G. KANGRO

KÕRGEM ALGEBRA

II

EESTI RIIKLIK KIRJASTUS

A-17176

G. KANGRO

KÕRGEM ALGEBRA

II

EESTI RIIKLIK KIRJASTUS
TALLINN 1950 TARTU

TARTU ÜLIKOOLI
RAAMATUKOGU

Eessõna.

Seoses viimaste aastakümnete jooksul toimunud põhjaliku ümberkorraldusega algebras on tekkinud mõõdapääsematu vajadus ülikooli algebra põhikursuse niisuguseks käsitluseks, kus erikursusteni jõudnud üliõpilastel oleks võimalik oma õpingute süvendamine kõrgema algebra põhikursust ümber õppimata, nagu seda tingis algebra klassikaline esitusviis. Käesolev õpik, mis on välja kujunenud autori samanimelistest loengutest Tartu Riiklikus Ülikoolis aastail 1944—1949, taotlebki kõrgema algebra põhikursuse käsitlust vastavalt kaasaegse algebra seisukohtadele, kuivõrd seda aga lubab esimeste kursuste üliõpilaste matemaatilise arengu tase. Vastupidi senisele tavale, käsitleda kõrgemat algebrat, lineaaralgebrat ja kaasaegset algebrat omaette distsipliinidena eri autorite poolt, püütakse käesolevas õpikus neid distsipliine liita ühtseks, orgaaniliseks tervikuks.

Peatükid I—V, mis on pühendatud polünoomide algebra ja neile lineaaralgebra küsimustele (maatriksi normaalkuju teooria), mille lahendus nõuab polünoomide algebra aluste tundmist, on koostatud selliselt, et nad koos peatükkidega II—VI õpiku esimesest osast koondaksid endasse NSV Liidu ülikoolide füüsika-matemaatikateaduskondadele määratud kõrgema algebra põhikursuse, vastavalt KHM 1949. a. programmile. Ülejäänud peatükid VI—VIII moodustavad aluse algebra erikursustele, kusjuures on silmas peetud nõuet, et nende peatükkide materjal oluliselt süvendaks ja täiendaks eelnevate peatükkide ainet, eriti peatükis IV lahendamata jäänud küsimuste osas. Ühtlasi peatükid VI—VIII, sisaldades rühma-, korpuse- ja Galois teooria aluseid, annavad lugejale vajaliku baasi orienteerumiseks kaasaegse algebra mitmesugustes küsimustes.

Autor.

I. Kompleksarvud ja Hermite'i vormid. Algebrad.

§ 1. Kompleksarvud.

1. Kompleksarvude korpus. Ülemineku lineaarvõrrandite vallast kõrgema-astmeliste algebraliste võrrandite valda tuleb meil arvestada järgmist uut momenti: lineaarvõrrand

$$bx + a = 0, \quad b \neq 0$$

on alati lahenduv põhikorpuses, kuhu kuuluvad selle võrrandi kordajad a ja b, aga juba ruutvõrrand ei tarvitse omada lahendit oma kordajate korpuses, nagu see nähtub võrrandist

$$x^2 - 2 = 0,$$

mis ei ole lahenduv ratsionaalarvude korpuses (I, § 4, art. 1). See võrrand on aga lahenduv reaalarvude korpuses, omades seal lahendeid $\sqrt{2}$ ja $-\sqrt{2}$. Seevastu võrrand

$$x^2 + 1 = 0$$

ei ole lahenduv ei ratsionaal- ega reaalarvude korpuses. Järgnevas näitame, et reaalarvude korpust on omakorda võimalik nõnda laiendada, et viimane võrrand saab laiendatud korpuses lahenduvaks.

Vaatleme selleks reaalarvuliste elementidega teist järku maatrikseid

$$(1) \qquad \alpha = \begin{Vmatrix} a & -b \\ b & a \end{Vmatrix},$$

kus peadiagonaali elemendid on võrdsed ja kõrvaldiagonaali elemendid teineteise vastandarvud. Olgu

$$\beta = \begin{Vmatrix} c & -d \\ d & c \end{Vmatrix}$$

veel teine sama liiki maatriks. Toetudes maatriksarvutuse eeskirjadele (I, § 21, art. 1), leiame:

$$\alpha = \beta, \text{ kui } a = c, \; b = d$$

$$\alpha + \beta = \begin{Vmatrix} a+c & -(b+d) \\ b+d & a+c \end{Vmatrix}$$

$$\alpha\beta = \begin{Vmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{Vmatrix} \tag{2}$$

$$\alpha - \beta = \begin{Vmatrix} a-c & -(b-d) \\ b-d & a-c \end{Vmatrix}.$$

Siit nähtub, et maatriksite α ja β summa, korrutis ja vahe on jälle seda liiki maatriksid, kus peadiagonaali elemendid on võrdsed ja kõrvaldiagonaali elemendid teineteise vastandarvud, s. o. vaadeldavat liiki maatriksite hulk on kinnine liitmise, korrutamise ja lahutamise suhtes. Et aga kõik reaalarvuliste elementidega teist järku maatriksid moodustavad ringi, siis moodustavad ka maatriksid (1) ringi. Sel ajal kui maatriksite korrutis on üldiselt mittekommutatiivne, osutub siin korrutis kommutatiivseks, sest

$$\beta\alpha = \begin{Vmatrix} ca-db & -(cb+da) \\ da+cb & -db+ca \end{Vmatrix} = \alpha\beta.$$

Veel enam, maatriksid (1) mitte ainult ei kujuta kommutatiivset ringi, vaid kujutavad koguni korpust. Tõepoolest, kasutades pöördmaatriksi valemit (I, § 21, art. 1), leiame

$$\beta^{-1} = \frac{1}{c^2+d^2} \begin{Vmatrix} c & -d \\ d & c \end{Vmatrix}' = \frac{1}{c^2+d^2} \begin{Vmatrix} c & d \\ -d & c \end{Vmatrix},$$

missugune tulemus on kehtiv iga $\beta \neq 0$ puhul, sest nimetaja $c^2 + d^2$ võib olla null ainult siis, kui korraga $c = 0$ ja $d = 0$,

s. o. kui $\beta = 0$. Seega on maatriksite (1) vallas kehtiv ka jagamise seadus, kusjuures

$$(3) \quad \frac{\alpha}{\beta} = \alpha\beta^{-1} = \frac{1}{c^2+d^2}\begin{Vmatrix} a & -b \\ b & a \end{Vmatrix}\begin{Vmatrix} c & d \\ -d & c \end{Vmatrix} = \frac{1}{c^2+d^2}\begin{Vmatrix} ac+bd & -(bc-ad) \\ bc-ad & ac+bd \end{Vmatrix},$$

mistõttu maatriksid (1) moodustavadki korpuse.

Siin erikujulised maatriksid

$$\begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix}$$

kui skalaarmaatriksid kujutavad reaalarve, nii et võime kirjutada

$$\begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix} = a.$$

Silmas pidades maatriksite liitmise ja skalaariga korrutamise eeskirju, saame seega maatriksile (1) anda kuju

$$\alpha = \begin{Vmatrix} a & -b \\ b & a \end{Vmatrix} = \begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix} + \begin{Vmatrix} 0 & -b \\ b & 0 \end{Vmatrix} = a + b\begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix}$$

ehk

$$\alpha = a + bi,$$

kus

$$i = \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix}.$$

Arvutades maatriksi i ruudu, leiame

$$i^2 = \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix}\begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix} = \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix}.$$

Siin viimane maatriks kujutab arvu -1, mistõttu

$$i^2 = -1,$$

nii et maatriks i rahuldab võrrandit $x^2 + 1 = 0$. Tähendab, maatriksit (1) võib esitada kujul

$$\alpha = a + bi,$$

kus a ja b on reaalarvud ja i niisugune maatriks, mille ruut on võrdne —1-ga.

Võtame nüüd kasutusele laiendatud arvu mõiste — kompleksarvu[1] mõiste, defineerides kompleksarve kui niisuguseid reaalarvuliste elementidega teist järku maatrikseid, kus peadiagonaali elemendid on võrdsed ja kõrvaldiagonaali elemendid teineteise vastandarvud. Lihtsuse mõttes eelistame kompleksarvu maatrikskujule (1) edaspidi kuju $\alpha = a + bi$, kus suurust a nimetatakse kompleksarvu α reaalosaks ja suurust bi selle kompleksarvu imaginaarosaks. Kompleksarvu imaginaarosa bi koosneb imaginaarosa kordajast b ja imaginaarühikust i. Erijuhul, kui $b = 0$, taandub kompleksarv α reaalarvuks a. Seevastu kui $a = 0$, siis saame nn. puht-imaginaararvu bi.

Opereerimisel kompleksarvudega

$$\alpha = a + bi, \quad \beta = c + di$$

tuleb valemite (2) ja (3) põhjal arvestada järgmisi eeskirju:

$$\begin{aligned} \alpha &= \beta, \text{ kui } a = c, \ b = d \\ \alpha + \beta &= (a + c) + (b + d)i \\ \alpha\beta &= (ac - bd) + (ad + bc)i \\ \alpha - \beta &= (a - c) + (b - d)i \\ \frac{\alpha}{\beta} &= \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2} i. \end{aligned}$$

Siin korrutise ja jagatise valemid, kuigi suhteliselt komplitseeritumad, on ka kergesti meelespeetavad. Tuleb vaid silmas pidada, et arvutamine kompleksarvudega $\alpha = a + bi$ ja $\beta = c + di$ allub peale korpuse seaduste veel tingimusele $i^2 = -1$. Nii saame korrutise $\alpha\beta$ jaoks:

$$\begin{aligned} \alpha\beta = (a + bi)(c + di) &= ac + adi + bci + bdi^2 = \\ &= (ac - bd) + (ad + bc)i \end{aligned}$$

[1] Kompleksarve nimetatakse sageli (eriti geomeetrias) imaginaararvudeks.

ja jagatise $\frac{\alpha}{\beta}$ jaoks pärast lugeja ja nimetaja korrutamist suurusega $c - di$:

$$\frac{\alpha}{\beta} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac - adi + bci - bdi^2}{c^2 - (di)^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2} i .$$

Suurust $c - di$ nimetatakse kompleksarvu $\beta = c + di$ kaaskompleksiks ja märgitakse sümboliga $\overline{\beta}$, s. o.

$$\overline{\beta} = c - di .$$

Seega tuleb jagatise $\frac{\alpha}{\beta}$ leidmiseks korrutada lugejat ja nimetajat nimetaja kaaskompleksiga $\overline{\beta}$.

Näiteks kui $\alpha = 8 - i$ ja $\beta = 2 + i$, siis

$$\alpha + \beta = 10$$
$$\alpha\beta = (16 + 1) + (8 - 2)i = 17 + 6i$$
$$\alpha - \beta = 6 - 2i$$
$$\frac{\alpha}{\beta} = \frac{(8-i)(2-i)}{(2+i)(2-i)} = \frac{(16-1) + (-8-2)i}{4+1} = 3 - 2i .$$

Näitame lõppeks, et igal kompleksarvul $\alpha = a + bi$ on ruutjuur, s. o. et võrrand

$$\xi^2 = \alpha$$

omab alati kompleksarvulist lahendit $\xi = \sqrt{\alpha}$. Tõepoolest, kui seda võrrandit rahuldab kompleksarv $\xi = x + yi$, siis peab olema

$$(x + yi)^2 = a + bi$$

ehk

$$(x^2 - y^2) + 2xyi = a + bi ,$$

kust kompleksarvude võrduse põhjal

$$\text{(4)} \qquad \begin{aligned} x^2 - y^2 &= a \\ 2xy &= b . \end{aligned}$$

Tõstes võrrandid (4) ruutu, saame tulemusi liites

$$(x^2 + y^2)^2 = a^2 + b^2 ,$$

millest

$$x^2 + y^2 = \sqrt{a^2 + b^2} ,$$

kus ruutjuur tuleb võtta märgiga pluss, sest $x^2 + y^2$ ei saa olla negatiivne. Viimane võrrand moodustab koos esimese võrrandiga (4) võrrandisüsteemi

$$x^2 + y^2 = \sqrt{a^2 + b^2}$$
$$x^2 - y^2 = a,$$

kust leiame

$$x^2 = \frac{\sqrt{a^2 + b^2} + a}{2}, \quad y^2 = \frac{\sqrt{a^2 + b^2} - a}{2}.$$

Et $\sqrt{a + bi} = \xi = x + yi$, siis

$$(5) \qquad \sqrt{a + bi} = \pm \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} \pm i \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}.$$

Valemis (5) tuleb märkide valikul silmas pidada teist võrrandit (4), millest nähtub, et juhul $b > 0$ peavad x ja y olema ühesuguste märkidega, juhul $b < 0$ aga vastupidiste märkidega. Proovimise teel võib veenduda, et siis valemi (5) parem pool rahuldab tõepoolest võrrandit $\xi^2 = a$.

Näide 1. Leida $\sqrt{5 - 12i}$.

Silmas pidades, et siin $a = 5$, $b = -12 < 0$, saame valemit (5) rakendades

$$\sqrt{5 - 12i} = \pm \left(\sqrt{\frac{\sqrt{25 + 144} + 5}{2}} - i \sqrt{\frac{\sqrt{25 + 144} - 5}{2}} \right) =$$

$$= \pm \left(\sqrt{\frac{13 + 5}{2}} - i \sqrt{\frac{13 - 5}{2}} \right) =$$

$$= \pm (\sqrt{9} - i \sqrt{4}) = \pm (3 - 2i).$$

2. Kaaskompleksid ja kompleksarvu absoluutväärtus. Kompleksarvu $a = a + bi$ kaaskompleksiks nimetasime kompleksarvu

$$\bar{a} = a - bi.$$

Et $\bar{a}$ kaaskompleksiks on omakorda a, siis on a ja $\bar{a}$ vastastikku teineteise kaaskompleksid. Iga kompleksarvu a ja tema kaas-

kompleksi $\bar{\alpha}$ summa ja korrutis kujutavad alati reaalarve, kusjuures

$$\alpha + \bar{\alpha} = 2a, \quad \alpha\bar{\alpha} = a^2 + b^2.$$

Erijuhul, kui α kujutab reaalarvu, s. t. kui $b = 0$, saame, et $\bar{\alpha} = \alpha$. Ümberpöördult, kui $\bar{\alpha} = \alpha$, s. o.

$$a - bi = a + bi \quad \text{ehk} \quad 2bi = 0,$$

siis on $b = 0$. Tähendab, *kompleksarv kujutab reaalarvu siis ja ainult siis, kui ta ühtib oma kaaskompleksiga.*

Olgu antud kaks kompleksarvu $\alpha = a + bi$ ja $\beta = c + di$. Et

$$\alpha + \beta = (a + c) + (b + d)i, \quad \alpha\beta = (ac - bd) + (ad + bc)i,$$

siis

$$\overline{\alpha + \beta} = (a + c) - (b + d)i = (a - bi) + (c - di) = \bar{\alpha} + \bar{\beta}$$
$$\overline{\alpha\beta} = (ac - bd) - (ad + bc)i = (a - bi)(c - di) = \bar{\alpha}\bar{\beta},$$

millest

$$\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}, \quad \overline{\alpha\beta} = \bar{\alpha}\bar{\beta}.$$

Seega seades igale kompleksarvule α vastavusse tema kaaskompleksi $\bar{\alpha}$, saame automorfismi

$$\alpha \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{\alpha},$$

s. o. kompleksarvude korpuse üksühese vastavuse iseendaga, kus summale $\alpha + \beta$ vastab summa $\bar{\alpha} + \bar{\beta}$ ja korrutisele $\alpha\beta$ korrutis $\bar{\alpha}\bar{\beta}$. Siit järeldub (I, § 9, art. 2), et ka

$$\overline{\alpha - \beta} = \bar{\alpha} - \bar{\beta}, \quad \overline{\left(\frac{\alpha}{\beta}\right)} = \frac{\bar{\alpha}}{\bar{\beta}}.$$

Üldiselt, kui ξ avaldub kompleksarvude $\alpha, \beta, \ldots, \lambda$ kaudu nelja põhitehte abil kujul

$$\xi = R(\alpha, \beta, \ldots, \lambda),$$

siis on

$$\bar{\xi} = R(\bar{\alpha}, \bar{\beta}, \ldots, \bar{\lambda}).$$

Nagu nägime, moodustavad kompleksarvud korpuse, s. o. kompleksarvude vallas on kehtivad kõik arvutuse põhiseadused. Seevastu järjestuse põhiseadused pole kompleksarvude vallas kehtivad. Tõepoolest, oletades, et kompleksarvude puhul leiavad aset järjestuse põhiseadused, peaks erijuhul imaginaarühiku i suhtes esinema üks kahest võimalusest: kas $i > 0$ või $i < 0$, sest võimalus $i = 0$ langeb ilmselt välja. Kui nüüd oleks $i > 0$, siis saaksime seda võrratust iseendaga korrutades vastuolulise tulemuse $i^2 > 0$ ehk $-1 > 0$. Kui aga oleks $i < 0$, siis peaks olema $-i > 0$, missugust võrratust iseendaga korrutades saaksime jälle sama vastuolulise tulemuse $i^2 > 0$ ehk $-1 > 0$. Seega ei oma mõisted „suurem" ja „väiksem" kompleksarvude vallas mõtet. Et kompleksarvud siiski leiavad laialdast rakendust matemaatilises analüüsis, siis toimub see tänu absoluutväärtuse mõiste ülekandmisele kompleksarvude valda.

Kompleksarvu $\alpha = a + bi$ absoluutväärtuseks ehk mooduliks nimetatakse mittenegatiivset ruutjuurt $\sqrt{a^2 + b^2}$ ja teda märgitakse sümboliga $|\alpha|$, nii et

$$|\alpha| = \sqrt{a^2 + b^2}$$

ehk

$$|\alpha| = \sqrt{\alpha\bar{\alpha}},$$

sest $\alpha\bar{\alpha} = a^2 + b^2$. On ilmne, et

$$|-\alpha| = |\alpha|, \quad |\bar{\alpha}| = |\alpha|.$$

Erijuhul, kui $b = 0$, s. o. kui α kujutab reaalarvu a, on

$$|\alpha| = \sqrt{a^2} = |a|,$$

millest nähtub, et kompleksarvu absoluutväärtus üldistab reaalarvu absoluutväärtuse mõistet. Näitame, et reaalarvude summa, vahe, korrutise ja jagatise absoluutväärtuse omadused jäävad kehtima ka kompleksarvude vallas, s. o. et

$$\begin{gathered} |\alpha| - |\beta| \leqslant |\alpha + \beta| \leqslant |\alpha| + |\beta| \\ |\alpha| - |\beta| \leqslant |\alpha - \beta| \leqslant |\alpha| + |\beta| \\ |\alpha\beta| = |\alpha|\,|\beta| \\ \left|\frac{\alpha}{\beta}\right| = \frac{|\alpha|}{|\beta|}. \end{gathered} \tag{6}$$

Kõigepealt on

$$|\alpha\beta| = \sqrt{\alpha\beta \cdot \overline{\alpha\beta}} = \sqrt{\alpha\beta \cdot \bar{\alpha}\bar{\beta}} = \sqrt{\alpha\bar{\alpha} \cdot \beta\bar{\beta}} =$$

$$= \sqrt{\alpha\bar{\alpha}} \cdot \sqrt{\beta\bar{\beta}} = |\alpha|\,|\beta|,$$

millega on kolmas omadus (6) tõestatud. Edasi leiame

$$|\alpha+\beta| = \sqrt{(\alpha+\beta)\,\overline{(\alpha+\beta)}} = \sqrt{(\alpha+\beta)\,(\bar{\alpha}+\bar{\beta})} =$$

$$= \sqrt{\alpha\bar{\alpha} + \alpha\bar{\beta} + \beta\bar{\alpha} + \beta\bar{\beta}} = \sqrt{|\alpha|^2 + 2R + |\beta|^2},$$

kus $2R = \alpha\bar{\beta} + \beta\bar{\alpha}$. Et $\beta\bar{\alpha}$ on $\alpha\bar{\beta}$ kaaskompleks, siis kujutab $\alpha\bar{\beta} + \beta\bar{\alpha}$ korrutise $\alpha\bar{\beta}$ kahekordset reaalosa, mistõttu R on korrutise $\alpha\bar{\beta}$ reaalosa. Nüüd on aga mistahes kompleksarvu $\alpha = a + bi$ puhul

$$|a| \leqslant \sqrt{a^2 + b^2} = |\alpha|.$$

Seega

$$|R| \leqslant |\alpha\bar{\beta}| = |\alpha|\,|\bar{\beta}| = |\alpha|\,|\beta|,$$

millest

$$-|\alpha|\,|\beta| \leqslant R \leqslant |\alpha|\,|\beta|.$$

Silmas pidades viimast võrratust, tuletub seosest

$$|\alpha+\beta| = \sqrt{|\alpha|^2 + 2R + |\beta|^2}$$

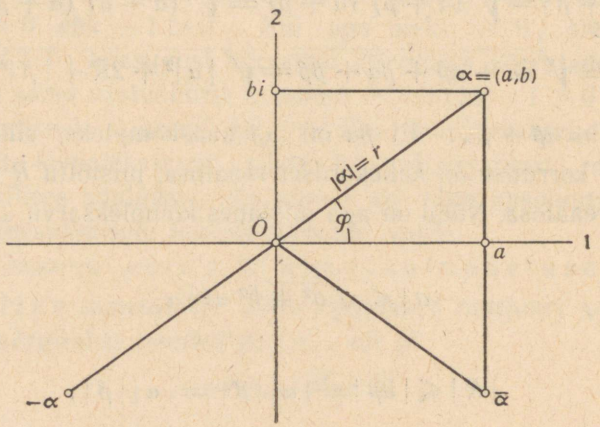
kergesti esimene omadus (6). Teine ja neljas omadus (6) tõestatakse analoogiliselt vastavalt esimese ja kolmanda omadusega (6).

Esimesed kaks kompleksarvu absoluutväärtuse omadust (6) saavad eriti läbipaistvaiks, kui interpreteerida kompleksarve geomeetriliselt.

3. **Kompleksarvude geomeetriline interpretatsioon.** Nii nagu reaalarve saab kujutada geomeetriliselt punktidena arvsirgel, kus on valitud nullpunkt ja ühikpunkt, nii saab kompleksarve

kujutada geomeetriliselt punktidena nn. komplekstasandil, kus on valitud Cartesiuse ristkoordinaadistik.

Kompleksarvu $\alpha = a + bi$ geomeetrilise kujutise all komplekstasandil mõistame niisugust punkti (a, b), mille esimeseks koordinaadiks on α reaalosa a ja teiseks koordinaadiks imaginaarosa kordaja b (joonis 1). Erijuhul, kui $b = 0$, taandub



Joonis 1.

α reaalarvuks a ja tema geomeetriline kujutis tuleb esimesele koordinaaditeljele. Kui aga $a = 0$, siis taandub α puht-imaginaararvuks bi ja tema geomeetriline kujutis tuleb teisele koordinaaditeljele. Vastavalt sellele nimetatakse komplekstasandi esimest koordinaaditelge reaalteljeks ja teist koordinaaditelge imaginaarteljeks.

On ilmne, et vastandarvude α ja $-\alpha$ kujutised asetsevad komplekstasandil sümmeetriliselt nullpunkti suhtes, kaaskomplekside α ja $\bar{\alpha}$ kujutised aga sümmeetriliselt reaaltelje suhtes. Mis puutub absoluutväärtusesse $|\alpha|$, siis kujutab viimane punkti α kaugust nullpunktist, s. o.

$$|\alpha| = O\alpha,$$

mistõttu saavad võrdused

$$|-\alpha| = |\alpha|, \quad |\bar{\alpha}| = |\alpha|$$

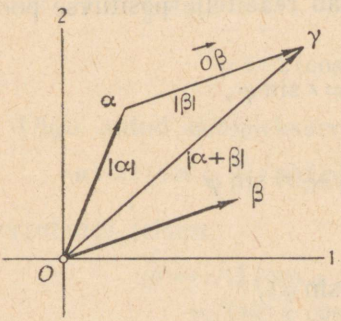
eriti läbinähtavaiks.

Kui meil on kaks kompleksarvu $\alpha = a + bi$ ja $\beta = c + di$, millele vastavad komplekstasandil punktid (a, b) ja (c, d), siis tähendab võrdus $\alpha = \beta$, et punktid (a, b) ja (c, d) langevad ühte. Tekib küsimus, kuidas interpreteerida geomeetriliselt tehteid kompleksarvudega.

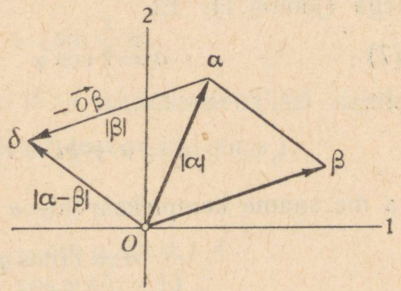
Et leida geomeetriliselt summat $\gamma = \alpha + \beta = (a + c) + (b + d)i$, vaatleme vektoreid, mis viivad nullpunktist vastavalt punktidesse α, β ja γ, s. o. kohavektoreid $\overrightarrow{O\alpha} = (a, b)$, $\overrightarrow{O\beta} = (c, d)$ ja $\overrightarrow{O\gamma} = (a + c, b + d)$. Et vektorite liitmisel tuleb nende vektorite vastavad komponendid liita, siis on

$$\overrightarrow{O\gamma} = \overrightarrow{O\alpha} + \overrightarrow{O\beta}.$$

Tähendab, *kompleksarvude liitmine taandub geomeetriliselt neile kompleksarvudele vastavate kohavektorite liitmisele* (joonis 2).



Joonis 2.



Joonis 3.

Et leida geomeetriliselt vahet $\delta = \alpha - \beta = (a - c) + (b - d)i$, vaatleme veel punkti δ viivat kohavektorit $\overrightarrow{O\delta} = (a - c, b - d)$. Vektorite lahutamise eeskirja kohaselt on

$$\overrightarrow{O\delta} = \overrightarrow{O\alpha} - \overrightarrow{O\beta}.$$

Tähendab, *kompleksarvude lahutamine taandub geomeetriliselt neile kompleksarvudele vastavate kohavektorite lahutamisele* (joonis 3).

Et kolmnurkades $O\alpha\gamma$ ja $O\alpha\delta$ on külgede pikkused vastavalt $|\alpha|$, $|\beta|$, $|\alpha+\beta|$ ja $|\alpha|$, $|\beta|$, $|\alpha-\beta|$ (joonised 2 ja 3), siis väljendavad esimesed kaks võrratust (6) kolmnurga tuntud omadust, mille järgi kolmnurgas üks külg on väiksem kui teiste külgede summa ja suurem kui teiste külgede vahe. Mis puutub esimeses kahes võrratuses (6) esinevatesse võrdusmärkidesse, siis ei ole raske näha, et need võrdusmärgid esinevad siis ja ainult siis, kui kolmnurgad $O\alpha\gamma$ ja $O\alpha\delta$ taanduvad lõikudeks.

Et nelinurgas $O\beta\alpha\delta$ on vastasküljed $O\beta$ ja $\alpha\delta$ võrdsed ja paralleelsed (joonis 3), siis kujutab nelinurk $O\beta\alpha\delta$ rööpkülikut, nii et eriti ka vastasküljed $O\delta$ ja $\alpha\beta$ tulevad võrdsed, s. o. *vahe absoluutväärtus* $|\alpha-\beta|$ *kujutab geomeetriliselt punktide* α *ja* β *vahelist kaugust.*

Kompleksarvude korrutise ja jagatise geomeetriline mõte tuleb ilmsiks, kui kasutada punkti α Cartesiuse koordinaatide a ja b asemel polaarkoordinaate r ja φ, kus $r=|\alpha|$ ja φ tähendab nurka, mille vektor $\overrightarrow{O\alpha}$ moodustab reaaltelje positiivse poolega (joonis 1). Et

$$a=r\cos\varphi, \qquad b=r\sin\varphi, \tag{7}$$

siis

$$\alpha=a+bi=r\cos\varphi+ri\sin\varphi$$

ja me saame kompleksarvule α kuju

$$\alpha=r(\cos\varphi+i\sin\varphi),$$

mis on tuntud kompleksarvu t r i g o n o m e e t r i l i s e k u j u nime all. Siin r on kompleksarvu α absoluutväärtus ehk moodul ja φ kannab kompleksarvu α a r g u m e n d i ehk a m p l i t u u d i nime ning teda märgitakse sümboliga $\arg\alpha$, s. o.

$$\varphi=\arg\alpha.$$

Et punkti α asukoht komplekstasandil ei muutu, kui muuta argu-

menti φ mingi täisarv korda 2π võrra, siis on kompleksarvu argument määratud vaid kuni 2π täisarvulise kordseni.

Kui $r \neq 0$, siis leiame argumendi φ jaoks valemeist (7)

$$\cos\varphi = \frac{a}{r}, \quad \sin\varphi = \frac{b}{r},$$

kus $r = \sqrt{a^2 + b^2}$. Mis puutub juhtu $r = 0$, siis on sel korral $a = 0$, $b = 0$ ja seega $\alpha = 0$. Arvu 0 jaoks ei defineerita argumenti, sest arv 0 on määratud juba üksi oma absoluutväärtusega $r = 0$. Seega on igal nullist erineval kompleksarvul olemas argument, mis on määratud kuni 2π täisarvulise kordseni.

Näide 2. Leida kompleksarvu $\alpha = -1 + i\sqrt{3}$ trigonomeetriline kuju.

Siin $a = -1$, $b = \sqrt{3}$ ja seega

$$r = \sqrt{a^2 + b^2} = \sqrt{1 + 3} = 2$$

$$\cos\varphi = \frac{a}{r} = \frac{-1}{2}, \quad \sin\varphi = \frac{b}{r} = \frac{\sqrt{3}}{2},$$

millest $\varphi = \frac{2}{3}\pi$, nii et

$$\alpha = 2\left(\cos\frac{2}{3}\pi + i\sin\frac{2}{3}\pi\right).$$

Olgu antud kompleksarvud α ja β trigonomeetrilisel kujul

$$\alpha = r(\cos\varphi + i\sin\varphi), \quad \beta = r_1(\cos\varphi_1 + i\sin\varphi_1).$$

Korrutades leiame

$$\alpha\beta = rr_1[(\cos\varphi\cos\varphi_1 - \sin\varphi\sin\varphi_1) + i(\sin\varphi\cos\varphi_1 + \cos\varphi\sin\varphi_1)]$$

ehk

$$\alpha\beta = rr_1[\cos(\varphi + \varphi_1) + i\sin(\varphi + \varphi_1)],$$

millest nähtub, et

$$|\alpha\beta| = rr_1, \quad \arg(\alpha\beta) = \varphi + \varphi_1.$$

Et aga $r = |\alpha|$, $r_1 = |\beta|$, $\varphi = \arg\alpha$, $\varphi_1 = \arg\beta$, siis on

$$|\alpha\beta| = |\alpha||\beta|, \quad \arg(\alpha\beta) = \arg\alpha + \arg\beta,$$

tähendab, *kompleksarvude korrutise absoluutväärtus võrdub tegurite absoluutväärtuste korrutisega ja korrutise argument tegurite argumentide summaga.* Ühtlasi oleme uuesti tuletanud kolmanda valemi (6).

Kui $\beta \neq 0$, s. o. $r_1 \neq 0$, siis leiame

$$\frac{\alpha}{\beta} = \frac{r(\cos\varphi + i\sin\varphi)(\cos\varphi_1 - i\sin\varphi_1)}{r_1(\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_1 - i\sin\varphi_1)} =$$

$$= \frac{r}{r_1}[(\cos\varphi\cos\varphi_1 + \sin\varphi\sin\varphi_1) +$$

$$+ i(\sin\varphi\cos\varphi_1 - \cos\varphi\sin\varphi_1)]$$

ehk

$$\frac{\alpha}{\beta} = \frac{r}{r_1}[\cos(\varphi - \varphi_1) + i\sin(\varphi - \varphi_1)],$$

millest nähtub, et

$$\left|\frac{\alpha}{\beta}\right| = \frac{r}{r_1}, \quad \arg\frac{\alpha}{\beta} = \varphi - \varphi_1,$$

s. o.

$$\left|\frac{\alpha}{\beta}\right| = \frac{|\alpha|}{|\beta|}, \quad \arg\frac{\alpha}{\beta} = \arg\alpha - \arg\beta.$$

Tähendab, *kompleksarvude jagatise absoluutväärtus võrdub jagatava ja jagaja absoluutväärtuste jagatisega ja jagatise argument jagatava ja jagaja argumentide vahega.* Ühtlasi oleme uuesti tuletanud neljanda valemi (6).

Nüüd ei ole enam raske leida geomeetriliselt kompleksarvude $\alpha = r(\cos\varphi + i\sin\varphi)$ ja $\beta = r_1(\cos\varphi_1 + i\sin\varphi_1)$ korrutist ja jagatist. Et saada geomeetriliselt korrutist $\alpha\beta$, konstrueerime kolmnurgale $O1\beta$ sarnase kolmnurga $O\alpha\gamma$ nii, et $O1\beta$ tippudele O ja 1 vastaksid $O\alpha\gamma$ tipud O ja α (joonis 4). Siis kolmnurga $O1\beta$ tipule β vastav $O\alpha\gamma$ tipp γ kujutabki korrutist $\alpha\beta$, s. o.

$$\gamma = \alpha\beta.$$

Tõepoolest, vektor $\overrightarrow{O\gamma}$ moodustab reaaltelje positiivse poolega nurga $\varphi + \varphi_1$, nii et $\arg\gamma = \varphi + \varphi_1$. Mis puutub γ absoluut-

väärtusse $|\gamma| = O\gamma$, siis leiame kolmnurkade $O\alpha\gamma$ ja $O1\beta$ sarnasust kasutades:

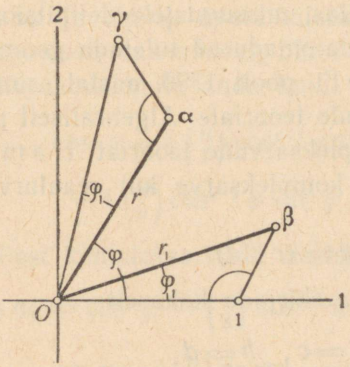
$$\frac{O\gamma}{O\alpha} = \frac{O\beta}{O1}$$

ehk

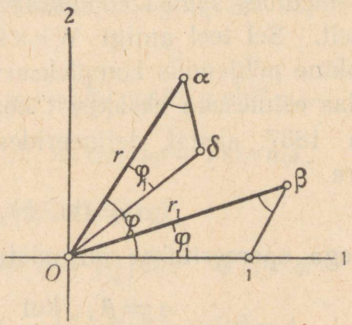
$$\frac{O\gamma}{r} = \frac{r_1}{1},$$

kust

$$O\gamma = rr_1.$$



Joonis 4.



Joonis 5.

Et saada geomeetriliselt jagatist $\frac{\alpha}{\beta}$, konstrueerime kolmnurgale $O\beta 1$ sarnase kolmnurga $O\alpha\delta$ nii, et $O\beta 1$ tippudele O ja β vastaksid $O\alpha\delta$ tipud O ja α (joonis 5). Siis kolmnurga $O\beta 1$ tipule 1 vastav $O\alpha\delta$ tipp δ kujutabki jagatist $\frac{\alpha}{\beta}$, s. o.

$$\delta = \frac{\alpha}{\beta}.$$

Tõepoolest, vektor $\overrightarrow{O\delta}$ moodustab reaaltelje positiivse poolega nurga $\varphi - \varphi_1$, nii et $\arg \delta = \varphi - \varphi_1$. Mis puutub δ absoluut-

väärtusse $|\delta| = O\delta$, siis leiame kolmnurkade $O\alpha\delta$ ja $O\beta 1$ sarnasust kasutades:

$$\frac{O\delta}{O\alpha} = \frac{O1}{O\beta}$$

ehk

$$\frac{O\delta}{r} = \frac{1}{r_1},$$

kust

$$O\delta = \frac{r}{r_1}.$$

Märkus. Ülal antud geomeetrilisi konstruktsioone võib kasutada ka ümberpöördult arvutusoperatsioonide defineerimiseks kompleksarvude vallas, missugustele definitsioonidele toetudes saab kompleksarvude omadused tuletada geomeetriliselt. Sel teel antigi Wessel'i poolt 1799. aastal esimene eksaktne põhjendus kompleksarvude teooriale. Algebraliselt põhjendas esimesena eksaktselt kompleksarvude teooriat Hamilton 1837. aastal, defineerides kompleksarve kui reaalarvude paare

$$\alpha = (a, b), \quad \beta = (c, d),$$

millega opereeritakse järgmiste eeskirjade kohaselt:

$$\alpha = \beta, \text{ kui } a = c, \quad b = d$$
$$\alpha + \beta = (a + c, b + d)$$
$$\alpha\beta = (ac - bd, ad + bc).$$

4. Kompleksarvude astendamine ja juurimine. Kui meil on n kompleksarvu

$$\alpha = r(\cos\varphi + i\sin\varphi), \quad \beta = r_1(\cos\varphi_1 + i\sin\varphi_1), \ldots,$$
$$\lambda = r_{n-1}(\cos\varphi_{n-1} + i\sin\varphi_{n-1}),$$

siis ei ole raske näha, et

$$\alpha\beta\ldots\lambda = rr_1\ldots r_{n-1}[\cos(\varphi + \varphi_1 + \ldots + \varphi_{n-1}) + i\sin(\varphi + \varphi_1 + \ldots + \varphi_{n-1})].$$

Erijuhul, kui $r = r_1 = \ldots = r_{n-1}$, $\varphi = \varphi_1 = \ldots = \varphi_{n-1}$, siis $\alpha = \beta = \ldots = \lambda$ ja ülemine valem omab kuju

$$\alpha^n = r^n(\cos n\varphi + i\sin n\varphi). \tag{8}$$

Valem (8) osutub eriti kasulikuks kõrgemate astmete arvutamisel. Nii on näiteks

$$(1+i)^{20} = \left[\sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)\right]^{20} =$$
$$= 2^{10}(\cos 5\pi + i\sin 5\pi) = -2^{10}.$$

Kirjutades valemis (8) a asemele $r(\cos\varphi + i\sin\varphi)$, leiame pärast r^n-ga jagamist

$$(\cos\varphi + i\sin\varphi)^n = \cos n\varphi + i\sin n\varphi.$$

Tulemus on tuntud Moivre'i valemi nime all. Moivre'i valemist saab kergesti tuletada trigonomeetrilised valemid $\cos n\varphi$ ja $\sin n\varphi$ avaldamiseks $\cos\varphi$ ja $\sin\varphi$ astmete kaudu. Tõepoolest, rakendades binoomvalemit (I, § 5, art. 3) võime Moivre'i valemile anda kuju

$$\cos^n\varphi + i\binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi -$$
$$- i\binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \ldots = \cos n\varphi + i\sin n\varphi,$$

millest kompleksarvude võrduse mõiste järgi

$$\cos n\varphi = \cos^n\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi + \binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi - \ldots$$
$$\sin n\varphi = \binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi +$$
$$+ \binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi - \ldots.$$

Erijuhul, kui näiteks $n=3$, saame viimastest valemitest

$$\cos 3\varphi = \cos^3\varphi - 3\cos\varphi\sin^2\varphi = \cos^3\varphi - 3\cos\varphi(1-\cos^2\varphi) =$$
$$= 4\cos^3\varphi - 3\cos\varphi$$
$$\sin 3\varphi = 3\cos^2\varphi\sin\varphi - \sin^3\varphi =$$
$$= 3(1-\sin^2\varphi)\sin\varphi - \sin^3\varphi = 3\sin\varphi - 4\sin^3\varphi.$$

Tuleme nüüd kompleksarvude juurimise küsimuse juurde. Kompleksarvu $a = r(\cos\varphi + i\sin\varphi)$ n-astme juure all mõistetakse võrrandi

$$\xi^n = a \tag{9}$$

lahendit, s. o. $\sqrt[n]{a} = \xi$. Kui võrrandil (9) leidub kompleksarvuline lahend $\xi = \varrho(\cos\Theta + i\sin\Theta)$, siis peab valemi (8) põhjal olema

$$\varrho^n(\cos n\Theta + i\sin n\Theta) = r(\cos\varphi + i\sin\varphi),$$

millest

$$\varrho^n = r, \quad n\Theta = \varphi + 2k\pi,$$

sest kompleksarvude võrduse korral on absoluutväärtused võrdsed, ent argumendid võivad erineda $2k\pi$ võrra, kus k tähendab mistahes täisarvu. Seega

$$\varrho = \sqrt[n]{r}, \quad \Theta = \frac{\varphi + 2k\pi}{n},$$

kusjuures ϱ kui võrrandi $\varrho^n = r$ positiivne lahend on üheselt määratud (I, § 4, art. 4). Et $\sqrt[n]{r(\cos\varphi + i\sin\varphi)} = \xi = \varrho(\cos\Theta + i\sin\Theta)$, siis

$$\sqrt[n]{r(\cos\varphi + i\sin\varphi)} = \sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right). \tag{10}$$

Proovimise teel võib veenduda, et valemi (10) parem pool rahuldab tõepoolest võrrandit (9).

Vastavalt igale k väärtusele saame valemist (10) ühe n-astme juure väärtuse ξ_k. Kuid kaugeltki kõik väärtused ξ_k pole üksteisest erinevad. Olgu k_0 mingi k väärtus. Jagades k_0 n-ga leiame

$$k_0 = q_0 n + r_0,$$

kus $0 \leqslant r_0 < n$ ja q_0 on teatav täisarv (I, § 7, art. 1). Seega

$$\frac{\varphi + 2k_0\pi}{n} = \frac{\varphi + 2(q_0 n + r_0)\pi}{n} = \frac{\varphi + 2r_0\pi}{n} + 2q_0\pi,$$

mistõttu valemi (10) järgi $\xi_{k_0} = \xi_{r_0}$. Et r_0 võib omada ainult n väärtust $0, 1, 2, \ldots, n-1$, siis saame n-astme juurele $\sqrt[n]{a}$ vaid n erinevat väärtust

$$\xi_0, \xi_1, \xi_2, \ldots, \xi_{n-1},$$

mis vastavad valemis (10) k väärtustele $0, 1, 2, \ldots, n-1$. Et need ξ väärtused on tõesti üksteisest erinevad, nähtub sellest, et vastavad argumendi väärtused

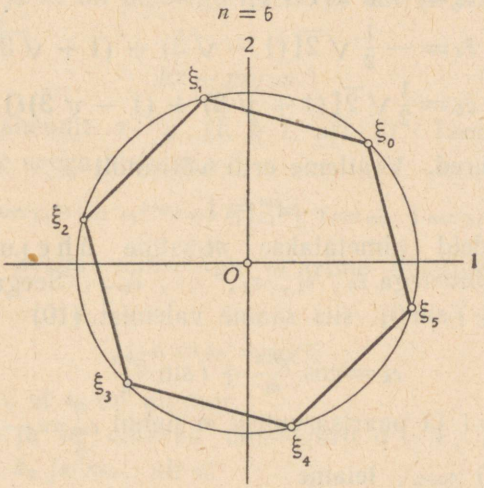
$$\frac{\varphi}{n}, \quad \frac{\varphi+2\pi}{n}, \quad \frac{\varphi+4\pi}{n}, \quad \ldots, \quad \frac{\varphi+2(n-1)\pi}{n}$$

erinevad üksteisest vähem kui 2π võrra.

Et n-astme juurtel $\sqrt[n]{a}$ on valemi (10) põhjal kõigil üks ja sama absoluutväärtus

$$|\sqrt[n]{a}| = \sqrt[n]{|a|},$$

siis asetsevad neid juuri kujutavad punktid $\xi_0, \xi_1, \xi_2, \ldots, \xi_{n-1}$ komplekstasandil ringjoonel, mis on tõmmatud nullpunktist raadiusega $\sqrt[n]{|a|}$, kusjuures vastavatest argumentidest nähtub, et punktid $\xi_0, \xi_1, \xi_2, \ldots, \xi_{n-1}$ jaotavad selle ringjoone n võrd-



Joonis 6.

seks osaks (joonis 6). *Seega kujutavad n-astme juured geomeetriliselt niisuguse korrapärase n-nurga tippe, mille keskpunkt asetseb nullpunktis.*

Näide 3. Leida $\sqrt[6]{-64i}$.

Et $-64i = 64\left(\cos\frac{3}{2}\pi + i\sin\frac{3}{2}\pi\right)$, siis saame valemist (10)

$$\sqrt[6]{-64i} = 2\left(\cos\frac{\frac{3}{2}\pi + 2k\pi}{6} + i\sin\frac{\frac{3}{2}\pi + 2k\pi}{6}\right) =$$

$$= 2\left[\cos\left(\frac{\pi}{4} + \frac{k\pi}{3}\right) + i\sin\left(\frac{\pi}{4} + \frac{k\pi}{3}\right)\right] =$$

$$= \sqrt{2}\left[\left(\cos\frac{k\pi}{3} - \sin\frac{k\pi}{3}\right) + i\left(\cos\frac{k\pi}{3} + \sin\frac{k\pi}{3}\right)\right].$$

Andes siin k-le väärtused 0, 1, 2, 3, 4, 5, leiame vastavalt:

$$\xi_0 = \sqrt{2}(1+i)$$

$$\xi_1 = \tfrac{1}{2}\sqrt{2}[(1-\sqrt{3}) + (1+\sqrt{3})i]$$

$$\xi_2 = -\tfrac{1}{2}\sqrt{2}[(1+\sqrt{3}) + (1-\sqrt{3})i]$$

$$\xi_3 = -\sqrt{2}(1+i)$$

$$\xi_4 = -\tfrac{1}{2}\sqrt{2}[(1-\sqrt{3}) + (1+\sqrt{3})i]$$

$$\xi_5 = \tfrac{1}{2}\sqrt{2}[(1+\sqrt{3}) + (1-\sqrt{3})i].$$

5. Ühejuured. Vaatleme eriti võrrandit

$$\xi^m = 1,$$

mille lahendeid nimetatakse m-astme ühejuurteks ja märgitakse tähtedega ε_0, ε_1, ε_2, ..., ε_{m-1}. Seega $\varepsilon_k{}^m = 1$. Et $1 = 1(\cos 0 + i\sin 0)$, siis saame valemist (10)

$$\varepsilon_k = \cos\frac{2k\pi}{m} + i\sin\frac{2k\pi}{m}. \tag{11}$$

Eriti on $\varepsilon_0 = 1$ ja paarisarvulise m puhul $\varepsilon_{\frac{m}{2}} = -1$. Arvutades valemist (11) ε_{m-k}, leiame

$$\varepsilon_{m-k} = \cos\frac{2(m-k)\pi}{m} + i\sin\frac{2(m-k)\pi}{m} =$$

$$= \cos\left(2\pi - \frac{2k\pi}{m}\right) + i\sin\left(2\pi - \frac{2k\pi}{m}\right) = \cos\frac{2k\pi}{m} - i\sin\frac{2k\pi}{m},$$

s. o. ühejuured ε_k ja ε_{m-k} kujutavad kaaskomplekse.

Komplekstasandil tulevad m-astme ühejuurte kujutised ühikringjoonele, moodustades korrapärase m-nurga tipud, kusjuures üheks tipuks on alati punkt 1.

Vaatleme eriti ühejuurt ε_1, mis avaldub valemi (11) järgi kujul

$$\varepsilon_1 = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}.$$

Moivre'i valemi põhjal (art. 4) võime kirjutada

$$\varepsilon_k = \varepsilon_1^k,$$

s. o. kõik m-astme ühejuured saadakse ühejuurest ε_1 astendamise teel. Niisugust ühejuurt, mille astendamisel saadakse kõik sama astme ühejuured, nimetatakse algjuureks. Tekib küsimus, missugused m-astme ühejuurtest on veel algjuured peale ε_1. Eritleme kahte juhtu selle järgi, kas ühejuure ε_k puhul m ja indeks k on ühistegurita või mitte.

1⁰ Kui k ja m on ühistegurita, s. o. kui $(k, m) = 1$, siis omab võrrand

$$kx + my = 1$$

täisarvulist lahendit x, y (I, § 7, art. 2). Toetudes seosele $\varepsilon_k = \varepsilon_1^k$, võime seega kirjutada

$$\varepsilon_k^x = \varepsilon_1^{kx} = \varepsilon_1^{1-my} = \varepsilon_1(\varepsilon_1^m)^{-y} = \varepsilon_1 \cdot 1 = \varepsilon_1,$$

s. o. $\varepsilon_1 = \varepsilon_k^x$. Seega võime iga m-astme ühejuure ε_j esitada kujul

$$\varepsilon_j = \varepsilon_1^j = \varepsilon_k^{xj},$$

millest nähtub, et ε_k on algjuur.

2⁰ Kui k ja m omavad ühistegurit $d > 1$, siis leiduvad naturaalarvud k_0 ja m_0, nii et

$$k = k_0 d, \quad m = m_0 d$$

ja seega

$$\varepsilon_k^{m_0} = \varepsilon_1^{km_0} = \varepsilon_1^{k_0 dm_0} = \varepsilon_1^{k_0 m} = (\varepsilon_1^m)^{k_0} = 1^{k_0} = 1,$$

s. o. $\varepsilon_k^{m_0} = 1$, kusjuures $d > 1$ tõttu $0 < m_0 < m$.

Oletame nüüd, et ε_k on algjuur, nii et iga m-astme ühejuur ε_l avaldub teatava astmena ε_k^n. Siinjuures võib üldsust kitsendamata eeldada, et n on üks arvudest $0, 1, 2, \ldots, m-1$, sest vastasel korral saaksime n-i jagamisel m-ga

$$n = qm + r, \quad 0 \leqslant r < m$$

ja seega

$$\varepsilon_k^n = \varepsilon_k^{qm+r} = (\varepsilon_k^m)^q \varepsilon_k^r = 1 \cdot \varepsilon_k^r = \varepsilon_k^r.$$

Niisiis avalduvad oletuse kohaselt kõik m-astme ühejuured astmetena

$$\varepsilon_k^0 = 1, \ \varepsilon_k^1, \ \varepsilon_k^2, \ \ldots, \ \varepsilon_k^{m-1},$$

mistõttu need astmed peavad olema kõik üksteisest erinevad. Kuid nagu nägime, on peale $\varepsilon_k^0 = 1$ veel $\varepsilon_k^{m_0} = 1$, kus $0 < m_0 < m$. Järelikult oletus, et ε_k on algjuur, ei pea paika.

Kokku võttes võime öelda, et ε_k *on algjuur siis ja ainult siis, kui* $(k, m) = 1$. Seega on näiteks 6-nda astme ühejuurtest vaid ε_1 ja ε_5 algjuured. Erijuhul, kui m kujutab algarvu, on kõik m-astme ühejuured, peale $\varepsilon_0 = 1$, algjuured.

Olgu lõppeks ξ_0 mingi m-astme juur kompleksarvust α, nii et $\xi_0^m = \alpha$. Siis kujutab iga korrutis $\xi_0 \varepsilon_k$ ka mingit m-astme juurt α-st, sest

$$(\xi_0 \varepsilon_k)^m = \xi_0^m \varepsilon_k^m = \alpha \cdot 1 = \alpha.$$

Et ühejuured $\varepsilon_0 = 1, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{m-1}$ on kõik üksteisest erinevad, siis on seda ka korrutised

$$\xi_0 \varepsilon_0 = \xi_0, \ \xi_0 \varepsilon_1, \ \xi_0 \varepsilon_2, \ \ldots, \ \xi_0 \varepsilon_{m-1},$$

esitades seega k õ i k i m-astme juuri arvust α. Nii näiteks teades 6-nda astme ühejuuri

$$\varepsilon_0 = 1, \ \varepsilon_1 = \frac{1}{2}(1 + i\sqrt{3}), \ \varepsilon_2 = -\frac{1}{2}(1 - i\sqrt{3}), \ \varepsilon_3 = -1,$$

$$\varepsilon_4 = -\frac{1}{2}(1 + i\sqrt{3}), \ \varepsilon_5 = \frac{1}{2}(1 - i\sqrt{3})$$

ja ühte 6-nda astme juurt arvust $-64i$, näiteks $\xi_0 = \sqrt{2}(1+i)$, leiame

$$\xi_1 = \xi_0\varepsilon_1 = \frac{1}{2}\sqrt{2}(1+i)(1+i\sqrt{3}) =$$
$$= \frac{1}{2}\sqrt{2}[(1-\sqrt{3}) + (1+\sqrt{3})i]$$
$$\xi_2 = \xi_0\varepsilon_2 = -\frac{1}{2}\sqrt{2}(1+i)(1-i\sqrt{3}) =$$
$$= -\frac{1}{2}\sqrt{2}[(1+\sqrt{3}) + (1-\sqrt{3})i]$$

jne., kooskõlas näite 3 tulemusega.

§ 2. Hermite'i vormid.

1. Unitaarmaatriksid. Vaatleme kompleksarvude teooria rakendusena maatriksit

$$A = \begin{Vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{Vmatrix},$$

mille elemendid a_{ik} on kompleksarvud. Asendades siin elemendid a_{ik} nende kaaskompleksidega $\bar{a}_{ik}$ ja vahetades read veergudega, saame maatriksi

$$A^* = \begin{Vmatrix} \bar{a}_{11} & \bar{a}_{21} & \dots & \bar{a}_{n1} \\ \bar{a}_{12} & \bar{a}_{22} & \dots & \bar{a}_{n2} \\ \dots & \dots & \dots & \dots \\ \bar{a}_{1n} & \bar{a}_{2n} & \dots & \bar{a}_{nn} \end{Vmatrix},$$

mis kannab A k a a s m a a t r i k s i nime. Märkides $\bar{A} = \| \bar{a}_{ik} \|$, võime seega kirjutada $A^* = \bar{A}'$. Silmas pidades, et kompleksarvude summa kaaskompleks on võrdne liidetavate kaaskomplekside summaga ja kompleksarvude korrutise kaaskompleks tegurite kaaskomplekside korrutisega (§ 1, art. 2), ei ole raske näha, et

$$(A+B)^* = A^* + B^*, \quad (AB)^* = B^*A^*.$$

Olgu A^{-1} maatriksi A pöördmaatriks. Et

$$A^{-1}A = E,$$

siis, üle minnes kaasmaatriksitele, saame

$$(A^{-1}A)^* = E^* \quad \text{ehk} \quad A^*(A^{-1})^* = E,$$

millest nähtub, et

$$(A^*)^{-1} = (A^{-1})^*.$$

Lõppeks on ilmselt $(A^*)^* = A$.

Niisugust kompleksmaatriksit, mille pöördmaatriks on võrdne kaasmaatriksiga, nimetatakse u n i t a a r m a a t r i k s i k s. Seega rahuldab unitaarmaatriks A tingimust

$$A^{-1} = A^*.$$

Erijuhul, kui maatriksi A elemendid on reaalarvud, $A^* = A'$ ja unitaarmaatriks taandub ortogonaalmaatriksiks (I, § 22, art. 2). Silmas pidades, et

$$AA^{-1} = E, \quad A^{-1}A = E,$$

saame $A^{-1} = A^*$ tõttu

$$AA^* = E, \quad A^*A = E.$$

Et

$$AA^* = \| \boldsymbol{a}_i \cdot \bar{\boldsymbol{a}}_k \|, \quad A^*A = \| \bar{\boldsymbol{a}}^i \cdot \boldsymbol{a}^k \|,$$

kus vektorid $\bar{\boldsymbol{a}}_k$ ja $\bar{\boldsymbol{a}}^i$ tähendavad vektorite $\boldsymbol{a}_k$ ja $\boldsymbol{a}^i$ k a a s v e k t o r e i d, s. o. niisuguseid vektoreid, mille komponentideks on vastavalt vektorite $\boldsymbol{a}_k$ ja $\boldsymbol{a}^i$ komponentide kaaskompleksid, siis on unitaarmaatriksi korral

$$\| \boldsymbol{a}_i \cdot \bar{\boldsymbol{a}}_k \| = E, \quad \| \bar{\boldsymbol{a}}^i \cdot \boldsymbol{a}^k \| = E,$$

millest nähtub, et [1]

$$\bar{\boldsymbol{a}}_i \cdot \boldsymbol{a}_k = \begin{cases} 1, & \text{kui } i = k \\ 0, & \text{kui } i \neq k \end{cases}$$

---

[1] Siin on suuruse $\boldsymbol{a}_i \cdot \bar{\boldsymbol{a}}_k$ asemel võetud kaaskompleks $\bar{\boldsymbol{a}}_i \cdot \boldsymbol{a}_k$, mis on lubatav, sest $\boldsymbol{a}_i \cdot \bar{\boldsymbol{a}}_k$ on reaalne.

ja

$$\bar{a}^i \cdot a^k = \begin{cases} 1, & \text{kui } i = k \\ 0, & \text{kui } i \neq k. \end{cases}$$

Kui kompleksvektori x puhul $\bar{x} \cdot x = 1$, siis öeldakse, et vektor x on u n i t a a r n o r m e e r i t u d. Kui kahe kompleksvektori x ja y puhul $\bar{x} \cdot y = 0$, siis öeldakse, et vektorid x ja y on u n i t a a r o r t o g o n a a l s e d. Tähendab, *unitaarmaatriksi reavektorid (veeruvektorid) moodustavad unitaarortogonaalse normeeritud süsteemi.*

Unitaarmaatriksit võib ka defineerida kui niisugust maatriksit, mille reavektorid (veeruvektorid) moodustavad unitaarortogonaalse normeeritud süsteemi. Seega on unitaarmaatriksi kaasmaatriks ja ühes sellega pöördmaatriks samuti unitaarsed.

Minnes võrduses $AA^* = E$ üle vastavatele determinantidele, saame

$$|A|\,|A^*| = 1.$$

Et siin $|A|$ ja $|A^*|$ kujutavad kaaskomplekse (§ 1, art. 2), siis on

$$\big||A|\big|^2 = 1,$$

kust

$$\big||A|\big| = 1,$$

s. o. *unitaarmaatriksi determinandi absoluutväärtus on* 1. Unitaarmaatriksite hulka kuulub näiteks maatriks

$$A = \begin{Vmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{Vmatrix},$$

kus $|A| = \frac{(1+i)^2}{4} - \frac{(1-i)^2}{4} = i$ ja seega tõesti $\big||A|\big| = 1$.

Olgu A ja B kaks unitaarmaatriksit, nii et

$$A^{-1} = A^*, \quad B^{-1} = B^*.$$

Siis on

$$(AB)^{-1} = B^{-1}A^{-1} = B^*A^* = (AB)^*,$$

s. o.

$$(AB)^{-1} = (AB)^*,$$

mis ütleb, et *kahe unitaarmaatriksi korrutis on ka unitaarmaatriks.*

Vaatleme lõppeks unitaarmaatriksitele vastavaid teisendusi — unitaarteisendusi. Teisendagu unitaarteisendus A vektori $\boldsymbol{x}$ vektoriks $\boldsymbol{u}$ ja vektori $\boldsymbol{y}$ vektoriks $\boldsymbol{v}$, s. o.

$$\boldsymbol{u} = A\boldsymbol{x}, \quad \boldsymbol{v} = A\boldsymbol{y}.$$

Siis, arvutades skalaarkorrutise $\bar{\boldsymbol{u}} \cdot \boldsymbol{v}$, leiame maatriksite korrutisele üle minnes (I, § 21, art. 3)

$$(12) \qquad \bar{\boldsymbol{u}} \cdot \boldsymbol{v} = \bar{\boldsymbol{u}}'\boldsymbol{v} = (\bar{A}\bar{\boldsymbol{x}})'A\boldsymbol{y} = \bar{\boldsymbol{x}}'\bar{A}'A\boldsymbol{y} = \bar{\boldsymbol{x}}'A^*A\boldsymbol{y}.$$

Et aga A on unitaarmaatriks, siis $A^*A = E$ ja seega

$$\bar{\boldsymbol{u}} \cdot \boldsymbol{v} = \bar{\boldsymbol{x}}'\boldsymbol{y} = \bar{\boldsymbol{x}} \cdot \boldsymbol{y},$$

s. o. *skalaarkorrutis $\bar{\boldsymbol{x}} \cdot \boldsymbol{y}$ on invariantne unitaarteisenduse suhtes.*

Märkus. Kompleksvektori $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ puhul nimetatakse avaldist

$$x = \sqrt{\bar{\boldsymbol{x}} \cdot \boldsymbol{x}} = \sqrt{|x_1|^2 + |x_2|^2 + \ldots + |x_n|^2}$$

vektori $\boldsymbol{x}$ pikkuseks. Kõigi kompleksvektorite hulk, kui temas on defineeritud pikkus ülalnäidatud viisil, kannab unitaarse ruumi nime. Piirdudes erijuhul ainult reaalsete vektoritega, saame nn. eukleidilise ruumi. Selle asemel, et kõnelda unitaarortogonaalsetest ja unitaarnormeeritud vektoritest, kõneldakse vastavalt ortogonaalsetest ja normeeritud vektoritest unitaarses ruumis. Analoogiliselt nimetatakse korrutist $\bar{\boldsymbol{x}} \cdot \boldsymbol{y}$ vektorite $\boldsymbol{x}$ ja $\boldsymbol{y}$ skalaarkorrutiseks unitaarses ruumis.

2. Hermite'i vormid. Kui A ei ole unitaarne, siis teisendub skalaarkorrutis $\bar{\boldsymbol{x}} \cdot \boldsymbol{y}$ valemi (12) järgi korrutiseks

$$\bar{\boldsymbol{u}} \cdot \boldsymbol{v} = \bar{\boldsymbol{x}} \cdot H\boldsymbol{y},$$

kus $H = A^*A$. Arvutades H kaasmaatriksi H^*, leiame

$$H^* = (A^*A)^* = A^*(A^*)^* = A^*A,$$

millest nähtub, et

$$H^* = H.$$

Niisugust kompleksmaatriksit, mis ühtib oma kaasmaatriksiga, nimetatakse Hermite'i ehk enesekaasmaatriksiks. Kui maatriksi H elemendid on h_{ik}, siis nähtub tingimusest $H = H^*$, et

$$h_{ik} = \bar{h}_{ki},$$

s. o. Hermite'i maatriksis kujutavad peadiagonaali suhtes sümmeetriliselt asetsevad elemendid kaaskomplekse. Eriti on peadiagonaali elementide h_{kk} korral

$$h_{kk} = \bar{h}_{kk},$$

millest järeldub (§ 1, art. 2), et Hermite'i maatriksi peadiagonaali elemendid on reaalarvud. Seega moodustavad Hermite'i maatriksi elementide reaalosad sümmeetrilise maatriksi ja imaginaarosad kaldsümmeetrilise maatriksi (I, § 22, art. 1). Hermite'i maatriksi determinant $|H|$ kujutab reaalarvu, sest

$$\overline{|H|} = |\bar{H}| = |\overline{H^*}| = |H'| = |H|.$$

Vaatleme nüüd lähemalt skalaarkorrutist

$$\boldsymbol{x} \cdot H\boldsymbol{y}.$$

Märkides siin $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$, $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$, leiame

$$\bar{\boldsymbol{x}} \cdot H\boldsymbol{y} = \sum_{i,k=1}^{n} h_{ik} \bar{x}_i y_k.$$

Niisiis kujutab skalaarkorrutis $\bar{\boldsymbol{x}} \cdot H\boldsymbol{y}$ suuruste $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n$ ja $y_1, y_2, \ldots, y_n$ suhtes bilineaarvormi (I, § 24, art. 1), mille maatriksiks on Hermite'i maatriks $H = \| h_{ik} \|$ ja mis kannab

vastavalt Hermite'i bilineaarvormi nime. Kui Hermite'i bilineaarvormis

$$y_1 = x_1, \quad y_2 = x_2, \quad \ldots, \quad y_n = x_n,$$

s. o. $\boldsymbol{y} = \boldsymbol{x}$, siis saame Hermite'i ruutvormi

$$F = \sum_{i,k=1}^{n} h_{ik} \bar{x}_i x_k$$

ehk

$$F = \bar{\boldsymbol{x}} \cdot H\boldsymbol{x}.$$

Erijuhul, kui maatriks H ja vektor $\boldsymbol{x}$ on reaalsed, taandub Hermite'i ruutvorm reaalseks ruutvormiks

$$\sum_{i,k=1}^{n} h_{ik} x_i x_k = \boldsymbol{x} \cdot H\boldsymbol{x}.$$

Hermite'i ruutvorm kujutab seega reaalse ruutvormi üldistust, kusjuures reaalsete ruutvormide põhiomadused (I, § 26) kanduvad analoogiliselt üle Hermite'i vormidele. Et siinjuures ka vastavate tõestuskäikude vahel valitseb täielik analoogia, siis piirdume järgnevas peamiselt resultaatide esitamisega.

Rakendades Hermite'i vormile $F = \bar{\boldsymbol{x}} \cdot H\boldsymbol{x}$ regulaarset lineaarteisendust $\boldsymbol{x} = P\boldsymbol{u}$, leiame

$$F = \overline{P\boldsymbol{u}} \cdot HP\boldsymbol{u} = (\overline{P\boldsymbol{u}})' HP\boldsymbol{u} = \bar{\boldsymbol{u}}' \bar{P}' HP\boldsymbol{u} = \bar{\boldsymbol{u}} \cdot P^* HP\boldsymbol{u}$$

ehk

$$F = \bar{\boldsymbol{u}} \cdot G\boldsymbol{u},$$

kus

$$G = P^* HP$$

kujutab jälle Hermite'i maatriksit, sest $H^* = H$ tõttu on

$$G^* = (P^* HP)^* = P^* H^* (P^*)^* = P^* HP = G.$$

Seega teisendab P Hermite'i vormi $\bar{\boldsymbol{x}} \cdot H\boldsymbol{x}$ uueks Hermite'i vormiks $\bar{\boldsymbol{u}} \cdot G\boldsymbol{u}$, kusjuures

$$|G| = |P^*| |H| |P| = \overline{|P|} |P| |H| = |P|^2 |H|,$$

s. o. *Hermite'i vormi determinant korrutub lineaarteisenduse rakendamisel teisenduse determinandi absoluutväärtuse ruuduga.*

Erijuhul, kui G osutub diagonaalmaatriksiks

$$G = \begin{Vmatrix} \lambda_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_r & \dots & 0 \\ 0 & 0 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 \end{Vmatrix},$$

saame Hermite'i vormile F kanoonilise kuju

$$\lambda_1 | u_1 |^2 + \lambda_2 | u_2 |^2 + \dots + \lambda_r | u_r |^2, \tag{13}$$

milles $\lambda_1, \lambda_2, \dots, \lambda_r$ kui Hermite'i maatriksi G peadiagonaali elemendid on reaalsed. Ei ole raske näha, et kanoonilist kuju (13) saab anda igale Hermite'i vormile, mille maatriksi H astak on r. Selleks tarvitseb vaid muuta maatriksis H peadiagonaali suhtes sümmeetrilised elemendid h_{ik} ja h_{ki} maatriksi ridade ja veergude kaaskomplekssete elementaarteisendustega nullideks (I, § 25, art. 2).

N ä i d e 4. Taandada Hermite'i vorm

$$F = | x_1 |^2 + | x_2 |^2 + i\bar{x}_1 x_3 - i\bar{x}_3 x_1 - i\bar{x}_2 x_4 + i\bar{x}_4 x_2 - i\bar{x}_3 x_4 + i\bar{x}_4 x_3$$

kanoonilisele kujule.

Teostame antud vormi maatriksiga

$$H = \begin{Vmatrix} 1 & 0 & i & 0 \\ 0 & 1 & 0 & -i \\ -i & 0 & 0 & -i \\ 0 & i & i & 0 \end{Vmatrix}$$

järgmised elementaarteisendused:

1⁰ liidame kolmanda reaga i-ga korrutatud esimese rea ja kolmanda veeruga $-i$-ga korrutatud esimese veeru;

2⁰ liidame neljanda reaga $-i$-ga korrutatud teise rea ja neljanda veeruga i-ga korrutatud teise veeru;

3⁰ liidame neljanda reaga i-ga korrutatud kolmanda rea ja neljanda veeruga $-i$-ga korrutatud kolmanda veeru. Tulemusena saame diagonaalmaatriksi

$$\begin{Vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{Vmatrix},$$

millele vastab F kanooniline kuju

$$|u_1|^2 + |u_2|^2 - |u_3|^2.$$

Rakendades maatriksi H veergudega teostatud elementaarteisendused samas järjekorras ühikmaatriksile E, leiame maatriksi

$$P = \begin{Vmatrix} 1 & 0 & -i & -1 \\ 0 & 1 & 0 & i \\ 0 & 0 & 1 & -i \\ 0 & 0 & 0 & 1 \end{Vmatrix}$$

millele vastav teisendus taandabki antud Hermite'i vormi F kanoonilisele kujule.

Nagu reaalset ruutvormi saab taandada kanoonilisele kujule ortogonaalteisenduse teel, nii saab Hermite'i vormi taandada kanoonilisele kujule unitaarteisenduse teel. Nagu nägime, teisendab lineaarteisendus $\boldsymbol{x} = P\boldsymbol{u}$ Hermite'i vormi $\bar{\boldsymbol{x}} \cdot H\boldsymbol{x}$ vormiks $\cdot G\boldsymbol{u}$, kus

$$G = P^* H P.$$

Erijuhul, kui P on unitaarmaatriks, on $P^* = P^{-1}$ ja seega

$$G = P^{-1} H P,$$

millest nähtub, et maatriks G on sarnane maatriksiga H. Et Hermite'i vormi kanoonilise kuju puhul peab G olema diagonaalmaatriks, siis on meil siin tegemist Hermite'i maatriksi H

taandamisega diagonaalkujule, mistõttu peavad maatriksi $P = \| p_{ik} \|$ veeruvektorid $\boldsymbol{p}^k$ rahuldama tingimust (I, § 23, art. 2)

$$H\boldsymbol{p}^k = \lambda_k \boldsymbol{p}^k \tag{14}$$

ehk üle minnes komponentidele

$$\begin{aligned} &(h_{11} - \lambda_k) p_{1k} + h_{12} p_{2k} + \ldots + h_{1n} p_{nk} = 0 \\ &h_{21} p_{1k} + (h_{22} - \lambda_k) p_{2k} + \ldots + h_{2n} p_{nk} = 0 \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &h_{n1} p_{1k} + h_{n2} p_{2k} + \ldots + (h_{nn} - \lambda_k) p_{nk} = 0 . \end{aligned} \tag{15}$$

Süsteem (15) kui homogeenne lineaarne võrrandisüsteem omab nullist erinevat lahendit siis ja ainult siis, kui λ_k rahuldab maatriksi H karakteristlikku võrrandit

$$\begin{vmatrix} h_{11} - \lambda & h_{12} & \ldots & h_{1n} \\ h_{21} & h_{22} - \lambda & \ldots & h_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ h_{n1} & h_{n2} & \ldots & h_{nn} - \lambda \end{vmatrix} = 0 \tag{16}$$

ehk

$$a_0 + a_1\lambda + a_2\lambda^2 + \ldots + a_n\lambda^n = 0 ,$$

kus $a_n = (-1)^n$. Näitame, et siin kõik kordajad a_k on reaalsed. Tõepoolest, asendades determinandis (16) suurused h_{ik} vastavalt kaaskompleksidega $\bar{h}_{ik}$, saame võrrandi

$$\bar{a}_0 + \bar{a}_1\lambda + \bar{a}_2\lambda^2 + \ldots + \bar{a}_n\lambda^n = 0 ,$$

mis peab eelmise võrrandiga ühtima langema, sest seose $h_{ik} = \bar{h}_{ki}$ tõttu ei muutu h_{ik} asendamisel $\bar{h}_{ik}$-ga determinant (16), vaid ainult tema read vahetuvad veergudega. Seega on $\bar{a}_k = a_k$, millest nähtubki, et kordajad a_k on reaalsed (§ 1, art. 2).

Algebraliste võrrandite teoorias tõestatakse (§ 12, art. 1), et igal reaalsete kordajatega algebralisel võrrandil on vähemalt üks kompleksarvuline lahend. Näitame, et võrrandi (16) lahendid on kõik reaalsed, s. o. *Hermite'i maatriksi karakteristlikud väärtused on reaalsed.* Eriti on siis ka reaalse sümmeetri-

lise maatriksi karakteristlikud väärtused kõik reaalsed. Nimelt, korrutades võrdust (14) skalaarselt vektoriga $\bar{p}^k$, saame

$$\bar{p}^k \cdot Hp^k = \lambda_k \bar{p}^k \cdot p^k,$$

millest

$$\lambda_k = \frac{\bar{p}^k \cdot Hp^k}{\bar{p}^k \cdot p^k},$$

kus lugeja ja nimetaja kujutavad Hermite'i vorme p^k suhtes. Kuid nagu nähtub Hermite'i vormi kanoonilisest kujust (13), omab Hermite'i vorm ainult reaalseid väärtusi.

Täiesti analoogiliselt reaalse ruutvormi juhuga (I, § 26, art. 1) võib nüüd tõestada, et *iga Hermite'i vormi saab unitaarteisenduse teel taandada kanoonilisele kujule.* Seejuures tuleb vaid sõnad „normeeritud" ja „ortogonaalne" asendada vastavalt sõnadega „unitaarnormeeritud" ja „unitaarortogonaalne".

Hermite'i vormide puhul kehtib ka inertsiseadus (I, § 26, art. 2): *Hermite'i vormi igas kanoonilises kujus on positiivsete (negatiivsete) liikmete arv üks ja sama sõltumata sellest, missuguse regulaarse teisendusega me taandame seda vormi kanoonilisele kujule.*

Positiivsete ja negatiivsete liikmete arvude vahe Hermite'i vormi kanoonilises kujus määrab selle vormi signatuuri. Nimetades kahte Hermite'i vormi ekvivalentseks, kui ühte vormi saab teisendada regulaarse teisenduse abil teiseks, järeldame Hermite'i vormide inertsiseadusest, et *kaks Hermite'i vormi on ekvivalentsed siis ja ainult siis, kui neil on üks ja sama astak ning üks ja sama signatuur.*

Hermite'i vormide inertsiseadus annab aluse Hermite'i vormide liigitamiseks määratud, poolmääratud ja määramata vormideks (I, § 26, art. 3). Seda, kas antud Hermite'i vorm on määratud või mitte, saab otsustada selle vormi maatriksi peadeterminantide

$$H_k = \begin{vmatrix} h_{11} & h_{12} & \dots & h_{1k} \\ h_{21} & h_{22} & \dots & h_{2k} \\ \dots & \dots & \dots & \dots \\ h_{k1} & h_{k2} & \dots & h_{kk} \end{vmatrix}, \quad k = 1, 2, \dots, n$$

järgi, mis Hermite'i maatriksite determinantidena kujutavad reaalarve. Nimelt võib näidata, et *Hermite'i vorm on positiivselt määratud siis ja ainult siis, kui vormi peadeterminandid on kõik positiivsed, ja negatiivselt määratud, kui vormi peadeterminandid on vaheldumisi negatiivsed ja positiivsed.*

§ 3. Algebrad.

1. Kvaternioonide korpus. Eesmärgiga laiendada reaalarvude korpust edasi väljapoole kompleksarvude valda vaatleme niisuguseid kompleksarvuliste elementidega teist järku maatrikseid

$$\alpha = \begin{Vmatrix} a+ci & -b+di \\ b+di & a-ci \end{Vmatrix},$$

kus peadiagonaali elemendid on kaaskompleksid ja kõrvaldiagonaali elemendid kaaskomplekside vastandarvud. Olgu

$$\beta = \begin{Vmatrix} a_1+c_1 i & -b_1+d_1 i \\ b_1+d_1 i & a_1-c_1 i \end{Vmatrix}$$

veel teine sama liiki maatriks. Toetudes maatriksarvutuse eeskirjadele (I, § 21, art. 1), leiame

$$\alpha = \beta, \text{ kui } a=a_1,\ b=b_1,\ c=c_1,\ d=d_1$$

$$\alpha+\beta = \begin{Vmatrix} (a+a_1)+(c+c_1)i & -(b+b_1)+(d+d_1)i \\ (b+b_1)+(d+d_1)i & (a+a_1)-(c+c_1)i \end{Vmatrix}$$

$$\alpha\beta = \begin{Vmatrix} A+Ci & -B+Di \\ B+Di & A-Ci \end{Vmatrix},$$

kus

$$A = aa_1 - bb_1 - cc_1 - dd_1, \qquad B = ab_1 + a_1 b + cd_1 - c_1 d,$$
$$C = ac_1 + a_1 c - bd_1 + b_1 d, \qquad D = ad_1 + a_1 d + bc_1 - b_1 c,$$

$$\alpha-\beta = \begin{Vmatrix} (a-a_1)+(c-c_1)i & -(b-b_1)+(d-d_1)i \\ (b-b_1)+(d-d_1)i & (a-a_1)-(c-c_1)i \end{Vmatrix}.$$

Saadud valemeist nähtub, et vaadeldavat liiki maatriksite hulk on kinnine liitmise, korrutamise ja lahutamise suhtes, moodus-

tades seega ringi ja nimelt mittekommutatiivse ringi, nagu selles võib kergesti veenduda.

Kasutades pöördmaatriksi valemit (I, § 21, art. 1), leiame

$$a^{-1} = \frac{1}{a^2+b^2+c^2+d^2} \begin{Vmatrix} a-ci & -b-di \\ b-di & a+ci \end{Vmatrix}' =$$

$$= \frac{1}{a^2+b^2+c^2+d^2} \begin{Vmatrix} a-ci & b-di \\ -b-di & a+ci \end{Vmatrix},$$

millest nähtub, et igal vaadeldavat liiki maatriksil on sama liiki pöördmaatriks, välja arvatud maatriks, kus $a=b=c=d=0$, s. o. nullmaatriks $a=0$. Seega on vaadeldavate maatriksite vallas kehtivad kõik korpuse postulaadid peale korrutise kommutatiivsuse seaduse ehk, teiste sõnadega, vaadeldavad maatriksid moodustavad mittekommutatiivse korpuse.

Silmas pidades maatriksite liitmise ja skalaariga korrutamise eeskirju, võime kirjutada

$$a = \begin{Vmatrix} a+ci & -b+di \\ b+di & a-ci \end{Vmatrix} = \begin{Vmatrix} a & 0 \\ 0 & a \end{Vmatrix} + \begin{Vmatrix} 0 & -b \\ b & 0 \end{Vmatrix} + \begin{Vmatrix} ci & 0 \\ 0 & -ci \end{Vmatrix} + \begin{Vmatrix} 0 & di \\ di & 0 \end{Vmatrix} =$$

$$= a + b \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix} + c \begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix} + d \begin{Vmatrix} 0 & i \\ i & 0 \end{Vmatrix}.$$

Siin maatriks $\begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix}$ kujutab imaginaarühikut i. Märkides

$$\begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix} = j, \quad \begin{Vmatrix} 0 & i \\ i & 0 \end{Vmatrix} = k,$$

saame maatriksile a kuju

$$a = a + bi + cj + dk.$$

Arvutades maatriksite i, j ja k ruudud ja omavahelised korrutised, leiame

$$\begin{array}{llll} i^2=-1, & ij=k, & ik=-j, \\ ji=-k, & j^2=-1, & jk=i, \\ ki=j, & kj=-i, & k^2=-1, \end{array} \tag{17}$$

millest eriti ilmnebki korrutise mittekommutatiivsus.

Suurused $a=a+bi+cj+dk$ on algebrasse toodud Hamiltoni poolt 1843. aastal. Nad kannavad kvaternioonide

nime. Nagu nägime, moodustavad kvaternioonid mittekommutatiivse korpuse. Kvaterniooni $a - bi - cj - dk$ nimetatakse a k a a s k v a t e r n i o o n i k s ja märgitakse sümboliga $\bar{a}$, s. o.

$$\bar{a} = a - bi - cj - dk .$$

Toetudes seostele (17), ei ole raske näha, et

$$a\bar{a} = a^2 + b^2 + c^2 + d^2 = \bar{a}a .$$

Kaaskvaternioone kasutatakse kvaternioonide jagamisel, kusjuures tuleb silmas pidada, et kvaternioonide korrutise mittekommutatiivsuse tõttu tuleb vahet teha vasakult ja paremalt jagamise vahel vastavalt võrrandite

$$\beta\xi = \alpha , \quad \eta\beta = \alpha$$

erinevusele.

N ä i d e 5. Lahendada võrrandid

$$(i + k)\xi = 1 + j , \quad \eta(i + k) = 1 + j .$$

Korrutades esimest võrrandit vasakult ja teist paremalt $i + k$ kaaskvaterniooniga $-i - k$, leiame $(i + k)(-i - k) = 2$ tõttu

$$2\xi = (-i - k)(1 + j), \quad 2\eta = (1 + j)(-i - k)$$

ehk

$$2\xi = -2k , \quad 2\eta = -2i ,$$

millest

$$\xi = -k , \quad \eta = -i .$$

2. Algebra mõiste. Kompleksarvu ja kvaterniooni mõisteid võib järgmiselt üldistada. Olgu P mingi ühikuga põhipiirkond — korpus, ring või integriteetkond. Vaatleme n-dimensionaalseid vektoreid

$$\boldsymbol{a} = (a_1 , a_2 , \ldots , a_n),$$

mille komponendid kuuluvad piirkonda P. Kõigi niisuguste vektorite hulka nimetatakse n - d i m e n s i o n a a l s e k s v e k t o r i r u u m i k s üle P ja märgitakse tähega P_n. Olgu vektoriruumis P_n defineeritud lisaks vektorite liitmise ja skalaariga

korrutamise operatsioonidele[1] veel vektorite omavaheline korrutamine nii, et see vektoriruum saaks teatavaks ringiks — kommutatiivseks või mittekommutatiivseks. Kui see vektorite omavaheline korrutamine osutub ka skalaariga korrutamise suhtes assotsiatiivseks, s. o. kui

$$(\lambda a)b = \lambda(ab) = a(\lambda b), \tag{18}$$

siis nimetatakse vektoriruumi P_n algebraks ehk hüperkomplekssüsteemiks üle P, kusjuures arv n kannab algebra järgu nime. Erijuhul, kui P_n on korpus, kõneldakse jagamisega algebrast ehk hüperkomplekskorpusest. Nii moodustavad näiteks kompleksarvud teist järku ja kvaternioonid neljandat järku jagamisega algebra üle reaalarvude korpuse.

Tekib küsimus, mis tähtsus on assotsiatiivsuse nõudel (18) algebra P_n suhtes. See nõue oleks ilmselt rahuldatud, kui skalaarid λ, s. o. põhipiirkonna P elemendid kuuluksid ise algebrasse P_n, s. o. kui algebra P_n kujutaks põhipiirkonna P laiendit. Ümberpöördult garanteerib assotsiatiivsuse nõue (18), et algebra P_n kujutab põhipiirkonna P laiendit, kui aga P_n osutub ühikuga ringiks.

Tõepoolest, olgu e ühikelement algebras P_n, nii et

$$ae = ea = a.$$

Seame igale P elemendile λ vastavusse suuruse λe algebras P_n. Siis vastavad erinevatele P elementidele λ ja μ erinevad λe ja μe, sest kui oleks $\lambda e = \mu e$, siis oleks $(\lambda - \mu)e = 0$ ja seega ka

$$[(\lambda - \mu)e]a = 0,$$

kus a võib olla mistahes suurus algebras P_n. Nüüd on aga (18) tõttu

$$[(\lambda - \mu)e]a = (\lambda - \mu)(ea) = (\lambda - \mu)a,$$

nii et $(\lambda - \mu)a = 0$. Võttes siin eriti $a = (1, 0, \ldots, 0)$, saame $\lambda - \mu = 0$, millest $\lambda = \mu$, vastupidi eeldusele.

[1] Skalaarkorrutist vaadeldakse vektoriruumis abikorrutisena.

Seega oleme saanud üksühese vastavuse

$$\lambda \longleftrightarrow \lambda e,$$

kusjuures ei ole raske näha, et see vastavus säilib tehete puhul, sest kuna

$$(\lambda + \mu)e = \lambda e + \mu e$$

ja $(\lambda\mu)e = \lambda(\mu e) = \lambda[e(\mu e)]$, nii et (18) tõttu

$$(\lambda\mu)e = (\lambda e)(\mu e),$$

siis

$$\lambda + \mu \longleftrightarrow \lambda e + \mu e, \quad \lambda\mu \longleftrightarrow (\lambda e)(\mu e),$$

s. o.

$$\lambda \overset{+}{\underset{\cdot}{\longleftrightarrow}} \lambda e.$$

Tähendab, algebras P_n on suuruste λe hulk isomorfne põhipiirkonnaga P, mistõttu võib suurusi λe vaadelda kui P elemente. Teiste sõnadega, *iga ühikuga algebra üle P kujutab põhipiirkonna P laiendit.*

Vaatleme nüüd, kuidas saab praktiliselt defineerida vektoriruumis P_n vektorite korrutist nii, et P_n muutuks algebraks. Esitame selleks vektorid

$$\boldsymbol{a} = (a_1, a_2, \ldots, a_n), \quad \boldsymbol{b} = (b_1, b_2, \ldots, b_n)$$

ühikvektorite

$$\begin{aligned} \boldsymbol{e}_1 &= (1, 0, \ldots, 0) \\ \boldsymbol{e}_2 &= (0, 1, \ldots, 0) \\ &\cdots\cdots\cdots\cdots \\ \boldsymbol{e}_n &= (0, 0, \ldots, 1) \end{aligned}$$

kaudu kujul (I, § 17, art. 3)

$$\boldsymbol{a} = a_1\boldsymbol{e}_1 + a_2\boldsymbol{e}_2 + \ldots + a_n\boldsymbol{e}_n, \quad \boldsymbol{b} = b_1\boldsymbol{e}_1 + b_2\boldsymbol{e}_2 + \ldots + b_n\boldsymbol{e}_n.$$

Kui vektoriruum P_n kujutab algebrat, siis võime esitada korrutise $\boldsymbol{ab}$ distributiivsuse seaduse ja assotsiatiivsuse nõude (18) tõttu kujul

$$\begin{aligned} \boldsymbol{ab} = {} & a_1b_1(\boldsymbol{e}_1\boldsymbol{e}_1) + a_1b_2(\boldsymbol{e}_1\boldsymbol{e}_2) + \ldots + a_1b_n(\boldsymbol{e}_1\boldsymbol{e}_n) + \\ & + a_2b_1(\boldsymbol{e}_2\boldsymbol{e}_1) + a_2b_2(\boldsymbol{e}_2\boldsymbol{e}_2) + \ldots + a_2b_n(\boldsymbol{e}_2\boldsymbol{e}_n) + \\ & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ & + a_nb_1(\boldsymbol{e}_n\boldsymbol{e}_1) + a_nb_2(\boldsymbol{e}_n\boldsymbol{e}_2) + \ldots + a_nb_n(\boldsymbol{e}_n\boldsymbol{e}_n) \end{aligned}$$

ehk lühemalt

$$ab = \sum_{i,k=1}^{n} a_i b_k (e_i e_k).$$

Siit nähtub, et algebras P_n taandub mistahes elementide a ja b korrutis ab nn. b a a s i e l e m e n t i d e $e_1, e_2, \ldots, e_n$ korrutistele $e_i e_k$. Korrutised $e_i e_k$, kui suurused algebras P_n avalduvad omakorda baasielementide kaudu kujul

$$(19) \qquad e_i e_k = \gamma_{ik}^1 e_1 + \gamma_{ik}^2 e_2 + \ldots + \gamma_{ik}^n e_n = \sum_{j=1}^{n} \gamma_{ik}^j e_j,$$

kus kordajad[1] γ_{ik}^j tähendavad kindlaid põhipiirkonna P elemente. Seega

$$(20) \qquad ab = \sum_{i,k,j=1}^{n} a_i b_k \gamma_{ik}^j e_j.$$

Kui meil on nüüd antud mingi vektoriruum P_n, siis defineerime siin kõigepealt ühikvektorite korrutised (19) nii, et sealjuures kehtiks assotsiatiivsuse seadus, s. o. nii, et oleks

$$e_i(e_k e_j) = (e_i e_k) e_j$$

iga i, k ja j puhul. Defineerides siis korrutise ab valemiga (20), ei ole raske näha, et vektoriruum P_n kujutab ringi, kusjuures leiab aset ka assotsiatiivsuse nõue (18) skalaariga korrutamise suhtes. Teiste sõnadega, valemiga (20) defineeritud korrutis määrab alati algebra, kui ainult baasielementide korrutis on assotsiatiivne. Erijuhul, kui baasielementide korrutis on kommutatiivne, saame kommutatiivse algebra.

On otstarbekas korraldada baasielementide korrutised tabelina — k o r r u t a m i s t a b e l i n a — nõnda, et korrutis $e_i e_k$ asetseks tabelis i-nda rea ja k-nda veeru lõikekohal. Nii saame näiteks kompleksarvude algebra ($e_1 = 1$, $e_2 = i$) ja kvaternioonide algebra ($e_1 = 1$, $e_2 = i$, $e_3 = j$, $e_4 = k$) jaoks vastavalt korrutamistabelid

[1] Siin j tähendab indeksit.

·	e_1	e_2
e_1	e_1	e_2
e_2	e_2	$-e_1$

	e_1	e_2	e_3	e_4
e_1	e_1	e_2	e_3	e_4
e_2	e_2	$-e_1$	e_4	$-e_3$
e_3	e_3	$-e_4$	$-e_1$	e_2
e_4	e_4	e_3	$-e_2$	$-e_1$

Näide 6. Kas korrutamistabel

	e_1	e_2	e_3
e_1	e_1	e_2	e_3
e_2	e_2	e_3	0
e_3	e_3	0	0

määrab algebra?

Kõigepealt nähtub antud tabelist, et siin korrutis on kommutatiivne, kusjuures e_1, olles neutraalne korrutamisel kõigi baasielementidega ja seega üldse kõigi elementidega, kujutab ühikelementi. Viimast asjaolu silmas pidades tarvitseb meil baasielementide korrutamise assotsiatiivsuse selgitamiseks vaadelda vaid neid korrutisi $e_i(e_ke_j)$, mida saab moodustada baasielementidest e_2 ja e_3. Selliseid korrutisi on üldse $2^3 = 8$ tükki, kuid korrutise kommutatiivsuse tõttu tarvitseb neist vaadelda ainult kahte, nimelt korrutisi

$$e_2(e_2e_3) \quad \text{ja} \quad e_2(e_3e_3).$$

Et

$$e_2(e_2e_3) = 0 = (e_2e_2)e_3$$
$$e_2(e_3e_3) = 0 = (e_2e_3)e_3,$$

siis määrab antud korrutamistabel algebra, kusjuures suuruste

$$a = a_1e_1 + a_2e_2 + a_3e_3 \quad \text{ja} \quad b = b_1e_1 + b_2e_2 + b_3e_3$$

korrutis avaldub kujul

$$\boldsymbol{ab} = a_1b_1\boldsymbol{e}_1 + (a_1b_2 + a_2b_1)\boldsymbol{e}_2 + (a_1b_3 + a_2b_2 + a_3b_1)\boldsymbol{e}_3 .$$

Olgu lõppeks $\boldsymbol{a}$ mistahes suurus algebras P_n. Et n-dimensionaalses vektoriruumis võib olla ülimalt n lineaarselt sõltumatut vektorit (I, § 17, art. 3), siis peab $\boldsymbol{a}$ astmete

$$\boldsymbol{a}^0 = \boldsymbol{e}, \boldsymbol{a}, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^n$$

vahel valitsema seos

$$c_0 + c_1\boldsymbol{a} + c_2\boldsymbol{a}^2 + \ldots + c_n\boldsymbol{a}^n = 0,$$

kus $c_0, c_1, c_2, \ldots, c_n$ on teatavad põhipiirkonna P elemendid, mis ei ole kõik korraga nullid. Tähendab, *algebras* P_n *rahuldab iga suurus* $\boldsymbol{a}$ *ülimalt n-astme võrrandit*

$$c_0 + c_1x + c_2x^2 + \ldots + c_nx^n = 0$$

üle P. Nii rahuldab näiteks kompleksarv $a = a + bi$ ruutvõrrandit

$$a^2 + b^2 - 2ax + x^2 = 0$$

ja kvaternioon $a = a + bi + cj + dk$ ruutvõrrandit

$$a^2 + b^2 + c^2 + d^2 - 2ax + x^2 = 0 .$$

3. Algebra esitus maatriksite abil. Vaatleme n-järku maatrikseid

$$A = \begin{Vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{Vmatrix},$$

mille elemendid a_{ik} kuuluvad teatavasse põhipiirkonda P. Et niisuguste maatriksite liitmist ja korrutamist skalaariga saab käsitella nagu nende maatriksite elementidest moodustatud n^2-dimensionaalsete vektorite

$$(a_{11}, a_{12}, \ldots, a_{nn})$$

liitmist ja korrutamist skalaariga, siis võib kõigi n-järku maatriksite hulka üle P vaadelda kui vektoriruumi P_{n^2}. Arvestades

ka maatriksite omavahelise korrutamise operatsiooni, mis on teatavasti assotsiatiivne skalaariga korrutamise suhtes, võime öelda, et vektoriruum P_{n^2} kujutab algebrat. Teiste sõnadega, kõik n-järku maatriksid, mille elemendid kuuluvad põhipiirkonda P, moodustavad n^2-järku algebra üle P.

Olgu E_{ik} n-järku maatriks, kus i-nda rea ja k-nda veeru elemendiks on P ühikelement ja kus kõik ülejäänud elemendid on nullid. Et

$$A = \sum_{i,k=1}^{n} a_{ik}E_{ik},$$

siis moodustavad maatriksid E_{ik} baasi maatriksite algebras P_{n^2}, kusjuures ei ole raske näha, et baasielementide E_{ik} ja E_{jl} korrutised avalduvad kujul

$$E_{ik}E_{jl} = \begin{cases} E_{il}, & \text{kui } k = j \\ 0, & \text{kui } k \neq j. \end{cases}$$

Tutvudes kompleksarvude ja kvaterniioonide algebratega, lähtusime nende esitistest maatriksite abil. Näitame, et üldiselt saab iga ühikuga algebrat esitada maatriksite abil ehk, täpsemalt: *iga ühikuga algebra on isomorfne teatava maatriksite algebraga.*

Olgu $\boldsymbol{a} = a_1\boldsymbol{e}_1 + a_2\boldsymbol{e}_2 + \ldots + a_n\boldsymbol{e}_n$ mingi suurus antud ühikuga algebras P_n. Märgime A-ga teisenduse, mis teisendab vektoriruumis P_n vektori $\boldsymbol{x}$ vektoriks $\boldsymbol{ax}$, s. o.

$$A\boldsymbol{x} = \boldsymbol{ax}.$$

Ei ole raske näha, et siin A kujutab lineaarteisendust (I, § 20, art. 1), sest kui λ tähendab mistahes elementi põhipiirkonnas P ja $\boldsymbol{x}_1$, $\boldsymbol{x}_2$ mistahes vektoreid vektoriruumis P_n, siis on

1^0 $$A(\lambda\boldsymbol{x}) = \boldsymbol{a}(\lambda\boldsymbol{x}) = \lambda(\boldsymbol{ax}) = \lambda(A\boldsymbol{x})$$

2^0 $$A(\boldsymbol{x}_1 + \boldsymbol{x}_2) = \boldsymbol{a}(\boldsymbol{x}_1 + \boldsymbol{x}_2) = \boldsymbol{ax}_1 + \boldsymbol{ax}_2 = A\boldsymbol{x}_1 + A\boldsymbol{x}_2,$$

millest ilmnebki teisenduse A lineaarsus.

Seame nüüd igale suurusele $\boldsymbol{a}$ algebras P_n vastavusse lineaarteisenduse A, mille puhul $A\boldsymbol{x} = \boldsymbol{ax}$. Siis vastavad erineva-

tele suurustele $\boldsymbol{a}$ ja $\boldsymbol{b}$ erinevad lineaarteisendused A ja B, sest kui oleks $A = B$, s. o.

$$\boldsymbol{ax} = \boldsymbol{bx},$$

siis võttes viimases võrduses $\boldsymbol{x} = \boldsymbol{e}$, kus $\boldsymbol{e}$ tähendab algebra P_n ühikelementi, saame $\boldsymbol{a} = \boldsymbol{b}$, vastupidi eeldusele.

Seega oleme saanud üksühese vastavuse

$$\boldsymbol{a} \leftrightarrow A.$$

Et võrdustest

$$A\boldsymbol{x} = \boldsymbol{ax}, \quad B\boldsymbol{x} = \boldsymbol{bx}$$

järeldub

$$(A + B)\boldsymbol{x} = (\boldsymbol{a} + \boldsymbol{b})\boldsymbol{x}$$
$$(AB)\boldsymbol{x} = A(\boldsymbol{bx}) = \boldsymbol{a}(\boldsymbol{bx}) = (\boldsymbol{ab})\boldsymbol{x},$$

siis

$$\boldsymbol{a} + \boldsymbol{b} \leftrightarrow A + B, \quad \boldsymbol{ab} \leftrightarrow AB,$$

s. o. korraldatud vastavus säilib tehete puhul [1]:

$$\boldsymbol{a} \overset{+}{\underset{\cdot}{\leftrightarrow}} A.$$

Tähendab, algebra P_n on isomorfne lineaarteisenduste ringiga $\{A\}$ ehk, mis sama on, maatriksite ringiga $\{A\}$. Maatriksi A leidmiseks peame silmas, et A veeruvektorid $\boldsymbol{a}^k$ kujutavad baasivektorite $\boldsymbol{e}_k$ teisendeid (I, § 20, art. 1), s. o.

$$\boldsymbol{a}^k = A\boldsymbol{e}_k,$$

millest

$$\boldsymbol{a}^k = \boldsymbol{ae}_k = a_1(\boldsymbol{e}_1\boldsymbol{e}_k) + a_2(\boldsymbol{e}_2\boldsymbol{e}_k) + \ldots + a_n(\boldsymbol{e}_n\boldsymbol{e}_k),$$

kus baasielementide korrūtised $\boldsymbol{e}_i\boldsymbol{e}_k$ saame korrutamistabelist.

Eriti on näites 6 vaadeldud algebra puhul

$$\boldsymbol{a} = a_1\boldsymbol{e}_1 + a_2\boldsymbol{e}_2 + a_3\boldsymbol{e}_3$$

ja seega

$$\boldsymbol{a}^1 = \boldsymbol{ae}_1 = a_1\boldsymbol{e}_1 + a_2\boldsymbol{e}_2 + a_3\boldsymbol{e}_3 = (a_1, a_2, a_3)$$
$$\boldsymbol{a}^2 = \boldsymbol{ae}_2 = a_1\boldsymbol{e}_2 + a_2\boldsymbol{e}_3 = (0, a_1, a_2)$$
$$\boldsymbol{a}^3 = \boldsymbol{ae}_3 = a_1\boldsymbol{e}_3 = (0, 0, a_1),$$

[1] Siin vastavus säilib ka skalaariga korrutamise puhul.

millest nähtub, et siin

$$A = \begin{Vmatrix} a_1 & 0 & 0 \\ a_2 & a_1 & 0 \\ a_3 & a_2 & a_1 \end{Vmatrix}.$$

Harjutusülesandeid.

1. Arvutada:

a) $\frac{(2+i)^2-2i+3}{1-i}+\frac{(2-i)^2+2i+3}{1+i}$; b) $\frac{(1-i)^7}{(1+i)^5}$;

c) $\frac{1}{\sqrt{-\frac{1}{4}-\frac{\sqrt{3}}{4}i}}$; d) $\sqrt[4]{-8+8i\sqrt{3}}$;

e) $\sqrt{4ab+2(a^2-b^2)i}$.

2. Lahendada võrrandid:

a) $x^2-(3-2i)x+5-5i=0$; b) $x^4-30x^2+289=0$;

c) $x+|x|=8+4i$; d) $x\bar{x}+3(x-\bar{x})=4-3i$.

3. Lahendada võrrandisüsteem:

$$\begin{aligned} x_1 - ix_2 - 2x_3 &= 10 \\ x_1 - x_2 - 2ix_3 &= 20 \\ -ix_1 - 3ix_2 - (1-i)x_3 &= 30. \end{aligned}$$

4. Anda kompleksarvudele

a) $\sqrt{3}-i$; b) $1+i\tan\alpha$

trigonomeetriline kuju.

5. Arvutada geomeetriliselt:

a) $(3-2i)(-2+i)-(2-5i)(1+i)$; b) $\frac{(2+i)^2+3-2i}{1-i}$.

