiv b_2 \pmod{m}$. *Siis*

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m} \qquad \textit{ja} \qquad a_1 b_1 \equiv a_2 b_2 \pmod{m}\,.$$

Tõestus. Eelduse põhjal leiduvad polünoomid $a, b \in K[x]$ nii, et $a_1 - a_2 = am$ ja $b_1 - b_2 = bm$. Nüüd

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = am + bm = (a + b)m\,,$$

millega on lause esimene väide tõestatud. Korrutise korral

$$\begin{aligned} a_1 b_1 - a_2 b_2 &= a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 = \\ &= a_1(b_1 - b_2) + b_2(a_1 - a_2) = a_1 bm + b_2 am = (a_1 b + b_2 a)m\,. \end{aligned}$$ □

Lause 2.1.24. *Olgu m mingi polünoom üle korpuse K, kusjuures $m \neq 0$ (m ei ole nullpolünoom). Siis iga polünoom $a \in K[x]$ on mooduli m järgi kongruentne üheselt määratud polünoomiga üle K, mille aste on väiksem kui polünoomi m aste.*

Tõestus. Jagame polünoomi a jäägiga polünoomiga m. Saame, et $a = mq + r$, kus $q, r \in K[x]$ ning $\deg r < \deg m$. Sellisel juhul $a - r = mq$, mistõttu $a \equiv r \pmod{m}$.

Jääb veel näidata ühesust. Oletame, et

$$a \equiv r \pmod{m} \tag{2.3}$$

ning

$$a \equiv s \pmod{m}\,, \tag{2.4}$$

kusjuures $\deg r < \deg m$ ja $\deg s < \deg m$. Näitame, et sellisel juhul $r = s$. Tingimused (2.3) ja (2.4) on samaväärsed tingimustega, et leiduvad polünoomid q_1 ja q_2 üle K nii, et

$$a - r = mq_1\,, \qquad a - s = mq_2\,.$$

Siis aga

$$r - s = m(q_2 - q_1)\,,$$

mis tähendab, et $m \mid (r-s)$. Kuna aga $\deg(r - s) < \deg m$, siis peab $r-s = 0$ ehk $r = s$. Sellega on ühesus näidatud. □

Võib veenduda, et definitsioonis 2.1.22 toodud seos $\equiv$ on ekvivalentsiseos hulgal $K[x]$, mistõttu vaadeldav hulk $K[x]$ jaguneb ekvivalentsiklassideks mooduli m järgi. Tähistame polünoomi $a \in K[x]$ ekvivalentsiklassi sümboliga $[a]$. Paneme tähele, et

$$[a] = \big\{f \in K[x] \;\big|\; a \equiv f \pmod{m}\big\} = \big\{f \in K[x] \;\big|\; m \mid (f - a)\big\} = \\ = \big\{f \in K[x] \;\big|\; \exists p \in K[x] : f = a + mp\big\}\,.$$

Ekvivalentsiklasside $[a]$ ja $[b]$ summa ja korrutis on defineeritud järgnevalt:

$$[a] + [b] = [a + b]\,, \qquad [a][b] = [ab]\,.$$

Lause 2.1.23 põhjal ei sõltu ekvivalentsiklasside $[a]$ ja $[b]$ summa ja korrutis ekvivalentsiklasside esindajate valikust. Kõigi ekvivalentsiklasside hulka mooduli $m \in K[x]$ järgi tähistame järgnevalt:

$$K[x]/\langle m\rangle\,.$$

Lause 2.1.24 põhjal iga ekvivalentsiklass [a] sisaldab üheselt määratud polünoomi, mille aste on väiksem kui polünoomi m aste, mida nimetame *polünoomi a taandatud vormiks*. Seega, ekvivalentsiklassidega tehete sooritamine on samaväärne taandatud vormidega tehete sooritamisega, lugedes, et $m = 0$. Klass $[m] = [0]$ kujutab seejuures liitmise suhtes ühikelementi hulgas $K[x]/\langle m\rangle$ ning klass, mille esindajaks on korpuse K ühikelement 1, kujutab korrutamise suhtes ühikelementi. Viimast ekvivalentsiklassi tähistame sümboliga [1]. Osutub, et $K[x]/\langle m\rangle$ on jäägiklasside liitmise ja korrutamise suhtes ring.

Teoreem 2.1.25. *Olgu m mingi polünoom üle korpuse K, $m \neq 0$. Siis hulga $K[x]/\langle m\rangle$ iga nullist erinev element omab pöördelementi hulgas $K[x]/\langle m\rangle$ siis ja ainult siis kui polünoom m on taandumatu üle K.*

Tõestus. Tarvilikkus. Oletame vastuväiteliselt, et m ei ole taandumatu üle K. Siis $m = ab$, kus $\deg a < \deg m$, $\deg b < \deg m$. Seejuures paneme tähele, et $[a][b] = [ab] = [m] = [0]$. Kuna $m \neq 0$, siis ka $a \neq 0$ ning eelduse tõttu leidub klassil $[a]$ pöördklass $[c]$. Sellisel juhul $[c][a] = [1]$ ning

$$[0] = [c][0] = [c]\,([a][b]) = ([c][a])\,[b] = [1][b] = [b]\,.$$

See tähendab, et $m \mid b$. Kuna $\deg b < \deg m$, siis peab $b = 0$ ning seega ka $m = ab = 0$. See on vastuolu, sest eelduse tõttu $m \neq 0$. Seega, kui mingil klassil $[a] \in K[x]/\langle m\rangle$ leidub pöördelement, siis m peab olema taandumatu.

Piisavus. Oletame, et m on taandumatu. Olgu $a \in K[x]$, kusjuures $[a] \neq [0]$ ehk $m \nmid a$. Sellisel juhul, kuna m on taandumatu, on polünoomide m ja a suurim ühistegur 1. Siis aga leiduvad polünoomid h ja k üle K nii, et $ha + km = 1$ (vt näiteks [2], lk 208, teoreem 3). Nüüd $[h][a] + [k][m] = [1]$. Kuid kuna $[m] = [0]$, siis

$$[1] = [h][a] + [k][m] = [h][a] + [k][0] = [h][a] + [0] = [h][a]\,.$$

Seega, klass $[h]$ on klassi [a] pöördklass. □

Järeldus 2.1.26. *Olgu m polünoom üle korpuse K, $m \neq 0$. Siis ring $K[x]/\langle m\rangle$ on korpus parajasti siis kui m on taandumatu üle K.*

Tõestus. Väide järeldub vahetult teoreemist 2.1.25, sest korpus on ring, mille igal nullist erineval elemendil leidub pöördelement. □

Oleme nüüd valmis klassifitseerima lihtlaiendeid.

Teoreem 2.1.27. *Olgu K korpus ning $\alpha \in \mathbb{C}$ mingi transtsendentne element üle K. Siis transtsendentne lihtlaiend $K(\alpha) : K$ on isomorfne jagatistekorpuse laiendiga $K(x) : K$.*

Tõestus. Defineerime kujutuse $\phi : K(x) \to K(\alpha)$ järgnevalt

$$\phi\left(\frac{f}{g}\right) = \frac{f(\alpha)}{g(\alpha)}\,. \tag{2.5}$$

Kui $g \neq 0$, siis ka $g(\alpha) \neq 0$, sest α on transtsendentne üle K, mistõttu sel definitsioonil on mõtet. Olgu $f_1/g_1, f_2/g_2 \in K(x)$ sellised, et

$$\frac{f_1}{g_1} = \frac{f_2}{g_2}\,. \tag{2.6}$$

Võrdus (2.6) ütleb meile seda, et

$$\frac{f_1(c)}{g_1(c)} = \frac{f_2(c)}{g_2(c)}$$

iga $c \in \mathbb{C}$ korral ratsionaalfunktsioonide f_1/g_1, f_2/g_2 määramispiirkonnast. Siis aga ka

$$\frac{f_1(\alpha)}{g_1(\alpha)} = \frac{f_2(\alpha)}{g_2(\alpha)}$$

ning võrdus (2.5) on korrektselt defineeritud.

Paneme tähele, et, korpuse tehteid "+", "−", "·", ":" silmas pidades,

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \,\middle|\, \frac{f}{g} \in K(x) \right\} .$$

Seega, kui $y \in K(\alpha)$ on suvaline, siis $y = f(\alpha)/g(\alpha)$ mingite polünoomide f, $g \in K[x]$ korral ($g \neq 0$). Elemendi y originaal kujutuse ϕ suhtes on seega ratsionaalfunktsioon f/g. Sellega oleme näidanud, et ϕ on sürjektiivne. Olgu nüüd $f_1(\alpha)/g_1(\alpha)$, $f_2(\alpha)/g_2(\alpha) \in K(\alpha)$ sellised, et

$$\frac{f_1(\alpha)}{g_1(\alpha)} = \frac{f_2(\alpha)}{g_2(\alpha)} .$$

Siis

$$f_1(\alpha)g_2(\alpha) = f_2(\alpha)g_1(\alpha) ,$$

mis ütleb meile seda, et α on polünoomi $f_1g_2 - f_2g_1$ üle K juur. Kuna element α on eelduse tõttu transtsendentne üle K, siis peab $f_1g_2 - f_2g_1 = 0$ ehk $f_1g_2 = f_2g_1$. Siis aga $f_1/g_1 = f_2/g_2$ ning kujutus ϕ on seega injektiivne.

Arvestades nüüd, kuidas on defineeritud tehted jagatistekorpuses ning kuidas me teostame tehteid murdudega hulgas $K(\alpha)$, võime veenduda, et kujutus ϕ on ka homomorfism. Seega, ϕ on isomorfism. Paneme tähele, et $\phi|_K$ on samasusteisendus. Definitsiooni 2.1.13 põhjal (vt antud definitsiooni all olevat selgitust) on laiendid $K(\alpha) : K$ ja $K(x) : K$ seega isomorfsed. □

Teoreem 2.1.28. *Olgu $K(\alpha) : K$ algebraline lihtlaiend ning olgu m selle laiendi määrav polünoom. Siis $K(\alpha) \cong K[x]/\langle m \rangle$, kusjuures isomorfismi $\phi : K[x]/\langle m \rangle \to K(\alpha)$ saab nii valida, et $\phi([x]) = \alpha$ ning, et $\phi([k]) = k$ iga $k \in K$ korral.*

Tõestus. Lause 2.1.20 põhjal on polünoom m taandumatu üle K, mistõttu järelduse 2.1.26 põhjal on $K[x]/\langle m \rangle$ korpus. Defineerime kujutuse $\phi : K[x]/\langle m \rangle \to K(\alpha)$ järgnevalt:

$$\phi([p]) = p(\alpha) ,$$

kus $[p]$ on polünoomi p ekvivalentsiklass mooduli m järgi. Veendume, et ϕ on korrektselt defineeritud. Olgu $[p] = [q]$. Siis $p \equiv q \pmod{m}$ ehk $m \mid p - q$, mistõttu $p - q = mt$ mingi polünoomi $t \in K[x]$ korral. Nüüd aga $p(\alpha) - q(\alpha) = m(\alpha)t(\alpha) = 0$, mistõttu $p(\alpha) = q(\alpha)$ ehk $\phi([p]) = \phi([q])$ ning ϕ on seega korrektselt defineeritud.

Paneme tähele, et kehtivad võrdused

$$\phi([p] + [q]) = \phi([p + q]) = (p + q)(\alpha) = p(\alpha) + q(\alpha) = \phi([p]) + \phi([q])\,,$$
$$\phi([p][q]) = \phi([pq]) = (pq)(\alpha) = p(\alpha)q(\alpha) = \phi([p])\phi([q])\,,$$

mistõttu ϕ on korpuste $K[x]/\langle m\rangle$ ja $K(\alpha)$ homomorfism.

Veendume, et kujutus ϕ on sürjektiivne. Selleks olgu $y \in K(\alpha)$ suvaline. Paneme jällegi tähele (nagu teoreemi 2.1.27 tõestuseski), et element y esitub, korpuse tehteid silmas pidades, kujul $y = \frac{f(\alpha)}{g(\alpha)}$, kus $f/g \in K(x)$ ning $g(\alpha) \neq 0$. Nüüd aga $m \nmid g$ (vastasel juhul peaks mingi polünoomi q korral $g(\alpha) = m(\alpha)q(\alpha) = 0q(\alpha) = 0$, mis on vastuoluline, sest $g(\alpha) \neq 0$). Seega, kuna m on taandumatu üle K, siis[1] $(m, g) = 1$, mistõttu leiduvad polünoomid $a, b \in K[x]$ nii, et $ag + bm = 1$. Nüüd aga $a(\alpha)g(\alpha) = 1$ ehk $\frac{1}{g(\alpha)} = a(\alpha)$ ning $\frac{f(\alpha)}{g(\alpha)} = f(\alpha)a(\alpha) = h(\alpha)$, kus $h \in K[x]$. Jagame polünoomi h jäägiga polünoomiga m. Saame, et $h = mq + r$, kus $\deg r < \deg m$. Nüüd

$$\phi([r]) = r(\alpha) = h(\alpha) - m(\alpha)q(\alpha) = h(\alpha) = f(\alpha)a(\alpha) = \frac{f(\alpha)}{g(\alpha)} = y\,,$$

mis tähendab, et elemendil y leidub originaal kujutuse ϕ suhtes. Sellega oleme näidanud, et ϕ on pealekujutus.

Veendume nüüd, et kujutus ϕ on ka injektiivne. Selleks olgu $y_1, y_2 \in K(\alpha)$ sellised, et $y_1 = y_2$. Olgu $[r_i] \in K(x)/\langle m\rangle$ elemendi y_i originaal kujutuse ϕ suhtes, $r_i \in K[x]$, $\deg r_i < \deg m$, $i \in \{1, 2\}$. Nüüd

$$\phi([r_1]) = r_1(\alpha) = y_1 = y_2 = r_2(\alpha) = \phi([r_2])\,,$$

millest $(r_1 - r_2)(\alpha) = r_1(\alpha) - r_2(\alpha) = 0$. Lause 2.1.20 põhjal siis $m \mid r_1 - r_2$. See aga tähendab, et $[r_1] = [r_2]$ ning ϕ on injektiivne.

Sellega oleme näidanud, et ϕ on isomorfism, mistõttu $K(\alpha) \cong K[x]/\langle m\rangle$. Paneme veel lõpuks tähele, et $\phi([x]) = \alpha$ ning, et $\phi([k]) = k$ iga $k \in K$ korral. □

Järeldus 2.1.29. *Olgu $K(\alpha) : K$ ja $K(\beta) : K$ sellised algebralised lihtlaiendid, milledel on sama määrav polünoom m üle K. Siis need kaks laiendit on isomorfsed, kusjuures korpuste $K(\alpha)$ ja $K(\beta)$ vahelise isomorfismi võib valida selliselt, et α kujutub elemendiks β ning et korpuse K elemendid jäävad invariantseks.*

[1] Sümboliga (f, g) tähistame polünoomide f ja g suurimat ühistegurit.

Tõestus. Teoreemi 2.1.28 põhjal $K(\alpha) \cong K[x]/\langle m\rangle$ ning $K(\beta) \cong K[x]/\langle m\rangle$. Seejuures saame valida isomorfismid $\iota : K[x]/\langle m\rangle \to K(\alpha)$ ja $j : K[x]/\langle m\rangle \to K(\beta)$ selliselt, et $\iota(x) = \alpha$ ja $j(x) = \beta$ ning nii, et $\iota|_K$ ja $j|_K$ oleksid samasusteisendused. Siis aga kujutus $j\iota^{-1} : K(\alpha) \to K(\beta)$ on isomorfism, kusjuures $j\iota^{-1}(\alpha) = \beta$ ning $j\iota^{-1}|_K$ on samasusteisendus. Definitsiooni 2.1.13 (vt definitsiooni all olevat selgitust) põhjal on laiendid $K(\alpha) : K$ ja $K(\beta) : K$ isomorfsed. □

Lause 2.1.30. *Olgu $\iota : K \to K'$ korpuste K ja K' isomorfism. Siis kujutus $\hat{\iota} : K[x] \to K'[x]$, mis on defineeritud seosega*

$$\hat{\iota}\left(k_0 + k_1 x + \ldots + k_n x^n\right) = \iota\left(k_0\right) + \iota\left(k_1\right) x + \ldots + \iota\left(k_n\right) x^n ,$$

kus $k_0, k_1, ..., k_n \in K$, on ringide $K[x]$ ja $K'[x]$ isomorfism.

Tõestus. Arvestades kahe polünoomi võrdsuse definitsiooni ning seda, et isomorfism ι on korrektselt defineeritud, saame, et kujutus $\hat{\iota}$ on korrektselt defineeritud. Paneme tähele, et $\hat{\iota}(1) = \iota(1) = 1$. St, $\hat{\iota}$ viib ringi $K[x]$ ühikelemendi ringi $K'[x]$ ühikelemendiks. Pidades silmas polünoomide liitmise ja korrutamise definitsiooni ning seda, et kujutus ι on homomorfism, võime veenduda, et ka kujutus $\hat{\iota}$ on ringide $K[x]$ ja $K'[x]$ homomorfism. Pidades jällegi kahe polünoomi võrdsuse definitsiooni silmas ning seda, et kujutus ι on injektiivne, võime veenduda, et ka kujutus $\hat{\iota}$ on injektiivne. Lõpuks, kuna kujutus ι on sürjektiivne, siis on seda ka kujutus $\hat{\iota}$. Seega on kujutus $\hat{\iota}$ isomorfism. □

Teoreem 2.1.31. *Olgu $\iota : K \to K'$ korpuste K ja K' isomorfism. Olgu $K(\alpha) : K$ ja $K'(\beta) : K'$ algebralised lihtlaiendid, millede määravad polünoomid on vastavalt m_α (üle K) ja m_β (üle K'). Oletame lisaks, et $m_\beta = \hat{\iota}(m_\alpha)$ (lause 2.1.30 tähistuses). Siis leidub isomorfism $j : K(\alpha) \to K'(\beta)$ nii, et $j|_K = \iota$ ning, et $j(\alpha) = \beta$.*

Tõestus. Piltlikult kirjeldades on olukord järgnev:

$$\begin{array}{ccc} K & \to & K(\alpha) \\ \iota\downarrow & & \downarrow j \\ K' & \to & K'(\beta) \end{array} ,$$

kus isomorfism j tuleb meil leida.

Teoreemi 2.1.28 tõestuses näidatu põhjal võime iga elemendi jaoks korpusest $K(\alpha)$ kasutada nn taandatud vormi, st iga elemendi $y \in K(\alpha)$ võime kirjutada kujul $p_y(\alpha)$, kus p_y on teatav polünoom üle K, mille aste on väiksem kui polünoomil m_α. Analoogiline väide kehtib ka korpuse $K'(\beta)$ kohta.

Defineerime nüüd kujutuse $j : K(\alpha) \to K'(\beta)$ seega järgnevalt:

$$j(p(\alpha)) = (\hat{\iota}(p))(\beta) ,$$

kus $p \in K[x]$, $\deg p < \deg m_\alpha$ ning $\hat{\iota} : K[x] \to K'[x]$ on defineeritud selliselt nagu lauses 2.1.30 defineeritud kujutus $\hat{\iota}$.

Veendume, et kujutus j on korrektselt defineeritud. Olgu $p(\alpha)$, $q(\alpha) \in K(\alpha)$ sellised, et $p(\alpha) = q(\alpha)$, $\deg p < \deg m_\alpha$ ning $\deg q < \deg m_\alpha$. Siis $p(\alpha) - q(\alpha) = 0$ ning lause 2.1.20 põhjal $m_\alpha \mid p - q$, mistõttu peab $p - q = 0$ ehk $p = q$. Nüüd aga ka $\hat{\iota}(p) = \hat{\iota}(q)$ ning seega $(\hat{\iota}(p))(\beta) = (\hat{\iota}(q))(\beta)$. Kujutus j on seega korrektselt defineeritud.

Veendume, et $j : K(\alpha) \to K'(\beta)$ on homomorfism. Polünoomide liitmise definitsiooni ning asjaolu, et $\hat{\iota} : K[x] \to K'[x]$ on homomorfism, kasutades leiame, et

$$\begin{aligned} j(p_1(\alpha) + p_2(\alpha)) = j((p_1 + p_2)(\alpha)) = (\hat{\iota}(p_1 + p_2))(\beta) = (\hat{\iota}(p_1) + \hat{\iota}(p_2))(\beta) = \\ = (\hat{\iota}(p_1))(\beta) + (\hat{\iota}(p_2))(\beta) = j(p_1(\alpha)) + j(p_2(\alpha))\,. \end{aligned}$$

Analoogiliselt võime veenduda, et ka $j(p_1(\alpha)p_2(\alpha)) = j(p_1(\alpha))j(p_2(\alpha))$. Sellega oleme näidanud, et $j : K(\alpha) \to K'(\beta)$ on homomorfism.

Näitame nüüd, et j on bijektiivne. Selleks piisab näidata, et kujutusel j leidub pöördkujutus (vt [5], lk 19, teoreem 1.5.17). Kuna $\hat{\iota} : K[x] \to K'[x]$ on isomorfism, siis leidub pöördkujutus $\hat{\iota}^{-1} : K'[x] \to K[x]$, mis on seejuures samuti isomorfism ning on defineeritud sarnaselt kujutusega $\hat{\iota}$, st,

$$\hat{\iota}^{-1}\left(k'_0 + k'_1 x + \ldots + k'_n x^n\right) = \iota^{-1}\left(k'_0\right) + \iota^{-1}\left(k'_1\right) x + \ldots + \iota^{-1}\left(k'_n\right) x^n\,,$$

kus $k'_0 + k'_1 x + \ldots + k'_n x^n \in K'[x]$ on suvaline ning ι^{-1} on kujutuse ι pöördkujutus.

Defineerime nüüd, sarnaselt kujutusega j, kujutuse $j' : K'(\beta) \to K(\alpha)$ järgnevalt:

$$j'(p'(\beta)) = (\hat{\iota}^{-1}(p'))(\alpha)\,,$$

kus $p' \in K'[x]$, $\deg p' < \deg m_\beta$. Sarnaselt nagu kujutuse j korralgi, võime veenduda, et ka j' on korrektselt defineeritud. Veendume, et j' on kujutuse j pöördkujutus. Selleks olgu $p'(\beta) \in K'(\beta)$ ($p' \in K'[x]$, $\deg p' < \deg m_\beta$) suvaline. Meie eelduse $m_\beta = \hat{\iota}(m_\alpha)$ tõttu on polünoomidel m_α ja m_β sama aste. Seega, $\deg \hat{\iota}^{-1}(p') = \deg p' < \deg m_\beta = \deg m_\alpha$, mistõttu kujutuste j ja j' definitsioone kasutades leiame, et

$$\begin{aligned} (jj')(p'(\beta)) = j(j'(p'(\beta))) = j((\hat{\iota}^{-1}(p'))(\alpha)) = (\hat{\iota}(\hat{\iota}^{-1}(p')))(\beta) = \\ = ((\hat{\iota}\hat{\iota}^{-1})(p'))(\beta) = p'(\beta)\,. \end{aligned}$$

Sarnaselt võime veenduda, et ka $(j'j)(p(\alpha)) = p(\alpha)$ suvalise $p(\alpha) \in K(\alpha)$ ($p \in K[x]$, $\deg p < \deg m_\alpha$) korral. Seega, j' on kujutuse j pöördkujutus ning j on seega bijektiivne.

Sellega oleme näidanud, et $j : K(\alpha) \to K'(\beta)$ on isomorfism. Kujutuse j definitsioonist järeldub ühtlasi ka, et $j|_K = \iota$ ning, et $j(\alpha) = \beta$. □

Viimatitoodud teoreem väidab, et teatud tingimustel on võimalik isomorfismi korpuste K ja K' vahel jätkata isomorfismiks korpuste $K(\alpha)$ ja $K'(\beta)$ vahel.

Lause 2.1.21 ja teoreem 2.1.28 kirjeldavad ära kõik algebralised lihtlaiendid polünoomide terminites. Iga lihtlaiend vastab üheselt määratud normeeritud polünoomile ning korpus K ja mingi taandumatu polünoom üle K määravad ära lihtlaiendi.

2.1.2 Laiendi aste

Laiendi astme mõiste toome sisse vektorruumi kaudu. Seda tehes on meie kasutada mitmed lineaaralgebra tulemused, milliseid tulemusi saame rakendada korpuse laiendite uurimisel.

Teoreem 2.1.32. *Olgu $L : K$ korpuse laiend. Siis L on vektorruum üle K tehete*

$$(k, a) \mapsto ka \qquad (k \in K,\, a \in L)\,,$$
$$(a, b) \mapsto a + b \qquad (a,\, b \in L)\,,$$

suhtes.

Tõestus. Vektorruumi aksioomid (vt [5], lk 55-56) on täidetud, sest L, olles korpus, on ühtlasi ka liitmise suhtes Abeli rühm ning kuna K ja L on korpuse $\mathbb{C}$ alamkorpused ja $K \subseteq L$, siis kehtivad ka ülejäänud vektorruumi aksioomid. □

Definitsioon 2.1.33. *Laiendi $L : K$ astmeks* nimetame vektorruumi L üle K mõõdet (ehk dimensiooni). Laiendi $L : K$ astet tähistame $[L : K]$.

Näide 2.1.34. Korpus $\mathbb{C}$ on kahemõõtmeline vektorruum üle $\mathbb{R}$, sest kaheelemendiline hulk $\{1, i\}$ moodustab vektorruumi $\mathbb{C}$ üle $\mathbb{R}$ baasi.

Lause 2.1.35. *Olgu korpuse laiendid $L : K$ ja $L' : K'$ isomorfsed. Siis vektorruumidel L üle K ja L' üle K' on sama mõõde.*

Tõestus. Kui mõlemad vektorruumid L üle K ja L' üle K' on lõpmatumõõtmelised, siis väide kehtib. Oletame nüüd konkreetsuse mõttes, et vektorruum L üle K on lõplikumõõtmeline. Olgu $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ vektorruumi L üle K baas ning olgu $\lambda : K \to K'$ ja $\mu : L \to L'$ korpuste isomorfismid, kusjuures $\mu|_K = \lambda$. Veendume, et $\{\mu(\alpha_1), \mu(\alpha_2), ..., \mu(\alpha_n)\}$ on vektorruumi L' üle K' baas, millest järeldubki, et nende vektorruumide mõõtmed on võrdsed. Olgu $x \in L'$ suvaline. Kuna kujutused λ ja μ on isomorfismid, siis $\exists\, \lambda^{-1} : K' \to K$ ja $\exists\, \mu^{-1} : L' \to L$, mis on seejuures samuti isomorfismid. Paneme veel tähele,

et tingimuse $\mu|_K = \lambda$ tõttu $\mu^{-1}|_{K'} = \lambda^{-1}$. Nüüd $\mu^{-1}(x) \in L$ ning me saame elemendi $\mu^{-1}(x)$ avaldada L baasivektorite kaudu:

$$\mu^{-1}(x) = k_1\alpha_1 + k_2\alpha_2 + \ldots + k_n\alpha_n\,,$$

$k_1, k_2, ..., k_n \in K$. Nüüd aga

$$\begin{aligned} x = \left(\mu\mu^{-1}\right)(x) = \mu\left(\mu^{-1}(x)\right) = \mu(k_1\alpha_1 + k_2\alpha_2 + \ldots + k_n\alpha_n) = \\ = \mu(k_1\alpha_1) + \mu(k_2\alpha_2) + \ldots + \mu(k_n\alpha_n) = \\ = \mu(k_1)\mu(\alpha_1) + \mu(k_2)\mu(\alpha_2) + \ldots + \mu(k_n)\mu(\alpha_n) = \\ = \lambda(k_1)\mu(\alpha_1) + \lambda(k_2)\mu(\alpha_2) + \ldots + \lambda(k_n)\mu(\alpha_n)\,. \end{aligned}$$

Sellega oleme näidanud, et suvaline element $x \in L'$ avaldub elementide $\mu(\alpha_1)$, $\mu(\alpha_2)$, ..., $\mu(\alpha_n)$ lineaarkombinatsioonina üle K'.

Olgu nüüd

$$l_1\mu(\alpha_1) + l_2\mu(\alpha_2) + \ldots + l_n\mu(\alpha_n) = 0$$

elementide $\mu(\alpha_1)$, $\mu(\alpha_2)$, ..., $\mu(\alpha_n)$ mingi nulliga võrduv lineaarkombinatsioon üle K', st, $l_1, l_2, ..., l_n \in K'$. Paneme tähele, et siis

$$\begin{aligned} 0 = \mu^{-1}(0) = \mu^{-1}\left(l_1\mu(\alpha_1) + l_2\mu(\alpha_2) + \ldots + l_n\mu(\alpha_n)\right) = \ldots \\ \ldots = \lambda^{-1}(l_1)\alpha_1 + \lambda^{-1}(l_2)\alpha_2 + \ldots + \lambda^{-1}(l_n)\alpha_n\,, \end{aligned}$$

kusjuures $\lambda^{-1}(l_1), \lambda^{-1}(l_2), ..., \lambda^{-1}(l_n) \in K$. Kuna aga $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ on vektorruumi L üle K baas, siis kujutab viimane võrdus nulliga võrduvat lineaarkombinatsiooni baasivektoritest α_1, α_2, ..., α_n üle K. Seega peab

$$\lambda^{-1}(l_1) = \lambda^{-1}(l_2) = \ldots = \lambda^{-1}(l_n) = 0$$

ning kuna λ^{-1} on isomorfism, siis

$$l_1 = l_2 = \ldots = l_n = 0\,.$$

Sellega oleme näidanud, et elemendid $\mu(\alpha_1)$, $\mu(\alpha_2)$, ..., $\mu(\alpha_n)$ on lineaarselt sõltumatud üle K' ning ühtlasi ka, et $\{\mu(\alpha_1), \mu(\alpha_2), ..., \mu(\alpha_n)\}$ on vektorruumi L' üle K' baas. Seega on vektorruumi L' üle K' mõõde sama, mis vektorruumi L üle K mõõde. □

Järgnev teoreem ja järeldus sellest ütlevad, kuidas arvutada laiendi astet, kui me teame teatud lihtsamate laiendite astmeid.

Teoreem 2.1.36. *Olgu K, L ja M sellised korpused, et $K \subseteq M \subseteq L$. Siis*

$$[L : K] = [L : M][M : K]\,.$$

Tõestus. Olgu $(x_i)_{i\in I}$ vektorruumi M üle K baas ning olgu $(y_j)_{j\in J}$ vektorruumi L üle M baas. Iga $i \in I$ ja iga $j \in J$ korral $x_i \in M$ ja $y_j \in L$. Kuna vektorruumi mõõde on selle vektorruumi baasivektorite hulga võimsus, siis teoreemi tõestamiseks piisab näidata, et $(x_i y_j)_{i\in I,\, j\in J}$ on vektorruumi L üle K baas (siin $x_i y_j$ on korrutis korpuses L), sest sellisel juhul on vektorruumi L üle K baasivektorite hulga võimsus $[L : K]$ võrdne korrutisega $[L : M][M : K]$.

Tõestame algul vektorite $x_i y_j$, $i \in I$, $j \in J$, lineaarse sõltumatuse. Olgu

$$\sum_{i\in I,\, j\in J} k_{ij} x_i y_j = 0$$

vektorite $x_i y_j$, $i \in I$, $j \in J$, mingi lõplik nulliga võrduv lineaarkombinatsioon üle K (st, $k_{ij} \in K$ iga $i \in I$, $j \in J$ korral, kusjuures lõplik arv kordajaid k_{ij} on nullist erinevad). Me võime selle kirjutada kujul

$$\sum_{j\in J} \left(\sum_{i\in I} k_{ij} x_i \right) y_j = 0\,.$$

Paneme tähele, et viimases lineaarkombinatsioonis vektorruumi L üle M baasivektorite y_j ($j \in J$) kordajad $\sum_{i\in I} k_{ij} x_i$ kuuluvad hulka M, mistõttu baasivektorite y_j lineaarse sõltumatuse tõttu iga $j \in J$ korral kehtib

$$\sum_{i\in I} k_{ij} x_i = 0\,.$$

Saadud võrdus kujutab aga iga $j \in J$ korral lineaarkombinatsiooni vektorruumi M üle K baasivektoritest x_i, $i \in I$, mistõttu peab iga $j \in J$ ja iga $i \in I$ korral kehtima $k_{ij} = 0$. Sellega oleme näidanud, et vektorid $x_i y_j$ on lineaarselt sõltumatud üle K.

Näitame nüüd, et $(x_i y_j)_{i\in I,\, j\in J}$ on vektorruumi L üle K moodustajate süsteem. Olgu $x \in L$ suvaline element. Kuna L on vektorruum üle M ning $(y_j)_{j\in J}$ on selle vektorruumi baas, siis

$$x = \sum_{j\in J} \lambda_j y_j \tag{2.7}$$

mingite $\lambda_j \in M$ korral ($j \in J$). Analoogiliselt, kuna M on vektorruum üle K ja $(x_i)_{i\in I}$ on selle vektorruumi baas, siis iga λ_j ($j \in J$) on esitatav kujul

$$\lambda_j = \sum_{i\in I} \lambda_{ij} x_i\,, \tag{2.8}$$

kus $\lambda_{ij} \in K$ ($i \in I$, $j \in J$). Asendades nüüd suurused λ_j, $j \in J$, võrdusest (2.8) võrdusesse (2.7), saame, et kehtib (arvestame, et tegemist on lõplike

summadega, st, lõplik arv kordajaid λ_{ij} on nullist erinevad)

$$x = \sum_{i\in I,\, j\in J} \lambda_{ij} x_i y_j \,,$$

mistõttu $(x_i y_j)_{i\in I,\, j\in J}$ on vektorruumi L üle K moodustajate süsteem.

Sellega oleme näidanud, et $(x_i y_j)_{i\in I,\, j\in J}$ on vektorruumi L üle K baas, mistõttu $[L : K] = [L : M][M : K]$. □

Järeldus 2.1.37. *Olgu K_0, K_1, ..., K_n, sellised korpused, et $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ ($n \in \mathbb{N}$). Siis*

$$[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \ldots [K_1 : K_0] \,. \tag{2.9}$$

Tõestus. Väite tõestame naturaalarvu n järgi matemaatilise induktsiooni meetodit kasutades.

Induktsiooni baas. Olgu $n = 1$. Paneme aga tähele, et sellisel juhul ei ole midagi tõestada.

Induktsiooni samm. Olgu $n > 1$ ning eeldame, et väide kehtib iga naturaalarvu k korral, kus $k < n$.

Teoreemi 2.1.36 põhjal kehtib

$$[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_0] \,. \tag{2.10}$$

Induktsiooni eelduse tõttu

$$[K_{n-1} : K_0] = [K_{n-1} : K_{n-2}] \ldots [K_2 : K_1][K_1 : K_0] \,. \tag{2.11}$$

Asendades suuruse $[K_{n-1} : K_0]$ võrdusest (2.11) võrdusesse (2.10), saamegi järelduse väite. □

Lause 2.1.38. *Olgu $K(\alpha) : K$ algebraline lihtlaiend, mille määrav polünoom on m, kusjuures* $\deg m = n$. *Siis $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ on vektorruumi $K(\alpha)$ üle K baas. Seejuures $[K(\alpha) : K] = n$.*

Tõestus. Teoreemi 2.1.28 põhjal $K(\alpha) \cong K[x]/\langle m\rangle$, kusjuures isomorfismi $\phi : K[x]/\langle m\rangle \to K(\alpha)$ võime nii valida, et $\phi([x]) = \alpha$ ning, et $\phi([k]) = k$ iga $k \in K$ korral.

Olgu nüüd $y \in K(\alpha)$ suvaline element ning olgu $[p] \in K[x]/\langle m\rangle$ elemendi y originaal kujutuse ϕ suhtes. Lause 2.1.24 põhjal võime seejuures eeldada, et klassi $[p]$ esindaja $p \in K[x]$ aste on väiksem kui polünoomil m. Seega, arvestades, kuidas on defineeritud tehted korpuses $K[x]/\langle m\rangle$, ning, et ϕ on isomorfism, saame, et

$$y = \phi([p]) = p(\alpha) \,.$$

Sellega oleme näidanud, et element y esitub elementide 1, α, α^2, ..., α^{n-1} lineaarkombinatsioonina üle K.

Veendume nüüd, et elemendid 1, α, α^2, ..., α^{n-1} on lineaarselt sõltumatud üle K. Selleks olgu

$$k_0 + k_1\alpha + k_2\alpha^2 + \ldots + k_{n-1}\alpha^{n-1} = 0\,,$$

elementide 1, α, α^2, ..., α^{n-1} mingi lineaarkombinatsioon üle K, st, k_0, k_1, k_2, ..., $k_{n-1} \in K$. Kui oletada, et mingi kordaja k_i, $i \in \{0, 1, 2, ..., n-1\}$, on nullist erinev, siis paneme tähele, et α on nullpolünoomist erineva polünoomi $k_0 + k_1x + k_2x^2 + \ldots + k_{n-1}x^{n-1}$ üle K juur. Selle polünoomi mingi korpuse K elemendi kordne on normeeritud, nullpolünoomist erinev, madalama astme polünoom kui m ning omab juurt α. See on aga vastuolus asjaoluga, et m on elemendi α minimaalne polünoom üle K. Seega peavad kõik kordajad k_i, $i \in \{0, 1, 2, ..., n-1\}$, olema nullid ning elemendid 1, α, α^2, ..., α^{n-1} on seega lineaarselt sõltumatud üle K.

Sellega oleme põhjendanud, et 1, α, α^2, ..., α^{n-1} on vektorruumi $K(\alpha)$ üle K baas. Kuna baasivektoreid on n tükki, siis $[K(\alpha) : K] = n$. □

Lause 2.1.39. *Olgu $K(\alpha) : K$ lihtlaiend. Kui see laiend on transtsendentne, siis $[K(\alpha) : K] = \infty$. Kui see laiend on algebraline, siis $[K(\alpha) : K] = \deg m$, kus m on vaadeldava laiendi määrav polünoom.*

Tõestus. Paneme tähele, et kui vaadeldav lihtlaiend on transtsendentne, siis elemendid $1, \alpha, \alpha^2, ...$ on lineaarselt sõltumatud üle K. Seega ei saa vektorruum $K(\alpha)$ üle K olla lõplikumõõtmeline.