6. Võrdkülgse kolmnurga kaks tippu asetsevad punktides 1 ja $2+i$. Leida kolmas tipp.

7. Näidata, et

$$|\alpha+\beta|^2+|\alpha-\beta|^2=2(|\alpha|^2+|\beta|^2)$$

ja anda tulemusele geomeetriline interpretatsioon.

8. Tuletada valemid $\cos 4\varphi$ ja $\sin 4\varphi$ jaoks.

9. Arvutada:

$$\text{a)}\ \left(\frac{1+i\sqrt{3}}{1-i}\right)^{20};\quad \text{b)}\ \sqrt[4]{i}.$$

10. Leida kompleksarvude

$$\text{a)}\ \left(\frac{1+i}{\sqrt{3}-i}\right)^{8}\left(\frac{1+i\sqrt{3}}{1-i}\right)^{6};\quad \text{b)}\ \frac{(1+i)^{16}\sqrt[7]{8-8i}}{(2-2i)^{14}\sqrt[5]{4+4i}}$$

absoluutväärtused.

11. Leida 8-nda astme algjuured.

12. Määrata suurused c_1, c_2, c_3 nii, et maatriks

$$\begin{Vmatrix} \frac{2}{3} & \frac{i}{3} & -\frac{2i}{3} \\ -\frac{i}{3} & \frac{2}{3} & \frac{2}{3} \\ c_1 & c_2 & c_3 \end{Vmatrix}$$

oleks unitaarne.

13. Lahendada võrrandisüsteem

$$\sum_{k=1}^{n} a_{ik}x_k=b_i,\quad i=1,\ 2,\ \ldots,\ n,$$

teades, et süsteemi maatriks on unitaarne.

14. Leida Hermite'i vormi

$$|x_1|^2-2|x_2|^2+(1+i)\bar{x}_1x_2+(1-i)\bar{x}_2x_1+i\bar{x}_2x_3-i\bar{x}_3x_2$$

determinant enne ja pärast teisendust

$$\begin{aligned} x_1&=u_1-iu_2-u_3\\ x_2&=u_1+u_2+iu_3\\ x_3&=iu_3. \end{aligned}$$

15. Taandada Hermite'i vormid

a) $|x_1|^2 + 2|x_2|^2 - |x_3|^2 + i\bar{x}_1x_2 - i\bar{x}_2x_1 - i\bar{x}_2x_3 + i\bar{x}_3x_2$;

b) $\bar{x}_1x_4 + \bar{x}_4x_1 - i\bar{x}_2x_3 + i\bar{x}_3x_2$

kanoonilisele kujule.

16. Taandada Hermite'i vormid

a) $|x_1|^2 + |x_2|^2 - 2|x_3|^2 + 2i\bar{x}_2x_3 - 2i\bar{x}_3x_2$;

b) $|x_1|^2 + |x_2|^2 + i\bar{x}_1x_3 - i\bar{x}_3x_1 - i\bar{x}_2x_4 + i\bar{x}_4x_2 - i\bar{x}_3x_4 + i\bar{x}_4x_3$

unitaarteisenduse teel kanoonilisele kujule.

17. Näidata, et Hermite'i vormid

$$H = 2|x_1|^2 - |x_3|^2 + i\bar{x}_2x_3 - i\bar{x}_3x_2$$

ja

$$G = 2|x_1|^2 + 2|x_2|^2 + |x_3|^2 - 2i\bar{x}_1x_2 + 2i\bar{x}_2x_1 - \\ - 3\bar{x}_1x_3 - 3\bar{x}_3x_1 - (1+2i)\bar{x}_2x_3 - (1-2i)\bar{x}_3x_2$$

on ekvivalentsed, ning leida teisendus, mis teisendab esimese vormi teiseks.

18. Missugused alljärgnevaist Hermite'i vormidest on määratud, ja kui on, siis kas positiivselt või negatiivselt:

a) $|x_1|^2 + |x_2|^2 + 4|x_3|^2 - \bar{x}_1x_2 - \bar{x}_2x_1 + \\ + (1+i)\bar{x}_2x_3 + (1-i)\bar{x}_3x_2$;

b) $2|x_1|^2 + |x_2|^2 + 3|x_3|^2 + (1-2i)\bar{x}_1x_3 + \\ + (1+2i)\bar{x}_3x_1$;

c) $-|x_1|^2 - |x_2|^2 - 2|x_3|^2 - 3|x_4|^2 - i\bar{x}_1x_4 + \\ + i\bar{x}_4x_1 - i\bar{x}_2x_3 + i\bar{x}_3x_2$;

d) $-|x_1|^2 - |x_2|^2 - |x_3|^2 - |x_4|^2 - \\ - (1+i)\bar{x}_2x_4 - (1-i)\bar{x}_4x_2$?

19. Arvutada

$$(1 - i + 2j - k)(i + k)^{-1} - (i + k)^{-1}(1 - i + 2j - k).$$

20. Lahendada võrrandid

a) $\xi(2+i-j-2k)=1-i+2j-k$;
b) $(b_1i+b_2j+b_3k)\xi=a_1i+a_2j+a_3k$;
c) $\xi^2+1=0$.

21. Missugused alljärgnevaist korrutamistabeleist määravad algebra:

a)

	e_1	e_2
e_1	e_1	e_2
e_2	e_2	0

b)

	e_1	e_2	e_3
e_1	e_1	e_2	e_3
e_2	e_2	e_1	e_3
e_3	e_3	$-e_3$	0

c)

	e_1	e_2
e_1	0	e_2
e_2	$-e_2$	e_1

22. Võttes kompleksarvude algebras uuteks baasielementideks suurused $b_1=1+i$, $b_2=1-i$, leida vastav korrutamistabel.

23. Leida kvaternioonide algebraga ja ülesandes 21 antud algebratega isomorfsed maatriksite algebrad.

II. Polünoomid üle korpuse.

§ 4. Polünoomide jaguvuse teooria.

1. Eukleidese algoritm. Olgu antud mingi ühikuga põhipiirkond P — ring, korpus või integriteetkond [1]. Vaatleme polünoome üle P, s. o. kõiki polünoome, mille kordajad kuuluvad piirkonda P. Opereerimine niisuguste polünoomidega

$$f(x) = \sum a_k x^k, \quad g(x) = \sum b_k x^k$$

toimub järgmiste eeskirjade kohaselt (I, § 10, art. 1):

$$f(x) = g(x), \text{ kui } a_k = b_k$$
$$f(x) + g(x) = \sum (a_k + b_k) x^k$$
$$f(x) \cdot g(x) = \sum c_k x^k, \quad c_k = \sum_{i+j=k} a_i b_j .$$

Nende arvutusoperatsioonide suhtes moodustavad vaadeldavad polünoomid ühikuga ringi — polünoomkonna $P[x]$. Erijuhul, kui põhipiirkonnaks on mingi integriteetkond I, saab näidata, et ka vastav polünoomkond $I[x]$ kujutab integriteetkonda, s. o. et polünoomkonnas $I[x]$ puuduvad nullitegurid.

Tõepoolest, kui $f(x) \neq 0$ ja $g(x) \neq 0$, siis omavad $f(x)$ ja $g(x)$ kindlaid astmeid n ja m, mistõttu võime kirjutada:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n, \quad a_0 \neq 0$$
$$g(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_{m-1} x + b_m, \quad b_0 \neq 0 .$$

Siin on polünoomide liikmed korraldatud nende astmete kahanevas järjekorras, alates kõige kõrgema astmega liikmest — polünoomi pealiikmest, kusjuures kordajate indeksid

[1] Põhipiirkonnana vaatleme käesolevas õpikus alati kommutatiivset piirkonda.

TARTU ÜLIKOOLI
RAAMATUKOGU

on märgitud endiselt kasvavas järjekorras. Korrutamise eeskirja kohaselt leiame

$$f(x)g(x) = a_0b_0x^{n+m} + (a_0b_1 + a_1b_0)x^{n+m-1} + \ldots + a_nb_m,$$

millest nähtub, et $f(x)g(x) \neq 0$, sest $a_0b_0 \neq 0$. Tähendab, polünoomkonnas $I[x]$ puuduvad nullitegurid.

Viimasest võrdusest ilmneb ühtlasi, et *polünoomkonnas $I[x]$ võrdub polünoomide korrutise pealiige tegurite pealiikmete korrutisega ja polünoomide korrutise aste tegurite astmete summaga.*

Kõik, mis on öeldud polünoomkonna $I[x]$ kohta, kehtib ka polünoomkonna $K[x]$ suhtes, kus põhipiirkonnaks on korpus K. Ei tule aga arvata, et polünoomkond $K[x]$ kujutab korpust, sest näiteks võrrandit

$$g(x)X = f(x),$$

kus $f(x)$ aste n on väiksem kui $g(x)$ aste m, ei saa rahuldada ühegi polünoomiga X. Nimelt kui seda võrrandit rahuldaks mingi polünoom X, mille aste on l, siis peaks eelnenu järgi olema

$$m + l = n$$

ja seega $n \geqslant m$, vastupidi eeldusele.

Küll võime saada vaadeldavale võrrandile iga $g(x) \neq 0$ puhul lahendi, kui laiendame integriteetkonda $K[x]$ vastavaks jagatistekorpuseks (I, § 9, art. 3), mis kannab antud juhul ratsionaalfunktsioonide korpuse nime ja märgitakse sümboliga $K(x)$. Ratsionaalfunktsioonide korpuse elementideks on murrud $\frac{f(x)}{g(x)}$ — ratsionaalfunktsioonid. Vastavalt sellele nimetatakse polünoome eriti ka täisratsionaalseteks funktsioonideks.

Käesoleva peatüki ülesandeks on uurida polünoomkonna $K[x]$ omadusi, kuna polünoomkond $I[x]$ tuleb vaatluse alla järgnevas peatükis. Polünoomkonnas $K[x]$ asendab jagamise operatsiooni jäägiga jagamise algoritm, mis toetub järgmisele lausele:

Teoreem 1. *Polünoomkonna $K[x]$ iga kahe polünoomi $f(x)$ ja $g(x) \neq 0$ vahel on kehtiv seos*

$$f(x) = q(x)g(x) + r(x),$$

kus $r(x)$ on $g(x)$ suhtes madalama astme polünoom[1] *ja $q(x)$ mingi kindel polünoom.*

Olgu tõestuseks

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$
$$g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m,$$

kusjuures $g(x) \neq 0$ tõttu võib eeldada, et $b_0 \neq 0$. Üldsust kitsendamata võime siin piirduda juhuga $n \geqslant m$, sest juhul $n < m$ on teoreem 1 ilmselt õige, nimelt on siis $f(x) = 0 \cdot g(x) + f(x)$, nii et $r(x) = f(x)$, $q(x) = 0$. Eesmärgiga alandada $f(x)$ astet moodustame vahe

$$f_1(x) = f(x) - \frac{a_0}{b_0} x^{n-m} g(x).$$

Et siin polünoomi $\frac{a_0}{b_0} x^{n-m} g(x)$ pealiige langeb ühte $f(x)$ pealiikmega a_0x^n, siis on $f_1(x)$ aste väiksem kui $f(x)$ aste. Olgu $f_1(x)$ aste n_1 ja pealiikme kordaja c_1. Moodustame vahe

$$f_2(x) = f_1(x) - \frac{c_1}{b_0} x^{n_1-m} g(x).$$

Nagu ennegi veendume, et $f_2(x)$ aste on väiksem kui $f_1(x)$ aste. Olgu $f_2(x)$ aste n_2 ja pealiikme kordaja c_2. Moodustame vahe

$$f_3(x) = f_2(x) - \frac{c_2}{b_0} x^{n_2-m} g(x)$$

jne., jätkates seda protsessi niikaua, kuni jõuame polünoomini

$$f_k(x) = f_{k-1}(x) - \frac{c_{k-1}}{b_0} x^{n_{k-1}-m} g(x),$$

mille aste $n_k < m$. Liites saadud k võrdust, leiame

$$f_k(x) = f(x) - \left(\frac{a_0}{b_0} x^{n-m} + \frac{c_1}{b_0} x^{n_1-m} + \frac{c_2}{b_0} x^{n_2-m} + \ldots + \frac{c_{k-1}}{b_0} x^{n_{k-1}-m} \right) g(x)$$

---

[1] Siin $r(x)$ võib olla ka nullpolünoom.

ehk

$$f(x) = \left(\frac{a_0}{b_0} x^{n-m} + \frac{c_1}{b_0} x^{n_1-m} + \frac{c_2}{b_0} x^{n_2-m} + \ldots + \right.$$
$$\left. + \frac{c_{k-1}}{b_0} x^{n_{k-1}-m}\right) g(x) + f_k(x),$$

millest nähtub, et polünoomid

$$r(x) = f_k(x), \quad q(x) = \frac{a_0}{b_0} x^{n-m} + \frac{c_1}{b_0} x^{n_1-m} + \frac{c_2}{b_0} x^{n_2-m} + \ldots +$$
$$+ \frac{c_{k-1}}{b_0} x^{n_{k-1}-m}$$

rahuldavadki teoreemi 1 nõudeid.

Näitame veel, et polünoomid $q(x)$ ja $r(x)$ on polünoomidega $f(x)$ ja $g(x)$ üheselt määratud. Tõepoolest, kui peale seose

$$f(x) = q(x)g(x) + r(x)$$

kehtiks veel seos

$$f(x) = q_1(x)g(x) + r_1(x),$$

kus $r_1(x)$ on $g(x)$ suhtes madalama astmè polünoom, siis peab olema

$$q(x)g(x) + r(x) = q_1(x)g(x) + r_1(x)$$

ehk

$$r(x) - r_1(x) = [q_1(x) - q(x)]g(x).$$

Kui siin $q_1(x) - q(x) \neq 0$, siis esineb viimases võrduses paremal pool võrdusmärki $g(x)$ suhtes kõrgema või vähemalt sama astme polünoom, vasakul pool võrdusmärki aga madalama astme polünoom, mistõttu võrdus ei saa aset leida. Järelikult peab olema $q_1(x) - q(x) = 0$, nii et $q_1(x) = q(x)$ ja seega $r_1(x) = r(x)$.

Üle minnes ratsionaalfunktsioonide korpusse, saame võrduse $f(x) = q(x)g(x) + r(x)$ mõlemaid pooli $g(x)$-ga jagades

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)},$$

millest nähtub, et $q(x)$ on jagatise $\frac{f(x)}{g(x)}$ täisosa ja $r(x)$ jääk. Teoreemi 1 tõestuskäik annab ühtlasi eeskirja polünoomide jäägiga jagamiseks. Näiteks juhul

$$f(x) = 4x^4 - 2x^3 + 3x^2 + 6x + 5, \quad g(x) = 2x^2 - 2x + 1$$

leiame, jättes lihtsuse mõttes polünoomides x-i astmed kirjutamata:

$$\begin{array}{rrrrr|rrr} 4 & -2 & 3 & 6 & 5 & 2 & -2 & 1 \\ \hline 4 & -4 & 2 & & & 2 & 1 & \frac{3}{2} \\ \hline & 2 & 1 & 6 & & & & \\ & 2 & -2 & 1 & & & & \\ \hline & & 3 & 5 & 5 & & & \\ & & 3 & -3 & \frac{3}{2} & & & \\ \hline & & & 8 & \frac{7}{2} & & & \end{array},$$

nii et $4x^4 - 2x^3 + 3x^2 + 6x + 5 = \left(2x^2 + x + \frac{3}{2}\right)(2x^2 - 2x + 1) + 8x + \frac{7}{2}$.

Toetudes jäägiga jagamise algoritmile, saab polünoomkonnas $K[x]$ arendada jaguvuse teooriat, mis on täiesti analoogiline täisarvude jaguvuse teooriaga (I, § 7, art. 1—3). Et siinjuures ka vastavate tõestuskäikude vahel valitseb täielik analoogia, siis piirdume järgnevas peamiselt resultaatide esitamisega.

Erijuhul, kui jääk $r(x) = 0$, s. o. kui polünoomide $f(x)$ ja $g(x)$ vahel kehtib seos $f(x) = q(x)g(x)$, siis $f(x)$ jagub $g(x)$-ga ehk, nagu öeldakse, $g(x)$ on $f(x)$ tegur ehk jagaja.

Olgu $\lambda \neq 0$ mingi konstant, s. o. põhikorpuse K element. Siis võime iga polünoomi $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ puhul kirjutada

$$f(x) = \lambda\left(\frac{a_0}{\lambda}x^n + \frac{a_1}{\lambda}x^{n-1} + \ldots + \frac{a_{n-1}}{\lambda}x + \frac{a_n}{\lambda}\right),$$

millest nähtub, et polünoomkonnas $K[x]$ jagub iga polünoom konstantse teguriga $\lambda \neq 0$ ehk, nagu öeldakse, polünoomkonnas $K[x]$ kujutab iga konstant $\lambda \neq 0$ triviaalset tegurit.

Kahe polünoomi puhul nimetatakse iga polünoomi, millega jaguvad mõlemad antud polünoomid, nende polünoomide ühisteguriks. Niisugune ühistegur, mis jagub iga teise ühisteguriga, kannab suurima ühisteguri nime. On ilmne, et kui $d(x)$ on polünoomide $f(x)$ ja $g(x)$ suurim ühistegur, siis on seda ka iga polünoom $\lambda d(x)$, kus λ tähendab mistahes nullist erinevat konstanti. Harilikult valitakse kõigi polünoomide $\lambda d(x)$ hulgast välja niisugune polünoom, mille pealiikme kordaja on 1. Selleks tuleb vaid võtta λ võrdseks $d(x)$ pealiikme kordaja pöördväärtusega. Polünoomi, mille pealiikme kordaja on 1, nimetatakse normeeritud polünoomiks. Polünoomide $f(x)$ ja $g(x)$ normeeritud suurimat ühistegurit märgitakse sümboliga (f, g). Kui $(f, g) = 1$, siis nimetatakse polünoome $f(x)$ ja $g(x)$ ühistegurita polünoomideks.

Polünoomide $f(x)$ ja $g(x)$ suurim ühistegur leitakse, nagu täisarvude a ja b suurim ühistegurgi, Eukleidese algoritmi abil järkjärgulise jagamise teel. Jagades kõigepealt $f(x)$ $g(x)$-ga, leiame jäägi $r_1(x)$; siis jagades $g(x)$ $r_1(x)$-ga, leiame jäägi $r_2(x)$; edasi jagades $r_1(x)$ $r_2(x)$-ga, leiame jäägi $r_3(x)$ jne. Et sel viisil jagamist toimetades jääkide astmed järjest kahanevad, siis peab kord tulema moment, kus jääk osutub nulliks. Nagu võib kergesti veenduda, kujutab siis viimane nullist erinev jääk $r_k(x)$ polünoomide $f(x)$ ja $g(x)$ suurimat ühistegurit (I, § 7, art. 1). Ühtlasi on Eukleidese algoritmiga tõestatud ka polünoomide suurima ühisteguri olemasolu.

Näide 1. Leida polünoomide

$$f(x) = x^4 - 3x^3 + 3x + 1, \quad g(x) = x^4 - x^2 - 2x - 1$$

suurim ühistegur.

Rakendades polünoomidele $f(x)$ ja $g(x)$ Eukleidese algoritmi, toimetame jagamist järgmise skeemi kohaselt:

$$
\begin{array}{rrrrr|rrrrr|rrrrr}
 & & & & & 1 & -3 & 0 & 3 & 1 & 1 & 0 & -1 & -2 & -1 \\
\cline{6-15}
 & & & & & 1 & 0 & -1 & -2 & -1 & 1 & & & & \\
\cline{6-15}
 & 3 & 0 & -3 & -6 & -3 & -3 & 1 & 5 & 2 & & & & & \\
\cline{6-15}
 & 3 & -1 & -5 & -2 & & -1 & (-1) & & & & & & & \\
\cline{2-5}
 & & 1 & 2 & -4 & -3 & & & & & & & & & \\
\cline{3-5}
 & & 3 & 6 & -12 & -9 & & & & & & & & & \\
 & & 3 & -1 & -5 & -2 & & & & & & & & & \\
\cline{3-5}
 & & & 7 & -7 & -7 & & & & & & & & & \\
\cline{4-5}
-3 & 1 & 5 & 2 & & & 1 & -1 & -1 & & & & & & \\
\cline{5-5}
-3 & 3 & 3 & & & & -3 & -2 & & & & & & & \\
\cline{1-4}
 & -2 & 2 & 2 & & & & & & & & & & & \\
 & -2 & 2 & 2 & & & & & & & & & & & \\
\cline{1-4}
 & & & 0. & & & & & & & & & & &
\end{array}
$$

Silmas pidades, et polünoomide suurim ühistegur on määratud vaid kuni konstantse tegurini, oleme Eukleidese algoritmi rakendamisel murdude vältimiseks kordajaid 1, 0, —1, —2, —1 ja 1, 2, —4, —3 korrutanud 3-ga ja kordajaid 7, —7, —7 jaganud 7-ga. Otsitav suurim ühistegur on määratud viimase nullist erineva jäägiga, mille kordajateks on 1, —1, —1, s. o.

$$(x^4 - 3x^3 + 3x + 1,\quad x^4 - x^2 - 2x - 1) = x^2 - x - 1\,.$$

2. Võrrandi $f(x)X + g(x)Y = h(x)$ lahenduvus polünoomides. Kasutades Eukleidese algoritmi, saab analoogiliselt täisarvude juhuga (I, § 7, art. 2) tõestada järgmise teoreemi.

Teoreem 2. *Võrrand $f(x)X + g(x)Y = d(x)$, kus $d(x) = (f, g)$, omab polünoomkonnas $K[x]$ alati lahendit X, Y.*

Teoreemi 2 tõestuskäik näitab ühtlasi kätte tee, kuidas tegelikult leida polünoome X ja Y. Kuid me jõuame siin kiiremini sihile, kasutades nõndanimetatud määramata kordajate meetodit.

Kõigepealt paneme tähele, et kui $f(x)$ ja $g(x)$ pole mõlemad konstandid, siis võime alati eeldada, et polünoomi X aste on väiksem kui $g(x)$ aste ja polünoomi Y aste väiksem kui $f(x)$ aste. Tõepoolest, kui viimane eeldus ei ole täidetud, siis jagades polünoomi X $g(x)$-ga, saame

$$X = q(x)g(x) + r(x),$$

kus $r(x)$ on $g(x)$ suhtes madalama astme polünoom. Asetades saadud X avaldise võrdusse

$$f(x)X + g(x)Y = d(x),$$

leiame

$$f(x)X' + g(x)Y' = d(x),$$

kus $X' = r(x)$, $Y' = Y + f(x)q(x)$. Siin $X' = r(x)$ aste on väiksem kui $g(x)$ aste. Samuti on Y' aste väiksem kui $f(x)$ aste, sest vastasel korral võrduks korrutise $g(x)Y'$ aste ja ühtlasi ka $d(x)$ aste vähemalt $f(x)g(x)$ astmega, s. o. $f(x)$ ja $g(x)$ astmete summaga, mis on ilmselt võimatu.

Seega kui n tähendab $f(x)$ astet ja m $g(x)$ astet, siis võime kirjutada

$$X = A_0x^{m-1} + A_1x^{m-2} + \ldots + A_{m-1}$$
$$Y = B_0x^{n-1} + B_1x^{n-2} + \ldots + B_{n-1}.$$

Asetades need X ja Y avaldised võrdusse

$$f(x)X + g(x)Y = d(x),$$

tekib viimase vasakul poolel $(n + m - 1)$-astme polünoom, mille kordajad — mida on arvult $n + m$ tükki — avalduvad lineaarselt A_0, A_1, ..., A_{m-1}, B_0, B_1, ..., B_{n-1} kaudu. Et polünoomide võrdus taandub vastavate kordajate võrdustele, saame $n + m$ suuruse A_0, A_1, ..., A_{m-1}, B_0, B_1, ..., B_{n-1} leidmiseks parajasti $n + m$ võrrandist koosneva lineaarse süsteemi.

Näide 2. Leida võrrandi $(x^4 - x^2 + 1)X + (x^3 - 1)Y = 1$ polünoomiline lahend.

Asetades antud võrrandisse X ja Y asemele vastavalt

$$X = A_0x^2 + A_1x + A_2, \quad Y = B_0x^3 + B_1x^2 + B_2x + B_3,$$

leiame pärast nõutavaid korrutamisi ja liitmisi

$$(A_0 + B_0)x^6 + (A_1 + B_1)x^5 + (A_2 - A_0 + B_2)x^4 + \\ + (B_3 - B_0 - A_1)x^3 + (A_0 - A_2 - B_1)x^2 + (A_1 - B_2)x + \\ + (A_2 - B_3) = 1,$$

kust polünoomide võrduse mõiste järgi

$$A_0 + B_0 = 0, \qquad A_1 + B_1 = 0$$
$$A_2 - A_0 + B_2 = 0, \quad B_3 - B_0 - A_1 = 0, \quad A_0 - A_2 - B_1 = 0$$
$$A_1 - B_2 = 0, \qquad A_2 - B_3 = 1.$$

Siin kahest esimesest ja kahest viimasest võrrandist saame

$$B_0 = -A_0, \quad B_1 = -A_1, \quad B_2 = A_1, \quad B_3 = A_2 - 1.$$

Asetades need B_0, B_1, B_2, B_3 väärtused ülejäänud kolme keskmisse võrrandisse, leiame

$$A_2 - A_0 + A_1 = 0$$
$$A_2 + A_0 - A_1 = 1$$
$$A_2 - A_0 - A_1 = 0,$$

millest

$$A_0 = \frac{1}{2}, \quad A_1 = 0, \quad A_2 = \frac{1}{2}$$

ja seega

$$B_0 = -\frac{1}{2}, \quad B_1 = 0, \quad B_2 = 0, \quad B_3 = -\frac{1}{2}.$$

Tähendab, antud võrrandit rahuldavad polünoomid

$$X = \frac{1}{2}x^2 + \frac{1}{2}, \quad Y = -\frac{1}{2}x^3 - \frac{1}{2}.$$

Üldiselt ei ole raske näha, et *võrrand* $f(x)X + g(x)Y = h(x)$ *on lahenduv polünoomkonnas* $K[x]$ *siis ja ainult siis, kui* $h(x)$ *jagub* $f(x)$ *ja* $g(x)$ *suurima ühisteguriga.*

3. Taandumatud polünoomid. Analoogiliselt täisarvude integriteetkonna juhuga võib tuletada teoreemist 2 järgmise lause:

Teoreem 3. *Kui korrutis $f(x)g(x)$ jagub polünoomiga $m(x)$, kusjuures $f(x)$ ja $m(x)$ on ühistegurita polünoomid, siis peab $g(x)$ jaguma $m(x)$-ga.*

Nagu nägime, kujutab polünoomkonnas $K[x]$ iga konstant $\lambda \neq 0$ triviaalset tegurit selles mõttes, et siin iga polünoom $f(x)$ jagub konstandiga λ (art. 1). Vastavalt sellele nimetame polünoomi $f(x)$ tegureiks lahutusi

$$f(x) = \lambda \cdot \frac{f(x)}{\lambda},$$

kus esineb triviaalne tegur λ, triviaalseteks lahutusteks. Kui mittekonstantne polünoom omab ainult triviaalseid tegureiks lahutusi, siis nimetatakse teda taandumatuks polünoomiks, vastasel korral aga taanduvaks polünoomiks. Nii on näiteks iga esimese astme polünoom $a_0x + a_1$ taandumatu, sest tema mistahes tegureiks lahutuses peab esinema ikka üks konstant, kuna juba kahe esimese astme polünoomi korrutis on teise astme polünoom. Kõrgema astme polünoomide puhul sõltub taanduvus aluseks võetud põhikorpusest K. Nii on näiteks polünoom $x^2 - 2$ taandumatu, kui põhikorpuseks on ratsionaalarvude korpus, sest taanduvuse korral peaks olema

$$x^2 - 2 = (a_0x + a_1)(b_0x + b_1),$$

kus a_0, a_1, b_0, b_1 tähendavad ratsionaalarve. Viimasest võrdusest nähtub eriti, et ratsionaalarv $x = -\frac{a_1}{a_0}$ rahuldab võrrandit $x^2 - 2 = 0$, mis on aga võimatu (I, § 4, art. 1). Kuid sama polünoom $x^2 - 2$ osutub taanduvaks, kui põhikorpuseks võtta reaalarvude korpus, sest siis võime kirjutada

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

Analoogiliselt on polünoom $x^2 + 1$ taandumatu, kui põhikorpuseks on reaalarvude korpus, seevastu aga taanduv, kui põhikorpuseks võtta kompleksarvude korpus, kusjuures

$$x^2 + 1 = (x - i)(x + i).$$

Kui tahame rõhutada põhikorpust K, mille suhtes me taandu-

vust vaatleme, siis kõneleme polünoomi taanduvusest korpuses K ehk üle korpuse K.

Teoreemist 3 järeldub, et kui korrutis $f(x)g(x)$ jagub taandumatu polünoomiga $p(x)$, siis peab vähemalt üks tegureist jaguma $p(x)$-ga. Tõepoolest, kui näiteks $f(x)$ ei jagu $p(x)$-ga, siis on $(f, p) = 1$ ja seega peab teoreemi 3 järgi $g(x)$ jaguma $p(x)$-ga.

Vaatleme nüüd mingit mittekonstantset polünoomi $f(x)$. Kui $f(x)$ ei ole taandumatu korpuses K, siis võib teda lahutada kahe mittetriviaalse teguri korrutiseks, kusjuures mõlemad tegurid on madalama astme polünoomid võrreldes $f(x)$-ga. Viimased tegurid lahutame võimaluse puhul omakorda madalama astme polünoomide korrutiseks jne. Et iga niisuguse tegureiks lahutuse puhul tegurite astmed kahanevad, siis peab kord tulema moment, kus lahutamine mittetriviaalseiks tegureiks pole enam võimalik, ja kus teguritena esinevad seega vaid taandumatud polünoomid $p_1(x)$, $p_2(x)$, ..., $p_k(x)$, s. o.

$$f(x) = p_1(x)p_2(x) \ldots p_k(x).$$

Erijuhul, kui $f(x)$ ise on taandumatu, saame korrutise asemel üheainsa teguri. Nagu täisarvude puhul, nii saab ka siin näidata, et polünoomid $p_1(x)$, $p_2(x)$, ..., $p_k(x)$ on kuni triviaalsete teguriteni üheselt määratud ehk, teiste sõnadega, ka polünoomkonnas $K[x]$ on kehtiv algtegureiks lahutamise lause (I, § 7, art. 3).

Teoreem 4. *Polünoomkonnas $K[x]$ laseb iga mittekonstantne polünoom $f(x)$ ennast lahutada taandumatute polünoomide korrutiseks*

$$f(x) = p_1(x)p_2(x) \ldots p_k(x),$$

kus polünoomid $p_1(x)$, $p_2(x)$, ..., $p_k(x)$ on kuni konstantsete teguriteni üheselt määratud.

Sageli vaadeldakse erikujulist tegureiks lahutust

$$(1) \qquad f(x) = a_0 p_1(x)p_2(x) \ldots p_k(x),$$

kus $p_1(x)$, $p_2(x)$, ..., $p_k(x)$ on normeeritud taandumatud polünoomid ja a_0 polünoomi $f(x)$ pealiikme kordaja. Et siin konstant a_0 peab kujutama just $f(x)$ pealiikme kordajat, ilmneb otse-

kohe, kui peame silmas, et polünoomide korrutise pealiige võrdub tegurite pealiikmete korrutisega (art. 1). On arusaadav, et korrutises (1) on tegurid üheselt määratud.

Taandumatud tegurid, mis esinevad korrutises (1), ei tarvitse olla kõik üksteisest erinevad. Olgu siin r erinevat tegurit $p_1(x)$, $p_2(x)$, ..., $p_r(x)$, $(r \leqslant k)$, kusjuures $p_1(x)$ esinegu korrutises (1) tegurina α_1 korda, $p_2(x)$ α_2 korda jne., lõppeks $p_r(x)$ α_r korda, nii et $\alpha_1 + \alpha_2 + \ldots + \alpha_r = k$. Võttes niisugused kordsed tegurid kokku astmeiks, võime valemi (1) esitada kujul

$$f(x) = a_0 p_1^{\alpha_1}(x) p_2^{\alpha_2}(x) \ldots p_r^{\alpha_r}(x).$$

Nii on näiteks ratsionaalarvude korpuses

$$x^7 + x^6 - x^5 - x^4 - x^3 - x^2 + x + 1 = (x-1)^2(x+1)^3(x^2+1).$$

§ 5. Polünoomi lahendid.

1. Polünoomi jagumine lineaarteguriga. Vaatleme polünoomkonnas $K[x]$ mingit polünoomi $f(x)$. Jagades seda polünoomi nullist erineva polünoomiga $g(x)$, saame

$$f(x) = q(x)g(x) + r(x),$$

kus $r(x)$ on $g(x)$ suhtes madalama astme polünoom (§ 4, art. 1). Erijuhul, kui $g(x)$ on lineaarpolünoom, mida käsitleme normeerituna kujul $g(x) = x - \xi$, kus ξ tähendab teatavat konstanti, osutub $r(x)$ ülimalt null-astme polünoomiks, s. o. konstandiks r, ja me võime kirjutada

$$f(x) = q(x)(x - \xi) + r.$$

Võttes siin $x = \xi$, leiame

$$r = f(\xi),$$

millega oleme saanud tuntud Bézout' teoreemi.

Teoreem 5. *Jääk, mis tekib polünoomi $f(x)$ jagamisel lineaarteguriga $x - \xi$, on võrdne $f(x)$ väärtusega kohal ξ.*

Juhul $r = 0$ järeldub Bézout' teoreemist, et *polünoom $f(x)$ jagub lineaarteguriga $x - \xi$ siis ja ainult siis, kui ξ kujutab*

$f(x)$ *lahendit.* Teiste sõnadega: polünoomi $f(x)$ lineaartegurite leidmine on samaväärne algebralise võrrandi

$$f(x) = 0$$

lahendite leidmisega.

Et lineaartegur $x - \xi$ kujutab alati taandumatut polünoomi, siis peab polünoomi $f(x)$ iga lineaartegur esinema ühe tegurina $f(x)$ lahutuses taandumatute tegurite korrutiseks. Kui nüüd $f(x)$ aste on n, siis saab $f(x)$ sisaldada ülimalt n lineaartegurit. Tähendab, *n-astme polünoomil võib olla korpuses ülimalt n lahendit.*

M ä r k u s. Viimane väide ei ole enam kehtiv ringis, sest näiteks jäägiklassiringis $R^{(8)}$ omab polünoom $x^2 - 1$ neli lahendit 1, 3, 5 ja 7. Samuti ei kehti see väide mittekommutatiivses korpuses, sest näiteks kvaternioonide korpuses omab polünoom $x^2 + 1$ lõpmata palju lahendeid $bi + cj + dk$, kus $b^2 + c^2 + d^2 = 1$.

Polünoomi $f(x)$ jagamiseks lineaarteguriga $x - \xi$ ja ühtlasi $f(x)$ väärtuse leidmiseks kohal ξ on olemas lihtne praktiline võte, mis on antud H o r n e r'i poolt 1819. aastal. Nimelt kui $f(x)$ aste on n, s. o.

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \quad a_0 \neq 0,$$

siis $f(x)$ jagamisel lineaarteguriga $x - \xi$ saadud täisosa $q(x)$ aste on $n - 1$, mistõttu võime kirjutada

$$q(x) = q_0x^{n-1} + q_1x^{n-2} + \ldots + q_{n-2}x + q_{n-1}.$$

Asetades need $f(x)$ ja $q(x)$ avaldised võrdusse $f(x) = q(x)(x - \xi) + r$, leiame pärast korrutamist ja liitmist

$$\begin{aligned} a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n = \\ = q_0x^n + (q_1 - \xi q_0)x^{n-1} + (q_2 - \xi q_1)x^{n-2} + \ldots + \\ + (q_{n-1} - \xi q_{n-2})x + (r - \xi q_{n-1}), \end{aligned}$$

millest

$$\begin{gathered} q_0 = a_0, \quad q_1 - \xi q_0 = a_1, \quad q_2 - \xi q_1 = a_2, \ \ldots, \\ q_{n-1} - \xi q_{n-2} = a_{n-1}, \quad r - \xi q_{n-1} = a_n \end{gathered}$$

ja seega

$$q_0 = a_0, \quad q_1 = a_1 + \xi q_0, \quad q_2 = a_2 + \xi q_1, \ \ldots,$$
$$q_{n-1} = a_{n-1} + \xi q_{n-2}, \quad r = a_n + \xi q_{n-1}.$$

Niisiis võime polünoomi $f(x)$ jagamisel lineaarteguriga $x - \xi$ tekkinud täisosa $q(x)$ kordajad q_k ja jäägi r üksteise järgi arvutada, korrutades q_k-le eelneva kordaja q_{k-1} ξ-ga ja liites tulemuse a_k-ga. Vastavad arvutused korraldame Horneri skeemi kohaselt järgmiselt:

$$\begin{array}{c|cccccc} & a_0 & a_1 & a_2 & \ldots & a_{n-1} & a_n \\ & & \xi q_0 & \xi q_1 & \ldots & \xi q_{n-2} & \xi q_{n-1} \\ \hline \xi & q_0 & q_1 & q_2 & \ldots & q_{n-1} & r = f(\xi). \end{array}$$

Näide 3. Jagada polünoom $f(x) = x^5 - 2x^3 - 4x^2 - 5x + 3$ lineaarteguriga $x - 2$.

Antud juhul on $a_0 = 1$, $a_1 = 0$, $a_2 = -2$, $a_3 = -4$, $a_4 = -5$, $a_5 = 3$ ja $\xi = 2$, mistõttu Horneri skeemi rakendamine annab

$$\begin{array}{c|cccccc} & 1 & 0 & -2 & -4 & -5 & 3 \\ & & 2 & 4 & 4 & 0 & -10 \\ \hline 2 & 1 & 2 & 2 & 0 & -5 & -7. \end{array}$$

Tulemusest nähtub, et $q(x) = x^4 + 2x^3 + 2x^2 - 5$, $r = -7 = f(2)$.

Vastavalt jagamise seadusele omab lineaarpolünoom $a_0 x + a_1$, kus $a_0 \neq 0$, korpuses K alati lahendit $-\frac{a_1}{a_0}$. Seevastu kõrgema astme polünoom ei tarvitse omada lahendeid põhikorpuses K, kuhu kuuluvad selle polünoomi kordajad. Nii näiteks korpuses K taandumatud polünoomid ei oma lahendeid selles korpuses, sest lahendi ξ olemasolu tooks endaga kaasa lineaarteguri $x - \xi$ olemasolu, s. o. taanduvuse. Kui nüüd mingil polünoomil $f(x)$ ei ole lahendit põhikorpuses K, siis tekib küsimus, kas ei saaks korpust K nõnda laiendada, et laiendatud korpuses $f(x)$ omaks lahendit. Et leida vastust sellele küsimu-

sele, moodustame analoogiliselt jäägiklassiringidele $R^{(m)}$ jäägiklassiringid polünoomide järgi.

2. Jäägiklassiringid polünoomide järgi. Vaatleme polünoomkonnas $K[x]$ mingit kindlat mittekonstantset polünoomi

$$m(x) = c_0 + c_1x + c_2x^2 + \ldots + c_kx^k, \quad c_k \neq 0.$$

Jaotame polünoomid polünoomkonnas $K[x]$ klassidesse, võttes kokku üheks klassiks kõik need polünoomid, mis annavad jagamisel $m(x)$-ga ühe ja sama jäägi $r(x)$. Sel teel moodustatud polünoomide klasse nimetatakse jäägiklassideks polünoomi $m(x)$ järgi. Niisuguseid jäägiklasse saame niipalju, kuipalju on erinevaid jääke $r(x)$, s. o. niipalju, kuipalju on polünoomkonnas $K[x]$ polünoome, mille aste ei ületa arvu $k-1$. Seega kui põhikorpus K sisaldab lõpmatu hulga elemente, siis on vaadeldavate jäägiklasside hulk ka lõpmatu.

Kui polünoomid $f(x)$ ja $g(x)$ kuuluvad samasse jäägiklassi, siis on

$$f(x) = q_1(x)m(x) + r(x)$$
$$g(x) = q_2(x)m(x) + r(x),$$

kust lahutades leiame

$$f(x) - g(x) = [q_1(x) - q_2(x)]m(x)$$

ehk

$$f(x) - g(x) = q(x)m(x),$$

kus $q(x) = q_1(x) - q_2(x)$ on mingi polünoom. Kaht polünoomi $f(x)$ ja $g(x)$, mis kuuluvad $m(x)$ suhtes samasse jäägiklassi, nimetame kongruentseteks $m(x)$ järgi ja kirjutame

$$f(x) \equiv g(x) \quad (m(x))$$

või, kui $m(x)$ on ette teada, siis lihtsalt

$$f(x) \equiv g(x).$$

Seega rahuldavad $m(x)$ järgi kongruentsed polünoomid $f(x)$ ja $g(x)$ tingimust

$$f(x) - g(x) = q(x)m(x)$$

ehk

$$f(x) = g(x) + q(x)m(x).$$

Toetudes analoogiale täisarvude vallas (I, § 8, art. 1), võib kergesti veenduda, et kongruents $f(x) \equiv g(x)$ on refleksiivne, sümmeetriline ja transitiivne, rahuldades seega võrduse postulaate. Selle alusel defineerime nüüd polünoomkonnas $K[x]$ uue võrduse, lugedes polünoomi $m(x)$ järgi kongruentsed polünoomid võrdseteks, jättes seejuures tehete definitsioonid endisteks. Analoogiliselt täisarvude juhuga (I, § 8, art. 2) saab näidata, et polünoomkond $K[x]$ kujutab uue võrduse seisukohalt ringi. Seda ringi nimetatakse jäägiklassiringiks $m(x)$ järgi ja märgitakse sümboliga $R^{(m(x))}$. Arvutamisel jäägiklassiringis $R^{(m(x))}$ võib piirduda ülimalt $(k-1)$-astme polünoomidega

$$r(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1},$$

mis esinevad jääkidena polünoomi $f(x)$ jagamisel $m(x)$-ga [1] ja mis kannavad $R^{(m(x))}$ taandatud elementide nime. Nii on näiteks jäägiklassiringis $R^{(2+x^3)}$, kui kasutada ka uue võrduse, s. o. kongruentsi kirjutamisel harilikku võrdusmärki:

$$(1 + x^2) + (1 - x - x^2) = 2 - x$$
$$(1 + x^2) \cdot (1 - x - x^2) = 3 + x$$
$$(1 + x^2) - (1 - x - x^2) = x + 2x^2.$$

Taandatud elemendid $r(x)$, käitudes liitmise ja skalaariga korrutamise suhtes nagu k-dimensionaalsed vektorid

$$a_0\boldsymbol{e}_1 + a_1\boldsymbol{e}_2 + a_2\boldsymbol{e}_3 + \ldots + a_{k-1}\boldsymbol{e}_k,$$

moodustavad k-dimensionaalse vektoriruumi K_k üle K. Taandatud elementide korrutis määrab selles vektoriruumis vektorite omavahelise korrutise, mis on ilmselt kommutatiivne ja skalaariga korrutamise suhtes assotsiatiivne. Teiste sõnadega, $R^{(m(x))}$ taandatud elemendid moodustavad k-järku kommutatiivse

[1] Nimelt kui $f(x)$ jagamisel $m(x)$-ga saame $f(x) = q(x)m(x) + r(x)$, siis $f(x) \equiv r(x)$.

algebra K_k üle K (§ 3, art. 2). Algebras K_k avalduvad baasielemendid

$$e_1 = 1\,, \quad e_2 = x\,, \quad e_3 = x^2,\ \ldots,\ e_k = x^{k-1}$$

kõik ühe baasielemendi $e_2 = x$ astmetena. Mis puutub elementide

$$a_0e_1 + a_1e_2 + \ldots + a_{k-1}e_k \text{ ja } b_0e_1 + b_1e_2 + \ldots + b_{k-1}e_k$$

korrutisse, siis avaldub see kujul

$$d_0e_1 + d_1e_2 + \ldots + d_{k-1}e_k\,,$$

kus d_0, d_1, $\ldots$, d_{k-1} tähendavad polünoomide korrutise

$$(a_0 + a_1x + \ldots + a_{k-1}x^{k-1})\,(b_0 + b_1x + \ldots + b_{k-1}x^{k-1})$$

jagamisel $m(x)$-ga tekkinud jäägi kordajaid. Jagades näiteks astme e_2^k leidmiseks x^k polünoomiga $m(x) = c_0 + c_1x + c_2x^2 + \ldots + c_kx^k$, saame jäägi

$$r(x) = -\frac{c_0}{c_k} - \frac{c_1}{c_k}\,x - \frac{c_2}{c_k}\,x^2 - \ldots - \frac{c_{k-1}}{c_k}\,x^{k-1}\,.$$

Seega $e_2^k = -\frac{c_0}{c_k}\,e_1 - \frac{c_1}{c_k}\,e_2 - \frac{c_2}{c_k}\,e_3 - \ldots - \frac{c_{k-1}}{c_k}\,e_k = -\frac{c_0}{c_k} - \frac{c_1}{c_k}\,e_2 - \frac{c_2}{c_k}\,e_2^2 - \ldots - \frac{c_{k-1}}{c_k}\,e_2^{k-1}$, millest

$$c_0 + c_1e_2 + c_2e_2^2 + \ldots + c_ke_2^k = 0$$

ehk

$$m(e_2) = 0\,,$$

s. o. algebra K_k baasielement $e_2 = (0\,,\ 1\,,\ 0\,,\ \ldots,\ 0)$ rahuldab võrrandit

$$m(x) = 0\,.$$

Et K_k kui ühikuga algebra kujutab põhikorpuse K laiendit (§ 3, art. 2), siis ongi meil K_k näol tegemist laiendiga, kus etteantud polünoom $m(x)$ omab lahendit. Kuid siin K_k ei tarvitse tingimata kujutada jagamisega algebrat, s. o. korpust. Seepärast selgitame veel, missugusel tingimusel K_k ehk, mis sama on, $R^{(m(x))}$ osutub korpuseks.

Selleks küsime kõigepealt, missugused $R^{(m(x))}$ elemendid omavad pöördelemente, s. o. missuguse $f(x)$ puhul on võrrand

$$f(x)X = 1$$

lahenduv jäägiklassiringis $R^{(m(x))}$. See võrrand on samaväärne võrrandiga

$$f(x)X \equiv 1$$

polünoomkonnas $K[x]$, s. o. võrrandiga

$$f(x)X = 1 + qm(x)$$

ehk

$$f(x)X - m(x)q = 1,$$

kus q tähendab mingit polünoomi. Seega seisneb küsimus selles, missuguse $f(x)$ puhul omab viimane võrrand polünoomilist lahendit X, q. Niisugune võrrand omab teatavasti polünoomilist lahendit siis ja ainult siis, kui $(f, m) = 1$ (§ 4, art. 2). Tähendab, jäägiklassiringis $R^{(m(x))}$ omavad pöördelemente need ja ainult need elemendid, mis kui polünoomid on ühistegurita $m(x)$ suhtes.

Erijuhul, kui $m(x)$ tähendab mingit korpuses K taandumatut polünoomi $p(x)$, on kõik nullist erinevad polünoomid

$$a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$$

ühistegurita $p(x)$ suhtes, mistõttu jäägiklassiringis $R^{(p(x))}$ on igal nullist erineval elemendil pöördelement ehk, teiste sõnadega, jäägiklassiring $R^{(p(x))}$ kujutab korpust — j ä ä g i k l a s s i k o r p u s t $p(x)$ j ä r g i (I, § 8, art. 3). Seevastu jäägiklassiring $R^{(m(x))}$, kus $m(x)$ on taanduv korpuses K, ei kujuta kunagi korpust, sest kui

$$m(x) = m_1(x)m_2(x),$$

siis on jäägiklassiringis $R^{(m(x))}$ kehtiva võrduse $m(x) = 0$ tõttu

$$m_1(x)m_2(x) = 0,$$

kusjuures $m_1(x) \neq 0$, $m_2(x) \neq 0$. Tähendab, $m_1(x)$ ja $m_2(x)$ kujutavad nullitegureid. *Seega taandub jäägiklassiring $R^{(m(x))}$ korpuseks siis ja ainult siis, kui $m(x)$ on taandumatu korpuses K.*

3. Polünoomi lahendite olemasolu. Olgu $f(x)$ mingi mittekonstantne polünoom üle korpuse K. Näitame, et põhikorpust K saab alati nii laiendada uueks korpuseks, et $f(x)$ omab selles laiendis ehk, nagu öeldakse, ülemkorpuses vähemalt ühte lahendit. Tõepoolest olgu $p(x)$ mingi taandumatu tegur polünoomis $f(x)$. Moodustame vastava jäägiklassikorpuse $R^{(p(x))}$ ehk, teiste sõnadega, algebra K_k, kus k tähendab polünoomi $p(x)$ astet. Nagu teame eelnevast artiklist, kujutab K_k baasielement $e_2 = (0, 1, 0, \ldots, 0)$ võrrandi $p(x) = 0$ lahendit, s. o. $p(e_2) = 0$. Siis on aga ka

$$f(e_2) = 0.$$

Seega oleme jõudnud polünoomi lahendi olemasolu lause juurde, mis on avaldatud esmakordselt Steinitz'i poolt 1910. aastal ja mida võib õigustatult nimetada polünoomide algebra põhilauseks.

Teoreem 6. *Polünoomkonnas $K[x]$ omab iga mittekonstantne polünoom $f(x)$ vähemalt ühte lahendit kas põhikorpuses K või vastavalt polünoomile $f(x)$ konstrueeritud ülemkorpuses K_k.*

Vaatleme näitena polünoomi $x^2 + 1$, mis on taandumatu reaalarvude korpuses K. Siin $k = 2$, nii et algebra K_2 koosneb suurustest

$$a_0 + a_1 e_2,$$

kus e_2 kujutabki $x^2 + 1$ lahendit, s. o. $e_2^2 = -1$. Ei ole raske näha, et opereerimine suurustega $a_0 + a_1 e_2$ ja $b_0 + b_1 e_2$ toimub algebras K_2 järgmiste eeskirjade kohaselt:

$$a_0 + a_1 e_2 = b_0 + b_1 e_2, \quad \text{kui} \quad a_0 = b_0, \quad a_1 = b_1$$
$$(a_0 + a_1 e_2) + (b_0 + b_1 e_2) = (a_0 + b_0) + (a_1 + b_1) e_2$$
$$(a_0 + a_1 e_2) \cdot (b_0 + b_1 e_2) = (a_0 b_0 - a_1 b_1) + (a_0 b_1 + a_1 b_0) e_2,$$

mis pole muud midagi kui kompleksarvudega $a_0 + a_1 i$ ja $b_0 + b_1 i$ opereerimise eeskirjad (§ 1, art. 1), kus on märgitud $i = e_2$. Tähendab, kompleksarvude korpust võib vaadelda kui jäägiklassikorpust polünoomi $x^2 + 1$ järgi.

Eespool nägime, et n-astme polünoomil võib olla korpuses ülimalt n lahendit (§ 5, art. 1). Toetudes polünoomide algebra põhilausele, ei ole raske näha, et iga n-astme polünoomi $f(x)$ puhul leidub niisugune ülemkorpus L, kus $f(x)$ omab parajasti n lahendit. Tõepoolest, leiame kõigepealt ülemkorpuse $K' = K_{k_1}$, kus $f(x)$ omab lahendit[1] ξ_1. Siis korpuses K' peab $f(x)$ jaguma lineaarteguriga $x - \xi_1$, s. o.

$$f(x) = (x - \xi_1) f_1(x).$$

Edasi leiame ülemkorpuse $K'' = K'_{k_2}$, kus $f_1(x)$ omab lahendit ξ_2. Siis korpuses K'' peab $f_1(x)$ jaguma lineaarteguriga $x - \xi_2$, nii et me saame

$$f(x) = (x - \xi_1)(x - \xi_2) f_2(x).$$

Seda toimingut jätkates jõuame $n - 1$ sammu järel ülemkorpuseni $L = K^{(n-1)}$, kus polünoomil $f(x)$ on n lahendit

$$\xi_1, \xi_2, \ldots, \xi_n,$$

ja kus $f(x)$ omab vastavalt kuju

$$f(x) = a_0(x - \xi_1)(x - \xi_2) \ldots (x - \xi_n), \tag{2}$$

milles a_0 peab olema konstant ja nimelt $f(x)$ pealiikme kordaja. Tähendab, *iga polünoomi puhul leidub niisugune ülemkorpus, kus see polünoom laguneb täielikult lineaartegurite korrutiseks.*

Seega vastab igale polünoomile $f(x)$ oma isiklik ülemkorpus, kus $f(x)$ laguneb lineaartegurite korrutiseks. Tekib küsimus, kas leidub niisugune üldine ülemkorpus, kus polünoomkonna $K[x]$ iga polünoom laguneb lineaartegurite korrutiseks. Steinitz on näidanud[2], et iga korpust K võib laiendada niisuguseks ülemkorpuseks L, kus mitte ainult polünoomkonna $K[x]$, vaid ka polünoomkonna $L[x]$ iga polünoom laguneb lineaartegurite korrutiseks. Niisugust korpust L, kus polünoomkonna $L[x]$ iga polünoom laguneb lineaartegurite korrutiseks, nimetatakse algebraliselt kinniseks korpuseks. Seega

[1] Kui $f(x)$ omab lahendit põhikorpuses K, siis võtame $K' = K$.

[2] Vt. Ван-дер-Варден, Современная алгебра I.

ütleb Steinitzi teoreem, et iga korpust võib laiendada algebraliselt kinniseks korpuseks.

Tuleb silmas pidada, et eespoolleitud lahendid $\xi_1, \xi_2, \ldots, \xi_n$ ei tarvitse olla kõik erinevad. Olgu nende lahendite hulgas r erinevat $\xi_1, \xi_2, \ldots, \xi_r$, $(r \leqslant n)$, mis esinegu lahenditena vastavalt $\alpha_1, \alpha_2, \ldots, \alpha_r$ korda, nii et $\alpha_1 + \alpha_2 + \ldots + \alpha_r = n$. Võttes niisugustele kordsetele lahenditele vastavad lineaartegurid kokku astmeiks, võime kirjutada valemi (2) kujul

$$f(x) = a_0(x - \xi_1)^{\alpha_1}(x - \xi_2)^{\alpha_2} \ldots (x - \xi_r)^{\alpha_r}.$$

Näide 4. Antud on polünoom

$$x^5 + x^3 + 2x^2 + 2,$$

mille kordajad kuuluvad jäägiklassikorpusse $R^{(7)}$. Leida niisugune ülemkorpus, kus see polünoom laguneb lineaartegurite korrutiseks.

Põhikorpuses $K = R^{(7)}$ laguneb antud polünoom korrutiseks

$$x^5 + x^3 + 2x^2 + 2 = (x^2 + 1)(x^3 + 2),$$

kus mõlemad tegurid on taandumatud, sest vastasel korral peaksid nad sisaldama lineaartegureid, mis on aga võimatu, sest neil tegureil pole lahendeid korpuses $R^{(7)}$, nagu selles võib proovimise teel kergesti veenduda.

Konstrueerime ülemkorpuse $K' = K_2$, milles polünoom $x^2 + 1$ omab lahendit. Korpus K' koosneb suurustest

$$a_0 + a_1 i,$$

kus $i^2 = -1$, ja milledega tuleb arvutada nagu harilike kompleksuurustega. Korpuses K' laguneb $x^2 + 1$ lineaartegurite korrutiseks

$$x^2 + 1 = (x - i)(x + i),$$

kuna $x^3 + 2$ on siin taandumatu. Tõepoolest, kui $x^3 + 2$ oleks taanduv korpuses K', siis peaks ta omama vähemalt ühte lahendit $a_0 + a_1 i$, kus a_0 ja $a_1 \neq 0$ kuuluvad põhikorpusse $K = R^{(7)}$, s. o.

$$(a_0 + a_1 i)^3 + 2 = 0$$

ehk

$$a_0^3 - 3a_0a_1^2 + 2 + (3a_0^2a_1 - a_1^3)i = 0,$$

millest $a_1 \neq 0$ tõttu

$$a_0^3 - 3a_0a_1^2 + 2 = 0, \quad 3a_0^2 - a_1^2 = 0.$$

Siin teisest võrdusest saame $a_1^2 = 3a_0^2$. Seega järeldub esimesest võrdusest, et

$$a_0^3 - 9a_0^3 + 2 = 0$$

ehk

$$a_0^3 - 2 = 0,$$

missugune tingimus aga pole rahuldatav põhikorpuses $K = R^{(7)}$, nagu seda näitab vahetu proovimine.

Konstrueerime nüüd ülemkorpuse $K'' = K'_3$, milles polünoom $x^3 + 2$ omaks lahendit. Korpus K'' koosneb suurustest

$$a_0 + a_1j + a_2j^2,$$

milledega arvutamisel tuleb silmas pidada, et $j^3 = -2$. Jagades polünoomi $x^3 + 2$ korpuses K'' lineaarteguriga $x - j$, leiame

$$x^3 + 2 = (x - j)(x^2 + jx + j^2),$$

kus polünoom $x^2 + jx + j^2$, omades korpuses K'' lahendeid

$$x = \frac{-j \pm \sqrt{j^2 - 4j^2}}{2} = \frac{-j \pm \sqrt{4j^2}}{2} = \frac{-j \pm 2j}{2} = \begin{cases} 4j \\ 2j \end{cases},$$

laguneb omakorda lineaartegurite korrutiseks

$$x^2 + jx + j^2 = (x - 2j)(x - 4j).$$

Seega laguneb antud polünoom korpuses K'' täielikult lineaartegurite korrutiseks:

$$x^5 + x^3 + 2x^2 + 2 = (x - i)(x + i)(x - j)(x - 2j)(x - 4j).$$

§ 6. Ratsionaalfunktsioonid ja interpolatsioonivalemid.

1. Ratsionaalfunktsioonide lahutamine osamurdudeks. Käesolevas paragrahvis tutvume polünoomide jaguvuse teooria kahe tähelepandava rakendusega. Laiendades polünoomkonna $K[x]$

kui integriteetkonna vastavaks jagatistekorpuseks — ratsionaalfunktsioonide korpuseks $K(x)$, saime ratsionaalfunktsioonid

$$\frac{f(x)}{g(x)},$$

kus $f(x)$ ja $g(x)$ tähendavad polünoome üle K (§ 4, art. 1). Rakendades polünoomidele $f(x)$ ja $g(x)$ jäägiga jagamise algoritmi, leiame

$$f(x) = q(x)g(x) + r(x),$$

kus $r(x)$ on $g(x)$ suhtes madalama astme polünoom. Seega

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)},$$

millest nähtub, et iga ratsionaalfunktsiooni võib esitada täisratsionaalfunktsiooni ja lihtmurru summana. Siinjuures nimetame l i h t m u r r u k s niisugust ratsionaalfunktsiooni, kus lugeja aste on väiksem kui nimetaja aste.

Toetudes ratsionaalfunktsioonide vallas kehtivaile arvutuseeskirjadele, ei paku raskust näidata, et kahe lihtmurru summa, korrutis ja vahe kujutavad jälle lihtmurde ehk, teiste sõnadega, lihtmurdude hulk on kinnine liitmise, korrutamise ja lahutamise suhtes. Seega moodustavad kõik lihtmurrud ringi.

Olgu antud lihtmurd

$$\frac{f(x)}{g(x)},$$

mille nimetaja laguneb kahe ühistegurita polünoomi korrutiseks, s. o.

$$g(x) = g_1(x)g_2(x),$$

kus $(g_1, g_2) = 1$. Teoreemi 2 põhjal (§ 4, art. 2) leiduvad siis polünoomid X ja Y, mis rahuldavad tingimust

$$g_1(x)X + g_2(x)Y = 1.$$

Korrutades viimast võrdust murruga $\frac{f(x)}{g(x)}$, saame

$$\frac{f(x)}{g(x)} = \frac{f(x)Y}{g_1(x)} + \frac{f(x)X}{g_2(x)}$$

ehk

$$\frac{f(x)}{g(x)} = \frac{f_1(x)}{g_1(x)} + \frac{f_2(x)}{g_2(x)},$$

kus $f_1(x) = f(x)Y$, $f_2(x) = f(x)X$. Eraldades ratsionaalfunktsioonide $\frac{f_1(x)}{g_1(x)}$ ja $\frac{f_2(x)}{g_2(x)}$ täisosad, s. o.

$$\frac{f_1(x)}{g_1(x)} = q_1(x) + \frac{r_1(x)}{g_1(x)}, \quad \frac{f_2(x)}{g_2(x)} = q_2(x) + \frac{r_2(x)}{g_2(x)},$$

leiame

$$\frac{f(x)}{g(x)} = q_1(x) + q_2(x) + \frac{r_1(x)}{g_1(x)} + \frac{r_2(x)}{g_2(x)}, \tag{3}$$

millest

$$q_1(x) + q_2(x) = \frac{f(x)}{g(x)} - \left[\frac{r_1(x)}{g_1(x)} + \frac{r_2(x)}{g_2(x)}\right].$$

Siin esineb võrduse vasakul poolel polünoom, paremal poolel aga lihtmurd. Niisugune võrdus võib aset leida vaid siis, kui võrduse mõlemad pooled taanduvad nullpolünoomideks. Seega peab olema $q_1(x) + q_2(x) = 0$, nii et võrdus (3) omab kuju

$$\frac{f(x)}{g(x)} = \frac{r_1(x)}{g_1(x)} + \frac{r_2(x)}{g_2(x)},$$

kus kõik murrud on lihtmurrud.

Üldiselt, kui $g(x) = g_1(x)g_2(x) \ldots g_n(x)$, kus polünoomid $g_1(x)$, $g_2(x)$, ..., $g_n(x)$ on paarikaupa ühistegurita, siis võib täieliku induktsiooni printsiibile toetudes näidata, et kehtib valem

$$\frac{f(x)}{g(x)} = \frac{r_1(x)}{g_1(x)} + \frac{r_2(x)}{g_2(x)} + \ldots + \frac{r_n(x)}{g_n(x)}, \tag{4}$$

kus kõik murrud on lihtmurrud.

Lahutades polünoomi $g(x)$ taandumatute polünoomide korrutiseks (§ 4, art. 3), saame [1]

$$g(x) = p_1^{\alpha_1}(x)p_2^{\alpha_2}(x) \ldots p_r^{\alpha_r}(x),$$

[1] Siin on eeldatud, et $g(x)$ on normeeritud. Kui $g(x)$ ei peaks olema normeeritud, siis jagame enne murru $\frac{f(x)}{g(x)}$ lugejat ja nimetajat $g(x)$ pealiikme kordajaga.

kus $p_1(x)$, $p_2(x)$, ..., $p_r(x)$ on üksteisest erinevad taandumatud polünoomid. Et polünoomid $p_1^{\alpha_1}(x)$, $p_2^{\alpha_2}(x)$, ..., $p_r^{\alpha_r}(x)$ on paarikaupa ühistegurita, siis leiame valemit (4) rakendades

$$(5) \qquad \frac{f(x)}{g(x)} = \frac{\varphi_1(x)}{p_1^{\alpha_1}(x)} + \frac{\varphi_2(x)}{p_2^{\alpha_2}(x)} + \ldots + \frac{\varphi_r(x)}{p_r^{\alpha_r}(x)}.$$

Siin iga üksik liidetav, kujutades lihtmurdu tüüpi $\frac{\varphi(x)}{p^{\alpha}(x)}$, laseb ennast lahutada omakorda lihtsamate lihtmurdude summaks. Nimelt kui polünoomi $p(x)$ aste on k, siis on $p^{\alpha}(x)$ aste αk ja $\varphi(x)$ aste väiksem kui αk. Jagades $\varphi(x)$ polünoomiga $p^{\alpha-1}(x)$, saame jäägi $r_1(x)$, mille aste on väiksem kui $(\alpha-1)k$. Jagades edasi $r_1(x)$ polünoomiga $p^{\alpha-2}(x)$, leiame jäägi $r_2(x)$, mille aste on väiksem kui $(\alpha-2)k$. Jagades $r_2(x)$ omakorda polünoomiga $p^{\alpha-3}(x)$, leiame jäägi $r_3(x)$, mille aste on väiksem kui $(\alpha-3)k$ jne. Sel teel $\alpha-1$ korda jagamist toimetades saame võrdused

$$\begin{aligned}
\varphi(x) &= q_1(x)p^{\alpha-1}(x) + r_1(x)\\
r_1(x) &= q_2(x)p^{\alpha-2}(x) + r_2(x)\\
r_2(x) &= q_3(x)p^{\alpha-3}(x) + r_3(x)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{\alpha-2}(x) &= q_{\alpha-1}(x)p(x) + r_{\alpha-1}(x),
\end{aligned}$$

kus polünoomide $q_1(x)$, $q_2(x)$, $q_3(x)$, ..., $q_{\alpha-1}(x)$ astmed on väiksemad kui k. Liikudes saadud võrduste ahelikus sammsammult allapoole, asendades igas võrduses esineva jäägi tema avaldisega järgnevast võrdusest ja märkides lõppeks sümmeetria mõttes $r_{\alpha-1}(x) = q_{\alpha}(x)$, saame

$$\varphi(x) = q_1(x)p^{\alpha-1}(x) + q_2(x)p^{\alpha-2}(x) + \ldots + q_{\alpha-1}(x)p(x) + q_{\alpha}(x),$$

millest

$$(6) \qquad \frac{\varphi(x)}{p^{\alpha}(x)} = \frac{q_1(x)}{p(x)} + \frac{q_2(x)}{p^2(x)} + \ldots + \frac{q_{\alpha-1}(x)}{p^{\alpha-1}(x)} + \frac{q_{\alpha}(x)}{p^{\alpha}(x)}.$$

Valemid (5) ja (6) kannavad o s a m u r d u d e k s l a h u t a m i s e v a l e m i t e nime. Neis valemeis on osamurdude nimetajad polünoomiga $g(x)$ üheselt määratud. Näitame, et ka

osamurdude lugejad on kindlad üheselt määratud polünoomid. Et tõestuskäik on valemite (5) ja (6) puhul analoogiline, siis piirdume näiteks valemiga (6). Korrutades valemi (6) mõlemat poolt polünoomiga $p^{\alpha}(x)$, leiame

$$\varphi(x) = [q_1(x)p^{\alpha-2}(x) + q_2(x)p^{\alpha-3}(x) + \ldots + q_{\alpha-1}(x)]\,p(x) + q_{\alpha}(x),$$

kus $q_{\alpha}(x)$ kui $\varphi(x)$ jagamisel $p(x)$-ga tekkinud jääk on üheselt määratud (§ 4, art. 1). Samuti on üheselt määratud jagatise täisosa

$$\varphi_1(x) = [q_1(x)p^{\alpha-3}(x) + q_2(x)p^{\alpha-4}(x) + \ldots + q_{\alpha-2}(x)]\,p(x) + q_{\alpha-1}(x),$$

millest omakorda nähtub, et $q_{\alpha-1}(x)$ kui $\varphi_1(x)$ jagamisel $p(x)$-ga tekkinud jääk on üheselt määratud jne.

Rakendades lihtmurrule $\frac{f(x)}{g(x)}$ valemeid (5) ja (6), saame vastavalt $g(x)$ igale tegurile $p^{\alpha}(x)$ nii mitu osamurdu $\frac{q_i(x)}{p^i(x)}$, kui suur on $p(x)$ kordsus. Erijuhul, kui $g(x)$ laguneb vaadeldavas korpuses täielikult lineaartegurite korrutiseks, s. o. kui

$$g(x) = (x-\xi_1)^{\alpha_1}(x-\xi_2)^{\alpha_2}\ldots(x-\xi_r)^{\alpha_r},$$

on tegureile $(x-\xi)^{\alpha}$ vastavate osamurdude $\frac{q_i(x)}{(x-\xi)^i}$ lugejad konstantsed. Praktiliselt leitakse osamurdude lugejad määramata kordajate meetodiga (§ 4, art. 2).

N ä i d e 5. Lahutada ratsionaalfunktsioon

$$\frac{x^2-x-4}{(x-1)^3(x^2+1)}$$

osamurdudeks ratsionaalarvude korpuses.

Siin tegurile $(x-1)^3$ vastab kolm osamurdu $\frac{A_1}{x-1}$, $\frac{A_2}{(x-1)^2}$, $\frac{A_3}{(x-1)^3}$ ja tegurile x^2+1 üks osamurd $\frac{A_4x+A_5}{x^2+1}$, nii et

$$\frac{x^2-x-4}{(x-1)^3(x^2+1)} = \frac{A_1}{x-1} + \frac{A_2}{(x-1)^2} + \frac{A_3}{(x-1)^3} + \frac{A_4x+A_5}{x^2+1},$$

kus A_1, A_2, A_3, A_4, A_5 on teatavad konstandid. Korrutades viimase võrduse mõlemaid pooli ühise nimetajaga $(x-1)^3(x^2+1)$, leiame

$$(7)\quad x^2-x-4=A_1(x-1)^2(x^2+1)+A_2(x-1)(x^2+1)+ \\ +A_3(x^2+1)+(A_4x+A_5)(x-1)^3,$$

millest pärast sulgude avamist ja liikmete ümberkorraldamist saame

$$x^2-x-4=(A_1+A_4)x^4+(-2A_1+A_2-3A_4+A_5)x^3+ \\ +(2A_1-A_2+A_3+3A_4-3A_5)x^2+(-2A_1+A_2-A_4+ \\ +3A_5)x+(A_1-A_2+A_3-A_5).$$

Seega peab polünoomide võrduse mõiste kohaselt olema

$$(8)\quad \begin{array}{rrrrrrr} A_1 & & +A_4 & & = & 0 \\ -2A_1+A_2 & & -3A_4+ & A_5 & = & 0 \\ 2A_1-A_2+A_3 & +3A_4 & -3A_5 & = & 1 \\ -2A_1+A_2 & & -A_4+3A_5 & = & -1 \\ A_1-A_2+A_3 & & -A_5 & = & -4. \end{array}$$

Lahendades võrrandisüsteemi (8), leiame

$$A_1=-1,\quad A_2=\frac{5}{2},\quad A_3=-2,\quad A_4=1,\quad A_5=-\frac{3}{2}$$

ja seega

$$\frac{x^2-x-4}{(x-1)^3(x^2+1)}=\frac{-1}{x-1}+\frac{\frac{5}{2}}{(x-1)^2}-\frac{2}{(x-1)^3}+\frac{x-\frac{3}{2}}{x^2+1}.$$

Märkus. Konstantide A_1, A_2, A_3, A_4, A_5 leidmise hõlbustamiseks süsteemist (8) võib toimida järgmiselt: anname võrduses (7) x-le väärtused, mis on võrdsed antud ratsionaalfunktsiooni nimetaja nullkohtadega. Andes nimelt võrduses (7) x-le väärtuse 1, saame

$$-4=2A_3,$$

millest $A_3=-2$; andes võrduses (7) x-le väärtuse i, saame

$$-5-i=(-2A_4+2A_5)+(2A_4+2A_5)i$$

ehk

$$-2A_4 + 2A_5 = -5$$
$$2A_4 + 2A_5 = -1,$$

millest $A_4 = 1$, $A_5 = -\frac{3}{2}$. Konstandid A_1 ja A_2 leiame nüüd juba kergesti süsteemi (8) kahest esimesest võrrandist, kuna ülejäänud kolme võrrandit võime sel korral kasutada arvutuse kontrollimiseks.

2. Newtoni interpolatsioonivalem. Olgu antud n-astme polünoom $f(x)$ ja suurused $\xi_0, \xi_1, \xi_2, \ldots, \xi_{n-1}$ põhikorpuses K. Jagades polünoomi $f(x)$ lineaarteguriga $x - \xi_0$, leiame

$$f(x) = f(\xi_0) + (x - \xi_0) q_1(x),$$

kus $q_1(x)$ kujutab $(n-1)$-astme polünoomi (§ 5, art. 1), mida omakorda lineaarteguriga $x - \xi_1$ jagades leiame

$$q_1(x) = q_1(\xi_1) + (x - \xi_1) q_2(x),$$

kus $q_2(x)$ kujutab $(n-2)$-astme polünoomi, mida lineaarteguriga $x - \xi_2$ jagades leiame

$$q_2(x) = q_2(\xi_2) + (x - \xi_2) q_3(x),$$

kus $q_3(x)$ kujutab $(n-3)$-astme polünoomi jne. Sel viisil jagamist jätkates jõuame n sammu järel võrduseni

$$q_{n-1}(x) = q_{n-1}(\xi_{n-1}) + (x - \xi_{n-1}) q_n,$$

kus q_n osutub konstandiks. Asendades esimeses võrduses $q_1(x)$ tema avaldisega teisest võrdusest, siis tulemuses $q_2(x)$ tema avaldisega kolmandast võrdusest jne., saame valemi

$$f(x) = f(\xi_0) + q_1(\xi_1)(x - \xi_0) + q_2(\xi_2)(x - \xi_0)(x - \xi_1) + \ldots + \\ + q_n(x - \xi_0)(x - \xi_1) \ldots (x - \xi_{n-1})$$

ehk

$$(9) \quad f(x) = c_0 + c_1(x - \xi_0) + c_2(x - \xi_0)(x - \xi_1) + \ldots + \\ + c_n(x - \xi_0)(x - \xi_1) \ldots (x - \xi_{n-1}),$$

kus

$$(10) \quad c_0 = f(\xi_0), \quad c_1 = q_1(\xi_1), \quad c_2 = q_2(\xi_2), \quad \ldots, \quad c_n = q_n.$$

Valem (9) kannab Newtoni interpolatsiooni-

valemi nime. Öeldakse, et valem (9) kujutab polünoomi $f(x)$ arendist kohtadel $\xi_0, \xi_1, \xi_2, \ldots, \xi_{n-1}$. Erijuhul, kui $\xi_0 = \xi_1 = \xi_2 = \ldots = \xi_{n-1}$, omab valem (9) kuju

$$f(x) = c_0 + c_1(x - \xi_0) + c_2(x - \xi_0)^2 + \ldots + c_n(x - \xi_0)^n,$$

mis on tuntud Taylori valemi nime all. Taylori valem kujutab polünoomi $f(x)$ arendist kohal ξ_0.

Praktiliselt leitakse Newtoni interpolatsioonivalemis esinevad kordajad (10) Horneri skeemi n-kordsel rakendamisel (§ 5, art. 1). Nimelt võttes polünoomi $f(x)$ Horneri skeemis $\xi = \xi_0$, saame joone all viimasel kohal kordaja $c_0 = f(\xi_0)$, selle ees aga jagatise $q_1(x)$ kordajad. Rakendades polünoomile $q_1(x)$ Horneri skeemi kohal $\xi = \xi_1$, saame joone all viimasel kohal kordaja $c_1 = q_1(\xi_1)$, selle ees aga jagatise $q_2(x)$ kordajad. Rakendades omakorda polünoomile $q_2(x)$ Horneri skeemi kohal $\xi = \xi_2$, saame joone all viimasel kohal kordaja $c_2 = q_2(\xi_2)$ jne. Rakendades eriti Horneri skeemi n korda ühel ja samal kohal $\xi = \xi_0$, saame kordajad Taylori valemi jaoks.

Näide 6. Leida polünoomi $f(x) = 2x^4 - 5x^2 + 3x - 1$ Newtoni arendis kohtadel $-2, -1, 1, 2$.

Lähtudes $f(x)$ kordajatest $2, 0, -5, 3, -1$, leiame Horneri skeemi järjest kohtadel $-2, -1, 1, 2$ rakendades[1]:

	2	0	−5	3	−1
−2	2	−4	3	−3	5
−1	2	−6	9	−12	
1	2	−4	5		
2	2	0			

Seega $c_0 = 5$, $c_1 = -12$, $c_2 = 5$, $c_3 = 0$, $c_4 = 2$, nii et

$$f(x) = 5 - 12(x + 2) + 5(x + 2)(x + 1) + 2(x + 2)(x + 1)(x - 1)(x - 2),$$

missugust tulemust on kerge vahetu arvutuse teel kontrollida.

[1] Siin on igakordsel Horneri skeemi rakendamisel jäetud kirjutamata üks rida, sest vastavad arvutused on kergesti peast teostatavad.

3. Interpolatsiooniprobleem. Nagu nägime, võib n-astme polünoomil olla korpuses ülimalt n lahendit (§ 5, art. 1). Siit järeldub, et kaks n-astme polünoomi, mis omavad enam kui n isesugusel kohal paarikaupa võrdseid väärtusi, on võrdsed. Tõepoolest, omagu polünoomid $f(x)$ ja $g(x)$ $n+1$ isesugusel kohal $\xi_0, \xi_1, \ldots, \xi_n$ vastavalt väärtusi

$$f(\xi_0) = g(\xi_0), \quad f(\xi_1) = g(\xi_1), \ldots, f(\xi_n) = g(\xi_n).$$

Siis omab polünoom $\varphi(x) = f(x) - g(x)$, mille aste on ülimalt n, neil kohtadel väärtust null, s. o. $\xi_0, \xi_1, \ldots, \xi_n$ on polünoomi $\varphi(x)$ lahenditeks, millest järeldub ainukese võimalusena, et $\varphi(x) = 0$ ja seega $f(x) = g(x)$.

Teiste sõnadega, leidub ülimalt üks n-astme polünoom, mis omab $n+1$ isesugusel kohal $\xi_0, \xi_1, \ldots, \xi_n$ etteantud väärtusi $f(\xi_0), f(\xi_1), \ldots, f(\xi_n)$. Tegelikult leidub ka alati niisugune polünoom $f(x)$, mis rahuldab püstitatud nõuet, nimelt polünoom

$$(11) \qquad f(x) = \frac{(x-\xi_1)(x-\xi_2)\ldots(x-\xi_n)}{(\xi_0-\xi_1)(\xi_0-\xi_2)\ldots(\xi_0-\xi_n)} f(\xi_0) +$$

$$+ \frac{(x-\xi_0)(x-\xi_2)\ldots(x-\xi_n)}{(\xi_1-\xi_0)(\xi_1-\xi_2)\ldots(\xi_1-\xi_n)} f(\xi_1) + \ldots + \frac{(x-\xi_0)(x-\xi_1)\ldots(x-\xi_{n-1})}{(\xi_n-\xi_0)(\xi_n-\xi_1)\ldots(\xi_n-\xi_{n-1})} f(\xi_n),$$

nagu selles võib proovimise teel kergesti veenduda. Tähendab, leidub parajasti üks ülimalt n-astme polünoom $f(x)$, mis omab $n+1$ isesugusel kohal $\xi_0, \xi_1, \ldots, \xi_n$ vabalt etteantud väärtusi $f(\xi_0), f(\xi_1), \ldots, f(\xi_n)$. Niisuguse polünoomi $f(x)$ leidmine moodustab nn. interpolatsiooniprobleemi sisu. Teades polünoomi $f(x)$, võime siis arvutada tema väärtused igal vahepealsel kohal ξ.

Valem (11), mis kannab Lagrange'i interpolatsioonivalemi nime, lahendabki teoreetiliselt interpolatsiooniprobleemi, kuid omab praktilise arvutuse seisukohalt ühe olulise puuduse. Nimelt seisneb praktikas interpolatsiooniprobleem tabelina antud funktsiooni lähendamises polünoomiga. Siinjuures esineb sageli suurema täpsuse saavutamiseks vajadus, pärast seda, kui on leitud polünoom $f(x)$, mis omab kohtadel $\xi_0, \xi_1, \ldots, \xi_n$ tabelis antud väärtusi, moodustada kõrgema

astme polünoom, mis omaks lisaks eelmistele väärtustele veel kohal ξ_{n+1} tabelis antud väärtust $f(\xi_{n+1})$. Rakendades Lagrange'i valemit, tuleb teise polünoomi saamiseks teostada kõik arvutused uuesti, ilma et saaks kasutada $f(x)$ leidmiseks juba toimetatud arvutusi. Sellest puudusest vaba on Newtoni interpolatsioonivalem, mille rakendamist interpolatsiooniprobleemi lahendamiseks vaatlemegi käesolevas artiklis.

Olgu

$$f(x) = c_0 + c_1(x - \xi_0) + c_2(x - \xi_0)(x - \xi_1) + \ldots + \\ + c_n(x - \xi_0)(x - \xi_1) \ldots (x - \xi_{n-1})$$

otsitava polünoomi Newtoni arendis kohtadel $\xi_0, \xi_1, \ldots, \xi_{n-1}$. Andes x-le järjest väärtused $\xi_0, \xi_1, \xi_2, \ldots, \xi_n$, saame sellest arendisest

$$\begin{aligned}
f(\xi_0) &= c_0 \\
f(\xi_1) &= c_0 + c_1(\xi_1 - \xi_0) \\
f(\xi_2) &= c_0 + c_1(\xi_2 - \xi_0) + c_2(\xi_2 - \xi_0)(\xi_2 - \xi_1) \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
f(\xi_n) &= c_0 + c_1(\xi_n - \xi_0) + c_2(\xi_n - \xi_0)(\xi_n - \xi_1) + \ldots + \\
&\quad + c_n(\xi_n - \xi_0)(\xi_n - \xi_1) \ldots (\xi_n - \xi_{n-1}).
\end{aligned}$$

Lahutades siin igast võrdusest, alates teisest võrdusest, esimese võrduse ja jagades siis iga tulemust vastavalt vahega $\xi_k - \xi_0$, leiame

$$\begin{aligned}
f(\xi_0, \xi_1) &= c_1 \\
f(\xi_0, \xi_2) &= c_1 + c_2(\xi_2 - \xi_1) \\
f(\xi_0, \xi_3) &= c_1 + c_2(\xi_3 - \xi_1) + c_3(\xi_3 - \xi_1)(\xi_3 - \xi_2) \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
f(\xi_0, \xi_n) &= c_1 + c_2(\xi_n - \xi_1) + c_3(\xi_n - \xi_1)(\xi_n - \xi_2) + \ldots + \\
&\quad + c_n(\xi_n - \xi_1)(\xi_n - \xi_2) \ldots (\xi_n - \xi_{n-1}),
\end{aligned}$$

kus

$$f(\xi_0, \xi_k) = \frac{f(\xi_k) - f(\xi_0)}{\xi_k - \xi_0}$$

nimetatakse polünoomi $f(x)$ tõusuks kohtadel ξ_0, ξ_k. Lahutades viimase süsteemi igast võrdusest, alates teisest võr-

dusest, esimese võrduse ja jagades siis iga tulemust vastavalt vahega $\xi_k - \xi_1$, saame

$$f(\xi_0, \xi_1, \xi_2) = c_2$$
$$f(\xi_0, \xi_1, \xi_3) = c_2 + c_3(\xi_3 - \xi_2)$$
$$f(\xi_0, \xi_1, \xi_4) = c_2 + c_3(\xi_4 - \xi_2) + c_4(\xi_4 - \xi_2)(\xi_4 - \xi_3)$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$f(\xi_0, \xi_1, \xi_n) = c_2 + c_3(\xi_n - \xi_2) + c_4(\xi_n - \xi_2)(\xi_n - \xi_3) + \dots + c_n(\xi_n - \xi_2)(\xi_n - \xi_3)\dots(\xi_n - \xi_{n-1}),$$

kus

$$f(\xi_0, \xi_1, \xi_k) = \frac{f(\xi_0, \xi_k) - f(\xi_0, \xi_1)}{\xi_k - \xi_1}$$

nimetatakse polünoomi $f(x)$ *teist järku tõusuks kohtadel* ξ_0, ξ_1, ξ_k. Sel viisil edasi minnes võime üksteise järel arvutada Newtoni interpolatsioonivalemi kordajad

$$c_0 = f(\xi_0), \quad c_1 = f(\xi_0, \xi_1), \quad c_2 = f(\xi_0, \xi_1, \xi_2), \dots,$$

kasutades ainult interpolatsiooniprobleemi andmeid. Ühtlasi nähtub siit, et Newtoni interpolatsioonivalemis on kordajad c_0, c_1, c_2, ..., c_n polünoomiga $f(x)$ üheselt määratud ja et juhul, kui meil on tarvis leida teine polünoom, mis omaks lisaks eelmistele väärtustele veel kohal ξ_{n+1} väärtust $f(\xi_{n+1})$, tarvitseb vaid arvutada kordaja c_{n+1}, kuna kõik eelnevad kordajad jäävad endisteks.

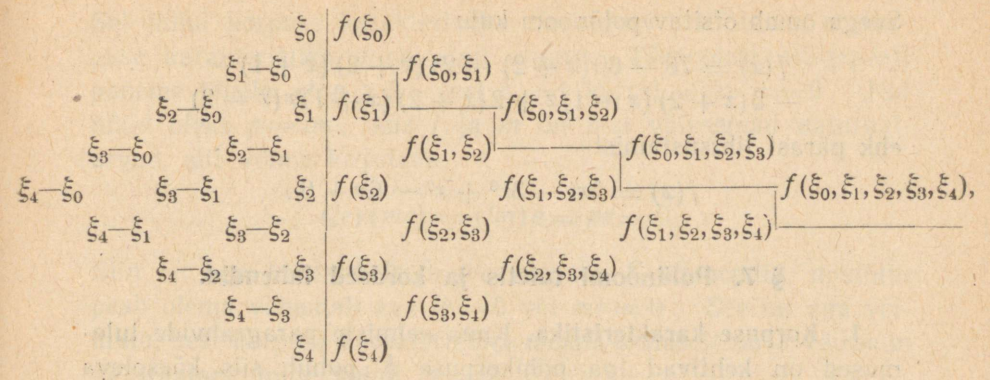
Et iga kordajat c_k võib vaadelda kui pealiikme kordajat polünoomis

$$c_0 + c_1(x - \xi_0) + c_2(x - \xi_0)(x - \xi_1) + \dots + c_k(x - \xi_0)(x - \xi_1)\dots(x - \xi_{k-1}),$$

mis omab kohtadel $\xi_0, \xi_1, \dots, \xi_k$ vastavalt väärtusi $f(\xi_0)$, $f(\xi_1)$, ..., $f(\xi_k)$, siis ei ole c_k arvutamisel oluline kohtade $\xi_0, \xi_1, \dots, \xi_k$ järjekord, sest viimane polünoom on interpolatsiooniprobleemi ühesuse tõttu sõltumatu sellest järjekorrast. Seetõttu võib kordajate c_k kui tõusude järk-järgulist arvutamist toimetada vastavalt järgmisele skeemile [1]:

---

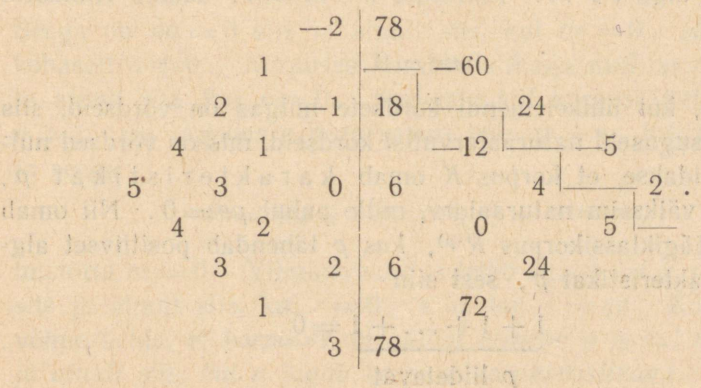
[1] Siin on näiteks kordaja $c_2 = f(\xi_0, \xi_1, \xi_2)$ arvutatud valemi $c_2 = \frac{f(\xi_0, \xi_2) - f(\xi_0, \xi_1)}{\xi_2 - \xi_1}$ asemel valemist $c_2 = \frac{f(\xi_1, \xi_2) - f(\xi_0, \xi_1)}{\xi_2 - \xi_0}$, mis vastab kohtade ξ_0, ξ_1, ξ_2 järjestusele ξ_1, ξ_0, ξ_2 jne.



kus $n=4$. Siin kaks keskmist veergu koosnevad interpolatsiooniprobleemi andmeist. Järgnevad veerud skeemi vasakpoolses osas kujutavad kõrvuti seisvate kohtade vahesid, siis vahesid üle ühe koha, vahesid üle kahe koha jne. Skeemi parempoolses osas saadakse iga veerg eelnevast, moodustades kõrvuti seisvate suuruste vahed ja jagades need vastavate vahedega skeemi vasakpoolses osas. Otsitavad kordajad c_k on eraldatud treppjoonega.

Näide 7. Leida madalaima astme polünoom, mis omab kohtadel −2, −1, 0, 2, 3 vastavalt väärtusi 78, 18, 6, 6, 78.

Ülal antud skeemi kohaselt arvutades leiame



Seega omab otsitav polünoom kuju

$$f(x) = 78 - 60(x+2) + 24(x+2)(x+1) - \\ - 5(x+2)(x+1)x + 2(x+2)(x+1)x(x-2)$$

ehk pärast lihtsustamist

$$f(x) = 2x^4 - 3x^3 + x^2 - 6x + 6 .$$

§ 7. Polünoomi tuletis ja kordsed lahendid.

1. Korpuse karakteristika. Kuna eelmiste paragrahvide tulemused on kehtivad iga põhikorpuse K puhul, siis käesoleva paragrahvi tulemused sõltuvad teataval määral aluseks võetud põhikorpusest. Seepärast teostame siin kõigepealt korpuste liigituse.

Olgu vaadeldava korpuse K ühikelement e. Moodustame selle ühikelemendi täisarvulised kordsed

$$\ldots, \; -3e, \; -2e, \; -e, \; 0, \; e, \; 2e, \; 3e, \; \ldots .$$

Kui need kordsed on kõik üksteisest erinevad, siis öeldakse, et korpus K omab karakteristikat null. Nii omab näiteks iga arvukorpus karakteristikat null.

Oletame nüüd, et ühikelemendi kordsete hulgas leidub kaks omavahel võrdset, s. o.

$$le = me ,$$

kusjuures olgu $l > m$. Märkides $l - m = n$, saame viimasest võrdusest

$$ne = 0 .$$

Tähendab, kui ühikelemendi kordsete hulgas on võrdseid, siis leidub niisuguseid naturaalarvulisi kordseid, mis on võrdsed nulliga. Öeldakse, et korpus K omab karakteristikat p, kui p on väikseim naturaalarv, mille puhul $pe = 0$. Nii omab näiteks jäägiklassikorpus $R^{(p)}$, kus p tähendab positiivset algarvu, karakteristikat p, sest siin

$$\underbrace{1 + 1 + \ldots + 1}_{p \text{ liidetavat}} = 0 .$$

Sel juhul korpuse karakteristika on algarv. Näitame, et korpuse karakteristika p on alati algarv. Tõepoolest, kõigepealt paneme tähele, et $p \geqslant 2$, sest $p = 1$ korral oleks $e = 0$. Kui nüüd oleks $p = lm$, kus l ja m on p-st väiksemad naturaalarvud, siis võime kirjutada

$$(le)(me) = (lm)e = pe = 0.$$

Siin on aga kordsed le ja me korpuse K elemendid, mistõttu peab olema vähemalt kas $le = 0$ või $me = 0$. See on aga võimatu, sest korpuse karakteristika mõiste kohaselt on p väikseim naturaalarv, mille puhul $pe = 0$.

Seega jagunevad kõik korpused kahte liiki: korpused karakteristikaga null ja korpused algarvulise karakteristikaga $p \geqslant 2$. Käesolevas paragrahvis piirdume peamiselt korpustega karakteristikaga null kui praktikas kõige sagedamini esinevate korpustega.

Olgu a mingi nullist erinev element korpuses K. Tekib küsimus, missuguse naturaalarvu n korral on $na = 0$. Et

$$na = \underbrace{a + a + \ldots + a}_{n \text{ liidetavat}} = a(\underbrace{e + e + \ldots + e}_{n \text{ liidetavat}}),$$

siis võib kordset na esitada korrutisena

$$na = a(ne).$$

Seega on $na = 0$ siis ja ainult siis, kui $ne = 0$, sest eelduse kohaselt $a \neq 0$. Korpuses karakteristikaga null on $ne = 0$ siis ja ainult siis, kui $n = 0$. Seevastu kui korpuse karakteristika $p \geqslant 2$, siis jagades n p-ga saame $n = qp + r$, kus $0 \leqslant r < p$, ja seega

$$ne = (qp + r)e = q(pe) + re = re,$$

mistõttu $re = 0$. Viimane võrdus leiab aga $0 \leqslant r < p$ tõttu aset siis ja ainult siis, kui $r = 0$, s. o. kui $n = qp$. Kokku võttes võime öelda, et *korpuses on nullist erineva a puhul $na = 0$ siis ja ainult siis, kui n jagub korpuse karakteristikaga.*

2. **Polünoomi tuletis.** Matemaatilises analüüsis defineeritakse funktsiooni $f(x)$ tuletist $f'(x)$ kui piirväärtust

$$\lim_{h\to 0}\frac{f(x+h)-f(x)}{h}.$$

Et piirväärtus ei oma mõtet iga põhikorpuse puhul, siis pole see definitsioon kohane polünoomi tuletise defineerimiseks algebras. Seepärast defineerime mistahes põhikorpuse K puhul polünoomi

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$$

tuletist lihtsalt kui polünoomi

$$f'(x)=na_0x^{n-1}+(n-1)a_1x^{n-2}+\ldots+2a_{n-2}x+a_{n-1}.$$

Siit nähtub, et n-astme polünoomi tuletis on ülimalt $(n-1)$-astme polünoom ja tingimata $(n-1)$-astme polünoom, kui põhikorpuse karakteristika on null. Kui

$$g(x)=b_0x^m+b_1x^{m-1}+\ldots+b_{m-1}x+b_m$$

tähendab veel mingit polünoomi üle K, siis on

$$g'(x)=mb_0x^{m-1}+(m-1)b_1x^{m-2}+\ldots+2b_{m-2}x+b_{m-1}.$$

Toetudes polünoomidega opereerimise eeskirjadele, ei ole raske näha, et kehtivad valemid

$$[f(x)+g(x)]'=f'(x)+g'(x)$$
$$[f(x)\cdot g(x)]'=f'(x)g(x)+f(x)g'(x)$$

ja üldiselt

$$[f_1(x)+f_2(x)+\ldots+f_n(x)]'=f_1'(x)+f_2'(x)+\ldots+f_n'(x)$$
$$[f_1(x)f_2(x)\ldots f_n(x)]'=f_1'(x)f_2(x)\ldots f_n(x)+$$
$$+f_1(x)f_2'(x)\ldots f_n(x)+\ldots+f_1(x)f_2(x)\ldots f_n'(x).$$

Erijuhul $f_1(x)=f_2(x)=\ldots=f_n(x)=f(x)$ saame viimasest valemist

$$[f^n(x)]'=nf^{n-1}(x)f'(x).$$

Peale tuletise $f'(x)$ defineerime veel teist järku tuletise $f''(x)$ kui tuletise tuletise, kolmandat järku tuletise $f'''(x)$ kui teist järku tuletise tuletise jne.

Vaatleme polünoomi $f(x)$ Taylori arendist kohal ξ_0 (§ 6, art. 2):

$$f(x) = c_0 + c_1(x - \xi_0) + c_2(x - \xi_0)^2 + \ldots + \\ + c_k(x - \xi_0)^k + c_{k+1}(x - \xi_0)^{k+1} + \ldots + c_n(x - \xi_0)^n.$$

Arvutades $f(x)$ k-järku tuletise, leiame

$$f^{(k)}(x) = k!c_k + (k+1)k \ldots 2c_{k+1}(x - \xi_0) + \ldots + \\ + n(n-1) \ldots (n-k+1)c_n(x - \xi_0)^{n-k}.$$

Andes tulemuses x-le väärtuse ξ_0, saame

$$f^{(k)}(\xi_0) = k!c_k. \tag{12}$$

Siin $k!c_k$ kujutab kordset, mida võime esitada korrutisena

$$k!c_k = (k!e)c_k.$$

Kui põhikorpuse K karakteristika on null, siis on $k!e \neq 0$ ja me saame valemist (12)

$$c_k = \frac{f^{(k)}(\xi_0)}{k!e}$$

ehk, nagu seda lihtsalt kirjutatakse,

$$c_k = \frac{f^{(k)}(\xi_0)}{k!}.$$

Seega kui põhikorpus on karakteristikaga null, siis võime Taylori valemile anda kuju

$$f(x) = f(\xi_0) + \frac{f'(\xi_0)}{1!}(x - \xi_0) + \frac{f''(\xi_0)}{2!}(x - \xi_0)^2 + \ldots + \\ + \frac{f^{(n)}(\xi_0)}{n!}(x - \xi_0)^n.$$

Seevastu näiteks jäägiklassikorpuses $R^{(3)}$ ei saa polünoomi $f(x) = 2x^4 + x + 1$ Taylori arendisele

$$f(x) = 1 + 2(x-1)^3 + 2(x-1)^4$$

anda ülaltoodud kuju, sest siin on $f'''(x) = 0$, $f^{IV}(x) = 0$ ja $3! = 0$, $4! = 0$.

3. Kordsed lahendid. Rakendame nüüd tuletise mõistet polünoomi kordsete lahendite uurimiseks. Nimetame suurust ξ, mis võib kuuluda kas põhikorpusse K või mingisse ülemkorpusse, polünoomi $f(x)$ α-kordseks lahendiks, kui $f(x)$ jagub $(x-\xi)^\alpha$-ga, kuid ei jagu $(x-\xi)^{\alpha+1}$-ga, s. o. kui

$$f(x) = (x-\xi)^\alpha \varphi(x),$$

kus $\varphi(x)$ ei jagu teguriga $x-\xi$ ja seega $\varphi(\xi) \neq 0$. Arvutades $f(x)$ tuletise, leiame

$$(13) \qquad f'(x) = \alpha(x-\xi)^{\alpha-1}\varphi(x) + (x-\xi)^\alpha \varphi'(x) = \\ = (x-\xi)^{\alpha-1}[\alpha\varphi(x) + (x-\xi)\varphi'(x)],$$

millest nähtub, et *polünoomi α-kordne lahend esineb tuletises vähemalt $(\alpha-1)$-kordse lahendina.* Seega esineb iga kordne lahend ka polünoomi tuletise lahendina. Seevastu harilik, s. o. ühekordne lahend ei esine enam lahendina tuletises, sest võttes võrduses (13) $\alpha = 1$, saame

$$f'(x) = \varphi(x) + (x-\xi)\varphi'(x),$$

millest ilmneb, et $f'(x)$ ei jagu teguriga $x-\xi$. Tähendab, *polünoomil $f(x)$ puuduvad kordsed lahendid siis ja ainult siis, kui $f(x)$ ja $f'(x)$ on ühistegurita, s. o. kui $(f, f') = 1$.*

Juhul kui põhikorpus K on karakteristikaga null, siis $\alpha\varphi(x)$ ei ole kunagi nullpolünoom ega saa seega jaguda teguriga $x-\xi$. Siis ei jagu aga ka summa $\alpha\varphi(x) + (x-\xi)\varphi'(x)$ teguriga $x-\xi$, mistõttu ξ on võrduse (13) põhjal $f'(x)$ jaoks parajasti $(\alpha-1)$-kordne lahend. Tähendab, *kui põhikorpuse karakteristika on null, siis on polünoomi α-kordne lahend tuletise $(\alpha-1)$-kordseks lahendiks.* Niisiis on korpuses karakteristikaga null ξ polünoomi $f(x)$ α-kordseks lahendiks siis ja ainult siis, kui

$$f(\xi) = 0, \quad f'(\xi) = 0, \quad f''(\xi) = 0, \quad \ldots, \quad f^{(\alpha-1)}(\xi) = 0, \\ f^{(\alpha)}(\xi) \neq 0.$$

Olgu tähendatud, et korpuses karakteristikaga $p \geqslant 2$ ei tarvitse polünoomi lahendi kordsus tuletise puhul ühe võrra väheneda. Nii on näiteks jäägiklassikorpuses $R^{(3)}$ polünoomi

$f(x) = (x-1)^3(x+1)$ kolmekordne lahend $\xi = 1$ ka tuletises kolmekordseks lahendiks, sest siin

$$f'(x) = 3(x-1)^2(x+1) + (x-1)^3 = (x-1)^3.$$

Et polünoomi $f(x)$ kordsed lahendid on ühtlasi ka tuletise $f'(x)$ lahenditeks, harilikud lahendid aga mitte, siis on $f(x)$ kordsed lahendid määratud $f(x)$ ja $f'(x)$ suurima ühisteguriga (f, f') selles mõttes, et (f, f') lahenditeks on $f(x)$ kordsed lahendid ja ainult need. Arvutades (f, f'), eraldame küll kordsed lahendid harilikest lahenditest, kuid sellega pole veel kordsed lahendid eraldatud nende kordsuste järgi, s. t. pole teada polünoomi, mille lahenditeks oleksid $f(x)$ ühe ja sama kordsusega lahendid ja ainult need. Seame nüüd endale ülesandeks eraldada kõik lahendid vastavalt nende kordsusele, piirdudes seejuures põhikorpustega, mille karakteristika on null.

Lahutades polünoomi $f(x)$ lineaartegurite korrutiseks, leiame [1]

$$f(x) = (x-\xi_1)^{\alpha_1}(x-\xi_2)^{\alpha_2}\ldots(x-\xi_r)^{\alpha_r}.$$

Olgu $f(x)$ lahendite suurim kordsus α. Tähendagu X_1 kõigile $f(x)$ harilikele lahenditele vastavate lineaartegurite korrutist, X_2 kõigile kahekordsetele lahenditele vastavate lineaartegurite korrutist, milles iga tegur on võetud ühekordselt, X_3 kõigile kolmekordsetele lahenditele vastavate lineaartegurite korrutist, milles iga tegur on võetud ühekordselt jne., lõppeks tähendagu X_α kõigile α-kordsetele lahenditele vastavate lineaartegurite korrutist, milles iga tegur on võetud ühekordselt. Kui polünoomil $f(x)$ puuduvad lahendid mingi kordsusega k, kus $k < \alpha$, siis võtame $X_k = 1$. Seega võime kirjutada

$$f(x) = X_1X_2^2X_3^3\ldots X_\alpha^\alpha.$$

Et siin iga lahend esineb tuletises ühe võrra väiksema kordsusega, siis märkides $d_1(x) = (f, f')$, võime kirjutada

$$d_1(x) = X_2X_3^2X_4^3\ldots X_\alpha^{\alpha-1}.$$

---

[1] Siin on eeldatud $f(x)$ normeerituna.

Märkides edasi, $d_2(x) = (d_1, d_1')$, siis $d_3(x) = (d_2, d_2')$ jne., lõppeks $d_\alpha(x) = (d_{\alpha-1}, d'_{\alpha-1})$, leiame analoogiliselt

$$\begin{aligned} d_2(x) &= X_3 X_4^2 \dots X_\alpha^{\alpha-2} \\ d_3(x) &= \quad X_4 \dots X_\alpha^{\alpha-3} \\ &\dots\dots\dots\dots\dots \\ d_{\alpha-1}(x) &= \quad X_\alpha \\ d_\alpha(x) &= \quad 1. \end{aligned}$$

Moodustades jagatised

$$\begin{aligned} g_1(x) &= \frac{f(x)}{d_1(x)} = X_1 X_2 X_3 \dots X_\alpha \\ g_2(x) &= \frac{d_1(x)}{d_2(x)} = X_2 X_3 \dots X_\alpha \\ g_3(x) &= \frac{d_2(x)}{d_3(x)} = X_3 \dots X_\alpha \\ &\dots\dots\dots\dots\dots\dots \\ g_{\alpha-1}(x) &= \frac{d_{\alpha-2}(x)}{d_{\alpha-1}(x)} = X_{\alpha-1} X_\alpha \\ g_\alpha(x) &= \frac{d_{\alpha-1}(x)}{d_\alpha(x)} = X_\alpha, \end{aligned}$$

leiame veelkord jagades

$$X_1 = \frac{g_1(x)}{g_2(x)}, \quad X_2 = \frac{g_2(x)}{g_3(x)}, \dots, \quad X_{\alpha-1} = \frac{g_{\alpha-1}(x)}{g_\alpha(x)}, \quad X_\alpha = g_\alpha(x).$$

Seega on polünoomi $f(x)$ lahendid eraldatud nende kordsuse järgi: polünoomi $f(x)$ lahendite leidmine on taandatud madalama astme polünoomide

$$X_1, \ X_2, \ \dots, \ X_\alpha$$

lahendite leidmisele, kusjuures polünoomi X_k lahendid kujutavad $f(x)$ k-kordseid lahendeid. Olgu rõhutatud, et ülalantud meetod polünoomi kordsete lahendite eraldamiseks on üldiselt rakendatav vaid korpuses karakteristikaga null.

Näide 8. Eraldada polünoomi

$$f(x) = x^6 + 3x^4 - 4$$

kordsed lahendid.

Arvutades tuletise $f'(x) = 6x^5 + 12x^3$, leiame Eukleidese algoritmi abil (§ 4, art. 1)

$$d_1(x) = (f, f') = x^2 + 2,$$

kust $d_1'(x) = 2x$ ja seega

$$d_2(x) = (d_1, d_1') = 1.$$

Moodustades jagatised

$$g_1(x) = \frac{f(x)}{d_1(x)} = x^4 + x^2 - 2$$

$$g_2(x) = \frac{d_1(x)}{d_2(x)} = x^2 + 2,$$

leiame

$$X_1 = \frac{g_1(x)}{g_2(x)} = x^2 - 1, \quad X_2 = g_2(x) = x^2 + 2.$$

Seega on $f(x)$ harilikeks lahenditeks polünoomi $x^2 - 1$ lahendid, s. o. ± 1 ja kahekordseteks lahenditeks polünoomi $x^2 + 2$ lahendid, s. o. $\pm i\sqrt{2}$.

Harjutusülesandeid.

24. Määrata a ja b nii, et polünoom $x^4 + 3x^2 + ax + b$ jaguks polünoomiga $x^2 - 2ax + 2$.

25. Leida polünoomide

a) $x^5 - x^2 - x + 1$, $x^4 - 2x^3 - 4x^2 + 2x + 3$;

b) $x^4 - 10x^2 + 1$, $x^4 - 4\sqrt{2}x^3 + 6x^2 + 4\sqrt{2}x + 1$

suurim ühistegur.

26. Leida polünoomid X ja Y nii, et

a) $(x^4 - 1)X + (x^3 + i)Y = x - i$;

b) $(4x^4 - 2x^3 - 16x^2 + 5x + 9)X + (2x^3 - x^2 - 5x + 4)Y = 3x - 3$.

27. Lahutada polünoom $x^8 - 1$ taandumatute polünoomide korrutiseks:

a) ratsionaalarvude korpuses;
b) reaalarvude korpuses;
c) kompleksarvude korpuses;
d) jäägiklassikorpuses $R^{(7)}$.

28. Jagada Horneri skeemi abil polünoom $2x^5 - 5x^3 - 8x$ lineaarteguriga

a) $x + 2$; b) $x - i$.

29. Leida algebras $R^{(x^2+1)}$ $\sqrt{3}$ ja $\sqrt{5}$ väärtused, kui põhikorpuseks on jäägiklassikorpus $R^{(7)}$.

30. Arvutada algebras $R^{(x^3+x^2+1)}$

$$\left(\frac{1+2j-3j^2}{1-2j+3j^2}\right)^2 + \left(\frac{1-2j+3j^2}{1+2j-3j^2}\right)^2,$$

kus $j^3 = -j^2 - 1$, kui põhikorpuseks on jäägiklassikorpus $R^{(5)}$.

31. Lahutada polünoom $x^3 + x + 1$ lineaartegurite korrutiseks, kui põhikorpuseks on jäägiklassikorpus $R^{(2)}$.

32. Lahutada ratsionaalfunktsioon

$$\frac{1}{(x^2+3)(x-1)^2}$$

osamurdudeks:

a) reaalarvude korpuses;
b) kompleksarvude korpuses;
c) jäägiklassikorpuses $R^{(5)}$.

33. Leida polünoomide

a) $x^5 - 2x^2 + x - 2$; b) $2x^5 - 3x^4 + 2x^2 - 3$

Newtoni arendised kohtadel -4, -1, 1, 3, 4.

34. Leida ülesande 33 polünoomide Taylori arendised kohal 2.

35. Lahutada ratsionaalfunktsioonid

a) $\frac{x^3+x-2}{(x+2)^5}$; b) $\frac{x^4+x^2-1}{(x+1)^5}$

osamurdudeks, rakendades lugejatele Taylori valemit.

36. Leida ülimalt neljanda astme polünoom, mis omab kohtadel

a) 1, 2, 3, 4, 6 vastavalt väärtusi 5, 6, 1, —4, 10;

b) $-2i$, $-i$, 0, i, $2i$ vastavalt väärtusi $31+16i$, $7+2i$, 3, $31-16i$, $7-2i$.

37. Ülimalt $(n-1)$-astme polünoom $f(x)$ omab kohtadel $\varepsilon_0, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n-1}$ vastavalt väärtusi $y_0, y_1, y_2, \ldots, y_{n-1}$. Leida $f(0)$, kui $\varepsilon_0, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n-1}$ tähendavad n-astme ühejuuri.

38. Määrata a ja b nii, et $\xi=1$ oleks polünoomi ax^4+bx^3+1 kahekordne lahend.

39. Missuguseid tingimusi peavad rahuldama a, b ja k, et neljanda astme polünoom

$$x^4+ax^k+b$$

omaks kolmekordset lahendit?

40. Leida neljanda astme polünoom, mis annab jagamisel $(x-1)^3$-ga jäägi 8 ja jagamisel $(x+1)^2$-ga jäägi —8.

41. Leida polünoomi

$$x^{2n+1}-\frac{n(n+1)(2n+1)}{6}x^{n+2}+\frac{(n-1)(n+2)(2n+1)}{2}x^{n+1}-$$
$$-\frac{(n-1)(n+2)(2n+1)}{2}x^n+\frac{n(n+1)(2n+1)}{6}x^{n-1}-1$$

lahendi $\xi=1$ kordsus.

42. Eraldada polünoomide

a) $x^5-6x^4+16x^3-24x^2+20x-8$,

b) $x^6+x^5+5x^4+4x^3+8x^2+4x+4$;

c) $x^7-3x^6+5x^5-7x^4+7x^3-5x^2+3x-1$

kordsed lahendid.

III. Polünoomid üle integriteetkonna.

§ 8. Polünoomi taanduvus täisarvude integriteetkonnas.

1. Algtegureiks lahutamise lause. Vaatleme mingit polünoomi $g(x)$ üle täisarvude integriteetkonna, s. o. polünoomi $g(x)$, mille kordajateks on täisarvud. Polünoom $g(x)$ omab alati triviaalseid tegureiks lahutusi, s. o. niisuguseid tegureiks lahutusi

$$g(x) = g(x) \cdot 1, \quad g(x) = [-g(x)] \cdot (-1),$$

kus üheks teguriks on 1 või -1. Kui nullist erinev täisarvuliste kordajatega polünoom, mis ei ole 1 ega -1, omab ainult triviaalseid tegureiks lahutusi, siis nimetame seda polünoomi taandumatuks täisarvude integriteetkonnas, vastasel korral aga taanduvaks. Nii on näiteks polünoom $2x - 4$ taanduv täisarvude integriteetkonnas, omades tegureiks lahutust

$$2x - 4 = 2(x - 2).$$

Seevastu ratsionaalarvude korpuses on sama polünoom taandumatu, kuna 2 on seal triviaalne tegur. Ümberpöördult saab näidata: *kui täisarvuliste kordajatega polünoom on taanduv ratsionaalarvude korpuses, siis on see polünoom taanduv ka täisarvude integriteetkonnas.*

Tõepoolest, olgu

$$g(x) = f_1(x) f_2(x),$$

kus $f_1(x)$ ja $f_2(x)$ tähendavad ratsionaalarvuliste kordajatega mittekonstantseid polünoome. Märkides $f_1(x)$ kordajate ühisnimetaja δ_1-ga ja $f_2(x)$ kordajate ühisnimetaja δ_2-ga, võime kirjutada

$$f_1(x) = \frac{g_1(x)}{\delta_1}, \quad f_2(x) = \frac{g_2(x)}{\delta_2}.$$

Siin polünoomide $g_1(x)$ ja $g_2(x)$ kordajad on täisarvud. Olgu polünoomi $g_1(x)$ kordajate suurim ühistegur d_1 ja polünoomi $g_2(x)$ kordajate suurim ühistegur d_2, nii et

$$g_1(x) = d_1\varphi_1(x), \quad g_2(x) = d_2\varphi_2(x)$$

ja seega

$$g(x) = \frac{d_1 d_2}{\delta_1 \delta_2}\varphi_1(x)\varphi_2(x)$$

ehk

$$g(x) = \frac{d}{\delta}\varphi_1(x)\varphi_2(x), \tag{1}$$

kus $\frac{d}{\delta}$ tähendab murdu $\frac{d_1 d_2}{\delta_1 \delta_2}$ taandatud kujul ja $\varphi_1(x)$, $\varphi_2(x)$ on niisugused polünoomid, mille kordajateks on ühistegurita täisarvud. Selliseid polünoome, mille kordajateks on ühistegurita täisarvud, nimetatakse Gauss'i järgi primitiivseteks polünoomideks.

Et $g(x)$ on täisarvuliste kordajatega polünoom, siis peab võrduse (1) järgi korrutis $\varphi_1(x)\varphi_2(x)$ jaguma δ-ga, s. o. δ peab olema $\varphi_1(x)\varphi_2(x)$ kordajate ühisteguriks. Gauss on aga näidanud, et *kahe primitiivse polünoomi korrutis kujutab ka primitiivset polünoomi*. Seetõttu peab olema $\delta = 1$, nii et võrdus (1) omab kuju

$$g(x) = d\varphi_1(x)\varphi_2(x),$$

millest nähtubki, et $g(x)$ on taanduv täisarvude integriteetkonnas.

Jääb tõestada ülalnimetatud Gaussi teoreem, mille järgi primitiivsete polünoomide

$$\varphi_1(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n,$$
$$\varphi_2(x) = \beta_0x^m + \beta_1x^{m-1} + \ldots + \beta_m$$

korrutis on ka primitiivne. Näitame selleks, et korrutise $\varphi_1(x)\varphi_2(x)$ kõik kordajad ei saa jaguda ühe ja sama algarvuga p. Et $\varphi_1(x)$ ja $\varphi_2(x)$ on primitiivsed polünoomid, siis ei saa kõik nende kordajad jaguda p-ga. Olgu a_i polünoo-

mis $\varphi_1(x)$ esimene kordaja [1], mis ei jagu p-ga ja β_k polünoomis $\varphi_2(x)$ esimene kordaja [1], mis ei jagu p-ga. Vaatleme korrutises

$$\varphi_1(x)\varphi_2(x) = \gamma_0 x^{n+m} + \gamma_1 x^{n+m-1} + \ldots + \gamma_{n+m}$$

kordajat

$$\gamma_{i+k} = \alpha_0\beta_{i+k} + \alpha_1\beta_{i+k-1} + \ldots + \alpha_{i-1}\beta_{k+1} + \alpha_i\beta_k + \alpha_{i+1}\beta_{k-1} + \ldots + \\ + \alpha_{i+k-1}\beta_1 + \alpha_{i+k}\beta_0 .$$

Et α_0, α_1, $\ldots$, α_{i-1} ja β_0, β_1, $\ldots$, β_{k-1} jaguvad p-ga, α_i ja β_k aga mitte, siis jaguvad γ_{i+k} avaldises kõik liidetavad p-ga peale $\alpha_i\beta_k$, mistõttu γ_{i+k} ei jagu p-ga. Seega ongi Gaussi teoreem tõestatud.

Niisiis toob täisarvuliste kordajatega polünoomi taanduvus ratsionaalarvude korpuses endaga kaasa taanduvuse täisarvude integriteetkonnas. Ümberpöördult ei tarvitse üldiselt polünoomi taanduvusest täisarvude integriteetkonnas järelduda taanduvus ratsionaalarvude korpuses, nagu see nähtus eespool vaadeldud polünoomist $2x + 4$. See polünoom ei ole aga primitiivne. Seevastu pole raske näha, et primitiivsete polünoomide vallas kattub taanduvuse mõiste täisarvude integriteetkonnas taanduvuse mõistega ratsionaalarvude korpuses. Eriti on seega iga primitiivse polünoomi $\varphi(x)$ puhul kehtiv algtegureiks lahutamise lause (§ 4, art. 3), mille järgi

$$\varphi(x) = p_1(x)p_2(x) \ldots p_k(x),$$

kus $p_1(x)$, $p_2(x)$, $\ldots$, $p_k(x)$ tähendavad taandumatuid primitiivseid polünoome, mis on üheselt määratud kuni triviaalsete teguriteni 1 ja -1.

Olgu nüüd $g(x)$ mistahes täisarvuliste kordajatega polünoom ja d tema kordajate suurim ühistegur, nii et

$$g(x) = d\varphi(x),$$

kus $\varphi(x)$ on primitiivne polünoom. Et täisarvude integriteetkon-

[1] Pealiikme poolt arvates.

nas on kehtiv algtegureiks lahutamise lause (I, § 7, art. 3), siis on $|d| > 1$ korral

$$d = q_1 q_2 \ldots q_l,$$

kus q_1, q_2, ..., q_l on algarvud, mis on üheselt määratud kuni triviaalsete teguriteni 1 ja -1. Seega kehtib ka polünoomkonnas üle täisarvude integriteetkonna algtegureiks lahutamise lause.

Teoreem 1. *Polünoomkonnas üle täisarvude integriteetkonna laseb iga polünoom*[1] $g(x)$ *ennast lahutada taandumatute polünoomide korrutiseks*

$$g(x) = q_1 q_2 \ldots q_l p_1(x) p_2(x) \ldots p_k(x),$$

kus tegurid q_1, q_2, ..., q_l, $p_1(x)$, $p_2(x)$, ..., $p_k(x)$ *on kuni triviaalsete teguriteni* 1 *ja* -1 *üheselt määratud.*

Siinjuures olgu tähendatud, et polünoomkonnas üle täisarvude integriteetkonna kujutavad algarvulised konstandid taandumatuid polünoome.

2. Eisenstein'i teoreem. Polünoomide taandumatust täisarvude integriteetkonnas saab paljudel juhtudel kindlaks teha järgmise kriteeriumi abil, mis on antud Eisenstein'i poolt 1850. aastal.

Teoreem 2. *Kui täisarvuliste kordajatega polünoomi*

$$g(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

kõik kordajad peale pealiikme kordaja a_0 *jaguvad mingi algarvuga* p, *seejuures aga vabaliige* a_n *ei jagu* p^2*-ga, siis on* $g(x)$ *taandumatu täisarvude integriteetkonnas.*

Tõestuseks oletame vastupidi, et $g(x)$ on taanduv, lagunedes kahe täisarvuliste kordajatega polünoomi korrutiseks:

$$g(x) = (b_0 x^m + b_1 x^{m-1} + \ldots + b_{m-1} x + b_m)(c_0 x^l + c_1 x^{l-1} + \ldots + c_{l-1} x + c_l),$$

kus $m + l = n$. Pärast korrutamist leiame x-i ühesuguste astmete kordajaid võrreldes:

[1] Välja arvatud nullpolünoom ja triviaalsed tegurid 1 ja -1.

$$
\begin{aligned}
a_0 &= b_0c_0\\
a_1 &= b_0c_1 + b_1c_0\\
&\dots\dots\dots\dots\dots\dots\\
a_l &= b_0c_l + b_1c_{l-1} + \dots + b_lc_0\\
&\dots\dots\dots\dots\dots\dots\\
a_{n-1} &= b_{m-1}c_l + b_mc_{l-1}\\
a_n &= b_mc_l\,.
\end{aligned}
\tag{2}
$$

Viimasest võrdusest (2) nähtub, et korrutis b_mc_l jagub p-ga, mistõttu peab üks tegureist, näiteks b_m, jaguma p-ga (I, § 7, art. 3). Siis aga c_l ei või enam jaguda p-ga, sest vastasel korral jaguks a_n p^2-ga. Edasi selgub eelviimasest võrdusest (2), et korrutis $b_{m-1}c_l$ peab jaguma p-ga. Et siin aga c_l ei jagu p-ga, siis peab b_{m-1} jaguma p-ga. Minnes sel viisil võrduste ahelikus (2) järkjärgult ülespoole, järeldame võrdusest

$$a_l = b_0c_l + b_1c_{l-1} + \dots + b_lc_0\,,$$

et b_0 peab jaguma p-ga. Esimese võrduse (2) järgi peab siis aga a_0 jaguma p-ga, vastupidi eeldusele. Tähendab, oletus $g(x)$ taanduvusest viib vastuolule.

Eisensteini teoreemi järgi on näiteks iga polünoom

$$g(x) = x^n + px + p\,,$$

kus p tähendab algarvu, taandumatu täisarvude integriteetkonnas. Vaatleme teise näitena polünoomi

$$g(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1\,,$$

kus p olgu algarv. Siin pole Eisensteini teoreem vahetult rakendatav. Kuid asendades $x = y + 1$ saame polünoomi

$$g(y+1) = \frac{(y+1)^p - 1}{y} = \frac{y^p + \binom{p}{1}y^{p-1} + \binom{p}{2}y^{p-2} + \dots + \binom{p}{1}y + 1 - 1}{y} =$$

$$= y^{p-1} + py^{p-2} + \frac{p(p-1)}{2}y^{p-3} + \dots + p\,,$$

mis on Eisensteini teoreemi järgi taandumatu. Siis on aga ka $g(x)$ taandumatu, sest kui $g(x)$ oleks taanduv, siis oleks ka $g(y+1)$ kui y polünoom taanduv.

Sageli saab polünoomi $g(x)$ taandumatust täisarvude integriteetkonnas kindlaks teha, vaadeldes $g(x)$ kordajaid kui mingi jäägiklassikorpuse $R^{(p)}$ elemente. Kui $g(x)$ osutub taandumatuks jäägiklassikorpuses $R^{(p)}$, siis on ta taandumatu ka täisarvude vallas, sest iga võrdus, mis on kehtiv täisarvude vallas, jääb püsima ka jäägiklassikorpuses $R^{(p)}$.

Vaatleme näitena polünoomi

$$g(x) = x^5 + x^3 + 1 .$$

Ei ole raske näha, et $g(x)$ on taandumatu jäägiklassikorpuses $R^{(2)}$. Tõepoolest, $g(x)$ taanduvuse korral peaks üks tegureist olema lineaar- või ruutpolünoom. Kuid jäägiklassikorpuses $R^{(2)}$ on vaid kaks lineaarpolünoomi x ja $x + 1$ ning üks taandumatu ruutpolünoom $x^2 + x + 1$, kusjuures proovimise teel pole raske veenduda, et $g(x)$ ei jagu ühegagi neist polünoomidest. Seega on $g(x)$ taandumatu jäägiklassikorpuses $R^{(2)}$ ja järelikult ka täisarvude vallas.

Vaatleme teise näitena polünoomi

$$g(x) = x^4 - 3x^3 + x^2 - 1 ,$$

mis laguneb jäägiklassikorpuses $R^{(2)}$ taandumatute polünoomide korrutiseks

$$g(x) = (x + 1)(x^3 + x + 1).$$

Seega kui $g(x)$ osutub taanduvaks täisarvude vallas, siis võib ta polünoomide taandumatuteks teguriteks lahutuse ühesuse tõttu laguneda vaid ühe lineaar- ja ühe kuupteguri korrutiseks. Kuid, nagu näeme järgnevas artiklis, ei saa polünoomil $g(x)$ olla täisarvuliste kordajatega lineaartegurit, mistõttu $g(x)$ peab olema taandumatu täisarvude vallas.

3. Ratsionaallahendite leidmine. Kui polünoom omab lineaartegurit $ax + b$, kus a ja b on täisarvud, siis peab sellel polünoomil olema ratsionaallahend $\xi = -\frac{b}{a}$. On olemas lihtne võte, mis lubab leida kõik täisarvuliste kordajatega polünoomi

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n , \quad a_0 \neq 0$$

ratsionaallahendid.

Korrutades antud polünoomi teguriga a_0^{n-1} ja märkides siis $a_0 x = y$, saame normeeritud polünoomi

$$y^n + a_1 y^{n-1} + a_2 a_0 y^{n-2} + \ldots + a_{n-1} a_0^{n-2} y + a_n a_0^{n-1},$$

mille lahenditest saadakse antud polünoomi lahendid valemi $x = \frac{y}{a_0}$ abil. Seega võib iga täisarvuliste kordajatega polünoomi lahendite leidmist taandada täisarvuliste kordajatega n o r m e e r i t u d polünoomi lahendite leidmisele, missuguse polünoomi kohta tõestame järgmise teoreemi.

T e o r e e m 3. *Täisarvuliste kordajatega normeeritud polünoom*

$$g(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n$$

võib omada ratsionaallahenditena ainult täisarvulisi lahendeid, kusjuures viimased peavad olema vabaliikme a_n tegureiks.

Oletades tõestuseks, et $g(x)$ omab ratsionaallahendit $\xi = \frac{a}{b}$, kus $\frac{a}{b}$ $(b > 0)$ tähendab taandatud murdu, leiame

$$\frac{a^n}{b^n} + a_1 \frac{a^{n-1}}{b^{n-1}} + a_2 \frac{a^{n-2}}{b^{n-2}} + \ldots + a_{n-1} \frac{a}{b} + a_n = 0,$$

millest

$$\frac{a^n}{b} = -(a_1 a^{n-1} + a_2 a^{n-2} b + \ldots + a_{n-1} a b^{n-2} + a_n b^{n-1}).$$

Siit nähtub, et $\frac{a^n}{b}$ peab olema täisarv. Seega peab olema $b = 1$, nii et $\xi = a$ kujutab täisarvu. Siis on aga

$$a^n + a_1 a^{n-1} + a_2 a^{n-2} + \ldots + a_{n-1} a + a_n = 0,$$

kust

$$a_n = -(a^{n-1} + a_1 a^{n-2} + a_2 a^{n-3} + \ldots + a_{n-1}) a,$$

s. o. $\xi = a$ on tõesti vabaliikme a_n teguriks.

Niisiis, toetudes teoreemile 3, tarvitseb normeeritud polünoomi $g(x)$ täisarvuliste lahendite saamiseks vaid leida kõik vabaliikme a_n tegurid, nii positiivsed kui ka negatiivsed, ja siis proovida, missugused neist tegureist rahuldavad võrrandit

$g(x) = 0$. Nii on näiteks eelmise artikli lõpus vaadeldud polünoomi

$$g(x) = x^4 - 3x^3 + x^2 - 1$$

vabaliikme -1 tegureiks ainult 1 ja -1, kusjuures $g(1) \neq 0$, $g(-1) \neq 0$. Seega pole sel polünoomil ei täis- ega ratsionaalarvulisi lahendeid ja järelikult ka mitte täisarvuliste kordajatega lineaartegureid.

Juhul kui $g(x)$ vabaliikmel a_n on palju tegureid, osutub proovimine, kas need tegurid rahuldavad võrrandit $g(x) = 0$, praktiliselt liiga aegaviitvaks. Seepärast kasutatakse siin järgmist võtet, mis lubab kergesti ära tunda suure hulga a_n tegureid, mis ei rahulda võrrandit $g(x) = 0$. Nimelt kui ξ tähendab polünoomi $g(x)$ lahendit, siis võttes valemis

$$g(x) = (x - \xi)q(x)$$

$x = 1$ ja $x = -1$, leiame vastavalt

$$\frac{g(1)}{\xi - 1} = q(1), \quad \frac{g(-1)}{\xi + 1} = -q(-1),$$

kus $q(1)$ ja $q(-1)$ kui täisarvuliste kordajatega polünoomi $q(x)$ väärtused kujutavad täisarve. Seega võivad võrrandit $g(x) = 0$ rahuldada vaid need vabaliikme a_n tegurid ξ, mille puhul jagatised

$$\frac{g(1)}{\xi - 1}, \quad \frac{g(-1)}{\xi + 1}$$

osutuvad täisarvudeks. Juhul kui peaks olema $g(1) = 0$ või $g(-1) = 0$, siis jagame polünoomi $g(x)$ enne vastavalt teguriga $x - 1$ või $x + 1$ ja otsime edasi juba saadud jagatise täisarvulisi lahendeid.

N ä i d e 1. Leida polünoomi

$$2x^3 - 7x^2 + 10x - 6$$

ratsionaallahendid.

Korrutades antud polünoomi 4-ga ja märkides siis $2x = y$, saame normeeritud polünoomi

$$y^3 - 7y^2 + 20y - 24,$$

mille ratsionaallahendeiks võivad olla ainult vabaliikme —24 tegurid, s. o. täisarvud

$$\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 8,\ \pm 12,\ \pm 24.$$

Neist annab jagatistele

$$\frac{g(1)}{\xi-1}=\frac{-10}{\xi-1},\quad \frac{g(-1)}{\xi+1}=\frac{-52}{\xi+1}$$

täisarvulised väärtused ainult $\xi=3$. Rakendades Horneri skeemi, leiame

$$\begin{array}{r|rrr|r} & 1 & -7 & 20 & -24 \\ & & 3 & -12 & 24 \\ \hline 3 & 1 & -4 & 8 & 0, \end{array}$$

millest nähtub, et 3 kujutab normeeritud polünoomi lahendit. Antud polünoomi ainuke ratsionaallahend on seega $\frac{3}{2}$.

Ülejäänud lahendid saame, lahendades võrrandi

$$y^2-4y+8=0,$$

millest

$$y=2\pm\sqrt{-4}=2\pm 2i.$$

Niisiis on antud polünoomi lahenditeks $\frac{3}{2}$, $1+i$, $1-i$.

4. Polünoomi taanduvus integriteetkonnas. Laiendame nüüd eelmiste artiklite tulemusi täisarvude integriteetkonnalt ühele laiemale integriteetkondade klassile. Selgitame kõigepealt, mis tuleb mõista triviaalsete tegurite all mistahes integriteetkonnas I. Triviaalseiks tegureiks nimetame integriteetkonna I niisuguseid elemente ε, millega jagub selle integriteetkonna iga element. Seega võib integriteetkonna I iga elementi a lahutada tegureiks kujul

$$a=q\varepsilon,$$

kus üheks teguriks on triviaalne tegur ε ja mis kannab vastavalt triviaalse tegureiks lahutuse nime. Kui nullist erinev integriteetkonna element, mis ei ole triviaalne tegur, omab ainult triviaalseid tegureiks lahutusi, siis nimetame seda elementi a l g-

elemendiks, vastasel korral liitelemendiks. Nii on näiteks täisarvude integriteetkonnas triviaalseteks teguriteks 1 ja —1 ning algelementideks algarvud, seevastu polünoomide integriteetkonnas üle korpuse on triviaalseteks teguriteks nullist erinevad konstandid ning algelementideks taandumatud polünoomid.

Kui integriteetkonnas I iga nullist erinev element a, välja arvatud triviaalsed tegurid, laguneb algelementide korrutiseks

$$a = p_1 p_2 \dots p_k,$$

kus $p_1, p_2, \dots, p_k$ on kuni triviaalsete teguriteni üheselt määratud, siis öeldakse, et integriteetkonnas I kehtib algtegureiks lahutamise lause. Ei tule arvata, et igas integriteetkonnas peab kehtima algtegureiks lahutamise lause. Nii näiteks pole integriteetkonnas

$$\{a + ib\sqrt{3}\},$$

kus a ja b tähendavad täisarve, kehtiv algtegureiks lahutamise lause, sest siin omab näiteks arv 4 kahte isesugust, mitte triviaalsete tegurite 1 või —1 poolest erinevat algtegureiks lahutust:

$$4 = 2 \cdot 2, \quad 4 = (1 + i\sqrt{3})(1 - i\sqrt{3}).$$

Viimasest võrdusest nähtub ühtlasi, et vaadeldavas integriteetkonnas jagub korrutis $(1 + i\sqrt{3})(1 - i\sqrt{3})$ algelemendiga 2, tegurid $1 + i\sqrt{3}$ ja $1 - i\sqrt{3}$ aga kumbki mitte. Näitame, et *kui integriteetkonnas I, milles on kehtiv algtegureiks lahutamise lause, jagub korrutis algelemendiga, siis peab vähemalt üks tegur jaguma selle algelemendiga.* Tõepoolest, kui korrutis ab jagub algelemendiga p, s. o.

$$ab = pq,$$

kus q on mingi I element, ja kui seejuures a ega b ei jaguks p-ga, siis, lahutades viimases võrduses a, b ja q algtegurite korrutiseks, saaksime vastuolus algtegureiks lahutamise lausega I elemendi ab jaoks kaks isesugust algtegureiks lahutust, millest üks ei sisalda algelementi p, teine aga sisaldab.

Toetudes viimasele tõsiasjale, ei paku olulist raskust laiendada teoreeme 1—3 (art. 1—3) mistahes integriteetkonnale, milles on kehtiv algtegureiks lahutamise lause, mistõttu piirdume siin vaid vastavate tulemuste sõnastustega.

Teoreem 4. *Kui integriteetkonnas I on kehtiv algtegureiks lahutamise lause, siis on ka polünoomkonnas $I[x]$ kehtiv algtegureiks lahutamise lause.*

Teoreem 5. *Kui polünoomis*

$$g(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

üle integriteetkonna I, milles on kehtiv algtegureiks lahutamise lause, kõik kordajad peale pealiikme kordaja a_0 jaguvad mingi algelemendiga p, seejuures aga vabaliige a_n ei jagu p^2-ga, siis on $g(x)$ taandumatu integriteetkonnas I.

Teoreem 6. *Normeeritud polünoom*

$$g(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$$

üle integriteetkonna I, milles on kehtiv algtegureiks lahutamise lause, võib omada ratsionaallahenditena ainult täisratsionaalseid lahendeid[1], *kusjuures viimased peavad olema vabaliikme a_n tegureiks.*

Teoreemidest 4—6 nähtub, kuivõrd tähtsat osa etendavad algebras integriteetkonnad, kus kehtib algtegureiks lahutamise lause. Ühe niisuguse integriteetkondade klassiga — nn. peaideaaliringidega — tutvume hiljem (§ 24, art. 3). Järgnevas aga asume vaatlema teisi integriteetkondi, kus kehtib algtegureiks lahutamise lause — mitme muutuja polünoomkondi.

§ 9. Sümmeetrilised polünoomid.

1. Mitme muutuja polünoomid. Olgu K mingi põhikorpus. Siis polünoomkond $K[x]$ kujutab integriteetkonda, milles on kehtiv algtegureiks lahutamise lause (§ 4, art. 3). Teoreemi 4 järgi

[1] Täisratsionaalse ja ratsionaalse lahendi all mõistame siin vastavalt integriteetkonda I või tema jagatistekorpusse kuuluvat lahendit.

(§ 8, art. 4) kehtib algtegureiks lahutamise lause siis ka kahe muutuja polünoomkonnas $K[x, y] = K[x][y]$, edasi ka kolme muutuja polünoomkonnas $K[x, y, z] = K[x, y][z]$ jne. Rakendades täieliku induktsiooni printsiipi, veendume, et algtegureiks lahutamise lause on üldiselt kehtiv n muutuja polünoomkonnas $K[x_1, x_2, \ldots, x_n]$, s. o. iga polünoomi

$$f(x_1, x_2, \ldots, x_n) = \sum a_{k_1 k_2 \ldots k_n} x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$$

puhul, mille kordajad $a_{k_1 k_2 \ldots k_n}$ kuuluvad korpusse K (I, § 10, art. 2).

Et mitme muutuja polünoomis võib esineda terve hulk ühe ja sama astmega liikmeid, siis pole siin võimalik liikmete järjestamine ainult nende astmete järgi. Seepärast kasutatakse mitme muutuja polünoomi liikmete järjestamisel sama printsiipi, mille järgi korraldatakse sõnad sõnastikus. Peame nimelt polünoomi $f(x_1, x_2, \ldots, x_n)$ kahest liikmest

$$ax_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} \quad \text{ja} \quad ax_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

seda liiget k õ r g e m a k s, milles x_1 astendaja on suurem; kui aga x_1 astendajad on mõlemas liikmes võrdsed, s. o. $a_1 = \alpha_1$, siis peame seda liiget kõrgemaks, kus x_2 astendaja on suurem; kui aga ka x_2 astendajad on mõlemas liikmes võrdsed, s. o. $a_2 = \alpha_2$, siis peame seda liiget kõrgemaks, kus x_3 astendaja on suurem jne. Seega on liige $ax_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ kõrgem võrreldes liikmega $ax_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ siis ja ainult siis, kui leidub niisugune naturaalarv i, et

$$a_1 = \alpha_1, \quad a_2 = \alpha_2, \quad \ldots, \quad a_{i-1} = \alpha_{i-1}, \quad a_i > \alpha_i.$$

Niisugust polünoomi liikmete järjestust, kus iga liige on eespool antud mõttes kõrgem järgnevast liikmest, nimetatakse l e k s i k o g r a a f i l i s e k s j ä r j e s t u s e k s. Liiget, mis tuleb leksikograafilise järjestuse puhul esikohale, nimetatakse polünoomi k õ r g e i m a k s l i i k m e k s. Arusaadav, et kõrgeim liige on olemas igal nullist erineval polünoomil. Järjestades näiteks polünoomi

$$f(x_1, x_2, x_3) = 2x_1^2x_2x_3 - 3x_1x_2^3 + \\ + x_1^3x_2^2 - 4x_1^4x_3 + 2x_1x_3^2$$

liikmed leksikograafiliselt, saame

$$f(x_1, x_2, x_3) = -4x_1^4x_3 + x_1^3x_2^2 + \\ + 2x_1^2x_2x_3 - 3x_1x_2^3 + 2x_1x_3^2,$$

kus $-4x_1^4x_3$ kujutab kõrgeimat liiget.

Näitame, et *polünoomide korrutise kõrgeim liige on võrdne tegurite kõrgeimate liikmete korrutisega.* Olgu nimelt $ax_1^{a_1}x_2^{a_2}\dots x_n^{a_n}$ polünoomi $f(x_1, x_2, \dots, x_n)$ kõrgeim liige, $ax_1^{a_1}x_2^{a_2}\dots x_n^{a_n}$ mingi muu liige ja $bx_1^{b_1}x_2^{b_2}\dots x_n^{b_n}$ polünoomi $g(x_1, x_2, \dots, x_n)$ kõrgeim liige ning $\beta x_1^{\beta_1}x_2^{\beta_2}\dots x_n^{\beta_n}$ mingi muu liige; siis leiduvad naturaalarvud i ja k, nii et

$$(3) \qquad \begin{array}{llll} a_1 = \alpha_1, & a_2 = \alpha_2, & \dots, & a_{i-1} = \alpha_{i-1}, \quad a_i > \alpha_i \\ b_1 = \beta_1, & b_2 = \beta_2, & \dots, & b_{k-1} = \beta_{k-1}, \quad b_k > \beta_k. \end{array}$$

Et kahe polünoomi korrutamisel tuleb ühe polünoomi iga liige korrutada teise polünoomi iga liikmega, siis koosneb korrutis fg peale f ja g kõrgeimate liikmete korrutamisel saadud liikme

$$(4) \qquad abx_1^{a_1+b_1}x_2^{a_2+b_2}\dots x_n^{a_n+b_n}$$

veel järgmist tüüpi liikmeist:

$$a\beta x_1^{a_1}x_2^{a_2+\beta_1}\dots x_n^{a_n+\beta_n}, \quad abx_1^{\alpha_1+b_1}x_2^{\alpha_2+b_2}\dots x_n^{\alpha_n+b_n},$$
$$a\beta x_1^{\alpha_1+\beta_1}x_2^{\alpha_2+\beta_2}\dots x_n^{\alpha_n+\beta_n}.$$

Silmas pidades seoseid (3) ei ole raske veenduda, et liige (4) on leksikograafilise järjestuse mõttes kõrgem võrreldes kolme viimase liikmega, kujutades seega tõesti kõrgeimat liiget korrutises fg.

Olgu nüüd polünoomi $f(x_1, x_2, \dots, x_n)$ aste m ja $g(x_1, x_2, \dots, x_n)$ aste l. Tähendagu $ax_1^{a_1}x_2^{a_2}\dots x_n^{a_n}$ kõrgeimat liiget f nende liikmete seas, mille aste on m ja $bx_1^{b_1}x_2^{b_2}\dots x_n^{b_n}$ kõrgeimat liiget g nende liikmete seas, mille

aste on l. Korrutades iga m-astme liikme polünoomis f iga l-astme liikmega polünoomis g, saame korrutise fg suurima astmega liikmed — $(m+l)$-astme liikmed, kusjuures nende kordajad ei või olla kõik nullid, sest näiteks nende kõrgeima liikme

$$abx_1^{a_1+b_1}x_2^{a_2+b_2}\ldots x_n^{a_n+b_n}$$

kordaja $ab \neq 0$, kuna $a \neq 0$, $b \neq 0$. Tähendab, ka mitme muutuja polünoomide puhul kehtib lause: *polünoomide korrutise aste on võrdne tegurite astmete summaga.*

Vaatleme leitud tulemuste rakendusena Vandermonde determinanti (I, § 13, art. 3)

$$V_n = \begin{vmatrix} 1 & 1 & \ldots & 1 & \ldots & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_k & \ldots & x_i & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_k^2 & \ldots & x_i^2 & \ldots & x_n^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_k^{n-1} & \ldots & x_i^{n-1} & \ldots & x_n^{n-1} \end{vmatrix}.$$

See determinant kujutab n muutuja x_1, x_2, ..., x_n polünoomi. Et determinandi iga liige sisaldab parajasti ühte elementi igast reast, siis kujutab V_n homogeenset polünoomi astmega

$$1+2+3+\ldots+(n-1) = \frac{n(n-1)}{2}.$$

Lahutades determinandi V_n i-ndast veerust k-nda veeru, näeme, et i-nda veeru elementidel tekib ühistegur $x_i - x_k$, mis on ühtlasi ka V_n teguriks. Niisuguseid tegureid $x_i - x_k$ saame üldse $\binom{n}{2} = \frac{n(n-1)}{2}$ tükki. Et V_n aste on parajasti $\frac{n(n-1)}{2}$, siis omab V_n algtegureiks lahutamise ühesuse tõttu kuju

$$\begin{aligned} V_n = c(x_2-x_1)(x_3-x_1)(x_4-x_1)\ldots(x_n-x_1) \\ (x_3-x_2)(x_4-x_2)\ldots(x_n-x_2) \\ (x_4-x_3)\ldots(x_n-x_3) \\ \ldots\ldots\ldots \\ (x_n-x_{n-1}), \end{aligned}$$

kus c tähendab konstanti. Selle konstandi leidmiseks vaatleme determinandi V_n pealiiget $x_2x_3^2 \dots x_n^{n-1}$. Sama liige esineb korrutises V_n kordajaga c, mistõttu peab olema $c=1$ ja seega

$$V_n = \prod_{i>k} (x_i - x_k),$$

kooskõlas varem leitud tulemusega.

Olgu antud n muutuja polünoom

$$f(x_1, x_2, \dots, x_n) = \sum a_{k_1k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}.$$

Asendades siin muutujad $x_1, x_2, \dots, x_n$ vastavalt polünoomidega $g_1(x), g_2(x), \dots, g_n(x)$, saame ühe muutuja polünoomi

$$f(g_1, g_2, \dots, g_n) = \sum a_{k_1k_2 \dots k_n} g_1^{k_1}(x) g_2^{k_2}(x) \dots g_n^{k_n}(x),$$

mille tuletis avaldub valemi (§ 7, art. 2)

$$\frac{d}{dx} f^n(x) = n f^{n-1}(x) \frac{df(x)}{dx}$$

tõttu kujul

$$\frac{d}{dx} f(g_1, g_2, \dots, g_n) =$$

$$= \sum a_{k_1k_2 \dots k_n} \left(k_1 g_1^{k_1-1} g_2^{k_2} \dots g_n^{k_n} \frac{dg_1}{dx} + k_2 g_1^{k_1} g_2^{k_2-1} \dots g_n^{k_n} \frac{dg_2}{dx} + \right.$$

$$\left. + \dots + k_n g_1^{k_1} g_2^{k_2} \dots g_n^{k_n-1} \frac{dg_n}{dx} \right) = f'_{x_1}(g_1, g_2, \dots, g_n) \frac{dg_1}{dx} +$$

$$+ f'_{x_2}(g_1, g_2, \dots, g_n) \frac{dg_2}{dx} + \dots + f'_{x_n}(g_1, g_2, \dots, g_n) \frac{dg_n}{dx}$$

ehk lühidalt

$$(5) \quad \frac{d}{dx} f(g_1, g_2, \dots, g_n) = \sum_{i=1}^{n} f'_{x_i}(g_1, g_2, \dots, g_n) \frac{dg_i}{dx},$$

kus

$$f'_{x_i}(x_1, x_2, \dots, x_n) = \sum k_i a_{k_1k_2 \dots k_n} x_1^{k_1} x_2^{k_2} \dots x_i^{k_i-1} \dots x_n^{k_n}$$

on polünoomi $f(x_1, x_2, \dots, x_n)$ osatuletis x_i järgi. Valem (5) väljendab nn. diferentseerimise ahelreeglit.

Diferentseerimise ahelreegli rakendusena vaatleme m-astme homogeenset polünoomi $f(x_1, x_2, \ldots, x_n)$. Niisuguse polünoomi puhul kehtib valem (I, § 10, art. 2)

$$f(\lambda x_1, \lambda x_2, \ldots, \lambda x_n) = \lambda^m f(x_1, x_2, \ldots, x_n).$$

Vaadeldes λ-t muutujana, arvutame viimase võrduse mõlemast poolest tuletise λ järgi:

$$\sum_{i=1}^{n} f'_{x_i}(\lambda x_1, \lambda x_2, \ldots, \lambda x_n) x_i = m\lambda^{m-1} f(x_1, x_2, \ldots, x_n).$$

Võttes siin $\lambda = 1$, saame Euler'i valemi

$$\sum_{i=1}^{n} f'_{x_i}(x_1, x_2, \ldots, x_n) x_i = m f(x_1, x_2, \ldots, x_n).$$

2. **Sümmeetriliste polünoomide põhilause.** Algebras leiavad laialdast rakendust erilised mitme muutuja polünoomid, mis ei muutu, kui muutujad ümber järjestada. Niisugust polünoomi $\varphi(x_1, x_2, \ldots, x_n)$, mis ei muutu muutujate $x_1, x_2, \ldots, x_n$ permuteerimisel, nimetatakse sümmeetriliseks polünoomiks. Sümmeetrilise polünoomi puhul on seega

$$\varphi(x_{\alpha_1}, x_{\alpha_2}, \ldots, x_{\alpha_n}) = \varphi(x_1, x_2, \ldots, x_n),$$

kus $\alpha_1, \alpha_2, \ldots, \alpha_n$ tähendavad indekseid $1, 2, \ldots, n$ mistahes järjekorras. Sümmeetriline polünoom on näiteks polünoom

$$x_1^2 + x_2^2 + \ldots + x_n^2.$$

On ilmne, et kahe sümmeetrilise polünoomi summa, korrutis ja vahe kujutavad ka sümmeetrilisi polünoome ehk, teiste sõnadega: sümmeetriliste polünoomide hulk on kinnine liitmise, korrutamise ja lahutamise suhtes. Kõik sümmeetrilised polünoomid, mille kordajad kuuluvad antud põhikorpusse K, moodustavad seega integriteetkonna.

Sümmeetriliste polünoomide seas etendavad tähelepandavat osa põlünoomid

$$
\begin{aligned}
&\sigma_1 = x_1 + x_2 + \ldots + x_n \\
&\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n \\
&\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n \\
&\qquad\qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&\sigma_n = x_1x_2 \ldots x_n ,
\end{aligned} \tag{6}
$$

mis kannavad sümmeetriliste põhipolünoomide nime. Siin σ_k sisaldab kõiki k-kaupa võetud korrutisi muutujatest $x_1, x_2, \ldots, x_n$, omades seega $\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!}$ liiget. Sümmeetriliste põhipolünoomide tähtsus seisneb selles, et iga sümmeetrilist polünoomi võib avaldada täisratsionaalselt, s. o. kolme esimese põhitehte abil sümmeetriliste põhipolünoomide kaudu. Nimelt on kehtiv järgmine lause, mis on tuntud sümmeetriliste polünoomide põhilause nime all.

Teoreem 7. *Iga sümmeetriline polünoom* $\varphi(x_1, x_2, \ldots, x_n)$ *avaldub põhikorpuses* K *täisratsionaalselt sümmeetriliste põhipolünoomide* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *kaudu, s. o.*

$$\varphi(x_1, x_2, \ldots, x_n) = F(\sigma_1, \sigma_2, \ldots, \sigma_n),$$

kus F *tähendab teatavat polünoomi üle* K.

Tõestuseks vaatleme $\varphi(x_1, x_2, \ldots, x_n)$ kõrgeimat liiget

$$ax_1^{a_1}x_2^{a_2}\ldots x_i^{a_i}x_{i+1}^{a_{i+1}}\ldots x_n^{a_n}. \tag{7}$$

Ei ole raske näha, et siin peavad astendajad $a_1, a_2, \ldots, a_n$ kulgema mittekasvavalt:

$$a_1 \geqslant a_2 \geqslant \ldots \geqslant a_i \geqslant a_{i+1} \geqslant \ldots \geqslant a_n .$$

Tõepoolest, kui oleks näiteks $a_i < a_{i+1}$, siis, paigutades kõrgeimas liikmes (7) x_i ja x_{i+1} ümber, saaksime liikme

$$ax_1^{a_1}x_2^{a_2}\ldots x_i^{a_{i+1}}x_{i+1}^{a_i}\ldots x_n^{a_n},$$

mis φ sümmeetria tõttu peab kujutama ka φ liiget. Kuid viimane liige on kõrgem võrreldes liikmega (7), sest mõlemas liikmes langevad $x_1, x_2, \ldots, x_{i-1}$ astendajad ühte, ent x_i asten-

daja on viimases liikmes suurem kui liikmes (7). Seega sisaldab oletus $a_i < a_{i+1}$ vastuolu.

Moodustame nüüd avaldise

$$F_1 = a\sigma_1^{a_1-a_2}\sigma_2^{a_2-a_3}\ldots\sigma_{n-1}^{a_{n-1}-a_n}\sigma_n^{a_n}, \tag{8}$$

mis kujutab $a_i \geqslant a_{i+1}$ tõttu muutujate x_1, x_2, ..., x_n suhtes polünoomi ja nimelt sümmeetrilist polünoomi, sest põhipolünoomid σ_1, σ_2, ..., σ_{n-1}, σ_n on sümmeetrilised. Et ühelt poolt polünoomide korrutise kõrgeim liige on võrdne tegurite kõrgeimate liikmete korrutisega (art. 1) ja teiselt poolt põhipolünoomide σ_1, σ_2, ..., σ_{n-1}, σ_n kõrgeimad liikmed on vastavalt x_1, x_1x_2, ..., $x_1x_2\ldots x_{n-1}$, $x_1x_2\ldots x_n$, siis avaldub F_1 kõrgeim liige kujul

$$ax_1^{a_1-a_2}(x_1x_2)^{a_2-a_3}\ldots(x_1x_2\ldots x_{n-1})^{a_{n-1}-a_n}(x_1x_2\ldots x_n)^{a_n} =$$
$$= ax_1^{a_1}x_2^{a_2}\ldots x_n^{a_n},$$

langedes ühte φ kõrgeima liikmega (7). Seetõttu on vahe

$$\varphi_1 = \varphi - F_1$$

kõrgeim liige madalam võrreldes φ kõrgeima liikmega.

Rakendame nüüd polünoomile φ_1, mis on ka sümmeetriline x_1, x_2, ..., x_n suhtes, samasugust kõrgeima liikme alandamise võtet nagu polünoomile φ. Olgu nimelt φ_1 kõrgeim liige

$$bx_1^{b_1}x_2^{b_2}\ldots x_n^{b_n}.$$

Lahutades φ_1-st avaldise

$$F_2 = b\sigma_1^{b_1-b_2}\sigma_2^{b_2-b_3}\ldots\sigma_{n-1}^{b_{n-1}-b_n}\sigma_n^{b_n}, \tag{9}$$

saame sümmeetrilise polünoomi

$$\varphi_2 = \varphi - F_1 - F_2,$$

mille kõrgeim liige on madalam kui φ_1 kõrgeim liige. Edasi rakendame polünoomile φ_2 kõrgeima liikme alandamise võtet jne. Et antud liikmest leksikograafilise järjestuse mõttes madala-

maid liikmeid on lõplik hulk, siis pole võimalik kõrgeima liikme alandamise võtet lõpmatuseni jätkata, vaid teatava k sammu järel peab saabuma moment, kus lahutamise tulemus osutub nulliks, s. o.

$$\varphi - F_1 - F_2 - \ldots - F_k = 0 ,$$

millest

$$\varphi = F_1 + F_2 + \ldots + F_k .$$

Et siin F_1, F_2, ..., F_k kujutavad sümmeetriliste põhipolünoomide σ_1, σ_2, ..., σ_n astmete korrutisi, siis on seega φ avaldatud täisratsionaalselt sümmeetriliste põhipolünoomide kaudu, millega on teoreem 7 tõestatud.

Esitatud tõestuskäik näitab ühtlasi kätte tee, mida võib lihtsamatel juhtudel kasutada sümmeetriliste polünoomide avaldamiseks sümmeetriliste põhipolünoomide kaudu ehk, nagu lühidalt öeldakse, sümmeetriliste polünoomide arvutamiseks. Vaatleme öeldu selgituseks sümmeetrilist polünoomi

$$\varphi(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3 + x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 .$$

Siin on kõrgeim liige x_1^3 ja seega

$$F_1 = \sigma_1^3 = (x_1 + x_2 + x_3)^3 = x_1^3 + x_2^3 + x_3^3 + 6x_1x_2x_3 + 3(x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2),$$

nii et

$$\varphi_1 = \varphi - F_1 = -2(x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2) - 6x_1x_2x_3 .$$

Polünoomi φ_1 kõrgeim liige on $-2x_1^2x_2$ ja seega

$$F_2 = -2\sigma_1\sigma_2 = -2(x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) = -2(x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2) - 6x_1x_2x_3 ,$$

mistõttu

$$\varphi_2 = \varphi_1 - F_2 = 0 .$$

Järelikult

$$\varphi = F_1 + F_2 = \sigma_1^3 - 2\sigma_1\sigma_2 .$$

Teeme sümmeetriliste polünoomide põhilause tõestusest kaks järeldust, mis lubavad lihtsustada sümmeetriliste polünoomide arvutamist. Olgu

$$\varphi(x_1, x_2, \ldots, x_n) = F(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Küsime, missugune on polünoomi $F(\sigma_1, \sigma_2, \ldots, \sigma_n)$ aste.

Kõigepealt on polünoomis $F = F_1 + F_2 + \ldots + F_k$ liikme F_1 aste (8) tõttu

$$(a_1 - a_2) + (a_2 - a_3) + \ldots + (a_{n-1} - a_n) + a_n = a_1 ,$$

mis on ühtlasi kõrgeim aste selles polünoomis, sest näiteks liikme F_2 aste on (9) tõttu

$$(b_1 - b_2) + (b_2 - b_3) + \ldots + (b_{n-1} - b_n) + b_n = b_1 ,$$

kusjuures $a_1 \geqslant b_1$, kuna $ax_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$ on kõrgem kui $bx_1^{b_1}x_2^{b_2}\ldots x_n^{b_n}$. Niisiis on $F(\sigma_1, \sigma_2, \ldots, \sigma_n)$ aste võrdne a_1-ga, s. o. $\varphi(x_1, x_2, \ldots, x_n)$ astmega x_1 suhtes. Et aga $\varphi(x_1, x_2, \ldots, x_n)$ on sümmeetriline polünoom, siis on tema aste iga üksiku muutuja suhtes üks ja sama. Tähendab, $F(\sigma_1, \sigma_2, \ldots, \sigma_n)$ *aste on võrdne* $\varphi(x_1, x_2, \ldots, x_n)$ *astmega ühe muutuja suhtes.*

Defineerime polünoomi $f(x_1, x_2, \ldots, x_n)$ kaalu mõiste analoogiliselt polünoomi astme mõistega. Kõigepealt nimetame polünoomi $f(x_1, x_2, \ldots, x_n)$ liikme $a_{k_1k_2\ldots k_n}x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}$ puhul avaldist $k_1 + 2k_2 + \ldots + nk_n$ liikme kaaluks. Suurim kaal, mis esineb nullist erinevate kordajatega liikmete puhul, määrab polünoomi kaalu. Kui polünoomis on kõik liikmed ühe ja sama kaaluga, siis kõneldakse isobaarsest polünoomist. Nii on näiteks polünoom

$$f(x_1, x_2, x_3) = 2x_1^2x_2x_3 - 3x_1x_2^3 + x_1^3x_2^2 - 4x_1^4x_3 + 2x_1x_3^2$$

isobaarne kaaluga 7.

Olgu $C\sigma_1^{k_1}\sigma_2^{k_2}\sigma_3^{k_3}\ldots\sigma_n^{k_n}$ mingisugune liige polünoomis $F(\sigma_1, \sigma_2, \ldots, \sigma_n)$. Selle liikme kaal on

$$k_1 + 2k_2 + 3k_3 + \ldots + nk_n . \tag{10}$$

Et ühelt poolt polünoomide korrutise aste on võrdne tegurite astmete summaga (art. 1) ja teiselt poolt sümmeetriliste põhipolünoomide $\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_n$ astmed on vastavalt $1, 2, 3, \ldots, n$, siis pole kaal (10) muud midagi kui liikme $C\sigma_1^{k_1}\sigma_2^{k_2}\sigma_3^{k_3}\ldots\sigma_n^{k_n}$ aste $x_1, x_2, \ldots, x_n$ suhtes. Tähendab, $F(\sigma_1, \sigma_2, \ldots, \sigma_n)$ *kaal on võrdne* $\varphi(x_1, x_2, \ldots, x_n)$ *astmega* $x_1, x_2 \ldots, x_n$ *suhtes.* Erijuhul, kui $\varphi(x_1, x_2, \ldots, x_n)$ on homogeenne astmega m, on $F(\sigma_1, \sigma_2, \ldots, \sigma_n)$ isobaarne kaaluga m.

Teades polünoomi $F(\sigma_1, \sigma_2, \ldots, \sigma_n)$ astet ja kaalu, on võimalik ette öelda, missugused liikmed tulevad $F(\sigma_1, \sigma_2, \ldots, \sigma_n)$ koosseisu. Nende liikmete kordajad leitakse siis määramata kordajate meetodiga.

N ä i d e 2. Avaldada sümmeetriline polünoom

$$\varphi(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3 + x_1^2x_2 + \\ + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2$$

sümmeetriliste põhipolünoomide kaudu.

Siin $F(\sigma_1, \sigma_2, \sigma_3)$ peab olema kolmanda astme isobaarne polünoom kaaluga 3, mistõttu ei ole raske näha, et $F(\sigma_1, \sigma_2, \sigma_3)$ peab omama kuju $\sigma_1^3 + A\sigma_1\sigma_2 + B\sigma_3$, s. o.

$$\varphi(x_1, x_2, x_3) = \sigma_1^3 + A\sigma_1\sigma_2 + B\sigma_3 .$$

Oleme võtnud σ_1^3 kordajaks 1, sest liige, mis sisaldab astet σ_1^3, on määratud $\varphi(x_1, x_2, x_3)$ kõrgeima liikmega x_1^3 ja omab sümmeetriliste polünoomide põhilause tõestuse järgi selle kõrgeima liikme kordajat. Kordajate A ja B leidmiseks anname ülemises võrduses muutujaile x_1, x_2, x_3 ükskord väärtused $1, 1, 0$, teinekord näiteks väärtused $1, 1, -2$. Et

$$\sigma_1 = x_1 + x_2 + x_3 , \quad \sigma_2 = x_1x_2 + x_1x_3 + x_2x_3 , \quad \sigma_3 = x_1x_2x_3 ,$$

siis on esimesel juhul $\sigma_1 = 2$, $\sigma_2 = 1$, $\sigma_3 = 0$ ja seega $\varphi(1, 1, 0) = 4$ tõttu

$$4 = 8 + 2A,$$

millest $A = -2$. Teisel juhul on $\sigma_1 = 0$, $\sigma_3 = -2$ ja seega $\varphi(1, 1, -2) = 0$ tõttu

$$0 = -2B,$$

millest $B = 0$. Järelikult

$$\varphi(x_1, x_2, x_3) = \sigma_1^3 - 2\sigma_1\sigma_2$$

kooskõlas varem leitud tulemusega.

3. Vieta valemid. Olgu

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$$

mingi normeeritud polünoom üle K ja $\xi_1, \xi_2, \xi_3, \ldots, \xi_n$ selle polünoomi lahendid, mis võivad kuuluda põhikorpusse K või mingisse ülemkorpusse. Siis on

$$f(x) = (x - \xi_1)(x - \xi_2)(x - \xi_3) \ldots (x - \xi_n).$$

Korrutades leiame

$$(x - \xi_1)(x - \xi_2) = x^2 - (\xi_1 + \xi_2)x + \xi_1\xi_2$$
$$(x - \xi_1)(x - \xi_2)(x - \xi_3) = x^3 - (\xi_1 + \xi_2 + \xi_3)x^2 + (\xi_1\xi_2 + \xi_1\xi_3 + \xi_2\xi_3)x - \xi_1\xi_2\xi_3$$

ja üldiselt

$$(x - \xi_1)(x - \xi_2)(x - \xi_3) \ldots (x - \xi_n) = x^n - (\xi_1 + \xi_2 + \ldots + \xi_n)x^{n-1} + (\xi_1\xi_2 + \xi_1\xi_3 + \ldots + \xi_{n-1}\xi_n)x^{n-2} - (\xi_1\xi_2\xi_3 + \xi_1\xi_2\xi_4 + \ldots + \xi_{n-2}\xi_{n-1}\xi_n)x^{n-3} + \ldots + (-1)^n\xi_1\xi_2 \ldots \xi_n,$$

nagu selles võib kergesti veenduda täieliku induktsiooni printsiipi rakendades. Märkides

$$\begin{aligned}
\sigma_1 &= \xi_1 + \xi_2 + \ldots + \xi_n \\
\sigma_2 &= \xi_1\xi_2 + \xi_1\xi_3 + \ldots + \xi_{n-1}\xi_n \\
\sigma_3 &= \xi_1\xi_2\xi_3 + \xi_1\xi_2\xi_4 + \ldots + \xi_{n-2}\xi_{n-1}\xi_n \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\sigma_n &= \xi_1\xi_2 \ldots \xi_n ,
\end{aligned}$$

võime kirjutada

$$\begin{aligned}
x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n = \\
= x^n - \sigma_1x^{n-1} + \sigma_2x^{n-2} - \sigma_3x^{n-3} + \ldots + (-1)^n\sigma_n ,
\end{aligned}$$

millest

$$a_1 = -\sigma_1 , \quad a_2 = \sigma_2 , \quad a_3 = -\sigma_3 , \ \ldots , \ a_n = (-1)^n\sigma_n ,$$

kus σ_1, σ_2, σ_3, ..., σ_n tähendavad sümmeetrilisi põhipolünoome lahenditest ξ_1, ξ_2, ..., ξ_n. Leitud valemid kannavad Vieta valemite nime. Vieta valemid väljendavad seoseid normeeritud polünoomi kordajate ja lahendite vahel, võimaldades koostada polünoomi etteantud lahenditega.

Näide 3. Moodustada neljanda astme polünoom $f(x)$, mis omaks jäägiklassikorpuses $R^{(7)}$ lahendeid 2, 6 ühekordsetena ja lahendit 3 kahekordsena.

Rakendades Vieta valemeid, leiame

$$\begin{aligned}
a_1 &= -\sigma_1 = -(2 + 6 + 3 + 3) = 0 \\
a_2 &= \sigma_2 = 2 \cdot 6 + 2 \cdot 3 + 2 \cdot 3 + 6 \cdot 3 + 6 \cdot 3 + 3 \cdot 3 = 6 \\
a_3 &= -\sigma_3 = -(2 \cdot 6 \cdot 3 + 2 \cdot 6 \cdot 3 + 2 \cdot 3 \cdot 3 + 6 \cdot 3 \cdot 3) = 3 \\
a_4 &= \sigma_4 = 2 \cdot 6 \cdot 3 \cdot 3 = 3 .
\end{aligned}$$

Seega omab otsitav polünoom kuju

$$f(x) = x^4 + 6x^2 + 3x + 3 .$$

Olgu nüüd $\varphi(\xi_1, \xi_2, \ldots, \xi_n)$ mingi normeeritud polünoomi $f(x)$ lahenditest ξ_1, ξ_2, ..., ξ_n moodustatud sümmeetriline täisratsionaalne avaldis üle põhikorpuse K. Sümmeetriliste polü-

noomide põhilause järgi avaldub $\varphi(\xi_1, \xi_2, \ldots, \xi_n)$ täisratsionaalselt sümmeetriliste põhipolünoomide $\sigma_1, \sigma_2, \ldots, \sigma_n$ kaudu, s. o.

$$\varphi(\xi_1, \xi_2, \ldots, \xi_n) = F(\sigma_1, \sigma_2, \ldots, \sigma_n),$$

kust Vieta valemeid silmas pidades leiame

$$\varphi(\xi_1, \xi_2, \ldots, \xi_n) = F(-a_1, a_2, \ldots, (-1)^n a_n).$$

Tähendab, *iga sümmeetriline täisratsionaalne avaldis normeeritud polünoomi $f(x)$ lahenditest avaldub täisratsionaalselt selle polünoomi kordajate kaudu.* Seega on võimalik, tarvitsemata teada polünoomi $f(x)$ lahendeid ega ülemkorpust, kuhu need lahendid kuuluvad, arvutada iga sümmeetrilist täisratsionaalset avaldist neist lahenditest.

N ä i d e 4. Leida polünoomi

$$f(x) = x^4 - 3x^3 + 2x^2 + 4x - 3$$

lahendite kuupide summa.

Olgu $\xi_1, \xi_2, \xi_3, \xi_4$ polünoomi $f(x)$ lahendid. Nende lahendite kuupide summa kui sümmeetriline polünoom avaldub kujul

$$\xi_1^3 + \xi_2^3 + \xi_3^3 + \xi_4^3 = \sigma_1^3 + A\sigma_1\sigma_2 + B\sigma_3.$$

Näite 2 eeskujul leiame kergesti

$$A = -3, \quad B = 3,$$

nii et

$$\xi_1^3 + \xi_2^3 + \xi_3^3 + \xi_4^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3.$$

Nüüd on aga Vieta valemite järgi

$$\sigma_1 = -a_1 = 3, \quad \sigma_2 = a_2 = 2, \quad \sigma_3 = -a_3 = -4,$$

mistõttu

$$\xi_1^3 + \xi_2^3 + \xi_3^3 + \xi_4^3 = 27 - 18 - 12 = -3.$$

Sümmeetriliste polünoomide põhilause tõestamisel kasutatud võte sümmeetrilise polünoomi $\varphi(x_1, x_2, \ldots, x_n)$ avaldamiseks

sümmeetriliste põhipolünoomide kaudu tõi meid ühe kindla polünoomi $F(\sigma_1, \sigma_2, \ldots, \sigma_n)$ juurde. Toetudes Vieta valemitele, näitame, et polünoom $F(\sigma_1, \sigma_2, \ldots, \sigma_n)$ on üheselt määratud selles mõttes, et $\varphi(x_1, x_2, \ldots, x_n)$ avaldub vaid ühel viisil sümmeetriliste põhipolünoomide kaudu. Tõepoolest, kui oleks peale

$$\varphi(x_1, x_2, \ldots, x_n) = F(\sigma_1, \sigma_2, \ldots, \sigma_n)$$

veel

$$\varphi(x_1, x_2, \ldots, x_n) = G(\sigma_1, \sigma_2, \ldots, \sigma_n),$$

kus $F \not\equiv G$, siis kehtiks põhipolünoomide $\sigma_1, \sigma_2, \ldots, \sigma_n$ vahel seos

$$F(\sigma_1, \sigma_2, \ldots, \sigma_n) - G(\sigma_1, \sigma_2, \ldots, \sigma_n) = 0.$$

Seega leiduks väärtuste süsteeme, mida $\sigma_1, \sigma_2, \ldots, \sigma_n$ ei saaks omada, missuguseid väärtusi me muutujaile $x_1, x_2, \ldots, x_n$ ka ei annaks kas põhikorpuses K või mingis ülemkorpuses. Sest näiteks $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ väärtuste etteandmisel ei oleks viimase seose tõttu σ_n väärtus enam vabalt valitav [1]. Teiselt poolt võime aga vastavalt igale $\sigma_1, \sigma_2, \ldots, \sigma_n$ väärtuste kombinatsioonile koostada polünoomi

$$x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \ldots + (-1)^n \sigma_n,$$

mis omab kas põhikorpuses K või sobivalt konstrueeritud ülemkorpuses n lahendit $\xi_1, \xi_2, \ldots, \xi_n$, millele vastavad sümmeetriliste põhipolünoomide väärtused on Vieta valemite järgi just antud $\sigma_1, \sigma_2, \ldots, \sigma_n$ väärtused. Seega võivad $\sigma_1, \sigma_2, \ldots, \sigma_n$ kohase $x_1, x_2, \ldots, x_n$ valiku puhul omada mistahes etteantud väärtusi. Niisiis oletus, et $F(\sigma_1, \sigma_2, \ldots, \sigma_n)$ ei ole üheselt määratud, viib vastuolule.

4. Astmesummad. Rakendustes esinevad sageli sümmeetrilised polünoomid

$$s_\lambda = x_1^\lambda + x_2^\lambda + \ldots + x_n^\lambda,$$

[1] Siin on eeldatud, et σ_n tegelikult seoses $F - G = 0$ esineb.

mille liikmeteks on muutujate $x_1, x_2, \ldots, x_n$ ühed ja samad astmed ja mis kannavad vastavalt a s t m e s u m m a d e nime. Nagu kõik sümmeetrilised polünoomid, nii avalduvad ka astmesummad täisratsionaalselt sümmeetriliste põhipolünoomide kaudu. Et aga suurema λ puhul on astmesummade avaldamine sümmeetriliste põhipolünoomide kaudu artiklis 2 näidatud viisil väga aeganõudev, siis anname käesolevas artiklis valmis valemid, mis lubavad arvutada astmesummasid $s_1, s_2, s_3, \ldots$ samm-sammult üksteise järel.

Moodustame muutujate $x_1, x_2, \ldots, x_n$ abil x-i polünoomi

$$f(x) = (x - x_1)(x - x_2) \ldots (x - x_n) =$$
$$= x^n + a_1 x^{n-1} + a_2 x^{n-2} + a_3 x^{n-3} + \ldots + a_n .$$

Arvutades $f(x)$ kui korrutise tuletise, saame

$$f'(x) = (x - x_2)(x - x_3) \ldots (x - x_n) + (x - x_1)(x - x_3) \ldots$$
$$\ldots (x - x_n) + \ldots + (x - x_1)(x - x_2) \ldots (x - x_{n-1})$$

ehk

$$f'(x) = \frac{f(x)}{x - x_1} + \frac{f(x)}{x - x_2} + \ldots + \frac{f(x)}{x - x_n} = \sum_{k=1}^{n} \frac{f(x)}{x - x_k} .$$

Horneri võtet kasutades leiame (§ 5, art. 1)

$$\frac{f(x)}{x - x_k} = x^{n-1} + (x_k + a_1) x^{n-2} + (x_k^2 +$$
$$+ a_1 x_k + a_2) x^{n-3} + \ldots + (x_k^{n-1} + a_1 x_k^{n-2} + a_2 x_k^{n-3} + \ldots + a_{n-1}) .$$

Andes siin k-le väärtused $1, 2, \ldots, n$, saame tulemusi liites

$$f'(x) = n x^{n-1} + (s_1 + n a_1) x^{n-2} + (s_2 + a_1 s_1 + n a_2) x^{n-3} + \ldots +$$
$$+ (s_{n-1} + a_1 s_{n-2} + a_2 s_{n-3} + \ldots + n a_{n-1}) .$$

Teiselt poolt on

$$f'(x) = n x^{n-1} + (n - 1) a_1 x^{n-2} + (n - 2) a_2 x^{n-3} + \ldots + a_{n-1} .$$

Võrreldes x-i ühesuguste astmete kordajaid kahes viimases valemis, leiame

$$s_1 + n a_1 = (n - 1) a_1$$
$$s_2 + a_1 s_1 + n a_2 = (n - 2) a_2$$
$$\ldots \ldots \ldots \ldots \ldots \ldots$$
$$s_{n-1} + a_1 s_{n-2} + a_2 s_{n-3} + \ldots + n a_{n-1} = a_{n-1} ,$$

millest

$$(11)\qquad \begin{aligned} &s_1 + a_1 = 0\\ &s_2 + a_1 s_1 + 2a_2 = 0\\ &\dots\dots\dots\dots\\ &s_{n-1} + a_1 s_{n-2} + a_2 s_{n-3} + \dots + (n-1)a_{n-1} = 0\,. \end{aligned}$$

Valemeist (11) võime samm-sammult üksteise järel arvutada astmesummad s_1, s_2, s_3, ..., s_{n-1}. Nii saame näiteks nelja esimese astmesumma jaoks valemid

$$s_1 = -a_1\,,\quad s_2 = a_1^2 - 2a_2\,,\quad s_3 = -a_1^3 + 3a_1a_2 - 3a_3\,,$$
$$s_4 = a_1^4 - 4a_1^2a_2 + 4a_1a_3 + 2a_2^2 - 4a_4\,.$$

Et leida valemeid ka nende astmesummade s_λ arvutamiseks, kus $\lambda \geqslant n$, korrutame võrdust $f(x_k) = 0$ astmega x_k^λ. Sel teel saame võrduse

$$x_k^{\lambda+n} + a_1 x_k^{\lambda+n-1} + a_2 x_k^{\lambda+n-2} + \dots + a_n x_k^\lambda = 0\,.$$

Andes siin k-le väärtused 1, 2, ..., n, leiame tulemusi liites

$$s_{\lambda+n} + a_1 s_{\lambda+n-1} + a_2 s_{\lambda+n-2} + \dots + a_n s_\lambda = 0\,,$$

millest vastavalt λ väärtustele 0, 1, 2, ... saame

$$(12)\qquad \begin{aligned} &s_n + a_1 s_{n-1} + a_2 s_{n-2} + \dots + a_n s_0 = 0\\ &s_{n+1} + a_1 s_n + a_2 s_{n-1} + \dots + a_n s_1 = 0\\ &s_{n+2} + a_1 s_{n+1} + a_2 s_n + \dots + a_n s_2 = 0\\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots \end{aligned}$$

Olles arvutanud valemeist (11) s_1, s_2, s_3, ..., s_{n-1}, võime valemeist (12) üksteise järel edasi arvutada s_n, s_{n+1}, s_{n+2}, ... Siinjuures tuleb võtta $s_0 = n$. Valemid (11) ja (12) kannavad Newtoni valemite nime. Paneme tähele, et valemid (12) saadakse valemeist (11), kui viimaseid formaalselt jätkata, võttes $a_{n+1} = 0$, $a_{n+2} = 0$, ... Sellest nähtub, et kui meil on arvutatud astmesumma s_λ n muutuja jaoks, siis tuleb selle astmesumma leidmiseks $m < n$ muutuja jaoks varem saadud s_λ

avaldises võtta $a_{m+1} = 0$, $a_{m+2} = 0$, ..., $a_n = 0$. Kasutades Vieta valemeid

$$a_1 = -\sigma_1, \quad a_2 = \sigma_2, \quad a_3 = -\sigma_3, \quad \ldots, \quad a_n = (-1)^n \sigma_n,$$

võime avaldada Newtoni valemitega leitud astmesummad s_λ vahetult sümmeetriliste põhipolünoomide kaudu. Nii leiame näiteks

$$s_1 = \sigma_1, \quad s_2 = \sigma_1^2 - 2\sigma_2, \quad s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3,$$
$$s_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2 - 4\sigma_4.$$

§ 10. Resultant ja diskriminant.

1. Resultant. Olgu antud kaks normeeritud polünoomi

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$$
$$g(x) = x^m + b_1 x^{m-1} + \ldots + b_{m-1}x + b_m$$

üle põhikorpuse K. Küsime, missugusel tingimusel omavad need polünoomid ühist lahendit ξ, kas põhikorpuses K või teatavas ülemkorpuses. Et lahendi ξ olemasolu on samaväärne jaguvusega lineaarteguriga $x - \xi$, siis taandub $f(x)$ ja $g(x)$ ühiste lahendite küsimus suurima ühisteguri (f, g) leidmisele. Kui $f(x)$ ja $g(x)$ kordajad on konkreetselt antud, siis leitakse (f, g) kergesti Eukleidese algoritmi abil. Eukleidese algoritmi rakendamine teeb aga raskusi, kui $f(x)$ ja $g(x)$ kordajad on täheliselt antud. Seevastu sümmeetriliste polünoomide teooria annab kahe polünoomi ühiste lahendite küsimuse otsustamiseks igal juhul rakendatava meetodi.

Olgu $\xi_1, \xi_2, \ldots, \xi_n$ polünoomi $f(x)$ ja $\eta_1, \eta_2, \ldots, \eta_m$ polünoomi $g(x)$ lahendid. Korrutist

$$R(f, g) = g(\xi_1)g(\xi_2)\ldots g(\xi_n), \tag{13}$$

mille teguriteks on polünoomi g väärtused polünoomi f nullkohtadel, nimetatakse polünoomide f ja g r e s u l t a n d i k s.

On ilmne, et polünoomid $f(x)$ ja $g(x)$ omavad ühist lahendit siis ja ainult siis, kui $R(f, g) = 0$. Et $g(x) = (x - \eta_1)(x - \eta_2) \dots (x - \eta_m)$, siis on

$$(14) \qquad \begin{aligned} R(f, g) = {} & (\xi_1 - \eta_1)(\xi_1 - \eta_2) \dots (\xi_1 - \eta_m) \\ & (\xi_2 - \eta_1)(\xi_2 - \eta_2) \dots (\xi_2 - \eta_m) \\ & \dots\dots\dots\dots\dots\dots \\ & (\xi_n - \eta_1)(\xi_n - \eta_2) \dots (\xi_n - \eta_m) \end{aligned}$$

ehk lühidalt

$$R(f, g) = \prod_{i,k=1}^{n,m} (\xi_i - \eta_k).$$

Võttes valemis (14) tegurid kokku veergude viisi, leiame tegurites esinevaid vahesid ümber pöörates ja valemit $f(x) = (x - \xi_1)(x - \xi_2) \dots (x - \xi_n)$ silmas pidades:

$$(15) \qquad R(f, g) = (-1)^{nm} f(\eta_1) f(\eta_2) \dots f(\eta_m)$$

ehk

$$R(f, g) = (-1)^{nm} R(g, f),$$

mis ütleb, et polünoomide f ja g järjekorra vahetamisel korrutub resultant $R(f, g)$ teguriga $(-1)^{nm}$.

Valemist (13) nähtub, et $R(f, g)$ on $\xi_1, \xi_2, \dots, \xi_n$ suhtes sümmeetriline polünoom, kusjuures selle polünoomi kordajad avalduvad täisratsionaalselt $b_1, b_2, \dots, b_m$ kaudu. Et $\xi_1, \xi_2, \dots, \xi_n$ on polünoomi $f(x)$ lahendid, siis saab resultanti $R(f, g)$ esitada täisratsionaalse avaldisena $a_1, a_2, \dots, a_n$ suhtes (§ 9, art. 3), kusjuures selle avaldise kordajad avalduvad omakorda täisratsionaalselt $b_1, b_2, \dots, b_m$ kaudu. Seega kujutab $R(f, g)$ lõppeks täisratsionaalset avaldist kordajate $a_1, a_2, \dots, a_n$ ja $b_1, b_2, \dots, b_m$ suhtes, s. o.

$$R(f, g) = \sum C a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} b_1^{l_1} b_2^{l_2} \dots b_m^{l_m}.$$

Selle avaldise leidmiseks moodustame järgmise võrrandisüsteemi $m + n$ võrrandiga

$$
\begin{aligned}
x^{m-1}f(x) &= x^{n+m-1} + a_1x^{n+m-2} + \ldots + a_nx^{m-1} &&= 0\\
x^{m-2}f(x) &= x^{n+m-2} + a_1x^{n+m-3} + \ldots + a_nx^{m-2} &&= 0\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots &&= 0\\
f(x) &= x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n &&= 0\\
x^{n-1}g(x) &= x^{n+m-1} + b_1x^{n+m-2} + \ldots + b_mx^{n-1} &&= 0\\
x^{n-2}g(x) &= x^{n+m-2} + b_1x^{n+m-3} + \ldots + b_mx^{n-2} &&= 0\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots &&= 0\\
g(x) &= x^m + b_1x^{m-1} + b_2x^{m-2} + \ldots + b_{m-1}x + b_m &&= 0,
\end{aligned}
$$

kus tundmatuteks loeme astmed x^{n+m-1}, x^{n+m-2} $\ldots$, x, $x^0 = 1$. Kui polünoomidel f ja g on ühine lahend ξ, siis omab viimane võrrandisüsteem mittetriviaalset lahendit ξ^{n+m-1}, ξ^{n+m-2}, $\ldots$, ξ, $\xi^0 = 1$. Ent see võrrandisüsteem kui võrdse tundmatute ja võrrandite arvuga homogeenne lineaarne süsteem saab omada mittetriviaalseid lahendeid siis ja ainult siis, kui süsteemi determinant [1]

$$
\Delta = \begin{vmatrix}
1 & a_1 & a_2 & \ldots & a_n & 0 & 0 & \ldots & 0 \\
0 & 1 & a_1 & a_2 & \ldots & a_n & 0 & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & \ldots & 1 & a_1 & a_2 & a_3 & \ldots \; a_n \\
1 & b_1 & b_2 & \ldots & b_m & 0 & 0 & \ldots & 0 \\
0 & 1 & b_1 & b_2 & \ldots & b_m & 0 & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & \ldots & 1 & b_1 & b_2 & b_3 & \ldots \; b_m
\end{vmatrix}
\begin{matrix}
\left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ rida} \\
\\
\\
\\
\left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rida}
\end{matrix}
$$

on võrdne nulliga. Näitame, et Δ kujutabki polünoomide f ja g resultanti, s. o. et $\Delta = R(f, g)$.

Kõigepealt paneme tähele, et asendades determinandis Δ suurused a_1, a_2, $\ldots$, a_n ja b_1, b_2, $\ldots$, b_m Vieta valemite abil vastavalt lahendite ξ_1, ξ_2, $\ldots$, ξ_n ja η_1, η_2, $\ldots$, η_m kaudu, saame viimaste suhtes polünoomi

$$\Delta = \Delta(\xi_1, \xi_2, \ldots, \xi_n, \eta_1, \eta_2, \ldots, \eta_m).$$

Küsime, missugune on selle polünoomi aste. Selleks vaatleme

[1] Siin on lihtsuse mõttes võetud $m = n$.

determinandis Δ mingit nullist erinevat liiget, mis koosneb esimese rea α_1-st elemendist a_{α_1-1}, teise rea α_2-st elemendist a_{α_2-2} jne., lõppeks $(m+n)$-nda rea α_{m+n}-ndast elemendist $b_{\alpha_{m+n}-n}$, s. o. vaatleme liiget

$$(-1)^{\sigma} a_{\alpha_1-1} a_{\alpha_2-2} \dots a_{\alpha_m-m} b_{\alpha_{m+1}-1} b_{\alpha_{m+2}-2} \dots b_{\alpha_{m+n}-n},$$

kus σ tähendab inversioonide arvu indeksite $1, 2, \dots, m+n$ permutatsioonis $\alpha_1 \alpha_2 \dots \alpha_{m+n}$. Selle liikme aste $\xi_1, \xi_2, \dots, \xi_n, \eta_1, \eta_2, \dots, \eta_m$ suhtes on

$$(\alpha_1 - 1) + (\alpha_2 - 2) + \dots + (\alpha_m - m) + (\alpha_{m+1} - 1) + \\ + (\alpha_{m+2} - 2) + \dots + (\alpha_{m+n} - n) = (\alpha_1 + \alpha_2 + \dots + \alpha_{m+n}) - \\ - (1 + 2 + \dots + m) - (1 + 2 + \dots + n) = 1 + 2 + \dots + \\ + (m+n) - (1 + 2 + \dots + m) - (1 + 2 + \dots + n) =$$

$$= \frac{(m+n)(m+n+1)}{2} - \frac{m(m+1)}{2} - \frac{n(n+1)}{2} = \frac{m(m+1)}{2} + \\ + \frac{mn}{2} + \frac{n(n+1)}{2} + \frac{nm}{2} - \frac{m(m+1)}{2} - \frac{n(n+1)}{2} = nm,$$

ega sõltu seega vaadeldavast Δ liikmest. Niisiis on Δ suuruste $\xi_1, \xi_2, \dots, \xi_n, \eta_1, \eta_2, \dots, \eta_m$ suhtes homogeenne polünoom astmega nm.

Olgu nüüd ξ_i polünoomi $f(x)$ mingi lahend ja η_k polünoomi $g(x)$ mingi lahend. Siis on võrduse $\xi_i = \eta_k$ korral $\Delta = 0$. Vaadeldes determinanti $\Delta(\xi_1, \xi_2, \dots, \xi_n, \eta_1, \eta_2, \dots, \eta_m)$ ainult ξ_i polünoomina (võttes ülejäänud muutujad kordajatesse), võime seega konstateerida, et η_k on Δ kui ξ_i polünoomi lahendiks, mistõttu Δ peab jaguma lineaarteguriga $\xi_i - \eta_k$ $(i = 1, 2, \dots, n;$ $k = 1, 2, \dots, m)$ ja algtegureiks lahutamise ühesuse tõttu siis ka korrutisega

$$\prod_{i,k=1}^{n,m} (\xi_i - \eta_k),$$

s. o. resultandiga $R(f, g)$. Et aga Δ ja $R(f, g)$ on $\xi_1, \xi_2, \dots, \xi_n, \eta_1, \eta_2, \dots, \eta_m$ suhtes mõlemad nm-astme

polünoomid, siis võivad nad erineda vaid konstantse teguri c poolest, nii et $\Delta = cR(f, g)$.

Konstandi c leidmiseks peame silmas, et determinandi Δ pealiige $b_m{}^n$ esineb resultandis $R(f, g)$ kordajaga 1, nagu see nähtub valemist (13), kui arvestada, et $g(x) = x^m + b_1 x^{m-1} + \ldots + b_{m-1}x + b_m$. Seepärast peab olema $c = 1$ ja seega

$$\Delta = R(f, g).$$

Vaatleme lõppeks polünoome

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$$
$$g(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_{m-1}x + b_m,$$

mis ei tarvitse olla normeeritud. Et meil rakendustes tuleb käsitleda ka juhtu, kus kordajad a_k ja b_k on teiste muutujate polünoomid, siis võib viimaste muutujate teatavate väärtuste puhul eriti olla ka $a_0 = 0$, $b_0 = 0$, mistõttu vaatleme polünoomi f kui ülimalt n-astme ja g kui ülimalt m-astme polünoomi. Seljuhul mõistame polünoomide f ja g resultandi $R(f, g)$ all $(m+n)$-järku determinanti [1]

$$R(f, g) = \begin{vmatrix} a_0 & a_1 & a_2 & \ldots & a_n & 0 & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & a_2 & \ldots & a_n & 0 & \ldots & 0 \\ \multicolumn{9}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\ 0 & 0 & 0 & \ldots & a_0 & a_1 & a_2 & a_3 & \ldots & a_n \\ b_0 & b_1 & b_2 & \ldots & b_m & 0 & 0 & \ldots & 0 \\ 0 & b_0 & b_1 & b_2 & \ldots & b_m & 0 & \ldots & 0 \\ \multicolumn{9}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\ 0 & 0 & 0 & \ldots & b_0 & b_1 & b_2 & b_3 & \ldots & b_m \end{vmatrix} \begin{matrix} \\ \\ \\ \} m \text{ rida} \\ \\ \\ \\ \} n \text{ rida,} \\ \\ \end{matrix}$$

mis on tuntud Sylvester'i determinandi nime all. Juhul $a_0 = 1$, $b_0 = 1$, s. o. normeeritud polünoomide puhul taandub Sylvesteri determinant eespool vaadeldud determinandiks Δ, mistõttu siin antud resultandi mõiste kujutab normeeritud polünoomide jaoks defineeritud resultandi üldistust. Resul-

[1] Siin on lihtsuse mõttes võetud $m = n$.

tant $R(f, g)$ kujutab kordajate $a_0, a_1, a_2, \ldots, a_n, b_0, b_1, b_2, \ldots, b_m$ suhtes polünoomi

$$R(f, g) = \sum C a_0^{k_0} a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n} b_0^{l_0} b_1^{l_1} b_2^{l_2} \ldots b_m^{l_m},$$

mille kohta saab näidata, et ta on isobaarne kaaluga nm, s. o.

$$0 \cdot k_0 + k_1 + 2k_2 + \ldots + nk_n + \\ + 0 \cdot l_0 + l_1 + 2l_2 + \ldots + ml_m = nm,$$

ja homogeenne astmega m kordajate $a_0, a_1, a_2, \ldots, a_n$ suhtes ning astmega n kordajate $b_0, b_1, b_2, \ldots, b_m$ suhtes.

Tõepoolest, võttes resultandis $R(f, g)$ $a_0 = 1$, $b_0 = 1$, saame varem vaadeldud resultandi

$$\sum C a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n} b_1^{l_1} b_2^{l_2} \ldots b_m^{l_m},$$

mis on $\xi_1, \xi_2, \ldots, \xi_n, \eta_1, \eta_2, \ldots, \eta_m$ suhtes valemi (14) järgi homogeenne astmega nm. Et siin teiselt poolt Vieta valemite põhjal $a_1, a_2, \ldots, a_n$ astmed $\xi_1, \xi_2, \ldots, \xi_n$ suhtes on vastavalt $1, 2, \ldots, n$ ja $b_1, b_2, \ldots, b_m$ astmed $\eta_1, \eta_2, \ldots, \eta_m$ suhtes $1, 2, \ldots, m$, siis on liikme

$$C a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n} b_1^{l_1} b_2^{l_2} \ldots b_m^{l_m}$$

aste $\xi_1, \xi_2, \ldots, \xi_n, \eta_1, \eta_2, \ldots, \eta_m$ suhtes võrdne avaldisega

$$k_1 + 2k_2 + \ldots + nk_n + l_1 + 2l_2 + \ldots + ml_m.$$

Seega

$$k_1 + 2k_2 + \ldots + nk_n + l_1 + 2l_2 + \ldots + ml_m = nm,$$

millega on väide $R(f, g)$ isobaarsuse kohta tõestatud. Mis puutub väitesse $R(f, g)$ homogeensuse kohta, siis ilmneb see vahetult $R(f, g)$ definitsioonist determinandina.

Tuleb silmas pidada, et alati on $R(f, g) = 0$, kui $a_0 = 0$, $b_0 = 0$ (sest siis on Sylvesteri determinandi esimese veeru elemendid kõik nullid) sõltumata sellest, kas polünoomidel f ja g on ühiseid lahendeid või mitte. Näitame, et juhtum $a_0 = 0$,

$b_0 = 0$ on ainuke, kus resultandi nulliga võrdumine ei tarvitse endaga kaasa tuua ühiste lahendite olemasolu.

Tõepoolest, kõigepealt kui $a_0 \neq 0$, $b_0 \neq 0$, siis võime kirjutada

$$f(x) = a_0 \bar{f}(x), \quad g(x) = b_0 \bar{g}(x),$$

kus

$$\bar{f}(x) = x^n + \frac{a_1}{a_0} x^{n-1} + \ldots + \frac{a_{n-1}}{a_0} x + \frac{a_n}{a_0}$$

$$\bar{g}(x) = x^m + \frac{b_1}{b_0} x^{m-1} + \ldots + \frac{b_{m-1}}{b_0} x + \frac{b_m}{b_0}$$

on normeeritud polünoomid. Võttes Sylvesteri determinandi ette igast esimesest m reast teguri a_0 ja igast ülejäänud n reast teguri b_0, leiame

$$R(f, g) = a_0^m b_0^n R(\bar{f}, \bar{g}),$$

millest nähtub, et $R(f, g) = 0$ siis ja ainult siis, kui $R(\bar{f}, \bar{g}) = 0$. Et aga $\bar{f}$ ja $\bar{g}$ on normeeritud polünoomid, siis tähendab võrdus $R(\bar{f}, \bar{g}) = 0$ ühiste lahendite esinemist polünoomidel $\bar{f}$ ja $\bar{g}$ ehk, mis sama on, polünoomidel f ja g.

Kui aga näiteks $a_0 \neq 0$, $b_0 = 0$, siis olgu b_r esimene nullist erinev kordaja polünoomis $g(x)$, nii et

$$b_0 = 0, \quad b_1 = 0, \quad \ldots, \quad b_{r-1} = 0, \quad b_r \neq 0.$$

Märkides

$$\bar{g}(x) = b_r x^{m-r} + b_{r+1} x^{m-r-1} + \ldots + b_{m-1} x + b_m,$$

leiame Sylvesteri determinanti Laplace'i valemi põhjal esimese r veeru determinantide järgi arendades (I, § 14, art. 1)

$$R(f, g) = a_0^r R(f, \bar{g}).$$

Seega on $R(f, g) = 0$ siis ja ainult siis, kui $R(f, \bar{g}) = 0$, s. o. kui polünoomidel f ja $\bar{g}$ ehk, mis sama on, polünoomidel f ja g on ühiseid lahendeid.

Viimaseid tulemusi võime kokku võtta järgmiseks teoreemiks:

Teoreem 8. *Polünoomide*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$
$$g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m$$

resultant on võrdne nulliga siis ja ainult siis, kui neil polünoomidel on ühiseid lahendeid või kui $a_0 = 0$, $b_0 = 0$.

Näiteks polünoomide

$$f(x) = a_0x^2 + a_1x + a_2, \quad g(x) = b_0x^2 + b_1x + b_2$$

resultant on

$$R(f, g) = \begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & 0 \\ 0 & b_0 & b_1 & b_2 \end{vmatrix}.$$

Arendades viimast determinanti Laplace'i valemi põhjal esimese ja kolmanda rea determinantide järgi, leiame

$$R(f, g) = (a_0b_2 - a_2b_0)^2 - (a_0b_1 - a_1b_0)(a_1b_2 - a_2b_1).$$

Kui näiteks $f(x) = 2x^2 + 3x - 2$, $g(x) = 2x^2 - x - 3$, siis

$$R(f, g) = (-2)^2 - (-8)(-11) = -84,$$

millest nähtub, et vaadeldavad polünoomid ei oma ühiseid lahendeid. Kui aga viimaste polünoomide kordajad kuuluvad jäägiklassikorpusse $R^{(7)}$, siis on $R(f, g) = 0$ ja polünoomidel on ühine lahend, nimelt $\xi = 5$.

Vaatleme eriti veel juhtu, kus polünoomides f ja g kordajad a_0, b_0 ei ole nullid. Nagu nägime, on siis

$$R(f, g) = a_0^m b_0^n R(\bar{f}, \bar{g}),$$

kus polünoomid $\bar{f} = \frac{f}{a_0}$, $\bar{g} = \frac{g}{b_0}$ omavad samu lahendeid mis f ja g. Et $\bar{f}$ ja $\bar{g}$ on normeeritud, siis on (13) järgi

$$R(\bar{f}, \bar{g}) = \bar{g}(\xi_1)\bar{g}(\xi_2) \ldots \bar{g}(\xi_n)$$

või (15) järgi

$$R(\bar{f}, \bar{g}) = (-1)^{nm}\bar{f}(\eta_1)\bar{f}(\eta_2)\dots\bar{f}(\eta_m)$$

ja seega

$$(16)\qquad \begin{aligned} R(f, g) &= a_0^m g(\xi_1)g(\xi_2)\dots g(\xi_n)\\ R(f, g) &= (-1)^{nm}b_0^n f(\eta_1)f(\eta_2)\dots f(\eta_m). \end{aligned}$$

2. **Diskriminant.** Leiame polünoomi

$$f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$$

ja tema tuletise

$$f'(x) = nx^{n-1} + (n-1)a_1x^{n-2} + \dots + a_{n-1}$$

resultandi. Esimese valemi (16) järgi on $a_0 = 1$ tõttu

$$R(f, f') = f'(\xi_1)f'(\xi_2)\dots f'(\xi_n),$$

kus $\xi_1, \xi_2, \dots, \xi_n$ tähendavad $f(x)$ lahendeid. Et

$$f(x) = (x-\xi_1)(x-\xi_2)\dots(x-\xi_n),$$

siis

$$\begin{aligned} f'(x) = {} & (x-\xi_2)(x-\xi_3)\dots(x-\xi_n) +\\ & + (x-\xi_1)(x-\xi_3)\dots(x-\xi_n) + \dots +\\ & + (x-\xi_1)(x-\xi_2)\dots(x-\xi_{n-1}) \end{aligned}$$

ja seega

$$\begin{aligned} R(f, f') = {} & (\xi_1-\xi_2)(\xi_1-\xi_3)\dots(\xi_1-\xi_n)\\ & (\xi_2-\xi_1)(\xi_2-\xi_3)\dots(\xi_2-\xi_n)\\ & \dots\dots\dots\dots\dots\dots\dots\\ & (\xi_n-\xi_1)(\xi_n-\xi_2)\dots(\xi_n-\xi_{n-1}). \end{aligned}$$

Saadud korrutises esineb koos iga teguriga $\xi_i - \xi_k$ ka tegur $\xi_k - \xi_i$, missuguseid tegureid paarikaupa korrutisteks $-(\xi_i - \xi_k)^2$ kokku võttes võime kirjutada

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} \prod_{i>k} (\xi_i - \xi_k)^2,$$

kus viimane korrutis tuleb moodustada kõigist neist tegureist $(\xi_i - \xi_k)^2$, mille puhul $i > k$.

Korrutist $\prod\limits_{i>k} (\xi_i - \xi_k)^2$ nimetatakse polünoomi $f(x)$ diskriminandiks ja märgitakse sümboliga $D(f)$, s. o.

$$D(f) = \prod_{i>k} (\xi_i - \xi_k)^2.$$

Silmas pidades seost

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} D(f)$$

võib öelda, et diskriminant $D(f)$ on võrdne nulliga siis ja ainult siis, kui polünoomidel $f(x)$ ja $f'(x)$ on ühiseid lahendeid, s. o. kui polünoom $f(x)$ omab kordseid lahendeid (§ 7, art. 3).

Diskriminandi $D(f)$ arvutamiseks kasutame Vandermonde determinanti (§ 9, art. 1)

$$V_n = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ \xi_1 & \xi_2 & \xi_3 & \dots & \xi_n \\ \xi_1^2 & \xi_2^2 & \xi_3^2 & \dots & \xi_n^2 \\ \dots & \dots & \dots & \dots & \dots \\ \xi_1^{n-1} & \xi_2^{n-1} & \xi_3^{n-1} & \dots & \xi_n^{n-1} \end{vmatrix} = \prod_{i>k} (\xi_i - \xi_k).$$

Et $D(f) = V_n^2$, siis leiame Vandermonde determinandi ruutu arvutades, korrutades selleks read ridadega

$$D(f) = \begin{vmatrix} s_0 & s_1 & s_2 & \dots & s_{n-1} \\ s_1 & s_2 & s_3 & \dots & s_n \\ s_2 & s_3 & s_4 & \dots & s_{n+1} \\ \dots & \dots & \dots & \dots & \dots \\ s_{n-1} & s_n & s_{n+1} & \dots & s_{2n-2} \end{vmatrix},$$

kus suurused $s_\lambda = \xi_1^\lambda + \xi_2^\lambda + \dots + \xi_n^\lambda$ kujutavad astmesummasid, mis on arvutatavad Newtoni valemeist (§ 9, art. 4).

Näiteks kui $f(x) = x^3 + px + q$, siis on

$$D(f) = \begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix},$$

kus Newtoni valemite järgi

$$s_0 = 3, \quad s_1 = 0, \quad s_2 = -2p, \quad s_3 = -3q, \quad s_4 = 2p^2.$$

Seega

$$D(f) = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} = -12p^3 - 27q^2 + 8p^3 = -27q^2 - 4p^3.$$

Kui $f(x) = x^3 + x - 2$, siis

$$D(f) = -108 - 4 = -112,$$

millest nähtub, et vaadeldaval polünoomil ei ole kordseid lahendeid. Kui aga viimase polünoomi kordajad kuuluvad jäägiklassikorpusse $R^{(7)}$, siis on $D(f) = 0$ ja polünoomil on kordne lahend, nimelt $\xi = 3$.

3. Eliminatsiooniprobleem. Vaatleme kahe tundmatuga ja kahe võrrandiga süsteemi

$$f(x, y) = 0, \quad g(x, y) = 0$$

üle põhikorpuse K, kus f olgu n-astme ja g m-astme polünoom x, y suhtes. Korraldades polünoomid f ja g muutuja y kahanevate astmete järgi, saame

$$\begin{aligned} f(x, y) &= a_0(x)y^\nu + a_1(x)y^{\nu-1} + \ldots + a_{\nu-1}(x)y + a_\nu(x) \\ g(x, y) &= b_0(x)y^\mu + b_1(x)y^{\mu-1} + \ldots + b_{\mu-1}(x)y + b_\mu(x), \end{aligned} \tag{17}$$

kus $\nu \leqslant n$, $\mu \leqslant m$. Olgu $R(x)$ polünoomide (17) kui ühe muutuja y polünoomide resultant. Nagu nähtub resultandi avaldisest determinandina (art. 1), kujutab $R(x)$ muutuja x polünoomi, mille kordajad kuuluvad põhikorpusse K.