Kui vaadeldav lihtlaiend on algebraline, siis järeldub lause väide vahetult lausest 2.1.38. □

Näide 2.1.40.

1. Leiame näitena lihtlaiendi $\mathbb{Q}(c) : \mathbb{Q}$, kus $c = \sqrt[3]{2} \in \mathbb{R}$, astme. Element c rahuldab võrrandit $x^3 - 2 = 0$, mistõttu vaadeldav lihtlaiend on algebraline. Polünoom $x^3 - 2$ on Eisensteini kriteeriumi (vt [2], lk 248, teoreem 2, kus on see kriteerium Eisensteini teoreemina sõnastatud) põhjal taandumatu üle $\mathbb{Q}$, mistõttu kujutab vaadeldav polünoom lause 2.1.20 põhjal laiendi $\mathbb{Q}(c) : \mathbb{Q}$ määravat polünoomi. Kuna selle polünoomi aste on 3, siis lause 2.1.38 põhjal $[\mathbb{Q}(c) : \mathbb{Q}] = 3$. Seejuures korpuse $\mathbb{Q}(c)$ iga element esitub kujul $p + qc + rc^2$, kus p, q, $r \in \mathbb{Q}$.

2. Leiame laiendi $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$ astme. Teoreemi 2.1.36 põhjal

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]\,.$$

Lihtlaiendi $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ aste on lause 2.1.39 põhjal 2, sest tema määravaks polünoomiks on x^2-2 üle $\mathbb{Q}$ (vaadeldav polünoom on taandumatu üle $\mathbb{Q}$, sest $\sqrt{2}$ ei ole ratsionaalarv). Lihtlaiendi $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})$ aste on samuti 2, sest polünoom $x^2 + 1$ on taandumatu üle $\mathbb{Q}(\sqrt{2})$ (vastasel korral peaks $i \in \mathbb{Q}(\sqrt{2})$), kujutades seega laiendi $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})$ määravat polünoomi. Seega on laiendi $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$ aste 4. Kuna $\left\{1, \sqrt{2}\right\}$ on lause 2.1.38 põhjal vektorruumi $\mathbb{Q}(\sqrt{2})$ üle $\mathbb{Q}$ ning $\{1, i\}$ on sama lause põhjal vektorruumi $\mathbb{Q}(\sqrt{2}, i)$ üle $\mathbb{Q}(\sqrt{2})$ baas, siis teoreemi 2.1.36 tõestuskäigu põhjal on $\left\{1, \sqrt{2}, i, \sqrt{2}i\right\}$ vektorruumi $\mathbb{Q}(\sqrt{2}, i)$ üle $\mathbb{Q}$ baas. Laiendi $\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$ iga element esitub seega üheselt kujul $p + q\sqrt{2} + ri + s\sqrt{2}i$, kus $p, q, r, s \in \mathbb{Q}$.

Definitsioon 2.1.41. Korpuse laiendit $L : K$ nimetame *lõplikuks laiendiks*, kui tema aste on lõplik.

Definitsioon 2.1.42. Korpuse laiendit $L : K$ nimetame *algebraliseks laiendiks*, kui korpuse L iga element on algebraline üle K.

Lause 2.1.43. *Olgu korpuse laiend $L : K$ lõplik ning olgu M ja N, $M \subseteq N$, mingid korpused korpuste K ja L vahel (st, $K \subseteq M \subseteq N \subseteq L$). Siis ka laiend $N : M$ on lõplik.*

Tõestus. Järelduse 2.1.37 põhjal $[L : K] = [L : N][N : M][M : K]$ ning sellest võrdusest järeldub vahetult laiendi $N : M$ lõplikkus. □

Lausest 2.1.39 järeldub, et iga algebraline lihtlaiend on lõplik. Millistel tingimustel on algebraline laiend lõplik, sellele annab vastuse järgnev lause.

Lause 2.1.44. *Kopruse laiend $L : K$ on lõplik laiend siis ja ainult siis kui $L : K$ on algebraline laiend ning leidub lõplik arv selliseid elemente $\alpha_1, \alpha_2, ..., \alpha_s \in L$, et $L = K(\alpha_1, \alpha_2, ..., \alpha_s)$.*

Tõestus. Tarvilikkus. Eeldame, et laiend $L : K$ on lõplik. Siis vektorruum L üle K on lõplikumõõtmeline. Olgu $\{\alpha_1, \alpha_2, ..., \alpha_s\}$ tema baasiks. Siis aga kehtib võrdus $L = K(\alpha_1, \alpha_2, ..., \alpha_s)$. Jääb veel näidata, et $L : K$ on algebraline laiend. Olgu $x \in L$ suvaline. Paneme tähele, et hulk $\{1, x, x^2, ..., x^s\}$ sisaldab $s+1$ elementi, mistõttu on need elemendid lineaarselt sõltuvad üle K. Seega, meil leiduvad elemendid $k_0, k_1, k_2, ..., k_s \in K$, mis ei ole kõik korraga nullid, nii, et kehtib

$$k_0 + k_1 x + k_2 x^2 + \ldots + k_s x^s = 0\,.$$

See aga tähendab, et element x on algebraline üle K (vt definitsioon 2.1.14).

Piisavus. Eeldame, et leidub lõplik arv selliseid elemente $\alpha_1, \alpha_2, ..., \alpha_s \in L$, et $L = K(\alpha_1, \alpha_2, ..., \alpha_s)$. Lause 2.1.10 ja järelduse 2.1.37 põhjal kehtib

$$\begin{aligned}[L : K] = [K(\alpha_1, \alpha_2, \ldots, \alpha_s) : K] = \\ = [K(\alpha_1, \alpha_2, \ldots, \alpha_{s-1})(\alpha_s) : K(\alpha_1, \alpha_2, \ldots, \alpha_{s-1})] \cdot \\ \cdot [K(\alpha_1, \alpha_2, \ldots, \alpha_{s-2})(\alpha_{s-1}) : K(\alpha_1, \alpha_2, \ldots, \alpha_{s-2})] \cdot \\ \cdot \ldots \cdot \\ \cdot [K(\alpha_1)(\alpha_2) : K(\alpha_1)] \cdot [K(\alpha_1) : K] \,. \quad (2.12)\end{aligned}$$

Kuna elemendid $\alpha_1, \alpha_2, ..., \alpha_s \in L$ on algebralised üle K, siis on kõik laiendid

$$\begin{gathered}K(\alpha_1, \alpha_2, \ldots, \alpha_{s-1})(\alpha_s) : K(\alpha_1, \alpha_2, \ldots, \alpha_{s-1}) \,, \\ K(\alpha_1, \alpha_2, \ldots, \alpha_{s-2})(\alpha_{s-1}) : K(\alpha_1, \alpha_2, \ldots, \alpha_{s-2}) \,, \\ \ldots \,, \\ K(\alpha_1)(\alpha_2) : K(\alpha_1) \,, \\ K(\alpha_1) : K\end{gathered}$$

algebralised lihtlaiendid ning on lause 2.1.39 tõttu lõplikud. Võrduse (2.12) tõttu on seega ka laiendi $L : K$ aste $[L : K]$ lõplik arv. □

Järeldus 2.1.45. *Kui laiend $L : K$ on lõplik, siis korpuse L suvaline element x on esitatav kujul*

$$x = p(\alpha_1, \alpha_2, \ldots, \alpha_s) \,,$$

kus p on mingi s muutuja polünoom üle K ning $\alpha_1, \alpha_2, ..., \alpha_s \in L$ on sellised elemendid, et $L = K(\alpha_1, \alpha_2, ..., \alpha_s)$.

Tõestus. Lause 2.1.44 põhjal leiduvad elemendid $\alpha_1, \alpha_2, ..., \alpha_s \in L$ selliselt, et $L = K(\alpha_1, \alpha_2, ..., \alpha_s)$. Sama lause põhjal on $L : K$ algebraline laiend. Tõestame väite matemaatilise induktsiooni meetodit kasutades elementide arvu s järgi.

Induktsiooni baas. Olgu $s = 1$. Siis $L = K(\alpha_1)$ ning $L : K$ on seega algebraline lihtlaiend. Lause 2.1.38 põhjal siis suvaline element $x \in L$ on esitatav kujul

$$x = p(\alpha_1) \,,$$

kus p on mingi ühe muutuja polünoom üle K.

Induktsiooni samm. Olgu nüüd $s > 1$ ning eeldame, et väide kehtib juhul kui $L : K$ on selline lõplik laiend, et $L = K(\alpha_1, \alpha_2, ..., \alpha_k)$, kus $k < s$. Lause 2.1.10 põhjal

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_s) = K(\alpha_1, \alpha_2, \ldots, \alpha_{s-1})(\alpha_s) \,.$$

Nüüd, laiend $L : K(\alpha_1, \alpha_2, ..., \alpha_{s-1})$ on algebraline lihtlaiend. Lause 2.1.38 põhjal siis suvaline element $x \in L$ on esitatav kujul

$$x = p_1(\alpha_s)\,,$$

kus p_1 on mingi ühe muutuja polünoom üle $K(\alpha_1, \alpha_2, ..., \alpha_{s-1})$. Induktsiooni eelduse tõttu on polünoomi p_1 kordajad a_i korpusest $K(\alpha_1, \alpha_2, ..., \alpha_{s-1})$ esitatavad kujul

$$a_i = q_i(\alpha_1, \alpha_2, \ldots, \alpha_{s-1})\,,$$

kus q_i on teatud $(s-1)$-muutuja polünoom üle K $(i \in 0, 1, 2, ..., \deg p_1)$. Siis aga saamegi, et

$$x = p(\alpha_1, \alpha_2, \ldots, \alpha_s)\,,$$

kus p on teatud s muutuja polünoom üle K. □

2.2 Polünoomi lahutuskorpus

Teatavasti saame iga kompleksarvuliste kordajatega polünoomi esitada teatavate esimese astme polünoomide korrutisena. Seega omab mõtet järgnev definitsioon.

Definitsioon 2.2.1. Olgu K korpus ning f polünoom üle K. Ütleme, et *polünoom f lahutub lineaartegurite korrutiseks üle korpuse K* kui ta on esitatav kujul

$$f(x) = k(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)\,,$$

kus $k, \alpha_1, \alpha_2, \ldots, \alpha_n \in K$.

Märgime, et viimases definitsioonis mainitud lineaartegurite all me peame silmas 1. astme polünoome $x - \alpha_1$, $x - \alpha_2$, ..., $x - \alpha_n$.

Kui f on polünoom üle korpuse K ning $L : K$ on korpuse laiend, siis polünoom f on ühtaegu ka polünoom üle korpuse L. Seega on mõtet rääkida, et f lahutub lineaartegurite korrutiseks üle korpuse L, mõeldes selle all, et f lahutub 1. astme polünoomide korrutiseks, milliste polünoomide kordajad kuuluvad korpusesse L. Meid huvitab sisalduvuse mõttes niiöelda "vähim" korpus, üle mille f lahutub lineaartegurite korrutiseks.

Definitsioon 2.2.2. Olgu f polünoom üle korpuse K. Korpust Σ nimetame *polünoomi f lahutuskorpuseks üle korpuse K* kui $K \subseteq \Sigma$ ning

1. f lahutub lineaartegurite korrutiseks üle Σ,
2. kui $K \subseteq \Sigma' \subseteq \Sigma$ ning kui f lahutub lineaartegurite korrutiseks üle Σ', siis $\Sigma' = \Sigma$.

Kui kontekstist on korpuse K roll selge, siis polünoomi f lahutuskorpust üle K nimetame ka lihtsalt polünoomi f lahutuskorpuseks.

Lause 2.2.3. *Olgu f polünoom üle korpuse K ning olgu Σ polünoomi f lahutuskorpus. Siis*

$$\Sigma = K(\alpha_1, \alpha_2, \ldots, \alpha_n)\,,$$

kus α_1, α_2, ..., α_n on polünoomi f kõik juured.

Tõestus. Definitsioonist 2.2.1 järeldub, et f lahutub lineaartegurite korrutiseks üle korpuse $K(\alpha_1, \alpha_2, ..., \alpha_n)$. Paneme tähele, et iga korpus, üle mille f lahutub lineaartegurite korrutiseks, peab sisaldama f kõiki juuri α_1, α_2, ..., α_n. Seega, kuna f lahutub lineaartegurite korrutiseks üle Σ, siis $\alpha_1, \alpha_2, ..., \alpha_n \in \Sigma$. Kuna ka lisaks $K \subseteq \Sigma$, siis $K(\alpha_1, \alpha_2, ..., \alpha_n) \subseteq \Sigma$. Nüüd aga definitsiooni 2.2.2 põhjal saame, et $\Sigma = K(\alpha_1, \alpha_2, ..., \alpha_n)$. □

Leiame nüüd lahutuskorpuse ühele konkreetsele polünoomile.

Näide 2.2.4. Olgu $f(x) = (x^2-2x-2)(x^2+1)$ polünoom üle $\mathbb{Q}$. Vaadeldava polünoomi juured korpuses $\mathbb{C}$ on $1+\sqrt{3}$, $1-\sqrt{3}$, i, $-i$, mistõttu lause 2.2.3 põhjal on f lahutuskorpuseks korpus $\mathbb{Q}(1+\sqrt{3}, 1-\sqrt{3}, i, -i)$, mis ühtib korpusega $\mathbb{Q}(\sqrt{3}, i)$.

Olles sidunud polünoomiga tema lahutuskorpuse, toome nüüd siinkohas paar olulist tulemust polünoomide kohta.

Lause 2.2.5. *Olgu f polünoom üle korpuse K, kusjuures* $\deg f > 0$. *Siis polünoomil f leidub juur korpuses $\mathbb{C}$, mille kordsus on suurem kui* 1, *siis ja ainult siis kui polünoom f ja tema tuletis*[2] *f' ei ole ühistegurita ringis $K[x]$ (st,* $\deg(f, f') > 0$).

Tõestus. Tarvilikkus. Olgu Σ polünoomi f lahutuskorpus ning olgu $\alpha \in \Sigma$ polünoomi f k-kordne juur, $k > 1$. Siis polünoomina üle Σ on f esitatav kujul

$$f = (x-\alpha)^k\, g\,, \tag{2.13}$$

kus $k > 1$ ning g on mingi polünoom üle Σ. Siis aga, polünoomi f tuletis f' on

$$f' = (x-\alpha)^{k-1}\left[(x-\alpha)g' + kg\right]\,. \tag{2.14}$$

Kuna $k-1 > 0$, siis järeldub võrdustest (2.13) ja (2.14), et $(x-\alpha) \mid f$ ning $(x-\alpha) \mid f'$ (ringis $\Sigma[x]$), mis tähendab, et α on nii polünoomi f kui ka polünoomi f' juur. Nüüd lause 2.1.20 põhjal jagab elemendi α minimaalne polünoom üle K nii polünoomi f kui ka polünoomi f' (ringis $K[x]$). Seega ei saa f ja f' olla ühistegurita ringis $K[x]$.

[2]Polünoomi f tuletis f' on funktsiooni $f = f(x)$ tuletis, mis on polünoom üle K.

Piisavus. Oletame vastuväiteliselt, et polünoomil f puuduvad kordsed juured korpuses Σ. Näitame matemaatilise induktsiooni meetodit kasutades polünoomi f astme järgi, et sellisel juhul polünoomidel f ja f' ei saa leiduda ühist tegurit. St, näitame, et f ja f' on sellisel juhul ühistegurita ringis $\Sigma[x]$ (või ringis $\mathbb{C}[x]$) ning seega ühistegurita ka ringis $K[x]$.

Induktsiooni baas. Kui $\deg f = 1$, siis $\deg f' = 0$, mis tähendab, et f' on korpuse K element ning f ja f' on seega ühistegurita.

Induktsiooni samm. Eeldame, et iga polünoomi f korral üle K, mille aste on väiksem kui k, $k \geq 2$, ning millel puuduvad kordsed juured korpuses $\mathbb{C}$, on f ja tema tuletis f' ühistegurita ringis $\mathbb{C}[x]$. Olgu

$$f = (x - \alpha)g\,, \tag{2.15}$$

kus $(x - \alpha) \nmid g$ (st, juure α kordsus on 1) ning $\deg f = k$. Sellisel juhul $\deg g = k - 1$ ning me võime polünoomi g jaoks ära kasutada induktsiooni eeldust. Paneme tähele, et

$$f' = (x - \alpha)g' + g\,. \tag{2.16}$$

Nüüd võrdustest (2.15) ja (2.16) ilmneb, et polünoomide f ja f' ühised tegurid saavad olla vaid polünoomi g tegurid, sest meie eelduse $(x - \alpha) \nmid g$ tõttu $(x - \alpha) \nmid f'$.

Kui nüüd leiduks taandumatu polünoom d üle Σ nii, et $d \mid g$, $d \mid f'$ ja $\deg d > 0$, siis võrdusest (2.16) järeldub, et ka $d \mid (x - \alpha)g'$. Kuna d on taandumatu üle Σ, siis kas $d \mid (x - \alpha)$ või $d \mid g'$ (vt [2], lk 212, omadus 2)).

Kui kehtiks $d \mid (x - \alpha)$, siis $\deg d = 1$ (sest $\deg d > 0$) ning seepärast ka $(x - \alpha) \mid d$. See aga tähendaks, et $(x - \alpha) \mid g$ (sest $(x - \alpha) \mid d$ ja $d \mid g$ ning seetõttu ka $(x - \alpha) \mid g$), mis on vastuolus meie eeldusega, et $(x - \alpha) \nmid g$.

Seega peab $d \mid g'$. Paneme aga tähele, et induktsiooni eelduse põhjal on polünoomid g ja g' ühistegurita, mistõttu ei saa see kehtida.

Sellega oleme põhjendanud, et polünoomi g ükski tegur ei saa olla polünoomi f' teguriks ning polünoomid f ja f' peavad seega olema ühistegurita. □

Järeldus 2.2.6. *Olgu K korpus ning olgu f taandumatu polünoom üle K. Siis polünoomi f juured on kõik ühekordsed. Teisisõnu, üle oma lahutuskorpuse või üle korpuse $\mathbb{C}$, on f esitatav kujul*

$$f = k(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)\,, \tag{2.17}$$

kus elemendid α_j, $j \in \{1, 2, ..., n\}$, on paarikaupa erinevad.

Tõestus. Kui polünoomi f mingi juure kordsus oleks suurem kui 1, siis oleks f vähemalt 2. astme polünoom ning lause 2.2.5 põhjal ei oleks polünoomid f üle K ja f' üle K ühistegurita. See on aga vastuoluline, sest f on taandumatu üle K. □

2.2.1 Lahutuskorpuse ühesus

Uurime nüüd polünoomi lahutuskorpuse ühesusega seotud küsimusi.

Teoreem 2.2.7. *Olgu K korpus ning f polünoom üle K. Siis polünoomi f lahutuskorpus Σ on üheselt määratud ning laiendi $\Sigma : K$ aste on lõplik.*

Tõestus. Olgu α_1, α_2, ..., α_n polünoomi f kõik juured. Kui Σ on polünoomi f lahutuskorpus üle K, siis lause 2.2.3 põhjal $\Sigma = K(\alpha_1, \alpha_2, ..., \alpha_n)$. Seega f lahutuskorpus on üheselt määratud.

Järelduse 2.1.37 ja lause 2.1.10 põhjal

$$\begin{aligned}[\Sigma : K] = [K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n) : K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})]\cdot \\ \cdot [K(\alpha_1, \alpha_2, \ldots, \alpha_{n-2})(\alpha_{n-1}) : K(\alpha_1, \alpha_2, \ldots, \alpha_{n-2})] \cdot \ldots \\ \ldots \cdot [K(\alpha_1)(\alpha_2) : K(\alpha_1)] \cdot [K(\alpha_1) : K]\,. \quad (2.18)\end{aligned}$$

Paneme tähele, et laiendid

$$\begin{gathered}K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})(\alpha_n) : K(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})\,, \\ K(\alpha_1, \alpha_2, \ldots, \alpha_{n-2})(\alpha_{n-1}) : K(\alpha_1, \alpha_2, \ldots, \alpha_{n-2})\,, \\ \ldots\,, \\ K(\alpha_1)(\alpha_2) : K(\alpha_1)\,, \\ K(\alpha_1) : K\end{gathered}$$

on kõik algebralised lihtlaiendid. Lause 2.1.39 põhjal on nende astmed lõplikud. Siis aga võrduse (2.18) tõttu on ka laiendi $\Sigma : K$ aste lõplik. □

Lause 2.2.8. *Olgu $\iota : K \to K'$ korpuste K ja K' isomorfism. Olgu f polünoom üle K ning olgu Σ polünoomi f lahutuskorpus. Olgu $L' : K'$ mistahes korpuse laiend, mille korral polünoom $\hat{\iota}\,(f)$* (lause 2.1.30 tähistustes) *lahutub lineaartegurite korrutiseks üle L'. Siis leidub selline monomorfism $j : \Sigma \to L'$, et $j|_K = \iota$.*

Tõestus. Piltlikult väljendades on olukord järgnev

$$\begin{array}{ccc} K & \to & \Sigma \\ \iota\downarrow & & \downarrow j \\ K' & \to & L' \end{array}\,,$$

kus monomorfism j tuleb leida. Tõestame väite matemaatilise induktsiooni meetodit kasutades polünoomi f astme $\deg f$ järgi.

Induktsiooni baas. Induktsiooni baasi tõestame juhul kui f on 1. astme polünoom üle korpuse K. Paneme tähele, et sellisel juhul $K = \Sigma$ ning monomorfismiks j võtame ι.

Induktsiooni samm. Eeldame nüüd, et väide kehtib kõikide polünoomide jaoks üle korpuse K, mille aste on väiksem kui n ($n > 1$). Olgu f mingi n-astme polünoom üle K. Polünoomina üle lahutuskorpuse Σ võime f kirjutada kujul

$$f = k(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)\,.$$

Olgu m elemendi α_1 minimaalne polünoom üle K. Lause 2.1.20 põhjal $f = qm$, kus q on mingi polünoom üle K. Kuna $\hat{\iota} : K[x] \to K'[x]$ on lause 2.1.30 tõttu isomorfism, siis

$$\hat{\iota}\,(f) = \hat{\iota}\,(qm) = \hat{\iota}\,(q)\,\hat{\iota}\,(m)\ , \tag{2.19}$$

mis tähendab, et polünoom $\hat{\iota}\,(m)$ jagab polünoomi $\hat{\iota}\,(f)$. Polünoom $\hat{\iota}\,(f)$ lahutub aga eelduse tõttu lineaartegurite korrutiseks üle L'. Võrduse (2.19) tõttu lahutub seega ka polünoom $\hat{\iota}\,(m)$ lineaartegurite korrutiseks üle L', st,

$$\hat{\iota}\,(m) = (x - \beta_1)(x - \beta_2)\dots(x - \beta_r)\,,$$

kus $\beta_1, \beta_2, ..., \beta_r \in L'$. Kuna $K[x] \cong K'[x]$ ning polünoom m on taandumatu üle K, siis on $\hat{\iota}\,(m)$ taandumatu üle K'. Seega on $\hat{\iota}\,(m)$ elemendi β_1 minimaalne polünoom üle K'. Teoreemi 2.1.31 põhjal leidub isomorfism

$$j_1 : K(\alpha_1) \to K'(\beta_1)\,,$$

kusjuures $j_1|_K = \iota$ ning $j_1(\alpha_1) = \beta_1$. Paneme tähele, et Σ on polünoomi $g = \frac{f}{x-\alpha_1}$ lahutuskorpus üle $K(\alpha_1)$ ning, et polünoom $\hat{j_1}\,(g) = \frac{\hat{j_1}(f)}{x-\beta_1}$ (üle $K'(\beta_1)$) lahutub lineaartegurite korrutiseks üle L'. Induktsiooni eelduse tõttu leidub nüüd monomorfism $j : \Sigma \to L'$ nii, et $j|_{K(\alpha_1)} = j_1$. Kuid sellisel juhul $j|_K = \iota$ ning väide on tõestatud. □

Teoreem 2.2.9. *Olgu $\iota : K \to K'$ korpuste K ja K' isomorfism. Olgu Σ polünoomi f lahutuskorpus üle K ning olgu Σ' polünoomi $\hat{\iota}\,(f)$ (lause* 2.1.30 *tähistuses) lahutuskorpus üle K'. Siis leidub isomorfism $j : \Sigma \to \Sigma'$ nii, et $j|_K = \iota$. Teisisõnu, laiendid $\Sigma : K$ ja $\Sigma' : K'$ on isomorfsed.*

Tõestus. Olukord on meil seekord järgnev

$$\begin{array}{ccc} K & \to & \Sigma \\ \iota\downarrow & & \downarrow j \\ K' & \to & \Sigma' \end{array}\ ,$$

kus nõutud tingimusi rahuldav isomorfism j tuleb leida. Kuna Σ on polünoomi f lahutuskorpus, siis polünoomina üle Σ võime f kirjutada kujul

$$f = k(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)\,.$$

Lause 2.2.8 põhjal leidub monomorfism $j : \Sigma \to \Sigma'$ nii, et $j|_K = \iota$. Seega, kuna kujutus $\hat{j} : \Sigma[x] \to j(\Sigma)[x]$ on lause 2.1.30 põhjal isomorfism, kehtib

$$\hat{\iota}(f) = \hat{j}(f) = \hat{j}(k)\hat{j}(x-\alpha_1)\hat{j}(x-\alpha_2)\dots\hat{j}(x-\alpha_n) = \\ = j(k)(x-j(\alpha_1))(x-j(\alpha_2))\dots(x-j(\alpha_n)).$$

Seega, polünoom $\hat{\iota}(f)$ lahutub lineaartegurite korrutiseks üle korpuse $j(\Sigma)$. Paneme ka tähele, et $K' \subseteq j(\Sigma) \subseteq \Sigma'$. Seega, definitsiooni 2.2.2 põhjal, $j(\Sigma) = \Sigma'$. See aga tähendab seda, et kujutus j on pealekujutus ning ühtlasi ka isomorfism. □

2.2.2 Normaalkorpus

Definitsioon 2.2.10. Korpuse laiendit $L : K$ nimetame *normaalseks* kui iga taandumatu polünoom üle K, mille juurtest vähemalt üks kuulub korpusesse L, lahutub lineaartegurite korrutiseks üle korpuse L. Korpust L nimetame sellisel juhul *normaalkorpuseks* (*korpuse K suhtes*).

Näide 2.2.11.

1. Laiend $\mathbb{C} : \mathbb{Q}$ on normaalne, sest algebra põhiteoreemi (vt [5], lk 232, teoreem 7.4.5) põhjal mistahes kompleksarvuliste kordajatega (ning seega ka ratsionaalarvuliste kordajatega) n-astme polünoomi f kõik n kompleksarvulist juurt kuuluvad korpusesse $\mathbb{C}$ (n on suvaline naturaalarv).

2. Laiend $\mathbb{Q}(c) : \mathbb{Q}$, kus $c = \sqrt[3]{2} \in \mathbb{R}$, aga ei ole normaalne. Polünoomi $x^3 - 2$ juur $\sqrt[3]{2} \in \mathbb{R}$ kuulub korpusesse $\mathbb{Q}(c)$. Vaadeldava polünoomi teised juured korpuses $\mathbb{C}$ on aga komplekssed ning ei kuulu seetõttu korpusesse $\mathbb{Q}(c)$. Seega laiend $\mathbb{Q}(c) : \mathbb{Q}$ ei ole tõepoolest normaalne.

Teoreem 2.2.12. *Korpuse laiend $L : K$ on normaalne ja lõplik siis ja ainult siis kui L on mingi polünoomi lahutuskorpus üle K.*

Tõestus. Tarvilikkus. Olgu laiend $L : K$ normaalne ja lõplik. Lause 2.1.44 põhjal siis $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$, kus elemendid α_1, α_2, ..., α_n on algebralised üle K. Olgu m_j elemendi α_j, $j \in \{1, 2, ..., n\}$, minimaalne polünoom üle K ning olgu $f = m_1 m_2 ... m_n$. Polünoomid m_j, $j \in \{1, 2, ..., n\}$, on taandumatud üle K ning α_j on polünoomi m_j juur. Kuna L on normaalkorpus K suhtes, siis polünoomid m_j, $j \in \{1, 2, ..., n\}$, lahutuvad lineaartegurite korrutiseks üle L, st, L sisaldab polünoomi f kõiki juuri β_1, β_2, ..., β_s. Lause 2.2.3 põhjal on $L = K(\beta_1, \beta_2, ..., \beta_s)$ seega polünoomi f lahutuskorpus.

Piisavus. Olgu L lahutuskorpuseks mingile polünoomile g üle korpuse K. Teoreemi 2.2.7 põhjal on laiendi $L : K$ aste lõplik. Näitame nüüd, et L on normaalkorpus K suhtes.

Olgu f mingi taandumatu polünoom üle K, mille juur θ_1 kuulub korpusesse L. Näitamaks, et L on normaalkorpus, tuleb meil definitsiooni 2.2.10 tõttu näidata, et f lahutub lineaartegurite korrutiseks üle korpuse L.

Olgu θ_2 polünoomi f suvaline juur. Üldisust kitsendamata võime seejuures eeldada, et f on normeeritud. Kuna f on taandumatu üle K, siis on f seega elementide θ_1 ja θ_2 minimaalne polünoom üle K.

Näitame, et

$$[L(\theta_1) : L] = [L(\theta_2) : L]\,. \tag{2.20}$$

Paneme tähele, et kehtivad järgnevad sisalduvused:

$$K \subseteq L \subseteq L(\theta_j)\,,$$
$$K \subseteq K(\theta_j) \subseteq L(\theta_j)\,,$$

kus $j \in \{1, 2\}$. Nüüd teoreemi 2.1.36 kasutades saame, et $j \in \{1, 2\}$ korral

$$[L(\theta_j) : L][L : K] = [L(\theta_j) : K] = [L(\theta_j) : K(\theta_j)][K(\theta_j) : K]\,. \tag{2.21}$$

Kuna f on laiendite $K(\theta_1) : K$ ja $K(\theta_2) : K$ määrav polünoom, siis lause 2.1.38 põhjal

$$[K(\theta_1) : K] = [K(\theta_2) : K]\,. \tag{2.22}$$

Paneme tähele, et kuna L on polünoomi g lahutuskorpus üle K, siis $L(\theta_j)$ on g lahutuskorpus üle $K(\theta_j)$, $j \in \{1, 2\}$. Lisaks paneme tähele, et järelduse 2.1.29 põhjal $K(\theta_1) \cong K(\theta_2)$. Seega, teoreemi 2.2.9 põhjal on laiendid $L(\theta_1) : K(\theta_1)$ ja $L(\theta_2) : K(\theta_2)$ isomorfsed ning lause 2.1.35 tõttu kehtib

$$[L(\theta_1) : K(\theta_1)] = [L(\theta_2) : K(\theta_2)]\,. \tag{2.23}$$

Nüüd aga saadud võrduste (2.21), (2.22) ja (2.23) põhjal

$$\begin{aligned}[L(\theta_1) : L][L : K] &= [L(\theta_1) : K(\theta_1)][K(\theta_1) : K] = \\ &= [L(\theta_2) : K(\theta_2)][K(\theta_2) : K] = [L(\theta_2) : L][L : K]\,,\end{aligned}$$

millest järeldubki, et kehtib võrdus (2.20).

Kuna polünoomi f juur θ_1 kuulub korpusesse L, siis $L(\theta_1) = L$ ning seega $[L(\theta_1) : L] = 1$. Polünoomi f teise juure θ_2 korral võrduse (2.20) põhjal siis ka $[L(\theta_2) : L] = 1$. See aga tähendab seda, et $\theta_2 \in L$. Kuna aga θ_2 oli polünoomi f suvaline juur, siis peavad f kõik juured sellisel juhul kuuluma korpusesse L.

Sellega oleme näidanud, et f lahutub lineaartegurite korrutiseks üle korpuse L ning laiend $L : K$ on seega normaalne. □

Kui korpus L on mingi polünoomi lahutuskorpus üle korpuse K, siis teoreemi 2.2.12 põhjal iga taandumatu polünoomi f korral üle K on kaks võimalust:

1. f lahutub lineaartegurite korrutiseks üle L.
2. f on taandumatu üle L.

2.3 Ülesanded

11. Tõestada, et seos "korpuse laiendid (K_1, L_1) ja (K_2, L_2) on isomorfsed" on ekvivalentsiseos.

12. Tõestada, et elemendid 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ on lineaarselt sõltumatud üle $\mathbb{Q}$. (Näpunäide: Oletame vastuväiteliselt, et $p+q\sqrt{2}+r\sqrt{3}+s\sqrt{6}=0$, kus ratsionaalarvud p, q, r ja s ei ole kõik korraga nullid. Näidata, et me võime sel juhul eeldada, et $s \neq 0$. Näidata seejärel, et siis

$$\sqrt{3} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = e + f\sqrt{2}\,,$$

kus $a, b, c, d, e, f \in \mathbb{Q}$. Lõpuks, näidata, et viimase võrduse ruutu tõstmisel saame vastuolu.)

13. Leida hulga $\mathbb{C}$ järgmiste alamhulkade poolt tekitatud korpused.

    a. $\{0, 1\}$.
    b. $\{0\}$.
    c. $\{0, 1, i\}$.
    d. $\{i, \sqrt{5}\}$.
    e. $\{\sqrt{2}, \sqrt{3}\}$. (Näpunäide: Kasutada ülesannet 12.)
    f. $\mathbb{R}$.
    g. $\mathbb{R} \cup \{i\}$.

14. Kas laiend $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ on lihtne? Põhjendada.

15. Leida järgmiste elementide minimaalsed polünoomid järgmiste laiendite korral.

    a. i, $\mathbb{C} : \mathbb{Q}$.
    b. $\left(\sqrt{2}+1\right)/2$, $\mathbb{C} : \mathbb{Q}$.
    c. $\left(i\sqrt{2}-1\right)/2$, $\mathbb{C} : \mathbb{Q}$.

16. Näidata, et kui elemendi α minimaalne polünoom on $x^2 - 2$ üle $\mathbb{Q}$ ning elemendi β minimaalne polünoom on $x^2 - 4x + 2$ üle $\mathbb{Q}$, siis laiendid $\mathbb{Q}(\alpha) : \mathbb{Q}$ ja $\mathbb{Q}(\beta) : \mathbb{Q}$ on isomorfsed.

17. Milliste järgnevate polünoomide m ja vastavate korpuste K korral leidub $\alpha \in \mathbb{C}$, et laiendi $K(\alpha) : K$ määravaks polünoomiks oleks m?

    a. $m = x^2 - 4$, $K = \mathbb{R}$.

    b. $m = x^2 - 3$, $K = \mathbb{R}$.

    c. $m = x^2 - 3$, $K = \mathbb{Q}$.

    d. $m = x^7 - 3x^6 + 4x^3 - x - 1$, $K = \mathbb{R}$.

18. Tõestada, et korpuse laiend $L : K$ on lõplik siis ja ainult siis kui leidub lõplik arv selliseid algebralisi elemente α_1, α_2, ..., α_s üle K, et $L = K(\alpha_1, \alpha_2, ..., \alpha_s)$.

19. Olgu $L : K$ lõplik korpuse laiend. Näidata, et korrutamine fikseeritud elemendiga korpusest L defineerib lineaarteisenduse vektorruumil L üle K. Millal on see lineaarteisendus mittesingulaarne? (St, millal on selle lineaarteisenduse maatriksi determinant nullist erinev?)

20. Olgu $L : K$ lõplik korpuse laiend ning olgu p taandumatu polünoom üle K, mille aste on vähemalt 2. Näidata, et kui arvud $\deg p$ ja $[L : K]$ on ühisteguriteta, siis polünoomi p ükski juur ei kuulu korpusesse L.

21. Leida lihtlaiendi $\mathbb{Q}\left(\sqrt{1+\sqrt{3}}\right) : \mathbb{Q}$ määrav polünoom ning ühtlasi ka vektorruumi $\mathbb{Q}\left(\sqrt{1+\sqrt{3}}\right)$ üle $\mathbb{Q}$ baas ja mõõde. (Näpunäide: Mõningate polünoomide taandumatust üle $\mathbb{Z}$ saab kindlaks teha Eisensteini kriteeriumi abil (vt [2], lk 248, teoreem 2). Iga taandumatu polünoom üle $\mathbb{Z}$ on taandumatu ka üle $\mathbb{Q}$ (vt [2], lk 246, lemma 2).)

22. Tähistame kõigi selliste kompleksarvude, mis on algebralised üle $\mathbb{Q}$, hulga tähega $\mathbb{A}$. Näidata, et hulk $\mathbb{A}$ on korpuse $\mathbb{C}$ alamkorpus järgneval moel.

    a. Näidata, et kompleksarv $\alpha \in \mathbb{A}$ siis ja ainult siis kui $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$. Järeldada, et $\mathbb{Q} \subseteq \mathbb{A}$.

    b. Olgu $\alpha, \beta \in \mathbb{A}$. Teoreemi 2.1.36 kasutades näidata, et $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] < \infty$.

    c. Osa *b.* tulemust ning teoreemi 2.1.36 kasutades näidata, et $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] < \infty$, $[\mathbb{Q}(-\alpha) : \mathbb{Q}] < \infty$, $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] < \infty$ ning, kui $\alpha \neq 0$, siis $[\mathbb{Q}(\alpha^{-1}) : \mathbb{Q}] < \infty$.

23. Eelmise ülesande tähistuses, näidata, et $[\mathbb{A} : \mathbb{Q}] = \infty$. Järeldada, et algebralised laiendid ei tarvitse olla lõplikud. (Näpunäide: Kasutada Eisensteini kriteeriumi, mille abil näidata, et leidub kuitahes kõrge astmega taandumatuid polünoome üle $\mathbb{Q}$.)

24. Olgu laiendid $M : L$ ja $L : K$ algebralised. Kas siis ka laiend $M : K$ on algebraline? (Vaadeldavad laiendid ei tarvitse olla lõplikud.)

25. Olgu f polünoom üle korpuse K, kusjuures $\deg f = n$. Olgu Σ polünoomi f lahutuskorpus üle K. Tõestada, et $[\Sigma : K]$ jagab arvu $n!$. (Näpunäide: Vaadata eraldi juhtusid kui f on taandumatu ja taanduv. Taanduva juhu korral kasutada matemaatilise induktsiooni meetodit. Panna tähele, et $a!b!$ jagab arvu $(a+b)!$ (miks?).)