Omagu antud võrrandisüsteem kas põhikorpuses K või teatavas ülemkorpuses mingit lahendit ξ, η. Andes polünoomides (17) muutujale x väärtuse ξ, saame muutuja y polünoomid

$$f(\xi, y), \quad g(\xi, y), \tag{18}$$

millele η on ühiseks lahendiks. Seega peab polünoomide (18)

resultant, s. o. $R(\xi)$ võrduma nulliga ehk, teiste sõnadega, ξ peab olema võrrandi

$$R(x) = 0$$

lahend.

Seega võib vaadeldava võrrandisüsteemi esimese tundmatu väärtuseks ξ olla vaid võrrandi $R(x) = 0$ lahend, millega on kahe võrrandiga süsteemi lahendamine taandatud ühe võrrandi lahendamisele. Öeldakse, et võrrand $R(x) = 0$ on saadud süsteemist $f(x, y) = 0$, $g(x, y) = 0$ tundmatu y elimineerimisel.

Ümberpöördult, kui $R(x)$ omab lahendit ξ, siis on polünoomide (18) resultant null, mistõttu neil polünoomidel on teoreemi 8 põhjal (art. 1) vähemalt üks ühine lahend η, s. o.

$$f(\xi, \eta) = 0, \quad g(\xi, \eta) = 0,$$

või olgu siis, et $a_0(\xi) = 0$, $b_0(\xi) = 0$.

Niisiis tuleb antud võrrandisüsteemi lahendamiseks kõigepealt lahendada võrrand $R(x) = 0$. Olgu ξ mingi selle võrrandi lahend. Leiame polünoomide $f(\xi, y)$ ja $g(\xi, y)$ suurima ühisteguri $d(\xi, y)$. Olgu η võrrandi $d(\xi, y) = 0$ mingi lahend. Kui nüüd $a_0(\xi)$ ja $b_0(\xi)$ ei ole korraga nullid, siis kujutab ξ, η kindlasti antud võrrandisüsteemi lahendit. Seevastu kui $a_0(\xi) = 0$, $b_0(\xi) = 0$, siis tuleb proovimise teel otsustada, kas ξ, η rahuldab antud võrrandisüsteemi või mitte.

Näide 5. Lahendada võrrandisüsteem

$$\begin{aligned} x^2y - y^2 - x + 1 &= 0 \\ xy^2 - x^2y + y^2 - 1 &= 0. \end{aligned}$$

Siin

$$\begin{aligned} f(x, y) &= -y^2 + x^2y + (1 - x) \\ g(x, y) &= (x + 1)y^2 - x^2y - 1 \end{aligned}$$

ja seega

$$R(x) = \begin{vmatrix} -1 & x^2 & 1-x & 0 \\ 0 & -1 & x^2 & 1-x \\ x+1 & -x^2 & -1 & 0 \\ 0 & x+1 & -x^2 & -1 \end{vmatrix}.$$

Arvutades viimase determinandi, leiame

$$R(x) = x^4(1-x^2),$$

nii et võrrandil $R(x) = 0$ on kolm erinevat lahendit

$$\xi_1 = 0, \quad \xi_2 = 1, \quad \xi_3 = -1,$$

mis kõik kujutavad esimese tundmatu x väärtusi, sest $a_0(x) = -1 \neq 0$. Neile lahenditele vastavad polünoomide paarid

$$\begin{aligned} f(0, y) &= -y^2 + 1, & g(0, y) &= y^2 - 1 \\ f(1, y) &= -y^2 + y, & g(1, y) &= 2y^2 - y - 1 \\ f(-1, y) &= -y^2 + y + 2, & g(-1, y) &= -y - 1, \end{aligned}$$

mille suurimad ühistegurid on

$$d(0, y) = y^2 - 1, \quad d(1, y) = y - 1, \quad d(-1, y) = y + 1.$$

Seega on antud võrrandisüsteemil neli lahendit:

$$0, 1; \quad 0, -1; \quad 1, 1; \quad -1, -1.$$

Seame lõppeks endale küsimuse võrrandisüsteemi

$$f(x, y) = 0, \quad g(x, y) = 0$$

lahendite arvu kohta. Selleks tuleb uurida resultandi $R(x)$ astet ühelt poolt ja suurima ühisteguri $d(\xi, y)$ astet teiselt poolt. Silmas pidades, et $f(x, y)$ on n-astme ja $g(x, y)$ m-astme polünoom x, y suhtes, võib valemeis (17) kordaja $a_k(x)$ aste olla ülimalt $n - \nu + k$ ja $b_k(x)$ aste ülimalt $m - \mu + k$. Seega ei ületa resultandis $R(x)$ liikme

$$Ca_0^{k_0}a_1^{k_1}a_2^{k_2} \dots a_\nu^{k_\nu}b_0^{l_0}b_1^{l_1}b_2^{l_2} \dots b_\mu^{l_\mu}$$

aste x-i suhtes suurust

$$k_0(n-\nu)+k_1(n-\nu+1)+k_2(n-\nu+2)+\ldots+k_\nu n+$$
$$+l_0(m-\mu)+l_1(m-\mu+1)+l_2(m-\mu+2)+\ldots+l_\mu m=$$
$$=(k_0+k_1+k_2+\ldots+k_\nu)(n-\nu)+k_1+2k_2+\ldots+\nu k_\nu+$$
$$+(l_0+l_1+l_2+\ldots+l_\mu)(m-\mu)+l_1+2l_2+\ldots+\mu l_\mu=$$
$$=\mu(n-\nu)+\nu(m-\mu)+\nu\mu=\mu n+\nu m-\nu\mu=$$
$$=nm-(n-\nu)(m-\mu)\leqslant nm,$$

sest $\nu\leqslant n$, $\mu\leqslant m$. Siinjuures on arvestatud asjaolu, et resultant $R(x)$ on isobaarne kaaluga $\nu\mu$ ja homogeenne astmega μ kordajate $a_0, a_1, a_2, \ldots, a_\nu$ suhtes ning astmega ν kordajate $b_0, b_1, b_2, \ldots, b_\mu$ suhtes, s. o.

$$k_1+2k_2+\ldots+\nu k_\nu+l_1+2l_2+\ldots+\mu l_\mu=\nu\mu$$
$$k_0+k_1+k_2+\ldots+k_\nu=\mu,\quad l_0+l_1+l_2+\ldots+l_\mu=\nu.$$

Tähendab, resultandi $R(x)$ aste on ülimalt võrdne polünoomide f ja g astmete korrutisega nm.

Seega, kui $R(x)$ ei ole nullpolünoom, siis võib võrrandisüsteemis

$$f(x, y)=0,\quad g(x, y)=0$$

tundmatu x omada ülimalt nm väärtust, mis avalduvad võrrandi $R(x)=0$ lahenditena. Igale x-i väärtusele ξ vastavad y väärtused leiame siis võrrandist $d(\xi, y)=0$. Jääb selgitada, mitu y väärtust vastab ühele x-i väärtusele ξ, s. o. missugune on polünoomi $d(\xi, y)$ aste. Oletame konkreetsuse mõttes, et x-i väärtusele ξ vastab kaks y väärtust ehk, teiste sõnadega, et polünoomidel

$$f(\xi, y)=a_0(\xi)y^\nu+a_1(\xi)y^{\nu-1}+\ldots+a_{\nu-1}(\xi)y+a_\nu(\xi)$$
$$g(\xi, y)=b_0(\xi)y^\mu+b_1(\xi)y^{\mu-1}+\ldots+b_{\mu-1}(\xi)y+b_\mu(\xi)$$

on kaks ühist lahendit η_1 ja η_2. Näitame, et sel korral on peale $R(\xi)=0$ kehtivad veel tingimused

$$\frac{\partial R(\xi)}{\partial a_0}=0,\quad \frac{\partial R(\xi)}{\partial a_1}=0,\ \ldots,\quad \frac{\partial R(\xi)}{\partial a_\nu}=0,$$

$$\frac{\partial R(\xi)}{\partial b_0}=0,\quad \frac{\partial R(\xi)}{\partial b_1}=0,\ \ldots,\quad \frac{\partial R(\xi)}{\partial b_\mu}=0.$$

Tõepoolest, resultanti $R(\xi)$ võib valemi (16) põhjal (art. 1) esitada kujul

$$R(\xi)=a_0{}^\mu g(\xi,\eta_1)g(\xi,\eta_2)\ldots g(\xi,\eta_\nu)$$

või

$$R(\xi)=(-1)^{\nu\mu}b_0{}^\nu f(\xi,\zeta_1)f(\xi,\zeta_2)\ldots f(\xi,\zeta_\mu),$$

kus $\eta_1, \eta_2, \ldots, \eta_\nu$ tähendavad polünoomi $f(\xi, y)$ lahendeid ja $\zeta_1, \zeta_2, \ldots, \zeta_\mu$ polünoomi $g(\xi, y)$ lahendeid. Silmas pidades et $\frac{\partial f(\xi,y)}{\partial a_k}=y^{\nu-k}$ ja $\frac{\partial g(\xi,y)}{\partial b_k}=y^{\mu-k}$, leiame viimastest valemitest

$$\frac{\partial R(\xi)}{\partial a_k}=(-1)^{\nu\mu}b_0{}^\nu[\zeta_1{}^{\nu-k}f(\xi,\zeta_2)f(\xi,\zeta_3)\ldots f(\xi,\zeta_\mu)+$$
$$+\zeta_2{}^{\nu-k}f(\xi,\zeta_1)f(\xi,\zeta_3)\ldots f(\xi,\zeta_\mu)+\ldots+$$
$$+\xi_\mu{}^{\nu-k}f(\xi,\zeta_1)f(\xi,\zeta_2)\ldots f(\xi,\zeta_{\mu-1})]$$

$$\frac{\partial R(\xi)}{\partial b_k}=a_0{}^\mu[\eta_1{}^{\mu-k}g(\xi,\eta_2)g(\xi,\eta_3)\ldots g(\xi,\eta_\nu)+$$
$$+\eta_2{}^{\mu-k}g(\xi,\eta_1)g(\xi,\eta_3)\ldots g(\xi,\eta_\nu)+\ldots+$$
$$+\eta_\nu{}^{\mu-k}g(\xi,\eta_1)g(\xi,\eta_2)\ldots g(\xi,\eta_{\nu-1})].$$

Kui nüüd polünoomidel $f(\xi, y)$ ja $g(\xi, y)$ on kaks ühist lahendit $\eta_1=\zeta_1$, $\eta_2=\zeta_2$, siis on $f(\xi,\zeta_1)=0$, $f(\xi,\zeta_2)=0$, $g(\xi,\eta_1)=0$, $g(\xi,\eta_2)=0$ ja seega

$$\frac{\partial R(\xi)}{\partial a_k}=0,\quad k=0,1,2,\ldots,\nu$$

$$\frac{\partial R(\xi)}{\partial b_k}=0,\quad k=0,1,2,\ldots,\mu.$$

Kasutades diferentseerimise ahelreeglit (§ 9, art. 1), leiame

$$R'(\xi)=\frac{\partial R(\xi)}{\partial a_0}a_0'(\xi)+\frac{\partial R(\xi)}{\partial a_1}a_1'(\xi)+\ldots+\frac{\partial R(\xi)}{\partial a_\nu}a_\nu'(\xi)+$$
$$+\frac{\partial R(\xi)}{\partial b_0}b_0'(\xi)+\frac{\partial R(\xi)}{\partial b_1}b_1'(\xi)+\ldots+\frac{\partial R(\xi)}{\partial b_\mu}b_\mu'(\xi),$$

millest nähtub, et

$$R'(\xi) = 0,$$

s. o. ξ on võrrandile $R(x) = 0$ vähemalt kahekordne lahend. Niisiis x-i väärtusele ξ võib vastata kaks y väärtust ainult siis, kui ξ on vähemalt kahekordne võrrandi $R(x) = 0$ lahend. Nii vastab näites 5 x-i väärtusele 0 kaks y väärtust 1 ja -1, kusjuures 0 on võrrandi $R(x) = 0$ neljakordne lahend.

Üldiselt saab näidata, et x-i väärtusele ξ, kus $R(\xi) = 0$, võib vastata arvult α y väärtust vaid siis, kui ξ on võrrandile $R(x) = 0$ vähemalt α-kordne lahend. Tähendab, *kui resultant* $R(x)$ *ei ole nullpolünoom, siis võib võrrandisüsteemil*

$$f(x, y) = 0, \quad g(x, y) = 0$$

olla ülimalt nm lahendit, kus n ja m on vastavalt f ja g astmed. See tulemus on antud esmakordselt Bézout' poolt 1799. a. geomeetrilises sõnastuses, mille järgi tasandil n-järku joon võib lõikuda m-järku joonega ülimalt nm punktis, kui neil joontel ei ole ühiseid tükke.

Kui $R(x)$ osutub nullpolünoomiks, siis ei ole antud võrrandisüsteemi lahendite arv korrutisega nm piiratud, sest siis võib tundmatu x omada iga väärtust ξ, mis ei ole $a_0(x)$ ja $b_0(x)$ ühiseks lahendiks. Niisugune juhtum leiab aset siis, kui polünoomidel $f(x, y)$ ja $g(x, y)$ on ühistegur $d(x, y)$, s. o. kui

$$f(x, y) = d(x, y)\overline{f}(x, y), \quad g(x, y) = d(x, y)\overline{g}(x, y),$$

sest antud süsteemi rahuldavad siis kõik võrrandi

$$d(x, y) = 0$$

lahendid, mille arv pole aga piiratud, kuna siin x-i väärtuse võib vabalt ette anda ja sellele vastavalt määrata y.

Teise äärmusena võib juhtuda, et antud võrrandisüsteemil pole ühtki lahendit, s. o. et süsteem on vastuoluline, nagu näiteks juhul

$$x^2y^2 + 1 = 0, \quad xy + 1 = 0,$$

kus

$$R(x) = \begin{vmatrix} x^2 & 0 & 1 \\ x & 1 & 0 \\ 0 & x & 1 \end{vmatrix} = 2x^2.$$

Siin võrrandi $R(x) = 0$ ainuke lahend $\xi = 0$ ei anna ilmselt lahendit vaadeldavale süsteemile, mis on seletatav sellega, et $\xi = 0$ on ühtlasi $a_0(x) = x^2$ ja $b_0(x) = x$ ühislahend.

Harjutusülesandeid.

43. Näidata, et polünoomid

a) $x^4 - 2x + 3$; b) $x^4 - x^3 + 2x + 1$;
c) $x^p - px + 2p - 1$ (p algarv)

on taandumatud täisarvude integriteetkonnas.

44. Rakendades ratsionaallahendite leidmise võtet, lahendada võrrandid:

a) $x^5 - 2x^4 - 4x^3 + 4x^2 - 5x + 6 = 0$;
b) $2x^3 + 3x^2 + 6x - 4 = 0$;
c) $6x^4 + 19x^3 - 7x^2 - 26x + 12 = 0$.

45. Näidata, et täisarvuliste kordajatega polünoomi

$$g(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

ratsionaallahenditeks võivad olla ainult niisugused taandatud murrud $\frac{a}{b}$, kus b on a_0 tegur, a on a_n tegur ja mille puhul avaldised $\frac{g(1)}{a-b}$, $\frac{g(-1)}{a+b}$ kujutavad täisarve.

46. Näidata Eisensteini kriteeriumi abil, et polünoom

$$xy^3 - x^2y^2 + 2x^2y - x^3 - x^2 + 2y^2 + 2x - 4y + 2$$

on taandumatu täisarvude integriteetkonnas.

47. Järjestada polünoom

$$(x_1^2 - x_3^2 - 2x_1x_2 + 3x_2x_3)(x_2^2 + x_3^2 + 2x_1x_2 - 3x_1x_3)$$

leksikograafiliselt.

48. Kontrollida polünoomi

$$x_1^3 - 3x_1^2x_2 + 2x_1x_3^2 + x_3^3$$

puhul Euleri valemit.

49. Avaldada sümmeetrilised polünoomid

a) $x_1^3 + x_2^3 + x_3^3 - 3x_1x_2x_3$; b) $(x_1 + x_2)(x_1 + x_3)(x_2 + x_3)$;
c) $x_1^4 + x_2^4 + \ldots + x_n^4 - 2(x_1^2x_2^2 + x_1^2x_3^2 + \ldots + x_{n-1}^2x_n^2)$

sümmeetriliste põhipolünoomide kaudu.

50. Näidata, et iga sümmeetrilise põhipolünoomi σ_i puhul kehtib valem

$$\sum_{k=1}^{n} \frac{\partial \sigma_i}{\partial x_k} = (n - i)\sigma_{i-1}.$$

51. Koostada madalaima astme polünoomid, mille lahenditeks on:

a) $\xi_1 = 1 + i$, $\xi_2 = 1 - i$, $\xi_3 = 2$, $\xi_4 = i$, $\xi_5 = -i$;
b) $\xi_1 = \sqrt{a} + \sqrt{b}$, $\xi_2 = \sqrt{a} - \sqrt{b}$, $\xi_3 = -\sqrt{a} + \sqrt{b}$,
$\xi_4 = -\sqrt{a} - \sqrt{b}$.

52. Leida polünoomi $4x^3 - 16x^2 - 9x + 36$ lahendid, teades, et kaks tema lahendit erinevad vaid märgi poolest.

53. Leida λ väärtus, mille puhul polünoomi $x^3 + 3x^2 + \lambda$ lahendid moodustavad aritmeetilise jada ja leida need lahendid.

54. Leida λ väärtus, mille puhul polünoomi $x^3 + x^2 + 2x + \lambda$ lahendid moodustavad geomeetrilise jada ja leida need lahendid.

55. Leida polünoomide

a) $x^3 - x + 1$; b) $x^6 - 4x^5 + 3x^3 - 4x^2 + x + 1$

lahendite neljandate astmete summa.

56. Leida kolm arvu, mille summa on 2, ruutude summa 6 ja kuupide summa 8.

57. Leida kolmnurga pindala ja ümberringi raadius, kui kolmnurga külgede pikkused on antud polünoomi $x^3 - ax^2 + bx - c$ lahenditena.

58. Näidata, et iga kolmanda astme polünoomi lahendite puhul kehtib seos

$$3(s_1^5 - s_5) = 5(s_1^3 - s_3)(\sigma_1^2 - \sigma_2).$$

59. Näidata resultandi arvutamise teel, et polünoomid

$$2x^3 - 3x^2 - x + 2, \quad x^4 - 2x^2 - 3x + 4$$

omavad ühiseid lahendeid ja leida need Eukleidese algoritmi rakendades.

60. Missuguse λ korral on polünoomidel

$$x^3 - \lambda x + 2, \quad x^2 + \lambda x + 2$$

ühislahend?

61. Näidata, et polünoomide

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$
$$a_0x^{n-1} + a_1x^{n-2} + \ldots + a_{n-2}x + a_{n-1}$$

resultant on $a_0^n a_n^{n-1}$.

62. Näidata, et

a) $R(f, g + \lambda f) = R(f, g)$; b) $R(f, g_1g_2) = R(f, g_1)R(f, g_2)$.

63. Näidata diskriminandi arvutamise teel, et polünoom $x^4 - x^3 - 3x^2 + x + 1$ omab jäägiklassikorpuses $R^{(5)}$ kordseid lahendeid ja eraldada need.

64. Missuguse λ korral omab polünoom $x^3 - 8x^2 + (13 - \lambda)x - (6 + 2\lambda)$ kordseid lahendeid?

65. Näidata, et polünoomi $x^n + a$ diskriminant on

$$(-1)^{\frac{n(n-1)}{2}} n^n a^{n-1}.$$

66. Näidata, et $D(f, g) = D(f)D(g)R^2(f, g)$.

67. Elimineerida y võrrandeist

a) $x^2 - xy + y^2 - 3 = 0$, $x^2y + xy^2 - 6 = 0$;

b) $x = y^3 - 2y^2 - 6y + 8$, $x = 2y^3 - 8y^2 + 5y + 2$.

IV. Algebralised võrrandid.

§ 11. Võrrandite algebraline lahendus.

1. Tschirnhaus'i teisendus. Polünoomide algebra põhilause järgi (§ 5, art. 3) omab iga mittekonstantne polünoom vähemalt ühte lahendit kas põhikorpuses K või sobivalt konstrueeritud ülemkorpuses. Käesolevas peatükis vaatleme, kuidas tegelikult leida antud polünoomi lahendeid. Polünoomi $f(x)$ lahendite leidmise ehk võrrandi $f(x) = 0$ lahendamise all mõistetakse klassikalises algebras nende lahendite arvutamist võrrandi kordajatest ratsionaalsete operatsioonide ja juurimise teel. Siinjuures tuleb silmas pidada, et juurimine tähendab omakorda teatava võrrandi, nn. binoomvõrrandi

$$x^n - a = 0$$

lahendamist. Seega tähendab algebralise võrrandi lahendamine klassikalises mõttes selle võrrandi taandamist ühe või mitme binoomvõrrandi lahendamisele, mistõttu me kõneleme siin võrrandi lahendusest radikaalides.

Et võrrandi mõlemaid pooli võib lahendeid mõjustamata jagada mistahes konstandiga, siis võime üldsust kitsendamata eeldada, et antud võrrand $f(x) = 0$ on normeeritud, s. o. et $f(x)$ pealiikme kordajaks on ühikelement, nii et $f(x)$ omab kuju

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n .$$

Märkides siin $x = y - \frac{a_1}{n}$, leiame binoomvalemit rakendades kergesti, et $f(x)$ saab kuju

$$y^n + b_2 y^{n-2} + \ldots + b_{n-1} y + b_n ,$$

kus puudub y^{n-1}-ga liige. Teisendus $x = y - \frac{a_1}{n}$ kannab Tschirnhausi teisenduse nime.

Olgu tähendatud, et jagamist naturaalarvuga n mõistetakse korpuses üldiselt jagamisena ühikelemendi kordsega ne (§ 7, art. 2), mistõttu Tschirnhausi teisendus kaotab oma mõtte, kui $ne = 0$. Võrdus $ne = 0$ leiab aga aset vaid korpuses karakteristikaga $p \geqslant 2$ ja nimelt juhul, kui n jagub p-ga (§ 7, art. 1). Seega võib iga võrrandit, mille aste n ei jagu põhikorpuse K karakteristikaga, muuta Tschirnhausi teisendusega võrrandiks, kus puudub liige tundmatu $(n-1)$-se astmega.

Et Tschirnhausi teisenduse puhul $y = x + \frac{a_1}{n}$, siis asetades selle y väärtuse teisendatud polünoomi, saame tagasi $f(x)$, s. o.

$$f(x) = \left(x + \frac{a_1}{n}\right)^n + b_2\left(x + \frac{a_1}{n}\right)^{n-2} + \ldots + b_{n-1}\left(x + \frac{a_1}{n}\right) + b_n .$$

Viimane võrdus kujutab polünoomi $f(x)$ Taylori arendist kohal $\xi = -\frac{a_1}{n}$ (§ 6, art. 2). Seega saame kordajad $b_1, \ldots, b_{n-1}, b_n$, leides $f(x)$ Taylori arendise kohal $\xi = -\frac{a_1}{n}$.

Rakendades näiteks ruutvõrrandile

$$x^2 + px + q = 0$$

Tschirnhausi teisendust $x = y - \frac{p}{2}$, saame

$$y^2 + q - \frac{p^2}{4} = 0 ,$$

millest $y = \pm\sqrt{\frac{p^2}{4} - q}$ ja seega

$$x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} ,$$

mis kujutab ruutvõrrandi tuntud lahendusvalemit. See valem on kehtiv igas korpuses, mille karakteristika ei ole 2.

2. Kolmanda astme võrrand. Kui põhikorpuse karakteristika ei ole 3, siis võib igale kolmanda astme võrrandile anda eelmise artikli põhjal kuju

$$x^3 + px + q = 0. \tag{1}$$

Märkides siin $x = u + v$, saame

$$u^3 + 3u^2v + 3uv^2 + v^3 + p(u + v) + q = 0$$

ehk

$$(u^3 + v^3 + q) + (3uv + p)(u + v) = 0.$$

Tulemusest nähtub, et $x = u + v$ rahuldab võrrandit (1), kui

$$u^3 + v^3 + q = 0, \quad 3uv + p = 0. \tag{2}$$

Tingimustest (2) järeldub aga, et

$$u^3 + v^3 = -q, \quad u^3v^3 = -\frac{p^3}{27},$$

mistõttu suurused u^3 ja v^3 osutuvad Vieta valemite põhjal ruutvõrrandi

$$z^2 + qz - \frac{p^3}{27} = 0$$

lahenditeks. Eeldades, et põhikorpuse karakteristika pole ka mitte 2, leiame viimast ruutvõrrandit lahendades

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

millest

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

ja seega $x = u + v$ tõttu

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

Saadud valem, mis kujutab kolmanda astme võrrandi (1) lahendust radikaalides, kannab Cardano valemi nime itaalia matemaatiku Cardano järgi, kes selle valemi esmakord-

selt avaldas 1545. a. Tegelikult on nimetatud valem leitud Ferro poolt juba 1515. a. ja uuesti Tartaglia poolt 1535. a. Seega on iga kolmanda astme võrrand radikaalides lahenduv, kui põhikorpuse karakteristika ei ole 2 ega 3.

Silmas pidades, et kuupjuurel on korpuses kolm väärtust — kui mitte põhikorpuses K, siis teatavas ülemkorpuses —, saame u jaoks kolm väärtust ja v jaoks kolm väärtust. Kui meil aga üks u väärtus on valitud, siis ei saa Cardano valemis enam v väärtust vabalt valida, vaid v tuleb määrata nii, et oleks täidetud teine tingimus (2), mille järgi

$$v = -\frac{p}{3u}.$$

Olgu u_1 kuupjuure u mingi väärtus ja $\varepsilon_0 = 1$, ε_1, ε_2 kolmanda astme ühejuured, s. o. võrrandi $x^3 - 1 = 0$ lahendid. Kuupjuure u ülejäänud väärtused on siis

$$u_2 = u_1\varepsilon_1, \quad u_3 = u_1\varepsilon_2,$$

sest

$$u_2^3 = u_1^3\varepsilon_1^3 = u_1^3, \quad u_3^3 = u_1^3\varepsilon_2^3 = u_1^3.$$

Kuupjuure v vastavad väärtused saame valemist $v = -\frac{p}{3u}$. Et Vieta valemite järgi $\varepsilon_0\varepsilon_1\varepsilon_2 = 1$, siis on $\varepsilon_0 = 1$ tõttu $\varepsilon_1\varepsilon_2 = 1$ ja seega, märkides

$$v_1 = -\frac{p}{3u_1},$$

leiame

$$v_2 = -\frac{p}{3u_2} = -\frac{p}{3u_1\varepsilon_1} = \frac{v_1}{\varepsilon_1} = v_1\varepsilon_2$$

$$v_3 = -\frac{p}{3u_3} = -\frac{p}{3u_1\varepsilon_2} = \frac{v_1}{\varepsilon_2} = v_1\varepsilon_1.$$

Niisiis võib kuupvõrrandi (1) lahendid avaldada kujul

(3) $\xi_1 = u_1 + v_1$, $\xi_2 = u_1\varepsilon_1 + v_1\varepsilon_2$, $\xi_3 = u_1\varepsilon_2 + v_1\varepsilon_1$,

kus u_1 tähendab kuupjuure $u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ mingit väärtust ja $v_1 = -\frac{p}{3u_1}$.

Näide 1. Lahendada kolmanda astme võrrand

$$x^3 + 6ix^2 - 6x + 8i = 0 .$$

Võtame kõigepealt ette Tschirnhausi teisenduse $x = y - 2i$, rakendades kolm korda Horneri võtet kohal $-2i$:

	1	$6i$	-6	$8i$
$-2i$	1	$4i$	2	$4i$
$-2i$	1	$2i$	6	
$-2i$	1	0.		

Seega omab antud võrrand pärast Tschirnhausi teisendust kuju

$$y^3 + 6y + 4i = 0 .$$

Arvutame nüüd kuupjuure $u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ mingi väärtuse. Antud juhul $p = 6$, $q = 4i$, nii et

$$-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = -2i + \sqrt{-4 + 8} = -2i + 2 =$$
$$= -\sqrt{8}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right),$$

mistõttu võime võtta

$$u_1 = -\sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = -1 - i$$

ja seega

$$v_1 = -\frac{p}{3u_1} = \frac{2}{1+i} = 1 - i .$$

Ühejuurte ε_1 ja ε_2 leidmiseks paneme tähele, et võrrand $x^3 - 1 = 0$ taandub $x^3 - 1 = (x - 1)(x^2 + x + 1)$ tõttu kaheks võrrandiks

$$x - 1 = 0 , \quad x^2 + x + 1 = 0 ,$$

millest viimase lahenditeks ongi ε_1 ja ε_2, s. o.

$$\varepsilon_1 = \frac{-1+i\sqrt{3}}{2}, \quad \varepsilon_2 = \frac{-1-i\sqrt{3}}{2}.$$

Rakendades valemit (3), saame teisendatud võrrandi lahendid

$$\eta_1 = u_1 + v_1 = -2i$$
$$\eta_2 = u_1\varepsilon_1 + v_1\varepsilon_2 = (1-\sqrt{3})i$$
$$\eta_3 = u_1\varepsilon_2 + v_1\varepsilon_1 = (1+\sqrt{3})i$$

ja seost $x = y - 2i$ silmas pidades antud võrrandi lahendid

$$\xi_1 = -4i, \quad \xi_2 = -(1+\sqrt{3})i, \quad \xi_3 = (-1+\sqrt{3})i.$$

Diskuteerime lõppeks veel Cardano valemit juhul, kui võrrandi (1) kordajad on reaalarvud. Et sel juhul näite 1 järgi

$$\varepsilon_1 = \frac{-1+i\sqrt{3}}{2}, \quad \varepsilon_2 = \frac{-1-i\sqrt{3}}{2},$$

siis omavad siin valemid (3) kuju

$$(4) \qquad \begin{aligned} \xi_1 &= u_1 + v_1 \\ \xi_2 &= -\frac{u_1+v_1}{2} + i\frac{u_1-v_1}{2}\sqrt{3} \\ \xi_3 &= -\frac{u_1+v_1}{2} - i\frac{u_1-v_1}{2}\sqrt{3}. \end{aligned}$$

Osutub, et reaalsete kordajatega kuupvõrrandi lahendite uurimisel etendab määravat osa ruutjuure aluse avaldise $\frac{q^2}{4}+\frac{p^3}{27}$ märk. Viimane avaldis on lihtsalt seotud kuupvõrrandi diskriminandiga D, mis omab, nagu nägime (§ 10, art. 2), kuju

$$D = -27q^2 - 4p^3.$$

Seega

$$\frac{q^2}{4}+\frac{p^3}{27} = -\frac{D}{108}.$$

1° Kui $\frac{q^2}{4}+\frac{p^3}{27} > 0$ $(D<0)$, siis esinevad Cardano valemis kuupjuure all reaalarvud. Võttes suuruseks u_1 vastava kuup-

juure reaalse väärtuse, saame seose $v_1 = -\frac{p}{3u_1}$ tõttu ka v_1 reaalsena. Seega nähtub valemist (4), et siin ξ_1 on reaalne ja ξ_2, ξ_3 kaaskompleksarvud. Tähendab, *juhul* $D < 0$ *omab kuupvõrrand* (1) *ühte reaalset ja kahte kaaskompleks-lahendit* (joonis 7).

2° Kui $\frac{q^2}{4} + \frac{p^3}{27} = 0$ $(D = 0)$, siis omavad Cardano valemis mõlemad kuupjuured kuju $\sqrt[3]{-\frac{q}{2}}$. Võttes u_1 reaalsena, saame seose $v_1 = -\frac{p}{3u_1}$ tõttu ka v_1 reaalsena, kusjuures $v_1 = u_1$, mistõttu valemid (4) annavad

$$\xi_1 = 2u_1, \quad \xi_2 = -u_1, \quad \xi_3 = -u_1.$$

Tähendab, *juhul* $D = 0$ *on kuupvõrrandi* (1) *lahendid kõik reaalsed, kusjuures üks lahend on kahekordne* (joonis 7).

3° Kui $\frac{q^2}{4} + \frac{p^3}{27} < 0$ $(D > 0)$, siis on Cardano valemis kuupjuure all kompleksarvud, mistõttu kõik u ja v väärtused tulevad kompleksed. Olgu $u_1 = a + bi$. Vastavalt kompleksarvuga jagamise eeskirjale leiame

$$v_1 = -\frac{p}{3u_1} = -\frac{p\bar{u}_1}{3u_1\bar{u}_1} = -\frac{p\bar{u}_1}{3|u_1|^2}.$$

Tingimusel $\frac{q^2}{4} + \frac{p^3}{27} < 0$ on aga

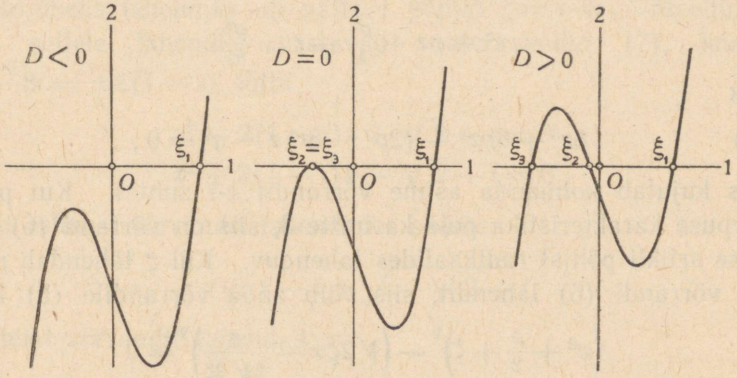
$$|u_1|^2 = \sqrt[3]{\left|-\frac{q}{2} + i\sqrt{-\frac{q^2}{4} - \frac{p^3}{27}}\right|^2} = \sqrt[3]{\frac{q^2}{4} - \frac{q^2}{4} - \frac{p^3}{27}} = -\frac{p}{3}$$

ja seega $v_1 = \bar{u}_1$, s. o. $v_1 = a - bi$, mistõttu saame valemeist (4)

$$\xi_1 = 2a, \quad \xi_2 = -a - b\sqrt{3}, \quad \xi_3 = -a + b\sqrt{3}.$$

Tähendab, *kui* $D > 0$, *siis on kuupvõrrandi* (1) *lahendid kõik reaalsed ja erinevad* (joonis 7).

Märkus. Olgu tähendatud, et Cardano valemid ei ole üldiselt kohased praktilisteks arvutusteks, eriti viimati vaadeldud juhul 3^0, kus vaatamata sellele, et kuupvõrrandi (1) lahendid on kõik reaalsed, lubab Cardano valem neid arvutada vaid komplekssuuruste kaudu.



Joonis 7.

Nagu hiljem näeme (§ 29, art. 3), ei avaldu sel juhul võrrandi (1) lahendid üldse mingil viisil reaalsete radikaalide kaudu. Seepärast nimetatakse juhtu 3^0 taandumatuks juhuks (casus irreducibilis).

3. Neljanda astme võrrand. Kui põhikorpuse karakteristika ei ole 2, siis võib igale neljanda astme võrrandile anda Tschirnhausi teisenduse teel kuju

$$x^4 + px^2 + qx + r = 0 . \tag{5}$$

Tuues sisse abisuuruse z, teisendame võrrandi (5) vasakut poolt järgmiselt:

$$x^4 + px^2 + qx + r = (x^2 + \frac{p}{2} + z)^2 + qx + r - \frac{p^2}{4} - z^2 -$$

$$- 2zx^2 - pz = (x^2 + \frac{p}{2} + z)^2 - [2zx^2 - qx +$$

$$+ (z^2 + pz + \frac{p^2}{4} - r)] .$$

Määrame nüüd z nõnda, et ka avaldis nurksulgudes osutuks täisruuduks, s. o. et oleks

$$2zx^2 - qx + \left(z^2 + pz + \frac{p^2}{4} - r\right) = \left(\sqrt{2z}x - \frac{q}{2\sqrt{2z}}\right)^2.$$

Avades selle võrduse paremal poolel sulud, saame z-i jaoks tingimuse

$$z^2 + pz + \frac{p^2}{4} - r = \frac{q^2}{8z}$$

ehk

$$8z^3 + 8pz^2 + (2p^2 - 8r)z - q^2 = 0, \tag{6}$$

mis kujutab kolmanda astme võrrandit z-i suhtes. Kui põhikorpuse karakteristika pole ka mitte 3, siis on võrrand (6) eelmise artikli põhjal radikaalides lahenduv. Kui ζ tähendab mingit võrrandi (6) lahendit, siis võib anda võrrandile (5) kuju

$$\left(x^2 + \frac{p}{2} + \zeta\right)^2 - \left(\sqrt{2\zeta}x - \frac{q}{2\sqrt{2\zeta}}\right)^2 = 0$$

ehk

$$\left(x^2 + \frac{p}{2} + \zeta - \sqrt{2\zeta}x + \frac{q}{2\sqrt{2\zeta}}\right)\left(x^2 + \frac{p}{2} + \zeta + \sqrt{2\zeta}x - \frac{q}{2\sqrt{2\zeta}}\right) = 0,$$

mistõttu võrrand (5) laguneb kaheks ruutvõrrandiks

$$\begin{aligned} x^2 - \sqrt{2\zeta}x + \frac{p}{2} + \zeta + \frac{q}{2\sqrt{2\zeta}} &= 0 \\ x^2 + \sqrt{2\zeta}x + \frac{p}{2} + \zeta - \frac{q}{2\sqrt{2\zeta}} &= 0. \end{aligned} \tag{7}$$

Viimased võrrandid on aga radikaalides lahenduvad. Seega on iga neljanda astme võrrand radikaalides lahenduv, kui põhikorpuse karakteristika ei ole 2 ega 3, kusjuures neljanda astme võrrandi lahendus taandub ühe kolmanda ja kahe teise astme võrrandi lahendusele.

Siin toodud neljanda astme võrrandi lahendus on esmakordselt antud Cardano õpilase Ferrari poolt ja avaldatud Cardano poolt koos kolmanda astme võrrandi lahendusega.

Näide 2. Lahendada neljanda astme võrrand

$$x^4 + 6ix^2 + 4\sqrt{2}(1 - i)x - 3 = 0.$$

Et siin $p=6i$, $q=4\sqrt{2}(1-i)$, $r=-3$, siis omab kuupvõrrand (6) kuju

$$8z^3+48iz^2-48z+64i=0$$

ehk

$$z^3+6iz^2-6z+8i=0,$$

mille üheks lahendiks on näite 1 põhjal $\zeta=-4i$. Moodustades sellele lahendile vastavad ruutvõrrandid (7), leiame $\sqrt{-8i}=\pm 2(1-i)$ tõttu

$$x^2-2(1-i)x+\sqrt{2}-i=0$$
$$x^2+2(1-i)x-\sqrt{2}-i=0,$$

kust esimest võrrandit lahendades saame

$$x=1-i\pm\sqrt{-\sqrt{2}-i}$$

ja teist võrrandit lahendades

$$x=-1+i\pm\sqrt{\sqrt{2}-i}.$$

Nüüd on aga (§ 1, art. 1)

$$\sqrt{-\sqrt{2}-i}=\sqrt{\frac{\sqrt{3}-\sqrt{2}}{2}}-\sqrt{\frac{\sqrt{3}+\sqrt{2}}{2}}\,i$$

$$\sqrt{\sqrt{2}-i}=\sqrt{\frac{\sqrt{3}+\sqrt{2}}{2}}-\sqrt{\frac{\sqrt{3}-\sqrt{2}}{2}}\,i$$

ja seega antud võrrandi lahendid on:

$$\xi_1=1+\sqrt{\frac{\sqrt{3}-\sqrt{2}}{2}}-\left(1+\sqrt{\frac{\sqrt{3}+\sqrt{2}}{2}}\right)i,$$

$$\xi_2=1-\sqrt{\frac{\sqrt{3}-\sqrt{2}}{2}}-\left(1-\sqrt{\frac{\sqrt{3}+\sqrt{2}}{2}}\right)i,$$

$$\xi_3=-1+\sqrt{\frac{\sqrt{3}+\sqrt{2}}{2}}+\left(1-\sqrt{\frac{\sqrt{3}-\sqrt{2}}{2}}\right)i,$$

$$\xi_4=-1-\sqrt{\frac{\sqrt{3}+\sqrt{2}}{2}}+\left(1+\sqrt{\frac{\sqrt{3}-\sqrt{2}}{2}}\right)i.$$

4. Pöördvõrrandid. Nimetame n-astme võrrandit $f(x)=0$ pöördvõrrandiks, kui $f(x)$ rahuldab tingimust

$$x^n f\left(\frac{1}{x}\right)=\lambda f(x), \tag{8}$$

kus λ tähendab konstanti. Tingimusest (8) nähtub, et kui mingi ξ puhul $f(\xi)=0$, siis ka $f\left(\frac{1}{\xi}\right)=0$, s. o. kui pöördvõrrandi lahendiks on ξ, siis on tema lahendiks ka pöördväärtus $\frac{1}{\xi}$, millest tulenebki pöördvõrrandi nimetus.

Asendades tingimuses (8) x-i tema pöördväärtusega $\frac{1}{x}$, leiame pärast x^n-ga korrutamist

$$f(x)=\lambda x^n f\left(\frac{1}{x}\right)$$

ja uuesti tingimust (8) silmas pidades

$$f(x)=\lambda^2 f(x),$$

kust $\lambda^2=1$, nii et $\lambda=\pm 1$. Selle järgi, kas $\lambda=1$ või $\lambda=-1$, kõneleme esimest või teist liiki pöördvõrrandist. Kui

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n,$$

siis

$$x^n f\left(\frac{1}{x}\right)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0.$$

Järelikult on esimest liiki pöördvõrrand iseloomustatud seostega

$$a_k=a_{n-k}$$

ja teist liiki pöördvõrrand seostega

$$a_k=-a_{n-k}.$$

Näitame, et juhul, kui põhikorpuse karakteristika ei ole 2, saab iga teist liiki pöördvõrrandi lahendamist taandada esimest liiki pöördvõrrandi lahendamisele.

Tõepoolest, võttes teist liiki pöördvõrrandi tingimuses

$$x^n f\left(\frac{1}{x}\right) = -f(x)$$

$x = 1$, saame $f(1) = -f(1)$, millest $2f(1) = 0$ ja seega $f(1) = 0$, sest põhikorpuse karakteristika ei ole 2. Järelikult peab $f(x)$ jaguma lineaarteguriga $x - 1$. Märkides

$$\frac{f(x)}{x-1} = g(x),$$

taandame võrrandi $f(x) = 0$ lahenduse $(n-1)$-astme võrrandi $g(x) = 0$ lahendusele. Nüüd on aga

$$x^{n-1} g\left(\frac{1}{x}\right) = x^{n-1} \frac{f\left(\frac{1}{x}\right)}{\frac{1}{x} - 1} = \frac{x^n f\left(\frac{1}{x}\right)}{1-x} = \frac{f(x)}{x-1} = g(x),$$

millest nähtub, et $g(x) = 0$ kujutab esimest liiki pöördvõrrandit. Nii näiteks taandub teist liiki pöördvõrrand $x^n - 1 = 0$ pärast jagamist lineaarteguriga $x - 1$ esimest liiki pöördvõrrandiks

$$x^{n-1} + x^{n-2} + \ldots + x + 1 = 0.$$

Piirdudes seepärast järgnevas esimest liiki pöördvõrranditega, näitame kõigepealt, et juhul, kui põhikorpuse karakteristika ei ole 2, võib iga esimest liiki pöördvõrrandit taandada paarisastmeliseks sama liiki pöördvõrrandiks. Nimelt kui esimest liiki pöördvõrrandi $f(x) = 0$ aste n on paaritu arv, siis võttes selle pöördvõrrandi tingimuses

$$x^n f\left(\frac{1}{x}\right) = f(x)$$

$x = -1$, saame $-f(-1) = f(-1)$, millest $2f(-1) = 0$ ja seega $f(-1) = 0$. Järelikult peab $f(x)$ jaguma lineaarteguriga $x + 1$. Märkides

$$\frac{f(x)}{x+1} = g(x),$$

taandame võrrandi $f(x) = 0$ lahenduse $(n-1)$-astme, s. o. paarisastmelise võrrandi $g(x) = 0$ lahendusele. Nüüd on aga

$$x^{n-1} g\left(\frac{1}{x}\right) = x^{n-1} \frac{f\left(\frac{1}{x}\right)}{\frac{1}{x}+1} = \frac{x^n f\left(\frac{1}{x}\right)}{x+1} = \frac{f(x)}{x+1} = g(x),$$

mis ütleb, et $g(x)$ kujutab esimest liiki pöördvõrrandit. Nii näiteks taandub paarituastmeline esimest liiki pöördvõrrand $x^{2m+1}+1=0$ pärast jagamist lineaarteguriga $x+1$ paarisastmeliseks esimest liiki pöördvõrrandiks $x^{2m} - x^{2m-1} + x^{2m-2} - \ldots + x^2 - x + 1 = 0$.

Seega tarvitseb meil vaadelda vaid paarisastmelist esimest liiki pöördvõrrandit $f(x) = 0$, kus

$$f(x) = a_0 x^{2m} + a_1 x^{2m-1} + \ldots + a_{m-1} x^{m+1} + a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0.$$

Jagades selle võrrandi mõlemaid pooli x^m-ga, saame võrdsete kordajatega liikmeid kokku võttes

$$a_0\left(x^m + \frac{1}{x^m}\right) + a_1\left(x^{m-1} + \frac{1}{x^{m-1}}\right) + \ldots + a_{m-1}\left(x + \frac{1}{x}\right) + a_m = 0.$$

Märkides $x + \frac{1}{x} = y$, leiame kergesti kontrollitava seose

$$x^{k+1} + \frac{1}{x^{k+1}} = y\left(x^k + \frac{1}{x^k}\right) - \left(x^{k-1} + \frac{1}{x^{k-1}}\right)$$

tõttu järk-järgult:

$$x + \frac{1}{x} = y$$

$$x^2 + \frac{1}{x^2} = y^2 - 2$$

$$x^3 + \frac{1}{x^3} = y^3 - 3y$$

$$x^4 + \frac{1}{x^4} = y^4 - 4y^2 + 2$$

$$x^5 + \frac{1}{x^5} = y^5 - 5y^3 + 5y$$

. . . . . .

Seega teisendub $2m$-astme võrrand $f(x) = 0$ asendusega $x + \frac{1}{x} = y$ m-astme võrrandiks y suhtes. Lahendades viimase võrrandi, leiame võrrandi $f(x) = 0$ lahendid seosest

$$x + \frac{1}{x} = y$$

ehk

$$x^2 - yx + 1 = 0,$$

millest

$$x = \frac{y \pm \sqrt{y^2 - 4}}{2}.$$

Kui põhikorpuse karakteristika ei ole 2 ega 3, siis, silmas pidades, et kõik võrrandid kuni 4-nda astmeni on radikaalides lahenduvad, ei ole raske näha, et kõik esimest liiki pöördvõrrandid kuni 9-nda astmeni ja teist liiki pöördvõrrandid kuni 10-nda astmeni on radikaalides lahenduvad.

Näide 3. Lahendada teist liiki pöördvõrrand

$$x^6 - x^5 + 2x^4 - 2x^2 + x - 1 = 0,$$

kui tema kordajad kuuluvad jäägiklassikorpusse $R^{(7)}$.

Jagades antud võrrandi mõlemat poolt lineaarteguriga $x - 1$, saame esimest liiki pöördvõrrandi

$$x^5 + 2x^3 + 2x^2 + 1 = 0,$$

mida omakorda lineaarteguriga $x + 1$ jagades leiame esimest liiki pöördvõrrandi

$$x^4 - x^3 + 3x^2 - x + 1 = 0$$

paarisarvulise astmega 4. Jagades siin võrrandi mõlemat poolt x^2-ga, saame

$$\left(x^2 + \frac{1}{x^2}\right) - \left(x + \frac{1}{x}\right) + 3 = 0$$

ehk, märkides $x + \frac{1}{x} = y$:

$$y^2 - y + 1 = 0.$$

Viimase ruutvõrrandi lahendamine annab

$$y = 4 \pm \sqrt{2 - 1} = 4 \pm 1 = \begin{cases} 5 \\ 3, \end{cases}$$

millele vastavad ruutvõrrandid

$$x^2 - 5x + 1 = 0, \quad x^2 - 3x + 1 = 0,$$

mida lahendades leiame vastavalt

$$x = 6 \pm \sqrt{1 - 1} = 6, \quad x = 5 \pm \sqrt{-3 - 1} = 5 \pm 2i,$$

kus $i^2 = -1$. Seega on antud võrrandi lahendid

$$\xi_1 = 1, \ \xi_2 = -1, \ \xi_3 = 6, \ \xi_4 = 6, \ \xi_5 = 5 + 2i, \ \xi_6 = 5 - 2i.$$

Pärast seda, kui Cardano avaldas kolmanda ja neljanda astme võrrandite lahendused radikaalides, püüti peagu kolme sajandi vältel lahendada sama probleemi kõrgema astme võrrandite jaoks. Need katsed lõppesid alles siis, kui norra matemaatik Abel 1826. a. tõestas, et kõrgema kui neljanda astme võrrandite puhul ei leidugi üldiseid lahendusvalemeid radikaalides, mis oleksid kehtivad kõigi ühe ja sama astme võrrandite puhul. Lõplikult lahendati algebraliste võrrandite radikaalides lahenduvuse probleem noore geniaalse prantsuse matemaatiku Galois' poolt 1831. a., kes andis tarviliku ja piisava tingimuse mistahes etteantud võrrandi lahenduvuseks radikaalides (§ 29, art. 1). Galois' uurimused, kujutades ühte sügavamat ja viljakamat teooriat, mida inimvaim kunagi on loonud, avaldasid määratut mõju algebra edasisele arengule, pannes eriti aluse rühmateooriale, mille meetodid on tänapäeval tunginud peagu kõigisse matemaatika distsipliinidesse.

§ 12. Kompleksarvude algebra põhilause.

1. Põhilause tõestus. Tuleme nüüd praktikas kõige sagedamini esineva juhu juurde, kus põhikorpuseks, kuhu kuuluvad vaadeldava võrrandi kordajad, on reaalarvude korpus. Tekib küsimus, missugune on sel korral ülemkorpus, kuhu kuuluvad

kõik antud võrrandi lahendid. Binoomvõrrandi $x^n - a = 0$ kohta teame, et tema lahendid, s. o. n-astme juured $\sqrt[n]{a}$ kuuluvad kõik kompleksarvude korpusse. Osutub, et viimane asjaolu on kehtiv iga reaalkordajatega algebralise võrrandi kohta. Nimelt leiab aset järgmine tähelepandav teoreem, mis kannab kompleksarvude algebra põhilause nime ja mis kujutab ühte põhilisemat saavutust matemaatikas üldse.

Teoreem 1. *Igal reaalsete kordajatega algebralisel võrrandil on vähemalt üks kompleksarvuline lahend.*

Teoreem 1 on esmakordselt tõestatud 1799. a. Gaussi poolt tema doktoridissertatsioonis. Sellele teoreemile on omistatud hiljem erakordselt suurt tähelepanu arvukate tõestuste esitamise näol. Kuid kõik need tõestused sisaldavad suuremal või vähemal määral mittealgebralisi momente seoses polünoomi kui funktsiooni pidevusomadustega. Osutub, et kompleksarvude algebra põhilause tõestust polegi võimalik anda ainult puht-algebra meetoditega, kui loeme algebralisteks vaid korpuse mõistega antud vahendeid, s. o. ratsionaalseid operatsioone, lülitades välja vahendid, mis toetuvad suurusjärjestuse mõistele. Käesolevas artiklis anname kompleksarvude algebra põhilausele ühe tõestuse, mis toetub sümmeetriliste polünoomide põhilausele ühelt poolt ja polünoomide algebra põhilausele teiselt poolt ja mille mittealgebraline osa on vähendatud miinimumini [1]. Esitame kõigepealt tõestuse mittealgebralise osa.

Olgu antud võrrand $f(x) = 0$, kus

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$$

kujutab reaalsete kordajatega mittekonstantset normeeritud polünoomi. Et paarituarvulise n korral

$$\lim_{x \to -\infty} f(x) = -\infty, \quad \lim_{x \to +\infty} f(x) = +\infty,$$

[1] Lihtsaima tõestuse kompleksarvude algebra põhilausele saab anda kompleksmuutuja funktsiooniteooria meetoditega.

siis võib alati leida absoluutselt küllalt suure negatiivse arvu a ja positiivse arvu b nii, et oleks

$$f(a) < 0, \quad f(b) > 0.$$

Silmas pidades pidevate funktsioonide tuntud omadust, mille järgi lõigul $[a, b]$ pideval funktsioonil, mis omab otspunktides a ja b vastupidiste märkidega väärtusi, on vähemalt üks nullkoht a ja b vahel, on ilmne, et iga paarituastmeline algebraline võrrand $f(x) = 0$ omab vähemalt ühte reaalarvulist lahendit.

Nüüd tõestuse algebraline osa. Eelnenu põhjal tuleb meil käsitleda vaid juhtu, kus võrrandi aste n on paarisarv, s. o. sisaldab tegurit 2. Kui 2 esineb arvus n tegurina k korda, siis võime kirjutada

$$n = 2^k p,$$

kus p on paaritu arv. Rakendades täieliku induktsiooni printsiipi, oletame, et kompleksarvude algebra põhilause on kehtiv kõigi nende võrrandite puhul, mille aste omab kuju $2^{k-1}q$, kus q võib olla mistahes paaritu arv, ja näitame, et siis see lause kehtib ka kõigi niisuguste võrrandite puhul, mille aste $n = 2^k p$, missugune ka ei ole paaritu arv p. Võttes põhikorpuseks K kompleksarvude korpuse, millesse võrrandi $f(x) = 0$ kordajad kui reaalarvud kindlasti kuuluvad, märgime tähega L ülemkorpuse, kus see võrrand omab n lahendit

$$\xi_1, \ \xi_2, \ \ldots, \ \xi_n.$$

Olgu c mingi reaalarv. Moodustame nende lahendite abil suurused

$$(9) \quad a_{ik} = \xi_i \xi_k + c(\xi_i + \xi_k), \ i, \ k = 1, 2, \ldots, n \quad (i \neq k),$$

mis kuuluvad ilmselt korpusse L ja mille arv on

$$\binom{n}{2} = \frac{n(n-1)}{2} = \frac{2^k p(2^k p - 1)}{2} = 2^{k-1} p(2^k p - 1) = 2^{k-1} q,$$

kus $q = p(2^k p - 1)$ kujutab paaritut arvu. Koostame polünoomi

$$g(x) = \prod_{i \neq k} (x - a_{ik}) = x^m + b_1 x^{m-1} + \ldots + b_{m-1} x + b_m,$$

mille lahenditeks on suurused a_{ik} ja mille aste on vastavalt $m = 2^{k-1}q$. Siin kordajad $b_1, \ldots, b_m$ on Vieta valemite järgi sümmeetrilised põhipolünoomid a_{ik} suhtes, osutudes seega seoste (9) tõttu polünoomideks ka võrrandi $f(x) = 0$ lahendite $\xi_1, \xi_2, \ldots, \xi_n$ suhtes, s. o.

$$b_1 = \varphi_1(\xi_1, \xi_2, \ldots, \xi_n)$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$b_m = \varphi_m(\xi_1, \xi_2, \ldots, \xi_n),$$

kusjuures need polünoomid on reaalsete kordajatega, sest c on eelduse järgi reaalarv. Veel enam, polünoomid $\varphi_1, \ldots, \varphi_m$ on $\xi_1, \xi_2, \ldots, \xi_n$ suhtes sümmeetrilised, sest, nagu nähtub seostest (9), muudab iga transpositsioon (ξ_i, ξ_j) vaid suuruste a_{ik} omavahelist järjekorda, muutes näiteks a_{ik} a_{jk}-ks ja a_{jk} a_{ik}-ks, mõjutamata kordajaid $b_1, \ldots, b_m$. Seega avalduvad polünoomid $\varphi_1, \ldots, \varphi_m$ reaalarvude korpuses täisratsionaalselt $f(x)$ kordajate $a_1, \ldots, a_n$ kaudu, nii et

$$b_1 = F_1(a_1, \ldots, a_n)$$
$$\ldots\ldots\ldots\ldots$$
$$b_m = F_m(a_1, \ldots, a_n)$$

kujutavad ka reaalarve. Järelikult kujutab $g(x)$ reaalsete kordajatega polünoomi, mille aste $m = 2^{k-1}q$. Niisuguste polünoomide puhul on aga induktsioonioletuse järgi kehtiv kompleksarvude algebra põhilause, mistõttu $g(x)$ peab omama vähemalt ühte kompleksarvulist lahendit.

Teiste sõnadega, vastavalt igale reaalarvule c leiduvad niisugused indeksid i, k, mille puhul suurus a_{ik} osutub kompleksarvuks, kuuludes seega mitte ainult ülemkorpusse L, vaid koguni põhikorpusse K. Arusaadav, et andes c-le mõne teise arvulise väärtuse, saame üldiselt teised indeksid i, k, mille puhul a_{ik} tuleb kompleksarv. Kuid kuna üksteisest erinevaid c väärtusi on lõpmata palju, erinevaid indeksite i, k paare aga vaid $\binom{n}{2}$ tükki, siis peab kindlasti leiduma kaks isesugust c väärtust c_1 ja c_2, nii et a_{ik} osutub $c = c_1$ ja $c = c_2$

korral kompleksarvuks ühe ja sama indeksite i, k paari juures, s. o.

$$\begin{aligned} \xi_i\xi_k + c_1(\xi_i + \xi_k) &= \alpha \\ \xi_i\xi_k + c_2(\xi_i + \xi_k) &= \beta, \end{aligned} \tag{10}$$

kus α ja β tähendavad kompleksarve. Lahutades ülemisest võrdusest (10) alumise, leiame

$$(c_1 - c_2)(\xi_i + \xi_k) = \alpha - \beta,$$

millest $c_1 \neq c_2$ tõttu

$$\xi_i + \xi_k = -u,$$

kus $u = \frac{\beta - \alpha}{c_1 - c_2}$ on kompleksarv. Siis aga nähtub ükskõik kummast võrdusest (10), et ka korrutis

$$v = \xi_i\xi_k$$

on kompleksarv. Vieta valemite järgi kujutavad seega ξ_i ja ξ_k kompleksete kordajatega ruutvõrrandi

$$x^2 + ux + v = 0$$

lahendeid, osutudes seetõttu ise ka kompleksarvudeks. Niisiis leidub võrrandi $f(x) = 0$ lahendite hulgas koguni kaks kompleksarvulist lahendit, millega ongi kompleksarvude algebra põhilause tõestatud.

2. Järeldusi põhilausest. Anname kõigepealt kompleksarvude algebra põhilausele teise kuju, millest ilmneb kompleksarvude algebra täiuslikkus ja sõltumatus teistest algebradest. Vaatleme selleks kompleksete kordajatega polünoomi

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n.$$

Polünoomi

$$\bar{f}(x) = x^n + \bar{a}_1x^{n-1} + \ldots + \bar{a}_{n-1}x + \bar{a}_n,$$

mille kordajaiks on $f(x)$ kordajate kaaskompleksid, nimetatakse

$f(x)$ *kaaspolünoomiks*. Näitame, et kui ξ on võrrandi $f(x)=0$ lahend, siis on kaaskompleks $\bar{\xi}$ võrrandi $f(x)=0$ lahend. Tõepoolest, et

$$f(\xi)=\xi^n+a_1\xi^{n-1}+\ldots+a_{n-1}\xi+a_n,$$

siis on kaaskomplekside omaduste põhjal (§ 1, art. 2)

$$\overline{f(\xi)}=\bar{\xi}^n+\bar{a}_1\bar{\xi}^{n-1}+\ldots+\bar{a}_{n-1}\bar{\xi}+\bar{a}_n,$$

s. o.

$$\overline{f(\xi)}=f(\bar{\xi}).$$

Kui nüüd $f(\xi)=0$, siis ka $\overline{f(\xi)}=0$ ja seega $f(\bar{\xi})=0$, mis ütlebki, et $\bar{\xi}$ on võrrandi $f(x)=0$ lahend.

Erijuhul, kui $f(x)$ on reaalsete kordajatega, on $\bar{f}(x)=f(x)$. Tähendab, *kui reaalsete kordajatega võrrandit rahuldab kompleksarv* ξ, *siis rahuldab seda võrrandit ka kaaskompleks* $\bar{\xi}$. Niisiis esinevad reaalsete kordajatega võrrandi komplekslahendid paarikaupa kaaskompleksidena.

Korrutades polünoomi $f(x)$ kaaspolünoomiga $\bar{f}(x)$, saame polünoomi

$$f(x)\bar{f}(x)=x^{2n}+b_1x^{2n-1}+\ldots+b_{2n-1}x+b_{2n},$$

kus

$$b_k=\sum_{i+j=k}a_i\bar{a}_j$$

ja seega

$$\bar{b}_k=\sum_{i+j=k}\bar{a}_ia_j.$$

Vahetades viimases summas indeksid i ja j omavahel ümber, näeme, et $\bar{b}_k=b_k$, mis ütleb, et b_k kujutab reaalarvu. Niisiis on võrrand $f(x)\bar{f}(x)=0$ reaalsete kordajatega ja omab seetõttu

kompleksarvude algebra põhilause järgi vähemalt ühte kompleksarvulist lahendit ξ, s. o.

$$f(\xi)\bar{f}(\xi) = 0,$$

millest $f(\xi) = 0$ või $\bar{f}(\xi) = 0$. Esimesel juhul on ξ võrrandi $f(x) = 0$ lahend, teisel juhul aga eelnenu põhjal $\bar{\xi}$ võrrandi $f(x) = 0$ lahend, sest $f(x)$ on $\bar{f}(x)$ kaaspolünoom. Tähendab, *igal kompleksse kordajatega algebralisel võrrandil on vähemalt üks kompleksarvuline lahend.*

Olgu nüüd ξ_1 võrrandi $f(x) = 0$ kompleksarvuline lahend. Siis peab $f(x)$ jaguma kompleksarvude korpuses lineaarteguriga $x - \xi_1$, s. o.

$$f(x) = (x - \xi_1) f_1(x),$$

kus $f_1(x)$ on kompleksse kordajatega polünoom. Olgu edasi ξ_2 võrrandi $f_1(x) = 0$ kompleksarvuline lahend. Siis peab $f_1(x)$ jaguma kompleksarvude korpuses lineaarteguriga $x - \xi_2$, s. o.

$$f_1(x) = (x - \xi_2) f_2(x),$$

kus $f_2(x)$ on kompleksse kordajatega polünoom jne. Sel viisil järk-järgult võrrandi $f(x) = 0$ lahendeid eraldades näeme, et siin kõik lahendid $\xi_1, \xi_2, \ldots, \xi_n$ peavad tulema kompleksse. Tähendab, kompleksse kordajatega algebralise võrrandi lahendid on kõik kompleksarvud (erijuhul reaalarvud) ehk, teiste sõnadega, kompleksse kordajatega polünoom laguneb kompleksarvude korpuses täielikult lineaartegurite korrutiseks. Lühidalt: *kompleksarvude korpus on algebraliselt kinnine korpus.* Kompleksarvude korpuse kinnisus peegeldabki kompleksarvude süsteemi täiuslikkust ja sõltumatust.

Et kompleksarvude korpuses laguneb iga mittekonstantne polünoom lineaartegurite korrutiseks, siis võivad siin taandumatuteks polünoomideks olla ainult lineaarpolünoomid. Tekib küsimus, missugused polünoomid võivad olla taandumatud reaalarvude korpuses. Olgu $f(x)$ mingi reaalsete kordajatega

mittekonstantne polünoom. Eelnenu põhjal laguneb $f(x)$ kompleksarvude korpuses täielikult lineaartegurite korrutiseks, s. o.

$$f(x) = a_0(x - \xi_1)(x - \xi_2) \ldots (x - \xi_n),$$

kus a_0 tähendab $f(x)$ pealiikme kordajat ja $\xi_1, \xi_2, \ldots, \xi_n$ on üldiselt kompleksarvud. Et reaalsete kordajatega võrrandi kompleksiahendid esinevad paarikaupa kaaskompleksidena, siis võttes niisugustele kaaskompleksiahenditele ξ ja $\bar{\xi}$ vastavad lineaartegurid $x - \xi$ ja $x - \bar{\xi}$ paarikaupa kokku korrutiseks, saame reaalsete kordajatega polünoomid

$$(x - \xi)(x - \bar{\xi}) = x^2 - (\xi + \bar{\xi})x + \xi\bar{\xi} = x^2 + px + q,$$

sest $p = -(\xi + \bar{\xi})$ ja $q = \xi\bar{\xi}$ on reaalarvud. Tähendab, *reaalarvude korpuses laguneb iga mittekonstantne polünoom lineaar- ja ruutpolünoomide korrutiseks.* Seega on reaalarvude korpuses taandumatuteks polünoomideks peale lineaarpolünoomide veel need ruutpolünoomid, mis ei oma reaallahendeid.

Nii laguneb näiteks polünoom

$$f(x) = x^5 - 2x^4 - 2x^3 + 8x^2 - 3x + 10$$

kompleksarvude korpuses lineaartegurite korrutiseks

$$f(x) = (x + 2)(x - i)(x + i)(x - 2 - i)(x - 2 + i).$$

Võttes siin tegurid $x - i$ ning $x + i$ kokku korrutiseks $x^2 + 1$ ja tegurid $x - 2 - i$ ning $x - 2 + i$ korrutiseks $x^2 - 4x + 5$, saame

$$f(x) = (x + 2)(x^2 + 1)(x^2 - 4x + 5),$$

mis kujutab $f(x)$ taandumatuiks tegureiks lahutust reaalarvude korpuses.

Olles selgitanud, et reaalsete kordajatega võrrandi lahendid on kas reaal- või kompleksarvud, tuleme järgnevas nende lahendite numbrilise arvutamise küsimuse juurde, piirdudes seejuures reaallahendite juhuga.

§ 13. Reaalkordajatega võrrandid.

1. Reaallahendite tõkked. Reaalkordajatega võrrandite lahendite numbrilise arvutuse all mõistame nende lahendite lähisarvutust etteantud täpsusega. Vastandina võrrandite lahendusele radikaalides on lahendite lähisarvutus alati teostatav, sõltumata võrrandi astmest. Siinjuures leiavad laialdast rakendamist matemaatilise analüüsi meetodid, mistõttu käesoleva paragrahvi sisu kuulub rohkem matemaatilise analüüsi kui algebra valdkonda. Seepärast piirdume siin iga reaallahenditega seotud küsimuse käsitlemisel vaid paari põhilise meetodi arendamisega, soovitades sellele, kes tahab vastava küsimusega põhjalikumalt tutvuda, kasutada matemaatilise analüüsi lähendusmeetodite kursusi [1].

Üheks esimeseks küsimuseks võrrandi reaallahendite uurimisel on tõkete leidmine, mille vahel asetsevad kõik selle võrrandi reaallahendid, eriti aga tõkete leidmine positiivsetele ja negatiivsetele lahenditele eraldi. Näitame kõigepealt, et osates leida võrrandi positiivsete lahendite ülemist tõket, võime kergesti leida ka võrrandi positiivsete lahendite alumise tõkke ja negatiivsete lahendite tõkked. Selleks tarvitseb meil vaadelda peale antud võrrandi

$$f(x) = 0$$

veel võrrandeid

$$f_1(x) = 0, \quad f_2(x) = 0, \quad f_3(x) = 0,$$

kus

$$f_1(x) = x^n f\left(\frac{1}{x}\right), \quad f_2(x) = x^n f\left(-\frac{1}{x}\right), \quad f_3(x) = f(-x).$$

Olgu viimaste võrrandite positiivsete lahendite ülemised tõkked vastavalt λ_1, λ_2 ja λ_3. Ei ole raske näha, et siis $\frac{1}{\lambda_1}$ kujutab võrrandi $f(x) = 0$ positiivsete lahendite alumist tõket, $-\frac{1}{\lambda_2}$ nega-

[1] Näiteks Безикович, Приближенные вычисления.

tiivsete lahendite ülemist tõket ja $-\lambda_3$ negatiivsete lahendite alumist tõket, nii et võrrandi $f(x) = 0$ positiivsed lahendid rahuldavad võrratust

$$\frac{1}{\lambda_1} < \xi < \lambda$$

ja negatiivsed lahendid võrratust

$$-\lambda_3 < \xi < -\frac{1}{\lambda_2}.$$

Tõepoolest, kui ξ on võrrandi $f(x) = 0$ mingi positiivne lahend, siis on $\frac{1}{\xi}$ võrrandi $f_1(x) = 0$ positiivne lahend ja seega

$$\frac{1}{\xi} < \lambda_1,$$

millest

$$\xi > \frac{1}{\lambda_1}.$$

Analoogiliselt tõestatakse ka negatiivsete lahendite tõkete juhud.

Anname nüüd kaks menetlust võrrandi $f(x) = 0$ positiivsete lahendite ülemise tõkke leidmiseks.

1° Üldsust kitsendamata võib eeldada, et võrrandis $f(x) = 0$ on polünoomi

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

pealiikme kordaja a_0 positiivne, sest vastasel korral võiksime selle võrrandi mõlemaid pooli korrutada -1-ga. Et vaadeldav võrrand omaks üldse positiivseid lahendeid, peab vähemalt üks tema kordajaist olema negatiivne. Olgu a_k pealiikme poolt arvates esimene negatiivne kordaja ja A negatiivsete kordajate suurim absoluutväärtus. Positiivsete lahendite ülemine tõke λ on siis antud Maclaurin'i valemiga

$$\lambda = 1 + \sqrt[k]{\frac{A}{a_0}}.$$

Maclaurini valemi tõestuseks vaatleme ühest suuremaid x-i väärtusi. Asendades iga kordaja $a_1, a_2, \ldots, a_{k-1}$ nulliga ja iga

kordaja a_k, a_{k+1}, ..., a_n suurusega $-A$, võib polünoomi $f(x)$ väärtus vaid kahaneda, s. o.

$$f(x) \geqslant a_0x^n - A(x^{n-k} + x^{n-k-1} + \ldots + x + 1) =$$

$$= a_0x^n - A\frac{x^{n-k+1}-1}{x-1} = a_0x^n - A\frac{x^{n-k+1}}{x-1} + \frac{A}{x-1}.$$

Et aga $x > 1$ tõttu $\frac{A}{x-1} > 0$, siis

$$f(x) > a_0x^n - A\frac{x^{n-k+1}}{x-1} = \frac{x^{n-k+1}}{x-1}[a_0x^{k-1}(x-1) - A],$$

kust $x > x - 1$ tõttu

$$f(x) > \frac{x^{n-k+1}}{x-1}[a_0(x-1)^k - A].$$

Seega ei saa olla võrrandi $f(x) = 0$ lahenditeks need x-i väärtused, mille puhul

$$a_0(x-1)^k - A \geqslant 0$$

ehk

$$x \geqslant 1 + \sqrt[k]{\frac{A}{a_0}},$$

millest nähtubki, et siin $\lambda = 1 + \sqrt[k]{\frac{A}{a_0}}$ on positiivsete lahendite ülemiseks tõkkeks.

2^0 Et saada teist menetlust võrrandi $f(x) = 0$ positiivsete lahendite ülemise tõkke leidmiseks, vaatleme algul erijuhtu, kus polünoomis $f(x)$ on kõik esimesed kordajad pealiikme kordajast alates mittenegatiivsed ja kõik viimased kordajad mittepositiivsed, s. o.

$$(11) \qquad f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{k-1}x^{n-k+1} - a_kx^{n-k} - a_{k+1}x^{n-k-1} - \ldots - a_n,$$

kus $a_i \geqslant 0$, $i = 0, 1, 2, \ldots, n$. Ei ole raske näha, et kui siin polünoom $f(x)$ omab kohal $\lambda > 0$ mittenegatiivset väärtust,

siis kujutab λ võrrandi $f(x) = 0$ positiivsete lahendite ülemist tõket. Selleks tarvitseb vaid $f(x)$ esitada kujul

$$f(x) = x^{n-k+1}\left[(a_0x^{k-1} + a_1x^{k-2} + \ldots + a_{k-1}) - \right.$$

$$\left. -\left(\frac{a_k}{x} + \frac{a_{k+1}}{x^2} + \ldots + \frac{a_n}{x^{n-k+1}}\right)\right],$$

kust ilmneb, et $f(x)$ kujutab $x > 0$ puhul kasvavat funktsiooni, sest $x > 0$ kasvamisel avaldis esimestes ümarsulgudes kasvab, avaldis teistes ümarsulgudes aga kahaneb. Seega kui $f(\lambda) \geqslant 0$, siis ammugi

$$f(x) > 0, \text{ kui } x > \lambda,$$

millest nähtubki, et λ on positiivsete lahendite ülemiseks tõkkeks.

Kui nüüd $f(x)$ ei oma kuju (11), siis võib teda liikmete rühmitamise teel alati esitada summana

$$f(x) = f_1(x) + f_2(x) + \ldots + f_r(x),$$

kus iga polünoom $f_i(x)$ omab kuju (11). Kui siin polünoomid $f_1(x)$, $f_2(x)$, ..., $f_r(x)$ on kõik kohal $\lambda > 0$ mittenegatiivsed, siis kujutabki λ võrrandi $f(x) = 0$ positiivsete lahendite ülemist tõket.

Viimati antud menetlust on soovitav kasutada Maclaurini valemiga leitud tõkete koomale surumiseks.

N ä i d e 4. Leida võrrandi

$$2x^5 - 10x^3 + 10x + 3 = 0$$

positiivsete ja negatiivsete lahendite tõkked.

1° Rakendades Maclaurini menetlust, leiame kõigepealt positiivsete lahendite ülemise tõkke λ valemist

$$\lambda = 1 + \sqrt[k]{\frac{A}{a_0}}.$$

Et antud juhul $a_0 = 2$, $k = 2$, $A = 10$, siis on

$$\lambda = 1 + \sqrt{5} < 4.$$

Leides samal viisil võrrandite

$$x^5 f\left(\frac{1}{x}\right) = 3x^5 + 10x^4 - 10x^2 + 2 = 0$$

$$x^5 f\left(-\frac{1}{x}\right) = 3x^5 - 10x^4 + 10x^2 - 2 = 0$$

$$f(-x) = 2x^5 - 10x^3 + 10x - 3 = 0$$

positiivsete lahendite ülemised tõkked λ_1, λ_2, λ_3, saame

$$\lambda_1 = 1 + \sqrt[3]{\frac{10}{3}} < 3, \quad \lambda_2 = 1 + \frac{10}{3} < 5, \quad \lambda_3 = 1 + \sqrt{5} < 4,$$

kust

$$\frac{1}{\lambda_1} > \frac{1}{3}, \quad -\frac{1}{\lambda_2} < -\frac{1}{5}, \quad -\lambda_3 > -4.$$

Seega asetsevad antud võrrandi positiivsed lahendid vahemikus $\left(\frac{1}{3}, 4\right)$ ja negatiivsed lahendid vahemikus $\left(-4, -\frac{1}{5}\right)$.

2^0 Teise menetluse rakendamiseks anname polünoomile $f(x) = 2x^5 - 10x^3 + 10x + 3$ kuju

$$f(x) = f_1(x) + f_2(x),$$

kus $f_1(x) = 2x^5 - 10x^3$, $f_2(x) = 10x + 3$. Et siin $f_1(3) > 0$, $f_2(3) > 0$, siis võib võtta $\lambda = 3$. Analoogiliselt leiame kergesti

$$\lambda_1 = 1, \quad \lambda_2 = 4, \quad \lambda_3 = 3,$$

kust

$$\frac{1}{\lambda_1} = 1, \quad -\frac{1}{\lambda_2} = -\frac{1}{4}, \quad -\lambda_3 = -3.$$

Seega oleme saanud positiivsete lahendite jaoks vahemiku $(1, 3)$ ja negatiivsete lahendite jaoks vahemiku $\left(-3, -\frac{1}{4}\right)$, mis on kitsamad kui Maclaurini valemiga leitud vahemikud.

Tuleb silmas pidada, et eespool antud võtted algebralise võrrandi reaallahendite tõkete leidmiseks ei määra leitud tõkete vahel asetsevate reaallahendite arvu ega garanteeri üldse reaallahendite olemasolu nende tõkete vahel, püstitades vaid formaalsed tõkked reaallahenditele. Kuid on olemas ka menetlused, mis

lubavad määrata reaallahendite arvu mistahes vahemikus ja mis võimaldavad lõppeks üksikuid reaallahendeid eraldada — sulgeda igaühte neist kindlasse vahemikku. Ühe niisuguse menetlusega tutvumegi järgnevas artiklis.

2. **Sturm'i lause.** Vaatleme võrrandit

$$f(x) = 0,$$

kust olgu kordsed lahendid eraldatud (§ 7, art. 3), nii et $f(x)$ ja $f'(x)$ on ühistegurita, s. o. $(f, f') = 1$. Rakendame polünoomidele $f(x)$ ja $f'(x)$ Eukleidese algoritmi, kusjuures korrutame aga pärast iga jagamist jääki -1-ga, nii et kui jagades näiteks polünoomi $f(x)$ tuletisega $f'(x)$ saame jäägi $r_1(x)$, siis vaatleme selle asemel polünoomi $f_1(x) = -r_1(x)$ jne. Sel viisil saame seosed

$$\begin{aligned} f(x) &= q_1(x) f'(x) \quad - f_1(x) \\ f'(x) &= q_2(x) f_1(x) \quad - f_2(x) \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ f_{k-2}(x) &= q_k(x) f_{k-1}(x) - f_k(x), \end{aligned} \tag{12}$$

kus $f_k(x)$ kujutab $f(x)$ ja $f'(x)$ suurimat ühistegurit, s. o. konstanti. Siin polünoomid

$$f(x),\ f'(x),\ f_1(x),\ f_2(x),\ \ldots,\ f_k(x)$$

moodustavad nn. S t u r m i a h e l i k u, mille puhul paneme tähele järgmist kahte omadust:

1° Sturmi ahelikus on kõrvuti asetsevad polünoomid $f_i(x)$ ja $f_{i+1}(x)$ ühistegurita;

2° kui ξ on Sturmi aheliku mingi seesmise polünoomi $f_i(x)$ nullkoht, siis omavad $f_{i-1}(\xi)$ ja $f_{i+1}(\xi)$ vastupidiseid märke.

1° Tõepoolest, kui polünoomid $f_i(x)$ ja $f_{i+1}(x)$ omaksid ühistegurit, siis peaks seose

$$f_{i-1}(x) = q_{i+1}(x) f_i(x) - f_{i+1}(x) \tag{13}$$

tõttu ka $f_{i-1}(x)$ jaguma selle teguriga, siis aga peaks seosele (13) eelneva seose

$$f_{i-2}(x) = q_i(x) f_{i-1}(x) - f_i(x)$$

tõttu ka $f_{i-2}(x)$ jaguma selle teguriga jne. Minnes sel viisil võrduste ahelikus (12) samm-sammult ülespoole, järeldaksime lõppeks, et $f(x)$ ja $f'(x)$ peaksid omama ühistegurit, vastupidi eeldusele.

2^0 Võttes seoses (13) $x = \xi$, saame $f_i(\xi) = 0$ tõttu

$$f_{i-1}(\xi) = -f_{i+1}(\xi).$$

Et 1^0 järgi $f_i(x)$ ja $f_{i+1}(x)$ ei või omada ühistegurit, siis on $f_{i+1}(\xi) \neq 0$, nii et $f_{i-1}(\xi)$ ja $f_{i+1}(\xi)$ omavad tõesti vastupidiseid märke.

Vaatleme nüüd Sturmi polünoomide väärtusi

$$f(\xi),\ f'(\xi),\ f_1(\xi),\ f_2(\xi),\ \ldots,\ f_k(\xi) \tag{14}$$

mingil kohal ξ. Kustutades siin kõik need väärtused, mis osutuvad nullideks, ütleme, et ahelikus (14) esineb m ä r g i m u u t, kui selles ahelikus kaks naaberväärtust on vastupidiste märkidega. Kõigi märgimuutude arvu ahelikus (14) tähistame $m(\xi)$-ga. Olgu (a, b) mingi vahemik. Sellesse vahemikku langevate võrrandi $f(x) = 0$ reaallahendite arvu määrab järgmine Sturmi poolt 1829. a. tõestatud tähelepandav lause, mis tõi oma autorile suure populaarsuse.

T e o r e e m 2. *Võrrandi $f(x) = 0$ reaallahendite arv vahemikus (a, b) on võrdne märgimuutude arvude vahega $m(a) - m(b)$ polünoomi $f(x)$ Sturmi ahelikus.*

Teoreemi 2 tõestuseks vaatleme kõigepealt Sturmi aheliku mingi seesmise polünoomi $f_i(x)$ nullkohta ξ. Siis on 2^0 järgi $f_{i-1}(\xi)$ ja $f_{i+1}(\xi)$ vastupidiste märkidega. Valime nii väikese ξ ümbruse $(\xi - \delta,\ \xi + \delta)$, et $f_{i-1}(x)$ ja $f_{i+1}(x)$ säilitaks selles ümbruses oma märki, kusjuures olgu näiteks $f_{i-1}(x) < 0$ ja seega $f_{i+1}(x) > 0$. Nagu nähtub vastavast märkide tabelist

x	$f_{i-1}(x)$	$f_i(x)$	$f_{i+1}(x)$	$m(x)$
$x < \xi$	$-$		$+$	1
$x > \xi$	$-$		$+$	1

,

on $f_i(x)$ nullkoha ξ ümbruses polünoomide $f_{i-1}(x)$, $f_i(x)$, $f_{i+1}(x)$ vahel tekkinud märgimuutude arv alati 1, sõltumata sellest, missugused märgid asetada $f_i(x)$ lahtrisse, s. o. sõltumata $f_i(x)$ märgist enne ja pärast nullkohta ξ. Seega kui x läbib Sturmi aheliku seesmise polünoomi $f_i(x)$ nullkohta, jääb üldine märgimuutude arv Sturmi ahelikus muutumatuks [1], mistõttu selles märgimuutude arvus võib tekkida muudatus vaid siis, kui x läbib $f(x)$ nullkohta, sest $f_k(x)$ kui nullist erinev konstant ei oma nullkohta.

Olgu seepärast ξ polünoomi $f(x)$ nullkoht, s. o. $f(\xi) = 0$. Et eelduse järgi kordsed lahendid on eraldatud, siis $f'(\xi) \neq 0$. Seetõttu võime valida ξ ümbruse $(\xi - \delta, \xi + \delta)$ nii väikese, et $f'(x)$ säilitaks seal oma märki ja et sellesse ümbrusse ei langeks teisi $f(x)$ nullkohti peale ξ. Olgu ümbruses $(\xi - \delta, \xi + \delta)$ näiteks $f'(x) > 0$; siis x-i kasvades $f(x)$ kasvab, minnes $f(\xi) = 0$ tõttu negatiivsetelt väärtustelt üle positiivsetele. Vastavast märkide tabelist

x	$f(x)$	$f'(x)$	$m(x)$
$x < \xi$	$-$	$+$	1
$x > \xi$	$+$	$+$	0

nähtub, et kui x läbib kasvades polünoomi $f(x)$ nullkohta, siis kahaneb märgimuutude arv $f(x)$ ja $f'(x)$ vahel ühe võrra [2]. Seega määrab märgimuutude arvude vahe $m(a) - m(b)$ tõesti võrrandi reaallahendite arvu vahemikus (a, b).

Osates leida võrrandi reaallahendite arvu antud vahemikus, võime asuda nende lahendite eraldamisele, s. o. niisuguste vahemike leidmisele, milles asetseks igaühes ainult üks lahend. Selleks tarvitseb vaid lähtevahemikku niikaua alajaotada, kuni igasse osavahemikku langeb ülimalt üks lahend.

---

[1] See kehtib ka juhul $f_{i-1}(x) > 0$.

[2] See kehtib ka juhul $f'(x) < 0$.

N ä i d e 5. Eraldada võrrandi

$$2x^5 - 10x^3 + 10x + 3 = 0$$

reaallahendid.

Märkides $f(x) = 2x^5 - 10x^3 + 10x + 3$, leiame

$$f'(x) = 10x^4 - 30x^2 + 10 .$$

Et Sturmi aheliku moodustamisel võib niihästi jagatavat kui ka jagajat korrutada mistahes positiivse teguriga, siis võtame $f'(x)$ asemel polünoomi $x^4 - 3x^2 + 1$. Rakendades Eukleidese algoritmi, saame jäägi märki igakord vastupidiseks muutes:

$$\begin{array}{rrrrrr|rrrrr}
 & & & & & & 2 & 0 & -10 & 0 & 10 & 3 & 1 & 0 & -3 & 0 & 1 \\
 & & & & & & 2 & 0 & -6 & 0 & 2 & & 2 & & & & \\
\hline
 & & & & & & & & -4 & 0 & 8 & 3 & & & & & \\
 & & & 4 & 0 & -12 & 0 & 4 & 4 & 0 & -8 & -3 & & & & & \\
 & & & 4 & 0 & -8 & -3 & & 1 & & & & & & & & \\
\hline
 & & & & & -4 & 3 & 4 & & & & & & & & & \\
 & 4 & 0 & -8 & -3 & 4 & -3 & -4 & & & & & & & & & \\
 & 4 & -3 & -4 & & 1 & (3) & & & & & & & & & & \\
\hline
 & & 3 & -4 & -3 & & & & & & & & & & & & \\
 & & 12 & -16 & -12 & & & & & & & & & & & & \\
 & & 12 & -9 & -12 & & & & & & & & & & & & \\
\hline
 & & & -7 & 0 & & & & & & & & & & & & \\
4 & -3 & -4 & 1 & 0 & & & & & & & & & & & & \\
4 & 0 & & 4 & -3 & & & & & & & & & & & & \\
\hline
 & -3 & -4 & & & & & & & & & & & & & & \\
 & -3 & 0 & & & & & & & & & & & & & & \\
\hline
 & & -4 & & & & & & & & & & & & & & \\
 & & 1 . & & & & & & & & & & & & & &
\end{array}$$

Seega on meil

$$f_1(x) = 4x^3 - 8x - 3$$
$$f_2(x) = 4x^2 - 3x - 4$$
$$f_3(x) = x$$
$$f_4(x) = 1 .$$

Silmas pidades, et näite 4 järgi vaadeldava võrrandi reaallahendid asetsevad vahemikes $\left(-3, -\frac{1}{4}\right)$ ja $(1, 3)$, koostame järgmise märkide tabeli:

x	$f(x)$	$f'(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$m(x)$
-3	$-$	$+$	$-$	$+$	$-$	$+$	5
-2	$-$	$+$	$-$	$+$	$-$	$+$	5
-1	$+$	$-$	$+$	$+$	$-$	$+$	4
$-\frac{1}{2}$	$-$	$+$	$-$	$-$	$-$	$+$	3
0	$+$	$+$	$-$	$-$	0	$+$	2
1	$+$	$-$	$-$	$-$	$+$	$+$	2
$\frac{3}{2}$	$-$	$-$	$+$	$+$	$+$	$+$	1
2	$+$	$+$	$+$	$+$	$+$	$+$	0

Tabelist nähtub, et antud võrrandil on 5 reaallahendit, mis asetsevad vastavalt vahemikes $(-2, -1)$, $\left(-1, -\frac{1}{2}\right)$, $\left(-\frac{1}{2}, -\frac{1}{4}\right)$, $\left(1, \frac{3}{2}\right)$ ja $\left(\frac{3}{2}, 2\right)$.

3. **Descartes'i reegel.** Et Sturmi aheliku koostamine on sageli praktikas suure ajakulutusega seotud, siis on antud rida praktiliselt kergemini rakendatavaid menetlusi, mis aga ei lahenda reaallahendite arvu küsimust ammendavalt, määrates üldiselt vaid maksimaalse reaallahendite arvu. Neist menetlustest lihtsaim on alljärgnev Descartes'i reegel.

Teoreem 3. *Võrrandi*

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0$$

positiivsete lahendite arv, loendatud vastavalt iga lahendi

kordsusele, on kas võrdne märgimuutude arvuga selle võrrandi kordajate jadas

$$a_0,\ a_1,\ \ldots,\ a_{n-1},\ a_n$$

või on sellest arvust paarisarvu võrra väiksem.

Mis puutub negatiivsete lahendite arvusse, siis tarvitseb selle leidmiseks rakendada vaid Descartes'i reeglit võrrandile

$$a_0(-x)^n + a_1(-x)^{n-1} + \ldots + a_{n-1}(-x) + a_n = 0.$$

Nii ütleb Descartes'i reegel, et näiteks võrrand

$$2x^5 - 10x^3 + 10x + 3 = 0$$

omab 2 või 0 positiivset lahendit ja 3 või 1 negatiivset lahendit, kooskõlas näite 5 tulemusega.

Erijuhul, kui võrrandi kordajate jadas esineb üksainus märgimuut, on sellel võrrandil Descartes'i reegli järgi parajasti üks positiivne reaallahend, nagu näiteks võrrandil $x^5 - 4x - 2 = 0$.

Teoreemi 3 tõestuseks näitame kõigepealt, et võrrandi $f(x) = 0$ positiivsete lahendite arv võib erineda selle võrrandi kordajate jada märgimuutude arvust m vaid paarisarvu poolest. Et meid ei huvita siin null-lahendid, siis võime üldsust kitsendamata eeldada, et $a_n \neq 0$. Vaatleme kahte juhtu selle järgi, kas m on paaris- või paaritu arv.

Kui m on paarisarv, siis peavad a_0 ja a_n olema sama märgiga, sest vastasel korral oleks võrrandi $f(x) = 0$ kordajate jadas

$$a_0,\ a_1,\ \ldots,\ a_{n-1},\ a_n$$

paaritu arv märgimuute. Et

$$\lim_{x \to +\infty} f(x) = \lim_{x \to +\infty} x^n \left(a_0 + \frac{a_1}{x} + \ldots + \frac{a_n}{x^n}\right) =$$

$$= \lim_{x \to +\infty} a_0 x^n = \begin{cases} +\infty, & \text{kui } a_0 > 0 \\ -\infty, & \text{kui } a_0 < 0, \end{cases}$$

siis omab $f(x)$ küllalt suure $x = b$ $(b > 0)$ puhul sama märki mis a_0 ja seega ka sama märki mis a_n. Kuid $a_n = f(0)$, nii et $f(0)$ ja $f(b)$ omavad sama märki, mistõttu vahemikus $(0, b)$ võib asetseda vaid paarisarv võrrandi $f(x) = 0$ lahendeid. Seega on võrrandil $f(x) = 0$ paarisarvulise m puhul ka paarisarv positiivseid lahendeid.

Kui aga m on paaritu arv, siis peavad a_0 ja a_n olema vastupidiste märkidega, sest vastasel korral oleks võrrandi $f(x)$ kordajate jadas paarisarv märgimuute. Seega omavad nüüd $f(0)$ ja $f(b)$ küllalt suure $b > 0$ puhul vastupidiseid märke, mistõttu vahemikus $(0, b)$ võib asetseda vaid paaritu arv võrrandi $f(x) = 0$ lahendeid. Seega on võrrandil $f(x) = 0$ paarituarvulise m puhul ka paaritu arv positiivseid lahendeid.

Jääb vaid näidata, et võrrandi $f(x) = 0$ positiivsete lahendite arv ei saa ületada selle võrrandi kordajate jada märgimuutude arvu m. Kasutame tõestuseks täieliku induktsiooni printsiipi. Nimelt on esimese astme võrrandi

$$a_0 x + a_1 = 0$$

puhul Descartes'i reegel ilmselt kehtiv, sest siin on ainuke olemasolev lahend $-\frac{a_1}{a_0}$ positiivne siis ja ainult siis, kui a_0 ja a_1 on vastupidiste märkidega, s. o. kui võrrandi kordajate jadas

$$a_0, \; a_1$$

esineb üks märgimuut. Oletades nüüd, et Descartes'i reegel on kehtiv iga $(n-1)$-astme võrrandi puhul näitame, et see reegel jääb kehtima ka iga n-astme võrrandi puhul. Vaatleme selleks võrrandit $f'(x) = 0$. Siin kordajate jadas

$$na_0, \; (n-1)a_1, \; \ldots, \; a_{n-1}$$

on ülimalt m märgimuutu. Et võrrandi $f'(x) = 0$ aste on $n-1$, siis on selle võrrandi puhul Descartes'i reegel induktsiooni oletuse kohaselt kehtiv, mistõttu on võrrandil $f'(x) = 0$ ülimalt m positiivset lahendit. Matemaatilise analüüsi kursusest tuntud

Rolle'i teoreemi järgi peab aga võrrandi $f(x) = 0$ iga kahe lahendi vahel asetsema vähemalt üks võrrandi $f'(x) = 0$ lahend. Seega omab võrrand $f(x) = 0$ ülimalt $m + 1$ positiivset lahendit. Kuid, nagu nägime, võib võrrandi $f(x) = 0$ positiivsete lahendite arv erineda selle võrrandi kordajate jada märgimuutude arvust m vaid paarisarvu poolest, mistõttu võrrand ei saa omada $m + 1$ positiivset lahendit ja võib seega omada ülimalt m positiivset lahendit.

4. Newtoni menetlus. Sturmi meetod lubab eraldada võrrandi $f(x) = 0$ reaallahendid, s. o. anda iga reaallahendi ξ jaoks vahemiku (a, b), millesse langeb ainult see lahend, nii et $a < \xi < b$. Siin a on ξ lähisväärtus puuduga ja b lähisväärtus liiaga, kusjuures need lähisväärtused kujutavad lahendit ξ veaga, mis on absoluutselt väiksem kui $b - a$. Silmas pidades reaalarvu mõistet kui lõiget ratsionaalarvude vallas (I, § 4, art. 2), mõistame reaallahendi ξ numbrilise arvutamise all niisuguste ratsionaalsete lähisväärtuste a_n ja b_n leidmist, mille puhul $a_n < \xi < b_n$ ja $b_n - a_n < \varepsilon$, kus ε tähendab etteantud positiivset suurust — lähisväärtuste absoluutse vea ülemmäära. Võrrandi reaallahendite numbriliseks arvutamiseks on olemas terve hulk meetodeid. Neist paistab silma oma teoreetilise lihtsuse ja üldsuse poolest Newtoni menetlus[1], millega tutvume üksikasjalisemalt käesolevas artiklis.

Olgu a võrrandi $f(x) = 0$ lahendi ξ lähisväärtus. Rakendades polünoomile $f(x)$ Taylori arendist kohal a (§ 7, art. 2), saame

$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \ldots + \frac{f^{(n)}(a)}{n!}(x-a)^n.$$

Et $f(\xi) = 0$, siis

$$f(a) + \frac{f'(a)}{1!}(\xi-a) + \frac{f''(a)}{2!}(\xi-a)^2 + \ldots + \frac{f^{(n)}(a)}{n!}(\xi-a)^n = 0.$$

[1] Newtoni menetlus on rakendatav ka transtsendentsete võrrandite puhul.

Kui $\xi - a$ on niivõrd väike, et tema kõrgemad astmed ei tule antud täpsuse piirides arvesse, siis on

$$f(a) + f'(a)(\xi - a) \approx 0,$$

millest

$$\xi \approx a - \frac{f(a)}{f'(a)}.$$

Siin suurus

$$a_0 = a - \frac{f(a)}{f'(a)} \tag{15}$$

kujutab lahendi ξ lähisväärtust. Nagu edaspidi näeme, osutub a_0 teatavatel tingimustel, mis on esmakordselt fikseeritud Fourier' poolt, paremaks lähendiks kui a. Olukorra selgitamiseks interpreteerime algul valemit (15), mis kannab Newtoni lähendusvalemi nime, geomeetriliselt. Vaatleme selleks polünoomi $f(x)$ graafiku tükki AB Cartesiuse ristkoordinaadistikus ja leiame punkti, kus sellele graafikule kohal $A = (a, f(a))$ võetud puutuja lõikab esimest koordinaaditelge (joonised 8 ja 9). Selle puutuja võrrand on

$$y - f(a) = f'(a)(x - a).$$

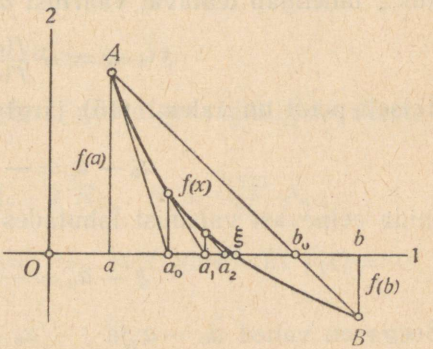
Võttes siin $y = 0$, saame otsitava lõikepunkti jaoks

$$x = a - \frac{f(a)}{f'(a)},$$

mis kujutabki valemiga (15) antud lähendit a_0. Joonisel 8 määrab valem (15) parema lähendi kui a, joonisel 9 aga halvema.

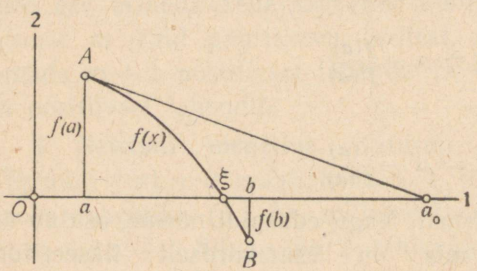
Tekib küsimus, missugustel tingimustel kujutab a_0 paremat lähendit kui a.

Kõigepealt võib üldsust kitsendamata eeldada, et $f'(\xi) \neq 0$ ja $f''(\xi) \neq 0$, sest vastasel korral võik-



Joonis 8.

sime ξ leidmiseks vaadelda võrrandi $f(x)=0$ asemel madalama astme võrrandit $f'(x)=0$ või $f''(x)=0$. Peale selle eeldame, et lõik $[a, b]$ mitte ainult ei sisalda ühtki teist võrrandi $f(x)=0$ lahendit peale ξ, vaid et selles lõigus ei leidu ka ühtki $f'(x)=0$ ja $f''(x)=0$ lahendit. Siis on eriti $f'(a)\neq 0$, nii et valem (15) omab mõtet. Ühtlasi on ilmne, et tehtud eeldustel muutub $f(x)$ monotoonselt lõigus $[a, b]$, omades selle lõigu otspunktides väärtusi $f(a)$ ja $f(b)$, mis on $f(\xi)=0$ tõttu vastupidiste märkidega. Et seejuures $f''(x)$ säilitab oma märki, siis omavad $f(x)$ ja $f''(x)$ lõigu $[a, b]$ ühes otspunktis samamärgilisi, teises otspunktis aga vastandmärgilisi väärtusi. Kui nüüd a tähendab seda otspunkti, kus $f(x)$ ja $f''(x)$ omavad samamärgilisi väärtusi, siis saab näidata, et a_0 kujutab ξ jaoks paremat lähendit kui a.



Joonis 9.

Tõepoolest, kasutades matemaatilise analüüsi kursusest tuntud Taylori arendise jääkliiget, võime kirjutada

$$f(\xi)=f(a)+\frac{f'(a)}{1!}(\xi-a)+R_1, \quad R_1=\frac{f''(\zeta)}{2!}(\xi-a)^2,$$

kus ζ tähendab teatavat väärtust a ja ξ vahel. Et $f(\xi)=0$, siis

$$\xi-a=-\frac{f(a)}{f'(a)}-\frac{R_1}{f'(a)}.$$

Teiselt poolt on valemi (15) järgi

$$a_0-a=-\frac{f(a)}{f'(a)},$$

mida eelnevast valemist lahutades leiame

$$\xi-a_0=-\frac{R_1}{f'(a)}.$$

Seega on vahed a_0-a ja $\xi-a_0$ eelduse tõttu samamärgilised, millest kergesti nähtub, et a_0 asetseb a ja ξ vahel (joonis 8).

Võttes nüüd Newtoni lähendusvalemis a asemel lähteväärtuseks parema lähendi a_0, saame uue lähendi

$$a_1 = a_0 - \frac{f(a_0)}{f'(a_0)},$$

mis on omakorda parem kui a_0, sest $f(a_0)$ ja $f''(a_0)$ on ühesuguste märkidega. Rakendades Newtoni lähendusvalemit lähendile a_1, saame veel parema lähendi

$$a_2 = a_1 - \frac{f(a_1)}{f'(a_1)}$$

jne. Sel viisil tekib lähendite jada

$$a_0, a_1, a_2, \ldots, a_{n-1}, a_n, \ldots,$$

kus

$$a_n = a_{n-1} - \frac{f(a_{n-1})}{f'(a_{n-1})} \tag{16}$$

ja iga lähend on parem eelnevast. Näitame, et selle jada piirväärtuseks on ξ, s. o.

$$\lim_{n \to \infty} a_n = \xi,$$

missugune asjaolu võimaldab arvutada reaallahendit ξ mistahes etteantud täpsusega.

Märkides $\xi - a_n = \eta_n$ ja analoogiliselt $\xi - a_{n-1} = \eta_{n-1}$, leiame

$$\eta_n = \eta_{n-1} - (a_n - a_{n-1}). \tag{17}$$

Teiselt poolt, kasutades Taylori arendise jääkliiget, võime kirjutada

$$f(\xi) = f(a_{n-1}) + \frac{f'(a_{n-1})}{1!}\eta_{n-1} + R_1, \quad R_1 = \frac{f''(\zeta)}{2!}\eta^2_{n-1},$$

kus ζ tähendab teatavat väärtust a_{n-1} ja ξ vahel. Et $f(\xi) = 0$, siis

$$\eta_{n-1} = -\frac{f(a_{n-1})}{f'(a_{n-1})} - \frac{R_1}{f'(a_{n-1})},$$

millest (16) tõttu

$$\eta_{n-1} = a_n - a_{n-1} - \frac{R_1}{f'(a_{n-1})}$$

ja lõppeks (17) tõttu

$$\eta_n = -\frac{R_1}{f'(a_{n-1})}.$$

Silmas pidades jääkliikme R_1 avaldist, saame

$$|\eta_n| = \frac{|f''(\zeta)|}{2|f'(a_{n-1})|}\eta^2_{n-1}.$$

Olgu lõigus $[a, b]$ $|f'(x)| > A$, $|f''(x)| < B$. Siis märkides $\frac{B}{2A} = M$ leiame

(18) $$|\eta_n| < M\eta^2_{n-1}.$$

Nüüd on aga ka

$$|\eta_{n-1}| < M\eta^2_{n-2}, |\eta_{n-2}| < M\eta^2_{n-3}, \ldots, |\eta_1| < M\eta_0{}^2$$

ja seega

$$|\eta_n| < M^3\eta^4_{n-2} < M^7\eta^8_{n-3} < \ldots < M^{2^n-1}\eta_0{}^{2^n}.$$

Kuid $|\eta_0| = |\xi - a_0| < |b - a|$, mistõttu

$$|\eta_n| < M^{2^n-1}|b - a|^{2^n}.$$

Olgu nüüd lõik $[a, b]$ küllalt väike, nii et

$$M|b - a| < 1.$$

Siis $\lim_{n\to\infty} \eta_n = 0$ ja seega

$$\lim_{n\to\infty} a_n = \xi.$$

Kui valemis (18) $M \leqslant 1$, siis $|\eta_n| < \eta^2_{n-1}$, millest nähtub, et kui lähend a_{n-1} sisaldab k õiget kümnendkohta, siis järgmine lähend a_n sisaldab juba $2k$ õiget kümnendkohta. Viimane asjaolu lubab orienteeruvalt hinnata Newtoni menetlusega saavu-

tatava lähendi täpsust. Vastavalt sellele on soovitav võtta otsitava lahendi esimene lähisväärtus võimalikult vähemalt täpsusega 0,1. Vajalikke polünoomi väärtuste arvutusi on kohane teostada Horneri skeemi abil.

Näide 6. Arvutada võrrandi

$$2x^5 - 10x^3 + 10x + 3 = 0$$

lahend, mis asetseb vahemikus $\left(-\frac{1}{2}, -\frac{1}{4}\right)$, veaga alla 10^{-7}.

Antud juhul on

$$f(x) = 2x^5 - 10x^3 + 10x + 3$$
$$f'(x) = 10(x^4 - 3x^2 + 1)$$
$$f''(x) = 20x(2x^2 - 3),$$

kusjuures, nagu kerge on veenduda, $f''(x) > 0$ lõigul $\left[-\frac{1}{2}, -\frac{1}{4}\right]$. Et siin $f\left(-\frac{1}{4}\right) = 0{,}65 > 0$, siis tuleb Newtoni menetluse rakendamiseks võtta lähteväärtuseks $-\frac{1}{4}$. Nüüd on aga $f'\left(-\frac{1}{4}\right) = 8{,}1$ ja seega valemi (15) järgi

$$a_0 = -\frac{1}{4} - \frac{0{,}65}{8{,}1} = -0{,}25 - 0{,}08 = -0{,}33,$$

mis on parem lähend kui $-\frac{1}{4}$. Võttes uueks lähteväärtuseks $-0{,}33$, leiame

$$f(-0{,}33) = 0{,}0515, \quad f'(-0{,}33) = 6{,}85$$

ja seega

$$a_1 = -0{,}33 - \frac{0{,}0515}{6{,}85} = -0{,}33 - 0{,}0076 = -0{,}3376,$$

mis on parem lähend kui $a_0 = -0{,}33$. Ühtlasi nähtub siit, et lähendis a_0 olid mõlemad kümnendkohad õiged. Võttes lõppeks lähteväärtuseks $-0{,}3376$, leiame

$$f(-0{,}3376) = 0{,}00000453, \quad f'(-0{,}3376) = 6{,}71$$

ja seega

$$a_2 = -0{,}3376 - \frac{0{,}00000453}{6{,}71} = -0{,}3376 - 0{,}00000067 =$$
$$= -0{,}33760067,$$

mis on parem lähend kui $a_1 = -0{,}3376$. Ühtlasi nähtub siit, et lähendis a_1 olid kõik neli kümnendkohta õiged, mistõttu võib oodata, et a_2 sisaldab 8 õiget kümnendkohta (antud juhul võiks arvutada a_2 koguni 12 kümnendkohaga, sest lähendi a_1 viga on tegelikult väiksem kui 10^{-6}). Seega on veaga alla 10^{-7}

$$\xi = -0{,}3376007 .$$

Vahel on kohane — eriti lähendi täpsuse hindamise mõttes — kasutada koos Newtoni menetlusega lineaarse interpolatsiooni võtet, mis oli tuntud juba vanadele egiptlastele ja mida nimetatakse sageli r e g u l a f a l s i nimega.

Olgu nimelt teada, et võrrandil $f(x) = 0$ on a ja b vahel üks harilik lahend ξ, nii et $f(a)$ ja $f(b)$ on vastupidiste märkidega. Leiame lineaarpolünoomi $g(x)$, mis omab kohtadel a ja b vastavalt väärtusi $f(a)$ ja $f(b)$. Newtoni interpolatsioonivalemi järgi on (§ 6, art. 2)

$$g(x) = c_0 + c_1(x - a),$$

kus

$$c_0 = f(a), \quad c_1 = \frac{f(b) - f(a)}{b - a}.$$

Vaatleme võrrandi $f(x) = 0$ lahendi ξ asemel võrrandi $g(x) = 0$, s. o. $c_0 + c_1(x - a) = 0$ lahendit

$$b_0 = a - \frac{c_0}{c_1} = a - \frac{f(a)}{\frac{f(b) - f(a)}{b - a}}$$

ehk

$$b_0 = a - \frac{(b - a)f(a)}{f(b) - f(a)}. \tag{19}$$

Ei ole raske näha, et b_0 asetseb alati a ja b vahel ning kujutab seega paremat lähendit kui a või b. Tõepoolest, kuna

$$b_0 - a = \frac{(a - b)f(a)}{f(b) - f(a)}$$

$$b - b_0 = \frac{(b - a)f(b)}{f(b) - f(a)},$$

aga $f(a)$ ja $f(b)$ on vastupidiste märkidega, siis on vahed $b_0 - a$ ja $b - b_0$ samamärgilised, mis ütlebki, et b_0 asetseb a ja b vahel.

Geomeetriliselt seisab lineaarse interpolatsiooni menetlus selles, et a ja b vahelises piirkonnas asendatakse polünoomi $f(x)$ graafik kõõluga AB, kus $A = (a, f(a))$, $B = (b, f(b))$ (joonis 8). Joonisest 8 nähtub, et kui Fourier tingimustel arvutatud Newtoni lähend a_0 kujutab ξ lähisväärtust puuduga, siis lineaarse interpolatsiooniga saadud lähend b_0 kujutab ξ lähisväärtust liiaga (ja ümberpöördult), nii et ξ jääb alati a_0 ja b_0 vahele.

Rakendame lineaarse interpolatsiooni menetlust näites 6 leitud viimase lähendi $a_2 = -0{,}33760067$ täpsuse hindamiseks. Vaatleme selleks eelmist lähendit $a_1 = -0{,}3376$, mis kujutab otsitava lahendi ξ lähisväärtust liiaga. Vastav lähisväärtus puuduga on $b_1 = -0{,}3377$, sest lähendis a_1 on kõik kümnendkohad õiged. Rakendades lähisväärtustele a_1 ja b_1 lineaarse interpolatsiooni menetlust, saame valemi (19) järgi lähendi

$$b_2 = a_1 - \frac{(b_1 - a_1) f(a_1)}{f(b_1) - f(a_1)} = -0{,}3376 - \frac{-0{,}0001 \cdot 0{,}00000453}{-0{,}000665 - 0{,}000005} =$$

$$= -0{,}3376 - \frac{0{,}00000453}{6{,}70} = -0{,}3376 - 0{,}00000068 = -0{,}33760068.$$

Seega on lähendi $a_2 = -0{,}33760067$ viga absoluutselt väiksem kui $|b_2 - a_2| = 10^{-8}$.

5. Lobatševski menetlus. Kui on vajalik arvutada võrrandi $f(x) = 0$ kõiki lahendeid, siis on kohane kasutada alljärgnevat menetlust, mille idee pärineb geniaalselt vene matemaatikult, mitte-eukleidilise geomeetria loojalt N. I. Lobatševski'lt. Kuigi Lobatševski menetlus on laiendatav ka komplekslahendite juhule, piirdume järgnevas juhuga, kus võrrandi $f(x) = 0$ lahendid $\xi_1, \xi_2, \ldots, \xi_n$ on kõik reaalsed ja üksteisest erinevad. Nummerdame need lahendid nii, et

$$|\xi_1| > |\xi_2| > \ldots > |\xi_n|.$$

Moodustame võrrandi $F(x) = 0$, mille lahenditeks on lahendite $\xi_1, \xi_2, \ldots, \xi_n$ k-ndad astmed $\xi_1^k, \xi_2^k, \ldots, \xi_n^k$. Olgu

$$F(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \sigma_3 x^{n-3} + \ldots + (-1)^n \sigma_n.$$

Siis on Vieta valemite järgi (§ 9, art. 3)

$$\sigma_1 = \xi_1^k + \xi_2^k + \ldots + \xi_n^k = \xi_1^k\left[1 + \left(\frac{\xi_2}{\xi_1}\right)^k + \ldots + \left(\frac{\xi_n}{\xi_1}\right)^k\right]$$

$$\sigma_2 = \xi_1^k\xi_2^k + \xi_1^k\xi_3^k + \ldots + \xi_{n-1}^k\xi_n^k = \xi_1^k\xi_2^k\left[1 + \left(\frac{\xi_3}{\xi_2}\right)^k + \right.$$

$$\left. + \ldots + \left(\frac{\xi_{n-1}}{\xi_1}\right)^k\left(\frac{\xi_n}{\xi_2}\right)^k\right]$$

(20)

$$\sigma_3 = \xi_1^k\xi_2^k\xi_3^k + \xi_1^k\xi_2^k\xi_4^k + \ldots + \xi_{n-2}^k\xi_{n-1}^k\xi_n^k =$$

$$= \xi_1^k\xi_2^k\xi_3^k\left[1 + \left(\frac{\xi_4}{\xi_3}\right)^k + \ldots + \left(\frac{\xi_{n-2}}{\xi_1}\right)^k\left(\frac{\xi_{n-1}}{\xi_2}\right)^k\left(\frac{\xi_n}{\xi_3}\right)^k\right]$$

. . . . . .

$$\sigma_n = \xi_1^k\xi_2^k \ldots \xi_n^k.$$

Et jagatised $\frac{\xi_2}{\xi_1}$, $\frac{\xi_3}{\xi_1}$, $\ldots$, $\frac{\xi_n}{\xi_{n-1}}$ on kõik absoluutselt väiksemad ühest, siis võime küllalt suure k korral valemeis (20) jätta ära liikmed, kus esinevad nende jagatiste k-ndad astmed, ja saame seega nõutava täpsuse piirides kehtivad seosed

$$\sigma_1 = \xi_1^k, \quad \sigma_2 = \xi_1^k\xi_2^k, \quad \sigma_3 = \xi_1^k\xi_2^k\xi_3^k, \quad \ldots, \quad \sigma_n = \xi_1^k\xi_2^k \ldots \xi_n^k,$$

kust jagades leiame

$$(21) \quad \xi_1^k = \sigma_1, \quad \xi_2^k = \frac{\sigma_2}{\sigma_1}, \quad \xi_3^k = \frac{\sigma_3}{\sigma_2}, \quad \ldots, \quad \xi_n^k = \frac{\sigma_n}{\sigma_{n-1}}.$$

Valemid (21) võimaldavad juurimise teel arvutada lahendite $\xi_1, \xi_2, \ldots, \xi_n$ absoluutväärtused nõutava täpsusega, kuid lahendite märgid tuleb määrata lihtsalt proovimise teel.

Jääb selgitada, kuidas leida polünoomi $F(x)$ kordajad $\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_n$. Neid kordajaid võiks arvutada üldise meetodiga nagu võrrandi $f(x) = 0$ lahendite sümmeetrilisi polünoome (§ 9, art. 3). Kuid hoopis kergemini jõuame sihile järgmisel teel. Vaadeldes kõigepealt juhtu $k = 2$, moodustame peale antud võrrandi $f(x) = 0$ ehk

$$x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = 0$$

veel võrrandi

$$x^n - a_1x^{n-1} + a_2x^{n-2} - \ldots + (-1)^n a_n = 0,$$

mille lahenditeks on $-\xi_1, -\xi_2, \ldots, -\xi_n$. Et

$$(x^n + a_1x^{n-1} + \ldots + a_n)(x^n - a_1x^{n-1} + \ldots + (-1)^n a_n) =$$
$$= (x - \xi_1)(x - \xi_2) \ldots (x - \xi_n)(x + \xi_1)(x + \xi_2) \ldots (x + \xi_n) =$$
$$= (x^2 - \xi_1^2)(x^2 - \xi_2^2) \ldots (x^2 - \xi_n^2),$$

siis, märkides viimases korrutises $x^2 = y$, saame n-astme võrrandi

$$F_1(y) = 0,$$

mille lahenditeks on $\xi_1^2, \xi_2^2, \ldots, \xi_n^2$, kusjuures ei ole raske näha, et

$$F_1(y) = y^n - (a_1^2 - 2a_2)y^{n-1} + (a_2^2 - 2a_1a_3 + 2a_4)y^{n-2} -$$
$$- (a_3^2 - 2a_2a_4 + 2a_1a_5 - 2a_6)y^{n-3} + \ldots .$$

Seega on juhul $k = 2$

$$\sigma_1 = a_1^2 - 2a_2, \quad \sigma_2 = a_2^2 - 2a_1a_3 + 2a_4, \tag{22}$$
$$\sigma_3 = a_3^2 - 2a_2a_4 + 2a_1a_5 - 2a_6, \ldots .$$

Rakendades sama võtet võrrandile $F_1(y) = 0$, saame võrrandi $F_2(z) = 0$, mille lahenditeks on antud võrrandi $f(x) = 0$ lahendite 4-ndad astmed. Võrrandist $F_2(z) = 0$ saame omakorda võrrandi, mille lahenditeks on võrrandi $f(x) = 0$ lahendite 8-ndad astmed jne. Arvutusi kordajate $\sigma_1, \sigma_2, \ldots, \sigma_n$ leidmiseks on otstarbekas teostada arvutusmasinaga.

N ä i d e 7. Arvutada kõik võrrandi

$$2x^5 - 10x^3 + 10x + 3 = 0$$

lahendid veaga alla 10^{-4}.

Jagades antud võrrandi mõlemad pooled 2-ga, näeme, et

$$a_1 = 0, \quad a_2 = -5, \quad a_3 = 0, \quad a_4 = 5, \quad a_5 = 1{,}5.$$

Toimetades arvutusi viiekohalise täpsusega, saame 7 korda valemeid (22) rakendades järgmise tabeli:

k	$a_1^2 - a_2$	$a_2^2 - 2a_1a_3 + 2a_4$	$a_3^2 - 2a_2a_4 + 2a_1a_5$	$a_4^2 - 2a_3a_5$	a_5^2
2	10	35	50	25	2,25
4	30	275	795	400	5,0625
8	350	28 725	41 233 · 10	15 195 · 10	25,626
16	65 050	53 680 · 10^4	16 129 · 10^7	23 068 · 10^6	656,84
32	31 579 · 10^5	26 717 · 10^{13}	25 988 · 10^{18}	53 213 · 10^{16}	43 144 · 10
64	94 380 · 10^{14}	71 216 · 10^{30}	67 539 · 10^{40}	28 316 · 10^{37}	18 614 · 10^7
128	88 934 · 10^{33}	50 717 · 10^{65}	45 615 · 10^{85}	80 178 · 10^{78}	34 648 · 10^{18}

Siin pole mõtet minna k väärtusest 128 kaugemale, sest juba $k = 256$ puhul oleks viiekohalise täpsuse piirides

$$\sigma_1 = a_1^2, \quad \sigma_2 = a_2^2, \quad \sigma_3 = a_3^2, \quad \sigma_4 = a_4^2, \quad \sigma_5 = a_5^2,$$

mistõttu valemid (21) annaksid $k = 256$ korral sama tulemuse nagu juhul $k = 128$. Kasutades viiekohalisi logaritme, leiame $k = 128$ jaoks

$$\log \sigma_1 = 37{,}94907; \quad \log \sigma_2 = 69{,}70515; \quad \log \sigma_3 = 89{,}65911;$$
$$\log \sigma_4 = 82{,}90406; \quad \log \sigma_5 = 22{,}53968.$$

Valemite (21) põhjal saame siit

$$\log |\xi_1| = 0{,}29648; \quad \log |\xi_2| = 0{,}24810; \quad \log |\xi_3| = 0{,}15590;$$

$$\log |\xi_4| = \bar{1}{,}94723; \quad \log |\xi_5| = \bar{1}{,}52840$$

ja seega

$$|\xi_1| = 1{,}9791; \quad |\xi_2| = 1{,}7705; \quad |\xi_3| = 1{,}4319; \quad |\xi_4| = 0{,}8856;$$
$$|\xi_5| = 0{,}3376.$$

Päris jämeda proovimise teel veendume, et

$$\xi_1 = -1{,}9791; \quad \xi_2 = 1{,}7705; \quad \xi_3 = 1{,}4319; \quad \xi_4 = -0{,}8856;$$
$$\xi_5 = -0{,}3376.$$

Siin ξ_5 kujutab näites 6 leitud lahendit (art. 4). Arvutades kontrolliks kõigi lahendite summa, leiame

$$\xi_1 + \xi_2 + \xi_3 + \xi_4 + \xi_5 = 0{,}0001,$$

mis erineb vaid 0,0001 võrra täpsest väärtusest 0.

Harjutusülesandeid.

68. Missuguse λ puhul teisendub võrrand

$$x^4 + 12x^3 + 49x^2 + \lambda x + 40 = 0$$

Tschirnhausi teisendusega biruutvõrrandiks?

69. Lahendada võrrandid:

a) $x^3 - 6x^2 + 57x - 196 = 0$;
b) $x^3 + 3x - 2i = 0$;
c) $x^4 + 4x^3 + 11x^2 + 14x + 12 = 0$;
d) $x^5 - 1 = 0$;
e) $x^7 - 2x^6 - x^4 - x^3 - 2x + 1 = 0$;
f) $x^3 - 3ax^2 + (3a^2 - b^2)x - a^3 + ab^2 = 0$;
g) $x^4 + 3ax^3 + (2a^2 + 3)x^2 + 5ax + 2 = 0$.

70. Lahendada jäägiklassikorpuses $R^{(7)}$ võrrandid:

a) $x^3 - 3x^2 + x + 1 = 0$;
b) $4x^4 - 4x^3 + 3x^2 - 2x + 1 = 0$;
c) $x^6 + 2x^5 - x^4 + x^2 - 2x - 1 = 0$.

71. Lahendada võrrandisüsteem

$$3x^3 + 9x^2y + 9xy^2 + 3y^3 + 2x^2 - 4xy + 2y^2 - 5 = 0$$
$$4x^3 + 12x^2y + 12xy^2 + 4y^3 - x^2 + 2xy - y^2 - 3 = 0,$$

kui tema kordajad kuuluvad:

a) täisarvude valda;
b) jäägiklassikorpusse $R^{(7)}$.

72. Teades, et võrrandi

$$x^6 + 4x^5 + 12x^4 + 18x^3 + 23x^2 + 14x + 12 = 0$$

üheks lahendiks on i, leida ülejäänud lahendid.

73. Lahutada polünoom $x^{12} - 1$ taandumatute polünoomide korrutiseks:

a) kompleksarvude korpuses;
b) reaalarvude korpuses.

74. Leida võrrandite

a) $2x^5 + 100x^2 - 5x - 40 = 0$;
b) $x^7 + 2x^5 + 4x^4 - 8x^2 - 32 = 0$

positiivsete ja negatiivsete lahendite tõkked.

75. Eraldada võrrandite

a) $x^4 - 4x^3 - 4x^2 + 4x + 1 = 0$;
b) $2x^5 - 10x^3 + 10x - 3 = 0$

reaallahendid.

76. Leida võrrandi $x^5 - 5ax^3 + 5a^2x + 2b = 0$ reaallahendite arv.

77. Leida võrrandite

a) $x^3 + x^2 - 2x - 1 = 0$;
b) $x^4 - x - 1 = 0$;
c) $x^5 - x^3 + 1 = 0$;
d) $x^3 + a^2x + b^2 = 0$

reaallahendite arv Descartes'i reegli abil.

78. Missuguste λ väärtuste puhul on võrrandil $3x^4 - 4x^3 - 6x^2 + 12x + \lambda = 0$ kõik lahendid reaalsed?

79. Missuguste λ väärtuste puhul on võrrandil $x^7 - 7x^2 + \lambda = 0$ kolm reaallahendit?

80. Arvutada võrrandi $x^4 - 3x^3 + 3x^2 - 2 = 0$ lahend, mis asetseb vahemikus (1, 2), veaga alla 10^{-7}.

81. Poolkera raadius on 1. Kui kaugele poolkera põhjast tuleks paigutada selle põhjaga paralleelne tasand, nii et ta jaotaks poolkera kaheks ruumvõrdseks osaks. Vastus anda veaga alla 10^{-5}.

82. Arvutada Lobatševski menetlusega võrrandi $x^4 + 4x^3 - 4x^2 - 2x - 8 = 0$ lahendid veaga alla 10^{-3}.

V. Polünoommaatriksid ja Jordan'i normaalkuju.

§ 14. Polünoommaatriksid.

1. **Polünoommaatriksi normaalkuju.** Seni oleme käsitelnud polünoome üle korpuse ja integriteetkonna. Käesolevas peatükis vaatleme eriti polünoome üle ühe ringi, nimelt üle n-järku maatriksite ringi. Olgu antud polünoom

$$F = A_0 + A_1 x + A_2 x^2 + \ldots + A_m x^m,$$

mille kordajad

$$A_0 = \| a_{ik} \|, \quad A_1 = \| b_{ik} \|, \quad A_2 = \| c_{ik} \|, \quad \ldots, \quad A_m = \| l_{ik} \|$$

tähendavad n-järku maatrikseid üle põhikorpuse K. Polünoomile F võime anda kuju

$$F = \| a_{ik} \| + \| b_{ik} \| x + \| c_{ik} \| x^2 + \ldots + \| l_{ik} \| x^m = \\ = \| a_{ik} + b_{ik} x + c_{ik} x^2 + \ldots + l_{ik} x^m \| = \| f_{ik}(x) \|,$$

kus

$$f_{ik}(x) = a_{ik} + b_{ik} x + c_{ik} x^2 + \ldots + l_{ik} x^m$$

kujutab polünoomi üle K. Tähendab, iga polünoomi, mille kordajaiks on n-järku maatriksid üle põhikorpuse K, võib esitada n-järku maatriksina, mille elementideks on polünoomid üle K, ja ümberpöördult. Niisugust maatriksit

$$F = \begin{Vmatrix} f_{11}(x) & f_{12}(x) & \ldots & f_{1n}(x) \\ f_{21}(x) & f_{22}(x) & \ldots & f_{2n}(x) \\ \ldots & \ldots & \ldots & \ldots \\ f_{n1}(x) & f_{n2}(x) & \ldots & f_{nn}(x) \end{Vmatrix},$$

mille elementideks $f_{ik}(x)$ on polünoomid, nimetatakse p o l ü n o o m m a a t r i k s i k s.

Polünoommaatriksitega opereerides lubame vaid niisuguseid teisendusi, mis ei vii välja polünoomkonnast $K[x]$. Vastavalt sellele mõistame elementaarteisenduste all polünoommaatriksite vallas järgmist kahte teisendust:

1⁰ maatriksi rea (veeru) korrutamine triviaalse teguriga, s. o. nullist erineva konstandiga c;

2⁰ ühele reale (veerule) mingi polünoomiga $f(x)$ korrutatud teise rea (veeru) liitmine.

Siin ei ole elementaarteisenduse 1⁰ puhul lubatud rea (veeru) korrutamine mittekonstantse polünoomiga $f(x)$ sel põhjusel, et niisugune teisendus poleks pööratav, sest $\frac{1}{f(x)}$ ei kujuta polünoomi.

Nii nagu konstantsete elementidega maatriksite puhul võib ka siin veenduda, et elementaarteisendused ei mõjuta maatriksi astakut (I, § 17, art. 2). Näitame, et igale polünoommaatriksile F, mille astak on r, saab elementaarteisenduste teel anda normaalkuju

$$(1) \qquad \begin{Vmatrix} e_1(x) & 0 & \dots & 0 & \dots & 0 \\ 0 & e_2(x) & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & e_r(x) & \dots & 0 \\ 0 & 0 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 \end{Vmatrix},$$

kus peadiagonaali iga element $e_i(x)$ kujutab normeeritud polünoomi, mis jagub kõigi eelnevate polünoomidega $e_1(x)$, $e_2(x)$, ..., $e_{i-1}(x)$.

Kõigepealt võime eeldada, et F ei ole nullmaatriks, sest viimane omab juba normaalkuju. Vaatleme kõiki maatrikseid, mida saab tuletada maatriksist F lõpliku arvu elementaarteisenduste teel ja valime nende hulgast välja ühe niisuguse maatriksi

$$G = \begin{Vmatrix} g_{11}(x) & g_{12}(x) & \dots & g_{1n}(x) \\ g_{21}(x) & g_{22}(x) & \dots & g_{2n}(x) \\ \dots & \dots & \dots & \dots \\ g_{n1}(x) & g_{n2}(x) & \dots & g_{nn}(x) \end{Vmatrix},$$

mille nullist erinevate elementide hulgas esineks kõigi teiste maatriksite elementidega võrreldes madalaima astme polünoom, näiteks $g_{11}(x)$ [1]. Toetudes elementaarteisendusele 1°, võime eeldada, et $g_{11}(x)$ on normeeritud. Ei ole raske näha, et maatriksis G peavad kõik esimese rea ja esimese veeru elemendid jaguma $g_{11}(x)$-ga. Nimelt, jagades näiteks $g_{1k}(x)$ polünoomiga $g_{11}(x)$, saame

$$g_{1k}(x) = q(x)g_{11}(x) + r(x),$$

kus $r(x)$ on $g_{11}(x)$ suhtes madalama astme polünoom. Teostame nüüd maatriksiga G järgmise elementaarteisenduse 2°: lahutame k-ndast veerust $q(x)$-ga korrutatud esimese veeru. Sel teel saame uue maatriksi $\bar{G}$, kus $g_{1k}(x)$ asemel on element

$$g_{1k}(x) - q(x)g_{11}(x) = r(x),$$

mistõttu peab olema $r(x) = 0$, sest vastasel korral esineks maatriksis $\bar{G}$ element $r(x)$, mis on madalama astmega kui $g_{11}(x)$, vastuolus G valikuga. Järelikult peab $g_{1k}(x)$ jaguma $g_{11}(x)$-ga.

Rakendades elementaarteisendust 2°, võime seega muuta kõik maatriksi G esimese rea ja esimese veeru elemendid nullideks peale $g_{11}(x)$. Sel teel saame maatriksi

$$G_1 = \begin{Vmatrix} g_{11}(x) & 0 & \dots & 0 \\ 0 & f_{22}^{1}(x) & \dots & f_{2n}^{1}(x) \\ \dots & \dots & \dots & \dots \\ 0 & f_{n2}^{1}(x) & \dots & f_{nn}^{1}(x) \end{Vmatrix},$$

[1] Selles mõttes, et üheski maatriksist F lõpliku arvu elementaarteisenduste teel tuletatud maatriksis ei esineks nullist erinevate elementide hulgas polünoomi, mis oleks madalama astmega kui $g_{11}(x)$.

kus polünoomid $f_{ik}^{1}(x)$ peavad jaguma $g_{11}(x)$-ga. Tõepoolest, kui näiteks $f_{ik}^{1}(x)$ ei jaguks $g_{11}(x)$-ga, siis, liites maatriksis G_1 esimese reaga i-nda rea, saame maatriksi $\overline{G}_1$, kus esimese rea k-s element $f_{ik}^{1}(x)$ ei jagu $g_{11}(x)$-ga, vastuolus eelnenuga, sest $\overline{G}_1$, olles saadud maatriksist F lõpliku arvu elementaarteisenduste teel, on samade omadustega nagu G.

Toimides nüüd $(n-1)$-järku maatriksiga

$$F_1 = \begin{Vmatrix} f_{22}^{1}(x) & f_{23}^{1}(x) & \dots & f_{2n}^{1}(x) \\ f_{32}^{1}(x) & f_{33}^{1}(x) & \dots & f_{3n}^{1}(x) \\ \dots & \dots & \dots & \dots \\ f_{n2}^{1}(x) & f_{n3}^{1}(x) & \dots & f_{nn}^{1}(x) \end{Vmatrix}$$

täpselt samuti nagu maatriksiga F, jõuame maatriksini

$$G_2 = \begin{Vmatrix} g_{11}(x) & 0 & 0 & \dots & 0 \\ 0 & g_{22}^{1}(x) & 0 & \dots & 0 \\ 0 & 0 & f_{33}^{2}(x) & \dots & f_{3n}^{2}(x) \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & f_{n3}^{2}(x) & \dots & f_{nn}^{2}(x) \end{Vmatrix},$$

kus iga polünoom $f_{ik}^{2}(x)$ jagub $g_{22}^{1}(x)$-ga ja $g_{22}^{1}(x)$ omakorda $g_{11}(x)$-ga[1]. Jätkates seda protsessi, saame maatriksile F $n-1$ sammu järel normaalkuju (1), kusjuures $g_{11}(x) = e_1(x)$, $g_{22}^{1}(x) = e_2(x)$ jne.

Näide 1. Anda polünoommaatriksile

$$\begin{Vmatrix} x & -x & x^2+1 \\ x^2 & -x^3+x^2 & x^2+x \\ 0 & 2x^3 & 2x^2 \end{Vmatrix}$$

normaalkuju.

Lahutades siin kolmandast veerust x-ga korrutatud esimese veeru, saame pärast esimese ja kolmanda veeru ümberpaigutust maatriksi

[1] Sest $g_{22}^{1}(x)$ on saadud polünoomidest $f_{ik}^{1}(x)$ liitmise ja korrutamise teel, polünoomid $f_{ik}^{1}(x)$ aga jaguvad kõik $g_{11}(x)$-ga.

$$\begin{Vmatrix} 1 & -x & x \\ -x^3+x^2+x & -x^3+x^2 & x^2 \\ 2x^2 & 2x^3 & 0 \end{Vmatrix},$$

kus muudame kõik esimese rea ja esimese veeru elemendid peale esimese elementaarteisenduste teel nullideks. Selleks liidame kõigepealt teise veeruga kolmanda veeru ja lahutame kolmandast veerust x-ga korrutatud esimese veeru, mille tulemusena leiame maatriksi

$$\begin{Vmatrix} 1 & 0 & 0 \\ -x^3+x^2+x & -x^3+2x^2 & x^4-x^3 \\ 2x^2 & 2x^3 & -2x^3 \end{Vmatrix}.$$

Liites siin teise reaga polünoomiga x^3-x^2-x korrutatud esimese rea ja lahutades kolmandast reast $2x^2$-ga korrutatud esimese rea, saame maatriksi

$$\begin{Vmatrix} 1 & 0 & 0 \\ 0 & -x^3+2x^2 & x^4-x^3 \\ 0 & 2x^3 & -2x^3 \end{Vmatrix},$$

millest eraldame teist järku maatriksi

$$\begin{Vmatrix} -x^3+2x^2 & x^4-x^3 \\ 2x^3 & -2x^3 \end{Vmatrix}.$$

Liites viimases maatriksis esimese reaga $\frac{1}{2}$-ga korrutatud teise rea, leiame pärast esimese veeru jagamist 2-ga

$$\begin{Vmatrix} x^2 & x^4-2x^3 \\ x^3 & -2x^3 \end{Vmatrix}.$$

Nüüd lahutame teisest reast x-ga korrutatud esimese rea ja teisest veerust polünoomiga x^2-2x korrutatud esimese veeru, mille tulemusena saame pärast teise rea korrutamist -1-ga

$$\begin{Vmatrix} x^2 & 0 \\ 0 & x^3(x^2-2x+2) \end{Vmatrix}.$$

Seega omab antud polünoommaatriks normaalkuju

$$\begin{Vmatrix} 1 & 0 & 0 \\ 0 & x^2 & 0 \\ 0 & 0 & x^3(x^2-2x+2) \end{Vmatrix}.$$

2. **Elementaarjagajad.** Käesolevas artiklis näitame, et polünoommaatriksi F normaalkuju (1) on maatriksiga F üheselt määratud selles mõttes, et siin peadiagonaali elemendid $e_1(x)$, $e_2(x)$, ..., $e_r(x)$ ei sõltu sellest, missuguseid elementaarteisendusi kasutada maatriksile F normaalkuju andmiseks. Need üheselt määratud polünoomid $e_1(x)$, $e_2(x)$, ..., $e_r(x)$ kannavad maatriksi F elementaarjagajate nime.

Olgu k mingi kindel naturaalarv, mis ei ületa maatriksi F järku n. Vaatleme F-i kõiki k-järku determinante ja märgime nende suurima ühisteguri sümboliga $d_k(x)$. Erijuhul, kui maatriksis F kõik k-järku determinandid on nullid, olgu $d_k(x) = 0$. Polünoome $d_k(x)$, mida mõistame alati normeeritutena, nimetatakse maatriksi F determinantjagajateks. Näitame kõigepealt, et polünoommaatriksi determinantjagajad on invariantsed elementaarteisenduste suhtes. Selle tõestuseks kasutame samasugust mõttekäiku, nagu maatriksi astaku invariantsuse põhjendamisel (I, § 17, art. 2). Vaatleme nimelt maatriksis F mingit k-järku determinanti $D_k(x)$ ja teisendatud maatriksis F' vastavat determinanti $D_k'(x)$.

Kui elementaarteisendus 1^0 puudutab determinanti $D_k(x)$, siis omab teisendatud determinant kuju $D_k'(x) = cD_k(x)$ ja seega on determinantidel $D_k'(x)$ sama suurim ühistegur mis determinantidel $D_k(x)$, s. o.

$$d_k'(x) = d_k(x),$$

kus $d_k'(x)$ tähendab teisendatud maatriksi F' determinantjagajat.

Kui elementaarteisendus 2^0 puudutab determinanti $D_k(x)$, siis vastavalt sellele, kas polünoomiga $f(x)$ korrutatud rida kuulub determinanti $D_k(x)$ või mitte, saame teisenduse tulemusena kas determinandi $D_k(x)$ enda või determinandi

$$D_k'(x) = D_k(x) + f(x)D_k(x),$$

kus $D_k(x)$ on teatav k-järku determinant maatriksis F (kui mitte arvestada ridade järjekorda). Seega jaguvad teisenda-

tud maatriksi F' kõik k-järku determinandid $D_k'(x)$ maatriksi F determinantjagajaga $d_k(x)$, mistõttu ka F' determinantjagaja $d_k'(x)$ peab jaguma F-i determinantjagajaga $d_k(x)$. Rakendades nüüd maatriksile F' elementaarteisendust 2^0, võttes $f(x)$ asemel $-f(x)$, saame tulemusena tagasi maatriksi F. Et seejuures teisendatud maatriksi determinantjagaja peab jaguma lähtemaatriksi determinantjagajaga, siis peab $d_k(x)$ jaguma $d_k'(x)$-ga. Kuid $d_k(x)$ ja $d_k'(x)$ kui normeeritud polünoomid võivad vastastikku teineteisega jaguda vaid siis, kui

$$d_k'(x) = d_k(x).$$

Polünoommaatriksi F determinantjagajate invariantsust silmas pidades võime need determinantjagajad arvutada ka F-i normaalkujust (1). Kui $k > r$, siis on selles normaalkujus kõik k-järku determinandid nullid ja seega $d_k(x) = 0$. Kui aga $k \leqslant r$, siis silmas pidades, et maatriksi (1) i-nda rea kustutamisel jäävad i-ndasse veergu ainult nullid, võib $D_k(x)$ olla nullist erinev vaid siis, kui ta saadakse maatriksist (1) ühe ja sama indeksiga ridade ja veergude kustutamisel. Seega omab maatriksi (1) iga nullist erinev determinant $D_k(x)$ kuju

$$D_k(x) = \begin{vmatrix} e_{\alpha_1}(x) & 0 & \dots & 0 \\ 0 & e_{\alpha_2}(x) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & e_{\alpha_k}(x) \end{vmatrix} = e_{\alpha_1}(x) e_{\alpha_2}(x) \dots e_{\alpha_k}(x),$$

kus

$$\alpha_1 \geqslant 1, \quad \alpha_2 \geqslant 2, \quad \dots, \quad \alpha_k \geqslant k.$$

Et iga elementaarjagaja jagub kõigi temale eelnevate elementaarjagajatega, siis peab eriti $e_{\alpha_i}(x)$ jaguma $e_i(x)$-ga, mistõttu iga k-järku determinant $D_k(x)$ peab jaguma korrutisega

$$e_1(x) e_2(x) \dots e_k(x).$$

Viimane korrutis on ühtlasi maatriksi (1) kõigi k-järku determinantide suurimaks ühisteguriks, sest see korrutis esineb ise

maatriksi (1) ühe k-järku determinandina. Seega avaldub maatriksi F determinantjagaja $d_k(x)$ juhul $k \leqslant r$ kujul

$$d_k(x) = e_1(x)e_2(x) \ldots e_k(x). \tag{2}$$

Eriti on siis

$$d_{k-1}(x) = e_1(x)e_2(x) \ldots e_{k-1}(x),$$

millega valemit (2) jagades saame

$$e_k(x) = \frac{d_k(x)}{d_{k-1}(x)}, \quad k = 1, 2, \ldots, r, \tag{3}$$

kusjuures $d_0(x)$ all tuleb mõista ühikelementi 1. Et determinantjagajad on invariantsed elementaarteisenduste suhtes, siis on valemi (3) järgi ka elementaarjagajad invariantsed elementaarteisenduste suhtes, mis ütlebki, et polünoommaatriksi F normaalkuju on üheselt määratud.

3. Ekvivalentsed polünoommaatriksid. On ilmne, et kahe polünoommaatriksi summa, korrutis ja vahe kujutavad omakorda polünoommaatrikseid, mistõttu polünoommaatriksid üle antud põhikorpuse K moodustavad ringi ja nimelt mittekommutatiivse ringi. Tekib küsimus, missugusel tingimusel kujutab polünoommaatriksi F pöördmaatriks F^{-1} ka polünoommaatriksit. Et $FF^{-1} = E$, kus E tähendab ühikmaatriksit, siis determinantidele üle minnes saame

$$|F|\,|F^{-1}| = 1.$$

Siin $|F|$ kujutab polünoomi. Kui F^{-1} on polünoommaatriks, siis kujutab ka $|F^{-1}|$ polünoomi. Kuid kahe polünoomi korrutis saab olla 1 vaid siis, kui mõlemad tegurid kujutavad nullist erinevaid konstante, mistõttu

$$|F| = c \quad (c \neq 0).$$

Ümberpöördult, kui $|F| = c$ $(c \neq 0)$, siis nähtub pöördmaatriksi valemist (I, § 21, art. 1)

$$F^{-1} = |F|^{-1} \| F_{ik} \|',$$

kus F_{ik} tähendab elemendi f_{ik} alamdeterminanti, et F^{-1} on polünoommaatriks.

Niisugust polünoommaatriksit, mille determinant kujutab nullist erinevat konstanti, nimetatakse unimodulaarmaatriksiks. Tähendab, *polünoommaatriksi F pöördmaatriks on polünoommaatriks siis ja ainult siis, kui F on unimodulaarne.* Nii on näiteks polünoommaatriks

$$F=\begin{Vmatrix} x-1 & 0 & x-2 \\ 1 & x+1 & 0 \\ 0 & x^2+x+1 & -x+1 \end{Vmatrix}$$

unimodulaarne, sest siin

$$|F|=\begin{vmatrix} x-1 & 0 & x-2 \\ 1 & x+1 & 0 \\ 0 & x^2+x+1 & -x+1 \end{vmatrix}=-3.$$

Seega

$$F^{-1}=-\frac{1}{3}\begin{Vmatrix} -x^2+1 & x^3-x^2-x-2 & -x^2+x+2 \\ x-1 & -x^2+2x-1 & x-2 \\ x^2+x+1 & -x^3+1 & x^2-1 \end{Vmatrix}.$$

Olgu antud mingi unimodulaarmaatriks F. Leiame F-i normaalkuju. Kõigepealt on siin $d_n(x)=1$, sest F ainuke n-järku determinant on $D_n(x)=|F|=c$. Võttes valemis (2) $k=n$, saame seega

$$e_1(x)e_2(x)\ldots e_n(x)=1,$$

millest nähtub, et

$$e_1(x)=e_2(x)=\ldots=e_n(x)=1,$$

s. o. *unimodulaarmaatriksi normaalkujuks on ühikmaatriks E.*

Unimodulaarmaatriksid etendavad polünoommaatriksite teoorias sama osa, mis regulaarmaatriksid konstantsete elementidega maatriksite teoorias. Konstantsete elementidega maatriksite puhul nimetatakse maatrikseid A ja B ekvivalentseiks, kui nende vahel kehtib seos

$$B=UAV,$$

kus U ja V tähendavad regulaarmaatrikseid (I, § 24, art. 3). Analoogiliselt nimetatakse polünoommaatrikseid F ja G ekvivalentseiks, kui nende vahel kehtib seos

$$G = UFV,$$

kus U ja V tähendavad unimodulaarmaatrikseid. Tekib küsimus, kuidas otsustada, kas kaks etteantud polünoommaatriksit F ja G on ekvivalentsed või mitte.

Olgu F ja G ekvivalentsed, s. o.

$$G = UFV,$$

kus U ja V tähendavad unimodulaarmaatrikseid. Et iga unimodulaarmaatriksi normaalkujuks on ühikmaatriks, siis on maatriksid U ja V tuletatavad ühikmaatriksist lõpliku arvu elementaarteisenduste teel. Silmas pidades, et iga maatriksi ridade (veergude) elementaarteisendus on samaväärne korrutamisega vasakult (paremalt) niisuguse maatriksiga, mis saadakse ühikmaatriksist E sama elementaarteisenduse rakendamisel (I, § 24, art. 2), võime kirjutada

$$U = M_p \dots M_2 M_1 E N_1 N_2 \dots N_q = M_p \dots M_2 M_1 N_1 N_2 \dots N_q,$$
$$V = P_k \dots P_2 P_1 E Q_1 Q_2 \dots Q_l = P_k \dots P_2 P_1 Q_1 Q_2 \dots Q_l,$$

kus M_i, N_i, P_i, Q_i tähendavad üksikutele elementaarteisendustele vastavaid maatrikseid. Asetades viimased U ja V avaldised võrdusse $G = UFV$, saame

$$(4) \qquad G = M_p \dots M_2 M_1 N_1 N_2 \dots N_q F P_k \dots P_2 P_1 Q_1 Q_2 \dots Q_l,$$

millest nähtub, et G saadakse maatriksist F lõpliku arvu elementaarteisenduste teel. Ümberpöördult, kui G saadakse maatriksist F lõpliku arvu elementaarteisenduste teel, siis, tõlgitsedes iga üksikut elementaarteisendust korrutamisena vasakult või paremalt vastava maatriksiga, näeme, et F ja G vahel kehtib seos (4) ehk lühidalt

$$G = UFV,$$

kus

$$U = M_p \dots M_2 M_1 N_1 N_2 \dots N_q, \quad V = P_k \dots P_2 P_1 Q_1 Q_2 \dots Q_l$$

kujutavad unimodulaarmaatrikseid. Nimelt on

$$|U| = \text{const}, \quad |V| = \text{const},$$

sest üksikutele elementaarteisendustele 1^0 ja 2^0 vastavate determinantide väärtused on vastavalt c ja 1. Tähendab, *kaks polünoommaatriksit on ekvivalentsed siis ja ainult siis, kui ühte neist saab tuletada teisest lõpliku arvu elementaarteisenduste teel.*

Et polünoommaatriksi elementaarjagajad on invariantsed elementaarteisenduste suhtes, siis on ekvivalentsetel polünoommaatriksitel ühed ja samad elementaarjagajad. Ümberpöördult, kui maatriksitel F ja G on ühed ja samad elementaarjagajad, siis saame neile maatriksitele elementaarteisenduste teel anda ühe ja sama normaalkuju (1). Seega on F ja G mõlemad ekvivalentsed maatriksiga (1) ja järelikult ekvivalentsed ka omavahel. Nii oleme saanud kahe polünoommaatriksi ekvivalentsuse otsustamiseks tarviliku ja piisava tingimuse, mis on praktiliselt rakendatav ja mille sõnastame järgmise teoreemina.

Teoreem 1. *Kaks polünoommaatriksit on ekvivalentsed siis ja ainult siis, kui neil on ühed ja samad elementaarjagajad.*

Erijuhul, kui F kujutab konstantsete elementidega maatriksit, on selle maatriksi kõik determinandid ka konstandid, mistõttu

$$e_1(x) = e_2(x) = \dots = e_r(x) = 1,$$

kus r tähendab maatriksi F astakut. Seega väljendab siin teoreem 1 tuntud tõsiasja, et kaks konstantsete elementidega maatriksit on ekvivalentsed siis ja ainult siis, kui nende astakud on võrdsed (I, § 24, art. 3).

Polünoommaatriksite teooria omab tähelepandavaid rakendusi konstantsete elementidega maatriksite teoorias. Enne nende rakenduste juurde asumist tutvume vektoriruumi nende omadustega, mis on seotud lineaarsete alamruumidega.

§ 15. Vektoriruumi lineaarsed alamruumid.

1. Lineaarse alamruumi mõiste. Vaatleme n-dimensionaalset vektoriruumi[1] K_n üle põhikorpuse K (§ 3, art. 2), s. o. kõigi niisuguste n-dimensionaalsete vektorite

$$\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$$

hulka, mille komponendid $x_1, x_2, \ldots, x_n$ kuuluvad põhikorpusse K. Olgu L mingi vektorite hulk vektoriruumis K_n. Nimetame hulka L vektoriruumi K_n l i n e a a r s e k s a l a m r u u m i k s, kui on täidetud järgmised kaks tingimust:

1^0 kui L sisaldab mingit vektorit $\boldsymbol{x}$, siis peab L sisaldama ka iga vektorit $c\boldsymbol{x}$, kus c tähendab skalaari, s. o. põhikorpuse K elementi;

2^0 kui L sisaldab vektoreid $\boldsymbol{x}_1$ ja $\boldsymbol{x}_2$, siis peab L sisaldama ka viimaste summat $\boldsymbol{x}_1 + \boldsymbol{x}_2$.

Teiste sõnadega, vektoriruumi K_n lineaarseks alamruumiks L nimetame niisugust K_n osahulka, mis on kinnine liitmise ja skalaariga korrutamise suhtes. Seejuures tuleb K_n alamruumide hulka lugeda antud definitsiooni kohaselt ka vektoriruumi K_n ennast. Omaette lineaarse alamruumi moodustab nullvektor $0 = (0, 0, \ldots, 0)$, mis kuulub ise igasse alamruumi L, nagu see nähtub tingimusest 1^0, kui seal võtta $c = 0$.

Et n komponendiga vektorite hulgas võib olla ülimalt n lineaarselt sõltumatut vektorit (I, § 17, art. 3), siis on lineaarselt sõltumatute vektorite arv igas alamruumis piiratud. Lineaarselt sõltumatute vektorite maksimaalarvu alamruumis L nimetatakse selle alamruumi d i m e n s i o o n i k s. Eriti on vektoriruum K_n ise n-dimensionaalne, kuna nullvektor $(0, 0, \ldots, 0)$ moodustab 0-dimensionaalse alamruumi. Olgu alamruumi L dimensioon m ja $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m$ lineaarselt sõltumatud vektorid ning $\boldsymbol{x}$ mistahes vektor selles alamruumis. Et lineaarselt sõltumatute vektorite maksimaalarv alamruumis L on m, siis peavad vektorid

$$\boldsymbol{x}, \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m$$

---

[1] Vektoriruumi asemel kõneldakse vahel ka l i n e a a r s e s t r u u m i s t.

olema lineaarselt sõltuvad üle K, nii et kehtib seos

$$\lambda_0 x + \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_m x_m = 0, \tag{5}$$

kus $\lambda_0, \lambda_1, \lambda_2, \ldots, \lambda_m$ on K elemendid, mis ei ole kõik korraraga nullid. Eriti peab olema $\lambda_0 \neq 0$, sest vastasel korral järelduks seosest (5), et vektorid $x_1, x_2, \ldots, x_m$ on lineaarselt sõltuvad, vastupidi eeldusele. Seega saame seosest (5)

$$x = c_1 x_1 + c_2 x_2 + \ldots + c_m x_m,$$

kus kordajad $c_1 = -\frac{\lambda_1}{\lambda_0}$, $c_2 = -\frac{\lambda_2}{\lambda_0}$, $\ldots$, $c_m = -\frac{\lambda_m}{\lambda_0}$ kujutavad K elemente.

Ümberpöördult, lineaarse alamruumi tingimustest 1^0 ja 2^0 nähtub, et koos vektoritega $x_1, x_2, \ldots, x_m$ kuulub alamruumi L ka iga nende lineaarne kombinatsioon

$$c_1 x_1 + c_2 x_2 + \ldots + c_m x_m.$$

Tähendab, m-dimensionaalne lineaarne alamruum L koosneb mingi oma m lineaarselt sõltumatu vektori $x_1, x_2, \ldots, x_m$ kõigist lineaarsetest kombinatsioonidest, s. o.

$$L = \{ c_1 x_1 + c_2 x_2 + \ldots + c_m x_m \}.$$

Seepärast nimetatakse lineaarselt sõltumatuid vektoreid $x_1, x_2, \ldots, x_m$ alamruumi L b a a s i v e k t o r i t e k s. Baasi alamruumis L moodustavad iga m lineaarselt sõltumatut vektorit selles alamruumis.

Erijuhul, kui K_n on harilik kolmedimensionaalne vektoriruum, s. o. kui K tähendab reaalarvude korpust ja $n = 3$, siis kujutades vektoreid suunatud lõikudena, mis lähtuvad kõik nullpunktist O, võime öelda, et ühedimensionaalne alamruum

$$\{ c_1 x_1 \}$$

kujutab punkti O läbivat sirget ja kahedimensionaalne alamruum

$$\{ c_1 x_1 + c_2 x_2 \}$$

punkti O läbivat tasandit (I, § 19, art. 2). Vastavalt sellele nimetatakse ka n-dimensionaalses vektoriruumis K_n üle mis-

tahes korpuse K iga ühedimensionaalset lineaarset alamruumi sirgeks ja iga kahedimensionaalset lineaarset alamruumi tasandiks. Üldiselt nimetatakse m-dimensionaalset lineaarset alamruumi $m > 2$ puhul m-dimensionaalseks tasandiks ja eriti $(n-1)$-dimensionaalset lineaarset alamruumi hüpertasandiks.

Toome lõppeks veel kaks näidet lineaarsete alamruumide kohta. Olgu nimelt

$$A = \| a_{ik} \|$$

mingi n-järku maatriks, mille kordajad kuuluvad põhikorpusse K ja mille astak on r.

Vaatleme kõiki vektoreid $\boldsymbol{y}$, mis esinevad lineaarteisenduses

$$\boldsymbol{y} = A\boldsymbol{x}$$

vektoriruumi K_n vektorite $\boldsymbol{x}$ teisenditena. Nende vektorite hulk $L = \{\boldsymbol{y}\}$ kujutab lineaarset alamruumi. Tõepoolest:

1° L sisaldab koos vektoriga $\boldsymbol{y} = A\boldsymbol{x}$ ka vektorit $c\boldsymbol{y}$, sest $c\boldsymbol{y} = A(c\boldsymbol{x})$;

2° L sisaldab koos vektoritega $\boldsymbol{y}_1 = A\boldsymbol{x}_1$ ja $\boldsymbol{y}_2 = A\boldsymbol{x}_2$ ka summat $\boldsymbol{y}_1 + \boldsymbol{y}_2$, sest $\boldsymbol{y}_1 + \boldsymbol{y}_2 = A(\boldsymbol{x}_1 + \boldsymbol{x}_2)$.

Et leida alamruumi L dimensiooni, esitame lineaarteisenduse $\boldsymbol{y} = A\boldsymbol{x}$ vektorite $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ ja $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ komponentides:

$$\begin{aligned} y_1 &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ y_2 &= a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ y_n &= a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n. \end{aligned}$$

Võttes viimased seosed veergude viisi kokku, saame

$$\boldsymbol{y} = x_1\boldsymbol{a}^1 + x_2\boldsymbol{a}^2 + \ldots + x_n\boldsymbol{a}^n,$$

kus $\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^n$ tähendavad maatriksi A veeruvektoreid. Kuid nende veeruvektorite hulgas on vaid r lineaarselt sõltumatut vektorit. Olgu need $\boldsymbol{a}^1, \boldsymbol{a}^2, \ldots, \boldsymbol{a}^r$. Avaldades ülejäänud veeruvek-

torid a^{r+1}, a^{r+2}, ..., a^n vektorite a^1, a^2, ..., a^r kaudu, võime anda vektorile y kuju

$$y = c_1a^1 + c_2a^2 + \ldots + c_ra^r,$$

kus c_1, c_2, ..., c_r tähendavad põhikorpuse K elemente ja a^1, a^2, ..., a^r lineaarselt sõltumatuid vektoreid alamruumis L. Siit nähtub, et L dimensioon on r.

Vaatleme nüüd niisuguseid vektoreid x, mis rahuldavad tingimust

$$Ax = 0.$$

Siin hulk $L = \{x\}$ kujutab jälle lineaarset alamruumi. Tõepoolest:

1° L sisaldab koos vektoriga x ka vektorit cx, sest tingimusest $Ax = 0$ järeldub $A(cx) = 0$;

2° L sisaldab koos vektoritega x_1 ja x_2 ka summat $x_1 + x_2$, sest tingimustest $Ax_1 = 0$, $Ax_2 = 0$ järeldub $A(x_1 + x_2) = 0$.

Alamruumi L dimensiooni leidmiseks paneme tähele, et tingimus $Ax = 0$ kujutab homogeenset lineaarset võrrandisüsteemi, mille üldlahend on

$$x = c_1x_1 + c_2x_2 + \ldots + c_{n-r}x_{n-r},$$

kus x_1, x_2, ..., x_{n-r} on sõltumatud erilahendid ja c_1, c_2, ..., c_{n-r} meelevaldsed elemendid põhikorpuses K (I, § 18, art. 2). Seega siin L-i dimensioon on $n - r$.

2. Alamruumide otsesumma. Olgu L_1 ja L_2 kaks lineaarset alamruumi vektoriruumis K_n. Kõik need K_n vektorid x, mis on esitatavad kujul

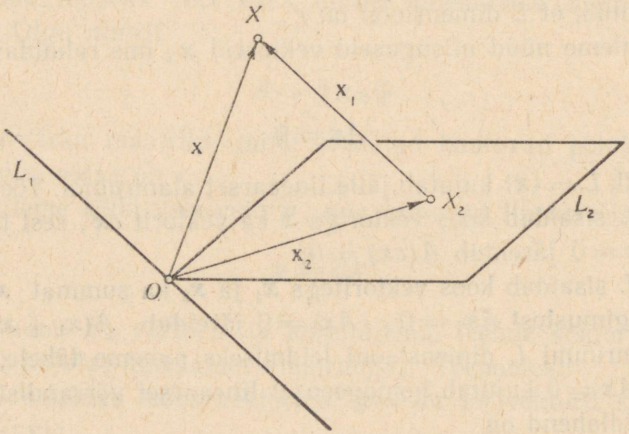
$$x = x_1 + x_2,$$

kus x_1 kuulub alamruumi L_1 ja x_2 alamruumi L_2, moodustavad hulga L, mis nimetatakse alamruumide L_1 ja L_2 summaks ning märgitakse sümboliga $L_1 + L_2$, s. o. $L = L_1 + L_2$. Ei ole raske näha, et alamruumide summa kujutab jälle alamruumi. Tõepoolest:

1° L sisaldab koos vektoriga x ka vektorit cx, sest tingimusest $x = x_1 + x_2$ järeldub $cx = cx_1 + cx_2$;

2^0 L sisaldab koos vektoritega $\boldsymbol{x}$ ja $\boldsymbol{y}$ ka summat $\boldsymbol{x}+\boldsymbol{y}$, sest tingimustest $\boldsymbol{x}=\boldsymbol{x}_1+\boldsymbol{x}_2$ ja $\boldsymbol{y}=\boldsymbol{y}_1+\boldsymbol{y}_2$ järeldub $\boldsymbol{x}+\boldsymbol{y}=$ $=(\boldsymbol{x}_1+\boldsymbol{y}_1)+(\boldsymbol{x}_2+\boldsymbol{y}_2)$.

Et iga lineaarne alamruum sisaldab nullvektorit, siis koosneb summa L_1+L_2 kõigist L_1 ja L_2 vektoritest ja seega ka kõigist L_1 ja L_2 vektorite lineaarsetest kombinatsioonidest.



Joonis 10.

Vaatleme näitena harilikku kolmedimensionaalset ruumi K_3, kus kujutame vektoreid punktist O lähtuvate suunatud lõikudena. Kui siin L_1 kujutab mingit sirget ja L_2 tasandit, mis ei läbi seda sirget, siis on ilmselt

$$L_1+L_2=K_3.$$

Ammugi on

$$L_1+L_2=K_3,$$

kui L_1 ja L_2 kujutavad teineteisest erinevaid tasandeid. Kuid tuleb silmas pidada põhilist erinevust kahe viimase summa vahel. Nimelt avaldub esimesel juhul K_3 iga vektor $\boldsymbol{x}$ üheselt kindla L_1 vektori $\boldsymbol{x}_1$ ja L_2 vektori $\boldsymbol{x}_2$ summana, kusjuures liidetavad vektorid $\boldsymbol{x}_1$ ja $\boldsymbol{x}_2$ saame, leides vektori $\boldsymbol{x}$ lõpp-punktist X sirgele L_1 tõmmatud paralleeli XX_2 lõikepunkti X_2 tasandiga L_2 (joo-

nis 10). Siis on $\overrightarrow{X_2X} = x_1$, $\overrightarrow{OX_2} = x_2$. Seevastu teisel juhul võib K_3 iga vektorit x avaldada lõpmata mitmel viisil summana $x_1 + x_2$, sest x_1 sihiks võime siin valida mistahes sihi tasandil L_1 ning rakendada siis x_1 ja x_2 leidmiseks esimesel juhul antud konstruktsiooni.

Olgu üldiselt $L = L_1 + L_2$, kus L_1 ja L_2 tähendavad lineaarseid alamruume vektoriruumis K_n. Kui siin L iga vektor x avaldub ühesel viisil summana $x = x_1 + x_2$, kus x_1 on L_1 vektor ja x_2 on L_2 vektor, siis nimetatakse summat L alamruumide L_1 ja L_2 o t s e s u m m a k s ning märgitakse sümboliga

$$L = L_1 + L_2 .$$

On oluline silmas pidada, et alamruumide otsesumma defineerimisel piisab nõuda L iga vektori x liidetavaiks lahutuse ühesuse asemel vaid nullvektori liidetavaiks lahutuse ühesust. Nimelt, kuna iga alamruum sisaldab nullvektorit, siis on nullvektori puhul alati kehtiv liidetavaiks lahutus

$$0 = 0 + 0 .$$

Oletame, et see on nullvektori jaoks ainuke võimalik liidetavaiks lahutus selles mõttes, et seosest

$$0 = a_1 + a_2 ,$$

kus a_1 kuulub alamruumi L_1 ja a_2 alamruumi L_2, järeldub

$$a_1 = 0 , \quad a_2 = 0 ,$$

ja näitame, et siis $L = L_1 + L_2$ kujutab otsesummat. Tõepoolest, kui L-i vektori x puhul kehtivad liidetavaiks lahutused

$$x = x_1 + x_2 , \quad x = y_1 + y_2 ,$$

kus x_1, y_1 kuuluvad alamruumi L_1 ja x_2, y_2 alamruumi L_2, siis lahutades esimesest võrdusest teise, saame

$$(x_1 - y_1) + (x_2 - y_2) = 0 ,$$

ja seega $x_1 - y_1 = 0$, $x_2 - y_2 = 0$, millest $x_1 = y_1$, $x_2 = y_2$.

Tähendab, *summa* $L = L_1 + L_2$ *kujutab otsesummat siis ja ainult siis, kui seosest*

$$0 = \boldsymbol{a}_1 + \boldsymbol{a}_2 ,$$

kus $\boldsymbol{a}_1$ *kuulub alamruumi* L_1 *ja* $\boldsymbol{a}_2$ *alamruumi* L_2, *järeldub* $\boldsymbol{a}_1 = 0$, $\boldsymbol{a}_2 = 0$.

Olgu nüüd L lineaarsete alamruumide L_1 ja L_2 otsesumma, s. o.

$$L = L_1 + L_2 ,$$

ja olgu $\boldsymbol{b}_1$, $\boldsymbol{b}_2$, ..., $\boldsymbol{b}_k$ alamruumi L_1 baasivektorid ning $\boldsymbol{b}_{k+1}$, $\boldsymbol{b}_{k+2}$, ..., $\boldsymbol{b}_{k+l}$ alamruumi L_2 baasivektorid. Näitame, et vektorid

$$\boldsymbol{b}_1 , \boldsymbol{b}_2 , \ldots , \boldsymbol{b}_{k+l}$$

moodustavad baasi alamruumis L. Vaatleme selleks alamruumis L mistahes vektori $\boldsymbol{x}$ liidetavaiks lahutust

$$\boldsymbol{x} = \boldsymbol{x}_1 + \boldsymbol{x}_2 ,$$

kus $\boldsymbol{x}_1$ kuulub alamruumi L_1 ja $\boldsymbol{x}_2$ alamruumi L_2, nii et

$$\boldsymbol{x}_1 = u_1\boldsymbol{b}_1 + u_2\boldsymbol{b}_2 + \ldots + u_k\boldsymbol{b}_k ,$$
$$\boldsymbol{x}_2 = u_{k+1}\boldsymbol{b}_{k+1} + u_{k+2}\boldsymbol{b}_{k+2} + \ldots + u_{k+l}\boldsymbol{b}_{k+l} .$$

Liites viimased kaks võrdust, saame

$$\boldsymbol{x} = u_1\boldsymbol{b}_1 + u_2\boldsymbol{b}_2 + \ldots + u_{k+l}\boldsymbol{b}_{k+l} .$$

Jääb näidata, et siin vektorid $\boldsymbol{b}_1$, $\boldsymbol{b}_2$, ..., $\boldsymbol{b}_{k+l}$ on lineaarselt sõltumatud. Tõepoolest, kui oleks

$$(\lambda_1\boldsymbol{b}_1 + \ldots + \lambda_k\boldsymbol{b}_k) + (\lambda_{k+1}\boldsymbol{b}_{k+1} + \ldots + \lambda_{k+l}\boldsymbol{b}_{k+l}) = 0 ,$$

kus λ_1, ..., λ_{k+l} tähendavad põhikorpuse K elemente, siis, silmas pidades, et L kujutab otsesummat, peab olema

$$\lambda_1\boldsymbol{b}_1 + \ldots + \lambda_k\boldsymbol{b}_k = 0 , \quad \lambda_{k+1}\boldsymbol{b}_{k+1} + \ldots + \lambda_{k+l}\boldsymbol{b}_{k+l} = 0 .$$

Et aga $\boldsymbol{b}_1$, ..., $\boldsymbol{b}_k$ kui L_1 baasivektorid ja $\boldsymbol{b}_{k+1}$, ..., $\boldsymbol{b}_{k+l}$ kui L_2 baasivektorid on omavahel lineaarselt sõltumatud, siis

$$\lambda_1 = 0 , \ \ldots , \ \lambda_k = 0 , \quad \lambda_{k+1} = 0 , \ \ldots , \ \lambda_{k+l} = 0 ,$$

mis ütleb, et vektorid $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_{k+l}$ on lineaarselt sõltumatud üle K ja moodustavad seega tõesti baasi alamruumis L.

Paneme tähele, et siin alamruumi L dimensioon on $k+l$, kus k on L_1 dimensioon ja l on L_2 dimensioon. Tähendab, *alamruumide otsesumma dimensioon on võrdne liidetavate alamruumide dimensioonide summaga.*

Ei ole raske näha, et kõike, mis siin on öeldud kahe alamruumi otsesumma kohta, saab üldistada ka mitme alamruumi otsesummale

$$L = L_1 + L_2 + \ldots + L_m .$$

3. Invariantsed alamruumid. Olgu n-dimensionaalses vektoriruumis K_n antud lineaarteisendus A, mis teisendab vektori $\boldsymbol{x}$ vektoriks $A\boldsymbol{x}$.

D e f i n i t s i o o n 1. Nimetame lineaarset alamruumi L i n v a r i a n t s e k s lineaarteisenduse A suhtes, kui A teisendab L iga vektori jälle mingiks L vektoriks.

Eriti kujutavad vektoriruum K_n ise ja nullvektorist koosnev alamruum invariantseid alamruume iga lineaarteisenduse suhtes. Vaatleme näitena veel harilikus kolmedimensionaalses vektoriruumis lineaarteisendust, mis koosneb pöördest ümber ühe koordinaaditelje. Siin pöördetelg kujutab ühedimensionaalset invariantset alamruumi ja selle teljega ristiolev koordinaaditasand kahedimensionaalset invariantset alamruumi vaadeldava pöörde suhtes.

Peatume nüüd juhul, kus vektoriruum K_n kujutab lineaarteisenduse A suhtes invariantsete alamruumide L_1 ja L_2 otsesummat, s. o.

$$K_n = L_1 + L_2 .$$

Valime mingi baasi $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k$ alamruumis L_1 ja mingi baasi $\boldsymbol{b}_{k+1}, \ldots, \boldsymbol{b}_n$ alamruumis L_2. Siis moodustavad vektorid

(6) $$\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$$

baasi vektoriruumis K_n (art. 2). Küsime, kuidas avaldub lineaarteisendus A baasil (6). Et L_1 ja L_2 on invariantsed vaadel-

dava lineaarteisenduse suhtes, peavad vektorid $Ab_1, \ldots, Ab_k$ kuuluma alamruumi L_1 ja vektorid $Ab_{k+1}, \ldots, Ab_n$ alamruumi L_2, nii et

$$\begin{aligned}
Ab_1 &= a_{11}b_1 + a_{21}b_2 + \ldots + a_{k1}b_k \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
Ab_k &= a_{1k}b_1 + a_{2k}b_2 + \ldots + a_{kk}b_k \\
Ab_{k+1} &= a_{k+1,\,k+1}b_{k+1} + a_{k+2,\,k+1}b_{k+2} + \ldots + a_{n,\,k+1}b_n \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
Ab_n &= a_{k+1,\,n}\,b_{k+1} + a_{k+2,\,n}\,b_{k+2} + \ldots + a_{nn}b_n .
\end{aligned}$$

Et lineaarteisenduse maatriksi veeruvektorid kujutavad baasivektorite teisendeid (I, § 20, art. 1), siis lineaarteisenduse A maatriks baasil (6) on

$$\left\|\begin{array}{cccc}
a_{11} & a_{1k} & 0 & \ldots\ 0 \\
\ldots & \ldots & \ldots & \ldots \\
a_{k1} & \ldots\ a_{kk} & 0 & \ldots\ 0 \\
0 & 0 & a_{k+1,\,k+1} & \ldots\ a_{k+1,\,n} \\
\ldots & \ldots & \ldots & \ldots \\
0 & 0 & a_{n,\,k+1} & \ldots\ a_{nn}
\end{array}\right\|,$$

mille kujulist maatriksit nimetatakse kast-diagonaalmaatriksiks ja märgitakse lühidalt sümboliga

$$\left\|\begin{array}{cc} A_1 & \\ & A_2 \end{array}\right\|,$$

kus

$$A_1 = \left\|\begin{array}{ccc} a_{11} & \ldots & a_{1k} \\ \ldots & \ldots & \ldots \\ a_{k1} & \ldots & a_{kk} \end{array}\right\|, \quad A_2 = \left\|\begin{array}{ccc} a_{k+1,\,k+1} & \ldots & a_{k+1,\,n} \\ \ldots & \ldots & \ldots \\ a_{n,\,k+1} & \ldots & a_{nn} \end{array}\right\|.$$

Üldiselt kui vektoriruum K_n kujutab lineaarteisenduse A suhtes invariantsete alamruumide $L_1, L_2, \ldots, L_m$ otsesummat, s. o.

$$K_n = L_1 \dot{+} L_2 \dot{+} \ldots \dot{+} L_m,$$

siis valides ruumis K_n baasi, mis koosneb kõikidest liidetavate

alamruumide baasivektoritest, saame vaadeldava lineaarteisenduse maatriksile kast-diagonaalkuju

$$\begin{Vmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_m \end{Vmatrix},$$

kus iga maatriksi A_i järk on võrdne vastava alamruumi L_i dimensiooniga.

Tutvume lõppeks ühe invariantsete alamruumide eriliigiga — nn. tsükliliste alamruumidega, mis etendavad tähtsat osa alamruumide struktuuri uurimisel.

Definitsioon 2. Nimetame lineaarteisenduse A suhtes invariantset alamruumi L tsükliliseks, kui leidub niisugune vektor $\boldsymbol{a}$, mille puhul vektorid

$$\boldsymbol{a},\ A\boldsymbol{a},\ A^2\boldsymbol{a},\ \ldots,\ A^{k-1}\boldsymbol{a} \tag{7}$$

moodustavad baasi alamruumis L.

Baas (7) kannab vastavalt alamruumi L tsüklilise baasi nime. Tsüklilisi alamruume on eriti kerge leida, kui vaadelda selliseid alamruumi L lineaarteisendusi B, mille puhul

$$B^l = 0,$$

kus l tähendab teatavat naturaalarvu. Niisugust teisendust B, kus $B^l = 0$, nimetatakse nilpotentseks teisenduseks. Nilpotentse teisenduse puhul on

$$|B|^l = 0$$

ja seega $|B| = 0$, s. o. iga nilpotentne teisendus on singulaarne.

Küsime nüüd, kuidas leida vektoriruumi K_n tsüklilisi alamruume nilpotentse teisenduse B suhtes. Võtame selleks vektoriruumis K_n mingi nullist erineva vektori $\boldsymbol{a}$ ja moodustame temast B abil vektorid

$$\boldsymbol{a},\ B\boldsymbol{a},\ B^2\boldsymbol{a},\ \ldots,\ B^{k-1}\boldsymbol{a},\ B^k\boldsymbol{a},\ \ldots.$$

Et $B^l = 0$, siis peavad ülemises jadas olema kõik vektorid teatavast kohast alates nullid. Olgu $B^k\boldsymbol{a}$ esimene nullvektor selles jadas, nii et

$$B^{k-1}\boldsymbol{a} \neq 0, \quad B^k\boldsymbol{a} = 0.$$

Näitame, et siis vektorid

$$\boldsymbol{a}, B\boldsymbol{a}, B^2\boldsymbol{a}, \ldots, B^{k-1}\boldsymbol{a} \tag{8}$$

on lineaarselt sõltumatud üle K. Oletame vastupidi, et vektorite (8) vahel valitseb seos

$$\lambda_1\boldsymbol{a} + \lambda_2 B\boldsymbol{a} + \lambda_3 B^2\boldsymbol{a} + \ldots + \lambda_k B^{k-1}\boldsymbol{a} = 0,$$

kus kordajad λ_i kuuluvad põhikorpusse K. Olgu siin λ_h esimene nullist erinev kordaja, nii et ülemine seos omab tegelikult kuju

$$\lambda_h B^{h-1}\boldsymbol{a} + \lambda_{h+1} B^h\boldsymbol{a} + \ldots + \lambda_k B^{k-1}\boldsymbol{a} = 0.$$

Et $B^k\boldsymbol{a} = 0$, $B^{k+1}\boldsymbol{a} = 0$, ..., siis, rakendades viimasele võrdusele teisendust B^{k-h}, saame

$$\lambda_h B^{k-1}\boldsymbol{a} = 0,$$

millest $B^{k-1}\boldsymbol{a} \neq 0$ tõttu $\lambda_h = 0$, vastuolus eeldusega. Seega peavad vektorid (8) olema tõesti lineaarselt sõltumatud.

Vaatleme vektorite (8) poolt moodustatud k-dimensionaalset alamruumi

$$L = \{ c_1\boldsymbol{a} + c_2 B\boldsymbol{a} + c_3 B^2\boldsymbol{a} + \ldots + c_k B^{k-1}\boldsymbol{a} \},$$

kus kordajad c_i tähendavad mistahes elemente põhikorpuses K. Et

$$B(c_1\boldsymbol{a} + c_2 B\boldsymbol{a} + c_3 B^2\boldsymbol{a} + \ldots + c_k B^{k-1}\boldsymbol{a}) = \\ = c_1 B\boldsymbol{a} + c_2 B^2\boldsymbol{a} + \ldots + c_{k-1} B^{k-1}\boldsymbol{a},$$

siis on alamruum L invariantne nilpotentse teisenduse B suhtes. Veel enam, alamruum L on tsükliline, sest tema baas (8) on tsükliline. Seega kujutabki L otsitavat alamruumi.

Olgu näiteks

$$B=\begin{Vmatrix}0&0&0&0\\1&0&0&0\\1&1&0&0\\1&1&1&0\end{Vmatrix}.$$

Siin

$$B^2=\begin{Vmatrix}0&0&0&0\\0&0&0&0\\1&0&0&0\\2&1&0&0\end{Vmatrix},\quad B^3=\begin{Vmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\1&0&0&0\end{Vmatrix},\quad B^4=0,$$

millest nähtub, et B on nilpotentne. Valides $\boldsymbol{a}=(1,\ 0,\ 0,\ 0)$, leiame

$$B\boldsymbol{a}=(0,\ 1,\ 1,\ 1),\ B^2\boldsymbol{a}=(0,\ 0,\ 1,\ 2),$$
$$B^3\boldsymbol{a}=(0,\ 0,\ 0,\ 1),\ B^4\boldsymbol{a}=0,$$

millele vastab neljadimensionaalne tsükliline alamruum

$$L_4=\{c_1(1,\ 0,\ 0,\ 0)+c_2(0,\ 1,\ 1,\ 1)+c_3(0,\ 0,\ 1,\ 2)+$$
$$+c_4(0,\ 0,\ 0,\ 1)\}=\{(c_1,\ c_2,\ c_2+c_3,\ c_2+2c_3+c_4)\}.$$

Valides $a=(0,\ 1,\ 0,\ 0)$, saame

$$B\boldsymbol{a}=(0,\ 0,\ 1,\ 1),\ B^2\boldsymbol{a}=(0,\ 0,\ 0,\ 1),\ B^3\boldsymbol{a}=0,$$

millele vastab kolmedimensionaalne tsükliline alamruum

$$L_3=\{c_1(0,\ 1,\ 0,\ 0)+c_2(0,\ 0,\ 1,\ 1)+c_3(0,\ 0,\ 0,\ 1)\}=$$
$$=\{(0,\ c_1,\ c_2,\ c_2+c_3)\}.$$

Valides $\boldsymbol{a}=(0,\ 0,\ 1,\ 0)$, leiame

$$B\boldsymbol{a}=(0,\ 0,\ 0,\ 1),\ B^2\boldsymbol{a}=0,$$

millele vastab kahedimensionaalne tsükliline alamruum

$$L_2=\{c_1(0,\ 0,\ 1,\ 0)+c_2(0,\ 0,\ 0,\ 1)\}=\{(0,\ 0,\ c_1,\ c_2)\}.$$

Lõppeks valides $\boldsymbol{a}=(0,\ 0,\ 0,\ 1)$, saame

$$B\boldsymbol{a}=0,$$

millele vastab ühedimensionaalne tsükliline alamruum

$$L_1 = \{c_1(0,\ 0,\ 0,\ 1)\} = \{(0,\ 0,\ 0,\ c_1)\}.$$

Olgu L k-dimensionaalne tsükliline alamruum nilpotentse teisenduse B suhtes. Küsime, kuidas avaldub lineaarteisendus B tsüklilisel baasil (8). Rakendades baasivektoritele (8) teisendust B, saame

$$\begin{aligned}
B\boldsymbol{a} &= 0 \cdot \boldsymbol{a} + 1 \cdot B\boldsymbol{a} \\
B(B\boldsymbol{a}) &= 0 \cdot B\boldsymbol{a} + 1 \cdot B^2\boldsymbol{a} \\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
B(B^{k-2}\boldsymbol{a}) &= 0 \cdot B^{k-2}\boldsymbol{a} + 1 \cdot B^{k-1}\boldsymbol{a} \\
B(B^{k-1}\boldsymbol{a}) &= 0 \cdot B^{k-1}\boldsymbol{a}.
\end{aligned}$$

Et lineaarteisenduse maatriksi veeruvektorid kujutavad baasivektorite teisendeid (I, § 20, art. 1), peab nilpotentse teisenduse B maatriks omama tsüklilisel baasil (8) kuju

$$\begin{Vmatrix} 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{Vmatrix},$$

mis kannab J o r d a n'i k a s t i k e s e nime.

§ 16. Jordani normaalkuju.

1. Maatriksi karakteristliku võrrandi omadusi. Maatriksite teooria üheks põhiülesandeks on leida antud maatriksiga $A = \| a_{ik} \|$ sarnane maatriks $\bar{A} = P^{-1}AP$, mis omaks võimalikult lihtsat kuju ehk, geomeetriliselt kõneldes: leida niisugune baas

$$\boldsymbol{b}_1,\ \boldsymbol{b}_2,\ \dots,\ \boldsymbol{b}_n,$$

millel antud lineaarteisendus A omaks võimalikult lihtsat kuju (I, § 23, art. 3). Kui maatriksi A karakteristlik võrrand $f(\lambda) = 0$,

kus

$$f(\lambda) = \begin{vmatrix} a_{11} - \lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - \lambda & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} - \lambda \end{vmatrix},$$

ei oma kordseid lahendeid, siis on niisuguseks lihtsaimaks kujuks diagonaalkuju (I, § 23, art. 2). Kuid me teame, et mitte igal maatriksil pole sarnast diagonaalkuju ehk, nagu öeldakse, mitte iga maatriks ei taandu diagonaalkujule. Seepärast tõusebki küsimus niisuguse lihtsaima kuju järgi, millele taanduks iga maatriks. Selle küsimuse lahendus on lähedalt seotud maatriksi karakteristliku võrrandiga, mille omadustega tutvumegi kõigepealt.

1° Maatriksi A karakteristliku võrrandi $f(\lambda) = 0$ vasak pool — karakteristlik polünoom $f(\lambda)$ — kujutab maatriksi

$$A - \lambda E = \begin{Vmatrix} a_{11} - \lambda & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - \lambda & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} - \lambda \end{Vmatrix}$$

determinanti, s. o.

$$f(\lambda) = |A - \lambda E|.$$

Siin maatriks $A - \lambda E$, kus E tähendab ühikmaatriksit, kannab maatriksi A karakteristliku maatriksi nime. Karakteristlik maatriks kujutab λ suhtes polünoommaatriksit, mille pöördmaatriks omab kuju (I, § 21, art. 1)

$$(A - \lambda E)^{-1} = \frac{1}{f(\lambda)} \| A_{ik}(\lambda) \|',$$

kus $A_{ik}(\lambda)$ tähendab karakteristliku maatriksi i-nda rea k-nda elemendi alamdeterminanti. Korrutades viimast võrdust maatriksiga $f(\lambda)(A - \lambda E)$, leiame

$$f(\lambda) E = (A - \lambda E) \| A_{ik}(\lambda) \|'.$$

Silmas pidades, et iga polünoommaatriksit võib vaadelda kui

polünoomi, mille kordajateks on maatriksid (§ 14, art. 1), on arusaadav, et viimases võrduses esinevad avaldised omavad mõtet ja võrdus jääb püsima, kui λ asendada maatriksiga A. Et selle asenduse puhul saab esimene tegur võrduse paremal poolel nulliks, siis on

$$f(A)E = 0$$

ehk

$$f(A) = 0.$$

Tulemus kannab Hamilton-Cayley' seose nime. Hamilton-Cayley seos ütleb, et maatriks A rahuldab oma karakteristlikku võrrandit $f(\lambda) = 0$.

2^0 Olgu antud mingi m-astme polünoom

$$g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m$$

ehk

$$g(x) = b_0(x - \eta_1)(x - \eta_2) \ldots (x - \eta_m),$$

kus $\eta_1, \eta_2, \ldots, \eta_m$ on polünoomi $g(x)$ lahendid. Küsime, kuidas on maatriksi $g(A)$ karakteristlikud väärtused seotud maatriksi A karakteristlike väärtustega $\lambda_1, \lambda_2, \ldots, \lambda_n$. Et

$$g(A) = b_0(A - \eta_1E)(A - \eta_2E) \ldots (A - \eta_mE),$$

siis determinantidele üle minnes leiame valemit $|cA| = c^n|A|$ kasutades

$$|g(A)| = b_0{}^n|A - \eta_1E||A - \eta_2E| \ldots |A - \eta_mE|$$

ehk

$$|g(A)| = b_0{}^nf(\eta_1)f(\eta_2) \ldots f(\eta_m).$$

Silmas pidades, et polünoomide f ja g resultant $R(f, g)$ avaldub kujul (§ 10, art. 1)[1]

$$R(f, g) = (-1)^{mn}b_0{}^nf(\eta_1)f(\eta_2) \ldots f(\eta_m)$$

---

[1] Siin tuleb arvestada, et $f(\lambda)$ pealiikme kordaja $a_0 = (-1)^n$.

või

$$R(f, g) = (-1)^{mn} g(\lambda_1) g(\lambda_2) \dots g(\lambda_n),$$

saame

$$|g(A)| = g(\lambda_1) g(\lambda_2) \dots g(\lambda_n).$$

Vaadeldes polünoomi $g(x)$ asemel polünoomi $g(x) - \lambda$, leiame viimasest valemist

$$|g(A) - \lambda E| = [g(\lambda_1) - \lambda]\,[g(\lambda_2) - \lambda] \dots [g(\lambda_n) - \lambda],$$

millest nähtub, et maatriksi $g(A)$ karakteristlikud väärtused on $g(\lambda_1)$, $g(\lambda_2)$, ..., $g(\lambda_n)$, kus λ_1, λ_2, ..., λ_n on A karakteristlikud väärtused.

3⁰ Vaatleme maatriksiga A sarnast maatriksit $\bar{A} = P^{-1}AP$, kus P tähendab mingit regulaarmaatriksit. Korrutades A karakteristlikku maatriksit $A - \lambda E$ paremalt maatriksiga P ja vasakult maatriksiga P^{-1}, saame

$$P^{-1}(A - \lambda E)P = P^{-1}AP - \lambda P^{-1}P = \bar{A} - \lambda E,$$

kust determinantidele üle minnes leiame

$$|\bar{A} - \lambda E| = |P^{-1}|\,|A - \lambda E|\,|P| = |A - \lambda E|,$$

sest $|P^{-1}|\,|P| = 1$. Tähendab, *sarnaste maatriksite karakteristlikud polünoomid langevad ühte.* Seega on sarnastel maatriksitel ka ühed ja samad karakteristlikud väärtused.

Karakteristlike polünoomide võrdus on küll tarvilik, kuid mitte piisav maatriksite sarnasuseks. Nii on näiteks maatriksite

$$E = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}, \qquad A = \begin{Vmatrix} 1 & 1 \\ 0 & 1 \end{Vmatrix}$$

karakteristlikud polünoomid võrdsed, aga A ei ole sarnane E-ga, sest missugune ka ei oleks maatriks P, ikka on

$$P^{-1}EP = P^{-1}P = E.$$

Niisuguse tingimusega, mis on ühtlasi tarvilik ja piisav maatriksite sarnasuseks, tutvume järgmises paragrahvis.

2. **Vektoriruumi lahutamine invariantsete alamruumide otsesummaks.** Tuleme nüüd maatriksi lihtsaimale kujule taandamise küsimuse juurde. Olgu maatriksi A karakteristlike väärtuste $\lambda_1, \lambda_2, \ldots, \lambda_n$ hulgas m erinevat väärtust. Eeldades, et A karakteristlikud väärtused kuuluvad korpusse K, näitame, et vektoriruumi K_n saab lahutada m A suhtes invariantse alamruumi $L_1, L_2, \ldots, L_m$ otsesummaks, s. o. et

$$K_n = L_1 \dotplus L_2 \dotplus \ldots \dotplus L_m .$$

Olgu $\lambda_1, \lambda_2, \ldots, \lambda_m$ üksteisest erinevad A karakteristlikud väärtused, kusjuures nende väärtuste kordsused olgu vastavalt $\alpha_1, \alpha_2, \ldots, \alpha_m$. Siis on

$$f(\lambda) = (-1)^n (\lambda - \lambda_1)^{\alpha_1} (\lambda - \lambda_2)^{\alpha_2} \ldots (\lambda - \lambda_m)^{\alpha_m} .$$

Lahutades ratsionaalfunktsiooni

$$\frac{1}{f(\lambda)} = \frac{(-1)^n}{(\lambda - \lambda_1)^{\alpha_1} (\lambda - \lambda_2)^{\alpha_2} \ldots (\lambda - \lambda_m)^{\alpha_m}}$$

osamurdude summaks, leiame (§ 6, art. 1)

$$\frac{1}{f(\lambda)} = \sum_{i=1}^{m} \frac{\varphi_i(\lambda)}{(\lambda - \lambda_i)^{\alpha_i}},$$

kus $\varphi_i(\lambda)$ tähendab ülimalt $(\alpha_i - 1)$-astme polünoomi. Korrutades viimast võrdust polünoomiga $f(\lambda)$, saame

$$1 = \sum_{i=1}^{m} \varphi_i(\lambda) \frac{f(\lambda)}{(\lambda - \lambda_i)^{\alpha_i}} .$$

Märkides

$$f_i(\lambda) = \varphi_i(\lambda) \frac{f(\lambda)}{(\lambda - \lambda_i)^{\alpha_i}}, \tag{9}$$

võime kirjutada

$$1 = \sum_{i=1}^{m} f_i(\lambda) .$$

Et iga $f_i(\lambda)$ kujutab polünoomi, siis võime siin asendada λ maatriksiga A ja saame seega

$$E = \sum_{i=1}^{m} f_i(A),$$

kus E tähendab ühikmaatriksit. Olgu $\boldsymbol{x}$ mingi K_n vektor. Korrutades viimase võrduse kumbagi poolt vektoriga $\boldsymbol{x}$, leiame

$$\boldsymbol{x} = \sum_{i=1}^{m} f_i(A)\boldsymbol{x}. \tag{10}$$

Siin $f_i(A)\boldsymbol{x}$ kujutab lineaarteisendust, mis teisendab vektori $\boldsymbol{x}$ vektoriks $f_i(A)\boldsymbol{x}$. Nagu nägime (§ 15, art. 1), moodustavad vektorid $f_i(A)\boldsymbol{x}$ teatava lineaarse alamruumi

$$L_i = \{f_i(A)\boldsymbol{x}\}.$$

Näitame, et sel teel saadud alamruumid $L_1, L_2, \ldots, L_m$ ongi otsitavad invariantsed alamruumid, nii et

$$K_n = L_1 \dot{+} L_2 \dot{+} \ldots \dot{+} L_m.$$

Silmas pidades alamruumide summa mõistet, nähtub võrdusest (10), et

$$K_n = L_1 + L_2 + \ldots + L_m. \tag{11}$$

Jääb näidata, et viimane summa on otsesumma ja alamruumid L_i on invariantsed lineaarteisenduse A suhtes.

1⁰ Tõestame kõigepealt valemi

$$f_i(A)\boldsymbol{x}_k = \begin{cases} \boldsymbol{x}_k, & \text{kui } i = k \\ 0, & \text{kui } i \neq k, \end{cases} \tag{12}$$

kus $\boldsymbol{x}_k$ tähendab mingit vektorit alamruumis L_k.

Et

$$\boldsymbol{x}_k = f_k(A)\boldsymbol{x}$$

ja valemi (9) järgi [1]

$$f_i(A) = \varphi_i(A)\left[\frac{f(\lambda)}{(\lambda-\lambda_i)^{\alpha_i}}\right]_{\lambda=A},$$

siis

$$f_i(A)\boldsymbol{x}_k = f_i(A)f_k(A)\boldsymbol{x} = \varphi_i(A)\varphi_k(A)\left[\frac{f^2(\lambda)}{(\lambda-\lambda_i)^{\alpha_i}(\lambda-\lambda_k)^{\alpha_k}}\right]_{\lambda=A}\boldsymbol{x}.$$

---

[1] Siin tuleb enne $f(\lambda)$ jagada $(\lambda-\lambda_i)^{\alpha_i}$-ga ja siis asetada $\lambda = A$.

Kui siin $i \neq k$, siis $f(\lambda)$ jagub korrutisega $(\lambda - \lambda_i)^{\alpha_i}(\lambda - \lambda_k)^{\alpha_k}$ ja seega sisaldab polünoom $\frac{f^2(\lambda)}{(\lambda - \lambda_i)^{\alpha_i}(\lambda - \lambda_k)^{\alpha_k}}$ tegurit $f(\lambda)$. Et Hamilton-Cayley seose järgi $f(A) = 0$ (art. 1), siis

$$f_i(A)\boldsymbol{x}_k = 0, \quad \text{kui} \quad i \neq k,$$

millega on valemi (12) teine osa tõestatud. Paigutades võrduses (10) $\boldsymbol{x}$-i asemele alamruumi L_k vektori $\boldsymbol{x}_k$, saame valemi (12) juba tõestatud osa kasutades

$$\boldsymbol{x}_k = f_k(A)\,\boldsymbol{x}_k,$$

mis kujutab valemi (12) esimest osa.

Toetudes valemile (12), ei ole raske veenduda, et summa (11) on otsesumma. Selleks tarvitseb vaid näidata, et võrdusest

$$\boldsymbol{x}_1 + \boldsymbol{x}_2 + \ldots + \boldsymbol{x}_m = 0,$$

kus $\boldsymbol{x}_k$ kuulub alamruumi L_k, järeldub $\boldsymbol{x}_k = 0$ (§ 15, art. 2). Tõepoolest, rakendades ülemise võrduse kummalegi poolele lineaarteisendust $f_k(A)$, saame

$$f_k(A)\boldsymbol{x}_1 + f_k(A)\boldsymbol{x}_2 + \ldots + f_k(A)\boldsymbol{x}_m = 0,$$

millest valemi (12) tõttu $\boldsymbol{x}_k = 0$.

2^0 Alamruumi L_i invariantsuse selgitamiseks näitame, et alamruumi L_i võib iseloomustada ka kui nende vektorite $\boldsymbol{y}$ hulka, mis rahuldavad võrrandit

$$(A - \lambda_i E)^{\alpha_i}\boldsymbol{y} = 0. \tag{13}$$

Veendume kõigepealt, et L_i iga vektor

$$\boldsymbol{x}_i = f_i(A)\boldsymbol{x}$$

rahuldab tingimust (13). Tõepoolest, asetades võrrandi (13) vasakusse poolde $\boldsymbol{y}$ asemele $\boldsymbol{x}_i$, saame

$$(A - \lambda_i E)^{\alpha_i}\boldsymbol{x}_i = (A - \lambda_i E)^{\alpha_i} f_i(A)\boldsymbol{x} =$$

$$= (A - \lambda_i E)^{\alpha_i}\varphi_i(A)\left[\frac{f(\lambda)}{(\lambda - \lambda_i)^{\alpha_i}}\right]_{\lambda = A}\boldsymbol{x} = \varphi_i(A)f(A)\boldsymbol{x} = 0,$$

sest Hamilton-Cayley seose põhjal on $f(A) = 0$ (art. 1).

Olgu, ümberpöördult, $\boldsymbol{y}$ mingi vektor, mis rahuldab võrrandit (13). Veendume, et $\boldsymbol{y}$ kuulub alamruumi L_i. Rakendades vektorile $\boldsymbol{y}$ võrdust (10), võime (9) põhjal kirjutada

$$\boldsymbol{y} = \sum_{k=1}^{m} f_k(A)\boldsymbol{y} = \sum_{k=1}^{m} \varphi_k(A) \left[\frac{f(\lambda)}{(\lambda-\lambda_k)^{\alpha_k}}\right]_{\lambda=A} \boldsymbol{y}.$$

Kui siin $k \neq i$, siis sisaldab polünoom $\dfrac{f(\lambda)}{(\lambda-\lambda_k)^{\alpha_k}}$ tegurit $(\lambda-\lambda_i)^{\alpha_i}$ ja seega on võrrandi (13) tõttu

$$\left[\frac{f(\lambda)}{(\lambda-\lambda_k)^{\alpha_k}}\right]_{\lambda=A} \boldsymbol{y} = 0, \quad \text{kui } k \neq i,$$

nii et

$$\boldsymbol{y} = f_i(A)\boldsymbol{y},$$

mis ütlebki, et $\boldsymbol{y}$ kuulub alamruumi L_i.

Seega võib alamruumi L_i iseloomustada võrrandiga (13). Toetudes sellele võrrandile, on kerge näidata alamruumi L_i invariantsust lineaarteisenduse $A\boldsymbol{x}$ suhtes. Tõepoolest, olgu $\boldsymbol{x}$ mingi vektor alamruumis L_i. Siis on (13) järgi

$$(A-\lambda_i E)^{\alpha_i}\boldsymbol{x} = 0.$$

Et maatriksi A astmete korrutis on kommutatiivne, siis

$$(A-\lambda_i E)^{\alpha_i} A\boldsymbol{x} = A(A-\lambda_i E)^{\alpha_i}\boldsymbol{x} = A0 = 0,$$

millest nähtub, et ka vektori $\boldsymbol{x}$ teisend $A\boldsymbol{x}$ kuulub alamruumi L_i, s. o. L_i on invariantne lineaarteisenduse A suhtes.

Valides nüüd igas alamruumis L_i mingi baasi, saame kõiki baasivektoreid kokku võttes baasi

$$\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n \tag{14}$$

vektoriruumis K_n. Sellel baasil omab lineaarteisenduse A maatriks kast-diagonaalkuju

$$\bar{A} = \begin{Vmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_m \end{Vmatrix},$$

milles iga maatriksi A_i järk on võrdne vastava alamruumi L_i dimensiooniga d_i (§ 15, art. 3). Näitame, et $d_i = \alpha_i$, kus α_i tähendab karakteristliku väärtuse λ_i kordsust.

Olgu $\boldsymbol{x}$ mingi vektor alamruumis L_i, nii et (13) järgi

$$(A - \lambda_i E)^{\alpha_i} \boldsymbol{x} = 0 .$$

Üle minnes baasile (14), omab viimane võrdus kuju

$$P^{-1}(A - \lambda_i E)^{\alpha_i} P\boldsymbol{u} = 0 ,$$

kus P on maatriks, mille veeruvektoreiks on baasivektorid (14), ja $\boldsymbol{u}$ vektor, mille komponentideks on vektori $\boldsymbol{x}$ komponendid uuel baasil (14) (I, § 23, art. 3). Et

$$P^{-1}(A - \lambda_i E)^{\alpha_i} P =$$
$$= \underbrace{[P^{-1}(A - \lambda_i E)P][P^{-1}(A - \lambda_i E)P] \ldots [P^{-1}(A - \lambda_i E)P]}_{\alpha_i \text{ tegurit}} =$$
$$= (P^{-1}AP - \lambda_i E)^{\alpha_i} = (\bar{A} - \lambda_i E)^{\alpha_i} ,$$

siis rahuldab L_i iga vektor $\boldsymbol{u}$ tingimust

$$(\bar{A} - \lambda_i E)^{\alpha_i} \boldsymbol{u} = 0 ,$$

ehk

$$\left\| \begin{matrix} A_1 - \lambda_i E_1 & & & \\ & A_2 - \lambda_i E_2 & & \\ & & \ddots & \\ & & & A_m - \lambda_i E_m \end{matrix} \right\|^{\alpha_i} \boldsymbol{u} = 0 ,$$

kus E_k tähendab d_k-järku ühikmaatriksit. Ei ole raske veenduda, et kast-diagonaalmaatriksi astendamiseks tuleb astendada eraldi iga kastikest, mistõttu võime kirjutada

$$\begin{Vmatrix} (A_1 - \lambda_i E_1)^{\alpha_i} & & & \\ & (A_2 - \lambda_i E_2)^{\alpha_i} & & \\ & & \ddots & \\ & & & (A_m - \lambda_i E_m)^{\alpha_i} \end{Vmatrix} \boldsymbol{u} = 0 .$$

Et $\boldsymbol{u}$ on alamruumi L_i vektor, siis on kõik tema komponendid baasil (14) nullid peale $u_{d+1}, u_{d+2}, \ldots, u_{d+d_i}$, kus $d = d_1 + d_2 + \ldots + d_{i-1}$. Seetõttu omab viimane tingimus lihtsalt kuju

$$(A_i - \lambda_i E_i)^{\alpha_i} \boldsymbol{v} = 0 ,$$

milles $\boldsymbol{v} = (u_{d+1}, u_{d+2}, \ldots, u_{d+d_i})$ on mistahes d_i-dimensionaalne vektor. Niisugune alamruumi L_i lineaarteisendus aga, mis teisendab L_i iga vektori nullvektoriks, peab olema ilmselt null, s. o.

$$(A_i - \lambda_i E_i)^{\alpha_i} = 0 , \tag{15}$$

mistõttu maatriksi $(A_i - \lambda_i E_i)^{\alpha_i}$ karakteristlikud väärtused tulevad ka nullid. Et viimase maatriksi karakteristlikud väärtused kujutavad maatriksi $A_i - \lambda_i E_i$ karakteristlike väärtuste α_i-ndaid astmeid (art. 1), siis peavad ka maatriksi $A_i - \lambda_i E_i$ karakteristlikud väärtused olema kõik nullid ja seega maatriksi A_i karakteristlikud väärtused kõik võrdsed λ_i-ga. Jääb selgitada λ_i kui A_i karakteristliku väärtuse kordsus, mis määrab maatriksi A_i järgu ja ühtlasi alamruumi L_i dimensiooni d_i.