26. Olgu m taandumatu polünoom üle korpuse K ning olgu ta elemendi α minimaalseks polünoomiks üle K. Kas laiend $K(\alpha) : K$ on sellisel juhul alati normaalne?

27. Olgu laiendi $L : K$ aste 2. Näidata, et siis laiend $L : K$ on normaalne.

28. Millised järgnevatest laienditest on normaalsed?

    a. $\mathbb{Q}\left(\sqrt{-2}\right) : \mathbb{Q}$.
    b. $\mathbb{Q}(\alpha) : \mathbb{Q}$, kus $\alpha = \sqrt[7]{2} \in \mathbb{R}$.
    c. $\mathbb{Q}\left(\alpha, \sqrt{2}\right) : \mathbb{Q}$, kus $\alpha = \sqrt[7]{2} \in \mathbb{R}$.
    d. $\mathbb{R}\left(\sqrt{-5}\right) : \mathbb{R}$.

29. Märkida järgnevad kas "Tõene" (T) või "väär" (V).

    a. Kui $X \subseteq \mathbb{Q}$, siis $\mathbb{Q}(X) = \mathbb{Q}$.
    b. Kui hulk X sisaldab irratsionaalarvu, siis $\mathbb{Q}(X) \neq \mathbb{Q}$.
    c. Korpuse $\mathbb{C}$ iga alamkorpus sisaldab korpust $\mathbb{R}$.
    d. Kõik irratsionaalarvud on transtsendentsed.
    e. Arvu π iga nullist erinev ratsionaalarvukordne on trantsendentne.
    f. Iga lihtlaiend on algebraline.
    g. Algebralised lihtlaiendid $K(\alpha) : K$ ja $K(\beta) : K$ on alati isomorfsed $(\alpha, \beta \in \mathbb{C})$.
    h. Transtsendentsed lihtlaiendid $K(\alpha) : K$ ja $K(\beta) : K$ on alati isomorfsed $(\alpha, \beta \in \mathbb{C})$.
    i. Korpuse $\mathbb{C}$ iga element on algebraline üle $\mathbb{R}$.
    j. Iga polünoom üle $\mathbb{Q}$ lahutub lineaartegurite korrutiseks üle teatava $\mathbb{C}$ alamkorpuse.
    k. Iga lõplik korpuse laiend on normaalne.
    l. Kui laiendid $L : M$ ja $M : K$ on normaalsed siis on ka laiend $L : K$ normaalne.
    m. Iga algebraline laiend on lõplik.

Peatükk 3

Galois' teooria

Olles teinud tutvust rühmade ja korpuste mõningate vajalike tulemustega, oleme nüüd valmis Galois' teooria põhjalikumaks uurimiseks. Seda teooriat kasutades näitame lõpuks, et leidub viienda astme võrrand, mis ei ole lahenduv radikaalides.

3.1 Galois' teooria sissejuhatus

3.1.1 Lagrange'i idee võrrandite lahendamiseks

Kuna Galois luges Lagrange'i töid, siis võib arvata, et just siit pärineb Galois' originaalne idee võrrandite radikaalides lahenduvuse probleemi lahendamiseks. Lagrange uuris võrrandite lahendamist selle võrrandi lahendite vahel kehtivate teatud sümmeetriate abil. Võrrandi lahendite vaheliste sümmeetriate kasutamine on üks põhiideedest ka Galois' teoorias.

Järgnevalt tutvumegi lähemalt Lagrange'i ideega teise, kolmanda ja neljanda astme võrrandite lahendamiseks. Idee seisneb selliste polünoomide leidmises võrrandi lahenditest, mis jäävad muutumatuks võrrandi lahendite permuteerimisel. Proovime seda meetodit rakendada ka 5. astme võrrandile.

Alustuseks meenutame, et n muutuja polünoomi $f = f(x_1, x_2, ..., x_n)$ nimetame sümmeetriliseks kui ta ei muutu muutujate mistahes substitutsiooni korral. Lagrange'i ideega tutvumisel puutume kokku sümmeetriliste põhipolünoomidega s_1, s_2, ..., s_n muutujatest x_1, x_2, ..., x_n, millised teatavasti defineeritakse järgnevalt:

$$\begin{gathered} s_1 = s_1(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \ldots + x_n \\ s_2 = s_2(x_1, x_2, \ldots, x_n) = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n\,, \\ \ldots\,, \\ s_n = s_n(x_1, x_2, \ldots, x_n) = x_1x_2 \ldots x_n\,, \end{gathered}$$

kus s_k ($k \in \{1, 2, ..., n\}$) on summa kõikidest k kaupa võetud erinevatest korrutistest muutujatest x_1, x_2, ..., x_n, kusjuures igas sellises korrutises esineb iga muutuja tegurina ülimalt ühe korra.

Kõikidest n muutujaga sümmeetrilistest polünoomidest kordajatega ringist $\mathbb{C}$ koosnev hulk moodustab ringi $\mathbb{C}[x_1, x_2, ..., x_n]$ alamringi (vt [5], lk 218, lause 6.17.4). Seda ringi tähistame[1] järgnevalt sümboliga $\mathbb{C}[s_1, s_2, ..., s_n]$.

Vaatame nüüd järgnevat muutujast x sõltuvat polünoomi F üle ringi $\mathbb{C}[x_1, x_2, ..., x_n]$:

$$F(x) = (x - x_1)(x - x_2) \dots (x - x_n) .$$

Matemaatilise induktsiooni meetodit kasutades võime veenduda, et peale sulgude avamist saame

$$F(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^{n-1} s_{n-1} x + (-1)^n s_n .$$

Definitsioon 3.1.1. Olgu s_1, s_2, ..., s_n sümmeetrilised põhipolünoomid algebralistest muutujatest x_1, x_2, ..., x_n kompleksarvude hulgas. *Üldiseks n-astme algebraliseks võrrandiks* nimetame võrrandit

$$x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^{n-1} s_{n-1} x + (-1)^n s_n = 0 \qquad (3.1)$$

üle ringi $\mathbb{C}[s_1, s_2, ..., s_n]$ jagatistekorpuse $\mathbb{C}(s_1, s_2, ..., s_n)$. Muutujaid x_1, x_2, ..., x_n nimetame selle *võrrandi lahenditeks*.

Definitsioon 3.1.2. *Üldist n-astme võrrandit* (3.1) *nimetame lahenduvaks radikaalides*, kui kõik tema lahendid x_1, x_2, ..., x_n on avaldatavad korpuse $\mathbb{C}(s_1, s_2, ..., s_n)$ elementide kaudu nelja aritmeetilist põhitehet (liitmine, lahutamine, korrutamine ja jagamine) ning mistahes naturaalarvuliste juurte võtmist kasutades. Sellisel juhul ütleme, et lahendid x_1, x_2, ..., x_n avalduvad korpuse $\mathbb{C}(s_1, s_2, ..., s_n)$ elementide kaudu *radikaalides*.

Kui me oskaksime lahendada üldist n-astme võrrandit radikaalides mingi fikseeritud naturaalarvu n korral, siis oleks ka iga konkreetne n-astme kompleksarvuliste kordajatega võrrand, mille pealiikme x^n kordaja on 1, lahenduv radikaalides. Meil tuleks selleks lihtsalt s_1, s_2, ..., s_n üldvõrrandi lahendivalemis asendada konkreetse võrrandi kordajatega. (Arvestades ka märkide erinevust!) Kuna iga võrrandit on võimalik ära normeerida (jagada läbi sellise arvuga, et pealiikme kordaja oleks 1), milline tegevus ei muuda võrrandi lahendeid, siis oleks iga konkreetne n-astme kompleksarvuliste kordajatega võrrand lahenduv radikaalides.

[1] Selline tähistus on põhjendatud sellega, et iga sümmeetrilist n muutuja polünoomi saame esitada polünoomina sümmeetrilistest põhipolünoomidest (vt [5], lk 219, teoreem 6.17.6).

Veendume nüüd järgnevas, et üldine teise, kolmanda ja neljanda astme võrrand on lahenduv radikaalides.

Vaatame üldist teise astme algebralist võrrandit

$$x^2 - s_1 x + s_2 = 0\,,$$

kus

$$\begin{aligned} s_1 &= s_1(x_1, x_2) = x_1 + x_2\,, \\ s_2 &= s_2(x_1, x_2) = x_1 x_2\,. \end{aligned} \tag{3.2}$$

Paneme tähele, et kahe muutuja polünoom

$$(x_1 - x_2)^2$$

on sümmeetriline muutujate x_1 ja x_2 suhtes. Seega saame ta esitada polünoomina sümmeetrilistest põhipolünoomidest s_1 ja s_2 (vt [5], lk 219, teoreem 6.17.6). Osutub, et

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 x_2 = s_1^2 - 4s_2\,, \tag{3.3}$$

millest

$$x_1 - x_2 = \pm\sqrt{s_1^2 - 4s_2}\,.$$

Arvestades lisaks võrduste (3.2) esimest võrdust, saame nüüd järgmise võrrandisüsteemi lahendite x_1 ja x_2 suhtes:

$$\begin{cases} x_1 + x_2 = s_1 \\ x_1 - x_2 = \pm\sqrt{s_1^2 - 4s_2}\,. \end{cases}$$

Selle lahendamisel saame, et[2]

$$\begin{aligned} x_1 &= \frac{s_1 + \sqrt{s_1^2 - 4s_2}}{2}\,, \\ x_2 &= \frac{s_1 - \sqrt{s_1^2 - 4s_2}}{2}\,. \end{aligned} \tag{3.4}$$

Sellega oleme näidanud, et üldine teise astme võrrand on lahenduv radikaalides.

Vaatame nüüd üldist 3. astme võrrandit

$$x^3 - s_1 x^2 + s_2 x - s_3 = 0\,, \tag{3.5}$$

[2]Lahendamisel valisime ruutjuure ees märgiks "+". Valides märgiks "−", saame samad lahendid.

kus

$$\begin{aligned} s_1 = s_1(x_1, x_2, x_3) = x_1 + x_2 + x_3\,, \\ s_2 = s_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3\,, \\ s_3 = s_3(x_1, x_2, x_3) = x_1x_2x_3\,. \end{aligned} \tag{3.6}$$

Olgu

$$\begin{aligned} y = y(x_1, x_2, x_3) = (x_1 + \zeta x_2 + \zeta^2 x_3)^3\,, \\ z = z(x_1, x_2, x_3) = (x_1 + \zeta^2 x_2 + \zeta x_3)^3\,, \end{aligned} \tag{3.7}$$

kus $\zeta = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ on 3. astme ühejuur. Paneme tähele, et vahetades omavahel ümber muutujad x_1 ja x_2 polünoomis y, saame

$$\begin{aligned} y(x_2, x_1, x_3) = (x_2 + \zeta x_1 + \zeta^2 x_3)^3 = (\zeta(x_1 + \zeta^2 x_2 + \zeta x_3))^3 = \\ = \zeta^3(x_1 + \zeta^2 x_2 + \zeta x_3)^3 = (x_1 + \zeta^2 x_2 + \zeta x_3)^3 = z(x_1, x_2, x_3)\,. \end{aligned}$$

Sarnaselt võime veenduda, et $z(x_2, x_1, x_3) = y(x_1, x_2, x_3)$, ning, mistahes kahe muutuja ümbervahetamisel saame polünoomist y polünoomi z ja vastupidi. Muutujate tsüklilisel ümberpaigutamisel jäävad polünoomid y ja z aga muutumatuks. Seega, eelöeldu tõttu, $y + z$ ja yz on sümmeetrilised polünoomid muutujate x_1, x_2, x_3 suhtes ning me saame nad seepärast esitada polünoomidena sümmeetrilistest põhipolünoomidest s_1, s_2, s_3. Olgu näiteks

$$\begin{aligned} y + z = a_1 = a_1(s_1, s_2, s_3)\,, \\ yz = a_2 = a_2(s_1, s_2, s_3)\,, \end{aligned}$$

kus a_1 ja a_2 on teatud kolme muutuja polünoomid üle $\mathbb{C}$.

Paneme tähele, et y ja z rahuldavad võrrandit

$$(x - y)(x - z) = 0$$

ehk, peale sulgude avamist, võrrandit

$$x^2 - a_1x + a_2 = 0 \tag{3.8}$$

üle $\mathbb{C}(s_1, s_2, s_3)$. Täpselt samal moel nagu üldise teise astme võrrandi puhul, võime veenduda, et y ja z on avaldatavad võrrandi (3.8) kordajate kaudu radikaalides (tuleb lugeda, et a_1 ja a_2 on sümmeetrilised põhipolünoomid muutujatest y ja z). Kuna aga võrrandi (3.8) kordajad kuuluvad korpusesse $\mathbb{C}(s_1, s_2, s_3)$, siis y ja z avalduvad korpuse $\mathbb{C}(s_1, s_2, s_3)$ elementide kaudu radikaalides. Siis aga avalduvad ka $\sqrt[3]{y}$ ja $\sqrt[3]{z}$ korpuse $\mathbb{C}(s_1, s_2, s_3)$ elementide kaudu radikaalides. Võrduste (3.6) esimese võrduse ja võrduste (3.7) põhjal saame nüüd aga järgneva süsteemi võrrandi (3.5) lahendite suhtes:

$$\begin{cases} x_1 + x_2 + x_3 = s_1 \\ x_1 + \zeta x_2 + \zeta^2 x_3 = \sqrt[3]{y} \\ x_1 + \zeta^2 x_2 + \zeta x_3 = \sqrt[3]{z}\,. \end{cases} \tag{3.9}$$

Liites need võrrandid omavahel ning arvestades, et ζ on polünoomi x^2+x+1 juur, saame, et

$$3x_1 = s_1 + \sqrt[3]{y} + \sqrt[3]{z}\,,$$

millest

$$x_1 = \frac{1}{3}(s_1 + \sqrt[3]{y} + \sqrt[3]{z})\,.$$

Korrutades nüüd süsteemi (3.9) teist võrrandit suurusega ζ^2, kolmandat võrrandit aga suurusega ζ, liites seejärel saadud võrrandid ja jagades saadud avaldist kolmega, saame, et

$$x_2 = \frac{1}{3}(s_1 + \zeta^2\sqrt[3]{y} + \zeta\sqrt[3]{z})\,.$$

Lõpuks, korrutades süsteemi (3.9) teist võrrandit suurusega ζ, kolmandat võrrandit aga suurusega ζ^2, liites seejärel saadud võrrandid ja jagades saadud avaldist kolmega, saame, et

$$x_3 = \frac{1}{3}(s_1 + \zeta\sqrt[3]{y} + \zeta^2\sqrt[3]{z})\,.$$

Seega, võrrandi (3.5) lahendid x_1, x_2 ja x_3 avalduvad radikaalides korpuse $\mathbb{C}(s_1, s_2, s_3)$ elementide kaudu ning üldine kolmanda astme võrrand on lahenduv radikaalides.

Vaatame nüüd üldist neljanda astme võrrandit

$$x^4 - s_1x^3 + s_2x^2 - s_3x + s_4 = 0\,, \tag{3.10}$$

kus

$$\begin{gathered} s_1 = s_1(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4\,, \\ s_2 = s_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4\,, \\ s_3 = s_3(x_1, x_2, x_3, x_4) = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4\,, \\ s_4 = s_4(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4\,. \end{gathered} \tag{3.11}$$

Olgu

$$\begin{aligned} y &= y(x_1, x_2, x_3, x_4) = (x_1 + x_2 - x_3 - x_4)^2\,, \\ z &= z(x_1, x_2, x_3, x_4) = (x_1 - x_2 + x_3 - x_4)^2\,, \\ w &= w(x_1, x_2, x_3, x_4) = (x_1 - x_2 - x_3 + x_4)^2\,. \end{aligned} \tag{3.12}$$

Võime veenduda, et $y+z+w$, $yz+yw+zw$ ja yzw on sümmeetrilised polünoomid muutujatest x_1, x_2, x_3 ja x_4, mistõttu saame nad esitada polünoomidena sümmeetrilistest põhipolünoomidest s_1, s_2, s_3 ja s_4. Olgu seega

$$\begin{gathered} y + z + w = a_1 = a_1(s_1, s_2, s_3, s_4)\,, \\ yz + yw + zw = a_2 = a_2(s_1, s_2, s_3, s_4)\,, \\ yzw = a_3 = a_3(s_1, s_2, s_3, s_4)\,, \end{gathered}$$

kus a_1, a_2 ja a_3 on teatud nelja muutuja polünoomid üle $\mathbb{C}$. Paneme jällegi tähele, et y, z ja w rahuldavad võrrandit

$$(x-y)(x-z)(x-w)=0$$

ehk, peale sulgude avamist, võrrandit

$$x^3-a_1x^2+a_2x-a_3=0 \tag{3.13}$$

üle $\mathbb{C}(s_1,s_2,s_3,s_4)$. Samal moel nagu üldise kolmanda astme võrrandi puhul, võime veenduda, et y, z ja w on avaldatavad koruse $\mathbb{C}(a_1,a_2,a_3)$ elementide kaudu radikaalides (tuleb lugeda, et a_1, a_2 ja a_3 on sümmeetrilised põhipolünoomid muutujatest y, z ja w). Kuna aga võrrandi (3.13) kordajad kuuluvad korpusesse $\mathbb{C}(s_1,s_2,s_3,s_4)$, siis y, z ja w avalduvad korpuse $\mathbb{C}(s_1,s_2,s_3,s_4)$ elementide kaudu radikaalides. Siis avalduvad ka $\sqrt{y}$, $\sqrt{z}$ ja $\sqrt{w}$ korpuse $\mathbb{C}(s_1,s_2,s_3,s_4)$ elementide kaudu radikaalides. Võrduste (3.11) esimese võrduse ja võrduste (3.12) põhjal saame nüüd aga järgneva süsteemi võrrandi (3.10) lahendite suhtes:

$$\begin{cases} x_1+x_2+x_3+x_4=s_1\,, \\ x_1+x_2-x_3-x_4=\pm\sqrt{y}\,, \\ x_1-x_2+x_3-x_4=\pm\sqrt{z}\,, \\ x_1-x_2-x_3+x_4=\pm\sqrt{w}\,. \end{cases} \tag{3.14}$$

Lahendades viimase süsteemi saamegi, et võrrandi (3.10) lahendid avalduvad korpuse $\mathbb{C}(s_1,s_2,s_3,s_4)$ elementide kaudu radikaalides. (Võrrandisüsteemist lahendi x_1 leidmiseks liidame kõik võrrandid ning jagame seejärel arvuga 4. Lahendi x_2 leidmiseks liidame omavahel esimese, teise ning arvuga (-1) korrutatud kolmanda ja neljanda võrrandi ning jagame seejärel arvuga 4. Sarnasel viisil leiame ülejäänud lahendid.) Seega, üldine neljanda astme võrrand on lahenduv radikaalides.

Vaatame lõpuks veel üldist viienda astme võrrandit

$$x^5-s_1x^4+s_2x^3-s_3x^2+s_4x-s_5=0\,.$$

Analoogiliselt eelnevate näidetega vaatame näiteks polünoomi

$$y=(x_1+\zeta x_2+\zeta^2x_3+\zeta^3x_4+\zeta^4x_5)^5\,, \tag{3.15}$$

kus $\zeta=e^{2\pi i/5}$ on 5. astme ühejuur. Muutujaid x_1, x_2, ..., x_5 võib ümber järjestada kokku $5!=120$ erineval moel. On veendutud, et kõigi nende ümberjärjestuste käigus omandab polünoom (3.15) kokku 24 erinevat kuju, mistõttu meie poolt eelnevalt demonstreeritud meetodit ei õnnestu rakendada. Ei ole ka leitud teisi polünoome muutujatest x_1, x_2, ..., x_5, mis

annaksid muutujate kõikvõimalikel ümberjärjestamistel kokku näiteks neli erinevat kuju y, z, w ja u selliselt, et y, z, w ja u osutuksid teatud neljanda astme võrrandi üle $\mathbb{C}(s_1, s_2, ..., s_5)$ lahenditeks, ning et õnnestuks rakendada eelnevalt demonstreeritud ideed.

Märgime märkusena, et äsjanäidatu põhjal avalduvad üldise kuupvõrrandi ja üldise neljanda astme võrrandi lahendid nende võrrandi kordajate ja teatud fikseeritud kompleksarvude kaudu radikaalides. Tekib aga küsimus, kas need fikseeritud kompleksarvud on esitatavad võrrandi kordajate kaudu radikaalides? Osutub, et see nii tõesti on, nagu selles võib veenduda vajalikke arvutusi teostades. Näiteks kuupvõrrandi lahendite avaldamiseks korpuse $\mathbb{C}(s_1, s_2, ..., s_n)$ elementide kaudu tõime sisse suuruse $\xi = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Ei ole aga raske näha, et suurus ξ on esitatav kuupvõrrandi pealiikme kordaja 1 kaudu nelja artitmeetilist põhitehet ning juurimisi kasutades. Konkreetsed valemid radikaalides kuupvõrrandi ja neljanda astme võrrandi jaoks ning teisi meetodeid nende valemite tuletamiseks võib seejuures leida allikatest [8] ja [10].

3.1.2 Idee Galois' teooria taga

Jätame nüüd üldise n-astme võrrandi vaatlemise ning asume konkreetsete võrrandite uurimise juurde. St, edasises on vaatluse all vaid kompleksarvuliste kordajatega võrrandid. Nagu nägime eelmises punktis, algebralise võrrandi lahendite vahel eksisteerivad alati teatud sümmeetriad. Neid sümmeetriaid kasutas oskuslikult ära Lagrange. Uurime neid sümmeetriaid nüüd edasi.

Olgu järgnevas $f(x) = 0$ mingi selline algebraline võrrand üle korpuse K, et polünoom f on taandumatu[3] üle K. Olgu $L \subseteq \mathbb{C}$ mingi selline korpus, et $K \subseteq L$ ning mis sisaldab polünoomi f kõiki juuri, milliseid tähistame α_1, α_2, ..., α_n. Järelduse 2.2.6 põhjal on polünoomi f taandumatuse tõttu juured α_1, α_2, ..., α_n paarikaupa erinevad. See asjaolu lihtsustab mõnevõrra meie teooriakäsitlust.

Meie eesmärgiks on avaldada polünoomi f juured tema kordajate kaudu nelja aritmeetilist põhitehet (liitmine, lahutamine, korrutamine ja jagamine) ning mistahes naturaalarvuliste juurte võtmist kasutades. Teisisõnu, meie eesmärgiks on avaldada polünoomi f juured tema kordajate kaudu radikaalides. Matemaatiliselt formuleerime selle ülesande järgnevalt. Rääkides, et f on polünoom üle K, peame üldiselt korpuse K all silmas sellist korpust, mis on saadud korpusest $\mathbb{Q}$ temale polünoomi f kordajate adjungeerimisel. Polünoomi f juurte avaldamine selle polünoomi kordajate kaudu radikaalides on siis samaväärne kui avaldada juured korpuse K elementide kaudu

[3]Kuna iga polünoomi on võimalik esitada taandumatute polünoomide korrutisena (vt [2], lk 213, teoreem 5), siis polünoomi juurte leidmiseks piisabki kui leida selle polünoomi taandumatute tegurite juured.

radikaalides. (Püstitatud ülesande konkreetsema matemaatilise formuleeringu anname hiljem, vt definitsioonid 3.3.1 ja 3.3.3 lehekülgedel 98 ja 98.)

Paneme tähele, et üldiselt võib korpuste K ja L vahel leiduda korpusi, mis ei ühti korpusega K ega L. Kui leidub selline juur α_i, et $K(\alpha_i) \neq L$, siis on selliseks korpuseks $K(\alpha_i)$ (kuna f on taandumatu üle K, siis ei saa tema juured kuuluda korpusesse K). Vaatame seega juhtu, kus leidub selline korpus M, et $K \subsetneqq M$ ning $M \subsetneqq L$. Oletame, et kõik M elemendid on avaldatavad korpuse K elementide ja elementide α_1 ja α_2 kaudu korpuse tehteid rakendades. Oletame, et me teame lisaks, et

$$\alpha_3 + \alpha_4\,,\ \alpha_3\alpha_4 \in M \tag{3.16}$$

ning, et

$$\alpha_1 + \alpha_2\,,\ \alpha_1\alpha_2 \in K\,. \tag{3.17}$$

Tähistades $c_1 = \alpha_3 + \alpha_4$ ning $c_2 = \alpha_3\alpha_4$, saame, et Viète'i valemite (vt [2], lk 269) põhjal, α_3 ja α_4 on ruutvõrrandi

$$x^2 - c_1 x + c_2 = 0$$

lahenditeks. Paneme aga tähele, et (3.16) tõttu $c_1, c_2 \in M$. Ruutvõrrandi lahendivalemit radikaalides kasutades (vt (3.4), leheküljel 55), saame, et

$$\begin{aligned} \alpha_3 &= \frac{c_1 + \sqrt{c_1^2 - 4c_2}}{2}\,, \\ \alpha_4 &= \frac{c_1 - \sqrt{c_1^2 - 4c_2}}{2}\,. \end{aligned} \tag{3.18}$$

St, polünoomi f juured α_3 ja α_4 avalduvad korpuse M elementide kaudu radikaalides. Kuna meie eelduse tõttu kõik M elemendid on avaldatavad korpuse K elementide ja elementide α_1 ja α_2 kaudu korpuse tehteid rakendades, siis

$$\begin{aligned} c_1 &= \frac{p_1(\alpha_1, \alpha_2)}{p_2(\alpha_1, \alpha_2)}\,, \\ c_2 &= \frac{q_1(\alpha_1, \alpha_2)}{q_2(\alpha_1, \alpha_2)}\,, \end{aligned} \tag{3.19}$$

kus p_1, p_2, q_1 ja q_2 on teatud 2 muutuja polünoomid üle K. Juured α_3 ja α_4 saame võrduste (3.18) ja (3.19) tõttu seega esitada juurte α_1, α_2 ning korpuse K elementide kaudu radikaalides.

Nüüd, tähistades $d_1 = \alpha_1 + \alpha_2$ ning $d_2 = \alpha_1\alpha_2$, märkame, et α_1 ja α_2 on ruutvõrrandi

$$x^2 - d_1 x + d_2 = 0\,, \tag{3.20}$$

lahenditeks. Sisalduvuste (3.17) tõttu aga võrrand (3.20) on võrrand üle korpuse K. Selle võrrandi lahendid avalduvad kujul

$$\begin{aligned} \alpha_1 &= \frac{d_1 + \sqrt{d_1^2 - 4d_2}}{2}\,, \\ \alpha_2 &= \frac{d_1 - \sqrt{d_1^2 - 4d_2}}{2}\,. \end{aligned} \tag{3.21}$$

Seega, polünoomi f juured α_1 ja α_2 avalduvad korpuse K elementide kaudu radikaalides. Siis aga ka võrduste (3.19) tõttu suurused c_1 ja c_2 avalduvad K elementide kaudu radikaalides ning seetõttu ka juured α_3 ja α_4 avalduvad (3.18) tõttu K elementide kaudu radikaalides.

Oleme näidanud, et eeldustel (3.16), (3.17) ning eeldusel, et korpuse M kõik elemendid avalduvad korpuse K elementide ja elementide α_1 ja α_2 kaudu korpuse tehteid rakendades, on meil võimalik avaldada polünoomi f juured α_1, α_2, α_3 ja α_4 tema kordajate kaudu radikaalides. Me eeldasime küll nii mõndagi, kuid vaatame nüüd olukorda, kus meil on antud järgnev korpuste jada:

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_m = L\,.$$

Oletame, et iga korpus K_i on teatava ülimalt 4. astme polünoomi f_i lahutuskorpuseks üle K_{i-1} ($i \in \{1, 2, ..., m\}$). Siis aga, arvestades teoreemi 2.2.12, lauset 2.2.3 ning lõpuks järeldust 2.1.45, saaksime lahendivalemeid radikaalides 2., 3. ja 4. astme võrrandite jaoks kasutades polünoomi f juured korpuses L avaldada järk-järgult korpuse K elementide kaudu radikaalides!

Selliste küsimuste uurimiseks uurime polünoomi f juurtega seotud sümmeetriaid edasi ning veendume, et me saame korpustega M, kus $K \subseteq M \subseteq L$, siduda teatud rühmad.

Definitsioon 3.1.3. Olgu $f(x) = 0$ selline algebraline võrrand, mille korral f on taandumatu polünoom üle korpuse K, $\deg f = n$. *Võrrandi* $f(x) = 0$ *lahenditevaheliseks ratsionaalseks seoseks* (*üle* K) nimetame iga seost kujul

$$p(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0\,, \tag{3.22}$$

kus α_1, α_2, ..., α_n on selle võrrandi kõik lahendid ning p on n muutuja polünoomide ringi $K[x_1, x_2, ..., x_n]$ jagatistekorpuse $K(x_1, x_2, ..., x_n)$ element.

Näide 3.1.4. Olgu polünoomiks f polünoom $x^4 - 5$ üle $\mathbb{Q}$. Vaadeldav polünoom on Eisensteini kriteeriumi põhjal taandumatu üle $\mathbb{Q}$ ning selle juured on $\alpha_1 = \xi = \sqrt[4]{5} \in \mathbb{R}$, $\alpha_2 = -\xi$, $\alpha_3 = i\xi$, $\alpha_4 = -i\xi$. Nende juurte vahel kehtivad näiteks järgnevad ratsionaalsed seosed

$$\alpha_1 + \alpha_2 = 0\,, \qquad \alpha_3 + \alpha_4 = 0\,, \qquad \alpha_1\alpha_3 - \alpha_2\alpha_4 = 0\,. \tag{3.23}$$

Definitsioon 3.1.5. Olgu $f(x) = 0$ selline algebraline võrrand, mille korral f on taandumatu polünoom üle korpuse K, $\deg f = n$. Ütleme, et *substitutsioon*

$$s = \begin{pmatrix} 1 & 2 & \dots & n \\ s_1 & s_2 & \dots & s_n \end{pmatrix}$$

jätab võrrandi $f(x) = 0$ *lahenditevahelise ratsionaalse seose*

$$p(\alpha_1, \alpha_2, \dots, \alpha_n) = 0\,,$$

$p \in K(x_1, x_2, ..., x_n)$, *invariantseks*, kui

$$p(\alpha_{s_1}, \alpha_{s_2}, \dots, \alpha_{s_n}) = 0\,.$$

Märgime, et polünoomi f taandumatuse tõttu juured α_1, α_2, ..., α_n ei kuulu korpusesse K (juhul kui $n > 1$) ning on paarikaupa erinevad, mistõttu on definitsioon korrektne.

Defineerime nüüd *hulga* G, kuhu arvame kõik sellised substitutsioonid n elemendist, mis jätavad invariantseks kõik võrrandi $f(x) = 0$ lahenditevahelised ratsionaalsed seosed üle K.

Näide 3.1.6. Jätkame näidet 3.1.4.

Hulka G ei saa antud juhul kindlasti kuuluda substitutsioon

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

sest "rakendades" seda substitutsiooni ratsionaalsele seosele

$$\alpha_1 + \alpha_2 = 0\,,$$

saame, et

$$\alpha_3 + \alpha_2 = i\xi - \xi \neq 0\,.$$

Seevastu substitutsioon

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

võib osutuda kuuluvaks hulka G, sest selle "rakendamisel" seostele (3.23), saame, et

$$\alpha_2 + \alpha_1 = -\xi + \xi = 0\,, \qquad \alpha_3 + \alpha_4 = i\xi - i\xi = 0\,,$$
$$\alpha_2\alpha_3 - \alpha_1\alpha_4 = -i\xi^2 + i\xi^2 = 0\,.$$

Paneme tähele, et selliselt defineeritud hulk G osutub rühmaks.

Lause 3.1.7. *Olgu $f(x) = 0$ selline n-astme algebraline võrrand üle korpuse K, mille korral polünoom f on taandumatu üle K. Olgu G selline hulk, mis koosneb kõigist sellistest substitutsioonidest rühmast $\mathbb{S}_n$, mis jätavad invariantseks võrrandi $f(x) = 0$ kõik lahenditevahelised ratsionaalsed seosed üle K. Siis hulk G on rühma $\mathbb{S}_n$ alamrühm.*

Tõestus. Paneme kõigepealt tähele, et $G \neq \emptyset$, sest ühiksubstitutsioon $e \in G$. Olgu seega $s', s'' \in G$ suvalised. Veendume, et $s's'' \in G$. Selleks olgu

$$p(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0 \tag{3.24}$$

võrrandi $f(x) = 0$ suvaline lahenditevaheline ratsionaalne seos üle K. Näitamaks, et $s's'' \in G$, tuleb näidata, et

$$p(\alpha_{s's''_1}, \alpha_{s's''_2}, \ldots, \alpha_{s's''_n}) = 0\,. \tag{3.25}$$

Kuna $s'' \in G$, siis

$$p(\alpha_{s''_1}, \alpha_{s''_2}, \ldots, \alpha_{s''_n}) = 0\,. \tag{3.26}$$

Seega, seos

$$q(\alpha_1, \alpha_2, \ldots, \alpha_n) = p(\alpha_{s''_1}, \alpha_{s''_2}, \ldots, \alpha_{s''_n}) = 0\,,$$

kus $q \in K(x_1, x_2, ..., x_n)$, on võrrandi $f(x) = 0$ lahenditevaheline ratsionaalne seos üle K. Kuna $s' \in G$, siis

$$q(\alpha_{s'_1}, \alpha_{s'_2}, \ldots, \alpha_{s'_n}) = 0\,,$$

ehk

$$p(\alpha_{s'_{s''_1}}, \alpha_{s'_{s''_2}}, \ldots, \alpha_{s'_{s''_n}}) = 0\,,$$

millest substitutsioonide korrutamise reeglit arvestades järeldubki võrduse (3.25) kehtivus.

Veendumaks, et G on rühma $\mathbb{S}_n$ alamrühm, jääb veel näidata, et igal elemendil hulgas G leidub pöördelement. Olgu seega $s \in G$ suvaline ning olgu m substitutsiooni s järk, st selline vähim naturaalarv, mille korral s^m on ühiksubstitutsioon. Paneme tähele, et siis $s^{-1} = s^{m-1}$. Tõestuseks tuleb seega näidata, et $s^{m-1} \in G$. See aga järeldub vahetult matemaatilise induktsiooni meetodit kasutades, arvestades, et eespoolnäidatu põhjal substitutsioonide korrutamise tehe on kinnine rühmas G.

Sellega oleme näidanud, et G on rühma $\mathbb{S}_n$ alamrühm. □

Rühma G kutsutakse nii võrrandi $f(x) = 0$ kui ka polünoomi f *Galois' rühmaks*. Selliselt defineeris võrrandi Galois' rühma Évariste Galois (ta tähistas siiski substitutsioone teisiti). Edasises teooriaarenduses tugineme aga Galois' rühma mõnevõrra teisele definitsioonile, milles me enam ei eelda polünoomi f taandumatust.

Definitsioon 3.1.8. Olgu $L : K$ korpuse laiend. *K-automorfismiks korpusel L* nimetame automorfismi $\alpha : L \to L$, mille korral

$$\alpha(k) = k \qquad \forall k \in K\,.$$

Märgime, et kui korpuse L roll on kontekstist selge, siis K-automorfismi korpusel L nimetame mõnikord ka lihtsalt *K-automorfismiks*.

Teoreem 3.1.9. *Olgu $L : K$ korpuse laiend. Siis kõigi K-automorfismide hulk korpusel L moodustab teisenduste korrutamise suhtes rühma.*

Tõestus. Kõik automorfismid korpusel L moodustavad rühma teisenduste korrutamise suhtes (vt [5], lk 76, lause 2.6.5). Seega piisab meile näidata, et kõigi K-automorfismide hulk korpusel L on selle rühma alamrühm.

Kuna samasusteisendus $I : L \to L$ on ühtlasi ka K-automorfism korpusel L, siis kõigi K-automorfismide hulk korpusel L ei ole mittetühi.

Olgu α ja β kaks K-automorfismi korpusel L. Kuna suvalise $k \in K$ korral

$$(\alpha\beta)(k) = \alpha(\beta(k)) = \alpha(k) = k\,,$$

siis $\alpha\beta$ on K-automorfism korpusel L.

Veendume lõpuks, et kui α on K-automorfism korpusel L, siis ka α^{-1} on K-automorfism korpusel L. Olgu $k \in K$ suvaline. Paneme tähele, et suvalise $k \in K$ korral

$$\alpha^{-1}(k) = \alpha^{-1}(\alpha(k)) = (\alpha^{-1}\alpha)(k) = I(k) = k\,,$$

mistõttu α^{-1} on K-automorfism korpusel L.

Sellega oleme näidanud, et kõigi K-automorfismide hulk korpusel L moodustab rühma teisenduste korrutamise suhtes. □

Definitsioon 3.1.10. *Korpuse laiendi $L : K$ Galois' rühmaks* nimetame rühma, mis koosneb kõikidest K-automorfismidest korpusel L. Laiendi $L : K$ Galois' rühma tähistame $\Gamma(L : K)$.

Näide 3.1.11.