Vaatleme kast-diagonaalmaatriksi $\bar{A}$ karakteristlikku võrrandit

$$\begin{vmatrix} A_1 - \lambda E_1 & & & \\ & A_2 - \lambda E_2 & & \\ & & \ddots & \\ & & & A_m - \lambda E_m \end{vmatrix} = 0 ,$$

millele võib Laplace'i valemi abil anda kuju (I, § 14, art. 1)

$$|A_1 - \lambda E_1|\,|A_2 - \lambda E_2|\,\ldots\,|A_m - \lambda E_m| = 0\,.$$

Siit nähtub, et A karakteristlikeks väärtusteks on maatriksite A_1, A_2, ..., A_m karakteristlikud väärtused, s. o. λ_1, λ_2, ..., λ_m vastavalt kordustega d_1, d_2, ..., d_m. Et aga sarnaste maatriksite A ja $\bar{A} = P^{-1}AP$ karakteristlikud väärtused langevad ühte (art. 1), siis on λ_i kui $\bar{A}$ karakteristliku väärtuse kordsus d_i võrdne λ_i kui A karakteristliku väärtuse kordsusega α_i, s. o.

$$d_i = \alpha_i\,.$$

3. **Jordani normaalkuju.** Maatriksi A edasiseks taandamiseks lihtsamale kujule märgime

$$A_i - \lambda_i E_i = B_i\,,$$

kus B_i määrab (15) järgi nilpotentse teisenduse α_i-dimensionaalses alamruumis L_i.

Olgu üldiselt B mistahes nilpotentne teisendus mingis vektoriruumis L. Näitame, et vektoriruumi L saab alati lahutada B suhtes tsüklilisteks alamruumide otsesummaks. Määrame naturaalarvu k nii, et oleks

$$B^{k-1} \neq 0\,,\quad B^k = 0$$

ja valime siis vektori $\boldsymbol{a}$ nõnda, et $B^{k-1}\boldsymbol{a} \neq 0$. Siis

$$U = \{c_1\boldsymbol{a} + c_2 B\boldsymbol{a} + c_3 B^2\boldsymbol{a} + \ldots + c_k B^{k-1}\boldsymbol{a}\}$$

kujutab tsüklilist alamruumi B suhtes (§ 15, art. 3). Näitame, et leidub alati B suhtes invariantne alamruum V (mitte tingimata tsükliline), nii et L osutub U ja V otsesummaks, s. o.

$$L = U \dotplus V\,.$$

Vaatleme selleks kõiki L-i invariantseid alamruume, millel ei ole U-ga peale nullvektori teisi ühiseid vektoreid, ja valime nende hulgast välja niisuguse alamruumi V, mille dimensioon on maksimaalne. Et U ja V ei oma peale nullvektori teisi ühi-

seid vektoreid, siis on $U+V$ otsesumma, sest vastasel korral leiduksid alamruumides U ja V vastavalt nullist erinevad vektorid $\boldsymbol{a}_1$ ja $\boldsymbol{a}_2$, nii et (§ 15, art. 2)

$$0=\boldsymbol{a}_1+\boldsymbol{a}_2 \quad \text{ehk} \quad \boldsymbol{a}_1=-\boldsymbol{a}_2,$$

millest nähtub, et $\boldsymbol{a}_1$ kuulub mitte ainult alamruumi U, vaid ka alamruumi V, vastupidi eeldusele. Jääb näidata, et summa $U+V$ sisaldab k õ i k i L vektoreid. Selle tõestuseks kasutame täieliku induktsiooni printsiipi, toetudes nn. vektori kõrguse mõistele. Vektori $\boldsymbol{x}$ k õ r g u s e all mõistame väikseimat astendajat h, mille puhul

$$B^h\boldsymbol{x}=0.$$

Nii on näiteks nullvektori kõrgus null, kusjuures nullvektor on ainuke vektor kõrgusega null, sest $B^0=E$ tõttu on $B^0\boldsymbol{x}=\boldsymbol{x}$. Et eelduse kohaselt $B^k=0$, siis on vektori kõrguse maksimaalne väärtus k. Vektori kõrgus h rahuldab seega tingimust

$$0\leqslant h\leqslant k.$$

Kuna nullvektor on ainuke vektor kõrgusega null, siis võime öelda, et summa $U+V$ sisaldab kõiki vektoreid kõrgusega null. Oletame nüüd, et $U+V$ sisaldab kõiki vektoreid, mille kõrgus ei ületa arvu h ja näitame, et $U+V$ peab siis sisaldama ka kõiki vektoreid kõrgusega $h+1$. Siinjuures võib eeldada, et $h\leqslant k-1$, sest juhul $h=k$ pole enam midagi tõestada.

Olgu $\boldsymbol{x}$ mingi L vektor kõrgusega $h+1$, nii et

$$B^{h+1}\boldsymbol{x}=0.$$

Tuleb näidata, et $\boldsymbol{x}$ kuulub alamruumi $U+V$. Seose

$$B^h(B\boldsymbol{x})=B^{h+1}\boldsymbol{x}=0$$

tõttu omab vektor $B\boldsymbol{x}$ kõrgust h ja kuulub seega induktsioonioletuse põhjal alamruumi $U+V$, mistõttu võime kirjutada

$$B\boldsymbol{x}=\boldsymbol{u}+\boldsymbol{v}, \tag{16}$$

kus $\boldsymbol{u}$ kuulub alamruumi U ja $\boldsymbol{v}$ alamruumi V. Rakendades võrdusele (16) teisendust B^h, saame

$$0 = B^h\boldsymbol{u} + B^h\boldsymbol{v}\,.$$

Et U ja V on invariantsed B suhtes, siis peab $B^h\boldsymbol{u}$ kuuluma alamruumi U ja $B^h\boldsymbol{v}$ alamruumi V, mistõttu

$$B^h\boldsymbol{u} = 0\,, \quad B^h\boldsymbol{v} = 0\,,$$

sest $U + V$ on otsesumma.

Silmas pidades, et $\boldsymbol{u}$ kuulub alamruumi U, võime kirjutada

$$\boldsymbol{u} = c_1\boldsymbol{a} + c_2B\boldsymbol{a} + c_3B^2\boldsymbol{a} + \ldots + c_kB^{k-1}\boldsymbol{a}\,,$$

kust teisenduse B^{k-1} rakendamisel leiame

$$B^{k-1}\boldsymbol{u} = c_1B^{k-1}\boldsymbol{a}\,,$$

sest $B^k\boldsymbol{a} = 0$, $B^{k+1}\boldsymbol{a} = 0$, ... Nüüd on aga $B^h\boldsymbol{u} = 0$ ja seega $h \leqslant k - 1$ tõttu ka $B^{k-1}\boldsymbol{u} = 0$, nii et

$$c_1B^{k-1}\boldsymbol{a} = 0\,,$$

millest $c_1 = 0$, sest $B^{k-1}\boldsymbol{a} \neq 0$. Niisiis omab $\boldsymbol{u}$ kuju

$$\begin{aligned}\boldsymbol{u} &= c_2B\boldsymbol{a} + c_3B^2\boldsymbol{a} + \ldots + c_kB^{k-1}\boldsymbol{a} = \\ &= B(c_2\boldsymbol{a} + c_3B\boldsymbol{a} + \ldots + c_kB^{k-2}\boldsymbol{a})\end{aligned}$$

ehk

$$\boldsymbol{u} = B\boldsymbol{u}'\,,$$

kus vektor $\boldsymbol{u}'$ kuulub ka alamruumi U. Seega on võrduse (16) järgi

$$B\boldsymbol{x} = B\boldsymbol{u}' + \boldsymbol{v}$$

ehk

$$B(\boldsymbol{x} - \boldsymbol{u}') = \boldsymbol{v}\,. \tag{17}$$

Vaatleme vektorite hulka

$$W = \{c(\boldsymbol{x} - \boldsymbol{u}') + \boldsymbol{v}'\}\,,$$

kus c võib olla mistahes element põhikorpuses K ja $\boldsymbol{v}'$ mistahes vektor alamruumis V. Hulk W kui alamruumide $\{c(\boldsymbol{x} - \boldsymbol{u}')\}$

ja V summa kujutab ise ka alamruumi, mis sisaldab alamruumi V. Seejuures on W invariantne B suhtes, sest (17) tõttu on

$$B[c(x-u')+v'] = cB(x-u')+Bv' = cv+Bv',$$

kus Bv' kuulub alamruumi V. Eritleme kahte juhtu selle järgi, kas $W=V$ või $W \neq V$.

1° Kui $W=V$, siis peab eriti vektor $x-u'$ kuuluma alamruumi V. Et $x=u'+(x-u')$, siis kuulub x alamruumi $U+V$.

2° Kui $W \neq V$, siis W — sisaldades alamruumi V — peab omama kõrgemat dimensiooni kui V. Kuid V oli valiku kohaselt maksimaalse dimensiooniga kõigi nende invariantsete alamruumide hulgas, millel ei olnud U-ga ühiseid vektoreid peale nullvektori. Järelikult on alamruumidel U ja W ühine nullist erinev vektor w, mis kui alamruumi W vektor peab omama kuju

$$w = c(x-u')+v'.$$

Siin $c \neq 0$, sest vastasel korral oleks $w=v'$ ja $w \neq 0$ kujutaks U ja V ühist vektorit, vastuolus V valikuga. Seega saame ülemisest võrdusest

$$x = (u'+\tfrac{1}{c}w)+(-\tfrac{1}{c}v'),$$

millest nähtub, et x kuulub alamruumi $U+V$.

Niisiis oleme lahutanud vektoriruumi L alamruumide otsesummaks

$$L = U \dotplus V,$$

kus U on tsükliline ja V invariantne B suhtes. Kui siin V ei peaks osutuma tsüklilliseks, siis, rakendades kogu eespool arendatud mõttekäiku V kohta, lahutame V omakorda ühe tsüklilise ja ühe invariantse alamruumi otsesummaks jne. Et iga niisuguse otsesummaks lahutuse puhul alamruumide dimensioonid kahanevad, siis peab see lahutuse protsess kord lõppema, s. o. peab kord tulema moment, kus kõik alamruumid osutuvad

tsüklilisteks. Tähendab, *vektoriruumi L saab alati lahutada nilpotentse teisenduse B suhtes tsükliliste alamruumide otsesummaks.*

Jätkame nüüd kast-diagonaalmaatriksi

$$\begin{Vmatrix} A_1 & & & & \\ & A_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & A_m \end{Vmatrix}$$

taandamist lihtsaimale kujule. Vaatleme selleks iga kastikese A_i asemel vahet

$$A_i - \lambda_i E_i = B_i,$$

mis määrab, nagu nägime, nilpotentse teisenduse alamruumis L_i. Lahutame alamruumi L_i eespool näidatud viisil tsükliliste alamruumide otsesummaks

$$L_i = L_{i1} + L_{i2} + \ldots + L_{ir_i}.$$

Valides siin igas alamruumis L_{ik} tsüklilise baasi, saame neid baase ühendades baasi alamruumis L_i. Sellel baasil omab nilpotentse teisenduse B_i maatriks alamruumide L_{ik} invariantsuse tõttu kast-diagonaalkuju

$$\bar{B}_i = \begin{Vmatrix} B_{i1} & & & & \\ & B_{i2} & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & B_{ir_i} \end{Vmatrix},$$

kus maatriksid B_{ik} kujutavad Jordani kastikesi (§ 15, art. 3), s. o.

$$B_{ik} = \begin{Vmatrix} 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & 1 & 0 \end{Vmatrix}.$$

Et $A_i = B_i + \lambda_i E_i$, siis, märkides P_i-ga maatriksi, mille veeruvektoreiks on L_i uued baasivektorid, saame A_i-le uuel L_i baasil kuju (I, § 23, art. 3)

$$\bar{A}_i = P_i^{-1} A_i P_i = P_i^{-1} B_i P_i + \lambda_i P_i^{-1} P_i = \bar{B}_i + \lambda_i E_i ,$$

millest nähtub, et

$$\bar{A}_i = \begin{Vmatrix} A_{i1} & & & & \\ & A_{i2} & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & A_{ir_i} \end{Vmatrix},$$

kus

$$A_{ik} = B_{ik} + \lambda_i E_{ik} = \begin{Vmatrix} \lambda_i & 0 & \dots & 0 & 0 \\ 1 & \lambda_i & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \lambda_i \end{Vmatrix}. \tag{18}$$

Seega võib igale maatriksile A anda kohase baasi valiku teel kast-diagonaalkuju

$$\bar{A} = \begin{Vmatrix} A_{11} & & & & \\ & A_{12} & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & A_{mr_m} \end{Vmatrix}, \tag{19}$$

mis kannab maatriksi A Jordani normaalkuju nime. Et maatriksi A Jordani normaalkuju oleks täiesti määratud, selleks peame teadma veel iga kastikese A_{ik} järku, s. o. iga tsüklilise alamruumi L_{ik} dimensiooni n_{ik}. Vastuse sellele küsimusele anname järgmises paragrahvis, rakendades A karakteristlikule maatriksile polünoommaatriksite teooriat. Ühtlasi saame siis ka lihtsa praktilise võtte maatriksi A Jordani normaalkuju leidmiseks, kuna käesolevas paragrahvis arendatud mõttekäigud,

mis tõestasid Jordani normaalkuju olemasolu, omavad eeskätt teoreetilist väärtust.

§ 17. Polünoommaatriksite teooria rakendus Jordani normaalkujule.

1. Jordani normaalkuju kastikeste järgud. Vaatleme maatriksi A karakteristlikku maatriksit $A - \lambda E$. Maatriksi $A - \lambda E$ kui polünoommaatriksi elementaarjagajaid nimetame edaspidi lihtsalt maatriksi A elementaarjagajateks. Näitame kõigepealt, et sarnastel maatriksitel A ja $\bar{A} = P^{-1}AP$ on ühed ja samad elementaarjagajad. Tõepoolest, korrutades maatriksit $A - \lambda E$ paremalt P-ga ja vasakult P^{-1}-ga saame

$$P^{-1}(A - \lambda E)P = P^{-1}AP - \lambda P^{-1}P = \bar{A} - \lambda E,$$

millest nähtub, et maatriksid $A - \lambda E$ ja $\bar{A} - \lambda E$ on ekvivalentsed, sest P ja P^{-1} kui konstantsete elementidega maatriksid on unimodulaarsed. Ekvivalentsetel maatriksitel on aga ühed ja samad elementaarjagajad (§ 14, art. 3).

Seame nüüd endale ülesandeks leida Jordani maatriksi (19) elementaarjagajad. Määrame selleks enne maatriksi (18) elementaarjagajad, s. o. polünoommaatriksi

$$(20) \qquad A_{ik} - \lambda E_{ik} = \begin{Vmatrix} \lambda_i - \lambda & 0 & \dots & 0 & 0 \\ 1 & \lambda_i - \lambda & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \lambda_i - \lambda \end{Vmatrix}$$

elementaarjagajad $e_1(\lambda)$, $e_2(\lambda)$, ..., $e_j(\lambda)$, kus $j = n_{ik}$ tähendab maatriksi A_{ik} järku. Leiame algul determinantjagajad $d_1(\lambda)$, $d_2(\lambda)$, ..., $d_j(\lambda)$. Siin $d_j(\lambda)$ on lihtsalt maatriksi (20) determinant kui λ polünoom normeeritud kujul, s. o.

$$d_j(\lambda) = (\lambda - \lambda_i)^j.$$

Edasi d_{j-1} on maatriksi (20) kõigi $(j-1)$-järku determinantide

suurim ühistegur. Et nende $(j-1)$-järku determinantide hulgas leidub determinant

$$\begin{vmatrix} 1 & \lambda_i-\lambda & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{vmatrix} = 1,$$

mis saadakse maatriksist (20) esimese rea ja viimase veeru ärajätmisel, siis on

$$d_{j-1}(\lambda) = 1.$$

Kasutades valemeid (§ 14, art. 2)

$$d_{j-1}(\lambda) = e_1(\lambda)e_2(\lambda)\dots e_{j-1}(\lambda), \quad e_j(\lambda) = \frac{d_j(\lambda)}{d_{j-1}(\lambda)},$$

leiame seetõttu

$$e_1(\lambda) = e_2(\lambda) = \dots e_{j-1}(\lambda) = 1, \quad e_j(\lambda) = (\lambda-\lambda_i)^j.$$

Seega võib polünoommaatriksile (20) anda elementaarteisenduste teel normaalkuju

$$N_{ik} = \begin{Vmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & (\lambda-\lambda_i)^j \end{Vmatrix}.$$

Toimides sel viisil iga polünoommaatriksiga (20), saame Jordani maatriksi (19) karakteristlikule maatriksile kuju

$$(21) \qquad \begin{Vmatrix} N_{11} & & & & \\ & N_{12} & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & N_{mr_m} \end{Vmatrix},$$

mis ei ole aga veel normaalkuju, sest siin diagonaali iga element ei jagu eelnevatega.

Leiame nüüd maatriksi (21) elementaarjagajad

$$e_1(\lambda),\ e_2(\lambda),\ \ldots,\ e_n(\lambda),$$

mis kujutavad ühtlasi ka otsitavaid Jordani maatriksi (19) elementaarjagajaid. Määrame algul determinantjagajad

$$d_1(\lambda),\ d_2(\lambda),\ \ldots,\ d_n(\lambda).$$

Siin $d_n(\lambda)$ kui maatriksi (21) determinant omab kuju

$$d_n(\lambda) = (\lambda - \lambda_1)^{n_{11}+n_{12}+\ldots+n_{1r_1}} \ldots (\lambda - \lambda_m)^{n_{m1}+n_{m2}+\ldots+n_{mr_m}},$$

milles tegur $\lambda - \lambda_i$ esineb astendajaga

$$n_{i1} + n_{i2} + \ldots + n_{ir_i}.$$

Olgu viimases summas liidetavad korraldatud kahanevas järjekorras, s. o.

$$n_{i1} \geqslant n_{i2} \geqslant \ldots \geqslant n_{ir_i}.$$

Siis ei ole raske näha, et determinantjagajas $d_{n-1}(\lambda)$, mis kujutab maatriksi (21) $(n-1)$-järku determinantide suurimat ühistegurit, esineb tegur $(\lambda - \lambda_i)$ astendajaga

$$n_{i2} + n_{i3} + \ldots + n_{ir_i},$$

sest maatriksi (21) ühe rea ja veeru ärajätmisel võib välja langeda tegur $\lambda - \lambda_i$ ülimalt astendajaga n_{i1}. Seega

$$d_{n-1}(\lambda) = (\lambda - \lambda_1)^{n_{12}+n_{13}+\ldots+n_{1r_1}} \ldots (\lambda - \lambda_m)^{n_{m2}+n_{m3}+\ldots+n_{mr_m}}.$$

Analoogiliselt veendume, et determinantjagajas $d_{n-2}(\lambda)$, mis kujutab maatriksi (21) $(n-2)$-järku determinantide suurimat ühistegurit, esineb tegur $(\lambda - \lambda_i)$ astendajaga

$$n_{i3} + n_{i4} + \ldots + n_{ir_i},$$

sest maatriksi (21) kahe rea ja veeru ärajätmisel võib välja langeda tegur $\lambda - \lambda_i$ ülimalt astendajaga $n_{i1} + n_{i2}$. Seega

$$d_{n-2}(\lambda) = (\lambda - \lambda_1)^{n_{13}+n_{14}+\ldots+n_{1r_1}} \ldots (\lambda - \lambda_m)^{n_{m3}+n_{m4}+\ldots+n_{mr_m}}$$

jne. Kasutades valemit (§ 14, art. 2)

$$e_k(\lambda) = \frac{d_k(\lambda)}{d_{k-1}(\lambda)}, \qquad k = 1,\ 2,\ \ldots,\ n,$$

saame

$$e_n(\lambda) = (\lambda - \lambda_1)^{n_{11}}(\lambda - \lambda_2)^{n_{21}} \ldots (\lambda - \lambda_m)^{n_{m1}}$$
$$e_{n-1}(\lambda) = (\lambda - \lambda_1)^{n_{12}}(\lambda - \lambda_2)^{n_{22}} \ldots (\lambda - \lambda_m)^{n_{m2}}$$
$$e_{n-2}(\lambda) = (\lambda - \lambda_1)^{n_{13}}(\lambda - \lambda_2)^{n_{23}} \ldots (\lambda - \lambda_m)^{n_{m3}}$$

jne.

Silmas pidades, et maatriks A on sarnane Jordani maatriksiga (19), peavad viimati leitud elementaarjagajad olema ühtlasi maatriksi A elementaarjagajateks ja on seetõttu maatriksiga A üheselt määratud. Seega saame maatriksi A Jordani normaalkuju leidmiseks järgmise eeskirja:

1^0 leiame maatriksi A elementaarjagajad $e_1(\lambda), e_2(\lambda), \ldots, e_n(\lambda)$;

2^0 lahendades võrrandi $e_n(\lambda) = 0$, määrame maatriksi A erinevad karakteristlikud väärtused $\lambda_1, \lambda_2, \ldots, \lambda_m$;

3^0 leiame igale karakteristlikule väärtusele λ_i vastavate kastikeste $A_{i1}, A_{i2}, \ldots, A_{ir_i}$ järgud $n_{i1}, n_{i2}, \ldots, n_{ir_i}$ kui teguri $\lambda - \lambda_i$ astendajad elementaarjagajates $e_n(\lambda), e_{n-1}(\lambda), \ldots, e_{n-r_i+1}(\lambda)$.

Ühtlasi nähtub siit, et maatriksi Jordani normaalkuju on kuni kastikeste A_{ik} järjekorrani üheselt määratud.

Näide 2. Leida maatriksi

$$A = \begin{Vmatrix} 4 & -1 & 0 & 0 \\ 4 & 0 & 0 & 0 \\ -4 & 2 & 2 & 0 \\ -4 & -1 & 0 & -1 \end{Vmatrix}$$

Jordani normaalkuju.

Moodustame A karakteristliku maatriksi

$$A - \lambda E = \begin{Vmatrix} 4-\lambda & -1 & 0 & 0 \\ 4 & -\lambda & 0 & 0 \\ -4 & 2 & 2-\lambda & 0 \\ -4 & -1 & 0 & -1-\lambda \end{Vmatrix}$$

ja leiame tema elementaarjagajad. Varem näidatud viisil saame (§ 14, art. 1)

$$e_1(\lambda) = 1\,,\quad e_2(\lambda) = 1\,,\quad e_3(\lambda) = \lambda - 2\,,\quad e_4(\lambda) = \\ = (\lambda - 2)^2(\lambda + 1)\,.$$

Seega maatriksi A erinevad karakteristlikud väärtused on

$$\lambda_1 = 2\,,\quad \lambda_2 = -1\,,$$

kusjuures karakteristlikule väärtusele $\lambda_1 = 2$ vastab üks teist ja üks esimest järku kastike ning karakteristlikule väärtusele $\lambda_2 = -1$ üks esimest järku kastike, nii et maatriksi A Jordani normaalkuju on

$$\begin{Vmatrix} 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & -1 \end{Vmatrix}.$$

2. Järeldusi Jordani normaalkujust. Eeldades, et maatriksi karakteristlikud väärtused kuuluvad korpusse K, lahendame Jordani normaalkuju abil kaks põhiküsimust maatriksite teooriast.

1° Küsime, missugusel tingimusel taandub antud maatriks A diagonaalkujule (I, § 23, art. 1). Teiste sõnadega, missugusel tingimusel osutub maatriksi A Jordani normaalkuju diagonaalmaatriksiks. Jordani maatriks, koosnedes üksikutest kastikestest A_{ik}, kujutab diagonaalmaatriksit siis ja ainult siis, kui iga kastike A_{ik} taandub üheksainsaks elemendiks. Et kastikese A_{ik} järk on võrdne teguri $\lambda - \lambda_i$ astendajaga maatriksi A elementaarjagajas $e_{n-k+1}(\lambda)$, siis on kõik kastikesed A_{ik} esimest järku, kui A elementaarjagajad ei oma kordseid lahendeid. Seega oleme saanud järgmise teoreemi:

Teoreem 2. *Maatriks taandub diagonaalkujule siis ja ainult siis, kui selle maatriksi elementaarjagajad ei oma kordseid lahendeid.*

Nii taandub näiteks maatriks

$$\begin{Vmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{Vmatrix}$$

diagonaalkujule, sest tema elementaarjagajad

$$e_1(\lambda) = 1\,,\quad e_2(\lambda) = \lambda + 1\,,\quad e_3(\lambda) = \lambda + 1\,,$$
$$e_4(\lambda) = (\lambda + 1)(\lambda - 3)$$

ei oma kordseid lahendeid.

2⁰ Küsime, missugusel tingimusel on kaks antud maatriksit A ja $\bar{A}$ sarnased. Nagu nägime (art. 1), on sarnastel maatriksitel A ja $\bar{A}$ ühed ja samad elementaarjagajad. Ümberpöördult, kui maatriksite A ja $\bar{A}$ elementaarjagajad langevad ühte, siis saame neile maatriksitele ühe ja sama Jordani normaalkuju, mis on seega sarnane niihästi A-ga kui ka $\bar{A}$-ga. Järelikult peavad A ja $\bar{A}$ olema sarnased ka omavahel. Seega oleme saanud järgmise teoreemi:

T e o r e e m 3. *Kaks maatriksit on sarnased siis ja ainult siis, kui neil maatriksitel on ühed ja samad elementaarjagajad.*

Nii on näiteks maatriksid

$$A = \begin{Vmatrix} 1 & 2 & 2 \\ 0 & -1 & -1 \\ 0 & 0 & -1 \end{Vmatrix}, \qquad \bar{A} = \begin{Vmatrix} 5 & 0 & 2 \\ -12 & 0 & -5 \\ -12 & 1 & -6 \end{Vmatrix}$$

sarnased, sest, nagu näitab arvutus, on neil ühised elementaarjagajad

$$e_1(\lambda) = 1\,,\quad e_2(\lambda) = 1\,,\quad e_3(\lambda) = (\lambda - 1)(\lambda + 1)^2.$$

3. Jordani normaalkujule vastava baasi leidmine. Seame lõppeks küsimuse, kuidas leida baasi

$$\boldsymbol{b}_1\,,\ \boldsymbol{b}_2\,,\ \ldots\,,\ \boldsymbol{b}_n\,,$$

millel teisendus A omab Jordani normaalkuju $\bar{A}$.

Olgu $P = \| p_{ik} \|$ maatriks, mille veeruvektoriteks on baasi-

vektorid $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$, nii et $\boldsymbol{p}^k = \boldsymbol{b}_k$. Siis peab olema (I, § 23, art. 3)

$$P^{-1}AP = \bar{A},$$

millest

$$AP = P\bar{A}.$$

Ei ole raske näha, et korrutise AP veeruvektoreid võib avaldada kujul

$$A\boldsymbol{p}^1, \ A\boldsymbol{p}^2, \ldots, \ A\boldsymbol{p}^n$$

ja analoogiliselt korrutise $P\bar{A}$ veeruvektoreid kujul

$$P\bar{\boldsymbol{a}}^1, \ P\bar{\boldsymbol{a}}^2, \ldots, \ P\bar{\boldsymbol{a}}^n,$$

kus $\bar{\boldsymbol{a}}^k$ tähendab maatriksi $\bar{A}$ k-nda veeru vektorit.

Vaatleme kõigepealt Jordani maatriksi $\bar{A}$ neid veeruvektoreid $\bar{\boldsymbol{a}}^1, \bar{\boldsymbol{a}}^2, \ldots, \bar{\boldsymbol{a}}^j$, mis vastavad esimesele kastikesele A_{11}, kus j tähendab kastikese A_{11} järku n_{11}. Et

$$A_{11} = \left\| \underbrace{\begin{matrix} \lambda_1 & 0 & \ldots & 0 & 0 \\ 1 & \lambda_1 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & \lambda_1 \end{matrix}}_{j \text{ veergu}} \right\|,$$

siis on

$$\begin{aligned} \bar{\boldsymbol{a}}^1 &= (\lambda_1, 1, 0, 0, \ldots, 0) = \lambda_1 \boldsymbol{e}_1 + \boldsymbol{e}_2 \\ \bar{\boldsymbol{a}}^2 &= (0, \lambda_1, 1, 0, \ldots, 0) = \lambda_1 \boldsymbol{e}_2 + \boldsymbol{e}_3 \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \bar{\boldsymbol{a}}^{j-1} &= (0, \ldots, 0, \lambda_1, 1, 0, \ldots, 0) = \lambda_1 \boldsymbol{e}_{j-1} + \boldsymbol{e}_j \\ \bar{\boldsymbol{a}}^j &= (\underbrace{0, \ldots, 0}_{j-1 \text{ nulli}}, 0, \lambda_1, 0, \ldots, 0) = \lambda_1 \boldsymbol{e}_j, \end{aligned}$$

kus $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_{j-1}, \boldsymbol{e}_j$ on n-dimensionaalsed ühikvektorid. Silmas pidades, et ühikvektorite teisendid kujutavad vastava

lineaarteisenduse maatriksi veeruvektoreid, s. o. $Pe_k = p^k$ (I, § 20, art. 1), leiame

$$\begin{aligned}
P\bar{a}^1 &= P(\lambda_1 e_1 + e_2) = \lambda_1 Pe_1 + Pe_2 = \lambda_1 p^1 + p^2 \\
P\bar{a}^2 &= P(\lambda_1 e_2 + e_3) = \lambda_1 Pe_2 + Pe_3 = \lambda_1 p^2 + p^3 \\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
P\bar{a}^{j-1} &= P(\lambda_1 e_{j-1} + e_j) = \lambda_1 Pe_{j-1} + Pe_j = \lambda_1 p^{j-1} + p^j \\
P\bar{a}^j &= P(\lambda_1 e_j) = \lambda_1 Pe_j = \lambda_1 p^j .
\end{aligned}$$

Võrreldes korrutiste AP ja $P\bar{A}$ esimest j veeruvektorit, saame seega

$$\begin{aligned}
Ap^1 &= \lambda_1 p^1 + p^2 & & (A - \lambda_1 E)p^1 = p^2 \\
Ap^2 &= \lambda_1 p^2 + p^3 & & (A - \lambda_1 E)p^2 = p^3 \\
&\dots\dots\dots & \text{ehk} & \dots\dots\dots \\
Ap^{j-1} &= \lambda_1 p^{j-1} + p^j & & (A - \lambda_1 E)p^{j-1} = p^j \\
Ap^j &= \lambda_1 p^j & & (A - \lambda_1 E)p^j = 0 .
\end{aligned}$$

Siin viimane maatriksvõrrand kujutab p^j komponentide suhtes homogeenset lineaarset võrrandisüsteemi, mille determinant

$$|A - \lambda_1 E| = 0 ,$$

sest λ_1 on maatriksi A karakteristlik väärtus. Seega on sel süsteemil nullist erinev lahend p^j. Teades p^j, arvutame p^{j-1} eelviimasest maatriksvõrrandist, mis kujutab p^{j-1} komponentide suhtes mittehomogeenset lineaarset võrrandisüsteemi. Teades p^{j-1}, arvutame eelnevast maatriksvõrrandist omakorda p^{j-2} jne., kuni lõppeks arvutame esimesest maatriksvõrrandist p^1.

Vastavalt igale Jordani maatriksi kastikesele A_{ik} saame analoogilised maatriksvõrrandite süsteemid, mida lahendades leiame kõik vektorid $p^k = b_k$. Juhul, kui mõned maatriksvõrrandid langevad ühte, tuleb lahendite valikul silmas pidada, et vektorid

$$p^1, p^2, \dots, p^n$$

oleksid lineaarselt sõltumatud, sest P peab olema regulaarne.

Näide 3. Leida baas, millel maatriks

$$\begin{Vmatrix} 4 & -1 & 0 & 0 \\ 4 & 0 & 0 & 0 \\ -4 & 2 & 2 & 0 \\ -4 & -1 & 0 & -1 \end{Vmatrix}$$

omab Jordani normaalkuju.

Näite 2 järgi on maatriksil A kaks erinevat karakteristlikku väärtust $\lambda_1 = 2$, $\lambda_2 = -1$, millest esimesele vastab üks teist ja üks esimest järku kastike ning teisele üks esimest järku kastike (art. 1). Vastavalt sellele saame otsitavate baasivektorite $\boldsymbol{p}^1$, $\boldsymbol{p}^2$, $\boldsymbol{p}^3$, $\boldsymbol{p}^4$ määramiseks maatriksvõrrandid

$$\begin{Vmatrix} 2 & -1 & 0 & 0 \\ 4 & -2 & 0 & 0 \\ -4 & 2 & 0 & 0 \\ -4 & -1 & 0 & -3 \end{Vmatrix} \boldsymbol{p}^1 = \boldsymbol{p}^2, \qquad \begin{Vmatrix} 2 & -1 & 0 & 0 \\ 4 & -2 & 0 & 0 \\ -4 & 2 & 0 & 0 \\ -4 & -1 & 0 & -3 \end{Vmatrix} \boldsymbol{p}^2 = 0,$$

$$\begin{Vmatrix} 2 & -1 & 0 & 0 \\ 4 & -2 & 0 & 0 \\ -4 & 2 & 0 & 0 \\ -4 & -1 & 0 & -3 \end{Vmatrix} \boldsymbol{p}^3 = 0, \qquad \begin{Vmatrix} 5 & -1 & 0 & 0 \\ 4 & 1 & 0 & 0 \\ -4 & 2 & 3 & 0 \\ -4 & -1 & 0 & 0 \end{Vmatrix} \boldsymbol{p}^4 = 0,$$

mida lahendades leiame

$$\boldsymbol{p}^2 = (1, 2, -2, -2), \qquad \boldsymbol{p}^1 = (0, -1, 0, 1),$$
$$\boldsymbol{p}^3 = (0, 0, 1, 0), \qquad \boldsymbol{p}^4 = (0, 0, 0, 1).$$

Harjutusülesandeid.

83. Anda polünoommaatriksitele

a) $\begin{Vmatrix} x-1 & -x^2 & x \\ x & x & x \\ x^2+1 & x^2 & x^2 \end{Vmatrix}$; b) $\begin{Vmatrix} 1 & -x & x-1 & 0 \\ 0 & x & -1 & x-1 \\ x-1 & 0 & 1 & x \\ 1 & x-1 & 0 & x \end{Vmatrix}$

normaalkuju.

84. Leida maatriksite

a) $\begin{Vmatrix} x & 1 & 0 & 0 \\ 0 & x & 1 & 0 \\ 0 & 0 & x & 1 \\ 1 & 1 & x & x+1 \end{Vmatrix}$; b) $\begin{Vmatrix} x(x+1) & 0 & 0 & 0 \\ 0 & x^2 & 0 & 0 \\ 0 & 0 & (x+1)^2 & 0 \\ 0 & 0 & 0 & x(x-1) \end{Vmatrix}$;

c) $\begin{Vmatrix} x+a & b & 1 & 0 \\ -b & x+a & 0 & 1 \\ 0 & 0 & x+a & b \\ 0 & 0 & -b & x+a \end{Vmatrix}$

determinantjagajad.

85. Kas polünoommaatriksid

$$F = \begin{Vmatrix} x^2-1 & x-1 & -1 & 2x-2 \\ x & 1 & 1 & 2 \\ 2 & x+1 & x+2 & 4 \\ x+1 & 2 & 3 & -x+5 \end{Vmatrix},$$

$$G = \begin{Vmatrix} -3x+1 & 2x-1 & x^2 & x^2-5x+2 \\ 1 & x-1 & x^2-1 & -2x+2 \\ x+1 & -x & x-2 & 2 \\ -x+3 & x-2 & x^2-x-1 & -3x+5 \end{Vmatrix}$$

on ekvivalentsed?

86. Näidata, et polünoommaatriksite teooria on täielikult üle kantav täisarvulistele, s. o. täisarvuliste elementidega maatriksitele.

87. Leida täisarvulise maatriksi

$$\begin{Vmatrix} 11 & 12 & -7 & 1 \\ -2 & -4 & 4 & 2 \\ 6 & 8 & 0 & -2 \\ 3 & 4 & -1 & -1 \end{Vmatrix}$$

determinantjagajad ja elementaarjagajad.

88. Näidata, et täisarvulised maatriksid

$$F = \begin{Vmatrix} -5 & 3 & 2 \\ -9 & 5 & -4 \\ 5 & -3 & 4 \end{Vmatrix}, \quad G = \begin{Vmatrix} -3 & -3 & -6 \\ -3 & -1 & -4 \\ 4 & 4 & 6 \end{Vmatrix}$$

on ekvivalentsed ning leida unimodulaarmaatriksid U ja V nii, et oleks $G = UFV$.

89. Leida neljadimensionaalse vektoriruumi K_4 alamruumide

$$\text{a) } \{A\boldsymbol{x}\}; \qquad \text{b) } A\boldsymbol{x} = 0$$

dimensioonid, kui

$$A = \begin{Vmatrix} 1 & 5 & 3 & -1 \\ 3 & 2 & -1 & 4 \\ -7 & 4 & 3 & -8 \\ -5 & 1 & -1 & -3 \end{Vmatrix}.$$

90. Leida ülesande 89 alamruumide summa. Kas viimane kujutab otsesummat?

91. Näidata, et alamruum $\{(2c_1, -c_1, -c_2, c_2)\}$ on invariantne maatriksiga

$$A = \begin{Vmatrix} 1 & 0 & 2 & -2 \\ 0 & 1 & -4 & -2 \\ 2 & -1 & 0 & 3 \\ -2 & 1 & 1 & -2 \end{Vmatrix},$$

määratud lineaarteisenduse suhtes.

92. Leida ühedimensionaalsed alamruumid, mis jäävad invariantseks ülesande 91 lineaarteisenduse suhtes.

93. Olgu n-järku maatriksi A karakteristlikud väärtused kõik üksteisest erinevad. Näidata, et siis kõigi A suhtes invariantsete alamruumide arv n-dimensionaalses vektoriruumis on 2^n.

94. Näidata, et maatriks

$$\begin{Vmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ a_{21} & 0 & 0 & \dots & 0 & 0 \\ a_{31} & a_{32} & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & 0 \\ a_{n1} & a_{n2} & a_{n3} & & a_{n,n-1} & 0 \end{Vmatrix}$$

määrab nilpotentse teisenduse.

95. Leida vektoriruumis K_4 üks kolmedimensionaalne tsükliline alamruum maatriksiga

$$B = \begin{Vmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{Vmatrix}$$

määratud nilpotentse teisenduse suhtes.

96. Kontrollida maatriksi

$$\begin{Vmatrix} 2 & 3 & 5 \\ 4 & 2 & 1 \\ 3 & 6 & 2 \end{Vmatrix}$$

puhul Hamilton-Cayley' seost, kui selle maatriksi elemendid kuuluvad jäägiklassikorpusse $R^{(7)}$.

97. Leida vektoriruumis K_4 võrranditega $(A - \lambda_i E)^{\alpha_i} x = 0$ määratud alamruumid, kui

$$A = \begin{Vmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{Vmatrix}.$$

98. Leida maatriksite

a) $\begin{Vmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{Vmatrix}$; b) $\begin{Vmatrix} -5 & -3 & -2 & 4 \\ 2 & 0 & 1 & -1 \\ 10 & 7 & 4 & -9 \\ 2 & 0 & 1 & 0 \end{Vmatrix}$; c) $\begin{Vmatrix} -2 & -1 & -1 & 3 & 2 \\ -4 & 1 & -1 & 3 & 2 \\ 1 & 1 & 0 & -3 & -2 \\ -4 & -2 & -1 & 5 & 1 \\ 4 & 1 & 1 & -3 & 0 \end{Vmatrix}$

Jordani normaalkuju.

99. Kas maatriksid

a) $\begin{Vmatrix} 1 & 6 & 1 \\ 1 & 1 & 6 \\ 6 & 1 & 1 \end{Vmatrix}$; b) $\begin{Vmatrix} 3 & 1 & 4 \\ 0 & 5 & 2 \\ 5 & 6 & 4 \end{Vmatrix}$

taanduvad diagonaalkujule, kui nende elemendid kuuluvad jäägiklassikorpusse $R^{(7)}$?

100. Näidata, et nn. idempotentne maatriks A, mille puhul $A^2 = A$, taandub diagonaalkujule, kusjuures peadiagonaali elemendid tulevad ühed ja nullid.

101. Missugused maatriksitest

$$\text{a)} \begin{Vmatrix} 3 & 1 & -3 \\ -4 & -2 & 12 \\ -1 & -1 & 5 \end{Vmatrix}; \quad \text{b)} \begin{Vmatrix} 2 & 1 & -1 \\ 7 & 4 & -22 \\ 2 & 1 & -5 \end{Vmatrix}; \quad \text{c)} \begin{Vmatrix} 2 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & -1 & 3 \end{Vmatrix}$$

on omavahel sarnased?

102. Leida baas, millel maatriksid

$$\text{a)} \begin{Vmatrix} 3 & 1 & 0 \\ -4 & -1 & 0 \\ 4 & -8 & -2 \end{Vmatrix}; \quad \text{b)} \begin{Vmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{Vmatrix}$$

omavad Jordani normaalkuju.

VI. Rühmateooria alused.

§ 18. Rühma mõiste.

1. Sümmeetriline rühm. Vaatleme mingit hulka G, mille elemente märgime tähtedega a, b, c, ... Olgu selles hulgas defineeritud üks arvutusoperatsioon, s. o. olgu G igale kahele kindlas järjekorras võetud elemendile a ja b seatud vastavusse teatav kolmas element v, mida nimetame harilikult elementide a ja b korrutiseks ning kirjutame $v = ab$.

Definitsioon 1. Ühe operatsiooniga hulka G nimetatakse rühmaks, kui hulgas G defineeritud operatsioon rahuldab alljärgnevat nelja arvutusseadust:

I. Korrutamise seadus: korrutis ab on teguritega a ja b üheselt määratud G element.

II. Assotsiatiivsuse seadus:

$$a(bc) = (ab)c.$$

III. Ühikelemendi olemasolu seadus: hulgas G leidub vähemalt üks element e, mis rahuldab tingimust

$$ae = a$$

G iga elemendi a puhul ja mida nimetatakse parempoolseks ühikelemendiks.

IV. Pöördelemendi olemasolu seadus: vastavalt igale elemendile a leidub hulgas G vähemalt üks element a^{-1}, mis rahuldab tingimust

$$aa^{-1} = e,$$

ja mida nimetatakse a parempoolseks pöördelemendiks.

Rühma defineerivad arvutusseadused I—IV kannavad rühma postulaatide nime. Kui rühmas G kehtib peale arvutusseaduste I—IV veel kommutatiivsuse seadus $ab = ba$, siis kõneldakse kommutatiivsest ehk Abeli rühmast. Rühma mõiste on üks neid kaasaegse matemaatika põhimõisteid, mis, koondades endas kõik arvudega opereerimisel ilmnevad olulised tehte omadused, on leidnud peale algebra tähelepandavaid rakendusi veel paljudes teistes matemaatilistes distsipliinides, nagu geomeetrias, kompleksmuutuja funktsiooniteoorias, kvantide mehhaanikas jm.

Vaatleme kõigepealt nn. sümmeetrilist rühma, mis etendab tähtsat osa algebraliste võrrandite teoorias ja mille uurimine on andnudki tõuke üldise rühmateooria tekkimiseks. Olgu antud n elementi, mida märgime lihtsuse mõttes numbritega $1, 2, \ldots, n$ ja olgu $a_1 a_2 \ldots a_n$ mingi permutatsioon numbritest $1, 2, \ldots, n$. Seame numbrile 1 vastavusse numbri a_1, numbrile 2 numbri a_2 jne., lõppeks numbrile n numbri a_n. Sel viisil saame numbrite hulga $\{1, 2, \ldots, n\}$ üksühese vastavuse iseendaga, mida nimetatakse substitutsiooniks ja märgitakse sümboliga

$$s = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}.$$

Siin seisab iga numbri all see number, mis vastab vaadeldavale numbrile substitutsioonis s. Öeldakse ka, et substitutsioon s teisendab numbri 1 numbriks a_1, numbri 2 numbriks a_2 jne., lõppeks numbri n numbriks a_n.

Substitutsioonis s esinevate numbrite arv n kannab substitutsiooni astme nime. Et erinevaid permutatsioone numbritest $1, 2, \ldots, n$ on üldse $n!$ tükki (I, § 5, art. 4), siis leidub ka $n!$ erinevat n-astme substitutsiooni. Substitutsioonide märkimisel tuleb silmas pidada, et siin pole oluline ülemise rea numbrite järjekord. Nii kujutavad sümbolid

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

ühte ja sama substitutsiooni, sest mõlemate puhul vastab 1-le 3, 2-le 4, 3-le 2 ja 4-le 1.

Olgu antud kaks n-astme substitutsiooni

$$s=\begin{pmatrix}1 & 2 & \dots & n\\ \alpha_1 & \alpha_2 & \dots & \alpha_n\end{pmatrix},\quad t=\begin{pmatrix}\alpha_1 & \alpha_2 & \dots & \alpha_n\\ \beta_1 & \beta_2 & \dots & \beta_n\end{pmatrix}.$$

Substitutsioonis s vastavad numbritele $1, 2, \dots, n$ numbrid $\alpha_1, \alpha_2, \dots, \alpha_n$, substitutsioonis t numbritele $\alpha_1, \alpha_2, \dots, \alpha_n$ numbrid $\beta_1, \beta_2, \dots, \beta_n$. Substitutsiooni, kus numbritele $1, 2, \dots, n$ vastavad numbrid $\beta_1, \beta_2, \dots, \beta_n$, nimetatakse substitutsioonide s ja t korrutiseks ning kirjutatakse

$$st=\begin{pmatrix}1 & 2 & \dots & n\\ \beta_1 & \beta_2 & \dots & \beta_n\end{pmatrix}.$$

Seega tähendab substitutsioonide korrutamine nende substitutsioonide järjest rakendamist. Näiteks kui

$$s=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 2 & 1\end{pmatrix},\quad t=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}=\begin{pmatrix}3 & 4 & 2 & 1\\ 4 & 1 & 3 & 2\end{pmatrix},$$

siis

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

Kuid

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

millest nähtub, et substitutsioonide korrutamine ei ole kommutatiivne.

Näitame, et kõigi n-astme substitutsioonide hulk kujutab ülal defineeritud korrutamisoperatsiooni suhtes rühma. Tõepoolest:

I. Korrutamise seadus on kehtiv, sest korrutis st kujutab n-astme substitutsiooni, mis on substitutsioonidega s ja t üheselt määratud.

II. Assotsiatiivsuse seadus $s(tu)=(st)u$ on kehtiv, sest kui

$$u=\begin{pmatrix}\beta_1 & \beta_2 & \dots & \beta_n\\ \gamma_1 & \gamma_2 & \dots & \gamma_n\end{pmatrix},$$

siis

$$s(tu)=\begin{pmatrix}1 & 2 & \dots & n\\ \alpha_1 & \alpha_2 & \dots & \alpha_n\end{pmatrix}\begin{pmatrix}\alpha_1 & \alpha_2 & \dots & \alpha_n\\ \gamma_1 & \gamma_2 & \dots & \gamma_n\end{pmatrix}=\begin{pmatrix}1 & 2 & \dots & n\\ \gamma_1 & \gamma_2 & \dots & \gamma_n\end{pmatrix}$$

$$(st)u=\begin{pmatrix}1 & 2 & \dots & n\\ \beta_1 & \beta_2 & \dots & \beta_n\end{pmatrix}\begin{pmatrix}\beta_1 & \beta_2 & \dots & \beta_n\\ \gamma_1 & \gamma_2 & \dots & \gamma_n\end{pmatrix}=\begin{pmatrix}1 & 2 & \dots & n\\ \gamma_1 & \gamma_2 & \dots & \gamma_n\end{pmatrix}$$

ja seega $s(tu)=(st)u$.

III. On olemas ühiksubstitutsioon ehk identne substitutsioon

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

mis rahuldab tingimust $se=s$.

IV. Igal substitutsioonil

$$s=\begin{pmatrix}1 & 2 & \dots & n\\ \alpha_1 & \alpha_2 & \dots & \alpha_n\end{pmatrix}$$

on olemas pöördsubstitutsioon

$$s^{-1}=\begin{pmatrix}\alpha_1 & \alpha_2 & \dots & \alpha_n\\ 1 & 2 & \dots & n\end{pmatrix},$$

mis rahuldab tingimust $ss^{-1}=e$.

Kõigi n-astme substitutsioonide rühma nimetatakse n-astme sümmeetriliseks rühmaks ja märgitakse tähega S_n. Nagu nägime, koosneb n-astme sümmeetriline rühm $n!$ elemendist. Rühma, mille elementide arv on lõplik, nimetatakse lõplikuks rühmaks, kusjuures elementide arv rühmas kannab rühma järgu nime. Seega on sümmeetrilise rühma S_n järk $n!$. Et substitutsioonide korrutamine ei ole kommutatiivne, siis kujutab S_n mittekommutatiivset rühma. Siiski on alati ilmselt

$$se=es=s,\quad ss^{-1}=s^{-1}s=e,$$

s. o. parempoolne ühiksubstitutsioon on ühtlasi vasakpoolseks ühiksubstitutsiooniks ja parempoolne pöördsubstitutsioon ka

vasakpoolseks pöördsubstitutsiooniks. Järgmises artiklis näeme, et viimane asjaolu leiab aset iga rühma puhul.

2. Järeldusi rühma postulaatidest. Diskuteerime lähemalt eelmises artiklis antud rühma postulaate. Selgitame kõigepealt assotsiatiivsuse seaduse mõtet. Defineerides hulgas G arvutusoperatsiooni, kõnelesime ainult kahe elemendi a ja b korrutisest ab. Mis puutub kolme elemendi a, b ja c korrutisse, siis võime viimast defineerida põhimõtteliselt kahel erineval viisil, kas

$$abc = a(bc) \quad \text{või} \quad abc = (ab)c .$$

Nüüd ütleb aga assotsiatiivsuse seadus, et mõlemad variandid langevad ühte. Teiste sõnadega: assotsiatiivsuse seadus väljendab kolme elemendi korrutise sõltumatust sulgude paigutusest. Veel enam, assotsiatiivsuse seadus lubab tõestada mistahes arvu elementide korrutise sõltumatust sulgude paigutusest [1], võimaldades seega üheselt defineerida n elemendi korrutist.

Väite tõestuseks kasutame täieliku induktsiooni printsiipi, lähtudes oletusest, et väide korrutise sõltumatuse kohta sulgude paigutusest on kehtiv iga korrutise puhul, kus tegurite arv on väiksem kui n. Olgu n teguri korrutises $a_1a_2 \dots a_n$ mingil viisil paigutatud sulud korrutamise järjekorra määramiseks. Kuidas need sulud ka ei oleks paigutatud, viimase sammuna tuleks meil teostada mingi korrutamine

$$(a_1a_2 \dots a_i)(a_{i+1}a_{i+2} \dots a_n),$$

kus $1 \leqslant i \leqslant n-1$. Siin kumbki osakorrutis $a_1a_2 \dots a_i$ ja $a_{i+1}a_{i+2} \dots a_n$, sisaldades mõlemad vähem kui n tegurit, on induktsiooni-oletuse järgi sõltumatu sulgude paigutusest ja seega üheselt määratud, mistõttu jääb vaid näidata, et iga i ja k puhul kehtib võrdus

$$(1)\quad (a_1a_2 \dots a_i)(a_{i+1}a_{i+2} \dots a_n) = (a_1a_2 \dots a_k)(a_{k+1}a_{k+2} \dots a_n).$$

[1] Viimast asjaolu oleme juba ringi, korpuse ja integriteetkonna puhul kasutanud, pidades seda enesestmõistetavaks.

Olgu konkreetselt $k > i$. Märgime $k - i = j$, s. o. $k = i + j$ ja vaatleme algul juhtu, kus $j = 1$, nii et $k = i + 1$. Tähistades siin

$$a_1 a_2 \ldots a_i = b, \qquad a_{i+2} a_{i+3} \ldots a_n = c,$$

näeme, et valem (1) taandub assotsiatiivsuse seaduseks

$$b(a_{i+1}c) = (ba_{i+1})c$$

ja on seega kehtiv. Üldjuhul, kui $j > 1$, tuleb valemi (1) tõestuseks rakendada vaid viimast mõttekäiku j korda.

Üle minnes ühikelemendi ja pöördelemendi olemasolu seaduste juurde, näitame, et rühmas G leidub ainult üks parempoolne ühikelement e, mis osutub ühtlasi ainsaks vasakpoolseks ühikelemendiks, rahuldades tingimust $ea = a$, ja et rühma G igal elemendil a on ainult üks parempoolne pöördelement a^{-1}, mis osutub ühtlasi ainsaks vasakpoolseks pöördelemendiks, rahuldades tingimust $a^{-1}a = e$.

Tõestame kõigepealt, et parempoolne pöördelement a^{-1} on ühtlasi ka vasakpoolseks pöördelemendiks, s. o. et

$$aa^{-1} = a^{-1}a = e.$$

Tõepoolest, korrutades võrdust

$$aa^{-1} = e$$

vasakult a^{-1}-ga, saame

$$a^{-1}aa^{-1} = a^{-1}e.$$

Et aga e on parempoolne ühikelement, siis $a^{-1}e = a^{-1}$ ja seega

$$a^{-1}aa^{-1} = a^{-1}.$$

Olgu nüüd a elemendi a^{-1} parempoolne pöördelement, nii et $a^{-1}a = e$. Siis, korrutades viimast võrdust paremalt a-ga, leiame sulgude paigutamise vabadust kasutades

$$(a^{-1}a)(a^{-1}a) = a^{-1}a,$$

millest $a^{-1}a = e$ tõttu

$$(a^{-1}a)e = e$$

ehk

$$a^{-1}a = e .$$

Viimane võrdus ütlebki, et a^{-1} on ka a vasakpoolne pöördelement.

Näitame edasi, et rühmas G parempoolne ühikelement e on ühtlasi ka vasakpoolseks ühikelemendiks, s. o. et

$$ae = ea = a .$$

Korrutades selleks võrdust $aa^{-1} = e$ paremalt a-ga, saame

$$(aa^{-1})a = ea$$

ehk, assotsiatiivsuse seadust rakendades,

$$a(a^{-1}a) = ea .$$

Et aga, nagu nägime, $a^{-1}a = e$, siis omab viimane võrdus kuju

$$ae = ea ,$$

mis ütlebki, et e on ka vasakpoolne ühikelement.

Jääb näidata, et e on ainuke ühikelement rühmas G ja a^{-1} ainuke a pöördelement. Tõesti, kui peale e leiduks rühmas G veel teine ühikelement e_1, siis peaks e_1 eelnenu põhjal olema ühtlasi vasakpoolne ühikelement, nii et

$$e_1 e = e .$$

Teiselt poolt on

$$e_1 e = e_1 ,$$

sest e on parempoolne ühikelement. Viimaseid võrdusi võrreldes näeme, et $e_1 = e$.

Lõppeks kui elemendil a oleks peale a^{-1} veel pöördelement β, siis peaks β eelnenu põhjal olema ühtlasi vasakpoolne pöördelement, nii et

$$\beta a = e .$$

Korrutades viimast võrdust paremalt a^{-1}-ga, saame

$$(\beta a)a^{-1} = ea^{-1}$$

ehk

$$\beta(aa^{-1}) = a^{-1},$$

millest $aa^{-1} = e$ tõttu $\beta = a^{-1}$.

Seega kaob vajadus lisada ühikelemendi ja pöördelemendi mõisteile sõna „parempoolne" või „vasakpoolne", samuti pole vajadust kõnelda neist mõisteist mitmuses.

Vaatleme võrrandeid

$$bx = a, \quad yb = a, \tag{2}$$

kus a ja b tähendavad mistahes elemente rühmas G. Korrutades esimest võrrandit (2) vasakult ja teist paremalt b pöördelemendiga b^{-1}, leiame

$$b^{-1}(bx) = b^{-1}a, \qquad (yb)b^{-1} = ab^{-1}$$

ehk

$$x = b^{-1}a, \qquad y = ab^{-1},$$

mis kujutavad võrrandite (2) ainsaid lahendeid. Tähendab, rühmas on võrrandid (2) alati üheselt lahenduvad ehk, nagu öeldakse, rühmas on kehtiv jagamise seadus.

Ei ole raske näha, et jagamise seadus on samaväärne rühma postulaatidega III ja IV, mis väidavad vastavalt parempoolse ühikelemendi ja pöördelemendi olemasolu. Tõepoolest, kehtigu hulgas G peale rühma postulaatide I ja II veel jagamise seadus [1]. Näitame, et siis kehtivad hulgas G ka postulaadid III ja IV, nii et G osutub rühmaks. Vaatleme selleks võrrandit $bx = b$, kus b tähendab teatavat kindlat G elementi. Jagamise seaduse põhjal omab see võrrand teatavat lahendit e, nii et

$$be = b.$$

Näitame, et e osutub G ühikelemendiks, s. o. et $ae = a$ iga a puhul hulgas G. Moodustame selleks võrrandi

$$yb = a.$$

[1] Siinjuures on piisav nõuda vaid võrrandite (2) lahenduvust ilma lahendi ühesuseta.

Korrutades seda võrrandit paremalt e-ga, leiame kahte viimast võrdust ja assotsiatiivsuse seadust silmas pidades:

$$ae = (yb)e = y(be) = yb = a,$$

millega ongi postulaadi III kehtivus põhjendatud. Mis puutub postulaadisse IV, siis järeldub see vahetult jagamise seadusest, mille järgi võrrand

$$ax = e$$

on iga a puhul lahenduv.

Seega võib rühma defineerida kui niisugust ühe operatsiooniga hulka, kus on kehtivad korrutamise, assotsiatiivsuse ja jagamise seadused.

Analoogiliselt ringiga defineeritakse rühmas elemendi a täisarvulised astmed järgmiselt:

$$a^n = \underbrace{a \cdot a \ldots a}_{n \text{ tegurit}}, \quad a^0 = e, \quad a^{-n} = (a^{-1})^n,$$

kus n tähendab positiivset täisarvu. Ei ole raske näha, et igas rühmas kehtivad ka valemid

$$a^m a^n = a^{m+n}, \quad (a^n)^m = a^{mn},$$

kus m ja n võivad olla mistahes täisarvud, kuna valem

$$(ab)^n = a^n b^n$$

kehtib üldiselt vaid Abeli rühmas, s. o. kommutatiivses rühmas.

Nagu juba tähendatud, nimetatakse rühmaoperatsiooni sageli korrutamiseks. Kui aga rühmaoperatsioon kannab liitmise nime, siis kõneldakse ühikelemendi e asemel nullelemendist 0, pöördelemendi a^{-1} asemel vastandelemendist $-a$ ja astme a^n asemel kordsest na. Rühma postulaate I—IV (art. 1) tuleb sel korral sõnastada järgmiselt:

I. Liitmise seadus: summa $a + b$ on liidetavatega a ja b üheselt määratud G element.

II. Assotsiatiivsuse seadus:

$$a + (b + c) = (a + b) + c.$$

III. Nullelemendi olemasolu seadus: hulgas G leidub vähemalt üks element 0, mis rahuldab tingimust

$$a + 0 = a$$

G iga elemendi a puhul.

IV. Vastandelemendi olemasolu seadus: vastavalt igale elemendile a leidub hulgas G vähemalt üks element $-a$, mis rahuldab tingimust

$$a + (-a) = 0 .$$

Kui mingis ringis (eriti korpuses või integriteetkonnas) vaadelda ainult liitmise operatsiooni, siis osutub ring selle operatsiooni suhtes rühmaks, mis kannab ringi aditiivse rühma nime. Nii kõneldakse näiteks maatriksite ringi aditiivsest rühmast, täisarvude integriteetkonna aditiivsest rühmast jne. Et liitmine on ringis alati kommutatiivne, siis kujutab aditiivne rühm Abeli rühma. Ümberpöördult on sageli viisiks märkida Abeli rühma puhul rühmaoperatsiooni aditiivselt summa märgi abil.

Kui mingis korpuses vaadelda ainult korrutamise operatsiooni, siis moodustavad selle korpuse nullist erinevad elemendid rühma, mida nimetatakse korpuse multiplikatiivseks rühmaks. Nii kõneldakse näiteks kvaternioonide korpuse multiplikatiivsest rühmast, jäägiklassikorpuse $R^{(p)}$ multiplikatiivsest rühmast jne. Kui korpus on kommutatiivne, siis kujutab tema multiplikatiivne rühm Abeli rühma.

3. Tsüklilised rühmad. Vaatleme m-astme ühejuuri, s. o. võrrandi $\xi^m = 1$ lahendeid

$$\varepsilon_0 = 1 , \quad \varepsilon_1 , \quad \varepsilon_2 , \quad \ldots , \quad \varepsilon_{m-1}$$

(§ 1, art. 5). Ei ole raske näha, et need ühejuured moodustavad korrutamise suhtes rühma. Tõepoolest, kõigepealt ühejuurte korrutis $\varepsilon_i \varepsilon_k$ kujutab ka ühejuurt, sest $\varepsilon_i^m = 1$, $\varepsilon_k^m = 1$ tõttu on $(\varepsilon_i \varepsilon_k)^m = \varepsilon_i^m \varepsilon_k^m = 1$. Teiseks ühejuurte kui kompleksarvude korrutis on assotsiatiivne. Kolmandaks leidub ühejuurte hulgas ühikelement $\varepsilon_0 = 1$. Neljandaks kujutab iga ühejuure ε_k pöördväärtus ka ühejuurt, sest $(\varepsilon_k^{-1})^m = (\varepsilon_k^m)^{-1} = 1$.

Et kompleksarvude korrutis on kommutatiivne, siis kujutab m-astme ühejuurte rühm Abeli rühma. Veel enam, me nägime, et kõik m-astme ühejuured avalduvad ühejuure

$$\varepsilon_1 = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}$$

astmetena, nimelt $\varepsilon_k = \varepsilon_1^k$. Niisugust rühma, kus kõik elemendid avalduvad ühe kindla elemendi astmetena, nimetatakse tsükliliseks rühmaks. Seega m-astme ühejuurte rühm on tsükliline.

Olgu nüüd G mistahes rühm ja a mingi tema element. Vaatleme kõiki a täisarvulisi astmeid

$$(3) \qquad \ldots, a^{-3}, a^{-2}, a^{-1}, a^0 = e, a^1 = a, a^2, a^3, \ldots .$$

Ei ole raske näha, et astmed (3) moodustavad rühma. Tõepoolest, kõigepealt astmete korrutis $a^k a^l = a^{k+l}$ kujutab ka astet. Teiseks on astmete (3) kui rühma G elementide korrutis assotsiatiivne. Kolmandaks leidub astmete (3) hulgas ühikelement $a^0 = e$. Neljandaks kujutab iga astme a^k pöördväärtus ka astet, sest $(a^k)^{-1} = a^{-k}$. Seega määravad astmed (3) rühma ja nimelt tsüklilise rühma, täpsemalt — elemendi a poolt moodustatud tsüklilise rühma.

Astmete (3) suhtes on kaks võimalust: emb-kumb, kas nende astmete hulgas leidub võrdseid või on nad kõik üksteisest erinevad.

1° Kui $a^k = a^l$, kus olgu $l > k$, siis seda võrdust a^{-k}-ga korrutades saame

$$a^{l-k} = e,$$

kus astendaja $l - k$ on naturaalarv. Väikseimat naturaalarvu, millega rühma G mingit elementi a astendades saame ühikelemendi, nimetatakse elemendi a järguks. Eriti on ühikelement e esimest järku.

Kui nüüd element a omab järku m, siis on astmed

$$(4) \qquad a^0 = e, a^1 = a, a^2, \ldots, a^{m-1}$$

kõik üksteisest erinevad, sest kui siin oleks $a^k = a^l$, kus olgu $l > k$, siis $a^{l-k} = e$, mis on $0 < l - k < m$ tõttu vastuolus elemendi a järgu mõistega. Mis puutub ülejäänud astmeisse (3), siis on igaüks neist võrdne teatava astmega (4). Nimelt kui n tähendab mingit täisarvu, siis saame teda m-ga jagades

$$n = qm + r,$$

kus $0 \leqslant r < m$. Seega

$$a^n = a^{qm+r} = a^{qm}a^r = (a^m)^q a^r = a^r,$$

sest $a^m = e$. Niisiis koosneb m-järku elemendi a poolt moodustatud tsükliline rühm parajasti m erinevast elemendist (4) ehk, teiste sõnadega: *m-järku element moodustab m-järku tsüklilise rühma.* Eriti nähtub võrdusest $a^n = a^r$, et $a^n = e$ siis ja ainult siis, kui $r = 0$, s. o. kui n jagub m-ga.

2^0 Kui jadas (3) on kõik astmed üksteisest erinevad, siis öeldakse, et element a on l õ p m a t u t j ä r k u. Arusaadav, et lõpmatut järku elemendid võivad esineda vaid lõpmatus rühmas, kuna lõpliku rühma iga element on lõplikku järku.

Vaatleme lõppeks Abeli rühmas G kahte elementi a ja b, mille järgud olgu vastavalt m ja l. Näitame, et kui m ja l on ühistegurita, siis on korrutise ab järk ml. Kuna

$$(ab)^{ml} = a^{ml}b^{ml} = (a^m)^l (b^l)^m = e^l e^m = e,$$

siis jääb väite tõestuseks vaid näidata, et kui

$$(ab)^k = e,$$

siis $k \geqslant ml$. Astendades viimast võrdust üks kord l-ga ja teine kord m-ga, saame $a^m = e$, $b^l = e$ tõttu

$$a^{kl} = e, \quad b^{km} = e,$$

millest eelnenu põhjal nähtub, et kl peab jaguma m-ga ja km l-ga. Et aga $(m, l) = 1$, siis peab k jaguma m-ga ja l-ga (I, § 7, art. 3). Tähendab, k peab omama kuju $k = qm$ ja ühtlasi jaguma l-ga. Kuid qm võib jaguda l-ga $(m, l) = 1$ tõttu vaid

siis, kui q jagub l-ga. Seega peab k jaguma korrutisega ml, nii et tõesti $k \geqslant ml$.

Vaatleme näitena 12-ndat järku tsüklilist rühma

$$G = \{e, a, a^2, a^3, \ldots, a^{11}\}.$$

Siin elemendi a^4 järk on 3, elemendi a^6 järk 2 ja seega korrutise $a^4 \cdot a^6 = a^{10}$ järk 6, nagu seda võib vahetult kergesti kontrollida.

§ 19. Alamrühmad.

1. Kompleksid. Enne kui asume rühma struktuuri uurimisele, tutvume käesolevas artiklis mõnede meile vajalike hulgateooria mõistetega.

Olgu antud rühm G — lõplik või lõpmatu — ja mingi hulk A. Kui A iga element kuulub rühma G, siis nimetatakse hulka A rühma G k o m p l e k s i k s ehk o s a h u l g a k s ja kirjutatakse

$$A \subset G \quad \text{ehk} \quad G \supset A,$$

lugedes vastavalt „A sisaldub G-s" ehk „G sisaldab A-d". Antud definitsiooni kohaselt tuleb G komplekside hulka arvata ka G ise. Asjaolu, et mingi element a kuulub kompleksi A, märgitakse lühidalt sümboliga

$$a \in A.$$

Seega $A \subset G$, kui iga $a \in A$ puhul ka $a \in G$.

Vaatleme nüüd kahte kompleksi A ja B. Kui siin ühtaegu $A \subset B$ ja $B \subset A$, siis nimetatakse komplekse A ja B võrdseteks ja kirjutatakse

$$A = B.$$

Seega tähendab komplekside A ja B võrdus, et need kompleksid koosnevad ühtedest ja samadest elementidest, kusjuures kompleksis pole oluline elementide järjekord. Komplekside A ja B summaks $A + B$ nimetame niisugust kompleksi, mis koosneb

kõigist A ja kõigist B elementidest. Lõppeks komplekside A ja B korrutiseks AB nimetame niisugust kompleksi, mis koosneb kõigist võimalikest korrutistest ab, kus a tähendab mingit A elementi ja b mingit B elementi.

Olgu komplekside A ja B üldelementide tähised vastavalt a ja b. Siis kirjutatakse $A=\{a\}$, $B=\{b\}$, nii et

$$A=B, \text{ kui } a=b$$
$$A+B=\{a, b\}$$
$$AB=\{ab\}.$$

Vaatleme näitena kolmanda astme sümmeetrilist rühma $S_3=\{e, s_1, s_2, s_3, s_4, s_5\}$ (§ 18, art. 1), mis koosneb kuuest substitutsioonist

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \quad s_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \quad s_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$
$$s_3=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \quad s_4=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \quad s_5=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

Siin näiteks komplekside

$$A=\{e, s_1, s_2\}, \quad B=\{e, s_1, s_4\}$$

puhul leiame

$$A+B=\{e, s_1, s_2, s_4\}$$
$$AB=\{e, s_1, s_2, s_3, s_4, s_5\}=S_3.$$

Ei ole raske veenduda, et arvutamisel kompleksidega kehtivad kõik arvutusseadused I—VII (I, § 5, art. 1), välja arvatud korrutise kommutatiivsuse seadus V, kui rühm G on mittekommutatiivne. Piirdudes näiteks distributiivsuse seaduse VII tõestusega, märgime

$$A=\{a\}, \quad B=\{b\}, \quad C=\{c\}.$$

Komplekside summa ja korrutise definitsiooni kohaselt on siis

$$A+B=\{a, b\}, \quad (A+B)C=\{ac, bc\}.$$

Nüüd on aga

$$\{ac,\ bc\} = \{ac\} + \{bc\} = AC + BC$$

ja seega tõepoolest

$$(A + B)C = AC + BC .$$

Täpselt samuti tõestatakse mittekommutatiivsel juhul ka valem

$$C(A + B) = CA + CB .$$

Peale komplekside A ja B summa ja korrutise tuleb meil veel vaadelda sellist kompleksi, mis koosneb komplekside A ja B kõigist ühistest elementidest. Niisugust kompleksi nimetatakse A ja B ühisosaks ja märgitakse sümboliga

$$A \cap B .$$

Seega $a \in A \cap B$, kui $a \in A$ ja $a \in B$. Ülal vaadeldud substitutsioonide komplekside $A = \{e,\ s_1,\ s_2\}$, $B = \{e,\ s_1,\ s_4\}$ puhul on

$$A \cap B = \{e,\ s_1\} .$$

2. **Alamrühma mõiste.** Rühma struktuuri uurimisel vaatleme eriti selliseid komplekse, mis kujutavad omakorda rühma. Rühma G kompleksi, mis osutub selle rühma operatsiooni suhtes ise ka rühmaks, nimetatakse rühma G alamrühmaks ehk jagajaks. Selle definitsiooni kohaselt tuleb vaadelda G-d ennast ka alamrühmana. Seepärast kui tahame rõhutada, et vaadeldav alamrühm ei kujuta G-d, siis kõneleme päris-alamrühmast. Omaette alamrühma moodustab G ühikelement e. Ainult ühikelemendist koosnevat rühma nimetatakse ühikrühmaks ja märgitakse tähega E, s. o. $E = \{e\}$.

Selleks, et otsustada, kas rühma G mingi kompleks H kujutab alamrühma, tarvitseb H suhtes kontrollida vaid rühma postulaate I ja IV. Täpsemalt, rühma G kompleks H kujutab alamrühma siis ja ainult siis, kui:

1^0 iga $a \in H$ ja $b \in H$ puhul ka $ab \in H$;

2^0 iga $a \in H$ puhul ka $a^{-1} \in H$.

Tõepoolest, postulaat II — assotsiatiivsuse seadus — kehtides rühmas G, kehtib ammugi kompleksis H, kuna postulaat III — ühikelemendi olemasolu seadus — järeldub kergesti rühma postulaatidest I ja IV, s. o. tingimustest 1^0 ja 2^0. Nimelt kui a tähendab mingit elementi kompleksis H, siis kuulub sellesse kompleksi 2^0 põhjal pöördelement a^{-1} ja seega 1^0 põhjal korrutis $aa^{-1} = e$.

Vaatleme näitena täisarvude aditiivses rühmas kindla täisarvu m kordsetest moodustatud kompleksi $H = \{km\}$, kus k tähendab mistahes täisarvu. Silmas pidades, et siin rühmaoperatsiooniks on liitmine, leiame:

$$1^0 \quad k_1 m + k_2 m = (k_1 + k_2) m;$$
$$2^0 \quad -(km) = (-k) m,$$

millest nähtub, et H on alamrühm.

Erijuhul, kui rühm G on lõplik, siis selleks, et otsustada, kas kompleks H on alamrühm või mitte, piisab vaid tingimuse 1^0 kontrollimisest, kuna tingimus 2^0 järeldub tingimusest 1^0. Tõepoolest, kui G on lõplik rühm, siis omab iga tema element a lõplikku järku m, nii et $a^m = e$ ehk $aa^{m-1} = e$, millest nähtub, et siin a^{m-1} kujutab a pöördelementi, s. o. $a^{-1} = a^{m-1}$. Kui nüüd a tähendab mingit H elementi, siis kuulub a^{-1} tingimuse 1^0 põhjal kompleksi H. Tähendab, *lõpliku rühma kompleks H kujutab alamrühma siis ja ainult siis, kui H on kinnine korrutamise suhtes.*

Nii on näiteks kolmanda astme sümmeetrilises rühmas S_3 kompleks $A = \{e, s_1, s_2\}$ alamrühm, sest siin $s_1^2 = s_2$, $s_1 s_2 = s_2 s_1 = e$, $s_2^2 = s_1$ kuuluvad kompleksi A, seevastu kompleks $B = \{e, s_1, s_4\}$ ei ole alamrühm, sest näiteks $s_1^2 = s_2$ ei kuulu kompleksi B.

Ei ole raske näha, et kahe alamrühma ühisosa on ka alamrühm. Olgu nimelt H_1, H_2 rühma G alamrühmad ja H nende alamrühmade ühisosa, s. o. $H = H_1 \cap H_2$. Kui nüüd a ja b

tähendavad H elemente, siis $a \in H_1$, $a \in H_2$, $b \in H_1$, $b \in H_2$. Et aga H_1 ja H_2 on rühmad, siis

$$ab \in H_1,\ a^{-1} \in H_1,\ ab \in H_2,\ a^{-1} \in H_2$$

ja seega

$$ab \in H,\quad a^{-1} \in H,$$

mis ütlebki, et H on G alamrühm.

Näitame lõppeks, et tsüklilise rühma alamrühmad on ka tsüklilised. Olgu nimelt $H = \{e, a^{n_1}, a^{n_2}, \ldots\}$ tsüklilise rühma G alamrühm, kusjuures n_1 tähendagu väikseimat naturaalarvu astendajate $n_1, n_2, \ldots$ seas. Vaatleme mingit H elementi a^{n_k}. Jagades n_k naturaalarvuga n_1, saame

$$n_k = qn_1 + r,$$

kus $0 \leqslant r < n_1$. Seega

$$a^{n_k} = (a^{n_1})^q a^r,$$

millest nähtub, et $a^r = a^{n_k}(a^{n_1})^{-q}$ kuulub alamrühma H. Et aga $r < n_1$, siis peab olema $r = 0$, nii et $n_k = qn_1$. Järelikult $a^{n_k} = (a^{n_1})^q$, mis ütlebki, et H on tsükliline.

3. **Kõrvalklassid.** Olgu H rühma G alamrühm ja a mingi G element. Moodustame korrutised Ha ja aH, kus a-d vaatleme kui ühe-elemendilist kompleksi. Korrutist Ha nimetatakse rühma G *parempoolseks kõrvalklassiks* ja korrutist aH *vasakpoolseks kõrvalklassiks* alamrühma H järgi, kusjuures element a kannab vastava kõrvalklassi *esindaja* nime. Silmas pidades komplekside korrutise mõistet, võime öelda, et parempoolne kõrvalklass Ha koosneb kõigist korrutistest ha ja vasakpoolne kõrvalklass aH kõigist korrutistest ah, kus h tähendab mistahes elementi alamrühmas H. Seega

$$Ha = \{ha\},\quad aH = \{ah\}.$$

Võttes siin h asemel eriti ühikelemendi e näeme, et iga kõrvalklass sisaldab elementi a, s. o. *kõrvalklassi esindaja kuulub tema poolt esindatavasse kõrvalklassi.*

Uurides kõrvalklasside omadusi, piirdume edaspidi tõestuste puhul parempoolsete kõrvalklassidega, kuna vasakpoolseid kõrvalklasse saab käsitleda täiesti analoogiliselt. Näitame kõigepealt, et kui a kuulub alamrühma H, siis

$$Ha = H, \quad aH = H,$$

nii et H kujutab ise ka kõrvalklassi. Nimelt kui $a \in H$, siis rühma postulaadi I põhjal $ha \in H$, s. o.

$$Ha \subset H.$$

Teiselt poolt võib alamrühma H iga elementi b esitada kujul $b = (ba^{-1})a = ha$, kus $h = ba^{-1}$ kujutab teatavat H elementi. Seega $b \in Ha$, s. o.

$$H \subset Ha.$$

Kahest viimasest seosest järeldubki võrdus $Ha = H$.

Olgu nüüd b mingi element kõrvalklassis Ha. Küsime, mida kujutab endast kõrvalklass Hb. Et $b \in Ha$, siis peab b avalduma kujul $b = ha$, $h \in H$. Seega

$$Hb = H(ha) = (Hh)a = Ha,$$

sest $h \in H$ tõttu on eelnenu põhjal $Hh = H$. Niisiis vastab kõrvalklassi Ha igale elemendile b sama kõrvalklass Ha ehk, teiste sõnadega, *kõrvalklassi iga element on selle kõrvalklassi esindajaks.*

Vaatleme näiteks sümmeetrilises rühmas S_3 alamrühma $H = \{e, s_3\}$ kõrvalklassi

$$Hs_1 = \{es_1, s_3s_1\} = \{s_1, s_4\}.$$

Selle kõrvalklassi esindajaks on peale s_1 ka s_4, sest

$$Hs_4 = \{es_4, s_3s_4\} = \{s_4, s_1\} = Hs_1.$$

Nüüd ei ole raske näha, et kaks isesugust kõrvalklassi Ha ja Hb ei saa omada ühtki ühist elementi, sest kui näiteks

$$c \in Ha, \quad c \in Hb,$$

siis oleks c niihästi kõrvalklassi Ha kui ka Hb esindajaks, nii et

$$Hc = Ha, \quad Hc = Hb$$

ja seega $Ha = Hb$, vastupidi eeldusele. Siit nähtub ühtlasi, et kõrvalklassidest Ha ainult $He = H$ kujutab alamrühma, sest vastasel korral oleks isesugustel kõrvalklassidel ühine element e, mis peab ju sisalduma igas rühmas.

Niisiis määravad kõik isesugused samapoolsed kõrvalklassid rühmas G klassijaotuse, kus G iga element kuulub ühte ja ainult ühte kõrvalklassi. Vastavalt sellele saame iga alamrühma H jaoks kaks G lahutust kõrvalklasside summaks:

$$G = \sum Ha, \quad G = \sum aH.$$

Näide 1. Leida kolmanda astme sümmeetrilise rühma S_3 parempoolseteks ja vasakpoolseteks kõrvalklassideks lahutused alamrühma $H = \{e, s_3\}$ järgi.

Võtame rühmas S_3 mingi elemendi, mis ei kuulu alamrühma H, näiteks elemendi s_1, ja moodustame kõrvalklassi

$$Hs_1 = \{es_1, s_3s_1\} = \{s_1, s_4\}.$$

Edasi võtame rühmas S_3 mingi elemendi, mis ei kuulu alamrühma H ega kõrvalklassi Hs_1, näiteks elemendi s_2, ja moodustame kõrvalklassi

$$Hs_2 = \{es_2, s_3s_2\} = \{s_2, s_5\}.$$

Et kõrvalklassidega H, Hs_1, Hs_2 on ammendatud kõik S_3 elemendid, siis võime kirjutada

$$S_3 = H + Hs_1 + Hs_2 \quad \text{ehk} \quad S_3 = \{e, s_3\} + \{s_1, s_4\} + \{s_2, s_5\}.$$

Analoogiliselt leiame S_3 lahutuse vasakpoolseteks kõrvalklassideks:

$$S_3 = H + s_1H + s_2H \quad \text{ehk} \quad S_3 = \{e, s_3\} + \{s_1, s_5\} + \{s_2, s_4\}.$$

Vaatleme lõppeks eriti juhtu, kus G on lõplik rühm. Olgu G järk, s. o. elementide arv n ja alamrühma H järk m. Siis on

igas kõrvalklassis Ha parajasti m elementi, sest kõrvalklassis $Ha = \{ha\}$ on niipalju elemente, kuipalju on erinevaid korrutisi ha, kus $h \in H$. Viimaseid on aga sama palju kui erinevaid h väärtusi, s. o. m tükki, sest kui $h_1 \neq h_2$ puhul oleks

$$h_1 a = h_2 a ,$$

siis saaksime viimast võrdust paremalt a^{-1}-ga korrutades $h_1 = h_2$, vastupidi oletusele.

Kui j tähendab H kõigi samapoolsete kõrvalklasside arvu, siis on kõigis kõrvalklassides kokku mj elementi, s. o.

$$n = mj .$$

Siit saame ühe tähtsa järelduse, mis on tuntud L a g r a n g e'i t e o r e e m i nime all.

T e o r e e m 1. *Lõplikus rühmas on iga alamrühma järk rühma järgu jagajaks.*

Seega võivad näiteks kuuendat järku rühmal olla vaid esimest, teist ja kolmandat järku päris-alamrühmad. Näiteks sümmeetrilisel rühmal S_3 on järgmised päris-alamrühmad:

$$E = \{e\}, \quad H = \{e, s_3\}, \quad H_1 = \{e, s_4\}, \quad H_2 = \{e, s_5\},$$
$$H_3 = \{e, s_1, s_2\}.$$

Arvu $j = \frac{n}{m}$ nimetatakse alamrühma H i n d e k s i k s G suhtes ja märgitakse sümboliga (H, G). Näite 1 puhul on $j = \frac{6}{2} = 3$. Niisiis omavad lõpliku rühma G kõrvalklassideks lahutused H järgi vastavalt kuju

$$G = H + Ha_2 + Ha_3 + \ldots + Ha_j$$
$$G = H + b_2 H + b_3 H + \ldots + b_j H.$$

4. Normaaljagaja. Rühma G alamrühmade hulgas etendavad erilist osa niisugused alamrühmad, mille puhul G parempoolne kõrvalklassideks lahutus langeb ühte vasakpoolsega.

D e f i n i t s i o o n 2. Kui rühma G parempoolne kõrvalklassideks lahutus alamrühma H järgi langeb ühte vasakpoolsega, siis nimetatakse alamrühma H rühma G n o r m a a l j a g a j a k s.

Teiste sõnadega, rühma G alamrühm H kujutab normaaljagajat siis ja ainult siis, kui on täidetud tingimus

$$Hx = xH . \tag{5}$$

iga $x \in G$ puhul. Viimane tingimus kannab H normaalsuse tingimuse nime. Silmas pidades, et $Hx = \{hx\}$, kus $h \in H$, ja et $xH = \{xh'\}$, kus $h' \in H$, võime öelda, et G alamrühm H kujutab normaaljagajat siis ja ainult siis, kui iga $x \in G$ puhul leidub vastavalt igale elemendile $h \in H$ teine element $h' \in H$, nii et

$$hx = xh' . \tag{6}$$

Eriti nähtub tingimusest (6), et Abeli rühma, s. o. kommutatiivse rühma iga alamrühm on normaaljagaja, sest siis on tingimus (6) täidetud, kui võtta $h' = h$. Normaaljagajate hulka tuleb arvata ka rühma G ennast. Seepärast, kui tahame rõhutada, et vaadeldav normaaljagaja ei ole G ise, siis kõneleme päris-normaaljagajast. Samuti kujutab ühikrühm $E = \{e\}$ normaaljagajat.

Vaatleme alamrühma

$$H_3 = \{e, s_1, s_2\}$$

sümmeetrilises rühmas S_3. Siin S_3 kõrvalklassideks lahutused H_3 järgi omavad kuju

$$S_3 = H_3 + H_3 s_3 = \{e, s_1, s_2\} + \{s_3, s_4, s_5\},$$
$$S_3 = H_3 + s_3 H_3 = \{e, s_1, s_2\} + \{s_3, s_4, s_5\},$$

millest ilmneb, et H_3 on normaaljagaja. Et mitte iga alamrühm ei ole normaaljagaja, see selgub näitest 1, kus alamrühm $H = \{e, s_3\}$ ei kujuta normaaljagajat.

Nagu nägime, on kahe alamrühma ühisosa ka alamrühm (art. 2). Seevastu kahe alamrühma korrutis ei tarvitse osutuda alamrühmaks, nagu see nähtub sümmeetrilise rühma S_3 alamrühmadest

$$H_1 = \{e, s_4\}, \quad H_2 = \{e, s_5\},$$

kus korrutis

$$H_1H_2 = \{e, s_1, s_4, s_5\}$$

ei saa Lagrange'i teoreemi järgi olla alamrühm. Siin kumbki alamrühmadest H_1, H_2 ei ole normaaljagaja. Kui aga vähemalt üks kahest alamrühmast on normaaljagaja, siis kujutab nende alamrühmade korrutis ka alamrühma.

Tõepoolest, olgu korrutises $H = H_1H_2$ tegur H_2 normaaljagaja. Vaadeldes kahte H elementi $a = \alpha_1\alpha_2$ ja $b = \beta_1\beta_2$, kus $\alpha_1 \in H_1$, $\alpha_2 \in H_2$ ja $\beta_1 \in H_1$, $\beta_2 \in H_2$, leiame

$$ab = (\alpha_1\alpha_2)(\beta_1\beta_2) = \alpha_1(\alpha_2\beta_1)\beta_2 .$$

Et H_2 kujutab normaaljagajat, siis on (6) järgi

$$\alpha_2\beta_1 = \beta_1\alpha_2',$$

milles α_2' tähendab teatavat H_2 elementi. Järelikult

$$ab = \alpha_1(\beta_1\alpha_2')\beta_2 = (\alpha_1\beta_1)(\alpha_2'\beta_2) = h_1h_2 ,$$

kus $h_1 = \alpha_1\beta_1$ kuulub alamrühma H_1 ja $h_2 = \alpha_2'\beta_2$ alamrühma H_2, nii et $ab \in H$. Seega rahuldab H alamrühma tingimust 1^0 (art. 2).

Edasi leiame seosest $a = \alpha_1\alpha_2$, et

$$a^{-1} = \alpha_2^{-1}\alpha_1^{-1},$$

sest

$$(\alpha_1\alpha_2)(\alpha_2^{-1}\alpha_1^{-1}) = \alpha_1(\alpha_2\alpha_2^{-1})\alpha_1^{-1} = \alpha_1\alpha_1^{-1} = e .$$

Et H_2 on normaaljagaja, siis on (6) järgi

$$\alpha_2^{-1}\alpha_1^{-1} = \alpha_1^{-1}h_2',$$

milles h_2' tähendab kindlat H_2 elementi, nii et $\alpha_1^{-1}h_2' \in H$, s. o. $a^{-1} \in H$. Seega rahuldab H ka alamrühma tingimust 2^0 ja kujutab järelikult alamrühma.

Normaaljagajate tähtsus võrreldes teiste alamrühmadega seisneb selles, et nad võimaldavad tuletada antud rühmast G uusi rühmi. Nimelt on kehtiv järgmine tähelepandav teoreem:

Teoreem 2. *Rühma G kõrvalklassid normaaljagaja järgi*[1] *moodustavad rühma nende kõrvalklasside kui komplekside korrutamise suhtes.*

Lihtsuse mõttes märgime edaspidi kõrvalklassi Ha tema esindaja a järgi lühidalt tähega $\bar{a}$, s. o. $\bar{a} = Ha$. Veendume, et kõrvalklassid normaaljagaja järgi rahuldavad rühma postulaate I—IV (§ 18, art. 1).

I. Korrutamise seadus. Komplekside korrutamise assotsiatiivsust silmas pidades leiame kõrvalklasside $\bar{a} = Ha$ ja $\bar{b} = Hb$ jaoks

$$\bar{a}\bar{b} = Ha \cdot Hb = H(aH)b .$$

Nüüd on aga normaalsuse tingimuse (5) kohaselt $aH = Ha$ ja seega

$$\bar{a}\bar{b} = H(Ha)b = H^2(ab).$$

Siin $H^2 = HH$ koosneb kõigist võimalikest korrutistest hh', kus $h \in H$, $h' \in H$. Et H on rühm, siis $hh' \in H$ ja järelikult

$$H^2 \subset H .$$

Teiselt poolt

$$H \subset H^2 ,$$

sest H iga elementi h võib esitada kujul $h = he$, kus $e \in H$. Niisiis

$$H^2 = H$$

ja seega

$$\bar{a}\bar{b} = Hab ,$$

millest nähtub, et kõrvalklasside $\bar{a}$ ja $\bar{b}$ korrutis kujutab kindlat kõrvalklassi, mille esindajaks on $\bar{a}$ ja $\bar{b}$ esindajate korrutis ab, s. o.

(7) $$\bar{a} \cdot \bar{b} = \overline{ab} \quad \text{ehk} \quad Ha \cdot Hb = Hab .$$

---

[1] Et normaaljagaja puhul ei ole vahet parempoolsete ja vasakpoolsete kõrvalklasside vahel, siis kõneleme siin lihtsalt kõrvalklassidest.

II. Assotsiatiivsuse seadus. Et assotsiatiivsuse seadus on kehtiv mistahes komplekside korrutamisel, siis on ta eriti kehtiv kõrvalklasside korrutamisel.

III. Ühikelemendi olemasolu seadus. Vaadeldes G ühikelemendile e vastavat kõrvalklassi $\overline{e} = He = H$, leiame kõrvalklasside korrutamise eeskirja (7) kohaselt

$$\overline{a} \cdot \overline{e} = \overline{ae} = \overline{a}.$$

Seega kujutab $\overline{e} = H$ kõrvalklasside hulgas ühikelementi.

IV. Pöördelemendi olemasolu seadus. Näitame, et kõrvalklassi $\overline{a} = Ha$ pöördelemendiks on a pöördelemendile a^{-1} vastav kõrvalklass $\overline{a^{-1}} = Ha^{-1}$. Tõepoolest, kõrvalklasside korrutamise eeskirja (7) kohaselt saame

$$\overline{a} \cdot \overline{a^{-1}} = \overline{aa^{-1}} = \overline{e},$$

mis ütlebki, et $\overline{a^{-1}}$ kujutab $\overline{a}$ pöördelementi.

Seega on teoreem 2 tõestatud. Rühma G kõrvalklasside rühma $\{Ha\}$, mis etendab põhilist osa rühmateoorias, nimetatakse G faktorrühmaks H järgi ja märgitakse sümboliga G/H, nii et

$$G/H = \{Ha\}.$$

Erijuhul, kui G on lõplik rühm, on ka faktorrühm G/H lõplik, kusjuures viimase järk on võrdne H indeksiga G suhtes. Nimelt kui

$$G = H + Ha_2 + Ha_3 + \ldots + Ha_j$$

kujutab G kõrvalklassideks lahutust H järgi, siis on

$$G/H = \{H, Ha_2, Ha_3, \ldots, Ha_j\},$$

kus $j = (H, G)$.

Nii omab näiteks sümmeetrilise rühma S_3 faktorrühm normaaljagaja $H = \{e, s_1, s_2\}$ järgi kuju

$$G/H = \{H, Hs_3\},$$

kus $Hs_3 = \{s_3, s_4, s_5\}$. Kuid ka lõpmatul rühmal võib olla lõplikke faktorrühmi, nagu see nähtub täisarvude aditiivsest rühmast. Vaatleme siin kindla täisarvu m kordsetest moodustatud alamrühma $H = \{km\}$, kus k tähendab mistahes täisarvu (art. 2). Et vaadeldav rühm on kommutatiivne, siis kujutab H normaaljagajat. Seoses sellega, et siin rühmaoperatsiooniks on liitmine, koosneb täisarvule a vastav kõrvalklass $\overline{a}$ kõigist summadest $h + a$, kus $h \in H$. Seepärast kirjutame

$$\overline{a} = \{h + a\} = H + a.$$

Moodustades täisarvudele $0, 1, 2, \ldots, |m| - 1$ vastavad kõrvalklassid, leiame

$$\overline{0} = H + 0 = \{km + 0\} = \{km\} = H$$
$$\overline{1} = H + 1 = \{km + 1\}$$
$$\overline{2} = H + 2 = \{km + 2\}$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\overline{|m| - 1} = H + |m| - 1 = \{km + |m| - 1\}.$$

Siin koosneb kõrvalklass $\overline{0} = H$ kõigist neist täisarvudest, mis jaguvad m-ga, kõrvalklass $\overline{1}$ kõigist neist täisarvudest, mis annavad jagamisel m-ga jäägi 1, kõrvalklass $\overline{2}$ kõigist neist täisarvudest, mis annavad jagamisel m-ga jäägi 2 jne., lõppeks koosneb kõrvalklass $\overline{|m| - 1}$ kõigist neist täisarvudest, mis annavad jagamisel m-ga jäägi $|m| - 1$. Seega pole kõrvalklassid $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{|m| - 1}$ muud midagi kui jäägiklassid täisarvu m järgi (I, § 8, art. 1). Märkides täisarvude aditiivse rühma tähega Γ, võime kirjutada

$$\Gamma/H = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{|m| - 1}\},$$

sest kõrvalklassid $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{|m| - 1}$ kui jäägiklassid m-i järgi sisaldavad kõiki täisarve. Mis puutub kõrvalklasside $\overline{a}$ ja $\overline{b}$ liitmisesse, siis toimub see valemi (7) põhjal eeskirja

$$\overline{a} + \overline{b} = \overline{a + b}$$

kohaselt, mille järgi kõrvalklasside liitmine taandub nende esindajate liitmisele. Seades kõrvalklassidele $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{|m|-1}$ vastavusse nende esindajad $0, 1, 2, \ldots, |m|-1$, ei ole raske näha, et faktorrühm Γ/H on isomorfne (§ 20, art. 1) jäägiklassiringi $R^{(m)}$ aditiivse rühmaga.

§ 20. Isomorfism.

1. Isomorfismi mõiste. Analoogiliselt kahe operatsiooniga hulkade isomorfismiga, s. o. ringide, korpuste ja integriteetkondade isomorfismiga (I, § 9, art. 2), toome sisse ühe operatsiooniga hulkade isomorfismi mõiste, s. o. rühmade isomorfismi mõiste.

Definitsioon 3. Nimetame kahte rühma G ja $\overline{G}$ isomorfseiks, kui nende elementide vahel saab korraldada niisuguse üksühese vastavuse, kus korrutisele vastab tegureile vastavate elementide korrutis.

Rühmade G ja $\overline{G}$ vahel korraldatud vastavust nimetatakse sel juhul isomorfseks vastavuseks ehk isomorfismiks. Niisiis on rühmade isomorfism niisugune üksühene vastavus, mis säilib rühmaoperatsioonide puhul. Tähendab, kui G elemendile a vastab $\overline{G}$ element $\overline{a}$ ja G elemendile b G element b, s. o. kui

$$a \leftrightarrow \overline{a}, \quad b \leftrightarrow \overline{b},$$

siis, märkides korrutisele ab vastava elemendi sümboliga $\overline{ab}$, võime isomorfismi korral kirjutada

$$\overline{ab} = \overline{a} \cdot \overline{b} \quad \text{ehk} \quad ab \leftrightarrow \overline{a} \cdot \overline{b}.$$

Vastavalt sellele märgime rühmade G ja $\overline{G}$ isomorfset vastavust kujul

$$a \leftrightarrow \overline{a} \quad \text{ehk} \quad G \leftrightarrow \overline{G}.$$

Isomorfsed rühmad erinevad teineteisest ülimalt elementide ja rühmaoperatsioonide tähistuse ja konkreetse tähenduse (inter-

pretatsiooni) poolest. Seetõttu võib isomorfseid rühmi pidada algebra mõttes mitteerinevaiks, vaadeldes neid kui ühe rühmatüübi mitmesuguseid esindajaid, kui erinevad väliselt ka ei näiks nende rühmade elemendid ja operatsioonid. Nii moodustavad näiteks positiivsed reaalarvud korrutamise suhtes rühma, kõik reaalarvud aga liitmise suhtes rühma — reaalarvude aditiivse rühma, kusjuures need kaks rühma on isomorfsed, sest kui

$$a \longleftrightarrow \log a\,, \quad b \longleftrightarrow \log b\,,$$

siis

$$ab \longleftrightarrow \log (ab) = \log a + \log b\,.$$

Rühma isomorfset vastavust mistahes ühe operatsiooniga hulgaga iseloomustab järgmine teoreem, mille tõestuse anname hiljem (§ 21, art. 1).

T e o r e e m 3. *Kui mingi ühe operatsiooniga hulk M on isomorfses vastavuses rühmaga G, siis osutub ka M rühmaks, kusjuures G ühikelemendile vastab M ühikelement ja G mingi elemendi pöördelemendile vastava M elemendi pöördelement.*

Rühmade isomorfismi rakendusena on Cayley näidanud, et iga lõplik rühm on isomorfne teatava substitutsioonide rühmaga. Nimelt korrutades antud rühma

$$G = \{a_1\,,\ a_2\,,\ \ldots\,,\ a_n\}$$

paremalt mingi tema elemendiga a, saame

$$Ga = \{a_1 a\,,\ a_2 a\,,\ \ldots\,,\ a_n a\},$$

kus korrutised $a_1 a\,,\ a_2 a\,,\ \ldots\,,\ a_n a$ kujutavad jälle G elemente ja nimelt k õ i k i G elemente, sest need korrutised on kõik üksteisest erinevad. Seega võime märkida

$$a_1 a = a_{\alpha_1},\ a_2 a = a_{\alpha_2}\,,\ \ldots\,,\ a_n a = a_{\alpha_n},$$

kus $\alpha_1\,,\ \alpha_2\,,\ \ldots\,,\ \alpha_n$ tähendavad indekseid $1\,,\ 2\,,\ \ldots\,,\ n$ teatavas järjekorras. Niisiis kutsub G korrutamine paremalt elemendiga a esile G elementide järjekorra indeksite substitutsiooni

$$s_a = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}.$$

Seades G igale elemendile a vastavusse substitutsiooni s_a, saamegi isomorfse vastavuse, nagu selles võib eriliste raskusteta veenduda. Teoreemi 3 põhjal moodustavad siis ka substitutsioonid s_a rühma.

Vaatleme näitena hulka

$$V_4 = \{e, a, b, c\},$$

kus korrutamine on määratud tabeliga

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Sellest tabelist nähtub kergesti, et V_4 on rühm ja nimelt Abeli rühm, kusjuures e kujutab ühikelementi. See rühm, mis on esmakordselt uuritud saksa matemaatiku Klein'i poolt, kannab neljarühma nime. Arvutades korrutised V_4e, V_4a, V_4b, V_4c, leiame

$$V_4e = \{e, a, b, c\}, \quad V_4a = \{a, e, c, b\}, \quad V_4b = \{b, c, e, a\},$$
$$V_4c = \{c, b, a, e\},$$

millest ilmneb, et

$$s_e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad s_a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad s_b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},$$
$$s_c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Seega võib neljarühma esitada neljanda astme substitutsioonide abil kujul

$$V_4 = \{e, s_a, s_b, s_c\},$$

kus s_e kui ühiksubstitutsioon on märgitud lihtsalt e-ga.

Märkus. Cayley teoreem lubab põhimõtteliselt abstraktsete lõplike rühmade teooriat taandada substitutsioonirühmade teooriale. Kuid osutub, et üleminek substitutsioonirühmadele ei kergenda enamikel juhtudel lõplike rühmade uurimist, vaid, vastupidi, raskendab seda. Seepärast, uurides paragrahvis 23 substitutsioonirühmi, ei tee me seda mitte üldiste rühmaomaduste avastamiseks, vaid substitutsioonirühmade rakenduslikult seisukohalt väärtuslike individuaalomaduste selgitamiseks.

2. Automorfism. Rühmateoorias pakuvad erilist huvi niisugused isomorfismid, mille puhul rühmale G vastab G ise, s. o. kus $\bar{G} = G$. Rühma isomorfset vastavust iseendaga nimetatakse automorfismiks. Automorfismi lihtsaima näitena esineb nn. identne automorfism, mille puhul rühma iga element jääb muutumatuks.

Kui x tähendab kindlat elementi rühmas G, siis vastavus, kus G elemendile a vastab element $\bar{a} = x^{-1}ax$, on automorfism. Tõepoolest, korrutades võrdust $\bar{a} = x^{-1}ax$ vasakult x-ga ja paremalt x^{-1}-ga, leiame

$$a = x\bar{a}x^{-1},$$

millest nähtub, et korraldatud vastavusest võtab G iga element $\bar{a}$ osa parajasti üks kord, vastates elemendile $a = x\bar{a}x^{-1}$. Teiste sõnadega, meil on tegemist üksühese vastavusega

$$a \leftrightarrow \bar{a},$$

mille puhul G-le vastab G ise. Vastaku veel G elemendile b element $\bar{b}$:

$$b \leftrightarrow \bar{b},$$

kus $\bar{b} = x^{-1}bx$. Korrutisele ab vastab siis element

$$\overline{ab} = x^{-1}(ab)x = (x^{-1}ax)(x^{-1}bx) = \bar{a}\bar{b},$$

s. o.

$$ab \leftrightarrow \bar{a}\bar{b}$$

Tähendab, korraldatud vastavus on automorfism.