1. Vaatame korpuse laiendit $\mathbb{C} : \mathbb{R}$. Olgu α $\mathbb{R}$-automorfism ning olgu $j = \alpha(i)$, kus $i = \sqrt{-1}$. Siis

   $$j^2 = (\alpha(i))^2 = \alpha(i^2) = \alpha(-1) = -1\,,$$

   sest iga $r \in \mathbb{R}$ korral $\alpha(r) = r$. Seega, kas $j = i$ või $j = -i$. Nüüd suvalise kompleksarvu $x + yi \in \mathbb{C}$, $x, y \in \mathbb{R}$, korral

   $$\alpha(x + yi) = \alpha(x) + \alpha(y)\alpha(i) = x + yj\,.$$

Seega, meil on kaks võimalikku $\mathbb{R}$-automorfismi:

$$\alpha_1 : x + yi \mapsto x + yi\,,$$
$$\alpha_2 : x + yi \mapsto x - yi\,.$$

Paneme tähele, et α_1 on samasusteisendus, mistõttu on ta tõepoolest $\mathbb{R}$-automorfism korpusel $\mathbb{C}$. Veendume, et ka α_2 on $\mathbb{R}$-automorfism. Teisendus α_2 jätab korpuse $\mathbb{R}$ elemendid invariantseks, sest suvalise $x \in \mathbb{R}$ korral

$$\alpha_2(x) = \alpha_2(x + 0 \cdot i) = x - 0 \cdot i = x\,.$$

Teisendus α_2 on homomorfism, sest suvaliste $x + yi, u + vi \in \mathbb{C}$ $(x, y, u, v \in \mathbb{R})$ korral

$$\begin{aligned}\alpha_2((x+yi)+(u+vi)) = \alpha_2((x+u)+(y+v)i) = (x+u)-(y+v)i = \\ = (x-yi)+(u-vi) = \alpha_2(x+yi)+\alpha_2(u+vi)\end{aligned}$$

ning

$$\begin{aligned}\alpha_2((x+yi)(u+vi)) = \alpha_2((xu-yv)+(yu+xv)i) = \\ = (xu-yv)-(yu+xv)i = (x-yi)(u-vi) = \\ = \alpha_2(x+yi)\alpha_2(u+vi)\,.\end{aligned}$$

Näitame, et teisendus α_2 on bijektiivne. Olgu $x + yi, u + vi \in \mathbb{C}$ sellised suvalised elemendid, et $x + yi \neq u + vi$. Oletame, et nende elementide kujutised on võrdsed, st, $x - yi = u - vi$. Siis peab kehtima $x - u = (y - v)i$. Viimane võrdus saab aga kehtida vaid siis kui $x = u$ ja $y = v$, st, vaid siis kui $x + yi = u + vi$. See on aga vastuolus meie tingimusega, et $x + yi \neq u + vi$. Sellega oleme näidanud, et teisendus α_2 on injektiivne. Paneme tähele, et elemendi $x + yi \in \mathbb{C}$ originaal on $x - yi$. Seega, α_2 on sürjektiivne ning ühtlasi ka bijektiivne. Sellega oleme näidanud, et α_2 on $\mathbb{R}$-automorfism.

Paneme tähele, et $\alpha_2^2 = \alpha_1$, mistõttu laiendi $\mathbb{C} : \mathbb{R}$ Galois' rühm on $\Gamma(\mathbb{C} : \mathbb{R}) = \{\alpha_2, \alpha_2^2\}$, st, $\Gamma(\mathbb{C} : \mathbb{R})$ on 2. järku tsükliline rühm moodustajaga α_2.

2. Olgu $c = \sqrt[3]{2} \in \mathbb{R}$ ning vaatame laiendit $\mathbb{Q}(c) : \mathbb{Q}$. Kui α on $\mathbb{Q}$-automorfism korpusel $\mathbb{Q}(c)$, siis

$$(\alpha(c))^3 = \alpha(c^3) = \alpha(2) = 2\,.$$

Kuna $\mathbb{Q}(c) \subseteq \mathbb{R}$, siis peab $\alpha(c) = c$. Seega on α samasusteisendus ning $\Gamma(\mathbb{Q}(c) : \mathbb{Q}) = \{\alpha\}$.

Seome nüüd defineeritud korpuse laiendi Galois' rühma algebraliste võrrandite ja polünoomidega. Edasises me ei eelda enam polünoomi f taandumatust.

Definitsioon 3.1.12. Olgu $f(x) = 0$ algebraline võrrand kordajatega korpusest K. Olgu Σ polünoomi f lahutuskorpus üle K. Nii *võrrandi* $f(x) = 0$ *kui ka polünoomi* f *Galois' rühmaks* nimetame korpuse laiendi $\Sigma : K$ Galois' rühma $\Gamma(\Sigma : K)$.

Enne, kui kirjeldame eespool defineeritud rühma G (vt lk 62) ja võrrandi $f(x) = 0$ Galois' rühma $\Gamma(\Sigma : K)$ omavahelist seotust, tõestame järgneva lause.

Lause 3.1.13. *Olgu* $f(x) = 0$ *algebraline võrrand, kordajatega korpusest* K. *Siis selle võrrandi Galois' rühma elemendid teisendavad võrrandi lahendid võrrandi lahenditeks.*

Tõestus. Olgu Σ polünoomi f lahutuskorpus üle K ning olgu $\tau \in \Gamma(\Sigma : K)$ suvaline. Nüüd, kuna τ on K-automorfism korpusel Σ, siis võrrandi $f(x) = 0$ suvalise lahendi α_i korral,

$$0 = \tau(f(\alpha_i)) = f(\tau(\alpha_i)),$$

mistõttu $\tau(\alpha_i)$ on võrrandi $f(x) = 0$ mingi lahend. □

Lause 3.1.14. *Olgu* f *taandumatu polünoom üle korpuse* K, *mille aste olgu* n $(n > 0)$. *Olgu* Σ *tema lahutuskorpus (üle* K*). Siis võrrandi* $f(x) = 0$ *Galois' rühm* $\Gamma(\Sigma : K)$ *on isomorfne substitutsioonide rühma* $\mathbb{S}_n$ *alamrühmaga* G, *mis koosneb kõigist sellistest substitutsioonidest, mis jätavad invariantseks kõik võrrandi* $f(x) = 0$ *lahenditevahelised ratsionaalsed seosed üle* K.

Tõestus. Lause 3.1.7 põhjal on hulk G tõepoolest rühm. Teoreemi 2.2.7 põhjal on laiendi $\Sigma : K$ aste lõplik ning lause 2.2.3 põhjal

$$\Sigma = K(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

kus α_1, α_2, ..., α_n on polünoomi f kõik juured, mis on järelduse 2.2.6 põhjal paarikaupa erinevad. Järelduse 2.1.45 põhjal korpuse Σ suvaline element x avaldub kujul

$$x = p(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

kus p on mingi n muutuja polünoom üle K.

Defineerime nüüd iga $s \in G$ korral kujutuse $\phi_s : \Sigma \to \Sigma$ järgnevalt:

$$\phi_s(q(\alpha_1, \alpha_2, \ldots, \alpha_n)) = q(\alpha_{s_1}, \alpha_{s_2}, \ldots, \alpha_{s_n}), \tag{3.27}$$

kus $q \in K[x_1, x_2, ..., x_n]$.

Olgu $s \in G$ fikseeritud ning veendume, et kujutus ϕ_s on korrektselt defineeritud. Selleks olgu $q_1(\alpha_1, \alpha_2, ..., \alpha_n)$ ja $q_2(\alpha_1, \alpha_2, ..., \alpha_n)$ sellised suvalised elemendid ($q_1, q_2 \in K[x_1, x_2, ..., x_n]$) korpusest Σ, et

$$q_1(\alpha_1, \alpha_2, \ldots, \alpha_n) = q_2(\alpha_1, \alpha_2, \ldots, \alpha_n)\,.$$

Veendume, et kehtib võrdus

$$\phi_s(q_1(\alpha_1, \alpha_2, \ldots, \alpha_n)) = \phi_s(q_2(\alpha_1, \alpha_2, \ldots, \alpha_n))\,.$$

Selleks piisab aga näidata võrduse

$$q_1(\alpha_{s_1}, \alpha_{s_2}, \ldots, \alpha_{s_n}) = q_2(\alpha_{s_1}, \alpha_{s_2}, \ldots, \alpha_{s_n}) \tag{3.28}$$

kehtivust. Viimane võrdus kehtib, sest paneme tähele, et kuna

$$(q_1 - q_2)(\alpha_1, \alpha_2, \ldots, \alpha_n) = q_1(\alpha_1, \alpha_2, \ldots, \alpha_n) - q_2(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$$

on ratsionaalne seos üle K ja s kui hulga G element jätab selle muutumatuks, siis

$$(q_1 - q_2)(\alpha_{s_1}, \alpha_{s_2}, \ldots, \alpha_{s_n}) = 0\,,$$

ehk

$$q_1(\alpha_{s_1}, \alpha_{s_2}, \ldots, \alpha_{s_n}) - q_2(\alpha_{s_1}, \alpha_{s_2}, \ldots, \alpha_{s_n}) = 0\,,$$

millest järeldubki võrduse (3.28) kehtivus.

Lause tõestamiseks jääb nüüd veel näidata, et $\phi_s \in \Gamma(\Sigma : K)$ ning, et kujutus $\Phi : G \to \Gamma(\Sigma : K)$, mis on defineeritud võrdusega

$$\Phi(s) = \phi_s\,, \tag{3.29}$$

on rühmade G ja $\Gamma(\Sigma : K)$ isomorfism.

Veendume, et $\phi_s \in \Gamma(\Sigma : K)$. Selleks näitame kõigepealt, et ϕ_s on automorfism korpusel Σ. Selleks olgu $x = q_1(\alpha_1, \alpha_2, ..., \alpha_n)$ ja $y = q_2(\alpha_1, \alpha_2, ..., \alpha_n)$ suvalised elemendid ($q_1, q_2 \in K[x_1, x_2, ..., x_n]$) korpusest Σ ning tõestame kõigepealt, et

$$\begin{aligned}\phi_s(x + y) &= \phi_s(x) + \phi_s(y)\,,\\ \phi_s(xy) &= \phi_s(x)\phi_s(y)\,.\end{aligned}$$

Veendume neist esimese võrduse kehtivuses (teise võrduse kehtivust saab näidata analoogiliselt). Arvestades, kuidas on defineeritud kahe mitme muutuja polünoomi summa (vt [2], lk 255), saame, et

$$\begin{aligned}\phi_s(x + y) &= \phi_s(q_1(\alpha_1, \alpha_2, \ldots, \alpha_n) + q_2(\alpha_1, \alpha_2, \ldots, \alpha_n)) =\\ &= \phi_s((q_1 + q_2)(\alpha_1, \alpha_2, \ldots, \alpha_n)) = (q_1 + q_2)(\alpha_{s_1}, \alpha_{s_2}, \ldots, \alpha_{s_n}) =\\ &= q_1(\alpha_{s_1}, \alpha_{s_2}, \ldots, \alpha_{s_n}) + q_2(\alpha_{s_1}, \alpha_{s_2}, \ldots, \alpha_{s_n}) =\\ &= \phi_s(q_1(\alpha_1, \alpha_2, \ldots, \alpha_n)) + \phi_s(q_2(\alpha_1, \alpha_2, \ldots, \alpha_n)) = \phi_s(x) + \phi_s(y)\,.\end{aligned}$$

Veendume, et ϕ_s on bijektiivne. Selleks paneme tähele, et kuna G on rühm, siis $s^{-1} \in G$ ning seega on defineeritud kujutus $\phi_{s^{-1}}$. Paneme tähele, et kujutus $\phi_{s^{-1}}$ osutub kujutuse ϕ_s pöördkujutuseks. Suvalise elemendi $x = q(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \Sigma$ ($q \in K[x_1, x_2, ..., x_n]$) korral

$$\begin{aligned}(\phi_s\phi_{s^{-1}})(x) = (\phi_s\phi_{s^{-1}})(q(\alpha_1, \alpha_2, \ldots, \alpha_n)) = \phi_s(\phi_{s^{-1}}(q(\alpha_1, \alpha_2, \ldots, \alpha_n))) = \\ = \phi_s(q(\alpha_{s^{-1}{}_1}, \alpha_{s^{-1}{}_2}, \ldots, \alpha_{s^{-1}{}_n})) = q(\alpha_{s_{s^{-1}{}_1}}, \alpha_{s_{s^{-1}{}_2}}, \ldots, \alpha_{s_{s^{-1}{}_n}}) = \\ = q(\alpha_{ss^{-1}{}_1}, \alpha_{ss^{-1}{}_2}, \ldots, \alpha_{ss^{-1}{}_n}) = q(\alpha_1, \alpha_2, \ldots, \alpha_n) = x\,.\end{aligned}$$

Analoogiliselt võime veenduda, et ka $(\phi_{s^{-1}}\phi_s)(x) = x$. Seega, kuna kujutusel ϕ_s leidub pöördkujutus, siis ϕ_s on bijektiivne. Sellega oleme näidanud, et ϕ_s on automorfism korpusel Σ.

Kujutuse ϕ_s definitsioonist (3.27) järeldub aga vahetult, et ϕ_s on K-automorfism korpusel Σ ning seepärast $\phi_s \in \Gamma(\Sigma : K)$. (Korpuse K suvaline element k esitub kujul $q(\alpha_1, \alpha_2, ..., \alpha_n) = k$, $q \in K[x_1, x_2, ..., x_n]$, ning jääb seetõttu kujutuse ϕ_s rakendamisel invariantseks.)

Veendume nüüd, et kujutus $\Phi : G \to \Gamma(\Sigma : K)$, mis on defineeritud võrdusega (3.29), on rühmade isomorfism. Kujutus Φ on korrektselt defineeritud, sest kui substitutsioonid $s', s'' \in G$ on võrdsed, siis ka suvalise elemendi $q(\alpha_1, \alpha_2, ..., \alpha_n) \in \Sigma$ ($q \in K[x_1, x_2, ..., x_n]$) korral

$$\begin{aligned}\phi_{s'}(q(\alpha_1, \alpha_2, \ldots, \alpha_n)) = q(\alpha_{s'{}_1}, \alpha_{s'{}_2}, \ldots, \alpha_{s'{}_n}) = q(\alpha_{s''{}_1}, \alpha_{s''{}_2}, \ldots, \alpha_{s''{}_n}) = \\ = \phi_{s''}(q(\alpha_1, \alpha_2, \ldots, \alpha_n))\,,\end{aligned}$$

st, $\phi_{s'} = \phi_{s''}$ ehk $\Phi(s') = \Phi(s'')$.

Veendume, et Φ on rühmade homomorfism. Selleks näitame, et suvaliste substitutsioonide $s', s'' \in G$ korral $\Phi(s's'') = \Phi(s')\Phi(s'')$, ehk, $\phi_{s's''} = \phi_{s'}\phi_{s''}$. Selleks olgu $q(\alpha_1, \alpha_2, ..., \alpha_n) \in \Sigma$ suvaline element ($q \in K[x_1, x_2, ..., x_n]$). Leiame, et

$$\begin{aligned}(\phi_{s'}\phi_{s''})(q(\alpha_1, \alpha_2, \ldots, \alpha_n)) = \phi_{s'}(\phi_{s''}(q(\alpha_1, \alpha_2, \ldots, \alpha_n))) = \\ = \phi_{s'}(q(\alpha_{s''{}_1}, \alpha_{s''{}_2}, \ldots, \alpha_{s''{}_n})) = q(\alpha_{s'_{s''{}_1}}, \alpha_{s'_{s''{}_2}}, \ldots, \alpha_{s'_{s''{}_n}}) = \\ = q(\alpha_{s's''{}_1}, \alpha_{s's''{}_2}, \ldots, \alpha_{s's''{}_n}) = \phi_{s's''}(q(\alpha_1, \alpha_2, \ldots, \alpha_n))\,.\end{aligned}$$

Seega, tõepoolest kehtib võrdus $\phi_{s's''} = \phi_{s'}\phi_{s''}$ ning Φ on rühmade homomorfism.

Veendume, et Φ on injektiivne. Paneme tähele, et kui $s', s'' \in G$ ning $s' \neq s''$, siis $s'_i \neq s''_i$ mingi indeksi i korral, $i \in \{1, 2, ..., n\}$. Kuna polünoomi f juured on paarikaupa erinevad, siis ka $\alpha_{s'_i} \neq \alpha_{s''_i}$. Seega,

$$\phi_{s'}(\alpha_i) = \alpha_{s'_i} \neq \alpha_{s''_i} = \phi_{s''}(\alpha_i)\,,$$

mistõttu $\phi_{s'} \neq \phi_{s''}$ ehk $\Phi(s') \neq \Phi(s'')$ ning Φ on injektiivne.

Veendume nüüd, et Φ on ka sürjektiivne. Selleks olgu τ suvaline K-automorfism korpusel Σ. Lause 3.1.13 põhjal teisendab τ polünoomi f juured (mis on antud juhul paarikaupa erinevad)

$$\alpha_1,\, \alpha_2,\, \ldots,\, \alpha_n$$

vastavalt juurteks

$$\alpha_{\tau_1},\, \alpha_{\tau_2},\, \ldots,\, \alpha_{\tau_n}\,,$$

kutsudes seega esile juurte α_1, α_2, ..., α_n substitutsiooni

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \tau_1 & \tau_2 & \ldots & \tau_n \end{pmatrix}, \tag{3.30}$$

mida tähistame sümboliga s_τ. Veendume, et $s_\tau \in G$. Selleks olgu

$$p(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0 \tag{3.31}$$

suvaline ratsionaalne seos üle K ($p \in K(x_1, x_2, ..., x_n)$). Paneme tähele, et rakendades seosele (3.31) K-automorfismi τ, saame, et

$$0 = \tau(p(\alpha_1, \alpha_2, \ldots, \alpha_n)) = p(\tau(\alpha_1), \tau(\alpha_2), \ldots, \tau(\alpha_n)) = p(\alpha_{\tau_1}, \alpha_{\tau_2}, \ldots, \alpha_{\tau_n})\,,$$

mistõttu substitutsioon $s_\tau \in G$. Jääb veel näidata, et $\phi_{s_\tau} = \tau$. See aga järeldub vahetult, sest polünoomi f suvalise juure α_i korral ($i \in \{1, 2, ..., n\}$

$$\phi_{s_\tau}(\alpha_i) = \alpha_{\tau_i} = \tau(\alpha_i)$$

ning seega ka suvalise elemendi $q(\alpha_1, \alpha_2, ..., \alpha_n) \in \Sigma$ ($q \in K[x_1, x_2, ..., x_n]$) korral

$$\phi_{s_\tau}(q(\alpha_1, \alpha_2, \ldots, \alpha_n)) = q(\alpha_{\tau_1}, \alpha_{\tau_2}, \ldots, \alpha_{\tau_n}) = q(\tau(\alpha_1), \tau(\alpha_2), \ldots, \tau(\alpha_n)) = \\ = \tau(q(\alpha_1, \alpha_2, \ldots, \alpha_n))\,.$$

Sellega oleme näidanud, et elemendi $\tau \in \Gamma(\Sigma : K)$ originaal kujutuse Φ suhtes on substitutsioon (3.30) ning Φ on seega sürjektiivne, kujutades ühtlasi isomorfismi rühmade G ja $\Gamma(\Sigma : K)$ vahel. □

Lause 3.1.14 tõestuses näidatu põhjal võime taandumatu polünoomi f Galois' rühma all mõelda teatavat substitutsioonide rühma $\mathbb{S}_n$ alamrühma, millise alamrühma iga substitutsioon kutsub esile polünoomi f juurte teatava permutatsiooni. Polünoomi f Galois' rühma iga element on seejuures üheselt määratud sellega, milleks ta teisendab polünoomi f iga juure.

Näide 3.1.15. Leiame polünoomi $x^4 - x^2 - 2$ üle $\mathbb{Q}$ Galois' rühma. Vaadeldava polünoomi juured on i, $-i$, $\sqrt{2}$, $-\sqrt{2}$ ning lahutuskorpus on $\mathbb{Q}(i, \sqrt{2})$.

Vaatleme lihtlaiendite paari

$$\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})\,, \qquad \mathbb{Q}(\sqrt{2})(-i) : \mathbb{Q}(\sqrt{2})$$

ning paari

$$\mathbb{Q}(i)(\sqrt{2}) : \mathbb{Q}(i)\,, \qquad \mathbb{Q}(i)(-\sqrt{2}) : \mathbb{Q}(i)\,.$$

Vaadeldavate laiendite paaride määravad polünoomid on vastavalt x^2+1 üle $\mathbb{Q}(\sqrt{2})$ ja $x^2 - 2$ üle $\mathbb{Q}(i)$ (vt näide 2.1.40(2)). Järelduse 2.1.29 põhjal leidub selline $\mathbb{Q}$-automorfism α korpusel $\mathbb{Q}(\sqrt{2}, i)$, et

$$\alpha(i) = -i\,, \qquad \alpha(\sqrt{2}) = \sqrt{2}\,,$$

ning selline $\mathbb{Q}$-automorfism β korpusel $\mathbb{Q}(\sqrt{2}, i)$, et

$$\beta(i) = i\,, \qquad \beta(\sqrt{2}) = -\sqrt{2}\,.$$

Nummerdades vaadeldava polünoomi juured i, $-i$, $\sqrt{2}$, $-\sqrt{2}$ vastavalt numbritega 1, 2, 3, 4, võime lauset 3.1.14 kasutades[4] samastada omavahel automorfismi α ja substitutsiooni $a = (12)$ ning automorfismi β ja substitutsiooni $b = (34)$ (millised substitutsioonid on esitatud sõltumatute tsüklite korrutisena, vt näide 1.1.8). $\mathbb{Q}$-automorfismide α ja β korrutisele vastab substitutsioon $c = (12)(34)$. Samasusteisendusele korpusel $\mathbb{Q}(i, \sqrt{2})$ vastab ühiksubstitutsioon e. Seega koosneb vaadeldava polünoomi Galois' rühm vähemalt neljast elemendist, millisteks võib lugeda substitutsioonid a, b, c ja e. Rohkem aga sobivaid $\mathbb{Q}$-automorfisme ei leidu, sest kui γ oleks mingi $\mathbb{Q}$-automorfism korpusel $\mathbb{Q}(i, \sqrt{2})$, siis

$$(\gamma(i))^2 = \gamma(i^2) = \gamma(-1) = -1\,,$$

mis tähendab, et kas $\gamma(i) = i$ või $\gamma(i) = -i$. Analoogiliselt saame, et ka $\gamma(\sqrt{2}) = \sqrt{2}$ või $\gamma(\sqrt{2}) = -\sqrt{2}$, mistõttu peab γ olema üks juba leitud $\mathbb{Q}$-automorfismidest. Seega, substitutsioonide terminites, polünoomi $x^4 - x^2 - 2$ Galois' rühm on rühma $\mathbb{S}_4$ alamrühm $\{e, a, b, c\}$.

Galois avastas, et eksisteerib bijektiivne vastavus

- laiendi $\Sigma : K$ Galois' rühma alamrühmade

[4]Paneme tähele, et antud juhul ei ole polünoom f taandumatu üle $\mathbb{Q}$, sest $f = (x^2 + 1)(x^2 - 2)$. Lugeja võib aga lihtsasti kontrollida, et selles punktis toodud teooriaarendus, sh lause 3.1.14, taandumatu polünoomi f jaoks jääb kehtima kui asendada nõue, et f on taandumatu üle K nõudega, et f juured on paarikaupa erinevad ega kuulu korpusesse K.

ja

- korpuse Σ selliste alamkorpuste M, et $K \subseteq M$,

vahel. Veel enam, kui võrrand $f(x) = 0$ on lahenduv radikaalides, siis selle võrrandi Galois' rühm $\Gamma(\Sigma : K)$ peab rahuldama teatud tingimust. Osutub, et see tingimus on seejuures ka piisavaks tingimuseks.

Galois' teooria idee on seega siduda korpustega M, kus $K \subseteq M \subseteq \Sigma$, teatud rühmad ning taandada võrrandi $f(x) = 0$ radikaalides lahenduvuse küsimuse uurimine selle võrrandi Galois' rühma uurimisele.

3.2 Galois' teooria põhiteoreem

Oleme nüüdseks polünoomiga f üle K sidunud teatava korpuse Σ – tema lahutuskorpuse –, korpuse laiendi $\Sigma : K$ ning Galois' rühma[5] $\Gamma(\Sigma : K)$. Nagu eelmise punkti lõpus mainisime, eksisteerib bijektiivne vastavus rühma $\Gamma(\Sigma : K)$ alamrühmade ning korpuste M, $K \subseteq M \subseteq \Sigma$, vahel. Selles punktis defineerime selle vastavuse suvalise korpuse laiendi $L : K$ jaoks ning tõestame vastavuse bijektiivsuse kui L on mingi polünoomi lahutuskorpus üle K. (Mainitud vastavus ei tarvitse iga laiendi $L : K$ korral osutuda bijektiivseks.) Veel enam, uurime ka laiendi $L : K$ ja rühma $\Gamma(L : K)$ omavahelist seotust. Seda kirjeldab kokkuvõtlikult nn Galois' teooria põhiteoreem (vt lk 89, teoreem 3.2.32). See punkt ongi selle teoreemi tõestusele ning teoreemi põhjalikumale mõistmisele pühendatud. Galois' teooria põhiteoreemi kasutades anname hiljem võrrandite radikaalides lahenduvuse kriteeriumi (tarviliku ja piisava tingimuse).

3.2.1 Galois' vastavus

Alustame järgneva definitsiooniga.

Definitsioon 3.2.1. Olgu $L : K$ korpuse laiend. Nimetame iga korpust M, mille korral $K \subseteq M \subseteq L$, *vahekorpuseks* (*korpuste K ja L vahel*).

Vaatleme korpuse laiendit $L : K$. Igale vahekorpusele M korpuste K ja L vahel seame vastavusse rühma

$$M^* = \Gamma(L : M) \tag{3.32}$$

kõigist M-automorfismidest korpusel L. Seega K^* on laiendi $L : K$ Galois' rühm ning L^* koosneb vaid samasusteisendusest korpusel L.

[5]Eeldusel, et f on mittekonstantne polünoom, sest vastasel juhul ei saa me rääkida algebralisest võrrandist $f(x) = 0$ (vt [5], lk 222, definitsioon 7.1.3).

Vastupidi, rühma $\Gamma(L:K)$ igale alamrühmale H seame vastavusse hulga L alamhulga

$$H^\dagger = \{x \in L \,|\, \alpha(x) = x \;\; \forall \alpha \in H\}\,. \tag{3.33}$$

Tõestame nüüd siinkohal mõned tulemused äsja formuleeritud vastavuste kohta.

Lause 3.2.2. *Olgu $L:K$ korpuse laiend ning M ja N sellised vahekorpused, et $M \subseteq N$. Siis $M^* \supseteq N^*$. Samuti, kui H ja G on rühma $\Gamma(L:K)$ sellised alamrühmad, et $H \subseteq G$, siis $H^\dagger \supseteq G^\dagger$.*

Tõestus. Olgu $\alpha \in N^*$ suvaline. Siis rühma N^* definitsiooni tõttu $\alpha(x) = x$ iga $x \in N$ korral. Kuna $M \subseteq N$, siis ka $\alpha(x) = x$ iga $x \in M$ korral. See aga tähendab, et $\alpha \in M^*$, mistõttu $N^* \subseteq M^*$.

Tõestame nüüd lause teise väite. Olgu $x \in G^\dagger$ ning $\alpha \in H$ suvalised. Kuna $H \subseteq G$, siis $\alpha \in G$ ning seetõttu $\alpha(x) = x$. See aga tähendab, et $x \in H^\dagger$, mistõttu $G^\dagger \subseteq H^\dagger$. □

Lause 3.2.3. *Olgu $L:K$ korpuse laiend. Kui H on rühma $\Gamma(L:K)$ alamrühm, siis $H^\dagger$ on korpuse L alamkorpus, mis sisaldab korpust K.*

Tõestus. Olgu $x, y \in H^\dagger$, $\alpha \in H$ suvalised. Veendumaks, et $H^\dagger$ on korpuse L alamkorpus, tuleb näidata, et

1. $x + y \in H^\dagger$,
2. $-x \in H^\dagger$,
3. $xy \in H^\dagger$,
4. kui $x \neq 0$, siis $x^{-1} \in H^\dagger$.

Paneme tähele, et kuna $x, y \in H^\dagger$ ning kuna α on automorfism korpusel L, siis

$$\begin{aligned} \alpha(x+y) &= \alpha(x) + \alpha(y) = x + y\,, \\ \alpha(-x) &= -\alpha(x) = -x\,. \end{aligned}$$

See tähendab, et $x + y \in H^\dagger$ ning $-x \in H^\dagger$. Analoogiliselt võime veenduda, et kehtivad ka tingimused 3. ja 4.

Kuna $\alpha \in H \subseteq \Gamma(L:K)$, siis $\alpha(k) = k$ iga $k \in K$ korral. See aga tähendab, et $K \subseteq H^\dagger$. □

Lause 3.2.4. *Olgu $L:K$ korpuse laiend, M vahekorpus korpuste K ja L vahel ning H rühma $\Gamma(L:K)$ alamrühm. Siis*

$$\begin{aligned} M &\subseteq M^{*\dagger}\,, \\ H &\subseteq H^{\dagger *}\,. \end{aligned} \tag{3.34}$$

Tõestus. Olgu $x \in M$ suvaline. Siis, vastavalt rühma M^* definitsioonile (3.32), iga $\alpha \in M^*$ korral $\alpha(x) = x$. Hulga $M^{*\dagger}$ definitsioonist (3.33) järeldub nüüd, et $x \in M^{*\dagger}$, mistõttu $M \subseteq M^{*\dagger}$.

Olgu nüüd $\alpha \in H$ suvaline. Siis, vastavalt hulga $H^\dagger$ definitsioonile (3.33), iga $x \in H^\dagger$ korral $\alpha(x) = x$. See tähendab, et α on $H^\dagger$-automorfism korpusel L ehk $\alpha \in H^{\dagger *}$, mistõttu $H \subseteq H^{\dagger *}$. □

Sisalduvustele (3.34) vastupidised sisalduvused ei tarvitse kehtida. Näite 3.1.11(2) laiendi $\mathbb{Q}(c) : \mathbb{Q}$ korral näiteks

$$\mathbb{Q}^{*\dagger} = \mathbb{Q}(c) \neq \mathbb{Q}\,.$$

Tähistame laiendi $L : K$ kõigi vahekorpuste hulga tähega $\mathcal{K}$ ning Galois' rühma $\Gamma(L : K)$ kõigi alamrühmade hulga tähega $\mathcal{R}$. Defineerime kaks kujutust $^* : \mathcal{K} \to \mathcal{R}$ ja $^\dagger : \mathcal{R} \to \mathcal{K}$ seostega

$$^*(M) = M^*\,, \qquad ^\dagger(H) = H^\dagger\,, \tag{3.35}$$

kus $M \in \mathcal{K}$ ja $H \in \mathcal{R}$. Defineeritud kujutused kujutavad endast punkti alguses mainitud vastavust Galois' rühma $\Gamma(L : K)$ alamrühmade ning korpuste K ja L vahekorpuste vahel. Kui M on vahekorpus, siis lause 3.2.2 põhjal $M^* \subseteq K^* = \Gamma(L : K)$ ning kui $H \in \mathcal{R}$, siis lause 3.2.3 põhjal $H^\dagger \in \mathcal{K}$, mistõttu on definitsioon korrektne. Lausete 3.2.2 ja 3.2.4 põhjal on kujutustel * ja † järgmised omadused:

$$\begin{gathered}
M, N \in \mathcal{K},\ M \subseteq N \ \Rightarrow\ ^*(M) \supseteq\ ^*(N)\,,\\
H, G \in \mathcal{R},\ H \subseteq G \ \Rightarrow\ ^\dagger(H) \supseteq\ ^\dagger(G)\,,\\
M \subseteq\ ^\dagger(^*(M)) \quad \forall M \in \mathcal{K}\,,\\
H \subseteq\ ^*\left(^\dagger(H)\right) \quad \forall H \in \mathcal{R}\,.
\end{gathered}$$

Anname nüüd formaalse definitsiooni.

Definitsioon 3.2.5. Olgu $L : K$ korpuse laiend ning olgu kujutused $^* : \mathcal{K} \to \mathcal{R}$ ja $^\dagger : \mathcal{R} \to \mathcal{K}$ defineeritud võrdustega (3.35). Kujutused * ja † seavad omavahel vastavusse teatavad hulkade $\mathcal{K}$ ja $\mathcal{R}$ elemendid, millist vastavust me nimetame (*laiendi* $L : K$) *Galois' vastavuseks* (*alamrühmade ja vahekorpuste vahel*).

Osutub, et kui laiend $L : K$ on normaalne ja lõplik (st, kui L on mingi polünoomi lahutuskorpus üle K, vt teoreem 2.2.12), siis kujutused * ja † on bijektiivsed, kujutades seega teineteise pöördkujutusi. Teisisõnu, Galois' vastavus on sel juhul bijektiivne. Selle väite tõestamine ei ole enam niivõrd triviaalne ning meil tuleb eelnevalt uurida põhjalikumalt vahekorpuste ja alamrühmade omavahelist seotust. Seda me peagi hakkame tegema. Enne toome veel ühe näite.

Näide 3.2.6. Olgu vaatluse all meile juba tuttav polünoom x^4-x^2-2 üle $\mathbb{Q}$. Vaadeldava polünoomi juured on $x_1 = i$, $x_2 = -i$, $x_3 = \sqrt{2}$, $x_4 = -\sqrt{2}$ ning lahutuskorpus on $\mathbb{Q}(i, \sqrt{2})$. Näites 3.1.15 leidsime, et vaadeldava polünoomi Galois' rühm on isomorfne substitutsioonide rühma $\mathbb{S}_4$ alamrühmaga

$$G = \{e, a, b, c\},$$

kus e on ühiksubstitutsioon ning $a = (12)$, $b = (34)$, $c = (12)(34)$. Rühma G pärisalamrühmad on

$$\{e\}, \qquad \{e, a\}, \qquad \{e, b\}, \qquad \{e, c\}. \tag{3.36}$$

Näites 2.1.40(2) leidsime, et

$$\mathbb{Q}(i, \sqrt{2}) = \{p + q\sqrt{2} + ri + s\sqrt{2}i \,|\, p, q, r, s \in \mathbb{Q}\}.$$

Leiame alamrühmale $\{e, c\}$ vastava vahekorpuse. Vaadeldavasse alamrühma kuuluvad samasusteisendus ι ning $\mathbb{Q}$-automorfism α korpusel $\mathbb{Q}(i, \sqrt{2})$, mille korral $\alpha(i) = -i$ ning $\alpha(\sqrt{2}) = -\sqrt{2}$. Seega, suvalise $x = p + q\sqrt{2} + ri + s\sqrt{2}i \in \mathbb{Q}(i, \sqrt{2})$ korral $\iota(x) = x$ ning

$$\alpha(x) = \alpha(p) + \alpha(q)\alpha(\sqrt{2}) + \alpha(r)\alpha(i) + \alpha(s)\alpha(\sqrt{2})\alpha(i) = \\ = p - q\sqrt{2} - ri + s\sqrt{2}i.$$

Võrdus $\alpha(x) = x$ ehk

$$p + q\sqrt{2} + ri + s\sqrt{2}i = p - q\sqrt{2} - ri + s\sqrt{2}i \tag{3.37}$$

kehtib vaid siis kui $q = 0$ ja $r = 0$, sest näite 2.1.40(2) põhjal kujutas hulk $\{1, \sqrt{2}, i, \sqrt{2}i\}$ vektorruumi $\mathbb{Q}(i, \sqrt{2})$ üle $\mathbb{Q}$ baasi ning võrdus (3.37) on samaväärne alljärgneva nulliga võrduva lineaarkombinatsiooniga baasivektoritest 1, $\sqrt{2}$, i ja $\sqrt{2}i$:

$$0 \cdot 1 + 2q \cdot \sqrt{2} + 2r \cdot i + 0 \cdot \sqrt{2}i = 0. \tag{3.38}$$

Kuna baasivektorid on lineaarselt sõltumatud, siis peab $2q = 0$ ja $2r = 0$, mis on samaväärne, et $q = 0$ ja $r = 0$. Seega, alamrühmale $\{e, c\}$ vastav vahekorpus (korpuste $\mathbb{Q}$ ja $\mathbb{Q}(i, \sqrt{2})$ vahel) on $\mathbb{Q}(\sqrt{2}i)$.

Sarnaselt võime leida ka ülejäänud alamrühmadele (3.36) vastavad vahekorpused. Osutub, et alamrühmadele (3.36) vastavad vahekorpused on vastavalt

$$\mathbb{Q}(i, \sqrt{2}), \qquad \mathbb{Q}(\sqrt{2}), \qquad \mathbb{Q}(i), \qquad \mathbb{Q}(\sqrt{2}i). \tag{3.39}$$

Võime ka veenduda, et vahekorpustele (3.39) vastavad alamrühmad on vastavalt rühmad (3.36). Korpused (3.39) osutuvad koos korpusega $\mathbb{Q}$ (mis

on vastavuses Galois' rühmaga G) ka ainsateks vahekorpusteks korpuste $\mathbb{Q}$ ja $\mathbb{Q}(i,\sqrt{2})$ vahel, sest vahekorpuse M iga element on ühtlasi ka korpuse $\mathbb{Q}(i,\sqrt{2})$ element ning peab seetõttu esituma kas kujul $p+q\sqrt{2}+ri+s\sqrt{2}i$, $p+q\sqrt{2}$, $p+ri$, $p+s\sqrt{2}i$ või kujul p, kus elemendid $p,q,r,s\in\mathbb{Q}$ on suvalised (arvestame, et laiendi $\mathbb{Q}(i,\sqrt{2})$ aste on näite 2.1.40(2) põhjal 4, mistõttu lause 2.1.36 põhjal saab iga vahekorpuse M korral laiendi $M:K$ aste olla kas 1, 2 või 4). Vaadeldud elemendid kujutavad aga vastavalt korpuste (3.39) ja korpuse $\mathbb{Q}$ elemente. Seega, vaadeldav Galois' vastavus on bijektiivne.

3.2.2 Loendamise printsiibid

Galois' teooria põhiteoreemi tõestamiseks teeme suure osa tööd ära selles alapunktis.

Definitsioon 3.2.7. Olgu K ja L korpused ning olgu $\mu_i : K\to L$, $i\in\{1,2,...,n\}$, $n\in\mathbb{N}$, korpuste K ja L monomorfismid. Ütleme, et *monomorfismid μ_i, $i\in\{1,2,...,n\}$, on lineaarselt sõltumatud (üle L)*, kui iga $x\in K$ korral kehtivast võrdusest

$$a_1\mu_1(x)+a_2\mu_2(x)+\ldots+a_n\mu_n(x)=0\,, \tag{3.40}$$

kus $a_1,a_2,...,a_n\in L$, järeldub, et

$$a_1=a_2=\ldots=a_n=0\,. \tag{3.41}$$

Vastasel juhul, st, kui leiduvad $a_1,a_2,...,a_n\in L$ selliselt, et $a_i\neq 0$ mingi $i\in\{1,2,...,n\}$ korral ning, et iga $x\in K$ korral kehtib võrdus

$$a_1\mu_1(x)+a_2\mu_2(x)+\ldots+a_n\mu_n(x)=0\,,$$

nimetame *monomorfisme μ_i, $i\in\{1,2,...,n\}$, lineaarselt sõltuvateks (üle L)*.

Teoreem 3.2.8 (Dedekindi teoreem)**.** *Olgu K ja L korpused ning olgu $\mu_i : K\to L$, $i\in\{1,2,...,n\}$, $n\in\mathbb{N}$, korpuste K ja L monomorfismid, mis on paarikaupa erinevad. Siis monomorfismid μ_i, $i\in\{1,2,...,n\}$, on lineaarselt sõltumatud üle L.*

Tõestus. Tõestamiseks kasutame matemaatilise induktsiooni meetodit.

Induktsiooni baas. Olgu $n=1$. Kuna iga monomorfism $\mu : K\to L$ on injektiivne, siis ei saa kehtida $\mu(x)=0\ \forall x\in K$. Seega võrdus (3.40), kus $n=1$, saab iga $x\in K$ korral kehtida vaid siis kui $a_1=0$.

Induktsiooni samm. Eeldame nüüd, et $n\geq 2$ ning, et meie väide kehtib siis kui monomorfisme on vähem kui n, st, mistahes $n-1$ või vähem paarikaupa erinevat monomorfismi korpuste K ja L vahel on lineaarselt sõltumatud.

Oletame vastuväiteliselt, et paarikaupa erinevad monomorfismid $\mu_i : K \to L$, $i \in \{1, 2, ..., n\}$, on lineaarselt sõltuvad. St, eeldame, et leiduvad elemendid a_1, a_2, ..., $a_n \in L$, mis on kõik nullist erinevad (kui mõni neist oleks null, siis väide kehtiks induktsiooni eelduse tõttu), ning, et iga $x \in K$ korral kehtib võrdus (3.40).

Kuna $\mu_1 \neq \mu_n$, siis leidub $y \in K$, et

$$\mu_1(y) \neq \mu_n(y)\,. \tag{3.42}$$

Siit järeldub muuseas, et $\mu_1(y) \neq 0$, sest vastasel juhul peaks μ_1 injektiivsuse tõttu kehtima $y = 0$ ning siis samal põhjusel ka $\mu_n(y) = 0$. Sellisel juhul aga tingimus (3.42) ei saaks kehtida.

Nüüd võrdus (3.40) kehtib ka siis kui argumendiks on yx, st, iga $x \in K$ korral kehtib võrdus

$$a_1\mu_1(yx) + a_2\mu_2(yx) + \ldots + a_n\mu_n(yx) = 0\,.$$

Kuna μ_i, $i \in \{1, 2, ..., n\}$, on monomorfismid, siis

$$a_1\mu_1(y)\mu_1(x) + a_2\mu_2(y)\mu_2(x) + \ldots + a_n\mu_n(y)\mu_n(x) = 0\,. \tag{3.43}$$

Korrutame võrduse (3.40) pooli suurusega $\mu_1(y) \neq 0$ ning lahutame sellest võrduse (3.43). Saame, et

$$a_2\left[\mu_1(y) - \mu_2(y)\right]\mu_2(x) + \ldots + a_n\left[\mu_1(y) - \mu_n(y)\right]\mu_n(x) = 0\,. \tag{3.44}$$

Kuna $x \in K$ oli meil suvaline, siis kehtib saadud võrdus iga $x \in K$ korral. Paneme aga tähele, et võrduses (3.44) suuruse $\mu_n(x)$ kordaja on $a_n\left[\mu_1(y) - \mu_n(y)\right]$, mis meie eelduse $a_n \neq 0$ ja tingimuse (3.42) tõttu ei võrdu nulliga. Seega on monomorfismid μ_2, ..., μ_n lineaarselt sõltuvad üle L. See on aga vastuolus meie induktsiooni eeldusega. □

Näide 3.2.9. Olgu $K = \mathbb{Q}(i, \sqrt{2})$. Näites 2.1.40(2) veendusime, et korpuse K iga element esitub kujul $p + q\sqrt{2} + ri + s\sqrt{2}i$, kus kus $p, q, r, s \in \mathbb{Q}$. Näites 3.1.15 aga leidsime, et leidub neli monomorfismi $K \to \mathbb{C}$, nimelt

$$\begin{aligned}
\mu_1 &: p + q\sqrt{2} + ri + s\sqrt{2}i \;\mapsto\; p + q\sqrt{2} + ri + s\sqrt{2}i\,,\\
\mu_2 &: p + q\sqrt{2} + ri + s\sqrt{2}i \;\mapsto\; p + q\sqrt{2} - ri - s\sqrt{2}i\,,\\
\mu_3 &: p + q\sqrt{2} + ri + s\sqrt{2}i \;\mapsto\; p - q\sqrt{2} + ri - s\sqrt{2}i\,,\\
\mu_4 &: p + q\sqrt{2} + ri + s\sqrt{2}i \;\mapsto\; p - q\sqrt{2} - ri + s\sqrt{2}i\,.
\end{aligned}$$

Veendume, ilma teoreemi 3.2.8 kasutamata, et monomorfismid μ_1, μ_2, μ_3 ja μ_4 on lineaarselt sõltumatud üle $\mathbb{C}$. Olgu $a_1, a_2, a_3, a_4 \in \mathbb{C}$ suvalised ning iga $x \in K$ korral kehtigu võrdus

$$a_1\mu_1(x) + a_2\mu_2(x) + a_3\mu_3(x) + a_4\mu_4(x) = 0\,.$$

Valides $x = 1, i, \sqrt{2}, \sqrt{2}i$, saame vastavalt, et kehtivad võrdused

$$\begin{aligned} a_1 + a_2 + a_3 + a_4 &= 0\,, \\ a_1 - a_2 + a_3 - a_4 &= 0\,, \\ a_1 + a_2 - a_3 - a_4 &= 0\,, \\ a_1 - a_2 - a_3 + a_4 &= 0\,. \end{aligned} \tag{3.45}$$

Saime võrrandisüsteemi suuruste a_1, a_2, a_3 ja a_4 suhtes. Osutub, et saadud süsteemi ainsaks lahendiks on $a_1 = a_2 = a_3 = a_4 = 0$ (liites näiteks omavahel kõik võrrandid (3.45), saame, et $4a_1 = 0$ ehk $a_1 = 0$ ning liitmisvõtet edasi kasutades saame ka teised lahendid kätte). Definitsiooni 3.2.7 põhjal on monomorfismid μ_1, μ_2, μ_3 ja μ_4 lineaarselt sõltumatud.

Järgnevalt vajame kahte lauset. Neist esimese esitame ilma tõestuseta (tõestuse võib leida näiteks õpikust [5], lk 157, teoreem 5.4.5).

Lause 3.2.10. *Olgu K korpus ning $n > m$, kus $m, n \in \mathbb{N}$. Siis n tundmatuga ning m võrrandiga homogeensel lineaarvõrrandite süsteemil*

$$a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n = 0\,, \quad i \in \{1, 2, \ldots, m\}\,,$$

kus kordajad $a_{ij} \in K$, $i \in \{1, 2, ..., m\}$, $j \in \{1, 2, ..., n\}$, leidub mittetriviaalne lahend korpuses K (st, selline lahend $x^* = (x_1^*, x_2^*, ..., x_n^*)$, kus $x_j^* \in K$ iga $j \in \{1, 2, ..., n\}$ korral ning leidub selline indeks $k \in \{1, 2, ..., n\}$, et $x_k^* \neq 0$).

Lause 3.2.11. *Olgu G lõplik rühm elementidega g_1, g_2, ..., g_n. Olgu $g \in G$ suvaline. Siis elemendid gg_j, $j \in \{1, 2, ..., n\}$, on paarikaupa erinevad, kujutades ühtlasi rühma G kõiki elemente.*

Tõestus. Defineerime kujutuse $\phi : G \to G$ seosega $\phi(g_j) = gg_j$, kus $j \in \{1, 2, ..., n\}$. Kui $g_j = g_i$ mingite $i, j \in \{1, 2, ..., n\}$ korral, siis ka $gg_j = gg_i$, mistõttu ϕ on korrektselt defineeritud. Lause tõestuseks piisab näidata, et ϕ on bijektiivne.

Olgu $h \in G$ suvaline. Siis $g^{-1}h = g_j$ mingi $j \in \{1, 2, ..., n\}$ korral ning seega $h = gg_j$. See aga tähendab, et elemendi h originaal kujutuse ϕ suhtes on g_j ning ϕ on seega sürjektiivne.

Olgu nüüd $gg_i = gg_j$ mingite $i, j \in \{1, 2, ..., n\}$ korral. Siis

$$g_i = \left(g^{-1}g\right) g_i = g^{-1}(gg_i) = g^{-1}(gg_j) = \left(g^{-1}g\right) g_j = g_j\,,$$

mis tähendab, et ϕ on injektiivne ning ühtlasi ka bijektiivne. □

Teoreem 3.2.12. *Olgu K korpus, G korpuse K automorfismirühma lõplik alamrühm ning olgu*

$$K_0 = G^\dagger = \{x \in K \mid g(x) = x \ \ \forall g \in G\}\ .$$

Siis $[K : K_0] = |G|$.

Tõestus. Märgime kõigepealt, et kõik automorfismid moodustavad tõepoolest rühma teisenduste korrutamise suhtes (vt [5], lk 76, lause 2.6.5). Samuti, sarnaselt lause 3.2.3 tõestuskäiguga, võime veenduda, et hulk K_0 on korpuse K alamkorpus, mistõttu saame rääkida korpuse laiendist $K : K_0$ ja tema astmest $[K : K_0]$.

Olgu $|G| = n$ ning koosnegu rühm G elementidest g_1, g_2, ..., g_n, kus g_1 olgu samasusteisendus.

Esmalt oletame vastuväiteliselt, et $[K : K_0] = m < n$. Olgu $\{x_1, x_2, ..., x_m\}$ vektorruumi K üle K_0 baas. Lause 3.2.10 põhjal leiduvad elemendid $y_1, y_2, ..., y_n \in K$, mis ei ole kõik korraga nullid, nii, et kehtib

$$y_1 g_1(x_i) + y_2 g_2(x_i) + \ldots + y_n g_n(x_i) = 0\,, \quad i \in \{1, 2, \ldots, m\}\,. \tag{3.46}$$

Olgu $x \in K$ suvaline element. Siis

$$x = k_1 x_1 + k_2 x_2 + \ldots + k_m x_m\,,$$

kus $k_1, k_2, ..., k_m \in K_0$. Paneme nüüd aga tähele, et tingimuste (3.46) tõttu kehtib

$$\begin{aligned}
&y_1 g_1(x) + y_2 g_2(x) + \ldots + y_n g_n(x) = \\
&\quad = y_1 g_1\left(\sum_{i=1}^{m} k_i x_i\right) + y_2 g_2\left(\sum_{i=1}^{m} k_i x_i\right) + \ldots + y_n g_n\left(\sum_{i=1}^{m} k_i x_i\right) = \\
&\qquad = \sum_{i=1}^{m} y_1 g_1(k_i x_i) + \sum_{i=1}^{m} y_2 g_2(k_i x_i) + \ldots + \sum_{i=1}^{m} y_n g_n(k_i x_i) = \\
&\qquad = \sum_{i=1}^{m} k_i y_1 g_1(x_i) + \sum_{i=1}^{m} k_i y_2 g_2(x_i) + \ldots + \sum_{i=1}^{m} k_i y_n g_n(x_i) = \\
&\qquad\qquad = \sum_{i=1}^{m} k_i [y_1 g_1(x_i) + y_2 g_2(x_i) + \ldots + y_n g_n(x_i)] = 0\,.
\end{aligned} \tag{3.47}$$

Kuna y_1, y_2, ..., y_n ei ole kõik korraga nullid, siis tähendaks saadud võrdus (3.47) definitsiooni 3.2.7 põhjal seda, et paarikaupa erinevad monomorfismid g_1, g_2, ..., g_n on lineaarselt sõltuvad üle K. See on aga vastuolus teoreemiga 3.2.8. Seega peab $m \geq n$.

Oletame nüüd, et $[K : K_0] > n$. Sellisel juhul leidub vektorruumis K üle K_0 vähemalt $n+1$ elementi, mis on lineaarselt sõltumatud üle K_0. Olgu seega $\{x_1, x_2, ..., x_{n+1}\}$ lineaarselt sõltumatud vektorid vektorruumis K. Lause 3.2.10 põhjal leiduvad nüüd elemendid $y_1, y_2, ..., y_{n+1} \in K$, mis ei ole kõik korraga nullid, nii, et kehtib

$$y_1 g_i(x_1) + y_2 g_i(x_2) + \ldots + y_{n+1} g_i(x_{n+1}) = 0\,, \quad i \in \{1, 2, \ldots, n\}\,. \tag{3.48}$$

Valime elemendid $y_1, y_2, ..., y_{n+1} \in K$ selliselt, et neist võimalikult vähe oleksid nullist erinevad ning, et kehtiks tingimus (3.48). St, kasutades vajadusel ümbernummerdust, me valime sellised $y_1, y_2, ..., y_{n+1} \in K$, et kehtiks tingimus (3.48) ning

$$y_1 \neq 0\,,\ y_2 \neq 0\,,\ \ldots\,,\ y_r \neq 0\,, \qquad y_{r+1} = y_{r+2} = \ldots = y_{n+1} = 0\,,$$

kus r oleks võimalikult väike naturaalarv. Tingimus (3.48) saab sellisel juhul kuju

$$y_1 g_i(x_1) + y_2 g_i(x_2) + \ldots + y_r g_i(x_r) = 0\,,\ \ i \in \{1, 2, \ldots, n\}\,. \tag{3.49}$$

Olgu $g \in G$ suvaline ning rakendame automorfismi g võrdustele (3.49). Seda tehes saame järgnevad võrdused:

$$g(y_1)[gg_i](x_1) + g(y_2)[gg_i](x_2) + \ldots + g(y_r)[gg_i](x_r) = 0\,,\ \ i \in \{1, 2, \ldots, n\}\,. \tag{3.50}$$

Lause 3.2.11 põhjal on automorfismid gg_i, $i \in \{1, 2, ..., n\}$, paarikaupa erinevad, kujutades rühma G kõiki automorfisme. Võrdused (3.50) on seega samaväärsed võrdustega

$$g(y_1) g_i(x_1) + g(y_2) g_i(x_2) + \ldots + g(y_r) g_i(x_r) = 0\,,\ \ i \in \{1, 2, \ldots, n\}\,. \tag{3.51}$$

Korrutame nüüd võrduseid (3.49) elemendiga $g(y_1)$ (mis ei võrdu nulliga, sest g on automorfism ning $y_1 \neq 0$) ning võrduseid (3.51) elemendiga y_1. Seejärel lahutame iga $i \in \{1, 2, ..., n\}$ korral võrduste (3.49) i-ndast võrdusest võrduste (3.51) i-nda võrduse. Seda tehes saame, et

$$[y_2 g(y_1) - g(y_2) y_1] g_i(x_2) + \ldots + [y_r g(y_1) - g(y_r) y_1] g_i(x_r) = 0\,,\ \ i \in \{1, 2, \ldots, n\}\,. \tag{3.52}$$

Saadud võrdused (3.52) on võrdused nagu (3.49), kuid väiksema kordajate arvuga. See oleks aga vastuolus meie elementide y_1, y_2, ..., y_{n+1} valikuga, kui just kordajad

$$[y_j g(y_1) - g(y_j) y_1]\,,\ \ j \in \{2, 3, \ldots, r\}\,,$$

ei oleks kõik nullid. Kui vaadeldavad kordajad oleksid kõik nullid, siis peaks kehtima

$$g(y_j) y_1 = y_j g(y_1)\,,\ \ j \in \{2, 3, \ldots, r\}\,, \tag{3.53}$$

ehk, pärast elementidega $g(y_1)^{-1}$ ja y_1^{-1} läbikorrutamist,

$$g\left(y_j y_1^{-1}\right) = y_j y_1^{-1}\,,\ \ j \in \{2, 3, \ldots, r\}\,. \tag{3.54}$$

Kuna $g \in G$ oli suvaline, siis tähendavad tingimused (3.54) (koos triviaalselt kehtiva tingimusega $g\left(y_1 y_1^{-1}\right) = g(1) = 1 = y_1 y_1^{-1}$) seda, et $y_j y_1^{-1} \in K_0$,

$j \in \{1, 2, ..., r\}$. Seega leiduvad nullist erinevad elemendid $z_1, z_2, ..., z_r \in K_0$ ning nullist erinev element $k \in K$ nii, et $y_j = kz_j$, $j \in \{1, 2, ..., r\}$ ($z_j = y_j y_1^{-1}$, $j \in \{1, 2, ..., r\}$, ja $k = y_1$). Nüüd võrduste (3.49) esimene võrdus (kus g_1 oli meie kokkuleppe kohaselt samasusteisendus) saab kuju

$$kz_1x_1 + kz_2x_2 + \ldots + kz_rx_r = 0\,. \tag{3.55}$$

Kuna $k \neq 0$, siis võime võrduse (3.55) pooli läbi jagada elemendiga k, misjärel saame võrduse

$$z_1x_1 + z_2x_2 + \ldots + z_rx_r + 0 \cdot x_{r+1} + \ldots + 0 \cdot x_{n+1} = 0\,. \tag{3.56}$$

Kuna elemendid $z_1, z_2, ..., z_r \in K_0$ on nullist erinevad ning elemendid x_1, x_2, ..., x_{n+1} on lineaarselt sõltumatud üle K_0, siis ei saa võrdus (3.56) kehtida ning saame vastuolu meie oletusega, et $[K : K_0] > n$.

Sellega oleme näidanud, et $[K : K_0] \not> n$ ning ühtlasi ka, et $[K : K_0] = n = |G|$. □

Järeldus 3.2.13. *Olgu K ja L korpused, kusjuures $K \subseteq L$ ning laiend $L : K$ on lõplik. Olgu G laiendi $L : K$ Galois' rühm ning olgu H rühma G lõplik alamrühm. Siis*

$$[H^\dagger : K] = [L : K]/|H|\,.$$

Tõestus. Lause 3.2.3 põhjal on $H^\dagger$ korpuse L alamkorpus, mis omakorda sisaldab korpust K. Teoreemi 2.1.36 põhjal $[L : K] = [L : H^\dagger][H^\dagger : K]$, mistõttu $[H^\dagger : K] = [L : K]/[L : H^\dagger]$. Teoreemi 3.2.12 põhjal aga $[L : H^\dagger] = |H|$ ning meie väide on tõestatud. □

Näide 3.2.14.

1. Koosnegu rühm G automorfismidest α_1 ja α_2 korpusel $\mathbb{C}$, mis on defineeritud võrdustega

$$\alpha_1(x + yi) = x + yi\,,$$
$$\alpha_2(x + yi) = x - yi\,,$$

   $x, y \in \mathbb{R}$. Näites 3.1.11(1) veendusime, et α_1 ja α_2 on tõepoolest automorfismid korpusel $\mathbb{C}$.

   Paneme tähele, et $G^\dagger = \mathbb{R}$, sest $\alpha_2(x + yi) = x - yi = x + yi$ siis ja ainult siis kui $y = 0$. Teoreemi 3.2.12 põhjal seega $[\mathbb{C} : \mathbb{R}] = |G| = 2$, milline tulemus ühtib näite 2.1.34 tulemusega.

2. Olgu $L = \mathbb{Q}(i, \sqrt{2})$ ning vaatleme juba eelpooluuritud laiendit $L : \mathbb{Q}$. Näites 3.2.6 veendusime, et kehtib järgmine bijektiivne Galois' vastavus

$$\{e\} \leftrightarrow L\,, \qquad \{e, a\} \leftrightarrow \mathbb{Q}(\sqrt{2})\,, \qquad \{e, b\} \leftrightarrow \mathbb{Q}(i)\,,$$
$$\{e, c\} \leftrightarrow \mathbb{Q}(\sqrt{2}i)\,, \qquad G \leftrightarrow \mathbb{Q}\,,$$

kus $G = \{e, a, b, c\}$. Teoreemi 3.2.12 põhjal nüüd $[L : \mathbb{Q}] = |G| = 4$, milline tulemus ühtib meie poolt varem saadud tulemusega (vt näide 2.1.40(2)). Järelduse 3.2.13 põhjal

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [L : \mathbb{Q}]/2 = 2\,,$$
$$[\mathbb{Q}(i) : \mathbb{Q}] = [L : \mathbb{Q}]/2 = 2\,,$$
$$[\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}] = [L : \mathbb{Q}]/2 = 2\,,$$
$$[\mathbb{Q} : \mathbb{Q}] = [L : \mathbb{Q}]/4 = 1\,,$$

millised tulemused ilmselt kehtivad, kui arvestada, et laiendite $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$, $\mathbb{Q}(i) : \mathbb{Q}$ ja $\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}$ määravad polünoomid üle $\mathbb{Q}$ on vastavalt $x^2 - 2$, $x^2 + 1$ ja $x^2 + 2$ (vt lause 2.1.39).

Definitsioon 3.2.15. Olgu K, L ja M korpused, kusjuures $K \subseteq M \subseteq L$. Monomorfismi $\phi : M \to L$, mille korral $\phi(k) = k$ iga $k \in K$ korral, nimetame *K-monomorfismiks* (*korpusest M korpusesse L*).

Näide 3.2.16. Olgu $K = \mathbb{Q}$, $M = \mathbb{Q}(c)$, kus $c = \sqrt[3]{2} \in \mathbb{R}$, ning $L = \mathbb{C}$. Näites 2.1.40(1) veendusime, et korpuse M iga element esitub kujul $p+qc+rc^2$, kus $p, q, r \in K$. Defineerime kujutuse $\phi : M \to L$ selliselt, et $\phi(k) = k$ iga $k \in K$ korral ning, et $\phi(c) = c\omega$, kus $\omega = e^{2\pi i/3}$, st,

$$\phi : p + qc + rc^2 \mapsto p + qc\omega + rc^2\omega^2\,,$$

kus $p, q, r \in K$. Paneme tähele, et polünoom $x^3 - 2$ on nii lihtlaiendi $M : K$ kui ka lihtlaiendi $\mathbb{Q}(c\omega) : K$ määravaks polünoomiks. Seega, järelduse 2.1.29 põhjal kujutab ϕ endast isomorfismi korpuste M ja $\mathbb{Q}(c\omega)$ vahel, mis jätab seejuures korpuse K elemendid invariantseks. See aga tähendab, et ϕ on K-monomorfism korpusest M korpusesse L.

Teoreem 3.2.17. *Olgu $L : K$ lõplik normaallaiend ning olgu M vahekorpus (korpuste K ja L vahel). Olgu $\tau : M \to L$ suvaline K-monomorfism. Siis leidub K-automorfism $\sigma : L \to L$ nii, et $\sigma|_M = \tau$.*

Tõestus. Teoreemi 2.2.12 põhjal on L mingi polünoomi f lahutuskorpus üle K. Paneme tähele, et kuna $\tau|_K$ on samasusteisendus, siis $\hat{\tau}(f) = f$ (lause

2.1.30 tähistuses). Korpus L on nüüd ühtaegu ka polünoomi f lahutuskorpuseks üle korpuse M ja polünoomi $\hat{\tau}(f)$ lahutuskorpuseks üle $\tau(M)$. Piltlikult kirjeldab meil olukorda diagramm

$$\begin{array}{ccc} M & \to & L \\ \tau\downarrow & & \downarrow\sigma \\ \tau(M) & \to & L \end{array},$$

kus σ tuleb meil leida. Teoreemi 2.2.9 põhjal leidub isomorfism $\sigma : L \to L$ nii, et $\sigma|_M = \tau$. Seega, σ on automorfism korpusel L, ning kuna $\sigma|_K = \tau|_K$ on samasusteisendus, siis σ on K-automorfism korpusel L. □

Lause 3.2.18. *Olgu $L : K$ lõplik normaallaiend ning olgu p taandumatu polünoom üle K, mille juured α ja β kuuluvad korpusesse L. Siis leidub selline K-automorfism σ korpusel L, et $\sigma(\alpha) = \beta$.*

Tõestus. Olgu polünoom m üle K laiendi $K(\alpha) : K$ määrav polünoom. Lause 2.1.20 põhjal $m \mid p$ ning kuna p on taandumatu, siis peab m olema polünoomi p korpuse K elemendi kordne. Sama aruteluga saame, et laiendi $K(\beta) : K$ määrav polünoom on polünoomi p mingi korpuse K elemendi kordne. Kuna aga määrav polünoom on normeeritud, siis peavad laiendite $K(\alpha) : K$ ja $K(\beta) : K$ määravad polünoomid kokku langema.

Järelduse 2.1.29 põhjal leidub nüüd isomorfism $\tau : K(\alpha) \to K(\beta)$ nii, et $\tau|_K$ on samasusteisendus ning, et $\tau(\alpha) = \beta$. Nüüd $\tau : K(\alpha) \to L$ on K-monomorfism, mistõttu teoreemi 3.2.17 põhjal leidub selline K-automorfism σ korpusel L, et $\sigma|_{K(\alpha)} = \tau$. Sellisel juhul aga $\sigma(\alpha) = \tau(\alpha) = \beta$. □

Olgu $L : K$ lõplik korpuse laiend, mis ei ole normaalne. Meid huvitab sisalduvuse mõttes vähim selline korpus N, et $L \subseteq N$, ning et laiend $N : K$ on normaalne. See toob meid järgneva definitsiooni juurde.

Definitsioon 3.2.19. Olgu $L : K$ lõplik korpuse laiend. Laiendi $L : K$ *normaalsulundiks* nimetame sellist laiendit $N : K$, et

1. $L \subseteq N$,
2. laiend $N : K$ on normaalne,
3. kui korpus M on selline, et $L \subseteq M \subseteq N$, ning et laiend $M : K$ on normaalne, siis $M = N$.

Paneme tähele, et toodud definitsioonist järeldub vahetult, et kui lõplik laiend on normaalne, siis on ta iseenda normaalsulundiks.

Teoreem 3.2.20. *Olgu $L : K$ lõplik korpuse laiend. Siis laiendil $L : K$ leidub normaalsulund, mis on seejuures üheselt määratud ja lõplik laiend.*

Tõestus. Kuna laiend $L : K$ on lõplik, siis on L vektorruumina üle K lõplikumõõtmeline. Olgu $\{x_1, x_2, ..., x_r\}$ vektorruumi L üle K baas. Olgu m_j elemendi x_j minimaalne polünoom üle korpuse K, $j \in \{1, 2, ..., r\}$ (lause 2.1.44 põhjal on elemendid x_1, x_2, ..., x_r algebralised üle K, mistõttu nende minimaalsed polünoomid tõepoolest eksisteerivad). Olgu Σ polünoomi $f = m_1 m_2 ... m_r$ lahutuskorpus üle K. Paneme tähele, et kuna Σ sisaldab korpust K ja vektorruumi L üle K kõiki baasielemente, siis $L \subseteq \Sigma$.

Teoreemi 2.2.12 põhjal on laiend $\Sigma : K$ lõplik ja normaalne. Olgu korpus P selline, et $L \subseteq P \subseteq \Sigma$, ning et laiend $P : K$ on normaalne. Paneme tähele, et iga polünoom m_j, $j \in \{1, 2, ..., r\}$, omab juurt korpuses P. Kuna laiend $P : K$ on normaalne, siis polünoomid m_j, $j \in \{1, 2, ..., r\}$, lahutuvad lineaartegurite korrutiseks üle P, mistõttu ka polünoom f lahutub lineaartegurite korrutiseks üle P (vt normaalkorpuse definitsiooni 2.2.10). Kuna aga Σ on polünoomi f lahutuskorpus, siis peab $\Sigma = P$ (vt lahutuskorpuse definitsiooni 2.2.2). Sellega oleme näidanud, et $\Sigma : K$ on laiendi $L : K$ normaalsulundiks.

Olgu nüüd laiendid $M : K$ ja $N : K$ laiendi $L : K$ normaalsulunditeks. Et $L \subseteq M$ ja $L \subseteq N$, siis M ja N sisaldavad polünoomi f juuri (vektorruumi L üle K baasivektorid). Kuna aga laiendid $M : K$ ja $N : K$ on normaalsed, siis lahutub f lineaartegurite korrutiseks nii üle kopruse M kui ka üle korpuse N. See aga tähendab seda, et $\Sigma \subseteq M$ ja $\Sigma \subseteq N$. Definitsiooni 3.2.19 põhjal saame nüüd, et $M = \Sigma = N$. □

Näide 3.2.21. Vaatame laiendit $\mathbb{Q}(c) : \mathbb{Q}$, kus $c = \sqrt[3]{2} \in \mathbb{R}$. Näites 2.2.11(2) leidsime, et vaadeldav laiend ei ole normaalne. Olgu Σ polünoomi $x^3 - 2$ lahutuskorpus üle $\mathbb{Q}$. Lause 2.2.3 põhjal $\Sigma = \mathbb{Q}(c, c\omega, c\omega^2) = \mathbb{Q}(c, \omega)$, kus $\omega = (-1 + \sqrt{3}i)/2$ on kompleksarvuline 3. astme ühejuur. Teoreemi 2.2.12 põhjal on laiend $\Sigma : \mathbb{Q}$ normaalne. Paneme tähele, et $[\Sigma : \mathbb{Q}(c)] = 2$ (lihtlaiendi $\Sigma : \mathbb{Q}(c)$ määrav polünoom on $x^2 + cx + c^2$, sest kuna $\omega \notin \mathbb{Q}(c)$, siis on see polünoom taandumatu üle $\mathbb{Q}(c)$). Seega, kui K on mingi korpus korpuste Σ ja $\mathbb{Q}(c)$ vahel, siis

$$2 = [\Sigma : \mathbb{Q}(c)] = [\Sigma : K][K : \mathbb{Q}(c)]\,,$$

mis tähendab seda, et $[\Sigma : K] = 1$ või $[K : \mathbb{Q}(c)] = 1$. St, $K = \Sigma$ või $K = \mathbb{Q}(c)$. Tulemus ütleb meile seda, et laiend $\Sigma : \mathbb{Q}$ on laiendi $\mathbb{Q}(c) : \mathbb{Q}$ normaalsulundiks.

Edasises osutub meil vajalikuks teada järgmist tulemust.

Lause 3.2.22. *Olgu $L : K$ lõplik laiend ning olgu $N : K$ tema normaalsulundiks. Kui laiend $N' : K$, kus $L \subseteq N'$, on normaalne, siis $N \subseteq N'$.*

Tõestus. Viitame siinkohas teoreemi 3.2.20 tõestusele. Selles näidatu põhjal on laiend $\Sigma : K$, kus Σ on selle sama teoreemi tõestuses defineeritud polünoomi f lahutuskorpus üle K, laiendi $L : K$ normaalsulundiks. Ning, mainitud

teoreemi tõestuses kasutatud mõttekäike kasutades, võime ka veenduda, et kuna $L \subseteq N'$ ning kuna laiend $N' : K$ on normaalne, siis $N = \Sigma \subseteq N'$. □

Laiendite normaalsulundid aitavad meil seada piiranguid monomorfismi kujutisele.

Lause 3.2.23. *Olgu K, L, M ja N sellised korpused, et $K \subseteq L \subseteq N \subseteq M$, kus laiend $L : K$ on lõplik ning $N : K$ on laiendi $L : K$ normaalsulundiks. Olgu $\tau : L \to M$ mingi K-monomorfism. Siis $\tau(L) \subseteq N$.*

Tõestus. Kuna laiend $L : K$ on lõplik, siis lause 2.1.44 põhjal on $L : K$ algebraline laiend, mistõttu on L iga element algebraline üle K. Olgu $\alpha \in L$ suvaline ning olgu m elemendi α minimaalne polünoom üle K. Siis $m(\alpha) = 0$ ning seega ka $\tau(m(\alpha)) = 0$. Kuna aga τ on K-monomorfism, siis $\tau(m(\alpha)) = m(\tau(\alpha))$, st, $m(\tau(\alpha)) = 0$ ning $\tau(\alpha)$ on polünoomi m juur. Kuna laiend $N : K$ on normaalne, siis $\tau(\alpha) \in N$. Seega $\tau(L) \subseteq N$. □

Lause 3.2.24. *Olgu $L : K$ lõplik korpuse laiend ning olgu M selline korpus, et $L \subseteq M$. Kui $\tau : L \to M$ on selline K-monomorfism, et $\tau(L) \subseteq L$, siis τ on K-automorfism korpusel L.*

Tõestus. Tõestuseks piisab näidata, et $L = \tau(L)$, sest sellisel juhul on τ sürjektiivne ning on seetõttu K-automorfism korpusel L.

Paneme tähele, et hulk $\tau(L)$ on korpuse L alamkorpus (vt [5], lk 66, lause 2.5.3). Kuna $K \subseteq \tau(L)$, siis saame rääkida vektorruumist $\tau(L)$ üle K. Märkame ka, et $\tau : L \to \tau(L)$ on vektorruumide L üle K ja $\tau(L)$ üle K isomorfism. Vektorruumide isomorfism viib aga vektorruumi L baasi $\{x_1, x_2, ..., x_n\}$ ($n \in \mathbb{N}$) vektorruumi $\tau(L)$ baasiks $\{\tau(x_1), \tau(x_2), ..., \tau(x_n)\}$ (vt [5], lk 98, järeldus 3.4.4). Kuna aga $\tau(L) \subseteq L$, siis on $\{\tau(x_1), \tau(x_2), ..., \tau(x_n)\}$, kui n lineaarselt sõltumatut vektorit sisaldav hulk, n-mõõtmelise vektorruumi L baas. Siit järeldub nüüd, et $L \subseteq \tau(L)$ ning seega ka, et $L = \tau(L)$. Sellega oleme näidanud, et τ on K-automorfism korpusel L. □

Teoreem 3.2.25. *Olgu $L : K$ lõplik laiend. Siis järgmised väited on samaväärsed:*

1. *Laiend $L : K$ on normaalne.*
2. *Leidub selline lõplik normaallaiend $N : K$ ($L \subseteq N$), et iga K-monomorfism $\tau : L \to N$ on K-automorfism korpusel L.*
3. *Iga lõpliku laiendi $M : K$ ($L \subseteq M$) korral iga K-monomorfism $\tau : L \to M$ on K-automorfism korpusel L.*

Tõestus. Tõestamiseks näitame, et (1) ⇒ (3) ⇒ (2) ⇒ (1).

(1) ⇒ (3). Olgu laiend $L : K$ normaalne. Siis $L : K$ on ühtlasi ka laiendi $L : K$ normaalsulundiks. Olgu $M : K$ selline lõplik laiend, et $L \subseteq M$ ning olgu $\tau : L \to M$ suvaline K-monomorfism. Lause 3.2.23 põhjal $\tau(L) \subseteq L$ ning väide järeldub nüüd lausest 3.2.24.

(3) ⇒ (2). Teoreemi 3.2.20 põhjal leidub lõplik normaallaiend $N : K$ ($L \subseteq N$). Väide järeldub nüüd väitest (3).

(2) ⇒ (1). Olgu $N : K$ väites (2) kirjeldatud lõplik normaallaiend. Olgu f suvaline taandumatu polünoom üle K, millel leidub juur korpuses L. Olgu selleks juureks α. Kuna N on normaalkorpus, siis f lahutub lineaarteguriteks korrutiseks üle N. Kui nüüd β on polünoomi f mingi teine juur (mis kuulub korpusesse N), siis lause 3.2.18 põhjal leidub selline K-automorfism $\sigma : N \to N$, et $\sigma(\alpha) = \beta$. Paneme tähele, et $\sigma|_L : L \to N$ on K-monomorfism ning meie eelduse (2) tõttu on $\sigma|_L$ K-automorfism korpusel L, mistõttu $\beta = \sigma|_L(\alpha) \in L$. Kuna f oli suvaline taandumatu polünoom üle K ning β oli polünoomi f suvaline juur, siis L sisaldab polünoomi f kõik juured ning laiend $L : K$ on normaalne. □

Teoreem 3.2.26. *Olgu $L : K$ lõplik laiend, mille aste on n ning olgu $N : K$ tema normaalsulundiks. Siis leidub täpselt n erinevat K-monomorfismi korpusest L korpusesse N (ning ühtlasi ka igasse korpusesse M, kus $M : K$ on selline lõplik normaallaiend, et $L \subseteq M$).*

Tõestus. Tõestame väite matemaatilise induktsiooni meetodit kasutades laiendi $L : K$ astme järgi.

Induktsiooni baas. Olgu $[L : K] = 1$. Siis $L = K$. Kui nüüd $\tau : L \to N$ on K-monomorfism, siis peab ta tingimuse $K = L$ tõttu olema samasusteisendus korpusel L. Seega, leidub parajasti üks K-monomorfism korpusest L korpusesse N.

Induktsiooni samm. Eeldame nüüd, et $[L : K] = n > 1$, ning et väide kehtib iga korpuse laiendi korral, mille aste on väiksem kui n. Olgu $\alpha \in L \setminus K$ suvaline ning olgu m elemendi α minimaalne polünoom üle K (milline polünoom eksisteerib, sest laiend $L : K$ on lõplik ning lause 2.1.44 põhjal seega algebraline). Nüüd, lause 2.1.38 põhjal,

$$\deg m = [K(\alpha) : K] = r > 1\,. \tag{3.57}$$

Teoreemi 2.1.36 põhjal

$$[L : K] = [L : K(\alpha)][K(\alpha) : K]\,,$$

mistõttu, arvestades tingimust (3.57), saame, et laiendi $L : K(\alpha)$ astme s jaoks kehtib

$$s = [L : K(\alpha)] = \frac{[L : K]}{[K(\alpha) : K]} = \frac{n}{r} < n\,.$$

Olgu $M : K(\alpha)$ laiendi $L : K(\alpha)$ normaalsulund. Induktsiooni eelduse tõttu leidub täpselt s erinevat $K(\alpha)$-monomorfismi $\rho_j : L \to M$, $j \in \{1, 2, ..., s\}$. Kuna laiend $N : K$ on teoreemi 3.2.20 põhjal lõplik, siis lauset 2.1.43 kasutades saame, et ka laiend $N : K(\alpha)$ on lõplik. Kuna laiend $N : K$ on lõplik ja normaalne, siis teoreemi 2.2.12 põhjal on N mingi polünoomi f lahutuskorpus üle K. Paneme tähele, et kuna $K(\alpha) \subseteq L \subseteq N$, siis on N ka polünoomi f lahutuskorpus üle $K(\alpha)$. Jällegi teoreemi 2.2.12 kasutades, saame, et laiend $N : K(\alpha)$ on normaalne. Lause 3.2.22 põhjal aga sellisel juhul $M \subseteq N$. Nüüd, lausele 3.2.23 tuginedes, iga $K(\alpha)$-monomorfism korpusest L korpusesse N on ühtaegu $K(\alpha)$-monomorfism korpusest L korpusesse M. Seega leidub täpselt s erinevat $K(\alpha)$-monomorfismi korpusest L korpusesse N ning nendeks on monomorfismid ρ_j, $j \in \{1, 2, ..., s\}$.