Automorfismi

$$a \longleftrightarrow x^{-1}ax$$

nimetatakse G siseautomorfismiks. Rühma siseautomorfismide hulka kuulub eriti ka identne automorfism $a \longleftrightarrow a$, mis vastab juhule $x = e$. Ei ole raske näha, et iga Abeli rühm omab vaid ühte siseautomorfismi — identset automorfismi, sest korrutise kommutatiivsuse tõttu on siin

$$a = x^{-1}ax = ax^{-1}x = ae = a,$$

sõltumata x-st.

Vastandina siseautomorfismidele nimetame kõiki rühma G ülejäänud automorfisme, mis ei avaldu kujul $a \longleftrightarrow x^{-1}ax$, G välisautomorfismideks. Rühma kõigi automorfismide leidmine ja nendevaheliste seoste püstitamine etendab olulist osa rühma struktuuri uurimisel.

Vaatleme näitena neljarühma $G = \{e, a, b, c\}$ (art. 1). Et automorfismi kui isomorfismi erijuhu puhul peab ühikelemendile vastama teoreemi 3 järgi ühikelement, siis on siin võimalikud järgmised 6 G üksühest vastavust iseendaga:

$$\begin{array}{cccccc}
e \longleftrightarrow e & e \longleftrightarrow e & e \longleftrightarrow e & e \longleftrightarrow e & e \longleftrightarrow e & e \longleftrightarrow e \\
a \longleftrightarrow a & a \longleftrightarrow a & a \longleftrightarrow b & a \longleftrightarrow b & a \longleftrightarrow c & a \longleftrightarrow c \\
b \longleftrightarrow b & b \longleftrightarrow c & b \longleftrightarrow a & b \longleftrightarrow c & b \longleftrightarrow a & b \longleftrightarrow b \\
c \longleftrightarrow c, & c \longleftrightarrow b, & c \longleftrightarrow c, & c \longleftrightarrow a, & c \longleftrightarrow b, & c \longleftrightarrow a.
\end{array}$$

Neist esimene vastavus kujutab identset automorfismi, mis on neljarühma kui Abeli rühma ainuke siseautomorfism. Mis puutub ülejäänud vastavustesse, siis ei ole raske näha, et nad osutuvad ka G automorfismideks — välisautomorfismideks. Selleks tarvitseb vaid kontrollida, et need vastavused säilivad korrutamise puhul. Nii vastab näiteks teises vastavuses a-le a ja b-le c, mistõttu korrutisele $ab = c$ vastab korrutis $ac = b$, kus b on tõesti c-le vastav element.

3. Kaaselemendid. Vaatleme rühma G siseautomorfismi

$$a \longleftrightarrow x^{-1}ax.$$

Vastavalt elemendi x valikule saame ühe või teise siseautomorfismi. Iga elementi $\bar{a} = x^{-1}ax$, mis mingis G siseautomorfismis vastab elemendile a, nimetatakse a kaaselemendiks. Ei ole raske näha, et kaasluse seos $\bar{a} = x^{-1}ax$ on refleksiivne, sümmeetriline ja transitiivne, rahuldades seega võrduse postulaate (I, § 5, art. 1). Tõepoolest:

1^0 iga element a on iseenda kaaselement, nagu see nähtub võrdusest $\bar{a} = x^{-1}ax$, võttes seal $x = e$;

2^0 kui $\bar{a}$ on a kaaselement, siis ka a on $\bar{a}$ kaaselement, sest võrdust $\bar{a} = x^{-1}ax$ vasakult x-ga ja paremalt x^{-1}-ga korrutades saame

$$a = x\bar{a}x^{-1} = (x^{-1})^{-1}\bar{a}x^{-1};$$

3^0 kui $\bar{a}$ on a kaaselement ja $\bar{\bar{a}}$ $\bar{a}$ kaaselement, siis $\bar{\bar{a}}$ on ka a kaaselement, sest kui $\bar{a} = x^{-1}ax$, $\bar{\bar{a}} = y^{-1}\bar{a}y$, siis

$$\bar{\bar{a}} = y^{-1}x^{-1}axy = (xy)^{-1}a(xy).$$

Jaotame nüüd rühmas G kõik elemendid klassideks — kaaselementide klassideks, võttes ühte klassi kokku kõik need G elemendid, mis on omavahel kaaselemendid. Elemendi a kõigi kaaselementide klassi märgime sümboliga $\{x^{-1}ax\}$. Siin erinevatel klassidel $\{x^{-1}ax\}$ ja $\{x^{-1}bx\}$ ei saa olla ühtki ühist elementi, sest kui niisugune ühine element c leiduks, siis kuuluksid a ja b kui c kaaselemendid ühte klassi, mistõttu vaadeldavad klassid peaksid langema ühte.

Näide 2. Leida sümmeetrilise rühma S_3 kaaselementide klassid.

Kõigepealt paneme tähele, et ühikelemendi e puhul on $x^{-1}ex = ex^{-1}x = e^2 = e$, millest nähtub, et ühikelement ei oma teisi kaaselemente peale iseenda, moodustades seega omaette klassi $\{x^{-1}ex\} = \{e\}$. Leiame nüüd mingi teise elemendi, näiteks s_1 kaaselementide klassi. Et

$$e^{-1}s_1e = s_1, \quad s_1^{-1}s_1s_1 = s_1, \quad s_2^{-1}s_1s_2 = s_1,$$
$$s_3^{-1}s_1s_3 = s_2, \quad s_4^{-1}s_1s_4 = s_2, \quad s_5^{-1}s_1s_5 = s_2,$$

siis $\{x^{-1}s_1x\} = \{s_1, s_2\}$. Edasi võtame mingi elemendi, mis ei esine eelmistes klassides, näiteks s_3, ja leiame tema kaaselementide klassi. Et

$$e^{-1}s_3e = s_3, \quad s_1^{-1}s_3s_1 = s_5, \quad s_2^{-1}s_3s_2 = s_4,$$
$$s_3^{-1}s_3s_3 = s_3, \quad s_4^{-1}s_3s_4 = s_5, \quad s_5^{-1}s_3s_5 = s_4,$$

siis $\{x^{-1}s_3x\} = \{s_3, s_4, s_5\}$. Seega lahutades sümmeetrilise rühma S_3 kaaselementide klassideks, saame

$$S_3 = \{e\} + \{s_1, s_2\} + \{s_3, s_4, s_5\}.$$

Tekib küsimus, kuidas otsustada, kui palju on erinevaid elemente klassis $\{x^{-1}ax\}$ ja kuidas neid leida, ilma et tarvitseks arvutada kõiki korrutisi $x^{-1}ax$. Vaatleme selle küsimuse selgitamiseks rühmas G niisuguseid elemente x, mis on kommuteeruvad antud elemendiga a, s. o. mille puhul

$$ax = xa.$$

Elemendiga a kommuteeruvate G elementide hulka nimetame elemendi a normalisaatoriks ja märgime tähega N_a. Näitame, et normalisaator N_a kujutab G alamrühma. Tõepoolest:

1⁰ kui $x \in N_a$ ja $y \in N_a$, s. o.

$$ax = xa, \quad ay = ya,$$

siis esimest võrdust paremalt y-ga korrutades leiame teist võrdust silmas pidades

$$axy = xay = xya,$$

mis ütleb, et $xy \in N_a$;

2⁰ kui $x \in N_a$, nii et $ax = xa$, siis, korrutades viimast võrdust mõlemalt poolt x^{-1}-ga, saame

$$x^{-1}a = ax^{-1},$$

mis ütleb, et $x^{-1} \in N_a$.

Lahutades rühma G parempoolseteks kõrvalklassideks elemendi a normalisaatori N_a järgi, leiame

$$G = \sum N_a c.$$

Näitame, et nendele x-i väärtustele, mis kuuluvad ühte ja samasse kõrvalklassi $N_a c$, vastab üks ja sama a kaaselement $c^{-1}ac$, kuna erinevatesse kõrvalklassidesse kuuluvatele x-i väärtustele vastavad erinevad kaaselemendid. Olgu n mistahes element a normalisaatoris N_a, nii et $N_a c = \{nc\}$. Leiame a kaaselemendi $(nc)^{-1}a(nc)$, mis vastab x-i väärtusele nc. Silmas pidades, et $(nc)^{-1} = c^{-1}n^{-1}$ ja $an = na$, saame

$$(nc)^{-1}a(nc) = c^{-1}n^{-1}anc = c^{-1}n^{-1}nac = c^{-1}ac,$$

mis ütleb, et kõigile x-i väärtustele kõrvalklassis $N_a c$ vastab üks ja sama a kaaselement $c^{-1}ac$. Tähendagu nüüd c_1 ja c_2 elemente erinevatest kõrvalklassidest N_a järgi. Kui oleks

$$c_1^{-1}ac_1 = c_2^{-1}ac_2,$$

siis seda võrdust vasakult c_1-ga ja paremalt c_2^{-1}-ga korrutades saaksime

$$ac_1c_2^{-1} = c_1c_2^{-1}a,$$

millest nähtub, et $c_1c_2^{-1}$ kujutab teatavat normalisaatori N_a elementi n, s. o.

$$c_1c_2^{-1} = n,$$

kust

$$c_1 = nc_2.$$

Viimase võrduse järgi peaks c_1 kuuluma kõrvalklassi Nc_2, tähendab samasse kõrvalklassi, kuhu kuulub c_2. Eelduse järgi pidid aga c_1 ja c_2 kuuluma erinevatesse kõrvalklassidesse.

Seega on meie väide tõestatud. Ühtlasi oleme saanud antud elemendi kaaselementide arvu määramiseks eeskirja, mille sõnastame järgmise teoreemina.

Teoreem 4. *Rühmas G on elemendi a kaaselementide arv võrdne a normalisaatori N_a indeksiga G suhtes.*

Erijuhul, kui G on lõplik rühm, on indeks (N_a, G) rühma G järgu jagaja (§ 19, art. 3). Tähendab, *lõplikus rühmas on iga elemendi kaaselementide arv rühma järgu jagajaks.*

Leiame näiteks sümmeetrilises rühmas S_3 elemendi s_3 kaaselemendid. Nagu näitab proovimine, kommuteeruvad S_3 elementidest s_3-ga vaid e ja s_3, nii et s_3 normalisaator omab kuju

$$N_{s_3} = \{e\,,\ s_3\} = H\,.$$

S_3 lahutus parempoolseteks kõrvalklassideks H järgi on näite 1 põhjal (§ 19, art. 3)

$$S_3 = H + Hs_1 + Hs_2\,.$$

Seega on elemendil s_3 kolm kaaselementi

$$e^{-1}s_3e = s_3\,,\quad s_1^{-1}s_3s_1 = s_5\,,\quad s_2^{-1}s_3s_2 = s_4\,,$$

kooskõlas varem saadud tulemusega.

4. Kaasalamrühmad. Olgu H rühma G alamrühm. G siseautomorfismis $a \longleftrightarrow x^{-1}ax$ vastab H-le alamrühm

$$\overline{H} = x^{-1}Hx\,.$$

Iga alamrühma $\overline{H} = x^{-1}Hx$, mis mingis G siseautomorfismis vastab alamrühmale H, nimetatakse H k a a s a l a m r ü h m a k s. H kaasalamrühmad, olles isomorfsed H-ga, on kõik omavahel isomorfsed. Nii nagu rühm G jaguneb kaaselementide klassideks $\{x^{-1}ax\}$ (art. 3), nii G kõigi alamrühmade hulk jaguneb kaasalamrühmade klassideks $\{x^{-1}Hx\}$. Et leida H kaasalamrühmade arvu, vaatleme rühmas G niisuguseid elemente x, mis on kommuteeruvad H-ga, s. o. mille puhul

$$Hx = xH\,.$$

Alamrühmaga H kommuteeruvate G elementide hulka nimetame a l a m r ü h m a H n o r m a l i s a a t o r i k s ja märgime tähega N_H. Täpselt nagu elemendi a normalisaatori N_a puhul saab näidata, et ka alamrühma H normalisaator N_H kujutab rühma. Samuti võib analoogiliselt teoreemile 4 tõestada teoreemi, mille järgi rühma G alamrühma H kaasalamrühmade arv on võrdne H normalisaatori N_H indeksiga G suhtes.

Vaatleme eriti juhtu, kus H on normaaljagaja. Sel korral on iga $x \in G$ puhul kehtiv võrdus

$$Hx = xH ,$$

mida vasakult x^{-1}-ga korrutades saame

$$x^{-1}Hx = H ,$$

s. o. normaaljagaja H ühtib kõigi oma kaasalamrühmadega. Ümberpöördult, kui mingi alamrühm H ühtib kõigi oma kaasalamrühmadega, siis on H normaaljagaja, sest võrdusest

$$x^{-1}Hx = H$$

järeldub pärast korrutamist vasakult x-ga võrdus

$$Hx = xH .$$

Tähendab, *alamrühm osutub normaaljagajaks siis ja ainult siis, kui ta ühtib kõigi oma kaasalamrühmadega.* Seega iseloomustab rühma G normaaljagajat tema invariantsus G kõigi siseautomorfismide suhtes, mistõttu nimetatakse normaaljagajat sageli ka i n v a r i a n t s e k s a l a m r ü h m a k s.

Näitame veel, et normaaljagajat H iseloomustavat tingimust $x^{-1}Hx = H$ võib asendada väliselt vähemnõudliku tingimusega

(8) $$x^{-1}Hx \subset H .$$

Tõepoolest, kui tingimus (8) on kehtiv iga $x \in G$ puhul, siis, võttes x-i asemel x^{-1}, saame

$$xHx^{-1} \subset H ,$$

kust pärast korrutamist vasakult x^{-1}-ga ja paremalt x-ga järeldub

$$H \subset x^{-1}Hx ,$$

millest koos tingimusega (8) nähtub, et $x^{-1}Hx = H$.

Niisiis on tingimus (8) tarvilik ja piisav selleks, et H oleks normaaljagaja ehk, teiste sõnadega: *alamrühm osutub normaaljagajaks siis ja ainult siis, kui ta sisaldab kõiki oma elemen-*

tide kaaselemente. Seega koosneb normaaljagaja tervetest kaaselementide klassidest, mistõttu rühma kaaselementide klasside tundmine kergendab normaaljagajate leidmist. Nii nähtub näites 2 (art. 3) leitud sümmeetrilise rühma S_3 kaaselementide klassidest

$$\{e\},\ \{s_1, s_2\},\ \{s_3, s_4, s_5\},$$

et S_3 ainukeseks pärisnormaaljagajaks peale ühikrühma on

$$H = \{e\} + \{s_1, s_2\} = \{e, s_1, s_2\},$$

kuna näiteks kombinatsioon $\{e\} + \{s_3, s_4, s_5\}$ ei moodusta Lagrange'i teoreemi põhjal (§ 19, art. 3) üldse alamrühma.

Näitame lõppeks tingimuse (8) rakendamise näitena, et kahe normaaljagaja H_1 ja H_2 ühisosa $H_1 \cap H_2$ ja korrutis H_1H_2 on ka normaaljagajad. Et $H_1 \cap H_2$ ja H_1H_2 on alamrühmad, seda tõestasime juba varem (§ 19, art. 2 ja 4), mistõttu jääb näidata, et viimased alamrühmad sisaldavad kõiki oma elementide kaaselemente.

Olgu h mingi element ühisosas $H_1 \cap H_2$, nii et $h \in H_1$ ja $h \in H_2$. Siin H_1 ja H_2 kui normaaljagajad sisaldavad kõiki h kaaselemente, mistõttu ka H sisaldab kõiki neid kaaselemente.

Olgu nüüd h mingi element korrutises H_1H_2, nii et $h = h_1h_2$, kus $h_1 \in H_1$ ja $h_2 \in H_2$. Et H_1 kui normaaljagaja sisaldab kõiki h_1 kaaselemente $x^{-1}h_1x$ ja H_2 kõiki h_2 kaaselemente $x^{-1}h_2x$, siis sisaldab korrutis H_1H_2 kõiki elemente

$$(x^{-1}h_1x)(x^{-1}h_2x) = x^{-1}h_1h_2x = x^{-1}hx,$$

s. o. kõiki h kaaselemente.

§ 21. Homomorfism.

1. Homomorfismi mõiste. Vaatleme ühelt poolt täisarvude aditiivset rühma

$$\Gamma = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

ja teiselt poolt mingi elemendi a poolt moodustatud tsüklilist rühma

$$\{\ldots, a^{-3}, a^{-2}, a^{-1}, e, a^1, a^2, a^3, \ldots\}.$$

Seades igale täisarvule k vastavusse astme a^k, näeme, et see vastavus säilib vaadeldavate rühmade operatsioonide puhul, sest kui

$$k \to a^k, \quad l \to a^l,$$

siis

$$k + l \to a^{k+l} = a^k a^l.$$

Erijuhul, kui tsükliline rühm on lõpmatu, on kõik a astmed üksteisest erinevad ja seega vastavad erinevatele täisarvudele erinevad a astmed, nii et korraldatud vastavus osutub üksüheseks. Tähendab, täisarvude aditiivne rühm on isomorfne lõpmatu tsüklilise rühmaga.

Seevastu, kui tsükliline rühm on lõplik, omades järku m, siis on

$$a^n = e$$

iga n puhul, mis jagub m-ga (§ 18, art. 3), mistõttu kõigile m-ga jaguvaile täisarvudele vastavad võrdsed a astmed. Seega pole korraldatud vastavus sel korral enam üksühene, mistõttu me ei või siin kõnelda isomorfismist.

Üldiselt, kui ühe hulga igale elemendile on seatud vastavusse kindel element teisest hulgast, nii et teise hulga iga element võtab sellest vastavusest osa vähemalt üks kord, s. o. vastab vähemalt ühele esimese hulga elemendile, siis öeldakse, et teine hulk on esimesega *üheses vastavuses*. Ühese vastavuse puhul vastavad esimese hulga võrdsetele elementidele võrdsed elemendid teises hulgas, kuna esimese hulga erinevatele elementidele ei tarvitse tingimata vastata erinevad elemendid teises hulgas.

Definitsioon 4. Kui rühma $\overline{G}$ on võimalik seada ühesesse vastavusse rühmaga G nii, et korrutisele rühmas G vastab tegureile vastavate elementide korrutis rühmas $\overline{G}$, siis öeldakse, et $\overline{G}$ on *homomorfne* rühmaga G.

Rühma $\overline{G}$ vastavust rühmaga G nimetatakse sel juhul *homomorfseks vastavuseks* ehk *homomorfismiks*. Niisiis on rühmade homomorfism niisugune ühene vas-

tavus, mis säilib rühmaoperatsioonide puhul. Rühma $\overline{G}$ homomorfset vastavust rühmaga G märgime sümboliga

$$G \rightarrow \overline{G}.$$

Erijuhul, kui siin vastavus on üksühene, taandub homomorfism isomorfismiks

$$G \leftrightarrow \overline{G}.$$

Nagu nägime, saab näiteks iga tsüklilist rühma seada homomorfsesse vastavusse täisarvude aditiivse rühmaga, kusjuures homomorfism taandub isomorfismiks, kui tsükliline rühm on lõpmatu.

Mistahes ühe operatsiooniga hulga homomorfset vastavust mingi rühmaga iseloomustab järgmine teoreem.

Teoreem 5. *Kui mingi ühe operatsiooniga hulk M on homomorfses vastavuses rühmaga G, siis osutub ka M rühmaks, kusjuures G ühikelemendile vastab M ühikelement ja G mingi elemendi pöördelemendile M vastava elemendi pöördelement.*

Erijuhul, kui homomorfism taandub isomorfismiks, järeldub siit teoreem 3 (§ 20, art. 1).

Teoreemi 5 tõestuseks näitame, et hulgas M kehtivad rühma postulaadid I—IV (§ 18, art. 1). Ühtlasi ilmneb seejuures G ja M ühikelementide ja pöördelementide vastavus.

I. Korrutamise seadus. Olgu $\bar{a}$ ja $\bar{b}$ mingid kaks elementi hulgas M. Homomorfismi tõttu peab $\bar{a}$ vastama vähemalt ühele G elemendile a ja $\bar{b}$ vähemalt ühele G elemendile b, s. o. leiduvad G elemendid a ja b, nii et

$$a \rightarrow \bar{a}, \quad b \rightarrow \bar{b},$$

kusjuures

$$ab \rightarrow \bar{a}\bar{b}.$$

Teiselt poolt peab korrutisele ab kui G elemendile vastama mingi M element. Vastavuse ühesuse tõttu peab seega $\bar{a}\bar{b}$ kuuluma hulka M.

II. Assotsiatiivsuse seadus. Märgime tähtedega $\bar{a}$, $\bar{b}$ ja $\bar{c}$ mingid kolm elementi hulgas M, mis vastaku G elementidele a, b ja c. Siis on homomorfismi tõttu

$$a(bc) \to \bar{a}(\bar{b}\bar{c}), \quad (ab)c \to (\bar{a}\bar{b})\bar{c}.$$

Et aga G on rühm, siis $a(bc) = (ab)c$ ja seega ka

$$\bar{a}(\bar{b}\bar{c}) = (\bar{a}\bar{b})\bar{c},$$

sest homomorfismis vastavad G võrdsetele elementidele võrdsed elemendid hulgas M.

III. Ühikelemendi olemasolu seadus. Märgime G ühikelemendi e-ga ja temale vastava M elemendi $\bar{e}$-ga. Olgu $\bar{a}$ mingi M element, mis vastaku G elemendile a. Et

$$ae = a,$$

siis saame homomorfismi tõttu

$$\bar{a}\bar{e} = \bar{a},$$

mis ütleb, et $\bar{e}$ on M ühikelement.

IV. Pöördelemendi olemasolu seadus. Olgu $\bar{a}$ mingi M element, mis vastaku G elemendile a. Märgime a pöördelemendi a^{-1}-ga ja temale vastava M elemendi $\overline{a^{-1}}$-ga. Et

$$aa^{-1} = e,$$

siis saame homomorfismi tõttu

$$\bar{a}\,\overline{a^{-1}} = \bar{e},$$

mis ütleb, et $\overline{a^{-1}}$ on $\bar{a}$ pöördelement.

Seega on teoreem 5 tõestatud.

2. Teoreem rühma homomorfismidest. Vaatleme homomorfismi näitena mistahes rühma G ja tema faktorrühma

$$G/H = \{Ha\},$$

kus H tähendab G normaaljagajat. Seades G igale elemen-

dile a vastavusse selle elemendiga esindatud kõrvalklassi Ha, näeme, et see vastavus säilib vaadeldavate rühmade operatsioonide puhul, sest kui

$$a \longrightarrow Ha, \quad b \longrightarrow Hb,$$

siis, silmas pidades kõrvalklasside korrutamise eeskirja (7) (§ 19, art. 4), leiame

$$ab \longrightarrow Hab = Ha \cdot Hb.$$

Seega oleme saanud homomorfismi

$$G \overset{\cdot}{\longrightarrow} G/H. \tag{9}$$

Tähendab, *G iga faktorrühma G/H võib seada homomorfsesse vastavusse rühma G endaga.* Huvitav on siinjuures asjaolu, et homomorfismidega (9) on ammendatud üldse kõik võimalikud rühma G homomorfismid. Nimelt on kehtiv järgmine tähelepandav teoreem rühma homomorfismidest.

Teoreem 6. *Kui rühm $\overline{G}$ on homomorfses vastavuses rühmaga G, siis on $\overline{G}$ isomorfne faktorrühmaga G/H, kus normaaljagaja H koosneb kõigist neist G elementidest, millele vastab homomorfismis $G \longrightarrow \overline{G}$ rühma $\overline{G}$ ühikelement.*

Lühidalt, kui $G \overset{\cdot}{\longrightarrow} \overline{G}$, siis $\overline{G} \overset{\cdot}{\longleftrightarrow} G/H$.

Teoreemi 6 tõestuseks jaotame rühma G elemendid klassidesse, võttes kõik need G elemendid, millele vastab antud homomorfismis üks ja sama $\overline{G}$ element $\overline{a}$, kokku üheks klassiks $M_{\overline{a}}$. Vaatleme kõigepealt klassi $M_{\overline{e}}$, mille elementidele vastab antud homomorfismis $\overline{G}$ ühikelement $\overline{e}$. Näitame, et $M_{\overline{e}}$ on G alamrühm. Tõepoolest:

1° kui $a \in M_{\overline{e}}$ ja $b \in M_{\overline{e}}$, siis

$$a \longrightarrow \overline{e}, \quad b \longrightarrow \overline{e}$$

ja seega homomorfismi tõttu

$$ab \longrightarrow \overline{e}\,\overline{e} = \overline{e},$$

millest nähtub, et $ab \in M_{\overline{e}}$;

2^0 kui $a \in M_{\bar{e}}$, siis $a \longrightarrow \bar{e}$ ja seega teoreemi 5 põhjal

$$a^{-1} \longrightarrow \bar{e}^{-1} = \bar{e},$$

millest nähtub, et $a^{-1} \in M_{\bar{e}}$.

Seega osutub klass $M_{\bar{e}}$ alamrühmaks, kusjuures märgime lühiduse mõttes $M_{\bar{e}} = H$.

Vaatleme nüüd üldiselt klassi $M_{\bar{a}}$. Olgu a mingi kindel, b aga mistahes element selles klassis, nii et klassi $M_{\bar{a}}$ mõiste kohaselt

$$a \longrightarrow \bar{a}, \quad b \longrightarrow \bar{a}.$$

Et rühmas G on võrrand $xa = b$ üheselt lahenduv (§ 18, art. 2), siis leidub G-s kindel element h, mille puhul

$$ha = b.$$

Viimasele võrdusele vastab antud homomorfismis võrdus

$$\bar{h}\bar{a} = \bar{a},$$

mis ütleb, et $\bar{h}$ on rühma $\bar{G}$ ühikelement, s. o. $\bar{h} = \bar{e}$. Seega kuulub h alamrühma H. Niisiis avaldub klassi $M_{\bar{a}}$ iga element b kujul

$$b = ha,$$

kus $h \in H$, mistõttu klass $M_{\bar{a}}$ kuulub kõrvalklassi Ha:

$$M_{\bar{a}} \subset Ha. \tag{10}$$

Ümberpöördult, kõrvalklassi Ha igale elemendile ha vastab antud homomorfismis element

$$\bar{h}\bar{a} = \bar{e}\bar{a} = \bar{a},$$

mistõttu ha kuulub klassi $M_{\bar{a}}$ ja seega

$$Ha \subset M_{\bar{a}}.$$

Siit ja seosest (10) järeldub, et

$$M_{\bar{a}} = Ha .$$

Vaadeldes võrrandi $xa = b$ asemel võrrandit $ax = b$, saab analoogiliselt näidata, et

$$M_{\bar{a}} = aH .$$

Kahest viimasest võrdusest nähtub aga, et $Ha = aH$, mis ütleb, et H on normaaljagaja.

Niisiis pole klassid $M_{\bar{a}}$ muud midagi kui kõrvalklassid normaaljagajaga $H = M_{\bar{e}}$ järgi ja moodustavad seega teoreemi 2 põhjal faktorrühma G/H (§ 19, art. 4). Näitame, et $\bar{G}$ on isomorfne selle faktorrühmaga. Seame selleks igale $\bar{G}$ elemendile $\bar{a}$ vastavusse kõrvalklassi $Ha = M_{\bar{a}}$. Siis vastavad erinevatele $\bar{G}$ elementidele $\bar{a}$ ja $\bar{b}$ erinevad kõrvalklassid $Ha = M_{\bar{a}}$ ja $Hb = M_{\bar{b}}$, sest kui oleks

$$Ha = Hb ,$$

siis vastaks homomorfismis $G \to \bar{G}$ kõrvalklassi $Ha = Hb$ elementidele niihästi element $\bar{a}$ kui ka $\bar{b}$, mistõttu vastavus selles homomorfismis poleks ühene. Järelikult on korraldatud vastavus üksühene. Ei ole raske näha, et see vastavus säilib korrutamise puhul. Nimelt kui

$$\bar{a} \leftrightarrow Ha , \quad \bar{b} \leftrightarrow Hb ,$$

siis

$$\bar{a}\bar{b} \leftrightarrow Hab ,$$

sest korrutisele ab vastab homomorfismis $G \to \bar{G}$ korrutis $\bar{a}\bar{b}$. Nüüd on aga kõrvalklasside korrutamise eeskirja (7) kohaselt (§ 19, art. 4)

$$Ha \cdot Hb = Hab$$

ja seega

$$\bar{a}\bar{b} \to Ha \cdot Hb .$$

Tähendab, $\bar{G} \leftrightarrow G/H$, millega on teoreem 6 tõestatud.

Vaatleme näitena artiklis 1 käsiteldud m-järku tsüklilise rühma homomorfset vastavust täisarvude aditiivse rühmaga Γ. Teoreemi 6 järgi peab siin tsükliline rühm olema isomorfne faktorrühmaga Γ/H, kus H koosneb kõigist neist täisarvudest n, mille puhul $a^n = e$, s. o. täisarvudest n, mis jaguvad m-ga (§ 18, art. 3). Seega

$$H = \{km\},$$

kus k tähendab mistahes täisarvu, mistõttu faktorrühm Γ/H on isomorfne jäägiklassiringi $R^{(m)}$ aditiivse rühmaga (§ 19, art. 4). Niisiis on m-järku tsükliline rühm isomorfne jäägiklassiringi $R^{(m)}$ aditiivse rühmaga.

3. Teoreem isomorfismist. Olgu H rühma G normaaljagaja ja A mistahes alamrühm. Siis kujutab korrutis HA ka alamrühma (§ 19, art. 4), mistõttu võime moodustada faktorrühma

$$HA/H.$$

Kui h tähendab mingit H elementi ja a mingit A elementi, siis, korraldades vastavuse

$$ha \longrightarrow Hha = (Hh)a = Ha,$$

saame homomorfismi (art. 2)

$$HA \longrightarrow HA/H.$$

Et selle homomorfismi puhul

$$a \longrightarrow Ha, \quad ha \longrightarrow Ha,$$

siis vastab siin juba alamrühmale A kogu faktorrühm HA/H, s. o.

$$A \longrightarrow HA/H.$$

Rakendades teoreemi rühma homomorfismidest, leiame

$$HA/H \longleftrightarrow A/H \cap A,$$

sest need A elemendid, millele vastab faktorrühma HA/H ühikelement H, moodustavad H ja A ühisosa $H \cap A$. Ühtlasi näh-

tub siit, et $H \cap A$ on A normaaljagaja[1]. Tulemus leiab väljenduse järgmises teoreemis isomorfismist.

Teoreem 7. *Kui H on rühma G normaaljagaja ja A mistahes alamrühm, siis kujutab ühisosa $H \cap A$ rühma A normaaljagajat, kusjuures*

$$HA/H \leftrightarrow A/H \cap A .$$

Vaatleme teoreemi 7 rakenduse näitena neljanda astme sümmeetrilist rühma S_4. Olgu siin H neljarühm V_4 (§ 20, art. 1) ja A kolmanda astme sümmeetriline rühm S_3. Korrutamise teel leiame kergesti, et $HA = S_4$. Kuna teiselt poolt $H \cap A$ kujutab ühikrühma, siis annab teoreem isomorfismist[2]

$$S_4/V_4 \leftrightarrow S_3 ,$$

s. o. sümmeetrilise rühma S_4 faktorrühm neljarühma V_4 järgi on isomorfne sümmeetrilise rühmaga S_3.

Uurime lõppeks veel alamrühmade vastavust homomorfismis $G \to \overline{G}$. Rakendades teoreemi rühma homomorfismidest, võime kirjutada

$$\overline{G} \leftrightarrow G/H ,$$

kus normaaljagaja H koosneb nendest G elementidest, millele vastab antud homomorfismis $\overline{G}$ ühikelement. Kui selles homomorfismis vastab G alamrühmale A rühma $\overline{G}$ alamrühm $\bar{A}$, siis võib $\bar{A}$ vastata peale A veel teistele G alamrühmadele, sest elementide vastavus pole homomorfismi puhul üksühene. Eesmärgiga saada üksühest vastavust G ja $\overline{G}$ alamrühmade vahel piirdume nende G alamrühmadega A, mis sisaldavad normaaljagajat H. Kõneldes $\overline{G}$ asemel temaga isomorfsest faktorrühmast G/H, võime siis sõnastada järgmise teoreemi:

Teoreem 8. *Seades faktorrühma $\overline{G} = G/H$ igale alamrühmale $\bar{A}$ vastavusse G osahulga A, mis koosneb kõigist alamrühma $\bar{A}$ kuuluvate kõrvalklasside elementidest, saame üksühese*

[1] Vt. teoreemi 6 tõestus (art. 2).
[2] V_4 on S_4 normaaljagaja, nagu nähtub hiljem (§ 23, art. 2).

vastavuse faktorrühma G kõigi alamrühmade ja G nende alamrühmade vahel, mis sisaldavad normaaljagajat H. Seejuures vastab $\bar{G}$ normaaljagajale G normaaljagaja ja ümberpöördult.

Näitame kõigepealt, et G osahulk A, mis koosneb alamrühma $\bar{A}$ koosseisu kuuluvate kõrvalklasside elementidest, on alamrühm. Nimelt kui a ja b tähendavad A elemente, siis peab $\bar{A}$ sisaldama kõrvalklasse Ha ja Hb. Et aga $\bar{A}$ on rühm, siis peab ta sisaldama ka korrutist $Ha \cdot Hb = Hab$ ja pöördelementi $(Ha)^{-1} = Ha^{-1}$, millest nähtub, et $ab \in A$ ja $a^{-1} \in A$. Seega on A tõesti alamrühm.

Et H kui G ühikelement kuulub igasse alamrühma $\bar{A}$, siis $A \supset H$. Ei ole raske näha, et vastavus $\bar{G}$ alamrühmade $\bar{A}$ ja G alamrühmade A vahel on üksühene, s. o.

$$\bar{A} \leftrightarrow A,$$

sest erinevatele $\bar{G}$ alamrühmadele $\bar{A}_1$ ja $\bar{A}_2$ vastavad ilmselt erinevad G alamrühmad A_1 ja A_2.

Olgu nüüd $\bar{A}$ faktorrühma $\bar{G}$ normaaljagaja. Et $G \to \bar{G}$, kus $\bar{G} = G/H$ ja $\bar{G} \to \bar{G}/\bar{A}$ (art. 2), siis saame homomorfismi

$$G \to \bar{G}/\bar{A},$$

kus need G elemendid, millele vastab $\bar{G}/\bar{A}$ ühikelement $\bar{A}$, moodustavad G alamrühma A, mistõttu A on teoreemi 6 tõestuse põhjal normaaljagaja (art. 2).

Ümberpöördult, kui A on G normaaljagaja, siis

$$Ax = xA$$

iga $x \in G$ puhul. Et homomorfismis $G \to \bar{G}$ vastab x-le kõrvalklass Hx ja A-le alamrühm $\bar{A}$, siis vastab siin võrdusele $Ax = xA$ võrdus

$$\bar{A} \cdot Hx = Hx \cdot \bar{A},$$

mis ütleb, et $\bar{A}$ on $\bar{G}$ normaaljagaja.

Seega on teoreem 8 tõestatud.

§ 22. Kompositsioonijadad.

1. Maksimaalne normaaljagaja. Rühmateoorias etendavad väga tähtsat osa teatavad alamrühmade jadad, kus iga alamrühm on eelneva suhtes normaaljagajaks. Niisugust rühma G alamrühmade jada

$$G \supset G_1 \supset G_2 \supset \ldots \supset G_k = E,$$

mis algab rühmaga G ja lõpeb ühikrühmaga E ja kus iga alamrühm G_i on eelneva alamrühma G_{i-1} suhtes pärisnormaaljagaja, nimetatakse rühma G n o r m a a l j a d a k s. Arusaadav, et igal rühmal G on olemas normaaljadasid, kui mitte muid, siis näiteks $G \supset E$. Faktorrühmad

$$G/G_1, \quad G_1/G_2, \quad \ldots, \quad G_{k-1}/G_k$$

kannavad vaadeldava normaaljada f a k t o r i t e nime. Nende faktorite arv k määrab normaaljada p i k k u s e.

Olgu H rühma G pärisnormaaljagaja, nii et $G \supset H$. Kui rühmas G ei leidu ühtki teist pärisnormaaljagajat, mis sisaldaks H-d, siis öeldakse, et H on G suhtes m a k s i m a a l n e n o r m a a l j a g a j a. Niisugust normaaljada, kus iga alamrühm G_i on eelneva alamrühma G_{i-1} suhtes maksimaalne normaaljagaja, nimetatakse G k o m p o s i t s i o o n i j a d a k s. Teiste sõnadega, kompositsioonijada on niisugune normaaljada, mida pole võimalik tihendada uute normaaljagajatega.

On olemas lihtne kriteerium, mis lubab otsustada, kas rühma G normaaljagaja H on maksimaalne või mitte. Toome kõigepealt sisse nn. algrühma mõiste. A l g r ü h m a k s nimetatakse niisugust rühma, millel ei ole ühtki pärisnormaaljagajat peale ühikrühma. Seega omab algrühm G vaid ühte normaaljada $G \supset E$, mis kujutab ühtlasi ka kompositsioonijada. Algrühmade hulka kuuluvad näiteks kõik need lõplikud rühmad, mille järk on algarv [1], sest niisugustel rühmadel pole üldse teisi pärisalamrühmi peale ühikrühma, kuna Lagrange'i teoreemi

[1] Näiteks jäägiklassikorpuste $R^{(p)}$ aditiivsed rühmad.

järgi peab alamrühma järk olema rühma järgu jagajaks (§ 19, art. 3).

Kui nüüd H on rühma G maksimaalne normaaljagaja, siis on faktorrühm $\overline{G} = G/H$ algrühm, sest kui $\overline{G}$ omaks peale ühikrühma pärisnormaaljagajat $\bar{A}$, siis vastaks sellele normaaljagajale teoreemi 8 järgi (§ 21, art. 3) G pärisnormaaljagaja A (mis on H-st erinev), nii et

$$G \supset A \supset H,$$

mistõttu H ei saaks olla G maksimaalne normaaljagaja. Ümberpöördult, kui faktorrühm $\overline{G} = G/H$ on algrühm, siis peab H olema G maksimaalne normaaljagaja, sest kui rühmas G leiduks pärisnormaaljagaja A, mis sisaldab H-d, siis vastaks sellele normaaljagajale teoreemi 8 järgi faktorrühma $\overline{G}$ pärisnormaaljagaja $\bar{A}$ (mis on $\bar{E}$-st erinev), mistõttu $\overline{G}$ ei saaks olla algrühm.

Tähendab, *normaaljagaja H on rühma G maksimaalseks normaaljagajaks siis ja ainult siis, kui faktorrühm G/H on algrühm.*

Olgu antud näiteks 12-ndat järku tsükliline rühm

$$G = \{e,\ a,\ a^2,\ a^3,\ \ldots,\ a^{11}\}.$$

Ei ole raske näha, et siin

$$G_1 = \{e,\ a^3,\ a^6,\ a^9\}, \qquad G_2 = \{e,\ a^6\},$$
$$H_1 = \{e,\ a^2,\ a^4,\ a^6,\ a^8,\ a^{10}\}, \qquad H_2 = \{e,\ a^4,\ a^8\}$$

on G alamrühmad ja ühtlasi normaaljagajad, sest G on Abeli rühm. Vaatleme normaaljadasid

$$G \supset G_1 \supset G_2 \supset E,$$
$$G \supset H_1 \supset H_2 \supset E.$$

Neile normaaljadadele vastavad faktorid

$$G/G_1 = \{G_1,\ G_1a,\ G_1a^2\},\ G_1/G_2 = \{G_2,\ G_2a^3\},\ G_2/E = \{E,\ Ea^6\},$$
$$G/H_1 = \{H_1,\ H_1a\},\ H_1/H_2 = \{H_2,\ H_2a^2\},\ H_2/E = \{E,\ Ea^4,\ Ea^8\}$$

on algarvulist järku ja kujutavad seetõttu algrühmi. Seega on vaadeldavad normaaljadad kompositsioonijadad. Asjaolu, et neid

jadasid pole võimalik tihendada uute normaaljagajatega, ilmneb otsekohe, kui silmas pidada Lagrange'i teoreemi.

Olgu lõppeks G_1 ja H_1 teineteisest erinevad maksimaalsed normaaljagajad rühmas G. Siis on ka korrutis G_1H_1 rühma G normaaljagaja (§ 20, art. 4). Et G_1H_1 sisaldab normaaljagajaid G_1 ja H_1, siis peab viimaste maksimaalsuse tõttu olema $G_1H_1 = G$. Seega, rakendades normaaljagajatele G_1 ja H_1 teoreemi isomorfismist (§ 21, art. 3), saame

$$(11) \qquad G/G_1 \longleftrightarrow H_1/D, \qquad G/H_1 \longleftrightarrow G_1/D,$$

kus $D = G_1 \cap H_1$. Et G_1 ja H_1 on G maksimaalsed normaaljagajad, siis on isomorfismides (11) vasakpoolsed ja seega ka parempoolsed faktorrühmad algrühmad. Teiste sõnadega, $D = G_1 \cap H_1$ on nii G_1 kui ka H_1 suhtes maksimaalne normaaljagaja.

2. Jordan-Hölder'i teoreem. Nagu eelmises artiklis nägime, võib ühel rühmal olla mitu kompositsioonijada. Ometi on nende kompositsioonijadade vahel tihe seos. Selle seose väljendamiseks toome sisse nn. isomorfsete normaaljadade mõiste. Nimetame kahte normaaljada teineteisega i s o m o r f s e i k s, kui ühe jada faktoreid saab seada üksühesesse vastavusse teise jada faktoritega nii, et vastavad faktorid tulevad isomorfsed. Eriti on seega isomorfsed normaaljadad ühepikkused. Nüüd võime sõnastada ühe rühmateooria põhiteoreemi, mis kannab J o r d a n - H ö l d e r i t e o r e e m i nime.

T e o r e e m 9. *Rühma iga kaks kompositsioonijada on isomorfsed.*

Kasutame teoreemi 9 tõestuseks täieliku induktsiooni printsiipi. Et teist järku rühmad kui algrühmad omavad ühtainsat kompositsioonijada $G \supset E$, siis on teoreem 9 kõigi teist järku rühmade puhul kehtiv. Oletades, et teoreem 9 on kehtiv kõigi rühmade puhul, mille järk on väiksem kui n, näitame, et see teoreem jääb kehtima ka iga n-järku rühma G puhul. Vaatleme selleks G mistahes kahte kompositsioonijada

$$(I) \qquad G \supset G_1 \supset G_2 \supset \ldots \supset G_k = E$$

$$(II) \qquad G \supset H_1 \supset H_2 \supset \ldots \supset H_l = E.$$

Märkides $D = G_1 \cap H_1$, moodustame mingi D kompositsioonijada

$$D \supset D_1 \supset D_2 \supset \ldots \supset D_h = E.$$

Nagu nägime eelmise artikli lõpus, on D nii G_1 kui ka H_1 suhtes maksimaalne normaaljagaja, mistõttu jadad

(III) $$G \supset G_1 \supset D \supset D_1 \supset \ldots \supset D_h = E$$

(IV) $$G \supset H_1 \supset D \supset D_1 \supset \ldots \supset D_h = E$$

kujutavad ka G kompositsioonijadasid. Toetudes isomorfismidele (11) (art. 1) ja pidades silmas, et jadad (III) ja (IV) langevad alamrühmast D alates ühte, võime öelda, et jadad (III) ja (IV) on isomorfsed, märkides seda sümboliga

$$(\text{III}) \longleftrightarrow (\text{IV}).$$

Et rühma G_1 järk on väiksem kui n, siis on induktsiooni oletuse kohaselt G_1 kompositsioonijadad

$$G_1 \supset G_2 \supset \ldots \supset G_k = E \quad \text{ja} \quad G_1 \supset D \supset D_1 \supset \ldots \supset D_h = E$$

ja järelikult ka jadad (I) ja (III) isomorfsed, s. o.

$$(\text{I}) \longleftrightarrow (\text{III}).$$

Samuti on induktsiooni oletuse kohaselt H_1 kompositsioonijadad

$$H_1 \supset H_2 \supset \ldots \supset H_l = E \quad \text{ja} \quad H_1 \supset D \supset D_1 \supset \ldots \supset D_h = E$$

isomorfsed, mistõttu ka

$$(\text{II}) \longleftrightarrow (\text{IV}).$$

Leitud kolmest isomorfismist järeldubki otsitav isomorfism

$$(\text{I}) \longleftrightarrow (\text{II}).$$

Seega on Jordan-Hölderi teoreem tõestatud kõigi lõplike rühmade jaoks. Mis puutub lõpmatutesse rühmadesse, siis ei tarvitse kaugeltki iga lõpmatu rühm üldse omada kompositsioonijada. Nii pole näiteks elemendi a poolt moodustatud lõpmatul tsüklilisel rühmal

$$G_a = \{\ldots, a^{-3}, a^{-2}, a^{-1}, e, a^1, a^2, a^3, \ldots\}$$

kompositsioonijada. Tõepoolest ei ole raske näha, et G_a maksimaalseks normaaljagajaks on elemendi a^2 poolt moodustatud lõpmatu tsükliline rühm

$$G_{a^2} = \{\ldots, a^{-6}, a^{-4}, a^{-2}, e, a^2, a^4, a^6, \ldots\},$$

G_{a^2} maksimaalseks normaaljagajaks omakorda elemendi a^4 poolt moodustatud lõpmatu tsükliline rühm

$$G_{a^4} = \{\ldots, a^{-12}, a^{-8}, a^{-4}, e, a^4, a^8, a^{12}, \ldots\}$$

jne. Seda maksimaalsete normaaljagajate eraldamise protsessi võib siin piiramata jätkata, ilma et jõuaksime ühikrühmani E.

Küsimus Jordan-Hölderi teoreemi kohaldamisest lõpmatutele rühmadele, millel ei ole kompositsioonijadasid, on lahendatud nõukogude matemaatiku Kuroš'i poolt 1935. a.[1].

Jordan-Hölderi teoreemist järeldub eriti, et rühma G igale kompositsioonijadale

$$G \supset G_1 \supset G_2 \supset \ldots \supset G_k = E$$

vastav indeksite jada

$$(G_1, G), (G_2, G_1), \ldots, (G_k, G_{k-1})$$

koosneb ühtedest ja samadest arvudest, mis võivad erineda vaid järjekorra poolest. Nii koosnevad eelmises artiklis vaadeldud 12-ndat järku tsüklilise rühma kompositsioonijadade puhul vastavad indeksite jadad arvudest 3, 2, 2 ja 2, 2, 3. Nimetatud tulemuseni jõudis esmakordselt Jordan 1870. a. Seevastu Jordan-Hölderi teoreemi eespool toodud üldises sõnastuses tõestas Hölder 1889. a.

3. Lahenduvad rühmad. Olgu

$$G \supset G_1 \supset G_2 \supset \ldots \supset G_k = E$$

rühma G mingi kompositsioonijada. Algebras pakuvad erilist huvi niisugused rühmad, kus nn. kompositsiooni-indeksid

$$(G_1, G), (G_2, G_1), \ldots, (G_k, G_{k-1})$$

[1] Курош, Теория групп.

on kõik algarvud. Rühma, mille kompositsiooni-indeksid on kõik algarvud, nimetatakse Jordani järgi lahenduvaks rühmaks[1].

Vaatleme lähemalt lahenduva rühma G kompositsioonifaktoreid

$$G/G_1, \quad G_1/G_2, \quad \ldots, \quad G_{k-1}/G_k.$$

Olgu $\bar{a}$ mingi ühikelemendist $\bar{e}$ erinev element faktorrühmas G_{i-1}/G_i. Elemendi $\bar{a}$ poolt moodustatud tsüklilise rühma järk m peab siis Lagrange'i teoreemi järgi kujutama faktorrühma G_{i-1}/G_i järgu p jagajat, nii et kas $m = 1$ või $m = p$. Kui oleks $m = 1$, siis $\bar{a} = \bar{e}$, vastupidi eeldusele. Järelikult peab olema $m = p$, mistõttu p-järku rühm G_{i-1}/G_i peab omama p-järku tsüklilist alamrühma $\{\bar{e}, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{p-1}\}$. Seega

$$G_{i-1}/G_i = \{\bar{e}, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{p-1}\},$$

s. o. *lahenduva rühma kompositsioonifaktorid on algarvulist järku tsüklilised rühmad.*

Niisiis on lahenduva rühma kompositsioonifaktorid Abeli rühmad. Näitame ümberpöördult, et iga rühm G, mille kompositsioonifaktorid on Abeli rühmad, on lahenduv. Vaatleme selle väite tõestuseks jälle G kompositsioonifaktori G_{i-1}/G_i mingi elemendi $\bar{a} \neq \bar{e}$ poolt moodustatud tsüklilist rühma

$$\{\bar{e}, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{m-1}\}.$$

Et Abeli rühmas on iga alamrühm ühtlasi normaaljagaja, siis ei või G_{i-1}/G_i kui algrühm omada ühtki pärisalamrühma peale ühikrühma, mistõttu

$$G_{i-1}/G_i = \{\bar{e}, \bar{a}, \bar{a}^2 \ldots, \bar{a}^{m-1}\},$$

ja seega $m = (G_i, G_{i-1})$. Siinjuures peab m olema algarv, sest kui oleks

$$m = pq, \quad 1 < p < m,$$

[1] Lahenduvat rühma nimetatakse Weber'i järgi vahel ka metatsüklilliseks rühmaks.

siis omaks G_{i-1}/G_i p-järku normaaljagajat

$$\{\overline{e},\ \overline{a}^q,\ \overline{a}^{2q},\ \ldots,\ \overline{a}^{(p-1)q}\}$$

ega saaks olla algrühm. Niisiis kujutab $m = (G_i,\ G_{i-1})$ algarvu, mis ütlebki, et G on lahenduv rühm.

Tähendab, *rühm on lahenduv siis ja ainult siis, kui kõik selle rühma kompositsioonifaktorid on Abeli rühmad.* Siit järeldub otsekohe, et iga Abeli rühm on lahenduv, sest Abeli rühma puhul on faktorrühmad G_{i-1}/G_i ka Abeli rühmad. Tõepoolest, kui G_ia ja G_ib tähendavad kõrvalklasse faktorrühmas G_{i-1}/G_i, siis

$$G_ia \cdot G_ib = G_iab\ ,\quad G_ib \cdot G_ia = G_iba\ ,$$

millest juhul $ab = ba$ saamegi

$$G_ia \cdot G_ib = G_ib \cdot G_ia\ .$$

Et iga tsükliline rühm kujutab Abeli rühma, siis on eriti kõik tsüklilised rühmad lahenduvad. Tutvume veel ühe lahenduvate rühmade klassiga, mida vajame edaspidi.

T e o r e e m 10. *Iga rühm, mille järk avaldub kujul p^n, kus p tähendab mingit algarvu ja n naturaalarvu, on lahenduv.*

Näitame kõigepealt, et iga algrühm G, mille järk on p^n, kujutab Abeli rühma ja on seega lahenduv. Oletades, vastupidi, et G ei ole Abeli rühm, vaatleme neid G elemente a, mis on kommuteeruvad iga elemendiga x, s. o. mille puhul

$$ax = xa\ ,$$

kui $x \in G$. Ei ole raske näha, et kõigi niisuguste elementide hulk Z, mis kannab rühma G t s e n t r i nime, kujutab alamrühma. Tõepoolest:

1⁰ kui $a \in Z$ ja $b \in Z$, siis

$$ax = xa\ ,\quad bx = xb\ .$$

Siin esimesest võrdusest leiame $a = xax^{-1}$ ja tulemust teise võrdusega paremalt korrutades:

$$abx = xax^{-1}xb = xab\ ,$$

millest nähtub, et $ab \in Z$;

2^0 kui $a \in Z$, siis $ax = xa$ ehk $a = xax^{-1}$. Seega $a^{-1} = xa^{-1}x^{-1}$, nii et

$$a^{-1}x = xa^{-1},$$

mis ütleb, et $a^{-1} \in Z$.

Niisiis on Z rühma G alamrühm ja nimelt normaaljagaja, sest iga Z elemendi a puhul on $ax = xa$. Kui nüüd G ei ole Abeli rühm, siis peab Z olema pärisnormaaljagaja ja nimelt $Z = E$, sest G on eelduse kohaselt algrühm. Lahutame rühma G kaaselementide klassideks. Olgu nende klasside arv s ja kaaselementide arvud klassides vastavalt

$$k_1, \; k_2, \; \ldots, \; k_s,$$

nii et

$$k_1 + k_2 + \ldots + k_s = p^n.$$

Et kaaselementide arvud k_i on rühma G järgu p^n jagajateks (§ 20, art. 3), siis kujutab iga k_i kas arvu 1 või p naturaalarvulist astet. Vaatleme kõigepealt ühe-elemendilisi klasse. Et klass $\{x^{-1}ax\}$ oleks ühe-elemendiline, selleks peab olema $x^{-1}ax = a$ ehk $ax = xa$ iga $x \in G$ puhul, s. o. a peab kuuluma rühma G tsentrisse Z. Kuid $Z = E$, mistõttu esineb vaid üks ühe-elemendiline klass $\{e\}$. Seega omab ülemine võrdus kuju

$$1 + p^{n_2} + p^{n_3} + \ldots + p^{n_s} = p^n,$$

kus $n_2, \; n_3, \; \ldots, \; n_s$ tähendavad naturaalarve. Siin võrduse parem pool jagub p-ga, vasak pool aga mitte, missugune vastuolu on tingitud oletusest, et G ei ole Abeli rühm. Seega iga algrühm, mille järk on p^n, peab kujutama Abeli rühma.

Olgu nüüd G mistahes rühm, mille järk on p^n. Siis on iga G kompositsioonifaktor G_{i-1}/G_i algrühm, mille järk kui G järgu jagaja kujutab ka p naturaalarvulist astet. Eelnenu põhjal peab siis iga G_{i-1}/G_i olema Abeli rühm, mis ütlebki, et G on lahenduv.

Olles andnud üldise rühmateooria alused, peatume järgnevas artiklis lühidalt kaasaegse rühmateooria arengul, eriti aga nõukogude matemaatikute juhtival osal selles arengus.

4. Nõukogude matemaatikute osa kaasaegse rühmateooria arengus. Rühmateoreetiliste uurimiste algus Nõukogude Liidus on seotud akadeemik Schmidt'i nimega, kes oma 1916. a. ilmunud monograafias „Абстрактная теория групп" avaldas esmakordselt rühmateooria alused niisugusel kujul, kus ei olnud eeldatud rühma lõplikkust. Kuid nõukogude matemaatikute süstemaatiline, võiks öelda koguni massiline töö rühmateooria küsimuste alal algas alles 1930. a., kui Schmidti poolt organiseeriti Moskvas rühmateooria seminar. See seminar, millest võtsid algul osa peamiselt Moskva riikliku ülikooli noored algebraistid, muutus kiiresti ulatusliku uurimise tsentrumiks rühmateooria alal, tsentrumiks, millega olid seotud peaaegu kõigi nõukogude matemaatikute rühmateoreetilised uurimused. Tänu sellele äärmiselt süstematiseeritud uurimistööle võis Kuroš juba 1944. a. avaldada suurepärase monograafia „Теория групп", milles ilmekalt peegeldub nõukogude matemaatikute eesrindlik osa kaasaegse rühmateooria arengus ja mis kuni tänapäevani on jäänud teenäitajaks kõigile rühmateooria alal töötajaile kogu maailmas.

Kaasaegse rühmateooria eesmärgiks on rühmade klassifitseerimine, katalogiseerimine. Selle klassifitseerimise teostamiseks on kõigepealt vajalik leida vahendeid, mis lubaksid taandada enam komplitseeritud struktuuriga rühmade uurimist lihtsamate rühmade uurimisele. Niisugusteks vahenditeks on nn. otsekorrutis ja vabakorrutis. Nimetame rühma G tema (ühikrühmast erinevate) alamrühmade H_α otsekorrutiseks ja kirjutame

$$G = \prod H_\alpha,$$

kui on täidetud järgmised kaks tingimust:

1^0 erinevatesse alamrühmadesse H_i, H_k kuuluvate elementide h_i, h_k korrutis on kommutatiivne, s. o. $h_i h_k = h_k h_i$;

2^0 G iga element a avaldub üheselt kujul

$$a = h_{\alpha_1} h_{\alpha_2} \dots h_{\alpha_n},$$

kus tegurid h_{α_i} kuuluvad kõik erinevatesse alamrühmadesse H_{α_i}.

Nii võib näiteks ratsionaalarvude multiplikatiivset rühma lahutada positiivsete ratsionaalarvude multiplikatiivse rühma ja teist järku tsüklilise rühma $\{1, -1\}$ otsekorrutiseks. Abeli rühmade puhul, kus rühmaoperatsiooniks on liitmine, kõneldakse otsekorrutise asemel vastavalt otsesummast (§ 15, art. 2).

Niisugust rühma, mis ei lagune oma alamrühmade otsekorrutiseks, nimetatakse mittelahutuvaks rühmaks. Mittelahutuva rühma näitena võiks nimetada ratsionaalarvude aditiivset rühma. Seoses otsekorrutisega tekib järgmine küsimus: kui mingi rühm G laguneb mittelahutuvate alamrühmade otsekorrutiseks, siis kas ühel või enamal viisil. Täpsemalt: kas kaks rühma G lahutust mittelahutuvate alamrühmade otsekorrutiseks on isomorfsed, s. o. kas nende lahutuste alamrühmi võib seada üksühesesse vastavusse, nii et vastavad alamrühmad oleksid isomorfsed? 1911. a. tõestas Remak, et kui mingi lõplik rühm laguneb kahel viisil mittelahutuvate alamrühmade otsekorrutiseks, siis on need lahutused isomorfsed. Otsustava sammu Remaki tulemuse ülekandmiseks lõpmatutele rühmadele tegi akadeemik Schmidt, üldistades 1928. a. Remaki teoreemi kõigi kompositsioonijadasid omavate lõpmatute rühmade jaoks. Schmidt'i tulemus, mis on kirjanduses tuntud Remak-Schmidti teoreemi nime all, leidis huvitavaid rakendusi ringiteoorias, üldistati 1932. a. Kuroši poolt ja 1938—1939. a. Kořínek'i ja Golovin'i poolt, kes näitasid, et Remak-Schmidti teoreemi kehtivuseks tarvitseb vaid nõuda, et rühma tsentri iga kahanev alamrühmade jada oleks lõplik. Viimane töö selles uurimuste sarjas kuulub Kurošile, kes 1945. a. veelkordselt üldistas Remak-Schmidti ja Kořínek-Golovini tulemusi.

Tuleme tagasi rühmateooria eesmärgi — rühmade klassifitseerimise küsimuse juurde. Klassikaliseks näiteks on siin nn. lõpliku arvu moodustajatega Abeli rühmad, s. o. niisugused Abeli rühmad, kus iga element avaldub lõpliku arvu kindlate elementide, nn. moodustajate kordsete summana. On arusaadav, et lõpliku arvu moodustajatega Abeli rühmade hulka kuuluvad kõik lõplikud Abeli rühmad. Klassifitseerimise aluse moodustab siin tuntud klassikaline teoreem,

mille järgi iga lõpliku arvu moodustajatega Abeli rühm laguneb lõpliku arvu tsükliliste alamrühmade otsesummaks. Siinjuures võivad mittelahutuvate tsükliliste alamrühmadena esineda vaid lõpmatud tsüklilised rühmad ja niisugused lõplikud tsüklilised rühmad, mille elementide järgud kujutavad ühe ja sama algarvu astmeid. Selliseid rühmi, mille elementide järgud kujutavad ühe ja sama algarvu astmeid, nimetatakse *primaarseteks* rühmadeks. Seega saame kõik lõpliku arvu moodustajatega Abeli rühmad, kui kirjutame välja kõik võimalikud tsükliliste rühmade süsteemid, s. o. lõplike primaarsete ja lõpmatute rühmade süsteemid, ja moodustame iga süsteemi rühmade otsesummad. Siinjuures garanteerib Remak-Schmidti teoreem, et kõik sel viisil konstrueeritud rühmad tulevad erinevad. Niisugune klassifitseerimine on osutunud sedavõrd otstarbekaks, et praegu vaevalt saab näidata mingit lõpliku arvu moodustajatega Abeli rühma puudutavat probleemi, mille lahendamine pakuks muid raskusi peale tehniliste. Näitena olgu nimetatud maatriksi Jordani normaalkuju olemasolu küsimus (§ 16, art. 2—3).

Peatume nüüd mistahes primaarsete Abeli rühmade juures. 1923. a. näitas Prüfer, et iga loenduv primaarne rühm laguneb tsükliliste alamrühmade otsesummaks, kui aga selles rühmas ei leidu *lõpmata kõrgeid elemente*, s. o. niisuguseid elemente $a \neq 0$, kus võrrand

$$p^k x = a$$

on lahenduv iga k puhul (§ 16, art. 3). 1939. a. Kuroš, uurides mitteloenduvaid primaarseid Abeli rühmi, konstrueeris näite niisugusest mitteloenduvast primaarsest rühmast ilma lõpmata kõrgete elementideta, mis ei lagune tsükliliste alamrühmade otsesummaks. Kuroši uurimised andsid omakorda tõuke ulatuslikele sügavale minevatele uurimustele Kulikovi poolt. Muuhulgas andis Kulikov 1945. a. Prüferi teoreemile tähelepandava üldistuse, mille järgi primaarne Abeli rühm G laguneb siis ja ainult siis tsükliliste alamrühmade otsesummaks, kui G kuju-

tab niisuguse kasvava jada alamrühmade summat, kus igas alamrühmas on elementide kõrgused tõkestatud.

Mistahes Abeli rühmade lagunemist alamrühmade otsesummaks uuris Ljapin, andes 1940. a. tarviliku ja piisava tingimuse mistahes Abeli rühma lagunemiseks tsükliliste ja teatavate mittetsükliliste alamrühmade otsesummaks.

Teiseks vahendiks, mis lubab mõningail juhtudel enam komplitseeritud struktuuriga rühmade uurimist taandada lihtsamate rühmade uurimisele, on, nagu tähendatud, vabakorrutis. Nimetame rühma G tema (ühikrühmast erinevate) alamrühmade H_α vabakorrutiseks ja kirjutame

$$G = \prod * H_\alpha,$$

kui G iga element a avaldub üheselt kujul

$$a = h_{\alpha_1} h_{\alpha_2} \dots h_{\alpha_n},$$

kus iga kaks kõrvuti asetsevat tegurit $h_{\alpha_{i-1}}$, h_{α_i} kuuluvad erinevatesse alamrühmadesse. Nii saab näiteks näidata, et nn. modulaarne rühm, s. o. rühm, mille moodustavad komplekstasandi murdlineaarsed teisendused

$$Z' = \frac{az+b}{cz+d}, \quad |ad-bc| = 1 \quad (a, b, c, d \text{ täisarvud}),$$

laguneb teisenduste $z' = -\frac{1}{z}$ ja $z' = \frac{z-1}{z}$ poolt moodustatud teist ja kolmandat järku tsükliliste rühmade vabakorrutiseks.

Otsekorrutise mõiste on ammugi kujunenud klassikaliseks, vabakorrutise mõiste anti aga Artini poolt alles 1926. a. Vabakorrutise süstemaatiline uurimine algas Kuroši töödega 1933. a., mis on seletatav sellega, et vabakorrutise mõiste ei puuduta lõplikke rühmi. Olgu nimelt G lahutatud alamrühmade vabakorrutiseks

$$G = \prod * H_\alpha.$$

Vaatleme kahte G elementi a_1 ja a_2, mis kuuluvad erinevatesse

alamrühmadesse H_1 ja H_2. Vabakorrutise mõiste kohaselt kujutavad korrutised

$$a_1a_2,\quad a_1a_2a_1a_2,\quad a_1a_2a_1a_2a_1a_2,\ \ldots,\ (a_1a_2)^n,\ \ldots$$

erinevaid G elemente, mistõttu G peab olema lõpmatu rühm. Tähendab, ainult lõpmatud rühmad võivad laguneda oma alamrühmade vabakorrutiseks. Vastandina otsekorrutisele kehtib vabakorrutise puhul Remak-Schmidti teoreemile vastav teoreem iga rühma puhul, mis laguneb mittelahutuvate alamrühmade vabakorrutiseks, nagu seda tõestas Kuroš 1936. a.

Väga tähelepandavaid tulemusi vabakorrutise uurimisel saavutas Gruško 1940. a. mistahes lõpliku arvu moodustajatega rühmade alal. Eriti järeldub Gruško uurimustest, et iga lõpliku arvu moodustajatega rühm laguneb lõpliku arvu mittelahutuvate alamrühmade vabakorrutiseks, kusjuures selle rühma moodustajate minimaalarv on võrdne üksikute alamrühmade moodustajate minimaalarvude summaga.

Peab tähendama, et otsekorrutise ja vabakorrutise mõisteist kaugeltki ei piisa rühmade klassifitseerimise küsimuse rahuldavaks lahendamiseks. Nii leidub näiteks lõplikke rühmi, mille lahutused mittelahutuvate alamrühmade otsekorrutiseks sisaldavad küllaltki komplitseeritud struktuuriga rühmi. Et, teiselt poolt, lõplikud rühmad pole lahutatavad alamrühmade vabakorrutiseks, siis pole tänapäevani õnnestunud isegi lõplike rühmade täielik klassifitseerimine, kuigi lõplikke rühmi on vaid loenduv hulk. Pole klassifitseeritud täielikult koguni lõplikud lahenduvad ega ka lõplikud primaarsed rühmad. Seepärast on seatud nõukogude rühmateoreetikute ette järjekordne ülesanne: anda üldine korrutise mõiste rühmateoorias, mõiste, millel oleksid analoogilised omadused otsekorrutise ja vabakorrutisega, ja rakendada siis seda korrutist ühe või teise rühmade klassi uurimisel.

§ 23. Substitutsioonirühmad.

1. Tsüklid. Rakendame nüüd üldise rühmateooria tulemusi substitutsioonirühmadele. Seame kõigepealt endale ülesandeks

anda n-astme substitutsioonile

$$s = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

arvutusteks kohasem kuju. Tähendagu $a_1, a_2, \dots, a_k, \dots, a_n$ numbreid $1, 2, \dots, n$ mingis kindlas järjestuses. Märgime sümboliga $(a_1 a_2 \dots a_k)$ niisuguse n-astme substitutsiooni, mis teisendab numbri a_1 a_2-ks, a_2 a_3-ks jne., a_{k-1} a_k-ks ja lõppeks a_k a_1-ks, jättes ülejäänud numbrid $a_{k+1}, \dots, a_n$ muutumatuks, s. o.

$$(a_1 a_2 \dots a_k) = \begin{pmatrix} a_1 & a_2 & \dots & a_{k-1} & a_k & a_{k+1} & \dots & a_n \\ a_2 & a_3 & \dots & a_k & a_1 & a_{k+1} & \dots & a_n \end{pmatrix}.$$

Iga niisugust substitutsiooni $(a_1 a_2 \dots a_k)$ nimetatakse *k-liikmeliseks tsükliks* ehk lihtsalt tsükliks. Tsükli märkimisel on oluline vaid tsükli numbrite ringjärjekord, mitte aga see number, millega algab tsükkel. Nii on näiteks $(3\ 4\ 2\ 1) = (2\ 1\ 3\ 4)$.

Näitame, et iga substitutsiooni

$$s = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

saab lahutada teatavate tsüklite korrutiseks, nii et iga number $1, 2, \dots, n$ esineb parajasti ühes tsüklis. Vaatleme s-i ülemises reas näiteks numbrit 1 — see teisendub numbriks a_1. Vaatleme s-i ülemises reas numbrit a_1 — see teisendub numbriks a_{a_1}. Vaatleme s-i ülemises reas numbrit a_{a_1} jne., kuni jõuame niisuguse numbrini, mis teisendub lähtenumbriks 1. Sel teel saame tsükli

$$\begin{pmatrix} 1 & a_1 & a_{a_1} \dots \\ a_1 & a_{a_1} & \dots\ 1 \end{pmatrix} = (1\ a_1\ a_{a_1} \dots).$$

Vaatleme nüüd s-i ülemises reas mingit numbrit β, mis ei esine eraldatud tsüklis; β teisendub numbriks a_β. Vaatleme s-i ülemises reas numbrit a_β — see teisendub numbriks a_{a_β}. Vaatleme

s-i ülemises reas numbrit α_{α_β} jne., kuni jõuame niisuguse numbrini, mis teisendub lähtenumbriks β. Sel teel saame tsükli

$$\begin{pmatrix} \beta & \alpha_\beta & \alpha_{\alpha_\beta} \dots \\ \alpha_\beta & \alpha_{\alpha_\beta} & \dots \ \beta \end{pmatrix} = (\beta \ \alpha_\beta \ \alpha_{\alpha_\beta} \dots).$$

Seda tsüklite eraldamise protsessi jätkame seni, kuni oleme eraldatud tsüklitega ammendanud kõik numbrid $1, 2, \dots, n$. Silmas pidades, et substitutsioonide korrutamine tähendab nende substitutsioonide järjest rakendamist, võime kirjutada

$$s = (1 \ \alpha_1 \ \alpha_{\alpha_1} \dots)(\beta \ \alpha_\beta \alpha_{\alpha_\beta} \dots) \dots,$$

kusjuures korrutises ei ole tsüklite järjekord oluline, sest iga number $1, 2, \dots, n$ esineb vaid ühesainsas tsüklis. Seega saab iga substitutsiooni lahutada üksteisest sõltumatute tsüklite korrutiseks, kusjuures tsüklid on kuni järjekorrani üheselt määratud.

N ä i d e 3. Lahutada substitutsioon

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

sõltumatute tsüklite korrutiseks.

Siin 1 teisendub 5-ks, 5 teisendub 2-ks ja 2 teisendub 1-ks, millega sulgub esimene tsükkel (1 5 2). Alates teist tsüklit näiteks 3-ga, näeme, et 3 teisendub 8-ks ja 8 omakorda 3-ks, millega sulgub teine tsükkel (3 8). Alates kolmandat tsüklit näiteks 4-ga, näeme, et 4 teisendub 9-ks, 9 teisendub 6-ks ja 6 teisendub 4-ks, millega sulgub kolmas tsükkel (4 9 6). Ülejäänud number 7 moodustab omaette üheliikmelise tsükli (7). Seega

$$s = (1 \ 5 \ 2)(3 \ 8)(4 \ 9 \ 6)(7).$$

Et üheliikmelised tsüklid tähistavad vaid muutumatuks jäävaid numbreid, siis jäetakse nad tavaliselt korrutises märkimata, mistõttu võime kirjutada

$$s = (1 \ 5 \ 2)(3 \ 8)(4 \ 9 \ 6).$$

Olgu antud peale substitutsiooni s veel mingi substitutsi-

oon t. Küsime, kuidas avaldub s-i k a a s s u b s t i t u t s i o o n $\bar{s} = t^{-1}st$ (§ 20, art. 3), kui s on antud tsüklite korrutisena. Siinjuures piisab, kui oskame arvutada ühe tsükli kaassubstitutsiooni, sest korrutise kaassubstitutsioon on võrdne tegurite kaassubstitutsioonide korrutisega. Tõepoolest, kui $\bar{s}_1 = t^{-1}s_1t$ ja $\bar{s}_2 = t^{-1}s_2t$, siis

$$\bar{s}_1\bar{s}_2 = t^{-1}s_1s_2t = t^{-1}s_1t \cdot t^{-1}s_2t = \bar{s}_1\bar{s}_2 .$$

Seepärast olgu $s = (a_1a_2 \ldots a_k)$. Kui

$$t = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix},$$

siis

$$\bar{s} = \begin{pmatrix} b_1 & b_2 & \ldots & b_n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \ldots & a_{k-1} & a_k & a_{k+1} & \ldots & a_n \\ a_2 & a_3 & \ldots & a_k & a_1 & a_{k+1} & \ldots & a_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix} =$$

$$= \begin{pmatrix} b_1 & b_2 & \ldots & b_{k-1} & b_k & b_{k+1} & \ldots & b_n \\ b_2 & b_3 & \ldots & b_k & b_1 & b_{k+1} & \ldots & b_n \end{pmatrix} = (b_1 \; b_2 \; \ldots \; b_k).$$

Tähendab, *tsükli s kaaselemendi $\bar{s} = t^{-1}st$ saamiseks tuleb s-i igale liikmele rakendada substitutsiooni t.*

Näiteks kui $s = (1\ 5\ 2)(3\ 8)(4\ 9\ 6)$, $t = (2\ 4\ 7\ 1\ 5)(9\ 6\ 8)$, siis

$$\bar{s} = t^{-1}st = (5\ 2\ 4)(3\ 9)(7\ 6\ 8),$$

sest 1 teisendub t mõjul numbriks 5, 5 numbriks 2, 2 numbriks 4 ja seega tsükkel (1 5 2) tsükliks (5 2 4) jne.

Tsüklite hulgas etendavad erilist osa kaheliikmelised tsüklid (a_1a_2), mis kannavad transpositsioonide nime ja millega tutvusime juba determinantide teoorias (I, § 12, art. 1). Ei ole raske näha, et iga tsüklit saab lahutada transpositsioonide korrutiseks. Nimelt võib substitutsioonide korrutamise mõistele toetudes kirjutada

$$(a_1a_2 \ldots a_k) = (a_1a_2)(a_1a_3) \ldots (a_1a_k).$$

Siinjuures tuleb silmas pidada, et viimases korrutises on olu-

line transpositsioonide järjekord, sest need transpositsioonid sisaldavad kõik ühist numbrit a_1. Et iga substitutsioon laguneb tsüklite korrutiseks, siis saab iga substitutsiooni lahutada lõppude-lõpuks transpositsioonide korrutiseks. Nii on näites 3 vaadeldud substitutsiooni s korral

$$s = (1\ 5\ 2)(3\ 8)(4\ 9\ 6) = (1\ 5)(1\ 2)(3\ 8)(4\ 9)(4\ 6).$$

Kuid substitutsioonide lahutamine transpositsioonide korrutiseks pole üheselt teostatav, sest näiteks viimase substitutsiooni s puhul võime ka kirjutada

$$s = (1\ 9)(4\ 6)(5\ 9)(1\ 6)(2\ 9)(1\ 9)(3\ 8).$$

Ometi saab näidata, et kuidas me ka lahutaksime antud substitutsiooni transpositsioonide korrutiseks, transpositsioonide arv korrutises võib muutuda vaid paarisarvu võrra.

Vaatleme viimase väite selgituseks substitutsiooni kujul

$$s = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix},$$

kus ülemise rea numbrid kulgevad loomulikus järjekorras. Nimetame substitutsiooni s p a a r i s - või p a a r i t u k s s u b s t i t u t s i o o n i k s selle järgi, kas alumine rida $a_1 a_2 \dots a_n$ kujutab paaris- või paaritut permutatsiooni. Kui nüüd substitutsioon s on lahutatud transpositsioonide korrutiseks, mis sisaldab σ transpositsiooni, siis, rakendades neid transpositsioone järjest loomulikule järjestusele $1\ 2 \dots n$, saame permutatsiooni $a_1 a_2 \dots a_n$. Selle järgi, kas permutatsioon $a_1 a_2 \dots a_n$ on paaris või paaritu, kujutab σ paaris- või paaritut arvu (I, § 12, art. 1). Seega laguneb paarissubstitutsioon alati paarisarvu ja paaritu substitutsioon paaritu arvu transpositsioonide korrutiseks.

Et paaris- ja paarituid permutatsioone on ühepalju, siis on ka paaris- ja paarituid substitutsioone ühepalju ja nimelt kumbigi $\frac{n!}{2}$ tükki.

2. **Vahelduv rühm.** Vaatleme n-astme substitutsioonide hulgas, s. o. sümmeetrilises rühmas S_n, eriti paarissubstitutsioone ja märgime kõigi paarissubstitutsioonide hulga tähega A_n. Näi-

tame, et A_n kujutab S_n alamrühma. Et S_n on lõplik rühm, siis tarvitseb vaid näidata, et A_n on kinnine korrutamise suhtes (§ 18, art. 2). Olgu s_1 ja s_2 mingid paarissubstitutsioonid ja lagunegu nad vastavalt $2\sigma_1$ ja $2\sigma_2$ transpositsiooni korrutiseks. Siis laguneb korrutis $s_1 s_2$ $2\sigma_1 + 2\sigma_2 = 2(\sigma_1 + \sigma_2)$ transpositsiooni korrutiseks ja on seega ka paarissubstitutsioon, mis ütlebki, et A_n on kinnine korrutamise suhtes ja kujutab seega rühma. Rühm A_n kannab n-astme v a h e l d u v a ehk a l t e r n e e r u v a r ü h m a nime. Vahelduva rühma A_n järk on $\frac{n!}{2}$. Lahutades sümmeetrilise rühma S_n kõrvalklassideks A_n järgi, saame $(A_n, S_n) = \frac{n!}{\frac{n!}{2}} = 2$ tõttu

$$S_n = A_n + A_n t, \quad S_n = A_n + t A_n,$$

kus t tähendab mistahes paaritut substitutsiooni. Viimast kahte võrdust võrreldes näeme, et

$$A_n t = t A_n,$$

mis ütleb, et A_n on normaaljagaja. Veel enam, A_n on S_n suhtes maksimaalne normaaljagaja, sest faktorrühm S_n/A_n, omades järku 2, kujutab algrühma.

Tekib küsimus, missuguseid normaaljagajaid omab vahelduv rühm A_n. Selle küsimuse selgituseks tõestame algul, et vahelduva rühma ükski pärisnormaaljagaja ei või sisaldada kolmeliikmelisi tsükleid.

Oletame, et A_n normaaljagaja H sisaldab kolmeliikmelist tsüklit $s = (a\ b\ c)$ ja näitame kõigepealt, et H peab siis sisaldama i g a kolmeliikmelist tsüklit $(p\ q\ r)$. Vaatleme selleks substitutsiooni $t = (ap)(bq)$, mis kui paarissubstitutsioon kuulub vahelduvasse rühma A_n, ja moodustame tema abil s kaassubstitutsiooni

$$\bar{s} = t^{-1} s t = t^{-1}(abc)t.$$

Tsükli kaassubstitutsiooni leidmise eeskirja kohaselt saame

$$\bar{s} = (pqc),$$

kusjuures $\bar{s}$ kui s kaaselement kuulub ka normaaljagajasse H (§ 20, art. 4). Et siin p ja q tähendavad mistahes numbreid, siis, asendades p r-ga ja q p-ga, jõuame tsüklini

$$s' = (rpc),$$

mis peab samuti kuuluma normaaljagajasse H. Seega peab H sisaldama ka korrutist

$$\bar{s}s' = (pqc)(rpc) = (pqr),$$

s. o. mistahes kolmeliikmelist tsüklit (pqr).

Veendume nüüd, et vahelduva rühma A_n iga substitutsiooni, s. o. mistahes paarissubstitutsiooni, võib avaldada kolmeliikmeliste tsüklite korrutisena. Kuna iga paarissubstitutsiooni saab lahutada paarisarvu transpositsioonide korrutiseks, siis on küllaldane näidata, et iga kahe transpositsiooni korrutist võib avaldada kolmeliikmeliste tsüklite korrutisena. Kahe transpositsiooni puhul esineb kaks juhtu: emb-kumb, kas need transpositsioonid omavad ühist numbrit või mitte. Esimesel juhul saame lihtsalt

$$(ab)(ac) = (abc),$$

teisel juhul aga pärast identse substitutsiooniga $(ac)(ca)$ täiendamist

$$(ab)(cd) = (ab)(ac) \cdot (ca)(cd) = (abc)(cad).$$

Seega avaldub A_n iga substitutsioon tõepoolest kolmeliikmeliste tsüklite korrutisena, mistõttu A_n normaaljagaja H, sisaldades kõiki kolmeliikmelisi tsükleid, sisaldab A_n iga substitutsiooni, s. o. $H = A_n$. Seepärast kui H on A_n pärisnormaaljagaja, siis H ei või sisaldada ühtki kolmeliikmelist tsüklit. Toetudes sellele tõsiasjale, võime anda vastuse eespool püstitatud küsimusele vahelduva rühma normaaljagajate kohta. Nimelt osutub, et juhul $n > 4$ pole vahelduval rühmal A_n ühtki pärisnormaaljagajat peale ühikrühma ehk, teiste sõnadega, on kehtiv järgmine teoreem:

Teoreem 11. *Vahelduv rühm A_n on juhul $n > 4$ algrühm.*

Teoreemi 11 tõestuseks oletame, vastupidi, et A_n omab peale ühikrühma veel pärisnormaaljagajat H. Vaatleme H kõiki substitutsioone, jättes välja vaid identse substitutsiooni; olgu s vaadeldavate substitutsioonide hulgas üks niisugune substitutsioon, mis muudab minimaalse arvu numbreid $1, 2, \ldots, n$, nii et ei leiduks ühtki H substitutsiooni peale identse substitutsiooni, mis muudaks vähem numbreid kui s. Lahutades substitutsiooni s üksteisest sõltumatute tsüklite korrutiseks ja pidades silmas, et s ei või eelnenu põhjal taanduda üheks kolmeliikmeliseks tsükliks ja — kui paarissubstitutsioon — ka mitte üheks kaheliikmeliseks tsükliks, saame s-i suhtes neli võimalust:

1^0 s sisaldab vähemalt ühte kaheliikmelist ja ühte kolmeliikmelist tsüklit:

$$s = (ab)(cde)\ldots;$$

2^0 s sisaldab vähemalt kahte kaheliikmelist tsüklit:

$$s = (ab)(cd)\ldots;$$

3^0 s sisaldab vähemalt kahte kolmeliikmelist tsüklit:

$$s = (abc)(def)\ldots;$$

4^0 s sisaldab vähemalt ühte enam kui kolmeliikmelist tsüklit:

$$s = (abcd\ldots)\ldots.$$

Näitame, et kõik loeteldud võimalused on vastuolus substitutsiooni s valikuga.

1^0 Arvutades substitutsiooni s^2, leiame

$$s^2 = (ab)(cde)(ab)(cde)\ldots = (ced)\ldots,$$

millest nähtub, et s^2 muudab vähem numbreid kui s, vastuolus s-i valikuga.

2^0 Vaatleme A_n substitutsiooni $t = (abe) = (ab)(ae)$, kus e tähendab mingit numbrit, mis erineb numbreist a, b, c, d, ja moodustame t abil s-i kaassubstitutsiooni

$$\bar{s} = t^{-1}st = t^{-1}(ab)(cd)\ldots t = (be)(cd)\ldots.$$

Et koos s-ga ka kaaselement $\bar{s}$ kuulub normaaljagajasse H (§ 20, art. 4), siis kuulub sinna ka korrutis

$$s\bar{s} = (ab)(cd) \ldots (be)(cd) \ldots = (ae \ldots) \ldots,$$

mis muudab aga vähem numbreid kui s, vastuolus s-i valikuga.

3⁰ Kasutades jälle A_n substitutsiooni $t = (abe)$, leiame tema abil s-i kaassubstitutsiooni

$$\bar{s} = t^{-1}st = t^{-1}(abc)(def) \ldots t = (bec)(daf) \ldots$$

ja moodustame korrutise

$$s\bar{s} = (abc)(def)(bec)(daf) \ldots = (aedcf) \ldots,$$

mis muudab jälle vähem numbreid kui s, vastuolus s-i mõistega.

4⁰ Vaatleme siin A_n substitutsiooni $t = (abc) = (ab)(ac)$ ja moodustame tema abil s-i kaassubstitutsiooni

$$\bar{s} = t^{-1}st = t^{-1}(abcd \ldots) \ldots t = (bcad \ldots) \ldots .$$

Et koos s-ga ka s^{-1} ja $\bar{s}$ kuuluvad normaaljagajasse H, siis kuulub sinna ka korrutis

$$s^{-1}\bar{s} = (\ldots dcba)(bcad \ldots) \ldots = (bda \ldots) \ldots,$$

mis muudab jälle vähem numbreid kui s, vastuolus s-i valikuga.

Seega oletus, et A_n omab peale ühikrühma veel pärisnormaaljagajat H, sisaldab vastuolu, mistõttu A_n peab $n > 4$ puhul olema algrühm. Siin tingimus $n > 4$ tuleneb sellest, et kasutasime igal juhul 1⁰—4⁰ vähemalt viit erinevat numbrit[1] a, b, c, d, e. Tegelikult polegi rühm A_4 enam algrühm, vaid omab normaaljagajat neljarühma V_4 näol (§ 20, art. 1). Et V_4 on vahelduva rühma A_4 alamrühm, nähtub vahetult V_4 substitutsioonide tsükliteks lahutustest:

$$e, \quad s_a = (1\ 2)(3\ 4), \quad s_b = (1\ 3)(2\ 4), \quad s_c = (1\ 4)(2\ 3),$$

[1] Ka juhul 4⁰ peab s-i koosseisus esinema vähemalt viis erinevat numbrit, sest omaette tsükkel $(abcd) = (ab)(ac)(ad)$ kui paaritu substitutsioon ei saa kuuluda normaaljagajasse H.

millest ilmneb ühtlasi, et V_4 on A_4 (ja ka S_4) normaaljagaja, sest s_a, s_b ja s_c kaaselemendid, koosnedes igaüks kahest sõltumatust transpositsioonist, kuuluvad kõik alamrühma V_4, kuna, nagu kergesti võib veenduda, s_a, s_b ja s_c on ainukesed substitutsioonid vahelduvas rühmas A_4 (ja ka S_4), mis koosnevad kahest sõltumatust transpositsioonist.

Silmas pidades, et A_n on sümmeetrilise rühma S_n maksimaalne normaaljagaja, olles seejuures ise $n > 4$ puhul algrühm, saame S_n kompositsioonijada juhul $n > 4$ kujul

$$S_n \supset A_n \supset E,$$

millele vastavad indeksid on

$$(A_n, S_n) = 2, \quad (E, A_n) = \frac{n!}{2}.$$

Siin teine indeks $\frac{n!}{2} = 3 \cdot 4 \cdot 5 \ldots n$ pole $n > 4$ puhul algarv. Tähendab, *sümmeetriline rühm S_n ei ole juhul $n > 4$ lahenduv.* Nagu edaspidi näeme (§ 29, art. 1), etendab viimane tulemus olulist osa tõsiasjas, et üldine kõrgema kui neljanda astme algebraline võrrand pole radikaalides lahenduv.

Seevastu juhul $n \leqslant 4$ on sümmeetriline rühm S_n lahenduv. Siin omavad nimelt rühmade S_2, S_3 ja S_4 kompositsioonijadad vastavalt kuju

$$S_2 \supset E, \; S_3 \supset A_3 \supset E, \; S_4 \supset A_4 \supset V_4 \supset \{e, (1\,2)(3\,4)\} \supset E,$$

mistõttu S_2, S_3 ja S_4 kompositsiooni-indeksid

$$2; \quad 2, 3; \quad 2, 3, 2, 2$$

on kõik algarvud.

3. Transitiivsus ja imprimitiivsus. Nimetame n-astme substitutsioonirühma G t r a n s i t i i v s e k s, kui selles rühmas leiduvad niisugused substitutsioonid, mis teisendavad numbri 1 vastavalt igaks numbriks $1, 2, \ldots, n$. Nii on näiteks substitutsioonirühm

(12) $\{e, (1\,2)(3\,4), \quad (1\,3)(2\,4), \quad (1\,4)(2\,3)\}$

transitiivne, seevastu

$$\{e,\ (1\ 2),\ (3\ 4),\ (1\ 2)(3\ 4)\} \tag{13}$$

aga mitte.

Näitame, et transitiivses substitutsioonirühmas G leidub alati ka niisugune substitutsioon u, mis teisendab mistahes numbri k mistahes numbriks l. Asjaolu, et u teisendab numbri k numbriks l, märgime edaspidi lühidalt sümboliga

$$ku = l.$$

Rühma G transitiivsuse tõttu leiduvad temas substitutsioonid s ja t, nii et

$$1s = k,\quad 1t = l.$$

Et s teisendab numbri 1 numbriks k, siis teisendab pöördsubstitutsioon s^{-1} numbri k numbriks 1, s. o.

$$ks^{-1} = 1.$$

Moodustades korrutise

$$u = s^{-1}t,$$

ei ole raske näha, et u teisendabki numbri k numbriks l. Tõepoolest:

$$ku = (ks^{-1})t = 1t = l.$$

Märkus. Transitiivsuse mõiste omab mõtet ainult substitutsioonirühmade, mitte aga abstraktsete rühmade puhul. Nimelt võib ühte ja sama abstraktset rühma esitada ükskord transitiivse, teinekord mittetransitiivse substitutsioonirühmana. Nii on näiteks neljarühm ühelt poolt isomorfne transitiivse substitutsioonirühmaga (12), teiselt poolt aga isomorfne ka mittetransitiivse substitutsioonirühmaga (13).

Transitiivset n-astme substitutsioonirühma G nimetatakse imprimitiivseks, kui numbreid $1, 2, \ldots, n$ on võimalik jaotada klassideks $M_1, M_2, \ldots, M_r$, nii et

1^0 iga klass M_i sisaldab vähemalt kaks numbrit;

2^0 erinevatel klassidel pole ühiseid numbreid;

3^0 iga G substitutsioon s teisendab mingi klassi M_i jälle mingiks klassiks M_j.

Niisugused klassid $M_1, M_2, \ldots, M_r$, mis rahuldavad tingimusi 1^0—3^0, kannavad vastavalt imprimitiivsuse klasside nime. G transitiivsuse tõttu peab G-s leiduma alati niisugune substitutsioon, mis teisendab näiteks klassi M_1 mistahes klassiks M_i. Siit nähtub, et kõik imprimitiivsuse klassid peavad sisaldama ühepalju numbreid.

Vaatleme näitena substitutsiooni $s = (1\ 2\ 3\ 4\ 5\ 6)$ poolt moodustatud 6-ndat järku tsüklilist rühma $\{e, s, s^2, s^3, s^4, s^5\}$, kus

$$s^2 = (1\ 3\ 5)(2\ 4\ 6), \quad s^3 = (1\ 4)(2\ 5)(3\ 6),$$
$$s^4 = (1\ 5\ 3)(2\ 6\ 4), \quad s^5 = (1\ 6\ 5\ 4\ 3\ 2).$$

Siin võib jaotada numbrid 1, 2, 3, 4, 5, 6 imprimitiivsuse klassideks järgmiselt:

$$M_1 = \{1, 3, 5\}, \quad M_2 = \{2, 4, 6\},$$

kusjuures ei ole raske näha, et substitutsioonid e, s^2, s^4 ei muuda klasse M_1, M_2, kuna substitutsioonid s, s^3, s^5 teisendavad klassi M_1 klassiks M_2 ja klassi M_2 klassiks M_1. Seega on vaadeldav substitutsioonirühm imprimitiivne.

Teise näitena vaatleme sümmeetrilist rühma S_n ja tõestame, et S_n ei ole imprimitiivne. Oletame selleks vastupidi, et siin on võimalik jaotada numbreid $1, 2, \ldots, n$ imprimitiivsuse klassideks

$$M_1 = \{a_1, a_2, \ldots, a_{m-1}, a_m\}$$
$$M_2 = \{b_1, b_2, \ldots, b_{m-1}, b_m\}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Rakendades klassile M_1 transpositsiooni $(a_m b_1)$, saame hulga

$$M = \{a_1, a_2, \ldots, a_{m-1}, b_1\},$$

mis ei ole imprimitiivsuse klass, vastuolus tingimusega 3^0, sest olles $b_1 \neq a_m$ tõttu M_1-st erinev, omab M siiski M_1-ga ühiseid numbreid.

Tõestame lõppeks veel ühe teoreemi, mida vajame edaspidi, et konstrueerida algebralisi võrrandeid, mis ei ole lahenduvad radikaalides.

Teoreem 12. *Iga transitiivne n-astme substitutsioonirühm, mis sisaldab mingit transpositsiooni, kujutab kas sümmeetrilist rühma S_n või imprimitiivset rühma.*

Sisaldagu transitiivne rühm G transpositsiooni (a_1a_2). Oletame, et G-s on üldse järgmised numbrit a_1 sisaldavad transpositsioonid

$$(a_1a_2),\quad (a_1a_3),\quad (a_1a_4),\quad \ldots,\quad (a_1a_m).$$

Kui siin $m=n$, siis peab G sisaldama iga transpositsiooni (pq), sest me võime transpositsiooni (pq) alati avaldada korrutisena

$$(pq)=(a_1p)\,(a_1q)\,(a_1p),$$

kus igas teguris on üheks numbriks a_1. Seega kui $m=n$, siis $G=S_n$.

Seevastu kui $m<n$, siis saab näidata, et G on imprimitiivne rühm, kusjuures hulk

$$M_1=\{a_1,\ a_2,\ \ldots,\ a_m\}$$

on üheks imprimitiivsuse klassiks. Vaatleme tõestuseks mingit substitutsiooni s rühmas G ja näitame, et kui a_1 teisend

$$b_1=a_1s$$

kuulub väljapoole hulka M_1, siis kuulub sinna ka iga a_k teisend

$$b_k=a_ks,\quad k=2,\ 3,\ \ldots,\ m.$$

Tõepoolest, arvutades (a_1a_k) kaassubstitutsiooni, leiame

$$s^{-1}(a_1a_k)s=(b_1b_k),$$

kusjuures (b_1b_k) peab kuuluma rühma G. Kui nüüd b_k kuuluks hulka M_1, siis kuuluks transpositsioon (a_1b_k) rühma G ja seega ka korrutis

$$(a_1b_k)\,(b_1b_k)\,(a_1b_k)=(a_1b_1),$$

mis on aga vastuolus eeldusega, sest b_1 ei kuulu hulka M_1. Täpselt samuti võib näidata, et kui a_1 teisend

$$b_1 = a_1 s$$

kuulub hulka M_1, siis kuulub sinna ka iga a_k teisend

$$b_k = a_k s, \quad k = 2, 3, \ldots, m.$$

Tähendab, G substitutsioon s teisendab hulga M_1 hulgaks

$$M_2 = \{b_1, b_2, \ldots, b_m\},$$

mis ei oma hulgaga M_1 ühtki ühist numbrit või langeb hulgaga M_1 ühte. Siinjuures kuuluvad transpositsioonid

$$(b_1 b_2), (b_1 b_3), \ldots, (b_1 b_m)$$

rühma G, nii et M_2 etendab G substitutsioonide suhtes sama osa mis M_1, mille puhul transpositsioonid

$$(a_1 a_2), (a_1 a_3), \ldots, (a_1 a_m)$$

kuulusid rühma G.

Vaatleme kõiki erinevaid hulki

$$M_1, M_2, \ldots, M_r, \tag{14}$$

mis saadakse hulgast M_1 rühma G substitutsioonide rakendamisel. G transitiivsuse tõttu sisaldavad hulgad (14) kõiki numbreid $1, 2, \ldots, n$. Olgu s_i rühma G substitutsioon, mis teisendab M_1 numbrid hulga M_i numbriteks, nii et $M_i = M_1 s_i$. Kui s tähendab mistahes substitutsiooni rühmas G, siis on

$$M_i s = (M_1 s_i) s = M_1 (s_i s) = M_1 s_j = M_j,$$

kus $s_j = s_i s$ on ka G substitutsioon. Seega on igal (14) hulkade paaril M_i, M_j samasugused omadused nagu paaril M_1, M_2, millest nähtub, et hulgad (14) kujutavad G imprimitiivsuse klasse.

Harjutusülesandeid.

103. Näidata, et maatriksid

$$E=\begin{Vmatrix}1&0&0\\0&1&0\\0&0&1\end{Vmatrix},\quad A_1=\begin{Vmatrix}2&-1&-1\\2&-1&-2\\1&-1&0\end{Vmatrix},\quad A_2=\begin{Vmatrix}-1&4&-5\\0&1&0\\0&0&1\end{Vmatrix}$$

$$A_3=\begin{Vmatrix}-2&7&-11\\-2&7&-12\\-1&3&-5\end{Vmatrix},\quad A_4=\begin{Vmatrix}1&2&-7\\2&-1&-2\\1&-1&0\end{Vmatrix},\quad A_5=\begin{Vmatrix}-1&6&-12\\-2&7&-12\\-1&3&-5\end{Vmatrix}$$

moodustavad rühma korrutamise suhtes.

104. Näidata, et korrutamistabelid

a)

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

b)

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

määravad rühma.

105. Näidata, et ratsionaalfunktsioonid

$$e=x,\quad f_1=\frac{1}{x},\quad f_2=1-x,\quad f_3=\frac{x}{x-1},\quad f_4=\frac{x-1}{x},\quad f_5=\frac{1}{1-x}$$

moodustavad rühma, kui arvutusoperatsioonina vaadelda liitfunktsiooni moodustamist.

106. Näidata, et kõik sama järku

a) regulaarmaatriksid;

b) ortogonaalmaatriksid;

c) unitaarmaatriksid;

d) unimodulaarmaatriksid

moodustavad rühma korrutamise suhtes.

107. Koostada ülesande 105 rühma korrutamistabel.

108. Leida 8-nda astme ühejuurte rühma elementide järgud.

109. Leida jäägiklassikorpuse $R^{(11)}$ multiplikatiivse rühma elementide 3, 6 ja 10 poolt moodustatud tsüklilised rühmad.

110. Näidata, et jäägiklassikorpuse $R^{(p)}$ multiplikatiivne rühm on tsükliline.

111. Arvutada ülesande 105 ratsionaalfunktsioonide komplekside

$$A = \{f_2, f_3\}, \quad B = \{e, f_2\}$$

summa ruut.

112. Leida ülesande 105 rühma kõik ühikrühmast erinevad pärisalamrühmad. Missugused nendest on normaaljagajad?

113. Leida sümmeetrilise rühma S_4 kolmandat järku tsüklilised alamrühmad.

114. Leida ülesande 105 rühma kõrvalklassideks lahutused kõigi alamrühmade järgi.

115. Leida jäägiklassikorpuse $R^{(13)}$ multiplikatiivse rühma kõrvalklassideks lahutus alamrühma $\{1, 5, 8, 12\}$ järgi.

116. Näidata, et parempoolse kõrvalklassi Ha elementide pöördelemendid moodustavad vasakpoolse kõrvalklassi $a^{-1}H$.

117. Näidata, et kompleksid

$$H_1 = \{1, -1\}, \quad H_2 = \{1, -1, i, -i\}, \quad H_3 = \{1, -1, j, -j\},$$
$$H_4 = \{1, -1, k, -k\}$$

kujutavad normaaljagajaid kvaternioonide multiplikatiivses rühmas.

118. Näidata, et ülesannete 103 ja 105 rühmad on isomorfsed sümmeetrilise rühmaga S_3.

119. Leida ülesande 104 rühmadega isomorfsed substitutsioonirühmad.

120. Näidata, et

$$G/E \longleftrightarrow G, \quad G/G \longleftrightarrow E,$$

kus E tähendab ühikrühma.

121. Näidata, et kõigil kaaselementidel on üks ja sama järk.

122. Leida 24-ndat järku tsüklilise rühma kõik kompositsioonijadad.

123. Leida 120-ndat järku tsüklilise rühma kompositsiooniindeksid.

124. Näidata, et kõigi sama järku regulaarmaatriksite multiplikatiivse rühma tsenter koosneb kõigist skalaarmaatriksitest.

125. Lahutada substitutsioon

$$(2\ 1)(3\ 5)(5\ 6)(1\ 4)(2\ 7)(3\ 4)(2\ 5)$$

sõltumatute tsüklite korrutiseks.

126. Antud on substitutsioonid

$$s = (1\ 2\ 8)(4\ 5)(3\ 6\ 7),$$
$$t = (2\ 1)(5\ 6)(2\ 7)(2\ 5)(3\ 5)(1\ 4)(3\ 4).$$

Leida $\bar{s} = t^{-1}st$ ja $\bar{t} = s^{-1}ts$.

127. Näidata, et iga k-liikmelise tsükli järk on k.

128. Lahutada rühm

$$H = \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),\ (1\ 2),\ (3\ 4),\ (1\ 3\ 2\ 4),\ (1\ 4\ 2\ 3)\}$$

kaaselementide klassideks ja leida ühikrühmast erinevad pärisnormaaljagajad.

129. Leida ülesande 128 rühma H kõik kompositsioonijadad.

130. Leida ülesande 128 rühmas H alamrühma $\{e, (1\ 3)(2\ 4)\}$ kaasalamrühmad.

131. Leida ülesande 128 rühma H elementide

a) $(1\ 2)$; b) $(1\ 4\ 2\ 3)$

ja alamrühmade

c) $\{e, (1\ 3)(2\ 4)\}$; d) $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$

normalisaatorid.