Kuna elemendi α minimaalne polünoom m üle K on taandumatu üle K, siis järelduse 2.2.6 põhjal on m juured α_1, α_2, ..., α_r paarikaupa erinevad. Et $\alpha \in L \subseteq N$ ning N on normaalkorpus, siis polünoomi m kõik juured kuuluvad korpusesse N. Lause 3.2.18 põhjal leidub nüüd r sellist erinevat K-automorfismi $\tau_i : N \to N$, et $\tau_i(\alpha) = \alpha_i$, $i \in \{1, 2, ..., r\}$. Defineerime iga $i \in \{1, 2, ..., r\}$ ja iga $j \in \{1, 2, ..., s\}$ korral kujutuse $\phi_{ij} : L \to N$ võrdusega

$$\phi_{ij} = \tau_i \rho_j \, .$$

Et kahe homomorfismi korrutis on homomorfism ning kahe injektiivse kujutuse korrutis on injektiivne kujutus, siis ϕ_{ij} on monomorfism. Sarnaselt lause 3.1.9 tõestuses tooduga võib aga veenduda, et kujutus ϕ_{ij} osutub koguni K-monomorfismiks. Kujutused ϕ_{ij} on ka paarikaupa erinevad. Kui $i_1 \neq i_2$, $i_1, i_2 \in \{1, 2, ..., r\}$, siis suvaliste $j_1, j_2 \in \{1, 2, ..., s\}$ korral

$$\phi_{i_1 j_1}(\alpha) = \tau_{i_1}(\rho_{j_1}(\alpha)) = \tau_{i_1}(\alpha) = \alpha_{i_1} \neq \alpha_{i_2} = \tau_{i_2}(\alpha) = \tau_{i_2}(\rho_{j_2}(\alpha)) = \phi_{i_2 j_2}(\alpha) \, .$$

St, $\phi_{i_1 j_1} \neq \phi_{i_2 j_2}$, kui $i_1 \neq i_2$. Kui aga $i_1 = i_2 = i$, $i \in \{1, 2, ..., r\}$, siis juhul kui $j_1 \neq j_2$, kus $j_1, j_2 \in \{1, 2, ..., s\}$, leidub tingimuse $\rho_{j_1} \neq \rho_{j_2}$ tõttu element $x \in L$ nii, et $\rho_{j_1}(x) \neq \rho_{j_2}(x)$. Siis aga, kuna kujutused τ_i, $i \in \{1, 2, ..., r\}$, on injektiivsed, kehtib

$$\phi_{ij_1}(x) = \tau_i(\rho_{j_1}(x)) \neq \tau_i(\rho_{j_2}(x)) = \phi_{ij_2}(x) \, .$$

St, $\phi_{ij_1} \neq \phi_{ij_2}$, kui $j_1 \neq j_2$. Sellega oleme näidanud, et kujutused ϕ_{ij} on paarikaupa erinevad. Seega leidub vähemalt $rs = n$ erinevat K-monomorfismi $L \to N$.

Olgu $\tau : L \to N$ suvaline K-monomorfism. Siis $0 = \tau(m(\alpha)) = m(\tau(\alpha))$, mis tähendab, et $\tau(\alpha) \in N$ on polünoomi m juur ning seega $\tau(\alpha) = \alpha_i$ mingi $i \in \{1, 2, ..., r\}$ korral. Defineerime kujutuse $\phi : L \to N$ seosega $\phi = \tau_i^{-1}\tau$. Kuna $\tau_i : N \to N$ on K-automorfism, siis leidub tal tõepoolest pöördkujutus,

mis osutub samuti K-automorfismiks (vt lause 3.1.9) ning kujutus ϕ on seega korrektselt defineeritud ning on K-monomorfism. Paneme aga tähele, et

$$\phi(\alpha) = \tau_i^{-1}(\tau(\alpha)) = \tau_i^{-1}(\alpha_i) = \alpha\,,$$

mistõttu ka $\phi(x) = x$ iga $x \in K(\alpha)$ korral ning ϕ on seega $K(\alpha)$-monomorfism. Eelnevalt põhjendasime, et ainsad $K(\alpha)$-monomorfismid $L \to N$ on monomorfismid ρ_j, $j \in \{1, 2, ..., s\}$. Seega $\phi = \rho_j$ mingi $j \in \{1, 2, ..., s\}$ korral. Nüüd aga paneme tähele, et

$$\tau = \left(\tau_i\tau_i^{-1}\right)\tau = \tau_i\left(\tau_i^{-1}\tau\right) = \tau_i\phi = \tau_i\rho_j = \phi_{ij}\,.$$

Seega, $\tau : L \to N$ on üks K-monomorfism meie poolt eelnevalt konstrueeritud rs K-monomorfismi seast, mistõttu leidub täpselt $n = rs$ K-monomorfismi korpusest L korpusesse N.

Kui nüüd $M : K$ on selline lõplik normaallaiend, et $L \subseteq M$, siis lause 3.2.22 põhjal $N \subseteq M$. Nüüd lause 3.2.23 põhjal iga K-monomorfism $L \to M$ on K-monomorfism $L \to N$ ning eeltõestatu põhjal on neid täpselt n tükki. □

Oleme nüüd valmis arvutama lõpliku normaallaiendi Galois' rühma järku.

Järeldus 3.2.27. *Olgu $L : K$ lõplik normaallaiend. Siis leidub täpselt $[L : K]$ erinevat K-automorfismi korpusel L, st,*

$$|\Gamma(L : K)| = [L : K]\,.$$

Tõestus. Kuna laiend $L : K$ on normaalne, siis on ta ka ühtlasi iseenda normaalsulundiks. Teoreemi 3.2.26 põhjal leidub täpselt $n = [L : K]$ erinevat K-monomorfismi $L \to L$. Lause 3.2.24 põhjal on aga need K-monomorfismid K-automorfismid korpusel L. □

Teoreem 3.2.28. *Olgu $L : K$ lõplik laiend, mille Galois' rühm on G. Kui $L : K$ on normaalne, siis $G^\dagger = K$.*

Tõestus. Olgu $G^\dagger = K_0$ ning olgu $[L : K] = n$. Järelduse 3.2.27 põhjal $|G| = n$. Lause 3.2.3 põhjal on K_0 korpuse L alamkorpus, mis sisaldab korpust K. Teoreemi 3.2.12 põhjal $[L : K_0] = n$. Nüüd, lauset 2.1.36 kasutades saame, et

$$n = [L : K] = [L : K_0][K_0 : K] = n[K_0 : K]\,,$$

st, $[K_0 : K] = 1$. Tulemus ütleb meile seda, et $K_0 = K$. □

Sellele teoreemile leidub ka pöördteoreem. Enne selle toomist vajame aga järgnevat teoreemi.

Teoreem 3.2.29. *Olgu K, L ja M sellised korpused, et $K \subseteq L \subseteq M$ ning, et laiend $M : K$ on lõplik. Siis erinevate K-monomorfismide arv korpusest L korpusesse M on ülimalt $[L : K]$.*

Tõestus. Paneme kõigepealt tähele, et lause 2.1.43 põhjal on laiendi $L : K$ aste lõplik. Teoreemi 3.2.20 põhjal leidub laiendi $L : K$ jaoks üheselt määratud normaalsulund, mis on lõplik. Olgu selleks laiend $N : K$. Teoreemi 3.2.26 põhjal leidub täpselt $n = [L : K]$ erinevat K-monomorfismi korpusest L korpusesse N ning ühtlasi ka igasse korpusesse M', kus $M' : K$ on selline lõplik normaallaiend, et $L \subseteq M'$. Olgu $M' : K$ laiendi $M : K$ normaalsulundiks. Teoreemi 3.2.20 põhjal on laiendi $M' : K$ aste lõplik. Kuna ka $L \subseteq M \subseteq M'$, siis eelöeldu põhjal leidub täpselt n erinevat K-monomorfismi korpusest L korpusesse M'. Kui aga $\phi : L \to M$ on K-monomorfism, siis tingimuse $M \subseteq M'$ tõttu on ϕ ühtlasi ka K-monomorfism korpusest L korpusesse M'. Selliseid K-monomorfisme ei saa seega olla rohkem kui n. □

Teoreem 3.2.30. *Olgu $L : K$ lõplik laiend ning olgu G tema Galois' rühm. Kui $G^\dagger = K$, siis laiend $L : K$ on normaalne.*

Tõestus. Olgu laiendi $L : K$ aste n. Kuna iga K-automorfism korpusel L on ühtlasi ka K-monomorfism korpusest L korpusesse L, siis teoreemi 3.2.29 põhjal ei saa K-automorfismide arv korpusel L olla suurem kui n. St, $|G|$ on lõplik. Teoreemi 3.2.12 põhjal aga siis $|G| = [L : G^\dagger] = [L : K] = n$.

Laiendi $L : K$ normaalsus järeldub nüüd vahetult teoreemist 3.2.25. Kui $M : K$ on mingi selline lõplik laiend, et $L \subseteq M$, siis teoreemi 3.2.29 põhjal ei saa erinevate K-monomorfismide arv korpusest L korpusesse M olla suurem kui n. Kuid, laiendi $L : K$ Galois' rühma kõik n elementi on ühtlasi K-monomorfismid $L \to M$. Seega, iga K-monomorfism $L \to M$ on K-automorfism korpusel L ning teoreemi 3.2.25 põhjal on laiend $L : K$ seega normaalne. □

3.2.3 Põhiteoreemi tõestus

Oleme nüüd valmis tõestama meie edasise teooriaarenduse seisukohalt olulist Galois' teooria põhiteoreemi. Suurem osa tööst on meil tegelikult juba tehtud. Siin osas "paneme vaid tükid kokku".

Meenutame siinkohal mõningaid eelnevalt kasutatud tähistusi ja tõestatud tulemusi. Olgu $L : K$ korpuse laiend, mille Galois' rühm on G, milline rühm kooseb kõigist K-automorfismidest korpusel L. Sümboliga $\mathcal{K}$ tähistasime kõigi vahekorpuste hulka, st, hulk $\mathcal{K}$ koosneb kõigist sellistest korpustest M, mille korral $K \subseteq M \subseteq L$. Sümboliga $\mathcal{R}$ tähistasime Galois' rühma G kõigi

alamrühmade hulka. Me defineerisime kaks kujutust (vt (3.35))

$$^* : \mathcal{K} \to \mathcal{R}\,,$$
$$^\dagger : \mathcal{R} \to \mathcal{K}\,,$$

järgnevalt: $^*(M) = M^*$ ning $^\dagger(H) = H^\dagger$, kus $M \in \mathcal{K}$ ja $H \in \mathcal{R}$. Näitasime ka, et kujutustel * ja † on järgmised omadused (vt laused 3.2.2 ja 3.2.4):

$$M, N \in \mathcal{K},\ M \subseteq N \ \Rightarrow\ ^*(M) \supseteq\ ^*(N)\,,$$
$$H, G \in \mathcal{R},\ H \subseteq G \ \Rightarrow\ ^\dagger(H) \supseteq\ ^\dagger(G)\,,$$
$$M \subseteq\ ^\dagger(^*(M)) \quad \forall M \in \mathcal{K}\,,$$
$$H \subseteq\ ^*\left(^\dagger(H)\right) \quad \forall H \in \mathcal{R}\,.$$

Enne kui asume Galois' teooria põhiteoreemi tõestuse juurde, tõestame veel ühe abitulemuse.

Lause 3.2.31. *Olgu $L : K$ lõplik korpuse laiend, M vahekorpus ning $\tau : L \to L$ suvaline K-automorfism. Siis $(\tau(M))^* = \tau M^* \tau^{-1}$.*

Tõestus. Tähistame järgnevas $M' = \tau(M)$. Märgime siinjuures, et hulk M' on korpus (vt [5], lk 66, lause 2.5.3), mis sisaldab korpust K, sest $\tau|_K = K$. Seega omab kirjutis $(M')^*$ mõtet.

Olgu $\gamma \in M^*$ ja $x_1 \in M'$ suvalised. Siis $x_1 = \tau(x)$ mingi $x \in M$ korral. Paneme tähele, et nüüd

$$(\tau\gamma\tau^{-1})(x_1) = (\tau\gamma)(\tau^{-1}(x_1)) = (\tau\gamma)(x) = \tau(\gamma(x)) = \tau(x) = x_1\,,$$

mistõttu $\tau\gamma\tau^{-1} \in (M')^*$. Kuna $\gamma \in M^*$ oli suvaline, siis $\tau M^* \tau^{-1} \subseteq (M')^*$.

Olgu nüüd $\gamma \in (M')^*$ ja $x \in M$ suvalised. Olgu $x_1 = \tau(x)$. Paneme tähele, et siis $x_1 \in M'$ ja

$$(\tau^{-1}\gamma\tau)(x) = (\tau^{-1}\gamma)(\tau(x)) = (\tau^{-1}\gamma)(x_1) = \tau^{-1}(\gamma(x_1)) = \tau^{-1}(x_1) = x\,,$$

mistõttu $\tau^{-1}\gamma\tau \in M^*$. Kuna $\gamma \in (M')^*$ oli suvaline, siis $\tau^{-1}\,(M')^*\,\tau \subseteq M^*$, millest järeldub, et $(M')^* \subseteq \tau M^* \tau^{-1}$.

Sellega oleme näidanud, et $(\tau(M))^* = \tau M^* \tau^{-1}$. □

Teoreem 3.2.32 (Galois' teooria põhiteoreem)**.** *Olgu $L : K$ lõplik normaallaiend, mille Galois' rühm on G ning olgu $\mathcal{K}$, $\mathcal{R}$, * ja † defineeritud nagu antud punkti sissejuhtavas tekstis. Siis*

1. *Galois' rühma G järk on $[L : K]$.*
2. *Kujutused * ja † on teineteise pöördkujutused, mistõttu laiendi $L : K$ Galois' vastavus on bijektiivne. Teisisõnu, hulkade $\mathcal{K}$ ja $\mathcal{R}$ elementide vahel on bijektiivne vastavus.*

3. *Kui M on vahekorpus, siis*

$$[L : M] = |M^*|\,, \qquad [M : K] = |G|/|M^*|\,.$$

4. *Laiend $N : M$, kus N ja M on vahekorpused ($M \subseteq N$), on normaalne siis ja ainult siis kui N^* on rühma M^* normaalne alamrühm.*

5. *Kui laiend $N : M$, kus N ja M on vahekorpused ($M \subseteq N$), on normaalne, siis laiendi $N : M$ Galois' rühm on isomorfne faktorrühmaga M^*/N^*.*

Tõestus. 1. Väide on järeldus 3.2.27.

2. Olgu $M \in \mathcal{K}$ suvaline vahekorpus. Kuna laiend $L : K$ on lõplik ja normaalne, siis teoreemi 2.2.12 põhjal on L mingi polünoomi lahutuskorpus üle K. Kuna M on vahekorpus, siis on L selle sama polünoomi lahutuskorpus ka üle M, mistõttu sama teoreemi 2.2.12 põhjal on laiend $L : M$ lõplik ja normaalne. Nüüd, kuna M^* on laiendi $L : M$ Galois' rühm, siis teoreemi 3.2.28 põhjal

$$M = M^{*\dagger}\,. \tag{3.58}$$

Olgu nüüd $H \in \mathcal{R}$ suvaline. Võrduse (3.58) põhjal (arvestades, et kujutuste järjestrakendamine on assotsiatiivne) $H^{\dagger *\dagger} = \left(H^\dagger\right)^{*\dagger} = H^\dagger$. Kuna H on lõpliku rühma (vt väide 1) alamrühm, siis on ta lõplik ning teoreemi 3.2.12 kasutades, $|H| = [L : H^\dagger] = [L : H^{\dagger *\dagger}]$. Kasutades uuesti teoreemi 3.2.12, seekord rühma $H^{\dagger *}$ jaoks, saame et $[L : H^{\dagger *\dagger}] = |H^{\dagger *}|$. Seega, $|H| = [L : H^{\dagger *\dagger}] = |H^{\dagger *}|$. Kuna aga H ja $H^{\dagger *}$ on lõplikud rühmad ning $H \subseteq H^{\dagger *}$, siis peab kehtima võrdus $H = H^{\dagger *}$. Sellega oleme teise väite tõestanud.

3. Olgu M vahekorpus. Väites 2 juba põhjendasime, et laiend $L : M$ on normaalne ja lõplik. Järelduse 3.2.27 põhjal $[L : M] = |M^*|$. Teoreemi 2.1.36 põhjal

$$[L : K] = [L : M][M : K]\,,$$

mistõttu

$$[M : K] = [L : K]/[L : M]$$

ehk, arvestades väidet 1, $[M : K] = |G|/|M^*|$.

4. Lause 2.1.43 põhjal on laiend $N : M$ lõplik. Paneme veel tähele, et lause 3.2.2 põhjal on N^* rühma M^* alamrühm.

Tarvilikkus. Olgu laiend $N : M$ normaalne, $K \subseteq M \subseteq N \subseteq L$. Veendume, et N^* on ka rühma M^* normaaljagaja. Olgu $\tau \in M^*$ suvaline.

Tarvilikkuse osa tõestuseks piisab näidata, et $\tau N^*\tau^{-1} = N^*$. Paneme tähele, et $\tau|_N : N \to L$ on M-monomorfism. Teoreemi 3.2.25 põhjal on $\tau|_N$ M-automorfism korpusel N (teoreemi 3.2.25 kasutades on meil korpuse K rollis korpus M, korpuse L rollis korpus N ning korpuse M rollis korpus L), st $\tau(N) = N$. Lause 3.2.31 põhjal nüüd $N^* = \tau N^*\tau^{-1}$.

Piisavus. Eeldame, et N^* on rühma M^* normaaljagaja. Tõestamaks, et laiend $N : M$ on normaalne, kasutame jällegi teoreemi 3.2.25. Selleks olgu $\sigma : N \to L$ suvaline M-monomorfism ning näitame, et σ on tegelikult M-automorfism korpusel N. Teoreemi 3.2.25 põhjal saame siis, et laiend $N : M$ on normaalne. Teoreemi 3.2.17 põhjal leidub M-automorfism $\tau : L \to L$ ($\tau \in M^*$) nii, et $\tau|_N = \sigma$. Kuna N^* on rühma M^* normaaljagaja, siis $\tau N^*\tau^{-1} = N^*$. Lauset 3.2.31 kasutades saame nüüd, et $(\tau(N))^* = N^*$ ning antud teoreemi 2. väite põhjal saame seega, et

$$N = (N^*)^\dagger = ((\tau(N))^*)^\dagger = \tau(N)\,.$$

Seega $\sigma(N) = (\tau|_N)(N) = \tau(N) = N$, mistõttu σ on M-automorfism korpusel N.

5. Olgu laiend $N : M$ normaalne, $K \subseteq M \subseteq N \subseteq L$. Olgu G' laiendi $N : M$ Galois' rühm. Defineerime kujutuse $\phi : M^* \to G'$ võrdusega

$$\phi(\tau) = \tau|_N\,,$$

kus $\tau \in M^*$. Teoreemi 3.2.25 põhjal on $\tau|_N$ M-automorfism korpusel N, mistõttu on kujutus ϕ korrektselt defineeritud. Nüüd suvaliste $\tau_1, \tau_2 \in M^*$ ja suvalise $x \in N$ korral

$$\begin{aligned}\phi(\tau_1\tau_2)(x) = ((\tau_1\tau_2)|_N)(x) = (\tau_1\tau_2)(x) = \tau_1(\tau_2(x)) = \\ = \tau_1|_N(\tau_2|_N(x)) = \tau_1|_N(\phi(\tau_2(x))) = \phi(\tau_1)(\phi(\tau_2(x))) = \\ = (\phi_1(\tau_1)\phi_2(\tau_2))(x)\,,\end{aligned}$$

st, $\phi(\tau_1\tau_2) = \phi(\tau_1)\phi(\tau_2)$, mistõttu ϕ on rühmade M^* ja G' homomorfism. Olgu $\sigma \in G'$ suvaline. Paneme tähele, et $\sigma : N \to L$ on M-monomorfism. Teoreemi 3.2.17 põhjal leidub selline M-automorfism $\tau : L \to L$, et $\tau|_N = \sigma$ (teoreemis 3.2.17 on meil laiendi $L : K$ rollis laiend $L : M$, mis on samuti lõplik ja normaalne, korpuse M rollis on korpus N). Teisisõnu, leidub selline $\tau \in M^*$, et $\phi(\tau) = \tau|_N = \sigma$, mis tähendab, et ϕ on sürjektiivne. Paneme veel tähele, et tingimuse $N^* \subseteq M^*$ tõttu kujutuse ϕ tuum

$$\ker\phi = \{\tau \in M^* \,|\, \tau|_N = I_N\} = \{\tau \in M^* \,|\, \tau(x) = x \;\; \forall x \in N\} = N^*\,,$$

kus $I_N \in G'$ on samasusteisendus korpusel N. Rühmade homomorfismiteoreemi (vt [5], lk 171, järeldus 6.2.5) põhjal nüüd

$$\Gamma(N:M) = G' \cong M^*/\ker\phi = M^*/N^*\,. \qquad \square$$

3.2.4 Selgitav näide

Galois' teooria põhiteoreemi 3.2.32 paremaks mõistmiseks esitame selles punktis ühe mahukama näite. Vaatluse all on meil polünoom x^4-2 üle korpuse $\mathbb{Q}$. Arutlus on selgema ülevaate eesmärgil jaotatud alapunktideks.

1. Tähistame $f = x^4-2 \in \mathbb{Q}[x]$ ning olgu Σ vaadeldava polünoomi lahutuskorpus. Paneme tähele, et

$$f = (x-\xi)(x+\xi)(x-\xi i)(x+\xi i)\,, \tag{3.59}$$

kus $\xi = \sqrt[4]{2} \in \mathbb{R}$. Lause 2.2.3 põhjal $\Sigma = \mathbb{Q}(\xi,-\xi,\xi i,-\xi i) = \mathbb{Q}(\xi,i)$. Teoreemi 2.2.12 põhjal on korpuse laiend $\Sigma:\mathbb{Q}$ lõplik ja normaalne.

2. Leiame laiendi $\Sigma:\mathbb{Q}$ astme. Teoreemi 2.1.36 põhjal

$$[\Sigma:\mathbb{Q}] = [\mathbb{Q}(\xi,i):\mathbb{Q}(\xi)][\mathbb{Q}(\xi):\mathbb{Q}]\,.$$

Paneme tähele, et lihtlaiendi $\mathbb{Q}(\xi)(i):\mathbb{Q}(\xi)$ määrav polünoom on x^2+1 üle $\mathbb{Q}(\xi)$, sest $i^2+1=0$ ning i ei ole ühegi esimese astme normeeritud polünoomi üle $\mathbb{Q}(\xi)$ juureks (kui oleks, siis peaks $i \in \mathbb{Q}(\xi) \subseteq \mathbb{R}$, mis oleks vastuoluline). Kuna lause 2.1.10 põhjal $\mathbb{Q}(\xi,i) = \mathbb{Q}(\xi)(i)$, siis lauset 2.1.39 kasutades saame nüüd, et $[\mathbb{Q}(\xi,i):\mathbb{Q}(\xi)] = 2$.

Element ξ on polünoomi f üle $\mathbb{Q}$ juureks. Vaadeldav polünoom f on aga Eisensteini kriteeriumi põhjal taandumatu üle $\mathbb{Q}$, mistõttu kujutab lihtlaiendi $\mathbb{Q}(\xi):\mathbb{Q}$ määravat polünoomi. Lause 2.1.39 põhjal jällegi $[\mathbb{Q}(\xi):\mathbb{Q}] = 4$. Seega

$$[\Sigma:\mathbb{Q}] = 2\cdot 4 = 8\,.$$

Lause 2.1.38 põhjal on $\{1,i\}$ vektorruumi $\mathbb{Q}(\xi,i)$ üle $\mathbb{Q}(\xi)$ baas ning sama lause põhjal on $\{1,\xi,\xi^2,\xi^3\}$ vektorruumi $\mathbb{Q}(\xi)$ üle $\mathbb{Q}$ baas. Teoreemi 2.1.36 tõestuses näidatu põhjal on $\{1,\xi,\xi^2,\xi^3,i,\xi i,\xi^2 i,\xi^3 i\}$ vektorruumi Σ üle $\mathbb{Q}$ baas. Seega,

$$\Sigma = \{a_0+a_1\xi+a_2\xi^2+a_3\xi^3+a_4 i+a_5\xi i+a_6\xi^2 i+a_7\xi^3 i \,|\, a_0,a_1,...,a_7 \in \mathbb{Q}\}\,. \tag{3.60}$$

3. Leiame laiendi $\Sigma:\mathbb{Q}$ Galois' rühma elemendid. Vaadeldava näite teises alapunktis veendusime, et lihtlaiendi $\mathbb{Q}(\xi):\mathbb{Q}$ määrav polünoom on f

üle $\mathbb{Q}$. Kuna ξi on polünoomi f juureks, siis on f ühtlasi ka lihtlaiendi $\mathbb{Q}(\xi i) : \mathbb{Q}$ määravaks polünoomiks. Polünoomi f esitusest kujul (3.59) nähtub, et f on taandumatu ka üle $\mathbb{Q}(i)$ (ükski polünoomidest $x - \xi$, $x + \xi$, $x - \xi i$, $x + \xi i$ ega ka ükski nende korrutamisel saadav teise astme polünoom ei ole polünoom üle $\mathbb{Q}(i)$). Seega on f ühtaegu ka lihtlaiendite $\mathbb{Q}(i)(\xi) : \mathbb{Q}(i)$ ja $\mathbb{Q}(i)(\xi i) : \mathbb{Q}(i)$ määravaks polünoomiks üle $\mathbb{Q}(i)$. Lause 2.1.10 põhjal $\mathbb{Q}(i)(\xi) = \Sigma = \mathbb{Q}(i)(\xi i)$. Nüüd, järeldust 2.1.29 kasutades, leidub selline $\mathbb{Q}$-automorfism $\sigma : \Sigma \to \Sigma$, et

$$\sigma(\xi) = \xi i \qquad \text{ning} \qquad \sigma(i) = i\,.$$

Näite alapunktis 2 veendusime, et polünoom $x^2 + 1$ on taandumatu üle $\mathbb{Q}(\xi)$ ning kujutab laiendi $\mathbb{Q}(\xi)(i) : \mathbb{Q}(\xi)$ määravat polünoomi. Paneme tähele, et $x^2 + 1$ on ühtaegu ka lihtlaiendi $\mathbb{Q}(\xi)(-i) : \mathbb{Q}(\xi)$ määravaks polünoomiks. Lause 2.1.10 põhjal aga $\mathbb{Q}(\xi)(i) = \Sigma = \mathbb{Q}(\xi)(-i)$. Nüüd jällegi järeldust 2.1.29 kasutades saame, et leidub selline $\mathbb{Q}$-automorfism $\tau : \Sigma \to \Sigma$, et

$$\tau(i) = -i \qquad \text{ning} \qquad \tau(\xi) = \xi\,.$$

Oleme leidnud kaks $\mathbb{Q}$-automorfismi σ ja τ korpusel Σ, st laiendi $\Sigma : \mathbb{Q}$ Galois' rühma kaks elementi. Nende kõikvõimalikud omavahelised korrutised annavad meile kaheksa erinevat $\mathbb{Q}$-automorfismi korpusel Σ, millised toome ära tabelis 3.1. Kujutuste σ ja τ teised kõikvõimalikud

Tabel 3.1: $\mathbb{Q}$-automorfismid korpusel Σ.

Automorfism ϕ	$\phi(\xi)$	$\phi(i)$
ι	ξ	i
σ	ξi	i
σ^2	$-\xi$	i
σ^3	$-\xi i$	i
τ	ξ	$-i$
$\sigma\tau$	ξi	$-i$
$\sigma^2\tau$	$-\xi$	$-i$
$\sigma^3\tau$	$-\xi i$	$-i$

omavahelised korrutised ei anna uusi $\mathbb{Q}$-automorfisme, sest $\sigma^4 = \tau^2 = \iota$, $\tau\sigma = \sigma^3\tau$, $\tau\sigma^2 = \sigma^2\tau$, $\tau\sigma^3 = \sigma\tau$.

Olgu nüüd $\gamma : \Sigma \to \Sigma$ suvaline $\mathbb{Q}$-automorfism. Paneme tähele, et siis

$$(\gamma(i))^2 = \gamma(i^2) = \gamma(-1) = -1\,,$$
$$(\gamma(\xi))^4 = \gamma(\xi^4) = \gamma(2) = 2\,,$$

mistõttu peab γ elemendi i kujutama elemendiks i või $-i$ ning elemendi ξ kujutama elemendiks ξ, $-\xi$, ξi või elemendiks $-\xi i$. Kokku on selliseid erinevaid kombinatsioone kaheksa, millised on kõik toodud tabelis 3.1. Seega on γ üks meie poolt eelnevalt leitud $\mathbb{Q}$-automorfismidest korpusel Σ ning tabelis 3.1 esitatud $\mathbb{Q}$-automorfismid on laiendi $\Sigma : \mathbb{Q}$ Galois' rühma kõik elemendid. Tulemus ühtib Galois' teooria põhiteoreemiga, millise teoreemi 1. väite põhjal on laiendi $\Sigma : \mathbb{Q}$ Galois' rühma järk $[\Sigma : \mathbb{Q}] = 8$ (vt alapunkt 2 antud näites).

4. Leiame laiendi $\Sigma : \mathbb{Q}$ Galois' rühma G kirjelduse. Tabelist 3.1 nähtub, et rühm G ei ole kommutatiivne ning on moodustatud elementide σ ja τ poolt. Seejuures

$$G = \langle \sigma, \tau \,|\, \sigma^4 = \tau^2 = 1\,,\ \tau^{-1}\sigma\tau = \sigma^{-1} \rangle\,.$$

   Siit nähtub, et $G \cong \mathbb{D}_8$, kus $\mathbb{D}_8$ on 8. järku dieedri rühm (vt [9], meil on see rühm küll natuke teisiti tähistatud).

5. Koostame rühma G alamrühmade tabeli. Tabeli selgituseks märgime, et kõik 4. järku rühmad on isomorfsed kas rühmaga $\mathbb{Z}_4$ või rühmaga $\mathbb{Z}_2 \times \mathbb{Z}_2$, kusjuures esimene neist on tsükliline ning teine mitte (väide on lihtsasti kontrollitav, sest kui 4. järku rühm ei ole tsükliline, siis peab tema iga ühikelemendist erineva elemendi järk olema 2).

8. järku:	G	$G \cong \mathbb{D}_8$
4. järku:	$S = \{\iota, \sigma, \sigma^2, \sigma^3\}$	$S \cong \mathbb{Z}_4$
	$T = \{\iota, \sigma^2, \tau, \sigma^2\tau\}$	$T \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
	$U = \{\iota, \sigma^2, \sigma\tau, \sigma^3\tau\}$	$U \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
2. järku:	$A = \{\iota, \sigma^2\}$	$A \cong \mathbb{Z}_2$
	$B = \{\iota, \tau\}$	$B \cong \mathbb{Z}_2$
	$C = \{\iota, \sigma\tau\}$	$C \cong \mathbb{Z}_2$
	$D = \{\iota, \sigma^2\tau\}$	$D \cong \mathbb{Z}_2$
	$E = \{\iota, \sigma^3\tau\}$	$E \cong \mathbb{Z}_2$
1. järku:	$I = \{\iota\}$	$I \cong \mathbb{Z}_1$

6. Leiame rühma G alamrühmadele vastavad vahekorpused. Galois' teooria põhiteoreemi 2. väite põhjal on laiendi $\Sigma : \mathbb{Q}$ Galois' vastavus bijektiivne. Paneme tähele, et $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ ja $\mathbb{Q}(\sqrt{2}i)$ on korpuse Σ alamkorpused ning laiendite $\mathbb{Q}(i) : \mathbb{Q}$, $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ ja $\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}$ astmed on 2 (laiendite määravad polünoomid on vastavalt x^2+1, x^2-2 ja x^2+2 üle $\mathbb{Q}$). Galois' teooria põhiteoreemi 3. väite põhjal vastavad nendele korpustele seega 4. järku G alamrühmad. Nüüd ei ole raske kontrollida, et vaadeldavatele korpustele vastavad vastavalt alamrühmad S, T ja U.

Leiame nüüd korpuse $C^\dagger$. Olgu $x \in \Sigma$ suvaline. Element x avaldub üheselt kujul (vt korpuse Σ kirjeldus, võrdus (3.60))

$$x = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5\xi i + a_6\xi^2 i + a_7\xi^3 i\,,$$

kus $a_0, a_1, ..., a_7 \in \mathbb{Q}$. Nüüd

$$\begin{aligned}(\sigma\tau)(x) &= \sigma(\tau(x)) = \\ &= \sigma(a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 - a_4 i - a_5\xi i - a_6\xi^2 i - a_7\xi^3 i) = \\ &= a_0 + a_1\xi i - a_2\xi^2 - a_3\xi^3 i - a_4 i + a_5\xi + a_6\xi^2 i - a_7\xi^3 = \\ &= a_0 + a_5\xi - a_2\xi^2 - a_7\xi^3 - a_4 i + a_1\xi i + a_6\xi^2 i - a_3\xi^3 i\,.\end{aligned}$$

Seega $(\sigma\tau)(x) = x$ siis ja ainult siis kui

$$\begin{aligned}a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4 i + a_5\xi i + a_6\xi^2 i + a_7\xi^3 i &= \\ = a_0 + a_5\xi - a_2\xi^2 - a_7\xi^3 - a_4 i + a_1\xi i + a_6\xi^2 i - a_3\xi^3 i\end{aligned} \quad (3.61)$$

ehk siis ja ainult siis kui

$$(a_1 - a_5)\xi + 2a_2\xi^2 + (a_3 + a_7)\xi^3 + 2a_4 i + (a_5 - a_1)\xi i + (a_7 + a_3)\xi^3 i = 0\,. \quad (3.62)$$

Võrdus (3.62) kujutab nulliga võrduvat lineaarkombinatsiooni vektorruumi Σ baasivektoritest. Seega, võrdus $(\sigma\tau)(x) = x$ kehtib parajasti siis kui kehtivad võrdused

$$a_1 = a_5\,, \qquad a_2 = a_4 = 0\,, \qquad a_3 = -a_7\,,$$

Elemendid a_0 ja a_6 võivad seejuures olla suvalised. Siit järeldub, et x peab esituma kujul

$$\begin{aligned}x &= a_0 + a_1\xi(1+i) + a_6\xi^2 i + a_3\xi^3(1-i) = \\ &= a_0 + a_1[\xi(1+i)] + \frac{a_6}{2}[\xi(1+i)]^2 - \frac{a_3}{2}[\xi(1+i)]^3\,.\end{aligned} \quad (3.63)$$

Võrdusest (3.63) nähtub, et võrdus $(\sigma\tau)(x) = x$ kehtib parajasti siis kui $x \in \mathbb{Q}(\xi(1+i))$ (vt lause 2.1.38 ning paneme seejuures tähele, et $[\xi(1+i)]^4 = 2(2i)(2i) = -8 \in \mathbb{Q}$), mistõttu

$$C^\dagger = \mathbb{Q}(\xi(1+i))\,.$$

Sarnaselt võime veenduda, et

$$A^\dagger = \mathbb{Q}(\sqrt{2}, i)\,, \qquad B^\dagger = \mathbb{Q}(\xi)\,, \qquad D^\dagger = \mathbb{Q}(\xi i)\,, \qquad E^\dagger = \mathbb{Q}((1-i)\xi)\,,$$

mis koos triviaalsete vastavustega

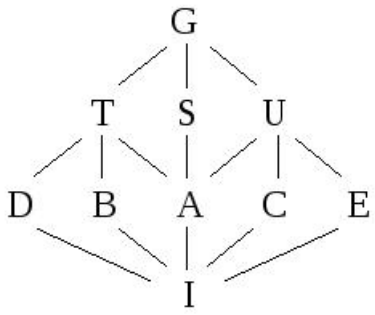
$$G^\dagger = \mathbb{Q} \qquad \text{ja} \qquad I^\dagger = \Sigma\,,$$

ning alapunkti algul leitud vastavustega

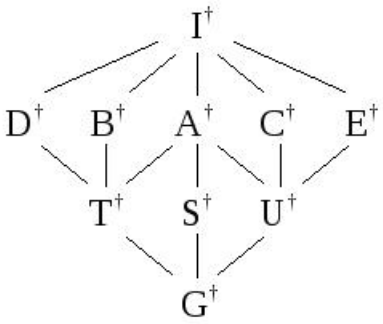
$$S^\dagger = \mathbb{Q}(i)\,, \qquad T^\dagger = \mathbb{Q}(\sqrt{2})\,, \qquad U^\dagger = \mathbb{Q}(\sqrt{2}i)\,,$$

kujutavad Galois' vastavuse bijektiivsuse tõttu kõiki vahekorpusi korpuste $\mathbb{Q}$ ja Σ vahel.

7. Vahekorpusi korpuste Σ ja $\mathbb{Q}$ vahel ning Galois' rühma G alamrühmi kirjeldavad vastavalt joonised 3.2 ja 3.1 (joonistel on hulk X hulga Y alamhulk, kui leidub hulgast Y allapoole suunduv lõikude jada hulgani X, näiteks $T^\dagger \subseteq I^\dagger$). Märgime, et alamrühmade joonise saame koostada vahetult näite 5. alapunktis koostatud rühma G alamrühmade tabelit kasutades. Vahekorpuste joonise saame seejärel koostada lauset 3.2.2 või näite 6. alapunkti tulemusi kasutades.



Joonis 3.1: Alamrühmad.



Joonis 3.2: Vahekorpused.

8. Võime veenduda, et rühma G normaaljagajad on G, S, T, U, A ja I. Galois' teooria põhiteoreemi 4. väite põhjal on seega vahekorpused $G^\dagger$, $S^\dagger$, $T^\dagger$, $U^\dagger$, $A^\dagger$ ja $I^\dagger$ normaalkorpused (korpuse $\mathbb{Q}$ suhtes) ning ainult need. See on ka tõepoolest nii, sest vaadeldavad korpused on lahutuskorpusteks vastavalt polünoomidele x, x^2+1, x^2-2, x^2+2, x^4-x^2-2 ja f üle $\mathbb{Q}$ ning ka teoreemi 2.2.12 põhjal on vaadeldavad korpused normaalsed (korpuse $\mathbb{Q}$ suhtes).

   Seevastu, näiteks korpus $B^\dagger$ ei ole tõepoolest normaalkorpus $\mathbb{Q}$ suhtes, sest polünoomi f juur ξ kuulub korpusesse $B^\dagger$, kuid vaadeldav polünoom ei lahutu lineaartegurite korrutiseks üle $B^\dagger$ (vt definitsioon 2.2.10).

9. Galois' teooria põhiteoreemi 5. väite põhjal on näiteks laiendi $A^\dagger : \mathbb{Q}$ Galois' rühm isomorfne faktorrühmaga G/A (sest laiend $A^\dagger : \mathbb{Q}$ on näite 8. alapunkti põhjal normaalne). Paneme tähele, et rühma G/A elemendid on kõrvalklassid $\{\iota, \sigma^2\}$, $\{\sigma, \sigma^3\}$, $\{\tau, \sigma^2\tau\}$, $\{\sigma\tau, \sigma^3\tau\}$. Siit nähtub, et rühm G/A ei ole tsükliline, mistõttu $G/A \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Näites 3.1.15 leidsime, et laiendi $A^\dagger : \mathbb{Q} = \mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}$ Galois' rühm koosneb neljast elemendist, millised esitame järgneva tabelina.

Automorfism ϕ	$\phi(\sqrt{2})$	$\phi(i)$
ι	$\sqrt{2}$	i
α	$\sqrt{2}$	$-i$
β	$-\sqrt{2}$	i
$\alpha\beta$	$-\sqrt{2}$	$-i$

   Tabelist nähtub, et rühm $\Gamma(A^\dagger : \mathbb{Q})$ ei ole tsükliline, mistõttu on vaadeldav rühm isomorfne rühmaga $\mathbb{Z}_2 \times \mathbb{Z}_2$ ning seega – tõepoolest – ka rühmaga G/A.

3.3 Võrrandite lahenduvus radikaalides

Selles punktis me kasutame Galois' teooria põhiteoreemi (teoreemi 3.2.32), et tuletada tingimus, mis peab olema täidetud selleks, et mingit polünoomi (ning seega ka algebralist võrrandit) oleks võimalik lahendada radikaalides. Etteruttavalt mainime, et selleks tingimuseks on, et vaadeldava polünoomi Galois' rühm peab olema lahenduv rühm. Näitame, et see tingimus osutub ka piisavaks tingimuseks. Toome ka seejärel ühe näite 5. astme polünoomist, mille Galois' rühm ei ole lahenduv ning mis ei ole seega lahenduv radikaalides.

3.3.1 Radikaalsed laiendid

"Maakeeli" öeldes, laiend $L : K$ on radikaalne kui L on saadud korpusest K temale teatavate naturaalarvuliste astmete juurte järkjärgulisel adjungeerimsel. Vaatleme näiteks järgmist avaldist:

$$\sqrt[3]{11}\sqrt[5]{\frac{7+\sqrt{3}}{2}}+\sqrt[4]{1+\sqrt[3]{4}}. \tag{3.64}$$

Adjungeerides korpusele $\mathbb{Q}$ üksteise järel elemendid $\alpha = \sqrt[3]{11}$, $\beta = \sqrt{3}$, $\gamma = \sqrt[5]{(7+\beta)/2}$, $\delta = \sqrt[3]{4}$ ja $\varepsilon = \sqrt[4]{1+\delta}$, saame korpuse $L = \mathbb{Q}(\alpha, \beta, \gamma, \delta, \varepsilon)$, mis sisaldab elementi (3.64), ning laiendi $L : \mathbb{Q}$, mis on radikaalne.

See annab põhjuse järgnevale formaalsele definitsioonile.

Definitsioon 3.3.1. *Korpuse laiendit* $L : K$ nimetame *radikaalseks*, kui $L = K(\alpha_1, \alpha_2, ..., \alpha_m)$, kus iga $j \in \{1, 2..., m\}$ korral leidub naturaalarv n_j nii, et

$$\alpha_j^{n_j} \in K(\alpha_1, \alpha_2, \ldots, \alpha_{j-1}) \tag{3.65}$$

($j = 1$ korral, loeme, et $\alpha_1^{n_1} \in K$). *Elemente* α_1, α_2, ..., α_m nimetame *radikaalideks*.

Näide 3.3.2. Laiend $\mathbb{Q}(\alpha, \beta, \gamma, \delta, \varepsilon) : \mathbb{Q}$, kus α, β, γ, δ ja ε on antud definitsioonile 3.3.1 eelnevas arutelus, on radikaalne, sest $\alpha^3 = 11 \in \mathbb{Q}$, $\beta^2 = 3 \in \mathbb{Q}(\alpha)$, $\gamma^5 = (7+\beta)/2 \in \mathbb{Q}(\alpha, \beta)$, $\delta^3 = 4 \in \mathbb{Q}(\alpha, \beta, \gamma)$ ning $\varepsilon^4 = 1 + \delta \in \mathbb{Q}(\alpha, \beta, \gamma, \delta)$.

Seome nüüd radikaalsed laiendid algebraliste võrranditega.

Definitsioon 3.3.3. Algebralist võrrandit $f(x) = 0$, kus f on polünoom üle korpuse K, nimetame *lahenduvaks radikaalides* (*üle* K), kui leidub korpus M nii, et polünoomi f lahutuskorpus $\Sigma \subseteq M$ ning, et $M : K$ on radikaalne laiend. Sellisel juhul ütleme ka, et polünoom f on *lahenduv radikaalides* (*üle* K).

Selgitame lähemalt definitsiooni 3.3.3. Olgu $f(x) = 0$ algebraline võrrand üle korpuse K (st, f on polünoom üle K). Siis võrrand $f(x) = 0$ on lahenduv radikaalides kui polünoom f on lahenduv radikaalides. Polünoom f on aga lahenduv radikaalides kui leiduvad radikaalid

$$\alpha_1 = \sqrt[n_1]{u_1}\,, \qquad \alpha_2 = \sqrt[n_2]{u_2}\,, \qquad \ldots\,, \qquad \alpha_m = \sqrt[n_m]{u_m}\,,$$

millede adjungeerimisel korpusele K saame korpuse $K(\alpha_1, \alpha_2, ..., \alpha_m)$, mis sisaldab polünoomi f lahutuskorpust. St, saame korpuse, mis sisaldab polünoomi f kõiki juuri ehk võrrandi $f(x) = 0$ kõiki lahendeid. Siinjuures tähendab

u_1 mingit K elementi, u_2 mingit $K(\alpha_1)$ elementi, u_3 mingit $K(\alpha_1, \alpha_2)$ elementi jne, kuni lõppeks u_m on teatav $K(\alpha_1, \alpha_2, ..., \alpha_{m-1})$ element. Teiste sõnadega, võrrand $f(x) = 0$ on radikaalides lahenduv kui tema lahendid avalduvad ratsionaalselt radikaalide α_1, α_2, ..., α_m ja korpuse K elementide kaudu (selle kohta ütleme edaspidi lihtsalt, et f lahendid avalduvad radikaalide kaudu). Nii on näiteks kuupvõrrand

$$x^3 + px + q = 0\,,$$

kus p ja q on korpuse K elemendid, lahenduv radikaalides, sest tema lahendid on esitatavad valemiga (vt [2], lk 287, 288)

$$x = u - \frac{p}{3u}\,, \qquad u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\,.$$

Tähistades

$$\alpha_1 = \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\,, \qquad \alpha_2 = \sqrt[3]{-\frac{q}{2} + \alpha_1}\,,$$

saame, et vaadeldava kuupvõrrandi lahendid avalduvad ratsionaalselt radikaalide α_1, α_2 kaudu kujul $x = \alpha_2 - \frac{p}{3\alpha_2}$.

Lause 3.3.4. *Radikaalne laiend $L : K$ on lõplik.*

Tõestus. Eelduse põhjal $L = K(\alpha_1, \alpha_2, ..., \alpha_r)$, kus $\alpha_i^{n_i} \in K(\alpha_1, \alpha_2, ..., \alpha_{i-1})$ mingi naturaalarvu n_i korral, $i \in \{1, 2, ..., r\}$. Seega α_1 on mingi polünoomi üle K juureks (näiteks polünoomi $x^{n_1} - \alpha_1^{n_1}$ juureks), α_2 on mingi polünoomi üle $K(\alpha_1)$ juureks jne kuni α_r on mingi polünoomi üle $K(\alpha_1, \alpha_2, ..., \alpha_{r-1})$ juureks. St, kõik lihtlaiendid

$$\begin{gathered} K(\alpha_1) : K\,, \\ K(\alpha_1)(\alpha_2) : K(\alpha_1)\,, \\ \dots\,, \\ K(\alpha_1, \alpha_2, \dots, \alpha_{r-1})(\alpha_r) : K(\alpha_1, \alpha_2, \dots, \alpha_{r-1}) \end{gathered}$$

on algebralised, mistõttu lause 2.1.39 põhjal on nende astmed lõplikud. Lause 2.1.10, järelduse 2.1.37 ja eelöeldu põhjal seega

$$\begin{aligned} [L : K] = [K(\alpha_1, \alpha_2, \dots, \alpha_{r-1})(\alpha_r) : K(\alpha_1, \alpha_2, \dots, \alpha_{r-1})] \cdot \dots \\ \dots \cdot [K(\alpha_1)(\alpha_2) : K(\alpha_1)] \cdot [K(\alpha_1) : K] < \infty\,. \quad \square \end{aligned}$$

Lause 3.3.5. *Olgu $L : K$ radikaalne laiend, $L = K(\alpha_1, \alpha_2, ..., \alpha_m)$, kus elemendid α_j, $j \in \{1, 2, ..., m\}$, rahuldavad tingimust* (3.65)*. Siis võime korpuse L esitada kujul $L = K(\beta_1, \beta_2, ..., \beta_n)$, kus elemendid β_i, $i \in \{1, 2, ..., n\}$, rahuldavad tingimust* (3.65)*, kusjuures naturaalarvud n_i on iga $i \in \{1, 2, ..., n\}$ korral algarvud.*

Tõestus. Olgu $K_1 = K(\alpha_1)$. Siis eelduse põhjal leidub naturaalarv n_1 nii, et $\alpha^{n_1} \in K$. Aritmeetika põhiteoreemi põhjal (vt [6], lk 7, teoreem 1.17) saab iga naturaalarvu esitada teatavate algarvude korrutisena. Seega võime naturaalarvu n_1 esitada kujul $n_1 = p_1 p_2 ... p_k$, kus p_i on algarvud, $i \in \{1, 2, ..., k\}$. Valime nüüd $\beta_1 = \alpha_1^{p_2 p_3 \cdots p_k}$, $\beta_2 = \alpha_1^{p_3 \cdots p_k}$,..., $\beta_k = \alpha_1$ ning paneme tähele, et laiend $K(\alpha_1) : K$ on selline, et $K(\alpha_1) = K(\beta_1, \beta_2, ..., \beta_k)$ ning

$$\beta_i^{p_i} \in K(\beta_1, \beta_2, \ldots, \beta_{i-1}), \qquad i \in \{1, 2, \ldots, k\}.$$

Lause 2.1.10 põhjal $L = K(\alpha_1, \alpha_2, ..., \alpha_m) = K(\alpha_1)(\alpha_2)...(\alpha_m)$. Nüüd teostame äsjakirjeldatud protseduuri iga laiendi

$$K(\alpha_1, \alpha_2, \ldots, \alpha_{r-1})(\alpha_r) : K(\alpha_1, \alpha_2, \ldots, \alpha_{r-1}), \qquad r \in \{1, 2, \ldots, m\},$$

jaoks eraldi, kuni saamegi, et

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_m) = K(\beta_1, \beta_2, \ldots, \beta_n),$$

kus iga $j \in \{1, 2, \ldots, n\}$ korral leidub algarv p_j nii, et

$$\beta_j^{p_j} \in K(\beta_1, \beta_2, \ldots, \beta_{j-1}). \qquad \square$$

Lause 3.3.6. *Olgu $L : K$ radikaalne laiend ning olgu $M : K$ laiendi $L : K$ normaalsulundiks. Siis ka laiend $M : K$ on radikaalne.*

Tõestus. Eelduse põhjal $L = K(\alpha_1, \alpha_2, ..., \alpha_r)$, kus $\alpha_i^{n_i} \in K(\alpha_1, \alpha_2, ..., \alpha_{i-1})$ mingi naturaalarvu n_i korral, $i \in \{1, 2, ..., r\}$. Olgu f_i elemendi α_i minimaalne polünoom üle korpuse K ($i \in \{1, 2, ..., r\}$). Paneme tähele, et iga $i \in \{1, 2, ..., r\}$ korral polünoomi f_i juur α_i kuulub korpusesse M. Kuna M on normaalkorpus, siis f_i lahutub lineaartegurite korrutiseks üle M. Siis aga ka polünoom $g = \prod_{i=1}^{r} f_i$ lahutub lineaartegurite korrutiseks üle M, mistõttu M sisaldab polünoomi g kõiki juuri ning lause 2.2.3 põhjal siis aga ka g lahutuskorpust Σ. Kuna Σ sisaldab polünoomi g juuri α_1, α_2, ..., α_r ning korpust K, siis $L \subseteq \Sigma$. Teoreemi 2.2.12 põhjal on laiend $\Sigma : K$ normaalne. Nüüd normaalsulundi definitsiooni 3.2.19 põhjal $M = \Sigma$, st, M on polünoomi g lahutuskorpus üle K.

Adjungeerime nüüd korpusele K kõigepealt polünoomi f_1 kõik juured β_{1j}, $j \in \{1, 2, ..., \deg f_1\}$. Saame korpuse $K_1 = K(\beta_{11}, \beta_{12}, ..., \beta_{1k_1})$, kus $k_1 = \deg f_1$, ning mis sisaldab korpust $K(\alpha_1)$. Seejärel adjungeerime korpusele K_1 polünoomi f_2 kõik juured β_{2j}, $j \in \{1, 2, ..., \deg f_2\}$. Saame korpuse $K_2 = K_1(\beta_{21}, \beta_{22}, ..., \beta_{2k_2})$, kus $k_2 = \deg f_2$, ning mis sisaldab korpust $K(\alpha_1, \alpha_2)$. Nii jätkame, kuni lõpuks adjungeerime korpusele K_{r-1} polünoomi f_r kõik juured β_{rj}, $j \in \{1, 2, ..., \deg f_r\}$. Saame korpuse $K_r = K_{r-1}(\beta_{r1}, \beta_{r2}, ..., \beta_{rk_r})$, kus $k_r = \deg f_r$, ning mis sisaldab korpust

$K(\alpha_1, \alpha_2, ..., \alpha_r)$. Lausetest 2.2.3, 2.1.10 ning meie konstruktsioonist järeldub, et $K_r = M$.

Olgu β_{ij} polünoomi f_i suvaline juur ($i \in \{1, 2, ..., r\}$, $j \in \{1, 2, ..., \deg f_i\}$). Järelduse 2.1.29 põhjal leidub isomorfism $\sigma : K(\alpha_i) \to K(\beta_{ij})$ nii, et $\sigma(\alpha_i) = \beta_{ij}$ ning $\sigma(k) = k$ iga $k \in K$ korral. Teoreemi 3.2.17 põhjal leidub selline K-automorfism $\gamma : M \to M$, et $\gamma|_{K(\alpha_i)} = \sigma$ (kuna M on polünoomi f lahutuskorpus, siis $M : K$ on lõplik ja normaalne, vt teoreem 2.2.12). Nüüd

$$\beta_{ij}^{n_i} = (\gamma(\alpha_i))^{n_i} = \gamma(\alpha_i^{n_i}) \in \gamma(K(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}))\,.$$

Tõestuseks piisab seega näidata, et suvalise K-automorfismi $\tau : M \to M$ ning suvalise $i \in \{0, 1, 2, ..., r-1\}$ korral

$$\tau(K(\alpha_1, \alpha_2, \ldots, \alpha_i)) \subseteq K_i\,, \tag{3.66}$$

kus $K_0 = K$. Olgu seega $\tau : M \to M$ suvaline K-automorfism. Sisalduvuse (3.66) tõestame matemaatilise induktsiooni meetodit kasutades.

Induktsiooni baas. Juhul $i = 0$ väide kehtib, sest kuna τ on K-automorfism, siis $\tau(K) = K = K_0$.

Induktsiooni samm. Olgu $k \in \{1, 2, ..., r-1\}$ ning eeldame, et sisalduvus (3.66) kehtib iga arvu i korral kui $0 \leq i < k$. Näitame, et sisalduvus (3.66) kehtib siis ka juhul $i = k$.

Paneme tähele, et $K(\alpha_1, \alpha_2, ..., \alpha_{k-1}, \alpha_k) = K(\alpha_1, \alpha_2, ..., \alpha_{k-1})(\alpha_k)$. Lause 2.1.38 põhjal on $\{1, \alpha_k, \alpha_k^2, ..., \alpha_k^m\}$ vektorruumi $K(\alpha_1, \alpha_2, ..., \alpha_{k-1})(\alpha_k)$ üle $K(\alpha_1, \alpha_2, ..., \alpha_{k-1})$ baas (siin m on teatav mittenegatiivne täisarv). Kuna τ on K-automorfism korpusel M, siis ta teisendab polünoomi f_k juure α_k mingiks juureks β_{kj}, kus $j \in \{1, 2, ..., \deg f_k\}$ (väite tõestus kordab lause 3.1.13 tõestust). Olgu nüüd $x \in K(\alpha_1, \alpha_2, ..., \alpha_k)$ suvaline. Siis x esitub kujul

$$x = l_0 + l_1\alpha_k + l_2\alpha_k^2 + \ldots + l_m\alpha_k^m\,,$$

kus $l_s \in K(\alpha_1, \alpha_2, ..., \alpha_{k-1})$, $s \in \{0, 1, 2, ..., m\}$. Nüüd aga

$$\tau(x) = \tau(l_0) + \tau(l_1)\beta_{kj} + \tau(l_2)\beta_{kj}^2 + \ldots + \tau(l_m)\beta_{kj}^m \in K_k\,,$$

sest induktsiooni eelduse tõttu $\tau(l_s) \in K_{k-1} \subseteq K_k$ iga $s \in \{0, 1, 2, ..., m\}$ korral ning korpuste K_k ($k \in \{1, 2, ..., r\}$) konstruktsiooni tõttu polünoomi f_k iga juur $\beta_{kj} \in K_k$ ($j \in \{1, 2, ..., \deg f_k\}$). Seega sisalduvus (3.66) tõepoolest kehtib. □

3.3.2 Galois' teoreem

Nagu juba mainitud, selleks, et mingi algebraline võrrand oleks lahenduv radikaalides, on tarvilik ja piisav, et vaadeldava võrrandi Galois' rühm oleks

lahenduv. Selle väite tõestusele me siin alapunktis keskendumegi. Tõestame eelnevalt paar abitulemust.

Lause 3.3.7. *Olgu K korpus ning Σ polünoomi $x^p - 1$ lahutuskorpus üle K, kus p on algarv. Siis laiendi $\Sigma : K$ Galois' rühm on Abeli rühm.*

Tõestus. Polünoomil $x^p - 1$ leidub algebra põhiteoreemi põhjal p juurt kompleksarvude hulgas. Nendeks juurteks on p-astme ühejuured $e^{2\pi ki/p}$, $k \in \{0, 1, 2, ..., p-1\}$, mis on seejuures paarikaupa erinevad (vt [5], lk 188) ning moodustavad korrutamise suhtes tsüklilise rühma (vt [5], lk 189, teoreem 6.8.2). Olgu ε selle rühma mingi moodustaja. Paneme tähele, et siis $\Sigma = K(\varepsilon)$.

Olgu $\alpha, \beta \in \Gamma(\Sigma : K)$ suvalised ning veendume, et $\alpha\beta = \beta\alpha$. Selles veendumiseks piisab lauset 2.1.38 ning asjaolu, et $\alpha\beta$ on K-automorfism korpusel Σ, silmas pidades, näidata, et $(\alpha\beta)(\varepsilon) = (\beta\alpha)(\varepsilon)$. Lause 3.1.13 põhjal $\alpha(\varepsilon) = \varepsilon^i$ ning $\beta(\varepsilon) = \varepsilon^j$ mingite $i, j \in \{1, 2, ..., p\}$ korral. Nüüd leiame, et

$$(\alpha\beta)(\varepsilon) = \alpha(\beta(\varepsilon)) = \alpha(\varepsilon^j) = (\alpha(\varepsilon))^j = (\varepsilon^i)^j = \varepsilon^{ij} = (\varepsilon^j)^i = (\beta(\varepsilon))^i = \\ = \beta(\varepsilon^i) = \beta(\alpha(\varepsilon)) = (\beta\alpha)(\varepsilon)\,.$$

Saadud võrdusest järeldub eelöeldu põhjal, et $\alpha\beta = \beta\alpha$ ning laiendi $\Sigma : K$ Galois' rühm on seega Abeli rühm. □

Lause 3.3.8. *Olgu K mingi selline korpus, üle mille polünoom $x^n - 1$ ($n \in \mathbb{N}$) lahutub lineaartegurite korrutiseks. Olgu Σ polünoomi $x^n - a$ lahutuskorpus üle K. Siis laiendi $\Sigma : K$ Galois' rühm on Abeli rühm.*

Tõestus. Polünoomi $x^n - 1$ juured on parajasti kõik n-astme ühejuured $e^{2\pi ki/n}$, $k \in \{0, 1, 2, ..., n-1\}$, mis on paarikaupa erinevad.

Olgu x_1 polünoomi $x^n - a$ mingi juur. Paneme tähele, et suvalise n-astme ühejuure ε korral on ka εx_1 polünoomi $x^n - a$ juureks. Eelöeldu tõttu leidub täpselt n erinevat n-astme ühejuurt. Seega, nende n-astme ühejuurte korrutised juurega x_1 annavad meile kokku n erinevat polünoomi $x^n - a$ juurt. Algebra põhiteoreemi põhjal ei saa polünoomil $x^n - a$ rohkem juuri leiduda. Kuna korpus K sisaldab lause eelduse põhjal polünoomi $x^n - 1$ kõiki juuri, siis eelöeldu ja lause 2.2.3 põhjal $\Sigma = K(x_1)$.

Olgu $\alpha, \beta \in \Gamma(\Sigma : K)$ suvalised ning veendume, et $\alpha\beta = \beta\alpha$. Selles veendumiseks piisab, kui näidata, et $(\alpha\beta)(x_1) = (\beta\alpha)(x_1)$ (vt eelmise lause tõestust). Nüüd, lause 3.1.13 ja eelöeldu põhjal,

$$\alpha(x_1) = \varepsilon x_1\,, \qquad \beta(x_1) = \eta x_1\,,$$

kus $\varepsilon, \eta \in K$ on teatavad n-astme ühejuured. Nüüd

$$(\alpha\beta)(x_1) = \alpha(\beta(x_1)) = \alpha(\eta x_1) = \alpha(\eta)\alpha(x_1) = \eta\varepsilon x_1 = \varepsilon\eta x_1 = \\ = \beta(\varepsilon)\beta(x_1) = \beta(\varepsilon x_1) = \beta(\alpha(x_1)) = (\beta\alpha)(x_1)\,.$$

Seega $\alpha\beta = \beta\alpha$ ning laiendi $\Sigma : K$ Galois' rühm on Abeli rühm. $\square$

Lause 3.3.9. *Kui korpuse laiend $L : K$ on normaalne ja radikaalne, siis rühm $\Gamma(L : K)$ on lahenduv.*

Tõestus. Olgu $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$, kus $\alpha_j^{n_j} \in K(\alpha_1, \alpha_2, ..., \alpha_{j-1})$ mingi naturaalarvu n_j korral, $j \in \{1, 2, ..., n\}$. Lause 3.3.4 põhjal on laiend $L : K$ lõplik. Lause 3.3.5 põhjal võime eeldada, et naturaalarvud n_j on algarvud iga $j \in \{1, 2, ..., n\}$ korral. Lause tõestame matemaatilise induktsiooni meetodil radikaalide arvu n järgi, $n \in \mathbb{N}$.

Induktsiooni baas. Olgu $n = 1$. Siis $L = K(\alpha)$, kusjuures võime eeldada, et $\alpha \notin K$ ja $\alpha^p \in K$ mingi algarvu p korral (juhul kui $\alpha \in K$, siis ühest elemendist koosnev rühm $\Gamma(K : K)$ on lahenduv). Olgu f elemendi α minimaalne polünoom üle K. Kuna laiend $L : K$ on normaalne, siis f lahutub lineaartegurite korrutiseks üle L. Kuna f on taandumatu üle K, siis järelduse 2.2.6 põhjal on f juured paarikaupa erinevad. Kuna $\alpha \notin K$, siis on f aste vähemalt 2. Olgu β polünoomi f mingi teine juur, $\beta \neq \alpha$. Nüüd järelduse 2.1.29 põhjal leidub selline isomorfism $\sigma : K(\alpha) \to K(\beta)$, et $\sigma(k) = k$ iga $k \in K$ korral ning, et $\sigma(\alpha) = \beta$. Seega,

$$\beta^p = (\sigma(\alpha))^p = \sigma(\alpha^p) = \alpha^p \,.$$

Kuna $\beta \notin K$, siis $\beta \neq 0$. Olgu $\varepsilon = \alpha/\beta \in L$. Paneme tähele, et $\varepsilon \neq 1$, ning $\varepsilon^p = 1$. Kuna p on algarv, siis elemendi ε järk rühmas L on p (kui k on elemendi ε järk, siis $k \mid p$ (vt näiteks [6], lk 28, lemma 7.3)). Seega, elemendid 1, ε, ε^2, ..., ε^{p-1} on paarikaupa erinevad, kujutades endast kõiki p-astme ühejuuri korpuses L. Olgu M polünoomi $x^p - 1$ lahutuskorpus üle K, st, $M = K(\varepsilon)$. Oleme saanud jada

$$K \subseteq M \subseteq M(\alpha) = L \,. \tag{3.67}$$

Paneme tähele, et $L = K(\alpha)$ on polünoomi $x^p - \alpha^p$ lahutuskorpus üle M, sest $M(\alpha)$ sisaldab kõiki p-astme ühejuuri ning polünoomi $x^p - \alpha^p$ üks juurtest $\alpha \in M(\alpha)$ (vt lause 3.3.8 tõestust). Nüüd, lause 3.3.8 põhjal on rühm $\Gamma(M(\alpha) : M)$ ehk rühm $\Gamma(L : M)$ Abeli rühm ning seega lahenduv (vt näide 1.2.6(1)).

Kuna $M = K(\varepsilon)$ on polünoomi $x^p - 1$ lahutuskorpus üle K, siis lause 2.2.12 põhjal on laiend $M : K$ normaalne. Galois' teooria põhiteoreemi viienda väite põhjal kehtib seega (meenutame, et $M^* = \Gamma(L : M)$)

$$\Gamma(M : K) \cong \Gamma(L : K)/\Gamma(L : M) \,. \tag{3.68}$$

Lause 3.3.7 põhjal on $\Gamma(M : K)$ Abeli rühm ning seega lahenduv. Seega, isomorfismi (3.68) ja lause 1.2.7 põhjal on ka rühm $\Gamma(L : K)/\Gamma(L : M)$ lahenduv. Nüüd, kuna lisaks ka rühm $\Gamma(L : M)$ on lahenduv, siis teoreemi 1.2.13 põhjal on rühm $\Gamma(L : K)$ lahenduv.

Induktsiooni samm. Olgu nüüd $n > 1$ mingi naturaalarv ning eeldame, et väide kehtib iga normaalse ja radikaalse korpuse laiendi $L' : K'$ korral, kus $L' = K'(\beta_1, \beta_2, ..., \beta_m)$, $\beta_i^{p_i} \in K'(\beta_1, \beta_2, ..., \beta_{i-1})$, p_i on algarv, $i \in \{1, 2, ..., m\}$ ning $m < n$.

Kui $\alpha_1 \in K$, siis $L = K(\alpha_2, ..., \alpha_n)$ ning meie väide kehtib induktsiooni eelduse tõttu. Võime seega eeldada, et $\alpha_1 \notin K$.

Tõestuse algus ühtib induktsiooni baasis näidatuga, mistõttu ei hakka seda kordama. Erinevused tulevad sisse alates võrdusest (3.67). Seega, jätkame induktsiooni sammu tõestust võrdusest (3.67) – kasutades samu tähistusi. Võrdus (3.67) saab nüüd kuju

$$K \subseteq M \subseteq M(\alpha_1) \subseteq L\,.$$

Kuna $x^p - 1$ lahutub lineaartegurite korrutiseks üle M ning $\alpha_1^p \in M$, siis lause 3.3.8 tõestusele tuginedes on $M(\alpha_1)$ polünoomi $x^p - \alpha_1^p$ lahutuskorpus üle M. Teoreemi 2.2.12 põhjal on laiend $M(\alpha_1) : M$ seega normaalne. Galois' teooria põhiteoreemi viienda väite põhjal kehtib seega

$$\Gamma(M(\alpha_1) : M) \cong \Gamma(L : M)/\Gamma(L : M(\alpha_1))\,. \tag{3.69}$$

Paneme tähele, et kuna $K \subseteq M$, siis lausele 2.1.10 tuginedes

$$L = M(\alpha_1)(\alpha_2, \ldots, \alpha_n)\,.$$

Nüüd, kuna laiend $L : K(\alpha_1)$ on radikaalne ning kuna $K(\alpha_1) \subseteq M(\alpha_1)$, siis ei ole raske näha, et ka laiend $L : M(\alpha_1)$ on radikaalne. Kuna $L : K$ on normaalne, siis on seda ka laiend $L : M(\alpha_1)$. Induktsiooni eelduse tõttu on rühm $\Gamma(L : M(\alpha_1))$ seega lahenduv. Lause 3.3.8 põhjal on $\Gamma(M(\alpha_1) : M)$ aga Abeli rühm ning seega lahenduv. Nüüd isomorfismi (3.69), lause 1.2.7 ja teoreemi 1.2.13 põhjal on rühm $\Gamma(L : M)$ lahenduv.

Kuna M on polünoomi $x^p - 1$ lahutuskorpus üle K, siis laiend $M : K$ on normaalne (vt teoreem 2.2.12). Galois' teooria põhiteoreemi viienda väite põhjal kehtib seega

$$\Gamma(M : K) \cong \Gamma(L : K)/\Gamma(L : M)\,.$$

Lause 3.3.7 põhjal on $\Gamma(M : K)$ Abeli rühm ning seega lahenduv. Kuna ka rühm $\Gamma(L : M)$ on eespoolnäidatu põhjal lahenduv, siis sama aruteluga nagu mõned read eespool saame, et $\Gamma(L : K)$ on lahenduv rühm ning lause on tõestatud. □

Meenutame, et kui $L : K$ on lõplik normaallaiend, siis teoreemi 3.2.32 esimese väite põhjal $[L : K] = |\Gamma(L : K)|$. Seda tulemust silmas pidades anname järgmise definitsiooni.

Definitsioon 3.3.10. Olgu $L : K$ lõplik normaallaiend, mille aste on n. *Elemendi $a \in L$ normiks* nimetame suurust

$$N(a) = \tau_1(a)\tau_2(a)\dots\tau_n(a)\,,$$

kus $\tau_1, \tau_2, ..., \tau_n$ on laiendi $L : K$ Galois' rühma kõik elemendid.

Järgnev teoreem pärineb David Hilberti 1893. aasta raportist algebraliste arvude kohta ning kannab seetõttu nime Hilberti Teoreem 90.

Teoreem 3.3.11 (Hilberti Teoreem 90)**.** *Olgu $L : K$ lõplik normaallaiend, mille Galois' rühm G on tsükliline, moodustajaga τ. Siis elemendi $a \in L$ norm on 1 ($N(a) = 1$) siis ja ainult siis kui*

$$a = b/\tau(b)\,,$$

mingi $b \in L$, $b \neq 0$, korral.

Tõestus. Piisavus. Kuna $L : K$ on normaalne ja lõplik, siis teoreemi 3.2.32 esimese väite põhjal on ka G lõplik. Olgu seega $|G| = n$. Kui $a = b/\tau(b)$, $b \neq 0$, siis

$$N(a) = a\tau(a)\tau^2(a)\dots\tau^{n-1}(a) = \frac{b}{\tau(b)}\frac{\tau(b)}{\tau^2(b)}\frac{\tau^2(b)}{\tau^3(b)}\dots\frac{\tau^{n-1}(b)}{\tau^n(b)} = 1\,,$$

sest τ^n on samasusteisendus korpusel L.

Tarvilikkus. Eeldame, et elemendi $a \in L$ norm on 1, st, $N(a) = 1$. Paneme tähele, et kuna a norm on 1, siis $a \neq 0$. Olgu $c \in L$ suvaline ning defineerime

$$\begin{aligned} d_0 &= ac\,,\\ d_1 &= [a\tau(a)]\tau(c)\,,\\ &\dots,\\ d_{n-1} &= [a\tau(a)\dots\tau^{n-1}(a)]\tau^{n-1}(c)\,. \end{aligned} \tag{3.70}$$

Paneme seejuures tähele, et

$$d_{n-1} = N(a)\tau^{n-1}(c) = \tau^{n-1}(c) \tag{3.71}$$

ning

$$d_{j+1} = a\tau(d_j)\,, \qquad j \in \{0, 1, \dots, n-2\}\,. \tag{3.72}$$

Defineerime veel

$$b = d_0 + d_1 + \dots + d_{n-1}\,.$$

Valime elemendi c selliselt, et $b \neq 0$. Oletame, et iga c valiku korral $b = 0$. Siis, arvestades võrduseid (3.70) ja (3.71), iga $c \in L$ korral kehtib

$$\lambda_0\tau^0(c) + \lambda_1\tau(c) + \dots + \lambda_{n-1}\tau^{n-1}(c) = 0\,,$$

kus $\lambda_j = a\tau(a)...\tau^j(a) \in L$, $j \in \{0, 1, ..., n-1\}$. Seejuures $\lambda_{n-1} = N(a) = 1 \neq 0$. Tulemus ütleb meile seda, et paarikaupa erinevad automorfismid τ^j, $j \in \{0, 1, ..., n-1\}$ (mis on ühtlasi ka monomorfismid korpusest L korpusesse L), on lineaarselt sõltuvad (vt definitsioon 3.2.7). See on aga vastuolus teoreemiga 3.2.8.

Seega, me saame valida elemendi c selliselt, et $b \neq 0$. Siis aga, arvestades võrduseid (3.72), võrdust (3.71) ning lõpuks veel võrduste (3.70) esimest võrdust, saame, et

$$\begin{aligned}\tau(b) &= \tau(d_0) + \tau(d_1) + \ldots + \tau(d_{n-1}) = \\ &= (1/a)(d_1 + \ldots + d_{n-1}) + \tau^n(c) = (1/a)(d_1 + \ldots + d_{n-1}) + c = \\ &= (1/a)(d_0 + d_1 + \ldots + d_{n-1}) = b/a\,,\end{aligned}$$

mistõttu $a = b/\tau(b)$. □

Teoreem 3.3.12. *Olgu $L : K$ normaalne laiend, mille aste on algarv p ning mille Galois' rühm G on tsükliline, moodustajaga τ. Sisaldagu lisaks korpus K kõiki p-astme ühejuuri. Siis leidub element $\alpha \in L$ nii, et $L = K(\alpha)$ ning $\alpha^p \in K$.*

Tõestus. Kuna laiend $L : K$ on normaalne ja lõplik, siis teoreemi 3.2.32 esimese väite põhjal $|G| = [L : K] = p$.

Kõik p-astme ühejuured moodustavad kompleksarvude korrutamise suhtes tsüklilise rühma (vt [5], lk 189, teoreem 6.8.2). Olgu ε selle rühma moodustaja. Paneme tähele, et lause eelduse tõttu $\varepsilon \in K$, mistõttu elemendi ε norm

$$N(\varepsilon) = \tau(\varepsilon)\tau^2(\varepsilon)\ldots\tau^p(\varepsilon) = \varepsilon^p = 1\,.$$

Teoreemi 3.3.11 põhjal siis

$$\varepsilon = \alpha/\tau(\alpha) \tag{3.73}$$

mingi $\alpha \in L$, $\alpha \neq 0$, korral. Näitame järgnevalt, et iga $i \in \{1, 2, ..., p\}$ korral

$$\tau^i(\alpha) = \varepsilon^{-i}\alpha\,. \tag{3.74}$$

Kui $i = 1$, siis võrdus $\tau(\alpha) = \varepsilon^{-1}\alpha$ järeldub võrdusest (3.73). Eeldame nüüd, et võrdus (3.74) kehtib juhul kui $i < k$, $k \in \{2, 3, ..., p\}$, ning näitame, et võrdus (3.74) kehtib ka juhul $i = k$. Leiame, et

$$\begin{aligned}\tau^k(\alpha) = \tau(\tau^{k-1}(\alpha)) = \tau(\varepsilon^{-(k-1)}\alpha) = \tau(\varepsilon^{-(k-1)})\tau(\alpha) = \\ = \varepsilon^{-(k-1)}\varepsilon^{-1}\alpha = \varepsilon^{-k}\alpha\end{aligned}$$

ning võrdus (3.74) kehtib seega iga $i \in \{1, 2, ..., p\}$ korral.

Võrdusest (3.74) järeldub juhul $i = p$, et $\tau(\alpha^p) = \alpha^p$. Seega, element α^p jääb invariantseks kõigi Galois' rühma elementide rakendamisel ning kuulub seetõttu korpussese $G^\dagger = K^{*\dagger}$, mis ühtib laiendi $L : K$ normaalsuse ja lõplikkuse tõttu teoreemi 3.2.32 teise väite põhjal korpusega K. St, $\alpha^p \in K$. Nüüd, kuna korpus K sisaldab kõiki p-astme ühejuuri, siis lausest 2.2.3 järeldub, et $K(\alpha)$ on polünoomi $x^p - \alpha^p$ lahutuskorpus üle K (vt lause 3.3.8 tõestust). Teoreemi 2.2.12 põhjal on laiend $K(\alpha) : K$ seega normaalne.

Veendume nüüd, et $\tau^i|_{K(\alpha)} \in \Gamma(K(\alpha) : K), \quad i \in \{1, 2, ..., p\}$. Olgu $i \in \{1, 2, ..., p\}$ suvaline. Paneme kõigepealt tähele, et lause 2.1.38 tõttu avaldub korpuse $K(\alpha)$ iga element lineaarkombinatsioonina elemendi α teatavatest astmetest üle K. Et aga korpus K sisaldab kõiki p-astme ühejuuri, siis võrduse (3.74) tõttu

$$\left(\tau^i|_{K(\alpha)}\right)(K(\alpha)) \subseteq K(\alpha)\,. \tag{3.75}$$

Nüüd, kuna τ^i on K-automorfism korpusel L, siis $\tau^i|_{K(\alpha)}$ on K-monomorfism $K(\alpha) \to K(\alpha)$. Lause 3.2.24 põhjal on $\tau^i|_{K(\alpha)}$ tegelikult K-automorfism korpusel $K(\alpha)$.

Nüüd, kuna võrduste (3.74) tõttu on kujutised $\left(\tau^i|_{K(\alpha)}\right)(\alpha)$, $i \in \{1, 2, ..., p\}$, paarikaupa erinevad, siis, arvestades ka teoreemi 3.2.32 esimest väidet (laiendi $K(\alpha) : K$ normaalsus on meil juba põhjendatud),

$$[K(\alpha) : K] = |\Gamma(K(\alpha) : K)| \geq p\,.$$

Kuna aga $[L : K] = p$, siis teoreemi 2.1.36 ja saadud võrdust kasutades saame, et $[K(\alpha) : K] = p$ ning $[L : K(\alpha)] = 1$. See aga tähendab seda, et $L = K(\alpha)$. □

Oleme nüüd valmis tõestama võrrandite radikaalides lahenduvuse kriteeriumit. Sõnastame selle järgneva teoreemina, mis kannab nime Galois' teoreem.

Teoreem 3.3.13 (Galois' teoreem)**.** *Olgu $f(x) = 0$ algebraline võrrand üle korpuse K. Võrrand $f(x) = 0$ on lahenduv radikaalides siis ja ainult siis kui selle võrrandi Galois' rühm on lahenduv.*

Tõestus. Tähistame järgnevas polünoomi f lahutuskorpust üle K tähega Σ. Paneme tähele, et teoreemi 2.2.12 põhjal on laiend $\Sigma : K$ lõplik ja normaalne. See tähendab seda, et me võime kasutada Galois' teooria põhiteoreemi (teoreemi 3.2.32) laiendi $\Sigma : K$ jaoks.

Tarvilikkus. Eeldame, et võrrand $f(x) = 0$ üle K ehk polünoom f üle K on lahenduv radikaalides. Eelduse põhjal leidub selline korpus M, et $\Sigma \subseteq M$ ning, et $M : K$ on radikaalne laiend. Olgu $N : K$ laiendi $M : K$ normaalsulundiks. Meil on nüüd alamkorpuste jada

$$K \subseteq \Sigma \subseteq M \subseteq N\,.$$

Kuna laiend $M : K$ on radikaalne, siis lause 3.3.6 põhjal on $N : K$ normaalne ja radikaalne laiend ning seega ka lõplik (lause 3.3.4). Lause 3.3.9 põhjal on rühm $\Gamma(N : K)$ lahenduv. Rakendame teoreemi 3.2.32, võttes laiendi $L : K$ rolli laiendi $N : K$. Kuna laiend $\Sigma : K$ on normaalne, siis teoreemi 3.2.32 viienda väite põhjal

$$\Gamma(\Sigma : K) \cong \Gamma(N : K)/\Gamma(N : \Sigma)\,.$$

Teoreemi 1.2.12 ja lause 1.2.7 põhjal on nüüd vaadeldava võrrandi Galois' rühm $\Gamma(\Sigma : K)$ lahenduv.

Piisavus. Eeldame nüüd, et võrrandi $f(x) = 0$ Galois' rühm $G = \Gamma(\Sigma : K)$ on lahenduv. See tähendab seda, et rühmal G leidub normaaljada, mille faktorid on Abeli rühmad. Lausele 1.2.16 eelneva arutelu põhjal leheküljel 12, võime seega vaadelda rühma G kompositsioonijada

$$G = G_0 \supsetneqq G_1 \supsetneqq \ldots \supset G_{n-1} \supsetneqq G_n = \{1\}\,, \tag{3.76}$$

mille faktorid on Abeli rühmad. Seejuures lause 1.2.16 põhjal on jada (3.76) faktorid algarvulist järku tsüklilised rühmad. Olgu seega algarv p_i faktorrühma G_{i-1}/G_i järk ($i \in \{1, 2, ..., n\}$). Lause 3.2.2 põhjal vastab alamrühmade jadale (3.76) polünoomi f lahutuskorpuse Σ alamkorpuste jada

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{n-1} \subseteq K_n = \Sigma\,, \tag{3.77}$$

kus $K_i = G_i^\dagger$, $i \in \{0, 1, 2, ..., n\}$ (teoreemi 3.2.32 põhjal seejuures $K_0 = G_0^\dagger = G^\dagger = K^{*\dagger} = K$). Kuna $G_i \trianglelefteq G_{i-1}$, siis teoreemi 3.2.32 teise, neljanda ja viienda väite põhjal on laiendid $K_i : K_{i-1}$ normaalsed ning

$$\Gamma(K_i : K_{i-1}) \cong K_{i-1}^*/K_i^* = G_{i-1}/G_i\,, \tag{3.78}$$

$i \in \{1, 2, ..., n\}$. Lause 2.1.43 põhjal on vaadeldavad laiendid $K_i : K_{i-1}$ ($i \in \{1, 2, ..., n\}$) ka lõplikud. Kasutades Galois' teooria põhiteoreemi nüüd iga laiendi $K_i : K_{i-1}$ ($i \in \{1, 2, ..., n\}$) jaoks eraldi, saame selle teoreemi 1. väite põhjal, et

$$|\Gamma(K_i : K_{i-1})| = [K_i : K_{i-1}]\,. \tag{3.79}$$

Nüüd, võrdustest (3.78) ja (3.79) saame, et

$$[K_i : K_{i-1}] = |G_{i-1}/G_i| = p_i\,, \qquad i \in \{1, 2, \ldots, n\}\,.$$

St, laiendite $K_i : K_{i-1}$ astmed on algarvud ($i \in \{1, 2, ..., n\}$). Olgu järgnevas $i \in \{1, 2, ..., n\}$ suvaline. Kuna laiend $K_i : K_{i-1}$ on lõplik, siis lause 2.1.44 põhjal leidub lõplik arv selliseid korpuse K_i elemente α_1, α_2, ..., α_s, et

$$K_i = K_{i-1}(\alpha_1, \alpha_2, \ldots, \alpha_s)\,.$$

Nüüd lause 2.1.10 ja järelduse 2.1.37 põhjal

$$[K_i : K_{i-1}] = [K_{i-1}(\alpha_1, \alpha_2, \ldots, \alpha_{s-1})(\alpha_s) : K_{i-1}(\alpha_1, \alpha_2, \ldots, \alpha_{s-1})] \cdot \\ \cdot [K_{i-1}(\alpha_1, \alpha_2, \ldots, \alpha_{s-2})(\alpha_{s-1}) : K_{i-1}(\alpha_1, \alpha_2, \ldots, \alpha_{s-2})] \cdot \ldots \\ \ldots \cdot [K_{i-1}(\alpha_1)(\alpha_2) : K_{i-1}(\alpha_1)] \cdot [K_{i-1}(\alpha_1) : K_{i-1}] \,. \quad (3.80)$$

Kuna laiendi $K_i : K_{i-1}$ aste on algarv, siis peavad võrduse (3.80) paremal pool olevas korrutises kõik korrutatavad peale ühe võrduma ühega. See aga tähendab seda, et leidub element $\xi \in K_i \setminus K_{i-1}$ nii, et $K_i = K_{i-1}(\xi)$ ($\xi = \alpha_j$ mingi indeksi $j \in \{1, 2, ..., s\}$ korral). Kuna $i \in \{1, 2, ..., n\}$ oli suvaline, siis sellega oleme näidanud, et kõik laiendid $K_i : K_{i-1}$ on lihtlaiendid, mille aste on algarv p_i ($i \in \{1, 2, ..., n\}$). Adjungeerime nüüd igale korpusele K_i ($i \in \{0, 1, 2, ..., n\}$) kõik p_1-, p_2-, ..., p_n-astme ühejuured. Seda tehes saame korpuste jada

$$K' = K'_0 \subseteq K'_1 \subseteq \ldots \subseteq K'_{n-1} \subseteq K'_n \,, \quad (3.81)$$

milles iga korpus K'_i sisaldab kõiki p_1-, p_2-, ..., p_n-astme ühejuuri, kusjuures $K_i \subseteq K'_i$ ($i \in \{0, 1, 2, ..., n\}$).

Teoreemi piisavuse osa tõestamiseks piisab nüüd näidata, et iga laiend $K'_{i+1} : K'_i$ ($i \in \{0, 1, 2, ..., n-1\}$) on kas algarvulise astmega normaallaiend, mille Galois' rühm $\Gamma(K'_{i+1} : K'_i)$ on tsükliline, või on laiend, mille aste on 1. Viimasel juhul $K'_{i+1} = K'_i$. Siis, "korrastades" vajadusel jada (3.81) nii, et sisalduvused oleksid ranged, saame lisaks teoreemi 3.3.12 ja lauset 2.1.10 kasutades, et leidub selline alamkorpuste jada

$$K' = K'_0 \subset K'_0(\theta_1) \subset K'_0(\theta_1, \theta_2) \subset \ldots \subset K'_0(\theta_1, \theta_2, \ldots, \theta_l) = K'_n \,, \quad (3.82)$$

et iga $i \in \{1, 2, ..., l\}$ korral leidub algarv q_i nii, et

$$\theta_i^{q_i} \in K'_0(\theta_1, \theta_2, \ldots, \theta_{i-1}) \,.$$

See aga tähendab definitsiooni 3.3.1 põhjal seda, et laiend $K'_n : K'$ on radikaalne. Kuna korpuse K' saime korpusest K adjungeerides viimasele teatud lõpliku arvu ühejuuri, siis on ka laiend $K' : K$ ning seega ka laiend $K'_n : K$ radikaalne. Kuna meie konstruktsiooni tõttu $L \subseteq K'_n$, siis definitsiooni 3.3.3 põhjal järelduks siit, et võrrand $f(x) = 0$ on lahenduv radikaalides.

Piirdume konkreetsuse mõttes näitamisel, et laiend $K'_1 : K'_0$ on kas algarvulise astmega normaallaiend, mille Galois' rühm $\Gamma(K'_1 : K'_0)$ on tsükliline, või on laiend, mille aste on 1. Ülejäänud laiendite $K'_{i+1} : K'_i$, $i \in \{1, 2, ..., n-1\}$, korral on tõestus analoogiline. Olgu ε_1, ε_2, ..., ε_n vastavalt p_1-, p_2-, ..., p_n-astme algjuured. Paneme tähele, et siis

$$K'_0 = K_0(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) \,, \qquad K'_1 = K_1(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) \,.$$

Eelnevalt veendusime, et laiend $K_1 : K_0$ on lihtlaiend. Olgu seega $\xi \in K_1$ selline, et $K_1 = K_0(\xi)$. Siis lauset 2.1.10 kasutades saame, et

$$K_1' = K_0(\xi)(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) = K_0(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)(\xi) = K_0'(\xi)\,,$$

millest nähtub, et ka laiend $K_1' : K_0'$ on lihtlaiend. Eelnevalt veendusime, et laiend $K_0(\xi) : K_0$ on lõplik ja normaalne. Lause 2.1.44 põhjal on ta seega ka algebraline. Olgu m algebralise lihtlaiendi $K_0(\xi) : K_0$ määrav polünoom. Paneme tähele, et kuna polünoomi m juur ξ kuulub normaalkorpusesse $K_0(\xi)$, siis m lahutub lineaartegurite korrutiseks üle $K_0(\xi)$ ning seega on korpus $K_0(\xi)$ ka vaadeldava polünoomi lahutuskorpus üle K_0 (vt lause 2.2.3). Polünoom m osutub ühtlasi ka polünoomiks üle K_0'. Definitsiooni 2.1.14 põhjal on seega ka laiend $K_0'(\xi) : K_0'$ algebraline lihtlaiend ning lause 2.1.44 põhjal ka lõplik. Olgu m' laiendi $K_0'(\xi) : K_0'$ määrav polünoom. Siis lause 2.1.20 põhjal $m' \mid m$. See aga tähendab seda, et polünoomi m' juured on ühtlasi ka polünoomi m juurteks. Kuna aga korpus $K_0(\xi)$, olles polünoomi m lahutuskorpus, sisaldab m kõiki juuri, siis sisalduvuse $K_0(\xi) = K_1 \subseteq K_1' = K_0'(\xi)$ tõttu sisaldab korpus $K_0'(\xi)$ kõiki polünoomi m' juuri ning on seetõttu m' lahutuskorpus üle K_0' (vt lause 2.2.3). Teoreemi 2.2.12 põhjal on laiend $K_0'(\xi) : K_0'$ seega normaalne.

Olgu $H = \Gamma(K_0(\xi) : K_0)$ ja $H' = \Gamma(K_0'(\xi) : K_0')$. Olgu $\alpha' \in H'$ suvaline K_0'-automorfism korpusel $K_0'(\xi)$. Kuna $K_0'(\xi)$ on polünoomi m' lahutuskorpus üle K_0', siis $\Gamma(K_0'(\xi) : K_0')$ on definitsiooni 3.1.12 põhjal polünoomi m' ja võrrandi $m'(x) = 0$ Galois' rühm. Lause 3.1.13 põhjal α' teisendab polünoomi m' juure ξ tema mingiks teiseks juureks ξ', mis kuulub seejuures eelpoolöeldu põhjal korpusesse $K_0(\xi)$. Lause 3.2.18 põhjal leidub selline K_0-automorfism α korpusel $K_0(\xi)$, et $\alpha(\xi) = \xi'$. Seega, kuna α' jätab korpuse K_0 elemendid invariantseks, siis lauset 2.1.38 kasutades võime veenduda, et $\alpha = \alpha'|_{K_0(\xi)}$. Seega saame defineerida kujutuse $\Phi : H' \to H$ võrdusega

$$\Phi(\alpha') = \alpha'|_{K_0(\xi)}\,. \tag{3.83}$$

Kui $\alpha' = \beta'$ $(\alpha', \beta' \in H')$, siis tingimuse $K_0(\xi) \subseteq K_0'(\xi)$ tõttu ka $\alpha'|_{K_0(\xi)} = \beta'|_{K_0(\xi)}$. Seega on kujutus (3.83) korrektselt defineeritud. Veendume, et Φ on monomorfism. Olgu $\alpha', \beta' \in H'$ suvalised. Siis

$$\begin{aligned}\Phi(\alpha'\beta')(\xi) &= (\alpha'\beta')|_{K_0(\xi)}(\xi) = (\alpha'\beta')(\xi) = \alpha'(\beta'(\xi)) = \\ &= \alpha'|_{K_0(\xi)}(\beta'|_{K_0(\xi)}(\xi)) = \Phi\left(\alpha'\right)(\Phi(\beta')(\xi)) = \left[\Phi(\alpha')\Phi(\beta')\right](\xi)\,,\end{aligned}$$

sest $\beta'(\xi) \in K_0(\xi)$. Seega

$$\Phi(\alpha'\beta')(\xi) = \left[\Phi(\alpha')\Phi(\beta')\right](\xi)\,,$$

mistõttu ka

$$\Phi(\alpha'\beta')(x) = \left[\Phi(\alpha')\Phi(\beta')\right](x)$$

iga $x \in K(\xi)$ korral, ehk

$$\Phi(\alpha'\beta') = \Phi(\alpha')\Phi(\beta')$$

ning Φ on seega rühmade H' ja H homomorfism. Olgu $\alpha', \beta' \in H'$ sellised, et $\alpha' \neq \beta'$. Siis $\alpha'(\xi) \neq \beta'(\xi)$, sest vastasel juhul peaks $\alpha' = \beta'$. Nüüd aga ka $\alpha'|_{K_0(\xi)} \neq \beta'|_{K_0(\xi)}$ ehk $\Phi(\alpha') \neq \Phi(\beta')$ ning Φ on injektiivne. Sellega oleme näidanud, et $\overline{H} = \operatorname{Im}\Phi$ on rühma H alamrühm (vt [5], lk 66, lause 2.5.3), kusjuures

$$\overline{H} \cong H' \,. \tag{3.84}$$

Võrduse (3.78) põhjal aga

$$H = \Gamma(K_0(\xi) : K_0) = \Gamma(K_1 : K_0) \cong K_0^*/K_1^* = G_0/G_1 \,. \tag{3.85}$$

Kuna G_0/G_1 on lahenduva rühma G kompositsioonijada (3.76) faktor, siis lause 1.2.16 põhjal on G_0/G_1 algarvulist järku tsükliline rühm. Siis aga isomorfismi (3.85) tõttu on H algarvulist järku tsükliline rühm. Kuna lõpliku rühma alamrühma järk on rühma järgu jagaja (vt [5], lk 164, teoreem 6.1.5), siis on H alamrühma $\overline{H}$ järk kas 1 või ühtib H järguga. St, $\overline{H}$ on kas üheelemendiline või ühtib rühmaga H. Paneme tähele, et teoreemi 3.2.32 esimese väite (laiendi $K_1' : K_0'$ normaalsus ja lõplikkus on meil põhjendatud) ja isomorfismi (3.84) põhjal

$$[K_1' : K_0'] = |\Gamma(K_1' : K_0')| = |H'| = \left|\overline{H}\right| \,. \tag{3.86}$$

Kui nüüd rühma $\overline{H}$ järk on üks, siis võrduse (3.86) tõttu $[K_1' : K_0'] = 1$, st $K_1' = K_0'$. Juhul kui $H = \overline{H}$, siis isomorfismi (3.84) tõttu on ka rühm H' tsükliline. See tähendab, laiendi $K_1' : K_0'$ Galois' rühm on tsükliline ning võrduse (3.86) tõttu on laiendi $K_1' : K_0'$ aste algarv.

Sellega on teoreem tõestatud. □

3.3.3 Mittelahenduv viienda astme võrrand

Teoreemi 3.3.13 rakendusena näitame nüüd lõpuks, et viienda astme algebraliste võrrandite jaoks ei leidu ühist lahendivalemit radikaalides. Selleks näitame, et leidub viienda astme võrrand, mis ei ole lahenduv radikaalides. Eelnevalt vajame järgnevat abitulemust.

Lause 3.3.14. *Olgu p algarv ning f p-astme taandumatu polünoom üle korpuse $\mathbb{Q}$. Kui vaadeldaval polünoomil on täpselt kaks kompleksarvulist juurt, siis selle polünoomi Galois' rühm on isomorfne substitutsioonide rühmaga $\mathbb{S}_p$.*

Tõestus. Olgu Σ polünoomi f lahutuskorpus ning $G = \Gamma(\Sigma : \mathbb{Q})$ polünoomi f Galois' rühm. Järelduse 2.2.6 põhjal on polünoomi f juured paarikaupa erinevad ning lause 3.1.14 põhjal on G isomorfne rühma $\mathbb{S}_p$ teatava alamrühmaga. Olgu $\hat{G}$ selleks alamrühmaks. Lause 2.2.3 põhjal tuleb polünoomi f lahutuskorpuse saamiseks adjungeerida korpusele $\mathbb{Q}$ polünoomi f kõik juured. Olgu α polünoomi f mingi juur. Paneme tähele, et f või tema mingi korpuse K elemendi kordne on laiendi $K(\alpha) : K$ määrav polünoom. Lause 2.1.39 põhjal seega $[K(\alpha) : K] = p$. Nüüd järeldust 2.1.37 kasutades, saame, et $[\Sigma : K]$ jagub algarvuga p. Teoreemi 2.2.12 põhjal on laiend $\Sigma : K$ lõplik ja normaalne ning seega teoreemi 3.2.32 esimese väite põhjal ka rühma G järk jagub algarvuga p. Cauchy teoreemi (teoreem 1.3.9) põhjal leidub rühmas G element, mille järk on p. Siis aga isomorfismi $G \cong \hat{G}$ tõttu leidub rühmas $\hat{G}$ element, mille järk on p (väide järeldub lausest 1.3.6). Järelduse 1.1.10 põhjal saab selleks elemendiks olla vaid mingi p-tsükkel, st, rühmas $\hat{G}$ leidub p-tsükkel s.

Vaatame kujutust $\phi : \mathbb{C} \to \mathbb{C}$, mis on defineeritud võrdusega

$$\phi(x + yi) = x - yi\,,$$

kus $x + yi \in \mathbb{C}$. Näites 3.1.11(1) veendusime, et ϕ on $\mathbb{R}$-automorfism korpusel $\mathbb{C}$. Polünoomi f komplekssed juured on teineteise kaaskompleksarvud (vt[5], lk 235, lemma 7.4.7). Seega, kujutus $\gamma = \phi|_\Sigma$ jätab polünoomi f kõik $p - 2$ reaalset juurt paigale, kuid kujutab polünoomi f ühe kompleksse juure tema kaaskompleksarvuks, mis eelöeldu põhjal on samuti selle polünoomi f juur. Seega, γ on $\mathbb{Q}$-monomorfism $\Sigma \to \Sigma$. Lausest 3.2.24 järeldub nüüd aga, et $\gamma \in G$. Arutlusest järeldame, et rühmas $\hat{G}$ leidub 2-tsükkel ehk transpositsioon (vt lause 3.1.14 tõestust ja sellele lausele järgnevat kommentaari leheküljel 69).

Üldisust kitsendamata võime eeldada, et rühm $\hat{G}$ sisaldab transpositsiooni (12) (võime polünoomi f juured alati ümber nummerdada). Lause 1.1.9 tõestuse põhjal leidub selline arv k, $0 < k < p$, et p-tsükkel s^k teisendab elemendi 1 elemendiks 2. Vajadusel polünoomi f juuri uuesti ümber nummerdades võime seega eeldada, et $\hat{G}$ sisaldab lisaks transpositsioonile $t = (12)$ ka p-tsüklit $c = (12...p)$. Lause tõestuseks näitame nüüd, et $\hat{G} = \mathbb{S}_p$. Paneme tähele, et

$$ctc^{-1} = (12\ldots p)(12)(p\ldots 21) = (23) \in \hat{G}\,.$$

Nüüd ka

$$(12\ldots p)(23)(p\ldots 21) = (34) \in \hat{G}\,.$$

Nii jätkates saame, et $\hat{G}$ sisaldab kõik transpositsioonid kujul $(m, m+1)$, kus $m \in \{1, 2, ..., p-1\}$. Edasi saame, et

$$(12)(23)(12) = (13) \in \hat{G}\,, \qquad (13)(34)(13) = (14) \in \hat{G}\,.$$

Analoogiliselt jätkates saame, et $\hat{G}$ sisaldab kõik transpositisoonid kujul $(1m)$, kus $m \in \{2, 3, ..., p\}$. Lõpuks, $\hat{G}$ sisaldab kõik transpositsioonid

$$(1m)(1r)(1m) = (mr)\,,$$

kus $m \neq r$, $m, r \in \{2, 3, ..., p\}$, ning seega sisaldab $\hat{G}$ rühma $\mathbb{S}_p$ kõiki transpositsioone. Teoreemi 1.1.17 põhjal on aga rühma $\mathbb{S}_p$ iga element esitatav transpositsioonide korrutisena. Seega $\hat{G} = \mathbb{S}_p$. □

Teoreem 3.3.15. *Algebraline võrrand $x^5 - 6x + 3 = 0$ ei ole lahenduv radikaalides.*

Tõestus. Tähistame $f = x^5 - 6x + 3$. Eisensteini kriteeriumi kasutades võime veenduda, et polünoom f on taandumatu üle korpuse $\mathbb{Q}$. Veendume, et vaadeldaval polünoomil leidub täpselt 3 reaalarvulist juurt. Sellisel juhul on polünoomi f ülejäänud 2 juurt kompleksarvulised ning kuna f aste 5 on algarv, siis lause 3.3.14 põhjal on vaadeldava polünoomi Galois' rühm ning seega ka võrrandi $f(x) = 0$ Galois' rühm isomorfne rühmaga $\mathbb{S}_5$. Järelduse 1.2.19 põhjal ei ole aga rühm $\mathbb{S}_5$ lahenduv ning seega lause 1.2.7 põhjal ei ole ka võrrandi $f(x) = 0$ Galois' rühm lahenduv (kui ta oleks lahenduv, siis peaks ka $\mathbb{S}_5$ olema lahenduv lause 1.2.7 põhjal). Teoreemi 3.3.13 põhjal ei ole vaadeldav võrrand seega lahenduv radikaalides.

Vaatame nüüd polünoomi f kui funktsiooni $f = f(x)$, mille määramispiirkonnaks on $\mathbb{R}$. Funktsiooni $f(x)$ nullkohad on polünoomi f reaalseteks juurteks. Paneme tähele, et $f(-2) = -17$, $f(-1) = 8$, $f(1) = -2$ ja $f(2) = 23$. Funktsioon $f(x)$ on pidev oma määramispiirkonnas ning seega pidev ka lõikudes $[-2; -1]$, $[-1; 1]$ ja $[1; 2]$, kusjuures tema väärtused vaadeldavate lõikude otspunktides on erinevate märkidega. See aga tähendab seda, et igaühes nendes vaadeldavates lõikudes leidub vähemalt üks funktsiooni $f(x)$ nullkoht (vt [3], lk 132, lemma 2). Seega, funktsiooni $f(x)$ nullkohtade arv on vähemalt 3. Funktsioon $f(x)$ on diferentseeruv oma määramispiirkonnas. Leiame, et $f'(x) = 5x^4 - 6$ ning tuletise $f'(x)$ nullkohad on $\sqrt[4]{6/5} \approx 1.05$ ja $-\sqrt[4]{6/5} \approx -1.05$. Seega, paneme tähele, et

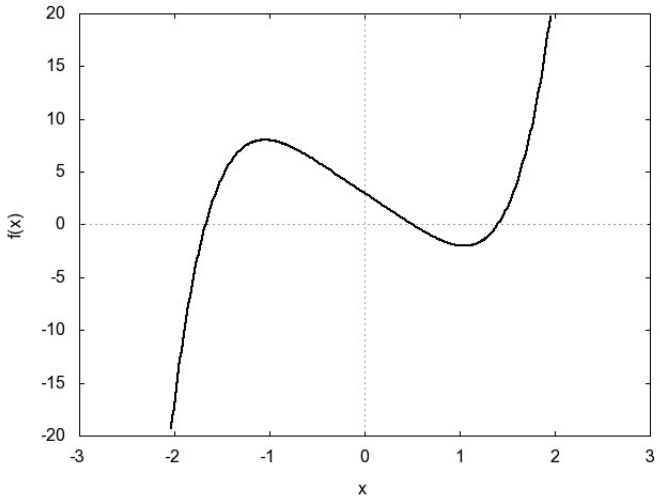
$$f'(x) > 0$$

kui $x \in (-\infty; -\sqrt[4]{6/5}) \cup (\sqrt[4]{6/5}\,; \infty)$ ning

$$f'(x) < 0$$

kui $x \in (-\sqrt[4]{6/5}\,;\ \sqrt[4]{6/5})$. Tulemus ütleb meile seda, et funktsioon $f(x)$ on rangelt kasvav vahemikes $(-\infty; -\sqrt[4]{6/5})$ ja $(\sqrt[4]{6/5}\,; \infty)$ ning rangelt kahanev vahemikus $(-\sqrt[4]{6/5}\,;\ \sqrt[4]{6/5})$ (vt [3], lk 248, lemma 2) ning seetõttu saab sel

funktsioonil igas vahemikus $(-\infty; -\sqrt[4]{6/5})$, $(-\sqrt[4]{6/5}\,;\ \sqrt[4]{6/5})$ ja $(\sqrt[4]{6/5}\,; \infty)$ olla ülimalt 1 nullkoht. Kuna aga $f(-\sqrt[4]{6/5}) \approx 8 \neq 0$ ja $f(\sqrt[4]{6/5}) \approx -2 \neq 0$, siis funktsioonil $f(x)$ saab olla ülimalt 3 nullkohta. Kuid, nagu veendusime, leidub sel funktsioonil vähemalt kolm nullkohta ning seega on funktsiooni $f(x)$ nullkohtade arv kolm ning ühtlasi on ka polünoomi f erinevate reaalarvuliste juurte arv 3. Järelduse 2.2.6 põhjal on aga polünoomi f juured paarikaupa erinevad ning seega peavad tema ülejäänud kaks juurt olema kompleksarvulised. □



Joonis 3.3: Kolme reaalarvulise juurega polünoom $f = x^5 - 6x + 3$.

3.4 Ülesanded

30. Leida kõik monomorfismid korpusest $\mathbb{Q}$ korpusesse $\mathbb{C}$.

31. Leida järgnevate laiendite Galois' rühmad.

    a. $\mathbb{Q}(\alpha) : \mathbb{Q}$, kus $\alpha = \sqrt[5]{3} \in \mathbb{R}$.

    b. $\mathbb{Q}(\beta) : \mathbb{Q}$, kus $\beta = \sqrt[7]{2} \in \mathbb{R}$.

    c. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$. (Näpunäide: Kasutada ülesannet 12.)

32. Leida eelmise ülesande laiendite normaalsulundid.

33. Näidata, et lause 3.2.23 väide ei kehti kui laiend $N : K$ ei ole normaalne, kuid kehtib iga laiendi $N : L$ korral, mille puhul $N : K$ on normaalne.

34. Olgu $L : K$ lõplik normaallaiend, mille Galois' rühm olgu G. Defineerime *jälje* $T : L \to L$ järgnevalt:

$$T(a) = \tau_1(a) + \tau_2(a) + \ldots + \tau_n(a)\,,$$

kus $a \in L$ ning paarikaupa erinevad automorfismid τ_1, τ_2, ..., τ_n kujutavad Galois' rühma kõiki elemente. Näidata, et $T(L) = K$.

35. Töötada alapunkti 3.2.4 eeskujul läbi teoreem 3.2.32, valides polünoomiks f polünoomi $x^4 - 3x^2 + 4$ üle $\mathbb{Q}$.

36. Olgu K korpus ning olgu $\alpha, \beta \in \mathbb{C}$ sellised, et $\alpha^2, \beta^2 \in K$, kuid $\alpha, \beta, \alpha\beta \notin K$. Näidata, et $\Gamma(K(\alpha, \beta) : K) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

37. Konstrueerida radikaalne laiend $L : \mathbb{Q}$ selliselt, et korpus L sisaldaks elementi $\left(\sqrt{11} - \sqrt[7]{23}\right) / \sqrt[4]{5}$.

38. Olgu p taandumatu polünoom üle korpuse K ning esitugu p mingi juur korpuse K elementide kaudu radikaalides. Tõestada, et siis p iga juur on esitatav korpuse K elementide kaudu radikaalides.

39. Näidata, et võrrand $x^5 - 4x^2 + 2 = 0$ ei ole lahenduv radikaalides.

40. Märkida järgnevad kas "tõene" (T) või "väär" (V).

    a. Erinevad automorfismid korpusel L on lineaarselt sõltumatud üle L.

    b. Lineaarselt sõltumatud automorfismid korpusel L on erinevad.

    c. Igal lõplikul korpuse laiendil leidub normaalsulund.

    d. Kui laiendi Galois' rühma järk on 1, siis see laiend on normaalne.

    e. Lõpliku normaallaiendi Galois' rühm on lõplik.

    f. Galois' vastavus ei tarvitse olla bijektiivne korpuse laiendi korral, mis ei ole normaalne.

    g. Normaallaiendi Galois' rühm on tsükliline.

    h. Kui laiend $L : K$ on normaalne ning M on vahekorpus, siis laiendi $L : M$ Galois' rühm M^* on laiendi $L : K$ Galois' rühma K^* normaalne alamrühm.

    i. Iga lõplik laiend on radikaalne.

    j. Iga taanduv viienda astme võrrand on lahenduv radikaalides.

    k. Seitsmenda astme polünoomi üle $\mathbb{Q}$, mis on taandumatu ning mille juurtest täpselt kaks on komplekssed, Galois' rühm on isomorfne rühmaga $\mathbb{S}_7$.

On the solvability of algebraic equations by radicals

Master's thesis
Raido Paas
Summary

In the thesis we studied the problem of solving the algebraic equations by radicals – a problem which has interested mathematicians for centuries. In particular we studied the group theory and the field theory which helped us to research into the matter of solving the algebraic equations by radicals. We then learned about Lagrange's idea of solving the equations of lower degree which served as a starting point for developing Galois theory. Using the latter, we were finally able to provide a criterion for solving the equations by radicals. By using that criterion we showed that not all equations of fifth degree can be solved by radicals. It became evident that in order to prove the fact a lot of work had to be done. Nevertheless, the original ideas from Lagrange and Galois are worth investigating. We just have to agree with the words of Professor Gunnar Kangro (see [1], page 154):

> *The research made by Galois presents one of the deepest and most fruitful theories, ever done by the spirit of man.*

Galois theory has been investigated further nowadays and there is an abstract theory for solving the equations by radicals. Current studying material is a good starting point for anyone who is interested in this theory.

Ülesannete vastused

1. $\{e, (123), (132)\}$.

2. $(1457)(263)$.

3. $\{e, (123), (132)\}$, $\{e, (124), (142)\}$, $\{e, (134), (143)\}$, $\{e, (234), (243)\}$.

7. Kaaselementide klassid: $\{e\}$, $\{(12), (13), (23)\}$, $\{(123), (132)\}$. Valitud elementide tsentralisaatorid: $C(e) = \{e\}$, $C((12)) = \{e, (12)\}$, $C((123)) = \{e, (123), (132)\}$.

10. *a.* T, *b.* T, *c.* V, *d.* V, *e.* V.

13. *a.* $\mathbb{Q}$, *b.* $\mathbb{Q}$, *c.* $\mathbb{Q}(i) = \{p + qi \,|\, p, q \in \mathbb{Q}\}$, *d.* $\{p + q\sqrt{5} + ri + s\sqrt{5}i \,|\, p, q, r, s \in \mathbb{Q}\}$, *e.* $\{p + q\sqrt{2} + r\sqrt{3} + s\sqrt{6} \,|\, p, q, r, s \in \mathbb{Q}\}$, *f.* $\mathbb{R}$, *g.* $\mathbb{C}$.

14. Jah, sest $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

15. *a.* $x^2 + 1$, *b.* $x^2 - x - 1/4$, *c.* $x^2 + x + 3/4$.

17. *c.*

19. Siis, kui vaadeldav element korpusest L on nullist erinev.

21. Määrav polünoom on $x^4 - 2x^2 - 2$, baas on $\left\{1, \sqrt{1 + \sqrt{3}}, \sqrt{3}, \sqrt{3 + 3\sqrt{3}}\right\}$ ning mõõde on 4.

26. Ei, näiteks juhul kui $K = \mathbb{Q}$, $m = x^3 - 2$ ning $\alpha = \sqrt[3]{2} \in \mathbb{R}$.

28. *a.*, *d.*

29. *a.* T, *b.* T, *c.* V, *d.* V, *e.* T, *f.* V, *g.* V, *h.* T, *i.* T, *j.* T, *k.* V, *l.* V (näiteks juhul kui $L = \mathbb{Q}(\alpha)$, kus $\alpha = \sqrt[4]{2} \in \mathbb{R}$, $M = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}$), *m.* V (vt ülesanne 23).

30. Leidub ainult üks.

31. *a*. $\mathbb{Z}_1$ (isomorfismi täpsuseni), *b*. $\mathbb{Z}_1$, *c*. $\mathbb{Z}_2 \times \mathbb{Z}_2$.

32. *a*. $\mathbb{Q}(\alpha, \xi) : \mathbb{Q}$, kus $\xi = e^{2\pi i/5}$, *b*. $\mathbb{Q}(\alpha, \xi) : \mathbb{Q}$, kus $\xi = e^{2\pi i/7}$, *c*. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$.

35. $\Sigma = \mathbb{Q}(\xi)$, kus $\xi = \sqrt{(3 + \sqrt{7}i)/2}$, $[\Sigma : \mathbb{Q}] = 4$, $\Gamma(\Sigma : \mathbb{Q}) \cong \mathbb{V}$ (Kleini neljarühm), vahekorpused on $\mathbb{Q}$, $\mathbb{Q}\left(\sqrt{7}i\right)$, $\mathbb{Q}\left(\sqrt{7}\right)$, $\mathbb{Q}(i)$, Σ.

37. $L = \mathbb{Q}(\alpha, \beta, \gamma)$, kus $\alpha = \sqrt{11}$, $\beta = \sqrt[7]{23}$, $\gamma = \sqrt[4]{5}$.

40. *a*. T, *b*. T, *c*. T, *d*. V, *e*. T, *f*. T, *g*. V, *h*. V, *i*. V, *j*. T, *k*. T.

Kirjandus

[1] G. Kangro, *Kõrgem algebra II*. Eesti Riiklik Kirjastus, Tartu, 1950

[2] G. Kangro, *Kõrgem algebra*. Eesti Riiklik Kirjastus, Tallinn, 1962

[3] G. Kangro, *Matemaatiline analüüs I. Teine, parandatud ja täiendatud trükk*. Valgus, Tallinn, 1982

[4] M. Kilp, *Algebra II*, Tartu, 1998

[5] M. Kilp, *Algebra I*. Eesti Matemaatika Selts, Tartu, 2005

[6] V. Laan, *Arvuteooria. Kevad* 2009 *Loengukonspekt*, 2009

[7] I. Stewart, *Galois Theory. Third Edition*. Chapman & Hall/CRC, Boca Raton, FL, 2004

[8] *Cubic function*,
http://en.wikipedia.org/wiki/Cubic_function, 3.2.2013

[9] *Dihedral group*,
http://en.wikipedia.org/wiki/Dihedral_group, 4.2.2013

[10] *Quartic function*,
http://en.wikipedia.org/wiki/Quartic_function, 25.11.2012

Indeks

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina Raido Paas

(sünnikuupäev: 21. september 1986)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
Algebraliste võrrandite lahenduvus radikaalides,
mille juhendaja on Mart Abel,
1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, 20. veebruar 2013