132. Kontrollida teoreemi isomorfismist (§ 21, art. 3), võttes A-ks substitutsiooni $(1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$ poolt moodustatud tsüklilise rühma ja H-ks substitutsiooni $(1\ 5\ 3\ 7)(2\ 8\ 4\ 6)$ poolt moodustatud tsüklilise rühma.

133. Leida ülesande 128 rühma H imprimitiivsuse klassid.

VII. Korpuseteooria alused.

§ 24. Ringiteooria alused.

1. **Ideaali mõiste.** Rakendame kõigepealt rühmateooria tulemusi ringi struktuuri uurimiseks, kusjuures vaatleme eranditult kommutatiivseid ringe. Rühmateoorias etendasid põhilist osa normaaljagaja ja faktorrühma mõisted. Analoogiliste mõisteteni võib jõuda ka ringiteoorias.

Olgu antud mingi ring R ja tema osahulk M. Niisugust osahulka, mis osutub ringioperatsioonide suhtes ise ka ringiks, nimetatakse ringi R a l a m r i n g i k s. Selle definitsiooni kohaselt loeme alamringide hulka ka ringi R ennast. Tahtes rõhutada, et vaadeldav alamring ei kujuta ringi R ennast, kõneleme p ä r i s a l a m r i n g i s t. Omaette alamringi moodustab — nagu selles kergesti võib veenduda — ringi R nullelemendist koosnev hulk $\{0\}$, mis kannab n u l l r i n g i nime.

Selleks et otsustada, kas osahulk M kujutab ringi R alamringi või mitte, tarvitseb kontrollida M suhtes vaid ringi postulaatide IV ja VIII (I, § 5, art. 1) kehtivust. Nimelt kujutab osahulk M ringi R alamringi siis ja ainult siis, kui iga $a \in M$ ja $b \in M$ puhul ka

$$1^0\ a - b \in M;\quad 2^0\ ab \in M,$$

s. o. kui M on kinnine lahutamise ja korrutamise suhtes. Arusaadav, et ringi postulaadid II, III, V, VI ja VII, mis kehtivad kogu ringis R, jäävad ammugi kehtima ka igas osahulgas M. Seevastu postulaat I järeldub tingimusest 1^0. Nimelt, võttes tingimuses 1^0 $a = 0$, näeme, et koos b-ga kuulub hulka M ka $-b$ ja siis ka

$$a - (-b) = a + b.$$

Nagu alamrühmade seas etendavad erilist osa normaaljagajad, nii alamringide seas omavad erilist tähtsust nn. ideaalid. Ideaaliteooria rajamisel on etendanud silmapaistvat osa vene matemaatik Zolotarjov.

Definitsioon 1. Ringi R osahulka m nimetatakse ideaaliks, kui:

1° m sisaldab koos elementidega a ja b ka vahet $a - b$;

2° m sisaldab koos elemendiga a ka iga korrutist ar, kus r tähendab mistahes elementi ringis R.

Siin esimene tingimus ütleb, et ideaal on kinnine lahutamise suhtes. Võttes teises tingimuses eriti $r = b$, kus $b \in$ m, näeme, et ideaal on kinnine ka korrutamise suhtes. Seega kujutab iga ideaal teatavat alamringi. Nagu nähtub ideaali definitsioonist, kujutab ka ring R ise ideaali — ühikideaali. Samuti kujutab ka nullring $\{0\}$ ideaali — nullideaali, sest

$$0 - 0 = 0, \quad 0 \cdot r = 0.$$

Olgu a mingi kindel element ringis R. Vaatleme R-i osahulka, mis koosneb kõigist elementidest

$$ar + na,$$

kus r tähendab ringi R mistahes elementi ja na elemendi a n-kordset. Osahulk $\{ar + na\}$ kujutab ideaali, sest:

1° $(ar_1 + n_1a) - (ar_2 + n_2a) = a(r_1 - r_2) + (n_1 - n_2)a = ar + na$, kus $r = r_1 - r_2$, $n = n_1 - n_2$;

2° $(ar_1 + n_1a)r_2 = ar_1r_2 + n_1ar_2 = a(r_1r_2 + n_1r_2) = ar + 0 \cdot a$, kus $r = r_1r_2 + n_1r_2$.

Ideaal $\{ar + na\}$ kannab elemendi a poolt moodustatud peaideaali nime ja märgitakse sümboliga (a), s. o.

$$(a) = \{ar + na\}.$$

Erijuhul, kui $a = 0$, saame nullideaali $(0) = \{0\}$. Ei ole raske näha, et peaideaal (a) on koosseisult väikseim ideaal, mis sisaldab elementi a, sest iga ideaal, mis sisaldab a-d, peab sisaldama ka kõiki korrutisi ar ja summasid $\pm(a + a + \ldots + a) = na$.

Kui R on ühikuga ring, kusjuures ühikelemendiks on e, siis võime distributiivsuse seaduse põhjal kirjutada

$$na = \pm(a + a + \ldots + a) = \pm a(e + e + \ldots + e) = a \cdot ne$$

ja seega

$$ar + na = ar + a \cdot ne = a(r + ne) = ar',$$

kus $r' = r + ne$ kujutab ringi R elementi. Niisiis võime ühikuga ringi puhul kirjutada

$$(a) = \{ar\},$$

kus r tähendab mistahes elementi ringis R. Erijuhul, kui $a = e$, saame ühikideaali $(e) = R$.

Lõppeks kui $a_1, a_2, \ldots, a_k$ on kindlad elemendid ja $r_1, r_2, \ldots, r_k$ mistahes elemendid ringis R, siis saab kergesti näidata, et R osahulk

$$(a_1, a_2, \ldots, a_k) = \{a_1r_1 + a_2r_2 + \ldots + a_kr_k + n_1a_1 + n_2a_2 + \\ + \ldots + n_ka_k\},$$

kus $n_1, n_2, \ldots, n_k$ tähendavad mistahes täisarve, kujutab ideaali. Ideaal $(a_1, a_2, \ldots, a_k)$ kannab elementide $a_1, a_2, \ldots, a_k$ poolt moodustatud ideaali nime ja on koosseisult väikseim ideaal, mis sisaldab elemente $a_1, a_2, \ldots, a_k$. Kui R on ühikuga ring, siis avaldub elementide $a_1, a_2, \ldots, a_k$ poolt moodustatud ideaal lihtsalt kujul

$$(a_1, a_2, \ldots, a_k) = \{a_1r_1 + a_2r_2 + \ldots + a_kr_k\}.$$

2. Jäägiklassiringid ideaalide järgi. Et ring R kujutab liitmise suhtes rühma, siis kujutab ideaal m kui alamring R-i alamrühma. Veel enam, ideaal m kujutab liitmise suhtes normaaljagajat, sest Abeli rühmas on iga alamrühm normaaljagaja. Vaatleme faktorrühma R/m. Et siin rühmaoperatsiooniks on liitmine, siis on kohane elemendile a vastavat kõrvalklassi $\bar{a}$ märkida kujul

$$\bar{a} = \mathrm{m} + a,$$

sest $\bar{a}$ koosneb kõigist elementidest $m + a$, kus m tähendab mistahes elementi ideaalis m. Eriti on

$$\bar{0} = \mathrm{m} + 0 = \{m + 0\} = \{m\} = \mathrm{m},$$

millest nähtub, et ideaal m kujutab R nullelemendile vastavat kõrvalklassi $\bar{0}$.

Kahe kõrvalklassi $\bar{a} = \mathrm{m} + a$ ja $\bar{b} = \mathrm{m} + b$ summa all mõistame valemi (7) (§ 19, art. 4) kohaselt kõrvalklassi

$$\overline{a + b} = \mathrm{m} + (a + b),$$

s. o.

$$(\mathrm{m} + a) + (\mathrm{m} + b) = \mathrm{m} + (a + b)$$

ehk lühidalt

$$\bar{a} + \bar{b} = \overline{a + b}.$$

Lisaks kõrvalklasside summale, mis on antud koos faktorrühma R/m mõistega, defineerime ka kõrvalklasside korrutise valemiga

$$(\mathrm{m} + a) \cdot (\mathrm{m} + b) = \mathrm{m} + ab$$

ehk lühidalt

$$\bar{a}\bar{b} = \overline{ab}.$$

Seega taandub kõrvalklassidega opereerimine nende kõrvalklasside esindajatega opereerimisele. Et kahe kõrvalklassi summa kujutab kindlat kõrvalklassi, nagu me rühmateooriast teame (§ 19, art. 4) ja, teiselt poolt, kõrvalklassi esindajaks võib olla selle kõrvalklassi iga element, siis ei sõltu kõrvalklasside summa esindajate valikust liidetavates kõrvalklassides. Täpsemalt, kui peale a kuulub kõrvalklassi $\bar{a}$ veel a_1 ja peale b kõrvalklassi $\bar{b}$ veel b_1, siis esindab $a_1 + b_1$ sama kõrvalklassi mis $a + b$, s. o.

$$\overline{a_1 + b_1} = \overline{a + b}.$$

Näitame, et ka kõrvalklasside korrutis ei sõltu esindajate valikust korrutatavates kõrvalklassides, nii et

$$\overline{a_1 b_1} = \overline{ab}\,.$$

Selleks laiendame kõigepealt täisarvude integriteetkonnas Γ ja polünoomkonnas $K[x]$ käsiteldud kongruentsi mõistet mistahes ringile R.

Olgu a ja b mingid kaks elementi ringis R. Kui osutub, et vahe $a - b$ kuulub ideaali m, siis öeldakse, et a ja b on kongruentsed ideaali m järgi ja kirjutatakse

$$a \equiv b\,(\mathrm{m})$$

ehk, kui m on ette teada, siis lihtsalt

$$a \equiv b\,.$$

Erijuhul, kui m on peaideaal, s. o. $\mathrm{m} = (m)$, kus m tähendab mingit kindlat elementi ringis R, kirjutatakse sümboli $a \equiv b\,((m))$ asemel lühemalt

$$a \equiv b\,(m).$$

Kui R on ühikuga ring, siis on $(m) = \{mr\}$, ja seega tähendab siin kongruents $a \equiv b\,(m)$, et vahe $a - b$ avaldub kujul mr, s. o. et vahe $a - b$ jagub m-ga.

Kehtigu mistahes ringis R kongruents

$$a \equiv b\,(\mathrm{m})$$

mingi ideaali m järgi. Siis $a - b \in \mathrm{m}$ ehk $a - b = m$, kus m tähendab teatavat elementi ideaalis m. Seega kehtib kongruentsi korral elementide a ja b vahel seos

$$a = b + m\,, \quad m \in \mathrm{m}\,,$$

mis ütleb, et a kuulub kõrvalklassi $\overline{b} = \mathrm{m} + b$, s. o. samasse kõrvalklassi, kuhu kuulub b. Ümberpöördult, kui a ja b kuuluvad ühte ja samasse kõrvalklassi, siis a, kuuludes kõrvalklassi $\overline{b} = \mathrm{m} + b$, peab omama kuju

$$a = b + m\,, \quad m \in \mathrm{m}\,,$$

millest $a - b = m$, s. o. $a - b \in \mathfrak{m}$. Tähendab, *ringis leiab kongruents* $a \equiv b\,(\mathfrak{m})$ *aset siis ja ainult siis, kui* a *ja* b *kuuluvad ühte ja samasse kõrvalklassi* $\mathfrak{m}$ *järgi.*

Analoogiliselt täisarvude kongruentsiga (I, § 8, art. 1) võib kergesti veenduda, et igal kongruentsil $a \equiv b\,(\mathfrak{m})$ on võrduse omadused, see tähendab refleksiivsuse, sümmeetria ja transitiivsuse omadused. Veel enam, kui

$$a_1 \equiv a, \quad b_1 \equiv b,$$

siis ei ole raske näha, et

$$\begin{aligned} a_1 + b_1 &\equiv a + b \\ a_1 b_1 &\equiv ab \\ a_1 - b_1 &\equiv a - b, \end{aligned} \tag{1}$$

s. o. kongruentse võib liikmeti liita, korrutada ja lahutada. Siin kongruents $a_1 b_1 \equiv ab$ ütleb, et $a_1 b_1$ ja ab kuuluvad ühte ja samasse kõrvalklassi, s. o.

$$\overline{a_1 b_1} = \overline{ab},$$

millega ongi eespool püstitatud väide kõrvalklasside korrutise sõltumatuse kohta kõrvalklasside esindajate valikust põhjendatud.

Ülejäänud kongruentsid (1) väljendavad meile juba tuntud tõsiasja, et faktorrühmas $R/\mathfrak{m}$ on liitmine ja lahutamine üheselt teostatavad. Seega kehtivad faktorrühmas $R/\mathfrak{m}$, kus peale liitmise kui rühmaoperatsiooni on defineeritud veel korrutamine, lisaks liitmisega seotud ringi postulaatidele I, II, III, VIII (I, § 5, art. 1) veel postulaat IV ja ka ülejäänud ringi postulaadid V, VI, VII, sest faktorrühmas $R/\mathfrak{m}$ taanduvad tehted kõrvalklassidega tehetele nende kõrvalklasside esindajatega, s. o. ringi R elementidega. Niisiis kujutab $R/\mathfrak{m}$, tänu juurde defineeritud korrutamisele, ringi — f a k t o r r i n g i.

Ei ole raske näha, et varem käsiteldud jäägiklassiringid $R^{(m)}$ (I, § 8, art. 2) ja $R^{(m(x))}$ (§ 5, art. 2) kujutavad faktorringi $R/\mathfrak{m}$ erijuhte, mis vastavad peaideaalidele $\mathfrak{m} = (m)$ (m täisarv)

ja $\mathfrak{m} = (m(x))$ ($m(x)$ polünoom). Jäägiklassiringide $R^{(m)}$ ja $R^{(m(x))}$ puhul kasutasime vaid kõrvalklasside, s. o. jäägiklasside võrduse $\bar{a} = \bar{b}$ asemel kongruentsi $a \equiv b$ kui uut võrdust, opereerides vastavalt sellele jäägiklasside asemel nende esindajatega — taandatud elementidega. Seetõttu nimetatakse kõrvalklasse $\mathfrak{m} + a$ ka jäägiklassideks ja faktorringi $R/\mathfrak{m}$ jäägiklassiringiks ideaali $\mathfrak{m}$ järgi.

Olles laiendanud jäägiklassiringi mõistet mistahes ringile R, selgitame järgnevas artiklis, missugustel tingimustel osutub jäägiklassiring $R/\mathfrak{m}$ korpuseks.

3. Peaideaaliringid. Täisarvude integriteetkonnal Γ ja polünoomkonnal $K[x]$ on rida tähelepandavaid individuaalomadusi [1], mis annavad neile erikoha kõigi integriteetkondade peres. Osutub, et nimetatud omadused on tingitud asjaolust, et integriteetkondades Γ ja $K[x]$ kujutab iga ideaal peaideaali. Viimase väite tõestuseks vaatleme integriteetkondades Γ ja $K[x]$ mistahes ideaali $\mathfrak{m}$, mille kohta võib üldsust kitsendamata eeldada, et ta ei ole nullideaal, sest nullideaal kujutab alati peaideaali. Seega peab $\mathfrak{m}$ sisaldama ka nullist erinevaid elemente. Olgu m Γ puhul absoluutselt väikseim nullist erinev täisarv ja $K[x]$ puhul madalaima astmega nullist erinev polünoom ideaalis $\mathfrak{m}$. Jagades ideaali $\mathfrak{m}$ mingi elemendi a m-ga, saame

$$a = qm + r,$$

kus Γ korral r tähendab nulli või naturaalarvu, mis on väiksem kui $|m|$, kuna $K[x]$ korral r tähendab nullpolünoomi või polünoomi, mille aste on väiksem kui m-i aste. Et

$$r = a - qm,$$

siis ideaali mõiste kohaselt $r \in \mathfrak{m}$. Seega peab olema $r = 0$, sest vastasel korral leiduks ideaalis $\mathfrak{m}$ Γ puhul naturaalarv r, mis on väiksem kui $|m|$ ja $K[x]$ puhul polünoom r, mille aste

[1] Näiteks omadused, mis väljenduvad jaguvusteoorias ja maatriksite teoorias üle integriteetkonna (§ 4 ja § 14).

oleks väiksem kui m-i aste. Viimasest võrdusest nähtub seetõttu, et $a = mq$, mis ütleb, et m kujutab peaideaali

$$\mathfrak{m} = (m).$$

Tähendab, integriteetkondades Γ ja $K[x]$ on iga ideaal peaideaal.

Niisugust integriteetkonda, kus iga ideaal on peaideaal, nimetatakse peaideaaliringiks. Kasutades peaideaaliringi mõistet, võime sõnastada järgmise teoreemi:

Teoreem 1. *Täisarvude integriteetkond Γ ja polünoomkond $K[x]$ kujutavad peaideaaliringe.*

Seevastu polünoomkond $\Gamma[x]$ ei ole peaideaaliring, sest siin näiteks ideaal $(2, x)$ ei kujuta peaideaali. Tõepoolest, vastasel korral peaks leiduma niisugune täisarvuliste kordajatega polünoom $m(x)$, et

$$(2, x) = (m(x)).$$

Järelikult peavad 2 ja x jaguma $m(x)$-ga, mistõttu $m(x) = \pm 1$. Seega peaks $(m(x))$, s. o. $(2, x)$ koosnema kõigist täisarvuliste kordajatega polünoomidest. Et aga $(2, x) = \{2r_1(x) + xr_2(x)\}$, siis koosneb $(2, x)$ vaid nendest täisarvuliste kordajatega polünoomidest, mille vabaliige on paarisarv.

Vaatleme näitena veel integriteetkonda $\{a + bi\}$, kus a ja b tähendavad täisarve. Siin arvud $a + bi$ kannavad Gaussi täisarvude ja vastava jagatistekorpuse elemendid $\frac{a+bi}{c+di}$ Gaussi ratsionaalarvude nime. Näitame, et Gaussi täisarvude integriteetkonnas kehtib jäägiga jagamise algoritm selles mõttes, et iga kahe Gaussi täisarvu α ja $\beta \neq 0$ vahel on kehtiv seos

$$\alpha = \lambda\beta + \mu,$$

kus $|\mu| < |\beta|$ ja λ on teatav Gaussi täisarv.

Vaatleme Gaussi ratsionaalarvu $\lambda' = \frac{\alpha}{\beta}$. Olgu $\lambda' = a' + b'i$, kus a' ja b' on ratsionaalarvud. Määrame Gaussi täisarvu

$\lambda = a + bi$ nii, et a oleks lähim täisarv a'-le ja b lähim täisarv b'-le, s. o. et

$$|a' - a| \leqslant \frac{1}{2}, \quad |b' - b| \leqslant \frac{1}{2}.$$

Märkides $\alpha - \lambda\beta = \mu$, millest $\alpha = \lambda\beta + \mu$, leiame

$$\mu = \lambda'\beta - \lambda\beta = (\lambda' - \lambda)\beta = [(a' - a) + (b' - b)i]\beta,$$

ja seega

$$|\mu| = \sqrt{(a' - a)^2 + (b' - b)^2}\,|\beta| \leqslant \sqrt{\frac{1}{4} + \frac{1}{4}}\,|\beta| < |\beta|.$$

Olgu tähendatud, et erinevalt harilike täisarvude ja polünoomide juhust pole siin λ ja μ üheselt määratud. Toetudes leitud jäägiga jagamise algoritmile, ei ole raske analoogiliselt harilike täisarvude ja polünoomide juhuga veenduda, et ka Gaussi täisarvude integriteetkond kujutab peaideaaliringi.

Näitame nüüd, et igas peaideaaliringis R kehtib jaguvuse teooria. Olgu a ja b mingid kaks elementi peaideaaliringis R. Siis peab eriti ka ideaal (a, b) kujutama peaideaali, s. o. peab leiduma niisugune element d, mille puhul

$$(a, b) = (d).$$

Seega peavad a ja b jaguma d-ga, s. o. d on a ja b ühistegur. Veel enam, d on a ja b suurim ühistegur selles mõttes, et d jagub a ja b iga ühisteguriga. Tõepoolest, viimasest ideaalide võrdusest nähtub, et missugune ka ei oleks R-i element r, ikka peavad leiduma niisugused elemendid r_1 ja r_2, et oleks

$$dr = ar_1 + br_2.$$

Erijuhul, kui siin $r = e$,

$$d = ar_1' + br_2', \tag{2}$$

millest ilmnebki, et d peab jaguma a ja b iga ühisteguriga.

Nagu integriteetkondades Γ ja $K[x]$, nii on üldiselt igas peaideaaliringis R suurim ühistegur üheselt määratud kuni triviaalsete teguriteni, s. o. niisuguste elementideni, millega jagub

R-i iga element (§ 8, art. 4). Elemente, mille suurim ühistegur on triviaalne, nimetatakse ü h i s t e g u r i t a e l e m e n t i d e k s. Võrdusest (2) järeldub vahetult alljärgnev teoreem.

T e o r e e m 2. *Võrrand* $ax + by = d$, *kus* d *tähendab* a *ja* b *suurimat ühistegurit, omab peaideaaliringis alati lahendit* x, y.

Üldiselt saab näidata, et *võrrand* $ax + by = c$ *on lahenduv peaideaaliringis siis ja ainult siis, kui* c *jagub* a *ja* b *suurima ühisteguriga.*

Analoogiliselt täisarvude integriteetkonna juhuga (I, § 7, art. 3) võib teha teoreemist 2 järgmise järelduse:

T e o r e e m 3. *Kui peaideaaliringis korrutis* ab *jagub* m*-ga, kusjuures* a *ja* m *on ühistegurita elemendid, siis peab* b *jaguma* m*-ga.*

Teoreemist 3 nähtub eriti, et kui korrutis jagub algelemendiga p, siis peab vähemalt üks tegureist jaguma selle algelemendiga p.

Vaatleme nüüd peaideaaliringis R mingit nullist erinevat elementi m, mis ei ole triviaalne tegur. Kui m ei ole algelement, siis saab teda lahutada kahe mittetriviaalse teguri korrutiseks. Viimased tegurid lahutame võimaluse korral omakorda mittetriviaalsete tegurite korrutiseks jne. Kui täisarvude integriteetkonna Γ või polünoomkonna $K[x]$ puhul on ilmne, et niisugune mittetriviaalseiks tegureiks lahutamine ei saa jätkuda lõpmatuseni, vajab viimane asjaolu mistahes peaideaaliringi korral lähemat põhjendust. Oletades, et elemendi m lahutamist mittetriviaalsete tegurite korrutiseks võib piiramata jätkata, saame elementide jada

$$a_1, a_2, \ldots, a_n, \ldots,$$

mille puhul $a_n = a_{n+1}q$, kus q tähendab mittetriviaalset tegurit. Vaadeldes nende elementide poolt moodustatud peaideaale, on ilmne, et

$$(3) \qquad (a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset \ldots .$$

Ei ole raske näha, et siin summa [1]

$$\mathfrak{m} = (a_1) + (a_2) + \ldots + (a_n) + \ldots$$

kujutab ka ideaali. Nimelt kui $a \in \mathfrak{m}$ ja $b \in \mathfrak{m}$, siis leiduvad niisugused i ja k, et $a \in (a_i)$ ja $b \in (a_k)$. Kui nüüd näiteks $i \leqslant k$, siis (3) tõttu $a \in (a_k)$. Järelikult a ja b, kuuludes mõlemad ideaali (a_k), rahuldavad tingimusi

$$a - b \in (a_k), \quad ar \in (a_k)$$

ja seega ammugi tingimusi

$$a - b \in \mathfrak{m}, \quad ar \in \mathfrak{m},$$

millest nähtubki, et m on ideaal. Et aga R on peaideaaliring, siis on siin ka m peaideaal, s. o.

$$\mathfrak{m} = (d).$$

Kuid d kui m-i element peab kuuluma mingisse peaideaali (a_n), nii et d peab jaguma a_n-ga. Teiselt poolt peab aga a_n kui peaideaali m element jaguma d-ga, mistõttu a_n võib erineda d-st ülimalt triviaalse teguri poolest. Täpselt samuti võib a_{n+1} erineda d-st ülimalt triviaalse teguri poolest. Järelikult saab a_{n+1} erineda a_n-st ka ülimalt triviaalse teguri poolest, mis ütleb, et jada $a_1, a_2, \ldots, a_n, \ldots$ peab hiljemalt a_n järel lõppema.

Seega laguneb element m lõpliku arvu algelementide korrutiseks:

$$m = p_1 p_2 \ldots p_k,$$

kusjuures täpselt nagu täisarvude integriteetkonna puhul saab näidata, et siin tegurid $p_1, p_2, \ldots, p_k$ on kuni triviaalsete teguriteni üheselt määratud, s. o. et peaideaaliringis kehtib algtegureiks lahutamise lause.

Teoreem 4. *Peaideaaliringis laseb iga nullist erinev element m, mis ei ole triviaalne tegur, ennast lahutada algelementide korrutiseks*

$$m = p_1 p_2 \ldots p_k,$$

[1] § 19, art. 1 mõttes.

kus tegurid p_1, p_2, ..., p_k *on kuni triviaalsete teguriteni üheselt määratud.*

Tuleme nüüd eelmise artikli lõpus püstitatud küsimuse juurde, missugustel tingimustel osutub jäägiklassiring $R/\mathfrak{m}$ korpuseks, eeldades seejuures, et R on peaideaaliring, nii et $\mathfrak{m} = (m)$. Selgitame selleks kõigepealt, missugused $R/\mathfrak{m}$ elemendid omavad pöördväärtusi, s. o. missuguste jäägiklasside $\bar{a}$ puhul on võrrand

$$\bar{a}\bar{x} = \bar{e}$$

lahenduv. Üle minnes jäägiklassidelt nende esindajatele, tuleb mõista viimast võrrandit kongruentsina

$$ax \equiv e(\mathfrak{m}),$$

s. o.

$$ax = e + mq$$

ehk

$$ax - mq = e, \tag{4}$$

kus q tähendab teatavat R elementi. Seega seisneb kogu küsimus selles, missuguste a väärtuste puhul omab võrrand (4) lahendit x, q peaideaaliringis R. Eelnenu põhjal on võrrand (4) lahenduv peaideaaliringis R siis ja ainult siis, kui e jagub a ja m suurima ühisteguriga, s. o. kui a ja m on ühistegurita. Tähendab, jäägiklassiringis $R/\mathfrak{m}$ omavad pöördväärtusi need ja ainult need jäägiklassid, mille esindajad on m-ga ühistegurita.

Erijuhul, kui m kujutab algelementi p, omavad temaga ühist tegurit vaid suurused pr, s. o. ideaali (p) elemendid. Seega omab jäägiklassiringis $R/(p)$ pöördväärtust iga jäägiklass, välja arvatud nullklass $\bar{0} = (p)$. Teiste sõnadega, jäägiklassiring $R/(p)$, kus p tähendab algelementi, moodustab korpuse — jäägiklassikorpuse. Seevastu jäägiklassiring $R/(m)$, kus m on liitelement, ei kujuta kunagi korpust, sest sel korral omab m kuju

$$m = m_1 m_2,$$

kust vastavatele jäägiklassidele üle minnes saame $m = \overline{0}$ tõttu

$$\overline{m_1}\,\overline{m_2} = \overline{0},$$

millest nähtub, et $\overline{m_1}$ ja $\overline{m_2}$ on nullitegurid jäägiklassiringis $R/(m)$.

Vaatleme veel ülejäänud juhtusid $m = 0$ ja $m = \varepsilon$, kus ε tähendab triviaalset tegurit. Juhul $m = 0$ kujutab (m) nulliideaali (0), mistõttu R elemendile a vastav jäägiklass $\overline{a}$ omab kuju

$$\overline{a} = (0) + a = \{0 + a\} = \{a\},$$

kust nähtub, et siin R jaotus jäägiklassideks tähendab jaotust üksikuteks elementideks, nii et $R/(0)$ taandub ringiks R.

Juhul $m = \varepsilon$ kujutab (m) ühikideaali R, mistõttu saame vaid ühe jäägiklassi

$$\overline{a} = R + a = R,$$

nii et R/R taandub nullringiks.

Kokku võttes võime öelda, et *jäägiklassiring* $R/(\mathrm{m})$ *kujutab korpust siis ja ainult siis, kui* m *on algelement.*

4. Ringide homomorfism. Analoogiliselt rühmade homomorfismi mõistega toome sisse ringide homomorfismi mõiste.

Definitsioon 2. Kui ringi $\overline{R}$ on võimalik seada ühesesse vastavusse ringiga R nii, et summale ringis R vastab liidetavaile vastavate elementide summa ringis $\overline{R}$ ja korrutisele ringis R tegureile vastavate elementide korrutis ringis $\overline{R}$, siis öeldakse, et $\overline{R}$ on homomorfne ringiga R.

Ringi $\overline{R}$ vastavust ringiga R nimetatakse sel juhul homomorfseks vastavuseks ehk homomorfismiks. Niisiis on ringide homomorfism niisugune ühene vastavus, mis säilib ringioperatsioonide puhul. Ringi $\overline{R}$ homomorfset vastavust ringiga R märgime sümboliga

$$R \overset{+}{\to} \overline{R}.$$

Erijuhul, kui siin vastavus on üksühene, taandub homomorfism isomorfismiks

$$R \overset{+}{\longleftrightarrow} R .$$

Mistahes kahe operatsiooniga hulga homomorfset vastavust ringiga iseloomustab järgmine teoreem, mis tõestatakse analoogiliselt teoreemiga 5 rühmateooriast (§ 21, art. 1).

Teoreem 5. *Kui mingi kahe operatsiooniga hulk M on homomorfses vastavuses ringiga R, siis osutub ka M ringiks, kusjuures R-i nullelemendile vastab M-i nullelement ja R-i mingi elemendi vastandelemendile M-i vastava elemendi vastandelement. Erijuhul, kui ringis R on ühikelement, vastab viimasele ringi M ühikelement, ja kui R-i mingil elemendil on pöördelement, siis vastab sellele M-i vastava elemendi pöördelement.*

Vaatleme ringide homomorfismi näitena mistahes ringi R ja tema jäägiklassiringi

$$R/\mathfrak{m} = \{\mathfrak{m} + a\},$$

kus $\mathfrak{m}$ tähendab mingit R-i ideaali. Seades R-i igale elemendile a vastavusse selle elemendiga esindatud jäägiklassi $\mathfrak{m} + a$, näeme, et see vastavus säilib vaadeldavate ringide operatsioonide puhul, sest kui

$$a \longrightarrow \mathfrak{m} + a , \quad b \longrightarrow \mathfrak{m} + b ,$$

siis, silmas pidades jäägiklasside liitmise ja korrutamise eeskirju (art. 2), leiame

$$\begin{aligned} a + b \longrightarrow \mathfrak{m} + (a + b) &= (\mathfrak{m} + a) + (\mathfrak{m} + b) \\ ab \longrightarrow \mathfrak{m} + ab \qquad &= (\mathfrak{m} + a) \cdot (\mathfrak{m} + b). \end{aligned}$$

Seega oleme saanud homomorfismi

$$R \overset{+}{\longrightarrow} R/\mathfrak{m} . \tag{5}$$

Tähendab, *R-i iga jäägiklassiringi $R/\mathfrak{m}$ võib seada homomorfsesse vastavusse ringi R endaga.* Nagu rühmade puhul, nii on siingi homomorfismidega (5) ammendatud kõik võimalikud ringi

homomorfismid. Nimelt on kehtiv järgmine teoreem ringi homomorfismidest, mida saab tõestada täiesti analoogiliselt teoreemiga 6 rühma homomorfismidest (§ 21, art. 2).

Teoreem 6. *Kui ring $\bar{R}$ on homomorfses vastavuses ringiga R, siis on $\bar{R}$ isomorfne jäägiklassiringiga $R/\mathfrak{m}$, kus ideaal* m *koosneb kõigist neist R-i elementidest, millele vastab homomorfismis $R \overset{+}{\to} \bar{R}$ ringi R nullelement.*

Lühidalt, kui $R \overset{+}{\to} \bar{R}$, siis $\bar{R} \overset{+}{\leftarrow\!\to} R/\mathfrak{m}$.

Võrreldes homomorfismi mõistet isomorfismiga, tuleb tähendada, et need kaks mõistet etendavad hoopis isesugust osa algebras. Sel ajal kui kahte isomorfset algebralist piirkonda võib pidada identseteks, ei saa algebralist piirkonda identifitseerida tema homomorfse piirkonnaga kas või juba seepärast, et näiteks integriteetkonnaga homomorfseks piirkonnaks võib olla niihästi ring ($R \overset{+}{\to} R/(m)$, m liitelement) kui ka korpus ($R \overset{+}{\to} R/(p)$, p algelement). Ometi huvitavad meid algebralise piirkonna homomorfismid seetõttu, et nende tundmine võimaldab teha järeldusi antud piirkonna enese struktuuri kohta.

Vaatleme lõppeks veel korpuse homomorfisme. Ei ole raske näha, et korpuses on ainukesteks ideaalideks nullideaal ja ühikideaal. Olgu nimelt m mingi ideaal (mitte nullideaal) korpuses R ja a selle ideaali nullist erinev element. Ideaali mõiste kohaselt peab siis m sisaldama koos a-ga ka kõiki korrutisi ar, kus $r \in R$, ja seega üldse korpuse R iga elementi b, sest me võime jagamise seaduse põhjal elemendi r alati nii valida, et oleks

$$ar = b.$$

Tähendab, kui korpuses R ideaal m ei ole nullideaal, siis kujutab m korpust R ennast, s. o. ühikideaali.

Kui nüüd mingi ring R on homomorfses vastavuses korpusega R, siis ütleb teoreem ringi homomorfismidest, et

$$\bar{R} \overset{+}{\leftarrow\!\to} R/\mathfrak{m}.$$

Sõltuvalt sellest, et korpuses võib m kujutada vaid nullideaali või ühikideaali, saame siin kaks võimalust:

$$1^0\ \bar{R} \overset{+}{\underset{\cdot}{\leftrightarrow}} R/(0);\quad 2^0\ \bar{R} \overset{+}{\underset{\cdot}{\leftrightarrow}} R/R.$$

Nagu nägime eelmise artikli lõpus, kujutab $R/(0)$ korpust R ennast ja R/R nullringi $\{0\}$. Seega on korpuse R puhul $\bar{R}$ suhtes kaks võimalust:

$$1^0\ \bar{R} \overset{+}{\underset{\cdot}{\leftrightarrow}} R;\qquad 2^0\ \bar{R} \overset{+}{\underset{\cdot}{\leftrightarrow}} \{0\}.$$

Tähendab, kui ring $\bar{R}$ on homomorfses vastavuses korpusega R, siis homomorfism kas taandub isomorfismiks või $\bar{R}$ koosneb ainult ühest elemendist — nullelemendist.

Järgnevas paragrahvis rakendame teoreemi ringi homomorfismidest korpuse struktuuri selgitamiseks.

§ 25. Algkorpused ja lihtlaiendid.

1. Algkorpused. Seame endale ülesandeks saada ülevaadet kõikidest võimalikkudest korpuse põhitüüpidest. Siinjuures vaatleme edaspidi vaid kommutatiivseid korpusi, mille kohta nõuame, et nad sisaldaks vähemalt kahte erinevat elementi — nullelementi ja ühikelementi.

Olgu Δ mingi osahulk korpuses K. Niisugust osahulka, mis osutub korpuseoperatsioonide suhtes ise ka korpuseks, nimetatakse korpuse K *alamkorpuseks*. Selle definitsiooni kohaselt loeme alamkorpuste hulka ka korpust K ennast. Tahtes rõhutada, et vaadeldav alamkorpus ei kujuta korpust K ennast, kõneleme *pärisalamkorpusest*.

Selleks et otsustada, kas osahulk Δ kujutab korpuse K alamkorpust või mitte, tarvitseb kontrollida Δ suhtes vaid korpuse postulaatide VIII ja IX (I, § 6, art. 1) kehtivust. Nimelt võib analoogiliselt alamringi juhuga näidata (§ 24, art. 1), et osa-

hulk A kujutab korpuse K alamkorpust siis ja ainult siis, kui iga $a \in A$ ja $b \in A$ puhul ka

$$1^0 \quad a - b \in A; \quad 2^0 \quad \frac{a}{b} \in A,$$

s. o. kui A on kinnine lahutamise ja jagamise suhtes.

Kasutades viimast tulemust, näitame, et kahe alamkorpuse A_1 ja A_2 ühisosa $A = A_1 \cap A_2$ on ka alamkorpus. Tõepoolest, kui a ja b tähendavad A elemente, siis $a \in A_1$, $a \in A_2$, $b \in A_1$, $b \in A_2$. Et aga A_1 ja A_2 on korpused, siis

$$a - b \in A_1, \quad \frac{a}{b} \in A_1, \quad a - b \in A_2, \quad \frac{a}{b} \in A_2$$

ja seega

$$a - b \in A, \quad \frac{a}{b} \in A,$$

mis ütlebki, et A on alamkorpus.

Vaatleme näitena reaalarvude korpuses osahulka

$$A = \{a + b\sqrt{u}\},$$

kus a ja b tähendavad meelevaldseid ratsionaalarve ja u mingit mitteruutarvu. Et

$$1^0 \quad (a + b\sqrt{u}) - (c + d\sqrt{u}) = (a - c) + (b - d)\sqrt{u};$$

$$2^0 \quad \frac{a + b\sqrt{u}}{c + d\sqrt{u}} = \frac{(a + b\sqrt{u})(c - d\sqrt{u})}{(c + d\sqrt{u})(c - d\sqrt{u})} = \frac{ac - ubd}{c^2 - ud^2} + \frac{bc - ad}{c^2 - ud^2}\sqrt{u},$$

kus $c^2 - ud^2 \neq 0$, siis A, olles kinnine lahutamise ja jagamise suhtes, kujutab reaalarvude korpuse alamkorpust.

Niisiis on reaalarvude korpusel lõpmatu hulk alamkorpusi. Seevastu ratsionaalarvude korpusel pole ühtki pärisalamkorpust, sest siin iga alamkorpus, sisaldades arve 0 ja 1, peab sisaldama kõiki summasid $\pm(1 + 1 + \ldots + 1)$, s. o. kõiki täisarve ja siis ka kõiki täisarvude jagatisi, s. o. kõiki ratsionaalarve. Niisugust korpust, millel ei ole ühtki pärisalamkorpust, nimetatakse a l g - k o r p u s e k s. Saab näidata, et iga korpust iseloomustab üks kindel algkorpus.

Teoreem 7. *Igas korpuses leidub üks ja ainult üks algkorpus.*

Teoreemi 7 tõestuseks vaatleme antud korpuse K kõigi alamkorpuste ühisosa, mille märgime P-ga. Nagu nägime, kujutab ka P alamkorpust. Näitame, et P on algkorpus. Vaatleme selleks mingit P alamkorpust Δ:

$$\Delta \subset P.$$

Et Δ on ühtlasi ka K alamkorpus, siis peab P kui K kõigi alamkorpuste ühisosa sisalduma eriti ka alamkorpuses Δ:

$$P \subset \Delta.$$

Viimasest kahest seosest järeldub, et $\Delta = P$, mis ütleb, et korpusel P pole ühtki pärisalamkorpust. Teiste sõnadega, P on algkorpus.

Niisiis leidub igas korpuses K teatav algkorpus P. Jääb näidata, et P on ainuke algkorpus korpuses K. Oletame vastupidi, et korpuses K leidub peale P veel algkorpus Q. Siis P kui korpuse K kõigi alamkorpuste ühisosa peab sisalduma ka alamkorpuses Q:

$$P \subset Q.$$

Et aga Q on algkorpus, siis peab olema $P = Q$, nii et P on tõesti ainuke K algkorpus.

Silmas pidades teoreemi 7, võime edaspidi kõnelda lihtsalt korpuse K algkorpusest P. Nii on näiteks iga arvukorpuse algkorpuseks ratsionaalarvude korpus. Kasutades teoreemi 6 ringi homomorfismidest (§ 24, art. 4), saab leida kõik algkorpuste tüübid.

Olgu P mingi algkorpus ja e tema ühikelement. Siis peavad korpusse P kuuluma kõik kordsed

$$me = \pm \underbrace{(e + e + \ldots + e)}_{|m| \text{ liidetavat}}.$$

Märgime ühikelemendi e kõigi kordsete hulga I-ga, s. o.

$$I = \{me\}.$$

Ei ole raske näha, et I on homomorfne täisarvude integriteetkonnaga Γ. Nimelt, korraldades Γ ja I vahel vastavuse

$$m \longrightarrow me\,, \quad n \longrightarrow ne\,,$$

leiame

$$m + n \longrightarrow (m+n)e = me + ne\,,$$
$$mn \longrightarrow (mn)e = m(ne) = me \cdot ne\,,$$

mis ütlebki, et

$$\Gamma \overset{+}{\cdot\!\!\rightarrow} I\,. \tag{6}$$

Seega I, olles homomorfne integriteetkonnaga Γ, on teoreemi 5 järgi ring ja nimelt ühikuga ring (§ 24, art. 4). Veel enam, ringis I kui korpuse P osahulgas puuduvad nullitegurid. Teiste sõnadega, I on integriteetkond.

Rakendades teoreemi ringi homomorfismidest, võime kirjutada:

$$I \overset{+}{\cdot\!\!\leftarrow\!\!\rightarrow} \Gamma/\mathfrak{m}\,, \tag{7}$$

kus ideaal $\mathfrak{m}$ koosneb kõigist neist täisarvudest, millele vastab homomorfismis (6) I nullelement, s. o. kõigist niisugustest täisarvudest m, mille puhul $me = 0$. Silmas pidades, et Γ kujutab teoreemi 1 järgi peaideaaliringi (§ 24, art. 3), peab eriti ka $\mathfrak{m}$ olema peaideaal, nii et

$$\mathfrak{m} = (p)\,.$$

Vaatleme eraldi kahte juhtu selle järgi, kas $p \neq 0$ või $p = 0$.

1° Kui $p \neq 0$, siis peab olema $|p| > 1$, sest kuna ideaal $\mathfrak{m} = (p)$ sisaldab eriti ka täisarvu p, siis on $pe = 0$, mis oleks võimatu, kui $|p| = 1$, s. o. kui $p = \pm 1$. Seega kujutab $\Gamma/\mathfrak{m}$ juhul $p \neq 0$ jäägiklassiringi $R^{(p)}$, nii et isomorfism (7) omab kuju

$$I \overset{+}{\cdot\!\!\leftarrow\!\!\rightarrow} R^{(p)}\,.$$

Et siin I on integriteetkond, siis peab p olema algarv, sest vastasel korral sisaldaks $R^{(p)}$ ja siis ka I nullitegureid. Seepärast

osutub $R^{(p)}$ ja ühtlasi ka I korpuseks. Et aga $I \subset P$, siis peab olema $I = P$, sest P on algkorpus. Seega

$$P \overset{+}{\underset{\cdot}{\longleftrightarrow}} R^{(p)}.$$

2⁰ Kui $p = 0$, siis kujutab $\Gamma/\mathfrak{m}$ integriteetkonda Γ ennast, nii et isomorfism (7) omab siin kuju

$$I \overset{+}{\underset{\cdot}{\longleftrightarrow}} \Gamma.$$

Kasutame nüüd lauset, mille järgi iga integriteetkonda võib laiendada korpuseks — selle integriteetkonna jagatistekorpuseks (I, § 9, art. 3). Märkides I jagatistekorpuse K-ga ja Γ jagatistekorpuse, s. o. ratsionaalarvude korpuse $R^{(0)}$-ga, ei ole raske näidata [1], et

$$K \overset{+}{\underset{\cdot}{\longleftrightarrow}} R^{(0)}.$$

Et aga $K \subset P$, siis peab olema $K = P$, sest P on algkorpus. Seega

$$P \overset{+}{\underset{\cdot}{\longleftrightarrow}} R^{(0)}.$$

Niisiis leidub vaid kahte tüüpi algkorpusi: ühed, mis on isomorfsed mingi jäägiklassikorpusega $R^{(p)}$, ja teised, mis on isomorfsed ratsionaalarvude korpusega $R^{(0)}$. Et $R^{(p)}$ karakteristika on p ja $R^{(0)}$ karakteristika 0 (§ 7, art. 1), siis on esimest tüüpi algkorpuste karakteristika p ja teist tüüpi algkorpuste karakteristika 0. Seega on algkorpuse tüüp täielikult määratud korpuse karakteristikaga.

Olles tutvunud algkorpuste tüüpidega, s. o. lihtsaimate korpuste tüüpidega, peatume järgnevas artiklis kaasaegse algebra looja Steinitzi eeskujul nende meetodite juures, mis lubavad tuletada igast antud korpusest viimase laiendamise teel uusi, ulatuslikumaid korpusi.

2. Korpuse laiendamine. Olgu antud mingi põhikorpus K. Iga korpust L, mille suhtes K on alamkorpuseks, nimetame K ülemkorpuseks ehk laiendiks. Olgu ülemkorpuses L antud mingi

[1] Vt. § 26, art. 1.

hulk M. Vaatleme neid L-i alamkorpusi, mis sisaldavad põhikorpust K ja hulka M, ja märgime kõigi niisuguste alamkorpuste ühisosa sümboliga $K(M)$. Paneme tähele, et $K(M)$ on koosseisult väikseim korpus, mis sisaldab põhikorpust K ja hulka M, kusjuures

$$K \subset K(M) \subset L.$$

Öeldakse, et laiend $K(M)$ on saadud põhikorpusest K hulga M adjungeerimisel. Anname laiendile $K(M)$ veel teise tõlgitsuse.

Et $K(M)$ sisaldab kõiki K ja M-i elemente, siis peab $K(M)$ kui korpus sisaldama ka kõiki neid elemente, mis saadakse K ja M-i elementidest ratsionaaloperatsioonide teel, s. o. liitmise, lahutamise, korrutamise ja jagamise teel. Moodustagu kõik need elemendid, mis saadakse K ja M-i elementidest ratsionaaloperatsioonide teel, hulga Δ, nii et

$$\Delta \subset K(M).$$

Ei ole raske näha, et Δ on korpus. Nimelt kui $a \in \Delta$ ja $b \in \Delta$, siis ka

$$a - b \in \Delta, \quad \frac{a}{b} \in \Delta,$$

sest kui a ja b saadakse K ja M-i elementidest ratsionaaloperatsioonide teel, siis saadakse ka $a - b$ ja $\frac{a}{b}$ K ja M-i elementidest ratsionaaloperatsioonide teel. Et Δ sisaldab põhikorpust K ja hulka M, kuid $K(M)$ on koosseisult väikseim korpus, mis sisaldab põhikorpust K ja hulka M, siis peab olema

$$K(M) \subset \Delta.$$

Seega $K(M) = \Delta$. Niisiis võime öelda, et *laiend $K(M)$ koosneb kõikidest nendest M-i elementide ratsionaalsetest avaldistest, mille kordajateks on K elemendid.*

Vaatleme nüüd laiendis L kahte hulka M_1 ja M_2. Adjungeerides põhikorpusele K hulga M_1 ja siis tulemusele $K(M_1)$ veel hulga M_2, saame laiendi $K(M_1)(M_2)$. Osutub, et niisugust

kahekordset adjungeerimist võib asendada ühe hulga adjungeerimisega, nimelt hulkade M_1 ja M_2 summa adjungeerimisega, s. o.

$$K(M_1)(M_2) = K(M_1 + M_2). \tag{8}$$

Valemi (8) tõestuseks paneme tähele, et $K(M_1)(M_2)$ sisaldab laiendit $K(M_1)$ ja hulka M_2, kusjuures $K(M_1)$ sisaldab omakorda põhikorpust K ja hulka M_1, nii et $K(M_1)(M_2)$ peab sisaldama põhikorpust K ja summat $M_1 + M_2$. Seega sisaldab $K(M_1)(M_2)$ laiendit $K(M_1 + M_2)$, s. o.

$$K(M_1)(M_2) \supset K(M_1 + M_2).$$

Ümberpöördult, $K(M_1 + M_2)$, sisaldades põhikorpust K ja summat $M_1 + M_2$, sisaldab põhikorpust K ja mõlemaid hulki M_1, M_2. Siis sisaldab $K(M_1 + M_2)$ aga ka laiendit $K(M_1)$ ja hulka M_2 ja siis ka laiendit $K(M_1)(M_2)$, s. o.

$$K(M_1 + M_2) \supset K(M_1)(M_2).$$

Viimasest kahest seosest järeldubki valem (8).

Rakendades täieliku induktsiooni printsiipi, saab kergesti näidata, et üldiselt

$$K(M_1)(M_2)\ldots(M_n) = K(M_1 + M_2 + \ldots + M_n). \tag{9}$$

Valemist (9) nähtub eriti, et hulkade M_1, M_2, ..., M_n adjungeerimisel ei ole oluline nende hulkade järjekord.

Käesolevas kursuses piirdume juhuga, kus adjungeeritav hulk M on lõplik, koosnedes n elemendist ξ_1, ξ_2, ..., ξ_n, s. o. $M = \{\xi_1, \xi_2, \ldots, \xi_n\}$. Vastavat laiendit $K(M)$ märgime sel juhul lihtsalt sümboliga

$$K(\xi_1, \xi_2, \ldots, \xi_n).$$

Rakendades siin valemit (9), saame

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

s. o. *lõpliku hulga adjungeerimine taandub selle hulga üksikute elementide adjungeerimisele.* Niisugust laiendit $K(\xi)$, mis saa-

dakse üheainsa elemendi ξ adjungeerimisel korpusele K, nimetatakse K lihtlaiendiks, kusjuures ξ kannab selle lihtlaiendi moodustava elemendi nime. Nii kujutab näiteks ratsionaalfunktsioonide korpus $K(x)$ põhikorpuse K lihtlaiendit, mis on saadud algebralise muutuja x adjungeerimisel.

Laiendi $K(M)$ uurimisel on teinekord otstarbekas vaadelda ainult neid elemente, mis saadakse K ja M-i elementidest täisratsionaalsete operatsioonide teel, s. o. liitmise, lahutamise ja korrutamise teel. Kõik niisugused elemendid, mis saadakse K ja M-i elementidest täisratsionaalsete operatsioonide teel, moodustavad hulga, mida märgitakse sümboliga $K[M]$. Võib öelda, et $K[M]$ *koosneb kõikidest nendest M-i elementide täisratsionaalsetest avaldistest, mille kordajateks on K elemendid.* Näiteks kui M koosneb algebralisest muutujast x, siis kujutab $K[M]$ polünoomkonda $K[x]$.

Analoogiliselt eelnenuga saab näidata, et $K[M]$ on ring ja nimelt ühikuga ring, sest, sisaldades K-d, sisaldab $K[M]$ ka ühikelementi. Veel enam, ringis $K[M]$ kui korpuse $K(M)$ osahulgas puuduvad nullitegurid. Teiste sõnadega, $K[M]$ on integriteetkond.

Erijuhul, kui $K[M]$ osutub korpuseks, langeb ta ühte laiendiga $K(M)$, s. o.

$$K[M] = K(M),$$

sest vastasel korral kujutaks $K[M]$ korpust, mis sisaldab põhikorpust K ja hulka M, ja mis on seejuures koosseisult väiksem kui $K(M)$, vastuolus laiendi $K(M)$ mõistega.

Olgu näiteks K ratsionaalarvude korpus ja L reaalarvude korpus. Võtame korpuses L irratsionaalarvu $\sqrt{u}$, kus u tähendab mitteruutarvu, ja vaatleme integriteetkonda $K[\sqrt{u}]$. Siin $K[\sqrt{u}]$ koosneb täisratsionaalsetest avaldistest

$$a_0 + a_1\sqrt{u} + a_2(\sqrt{u})^2 + \ldots + a_n(\sqrt{u})^n,$$

kus kordajad a_0, a_1, a_2, ..., a_n on ratsionaalarvud. Ei ole

raske näha, et neile avaldistele saab anda pärast astendamist ja liikmete rühmitamist kuju

$$a + b\sqrt{u},$$

kus a ja b tähendavad ratsionaalarve. Seega

$$K[\sqrt{u}] = \{a + b\sqrt{u}\},$$

kus $\{a + b\sqrt{u}\}$ kujutab korpust (art. 1), mistõttu

$$K[\sqrt{u}] = K(\sqrt{u}).$$

3. Lihtlaiendid. Olgu antud põhikorpus K, ülemkorpus L ja mingi element ξ ülemkorpuses L. Seame endale ülesandeks leida kõik lihtlaiendite $K(\xi)$ tüübid, nii nagu leidsime artiklis 1 kõik algkorpuste tüübid. Vaatleme selleks $K(\xi)$ asemel integriteetkonda $K[\xi]$, mis koosneb kõigist täisratsionaalsetest avaldistest

$$a_0 + a_1\xi + a_2\xi^2 + \ldots + a_n\xi^n,$$

kus kordajad a_0, a_1, a_2, $\ldots$, a_n tähendavad põhikorpuse K elemente. Ei ole raske näha, et $K[\xi]$ on homomorfne polünoomkonnaga $K[x]$. Nimelt, korraldades $K[x]$ ja $K[\xi]$ vahel vastavuse

$$f(x) \longrightarrow f(\xi), \quad g(x) \longrightarrow g(\xi),$$

kus

$$\begin{aligned} f(x) &= a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \\ f(\xi) &= a_0 + a_1\xi + a_2\xi^2 + \ldots + a_n\xi^n \\ g(x) &= b_0 + b_1x + b_2x^2 + \ldots + b_mx^m \\ g(\xi) &= b_0 + b_1\xi + b_2\xi^2 + \ldots + b_m\xi^m, \end{aligned}$$

leiame polünoomide summa ja korrutise mõistet silmas pidades

$$\begin{aligned} f(x) + g(x) \rightarrow (a_0 + b_0) + (a_1 + b_1)\xi + (a_2 + b_2)\xi^2 + \ldots = \\ = f(\xi) + g(\xi), \\ f(x) \cdot g(x) \rightarrow a_0b_0 + (a_0b_1 + a_1b_0)\xi + \\ + (a_0b_2 + a_1b_1 + a_2b_0)\xi^2 + \ldots = f(\xi)g(\xi), \end{aligned}$$

mis ütlebki, et

$$K[x] \overset{+}{\cdot\!\!\rightarrow} K[\xi]. \tag{10}$$

Rakendades teoreemi 6 ringi homomorfismidest (§ 24, art. 4), võime kirjutada, et

$$K[\xi] \overset{+}{\cdot\!\!\leftrightarrow} K[x]/\mathfrak{m}, \tag{11}$$

kus ideaal $\mathfrak{m}$ koosneb kõigist neist polünoomidest üle K, millele vastab homomorfismis (10) $K[\xi]$ nullelement, s. o. kõigist niisugustest polünoomidest $f(x)$, mille puhul $f(\xi) = 0$. Silmas pidades, et $K[x]$ kujutab teoreemi 1 järgi peaideaaliringi (§ 24, art. 3), peab eriti ka $\mathfrak{m}$ olema peaideaal, nii et

$$\mathfrak{m} = (p(x)).$$

Vaatleme eraldi kahte juhtu selle järgi, kas $p(x) \neq 0$ või $p(x) = 0$.

1° Kui $p(x) \neq 0$, siis peab olema $p(x)$ aste suurem kui 0, sest kuna ideaal $\mathfrak{m} = (p(x))$ sisaldab eriti ka polünoomi $p(x)$, siis on $p(\xi) = 0$, mis oleks võimatu, kui $p(x)$ on konstant. Seega kujutab $K[x]/\mathfrak{m}$ juhul $p(x) \neq 0$ jäägiklassiringi $R^{(p(x))}$, nii et isomorfism (11) omab kuju

$$K[\xi] \overset{+}{\cdot\!\!\leftrightarrow} R^{(p(x))}.$$

Et siin $K[\xi]$ on integriteetkond, siis peab $p(x)$ olema taandumatu korpuses K, sest vastasel korral sisaldaks $R^{(p(x))}$ ja siis ka $K[\xi]$ nullitegureid. Seepärast osutub $R^{(p(x))}$ ja ühtlasi ka $K[\xi]$ korpuseks, mistõttu $K[\xi] = K(\xi)$ ja seega

$$K(\xi) \overset{+}{\cdot\!\!\leftrightarrow} R^{(p(x))}.$$

2° Kui $p(x) = 0$, siis kujutab $K[x]/\mathfrak{m}$ polünoomkonda $K[x]$ ennast, nii et isomorfism (11) omab siin kuju

$$K[\xi] \overset{+}{\cdot\!\!\leftrightarrow} K[x].$$

Laiendades integriteetkonnad $K[\xi]$ ja $K[x]$ jagatistekorpusteks,

saame vastavalt lihtlaiendi $K(\xi)$ ja ratsionaalfunktsioonide korpuse $K(x)$, kusjuures [1]

$$K(\xi) \overset{+}{\longleftrightarrow} K(x).$$

Niisiis on põhikorpuse K lihtlaiendid kahte tüüpi: ühed, mis on isomorfsed mingi jäägiklassikorpusega $R^{(p(x))}$, ja teised, mis on isomorfsed ratsionaalfunktsioonide korpusega üle K. Et ideaal $\mathfrak{m} = (p(x))$ koosneb kõigist neist polünoomidest $f(x)$, mille puhul $f(\xi) = 0$, siis rahuldab esimest tüüpi lihtlaiendi $K(\xi)$ moodustav element ξ algebralist võrrandit $p(x) = 0$, kuna teist tüüpi lihtlaiendi moodustav element ei rahulda mingit algebralist võrrandit üle K. Niisugust ülemkorpuse L elementi ξ, mis rahuldab teatavat algebralist võrrandit üle K, nimetatakse algebraliseks elemendiks K suhtes, ja vastavat lihtlaiendit $K(\xi)$ algebraliseks lihtlaiendiks. Seevastu niisugust ülemkorpuse L elementi ξ, mis ei rahulda ühtki algebralist võrrandit üle K, nimetatakse transtsendentseks elemendiks K suhtes, ja vastavat lihtlaiendit $K(\xi)$ transtsendentseks lihtlaiendiks. Erijuhul, kui K on ratsionaalarvude korpus ja L kompleksarvude korpus, kõneldakse vastavalt algebralistest ja transtsendentsetest arvudest.

Peatume kõigepealt lähemalt algebraliste lihtlaiendite juures. Igale algebralisele lihtlaiendile $K(\xi)$ vastab, nagu nägime, korpuses K taandumatu polünoom $p(x)$, mille lahendiks on ξ. Ei ole raske näha, et $p(x)$ on kuni konstantse tegurini määratud kui ainuke taandumatu (madalaima astme) polünoom, mille lahendiks on ξ. Tõepoolest iga polünoom $f(x)$, mille lahendiks on ξ, peab kuuluma ideaali $\mathfrak{m} = (p(x))$, omades seega kuju

$$f(x) = p(x)r(x),$$

kus $r(x)$ tähendab teatavat polünoomi üle K. Et aga $f(x)$ on taandumatu (madalaima astme) polünoom ideaalis $\mathfrak{m}$, siis peab $r(x)$ olema konstant. Polünoom $p(x)$ kannab algebralise liht-

[1] Vt. § 26, art. 1.

laiendi $K(\xi)$ määrava polünoomi nime. Ümberpöördult, vastavalt igale korpuses K taandumatule polünoomile $p(x)$ võime alati konstrueerida niisuguse algebralise lihtlaiendi $K(\xi)$, millele $p(x)$ on määravaks polünoomiks. Selleks tarvitseb vaid võtta ξ-ks polünoomi $p(x)$ mingi lahend, mis polünoomide algebra põhilause järgi alati eksisteerib vastavalt polünoomile $p(x)$ konstrueeritud ülemkorpuses (§ 5, art. 3).

Olgu algebralise lihtlaiendi $K(\xi)$ määrava polünoomi $p(x)$ aste k. Nagu nägime, leiab aset isomorfism

$$K(\xi) \overset{+}{\longleftrightarrow} R^{(p(x))},$$

kusjuures selle isomorfismi saame, seades $K(\xi)$ elemendile $f(\xi)$ vastavusse $R^{(p(x))}$ elemendi $f(x)$. Siin $f(x)$ avaldub alati ülimalt $(k-1)$-astme polünoomina, mistõttu $K(\xi)$ iga elementi Θ võib avaldada ξ kaudu kujul

$$\Theta = a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{k-1}\xi^{k-1},$$

kus a_0, a_1, a_2, $\ldots$, a_{k-1} on kindlad põhikorpuse K elemendid.

Et $R^{(p(x))}$ kujutab k-järku algebrat üle K, siis peab $K(\xi)$ iga element Θ rahuldama ülimalt k-astme algebralist võrrandit

$$c_0 + c_1x + c_2x^2 + \ldots + c_kx^k = 0$$

üle K (§ 3, art. 2). Tähendab, *algebralise lihtlaiendi iga element on algebraline põhikorpuse suhtes.* Üldse nimetatakse iga laiendit, mille kõik elemendid on algebralised põhikorpuse suhtes, algebraliseks laiendiks.

Vaatleme kõiki algebralisi võrrandeid üle K, mida rahuldab mingi $K(\xi)$ element Θ. Jättes kõrvale konstantse teguri, peab nende võrrandite hulgas, nagu nägime, leiduma üks, mis on taandumatu põhikorpuses K ja ühtlasi madalaima astmega. Selle võrrandi astet nimetatakse elemendi Θ astmeks K suhtes ja märgitakse sümboliga $(\Theta : K)$. Nii on näiteks irratsionaalarvu $\Theta = \sqrt[3]{1+\sqrt{3}}$ aste ratsionaalarvude korpuse suhtes 6, sest kuna

$$\Theta^3 = 1 + \sqrt{3}, \quad \Theta^3 - 1 = \sqrt{3}, \quad \Theta^6 - 2\Theta^3 + 1 = 3,$$

siis rahuldab Θ 6-nda astme võrrandit

$$x^6 - 2x^3 - 2 = 0,$$

mis on Eisensteini teoreemi järgi taandumatu ratsionaalarvude korpuses (§ 8, art. 2). Erijuhul, kui Θ kuulub põhikorpusse K, on $(\Theta : K) = 1$, sest Θ rahuldab siin võrrandit $x - \Theta = 0$ üle K.

Et $K(\xi)$ iga element Θ rahuldab ülimalt k-astme võrrandit, siis on

$$(\Theta : K) \leqslant k.$$

Teiselt poolt on $(\xi : K) = k$, sest ξ rahuldab võrrandit $p(x) = 0$. Tekib küsimus, missugusel tingimusel on

$$(\Theta : K) = k.$$

Vastuse sellele annab alljärgnev teoreem.

Teoreem 8. *Algebralise lihtlaiendi $K(\xi)$ mingi elemendi Θ aste K suhtes on võrdne moodustava elemendi ξ astmega siis ja ainult siis, kui $K(\Theta) = K(\xi)$.*

Teoreemi 8 tõestuseks oletame kõigepealt, et

$$(\Theta : K) = k.$$

Siis Θ ei rahulda mingit tingimust

$$c_0 + c_1\Theta + c_2\Theta^2 + \ldots + c_{k-1}\Theta^{k-1} = 0,$$

kus kordajad $c_0, c_1, c_2, \ldots, c_{k-1}$ ei ole kõik korraga nullid. Teiste sõnadega, astmed $\Theta^0 = e, \Theta, \Theta^2, \ldots, \Theta^{k-1}$ on lineaarselt sõltumatud üle K. Need astmed kui $K(\xi)$ elemendid avalduvad aga kujul

$$\begin{aligned}
&\Theta^0 = e \\
&\Theta = a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{k-1}\xi^{k-1} \\
&\Theta^2 = b_0 + b_1\xi + b_2\xi^2 + \ldots + b_{k-1}\xi^{k-1} \qquad (12) \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&\Theta^{k-1} = l_0 + l_1\xi + l_2\xi^2 + \ldots + l_{k-1}\xi^{k-1}.
\end{aligned}$$

Seosed (12) moodustavad $\xi^0 = e, \xi, \xi^2, \ldots, \xi^{k-1}$ suhtes lineaarse

võrrandisüsteemi, mille determinant peab olema nullist erinev, sest vastasel korral oleksid võrrandite (12) paremad pooled ja siis ka vabaliikmed $\Theta^0, \Theta, \Theta^2, \ldots, \Theta^{k-1}$ lineaarselt sõltuvad. Arvutades süsteemist (12) Crameri valemite järgi tundmatu ξ, ei ole raske näha, et ξ avaldub vabaliikmete $\Theta^0, \Theta, \Theta^2, \ldots, \Theta^{k-1}$ lineaarse kombinatsioonina:

$$\xi = d_0 + d_1\Theta + d_2\Theta^2 + \ldots + d_{k-1}\Theta^{k-1},$$

kus kordajad $d_0, d_1, d_2, \ldots, d_{k-1}$ kuuluvad põhikorpusse K. Siit nähtub, et ξ kuulub laiendisse $K(\Theta)$, mille moodustavaks elemendiks on Θ. Seega

$$K(\xi) \subset K(\Theta).$$

Teiselt poolt kuulub Θ laiendisse $K(\xi)$, mistõttu

$$K(\Theta) \subset K(\xi).$$

Viimasest kahest seosest järeldub võrdus

$$K(\Theta) = K(\xi).$$

Ümberpöördult, kui $K(\Theta) = K(\xi)$, siis kuulub Θ laiendisse $K(\xi)$ ja seega

$$(\Theta : K) \leqslant k;$$

samuti kuulub siis ξ laiendisse $K(\Theta)$, mistõttu

$$k \leqslant (\Theta : K).$$

Järelikult $(\Theta : K) = k$, millega on teoreem 8 täielikult tõestatud.

Võrdus $K(\Theta) = K(\xi)$ ütleb, et Θ on ka laiendi $K(\xi)$ moodustav element. Niisiis on teoreemi 8 põhjal algebralise lihtlaiendi kõigil moodustavatel elementidel üks ja sama aste k. Seda moodustavate elementide ühist astet nimetatakse lihtlaiendi $K(\xi)$ astmeks K suhtes ja märgitakse sümboliga $(K(\xi) : K)$. Seega $(K(\xi) : K) = k$.

Tulles transtsendentsete lihtlaiendite juurde, näitame, et *transtsendentse lihtlaiendi kõik elemendid, välja arvatud põhikorpuse omad, on transtsendentsed põhikorpuse suhtes.*

Viimase väite tõestuseks vaatleme mingit transtsendentse lihtlaiendi $K(\xi)$ nullist erinevat elementi $\Theta = \frac{f(\xi)}{g(\xi)}$. Isomorfismi

$$K(\xi) \overset{+}{\longleftrightarrow} K(x)$$

tõttu käitub Θ nagu ratsionaalfunktsioon $\frac{f(x)}{g(x)}$. Oletame, et Θ on algebraline element K suhtes, s. o. et

$$c_0 + c_1\Theta + c_2\Theta^2 + \ldots + c_n\Theta^n = 0, \tag{13}$$

kus $c_n \neq 0$. Siinjuures võime üldsust kitsendamata eeldada, et ka vabaliige $c_0 \neq 0$, sest kui oleks üldiselt

$$c_0 = 0, \quad c_1 = 0, \quad \ldots, \quad c_{k-1} = 0, \quad c_k \neq 0,$$

siis rahuldaks Θ tingimust

$$c_k\Theta^k + c_{k+1}\Theta^{k+1} + \ldots + c_n\Theta^n = 0$$

ehk

$$c_k + c_{k+1}\Theta + \ldots + c_n\Theta^{n-k} = 0,$$

kus nüüd vabaliige $c_k \neq 0$.

Asetame võrduses (13) Θ asemel $\frac{f(\xi)}{g(\xi)}$, kusjuures eeldame, et murd $\frac{f(\xi)}{g(\xi)}$ on taandatud, nii et $(f, g) = e$. Pärast nimetajatest vabanemist leiame

$$c_0 g^n(\xi) + c_1 g^{n-1}(\xi) f(\xi) + \ldots + c_{n-1} g(\xi) f^{n-1}(\xi) + c_n f^n(\xi) = 0,$$

millest, ühelt poolt

$$f(\xi)\,[c_n f^{n-1}(\xi) + c_{n-1} g(\xi) f^{n-2}(\xi) + \ldots + c_1 g^{n-1}(\xi)] = -c_0 g^n(\xi)$$

ja, teiselt poolt

$$g(\xi)\,[c_0 g^{n-1}(\xi) + c_1 f(\xi) g^{n-2}(\xi) + \ldots + c_{n-1} f^{n-1}(\xi)] = \\ = -c_n f^n(\xi).$$

Siin eelviimasest võrdusest nähtub, et $g^n(\xi)$ jagub $f(\xi)$-ga. Et aga $(f, g) = e$, siis võib $g^n(\xi)$ jaguda $f(\xi)$-ga ainult sel korral, kui $f(\xi)$ osutub konstandiks, s. o. $f(\xi) = a$. Täpselt samuti saab järeldada viimasest võrdusest, et ka $g(\xi)$ osutub konstandiks, s. o. $g(\xi) = b$. Seega $\Theta = \frac{a}{b}$, millest nähtub, et Θ kujutab põhikorpuse K elementi. Tähendab, transtsendentses lihtlaiendis on ainult põhikorpuse elemendid algebralised.

Üldse nimetatakse iga laiendit, milles leidub põhikorpuse suhtes transtsendentseid elemente, transtsendentseks laiendiks.

§ 26. Polünoomi lahutuskorpus.

1. Lahutuskorpuse ühesus. Algebraliste laiendite hulgas etendavad erilist osa niisugused laiendid, mis saadakse antud polünoomi $f(x)$ lahendite adjungeerimisel põhikorpusele K.

Definitsioon 3. Laiendit $\Delta = K(\xi_1, \xi_2, \ldots, \xi_n)$, mis saadakse põhikorpusest K polünoomi $f(x)$ lahendite $\xi_1, \xi_2, \ldots, \xi_n$ adjungeerimisel, nimetatakse polünoomi $f(x)$ lahutuskorpuseks K suhtes.

Lahutuskorpuses Δ laguneb polünoom $f(x)$ seega lineaartegurite korrutiseks:

$$f(x) = a_0(x - \xi_1)(x - \xi_2) \ldots (x - \xi_n), \tag{14}$$

kus a_0 on $f(x)$ pealiikme kordaja. Lahutuskorpuse Δ leidmiseks tuleb algul konstrueerida mingi niisugune ülemkorpus L, kus $f(x)$ laguneb lineaartegurite korrutiseks (14) (§ 5, art. 3) ja adjungeerida siis põhikorpusele K ülemkorpuse L elemendid $\xi_1, \xi_2, \ldots, \xi_n$. Et ülemkorpust L võib väga mitmel viisil konstrueerida, sellepärast tekib küsimus, kuivõrd on lahutuskorpus Δ üldse üheselt määratud ja kas mitte $f(x)$ lahendite omadused ei sõltu ülemkorpuse L konstrueerimise viisist. Selle küsimuse selgitamiseks toome sisse nn. isomorfismi jätku mõiste.

Definitsioon 4. Kui põhikorpus K on isomorfses vastavuses korpusega K ja K laiend Δ korpuse $\bar{K}$ laiendiga $\bar{\Delta}$, siis nimetatakse laiendite isomorfismi $\Delta \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{\Delta}$ põhikorpuste isomorfismi $K \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{K}$ jätkuks, kui põhikorpuse K igale elemendile a vastab laiendite isomorfismis $\Delta \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{\Delta}$ sama element $\bar{a}$ mis põhikorpuste isomorfismis $K \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{K}$.

Teiste sõnadega, laiendite isomorfism kujutab põhikorpuste isomorfismi jätku, kui laiendite isomorfismis säilib põhikorpuste isomorfism. Olgu tähendatud, et isomorfismi jätkust kõneldakse üldiselt ka mistahes põhipiirkondade — ringi, korpuse, integriteetkonna — ja mistahes laiendite puhul. Näitame, et iga integriteetkondade isomorfismi $I \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{I}$ saab jätkata vastavate jagatistekorpuste isomorfismini $K \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{K}$ (I, § 9, art. 3) ja mistahes põhipiirkondade isomorfismi $P \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{P}$ vastavate polünoomkondade isomorfismini $P[x] \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{P}[x]$ (I, § 10, art. 1).

Väite esimese osa tõestuseks seame jagatistekorpuse K elemendile $a = \frac{a}{b}$ vastavusse jagatistekorpuse $\bar{K}$ elemendi $\bar{a} = \frac{\bar{a}}{\bar{b}}$, kus $\bar{a}$ tähendab a-le ja $\bar{b}$ b-le vastavat elementi integriteetkondade isomorfismis $I \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{I}$. Toetudes integriteetkonna jagatistekorpuses kehtivaile võrdusele ja tehetele, ei ole raske näidata, et $K \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{K}$. Erijuhul, kui $b = e$, on $\bar{b} = \bar{e}$ ja seega vastab isomorfismis $K \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{K}$ I elemendile $a = a$ $\bar{I}$ element $\bar{a} = \bar{a}$, nii nagu see oli integriteetkondade isomorfismis $I \overset{+}{\underset{\cdot}{\longleftrightarrow}} \bar{I}$.

Väite teise osa tõestuseks seame $P[x]$ polünoomile $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ vastavusse $\bar{P}[x]$ polünoomi $\bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \bar{a}_2 x^2 + \ldots + \bar{a}_n x^n$, kus $\bar{a}_i$ tähendab a_i-le vas-

tavat elementi põhipiirkondade isomorfismis $P \overset{+}{\longleftrightarrow} \bar{P}$. Toetudes polünoomkonnas kehtivaile võrdusele ja tehetele ei ole raske näidata, et $P[x] \overset{+}{\longleftrightarrow} \bar{P}[x]$. Erijuhul, kui $a_1 = 0$, $a_2 = 0$, ..., $a_n = 0$, ka $\bar{a}_1 = 0$, $\bar{a}_2 = 0$, ..., $\bar{a}_n = 0$ ja seega vastab isomorfismis $P[x] \overset{+}{\longleftrightarrow} \bar{P}[x]$ P elemendile $f(x) = a_0$ $\bar{P}$ element $\bar{f}(x) = \bar{a}_0$, nii nagu see oli põhipiirkondade isomorfismis $P \overset{+}{\longleftrightarrow} \bar{P}$.

Tõestame kaks põhilise tähtsusega teoreemi algebraliste laiendite isomorfismi jätku kohta, millega saame ühtlasi vastuse polünoomi lahutuskorpuse ühesuse küsimusele.

Teoreem 9. *Põhikorpuste isomorfismi* $K \overset{+}{\longleftrightarrow} \bar{K}$ *võib jätkata algebraliste lihtlaiendite isomorfismini*

$$K(\xi) \overset{+}{\longleftrightarrow} \bar{K}(\bar{\xi}),$$

nii et seejuures ξ*-le vastab* $\bar{\xi}$*, kus* $\bar{\xi}$ *on* $K(\xi)$ *määravale polünoomile* $p(x)$ *isomorfismis*[1] $K[x] \overset{+}{\longleftrightarrow} \bar{K}[x]$ *vastava polünoomi* $\bar{p}(x)$ *lahend.*

Teoreemi 9 tõestuseks peame silmas, et $K(\xi)$ iga element avaldub kujul

$$f(\xi) = a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{k-1}\xi^{k-1},$$

kus k tähendab polünoomi $p(x)$ astet ja kordajad a_i kuuluvad põhikorpusse K. Et $p(x)$-le vastava polünoomi $\bar{p}(x)$ aste on samuti k, siis avaldub $\bar{K}(\bar{\xi})$ iga element kujul

$$\bar{f}(\bar{\xi}) = \bar{a}_0 + \bar{a}_1\bar{\xi} + \bar{a}_2\bar{\xi}^2 + \ldots + \bar{a}_{k-1}\bar{\xi}^{k-1},$$

kus kordajad $\bar{a}_i$ kuuluvad põhikorpusse $\bar{K}$. Seades $K(\xi)$ elemendile $f(\xi)$ vastavusse $\bar{K}(\bar{\xi})$ elemendi $\bar{f}(\bar{\xi})$, võttes kordajaiks

[1] See polünoomkondade isomorfism on põhikorpuste isomorfismi poolt esile kutsutud eespool näidatud viisil.

$\bar{a}_i$ kordajaile a_i vastavad elemendid põhikorpuste isomorfismis $K \overset{+}{\longleftrightarrow} \bar{K}$, saame ilmselt üksühese vastavuse

$$f(\xi) \longleftrightarrow \bar{f}(\bar{\xi}),$$

kusjuures saab näidata, et see vastavus säilib tehete puhul. Nimelt kui

$$g(\xi) = b_0 + b_1\xi + b_2\xi^2 + \ldots + b_{k-1}\xi^{k-1}$$

on veel mingi $K(\xi)$ element ja

$$g(\xi) \longleftrightarrow \bar{g}(\bar{\xi}),$$

kus

$$\bar{g}(\bar{\xi}) = \bar{b}_0 + \bar{b}_1\bar{\xi} + \bar{b}_2\bar{\xi}^2 + \ldots + \bar{b}_{k-1}\bar{\xi}^{k-1},$$

siis ei ole raske näha, et

$$f(\xi) + g(\xi) \longleftrightarrow (\overline{a_0 + b_0}) + (\overline{a_1 + b_1})\bar{\xi} + (\overline{a_2 + b_2})\bar{\xi}^2 + \ldots + (\overline{a_{k-1} + b_{k-1}})\bar{\xi}^{k-1} = \bar{f}(\bar{\xi}) + \bar{g}(\bar{\xi}).$$

Mis puutub korrutisse $f(\xi)g(\xi)$, siis on

$$f(\xi)g(\xi) = r_0 + r_1\xi + r_2\xi^2 + \ldots + r_{k-1}\xi^{k-1} = r(\xi),$$

kus $r(\xi)$ tähendab jääki, mis saadakse $f(\xi)g(\xi)$ kui polünoomide korrutise jagamisel $p(\xi)$-ga. Analoogiliselt

$$\bar{f}(\bar{\xi})\bar{g}(\bar{\xi}) = \bar{r}_0 + \bar{r}_1\bar{\xi} + \bar{r}_2\bar{\xi}^2 + \ldots + \bar{r}_{k-1}\bar{\xi}^{k-1} = \bar{r}(\bar{\xi}),$$

kus $\bar{r}(\bar{\xi})$ tähendab jääki, mis saadakse $\bar{f}(\bar{\xi})\bar{g}(\bar{\xi})$ kui polünoomide korrutise jagamisel $\bar{p}(\bar{\xi})$-ga. Et $\bar{f}(\bar{\xi})$, $\bar{g}(\bar{\xi})$ ja $\bar{p}(\bar{\xi})$ kordajad kujutavad $f(\xi)$, $g(\xi)$ ja $p(\xi)$ kordajatele vastavaid elemente põhikorpuste isomorfismis, siis osutub ka iga $\bar{r}_i$ selles isomorfismis r_i-le vastavaks elemendiks. Seega

$$f(\xi)g(\xi) \longleftrightarrow \bar{f}(\bar{\xi})\bar{g}(\bar{\xi}),$$

mistõttu korraldatud vastavus kujutab isomorfismi

$$K(\xi) \overset{+}{\longleftrightarrow} \bar{K}(\bar{\xi}),$$

kus ξ-le vastab ilmselt $\bar{\xi}$. Erijuhul, kui $a_1 = 0$, $a_2 = 0$, ..., $a_{k-1} = 0$, ka $\bar{a}_1 = 0$, $\bar{a}_2 = 0$, ..., $\bar{a}_{k-1} = 0$, nii et isomorfismis $K(\xi) \overset{+}{\longleftrightarrow} \bar{K}(\bar{\xi})$ vastab K elemendile $f(\xi) = a_0$ $\bar{K}$ element $\bar{f}(\bar{\xi}) = \bar{a}_0$, nagu see oli põhikorpuste isomorfismis.

Teeme teoreemist 9 ühe järelduse, vaadeldes erijuhtu, kus põhikorpuste isomorfism taandub identseks automorfismiks $K \overset{+}{\longleftrightarrow} K$, nii et K igale elemendile vastab see element ise. Sel korral on $\bar{p}(x) = p(x)$, mistõttu ξ ja $\bar{\xi}$ tähendavad ühe ja sama taandumatu polünoomi $p(x)$ lahendeid. Seega ütleb siin teoreem 9, et taandumatu polünoomi $p(x)$ lahenditele ξ ja $\bar{\xi}$ vastavate lihtlaiendite $K(\xi)$ ja $K(\bar{\xi})$ vahel saab korraldada niisuguse isomorfse vastavuse, kus põhikorpuse K elemendid jäävad invariantseks ja kus ξ-le vastab $\bar{\xi}$.

D e f i n i t s i o o n 5. Kui põhikorpuse K laiendite Δ_1 ja Δ_2 vahel saab korraldada niisuguse isomorfse vastavuse, kus K elemendid jäävad invariantseks, siis nimetatakse laiendeid Δ_1 ja Δ_2 e k v i v a l e n t s e t e k s K s u h t e s.

Laiendite ekvivalentsus tähendab, et iga mõiste ja teoreem, mis seob ühe laiendi elemente põhikorpuse elementidega, kandub automaatselt üle ka ekvivalentsele laiendile, mistõttu võib ekvivalentseid laiendeid pidada põhikorpuse seisukohalt mitteerinevaiks. Ekvivalentsete laiendite kohta öeldakse, et nad on sama t ü ü p i.

Olgu tähendatud, et laiendite ekvivalentsusest kõneldakse ka mistahes põhipiirkondade — ringi, korpuse, integriteetkonna — ja mistahes laiendite puhul. Nii järeldub eespool tõestatud integriteetkondade isomorfismi jätkamise võimalusest jagatistekorpuste isomorfismini, et antud integriteetkonna jagatistekorpused on kõik ekvivalentsed. Samuti järeldub põhipiirkondade isomorfismi jätkamise võimalusest polünoomkondade isomorfismini, et polünoomkonnad üle antud põhipiirkonna on kõik ekvivalentsed. Need tulemused on olúliseks täienduseks teoreemidele 5 (I, § 9, art. 3) ja 6 (I, § 10, art. 1), kus me konstruee-

risime vaid ühe konkreetse jagatistekorpuse, vastavalt polünoomkonna, mis rahuldasid nõutud tingimusi.

Nagu nägime, on ühe ja sama taandumatu polünoomi lahenditele vastavad algebralised lihtlaiendid ekvivalentsed. Mis puutub aga transtsendentsetesse lihtlaienditesse, siis on nad kõik omavahel ekvivalentsed. Nimelt transtsendentse lihtlaiendi $K(\xi)$ puhul on (§ 25, art. 3)

$$K(\xi) \overset{+}{\longleftrightarrow} K(x),$$

kusjuures

$$\frac{f(\xi)}{g(\xi)} \longleftrightarrow \frac{f(x)}{g(x)}.$$

Ei ole raske näha, et siin jääb põhikorpuse K iga element a invariantseks, sest kui $f(\xi) = a$, $g(\xi) = e$, siis ka $f(x) = a$, $g(x) = e$, ja seega omab viimane vastavus kuju

$$a \longleftrightarrow a.$$

Niisiis on iga transtsendentne lihtlaiend $K(\xi)$ ekvivalentne ratsionaalfunktsioonide korpusega, mistõttu on kõik transtsendentsed lihtlaiendid ekvivalentsed ka omavahel.

Tuleme nüüd isomorfismi jätku teise teoreemi juurde, millest järeldubki polünoomi lahutuskorpuse ühesus.

Teoreem 10. *Põhikorpuste isomorfismi* $K \overset{+}{\longleftrightarrow} \bar{K}$ *võib jätkata polünoomide* $f(x)$ *ja* $\bar{f}(x)$ *lahutuskorpuste isomorfismini*

$$K(\xi_1, \xi_2, \ldots, \xi_n) \overset{+}{\longleftrightarrow} \bar{K}(\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_n),$$

nii et seejuures $f(x)$ *lahenditele* ξ_i *vastavad* $f(x)$ *lahendid* $\bar{\xi}_i$, *kus* $\bar{f}(x)$ *on polünoomile* $f(x)$ *isomorfismis*[1] $K[x] \overset{+}{\longleftrightarrow} \bar{K}[x]$ *vastav polünoom.*

Teoreemi 10 tõestuseks lahutame polünoomi $f(x)$ korpuses K taandumatute polünoomide korrutiseks

$$(15)\quad f(x) = (x - \xi_1)(x - \xi_2) \ldots (x - \xi_r) p_1(x) p_2(x) \ldots p_k(x),$$

[1] See polünoomkondade isomorfism on põhikorpuste isomorfismi poolt esile kutsutud eespool näidatud viisil.

kus on eraldi kirjutatud lineaar- ja kõrgema astme tegurid, nii et $\xi_1, \xi_2, \ldots, \xi_r$ tähendavad $f(x)$ neid lahendeid, mis langevad põhikorpusse K. Et põhikorpuste isomorfism $K \overset{+}{\longleftrightarrow} \bar{K}$ kutsub esile polünoomkondade isomorfismi $K[x] \overset{+}{\longleftrightarrow} \bar{K}[x]$, siis vastab $f(x)$ tegureiks lahutusele (15) polünoomi $\bar{f}(x)$ tegureiks lahutus

$$\bar{f}(x) = (x - \bar{\xi}_1)(x - \bar{\xi}_2) \ldots (x - \bar{\xi}_r)\bar{p}_1(x)\bar{p}_2(x) \ldots \bar{p}_k(x),$$

kus $\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_r$ osutuvad $\bar{f}(x)$ lahenditeks, mis langevad põhikorpusse $\bar{K}$. Olgu ξ_{r+1} polünoomi $p_1(x)$ mingi lahend ja $\bar{\xi}_{r+1}$ polünoomi $\bar{p}_1(x)$ lahend. Teoreemi 9 järgi võib siis põhikorpuste isomorfismi $K \overset{+}{\longleftrightarrow} \bar{K}$ jätkata isomorfismini

$$K(\xi_{r+1}) \overset{+}{\longleftrightarrow} \bar{K}(\bar{\xi}_{r+1}), \tag{16}$$

nii et ξ_{r+1}-le vastab $\bar{\xi}_{r+1}$. Laiendis $K(\xi_{r+1}) = K(\xi_1, \xi_2, \ldots, \xi_{r+1})$ laguneb $f(x)$ taandumatute polünoomide korrutiseks

$$f(x) = (x - \xi_1)(x - \xi_2) \ldots (x - \xi_s)q_1(x)q_2(x) \ldots q_l(x), \quad s > r,$$

millele vastab polünoomi $\bar{f}(x)$ tegureiks lahutus

$$\bar{f}(x) = (x - \bar{\xi}_1)(x - \bar{\xi}_2) \ldots (x - \bar{\xi}_s)\bar{q}_1(x)\bar{q}_2(x) \ldots \bar{q}_l(x)$$

laiendis $\bar{K}(\bar{\xi}_{r+1}) = \bar{K}(\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_{r+1})$. Olgu ξ_{s+1} polünoomi $q_1(x)$ mingi lahend ja $\bar{\xi}_{s+1}$ polünoomi $\bar{q}_1(x)$ lahend. Teoreemi 9 järgi võib siis isomorfismi (16) jätkata omakorda isomorfismini

$$K(\xi_{r+1}, \xi_{s+1}) \overset{+}{\longleftrightarrow} \bar{K}(\bar{\xi}_{r+1}, \bar{\xi}_{s+1})$$

jne., kuni jõuame lõppeks otsitava isomorfismini

$$K(\xi_1, \xi_2, \ldots, \xi_n) \overset{+}{\longleftrightarrow} \bar{K}(\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_n).$$

Vaatleme erijuhtu, kus põhikorpuste isomorfism taandub

identseks automorfismiks $K \overset{+}{\longleftrightarrow} K$, nii et K igale elemendile vastab see element ise. Sel korral on $\bar{f}(x) = f(x)$, mistõttu $K(\xi_1, \xi_2, \ldots, \xi_n)$ ja $K(\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_n)$ tähendavad ühe ja sama polünoomi $f(x)$ lahutuskorpusi K suhtes. Seega ütleb siin teoreem 10, et polünoomi $f(x)$ lahutuskorpuste $K(\xi_1, \xi_2, \ldots, \xi_n)$ ja $K(\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_n)$ vahel saab korraldada niisuguse isomorfse vastavuse, kus põhikorpuse K elemendid jäävad invariantseks. Teiste sõnadega, *polünoomi $f(x)$ lahutuskorpused on kõik ekvivalentsed.* Seega on polünoomi lahutuskorpus üheselt määratud kuni ekvivalentsini. Öeldakse, et polünoomi lahutuskorpused on kõik ühte tüüpi.

Erijuhul, kui lahutuskorpused $K(\xi_1, \xi_2, \ldots, \xi_n)$ ja $K(\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_n)$ asetsevad ühes ja samas ülemkorpuses L, siis langevad need lahutuskorpused ühte. Tõepoolest, ülemkorpuses L on siis

$$f(x) = a_0(x - \xi_1)(x - \xi_2) \ldots (x - \xi_n)$$
$$f(x) = a_0(x - \bar{\xi}_1)(x - \bar{\xi}_2) \ldots (x - \bar{\xi}_n).$$

Algtegureiks lahutamise lause põhjal (§ 4, art. 3) võivad viimased $f(x)$ tegureiks lahutused erineda ülimalt tegurite järjekorra poolest, mistõttu lahendid $\xi_1, \xi_2, \ldots, \xi_n$ ühtivad kuni järjekorrani lahenditega $\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_n$ ja seega

$$K(\xi_1, \xi_2, \ldots, \xi_n) = K(\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_n).$$

2. Galois korpus. Polünoomi $f(x)$ lahutuskorpuse $\Delta = K(\xi_1, \xi_2, \ldots, \xi_n)$ mõiste järgi laguneb $f(x)$ lahutuskorpuses Δ lineaartegurite korrutiseks. Tekib küsimus, kuidas käitub mingi teine polünoom $p(x)$ Δ suhtes lineaartegureiks lagunemise mõttes. See küsimus toob meid lahutuskorpuse põhiomaduse juurde, mille esitame alljärgneva teoreemina.

T e o r e e m 11. *Olgu Δ polünoomi $f(x)$ lahutuskorpus K suhtes ja $p(x)$ mistahes taandumatu polünoom üle K. Siis $p(x)$ kas*

üldse ei oma lahendeid korpuses Δ või laguneb seal täielikult lineaartegurite korrutiseks.

Teoreemi 11 tõestuseks oletame, vastupidi, et $p(x)$, omades $f(x)$ lahutuskorpuses Δ lahendit ξ, ei lagune seal täielikult lineaartegurite korrutiseks. Seega peab $p(x)$ omama väljaspool korpust Δ vähemalt ühte lahendit $\bar{\xi}$. Et ξ ja $\bar{\xi}$ on ühe ja sama taandumatu polünoomi $p(x)$ lahendid, siis on lihtlaiendid $K(\xi)$ ja $K(\bar{\xi})$ eelmise artikli põhjal ekvivalentsed, mistõttu võime nende vahel korraldada niisuguse isomorfse vastavuse

$$K(\xi) \overset{+}{\longleftrightarrow} K(\bar{\xi}), \tag{17}$$

kus põhikorpuse K elemendid jäävad invariantseks ja ξ-le vastab $\bar{\xi}$. Et isomorfismis (17) jäävad eriti ka $f(x)$ kordajad invariantseks, siis on selle isomorfismi poolt esile kutsutud polünoomkondade isomorfismis $K(\xi)[x] \overset{+}{\longleftrightarrow} K(\bar{\xi})[x]$ $\bar{f}(x) = f(x)$. Seepärast, märkides $f(x)$ lahendid korpuses Δ tähtedega $\xi_1, \xi_2, \ldots, \xi_n$, võime teoreemi 10 järgi (art. 1) isomorfismi (17) jätkata $f(x)$ lahutuskorpuste isomorfismini

$$K(\xi, \xi_1, \xi_2, \ldots, \xi_n) \overset{+}{\longleftrightarrow} K(\bar{\xi}, \xi_1, \xi_2, \ldots, \xi_n), \tag{18}$$

nii et ξ-le vastab $\bar{\xi}$ ja igale lahendile ξ_i mingi lahend ξ_{α_i}.

Et eelduse järgi ξ asetseb $f(x)$ lahutuskorpuses $\Delta = K(\xi_1, \xi_2, \ldots, \xi_n)$, siis avaldub ξ ratsionaalselt lahendite $\xi_1, \xi_2, \ldots, \xi_n$ kaudu kujul

$$\xi = R(\xi_1, \xi_2, \ldots, \xi_n).$$

Viimasele võrdusele vastab isomorfismi (18) tõttu võrdus

$$\bar{\xi} = R(\xi_{\alpha_1}, \xi_{\alpha_2}, \ldots, \xi_{\alpha_n}),$$

kus $\xi_{\alpha_1}, \xi_{\alpha_2}, \ldots \xi_{\alpha_n}$ tähendavad lahendeid $\xi_1, \xi_2, \ldots, \xi_n$ mingis teises järjekorras. Seega $\bar{\xi}$, avaldudes ratsionaalselt $\xi_1, \xi_2, \ldots, \xi_n$ kaudu, kuulub korpusse Δ, vastupidi eeldusele.

Tähendab, kui $p(x)$ omab $f(x)$ lahutuskorpuses ühte lahendit ξ, siis peavad kõik $p(x)$ lahendid kuuluma korpusse Δ, s. o. $p(x)$ peab lagunema korpuses Δ täielikult lineaartegurite korrutiseks.

Polünoomi lahutuskorpus kuulub erijuhuna üldisemate algebraliste laiendite — nn. Galois korpuste hulka.

D e f i n i t s i o o n 6. Algebralist laiendit, kus iga põhikorpuses K taandumatu polünoomi $p(x)$ suhtes on kaks võimalust: emb-kumb, kas $p(x)$ üldse ei oma lahendeid selles laiendis või laguneb seal täielikult lineaartegurite korrutiseks, nimetatakse G a l o i s k o r p u s e k s[1] K suhtes.

Küsime, missugusel tingimusel osutub algebraline lihtlaiend $K(\xi)$ Galois korpuseks põhikorpuse K suhtes.

Olgu $p(x)$ algebralise lihtlaiendi $K(\xi)$ määrav polünoom, k polünoomi $p(x)$ aste ja $\xi_1 = \xi, \xi_2, \ldots, \xi_k$ polünoomi $p(x)$ lahendid. Kui nüüd $K(\xi)$ on Galois korpus, siis peab siin $p(x)$ lagunema täielikult lineaartegurite korrutiseks, nii et lahendid ξ_i kuuluvad kõik korpusse $K(\xi)$. Et iga ξ_i aste K suhtes on võrdne $K(\xi)$ moodustava elemendi ξ astmega k, siis on teoreemi 8 järgi (§ 25, art. 3)

$$K(\xi_i) = K(\xi).$$

Ümberpöördult, kui viimane võrdus leiab aset iga $i = 1, 2, \ldots, k$ puhul, siis asetsevad $p(x)$ lahendid ξ_i kõik laiendis $K(\xi)$, mistõttu

$$K(\xi) = K(\xi_1, \xi_2, \ldots, \xi_k)$$

osutub $p(x)$ lahutuskorpuseks K suhtes ja on seega eriti Galois korpus.

Edaspidi nimetame iga korpuses K taandumatu polünoomi $p(x)$ lahendeid $\xi_1, \xi_2, \ldots, \xi_k$ üksteise k a a s e l e m e n t i d e k s K suhtes ja kaaselementide poolt moodustatud lihtlaiendeid

$$K(\xi_1), K(\xi_2), \ldots, K(\xi_k)$$

üksteise k a a s l a i e n d i t e k s K suhtes. Nagu nägime eelne-

[1] Galois korpust nimetatakse teisiti ka n o r m a a l k o r p u s e k s.

nud artiklis, on kaaslaiendid kõik omavahel ekvivalentsed. Kasutades kaaslaiendi mõistet, võime öelda, et *algebraline lihtlaiend $K(\xi)$ kujutab Galois korpust siis ja ainult siis, kui $K(\xi)$ ühtib kõigi oma kaaslaienditega.*

3. Teoreem primitiivsest elemendist. Olgu $\xi_1, \xi_2, \ldots, \xi_n$ algebralised elemendid põhikorpuse K suhtes ja $K(\xi_1, \xi_2, \ldots, \xi_n)$ laiend, mis on saadud nende elementide adjungeerimisel K-le. Osutub, et kui põhikorpuse K karakteristika on null, siis kujutab laiend $K(\xi_1, \xi_2, \ldots, \xi_n)$ tegelikult lihtlaiendit. Nimelt on kehtiv järgmine teoreem, mis on esmakordselt tõestatud Abeli poolt sümmeetriliste polünoomide põhilause abil.

Teoreem 12. *Kui $\xi_1, \xi_2, \ldots, \xi_n$ on mistahes algebralised elemendid mingi põhikorpuse K suhtes, mille karakteristika on null, siis leidub teatav algebraline element Θ, nii et*

$$K(\xi_1, \xi_2, \ldots, \xi_n) = K(\Theta).$$

Siin elementi Θ nimetatakse laiendi $K(\xi_1, \xi_2, \ldots, \xi_n)$ primitiivseks elemendiks ja vastavalt sellele teoreemi 12 teoreemiks primitiivsest elemendist.

Näitame kõigepealt, et juhul, kui põhikorpuse K karakteristika on null, ei saa selles korpuses taandumatu polünoom $p(x)$ omada kordseid lahendeid üheski ülemkorpuses. Tõepoolest, kui

$$p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_kx^k, \quad a_k \neq 0$$

omaks kordset lahendit, siis peaks see lahend olema ka tuletise

$$p'(x) = a_1 + 2a_2x + 3a_3x^2 + \ldots + ka_kx^{k-1}$$

lahendiks, mistõttu polünoomide $p(x)$ ja $p'(x)$ suurim ühistegur $d(x) = (p, p')$ peab olema vähemalt esimese astme polünoom. Jagades polünoomi $p(x)$ $d(x)$-ga, saame

$$p(x) = q(x)d(x),$$

kus $q(x)$ on konstant, sest $p(x)$ on taandumatu polünoom. Seega peab $d(x)$ olema k-astme polünoom. Et aga korpuses karakteristikaga null on $ka_k \neq 0$, kui $k \neq 0$ (§ 7, art. 1), siis on $p'(x)$

$(k-1)$-astme polünoom ega saa seetõttu jaguda $d(x)$-ga. Niisiis oletus, et $p(x)$ omab kordset lahendit, ei pea paika.

Tõestame nüüd teoreemi 12 algul kahe algebralise elemendi ξ ja η puhul. Rahuldagu ξ k-astme võrrandit $p(x)=0$ ja η l-astme võrrandit $q(x)=0$, kus $p(x)$ ja $q(x)$ on korpuses K taandumatud polünoomid. Vaatleme laiendit $K(\xi, \eta)$. Kui siin $p(x)$ ja $q(x)$ ei peaks lagunema täielikult lineaartegurite korrutiseks, siis laiendame korpust $K(\xi, \eta)$ polünoomi $p(x)q(x)$ lahutuskorpuseks Δ. Olgu polünoomide $p(x)$ ja $q(x)$ lahendid korpuses Δ vastavalt

$$\xi_1=\xi, \ \xi_2, \ \ldots, \ \xi_k; \quad \eta_1=\eta, \ \eta_2, \ \ldots, \ \eta_l.$$

Näitame, et primitiivseks elemendiks on antud juhul element

$$\Theta=\xi+\lambda\eta, \tag{19}$$

kus λ tähendab mingit K elementi, mis ei ole võrdne ühegi jagatisega [1]

$$\frac{\xi_h-\xi}{\eta-\eta_j}, \quad h=1, \ 2, \ \ldots, \ k; \quad j=2, \ 3, \ \ldots, \ l.$$

Et seose (19) tõttu $\xi=\Theta-\lambda\eta$, siis on η polünoomide

$$p(\Theta-\lambda x), \quad q(x) \tag{20}$$

ühine lahend. Veendume, et neil polünoomidel pole teisi ühiseid lahendeid peale η. Tõepoolest, nende polünoomide ühiseks lahendiks võiks olla peale η vaid mingi η_j, $j>1$. Siis peaks aga olema

$$p(\Theta-\lambda\eta_j)=0$$

ja seega

$$\Theta-\lambda\eta_j=\xi_h$$

ehk (19) tõttu

$$\xi+\lambda\eta-\lambda\eta_j=\xi_h,$$

[1] Et K kui korpus karakteristikaga null sisaldab lõpmatu hulga elemente, siis leidub alati niisugune element λ.

millest

$$\lambda = \frac{\xi_h - \xi}{\eta - \eta_j},$$

vastuolus λ valikuga. Kuna, teiselt poolt, $q(x)$ kui taandumatu polünoom korpuses karakteristikaga null ei saa omada kordseid lahendeid üheski ülemkorpuses, siis omab polünoomide (20) suurim ühistegur kuju

$$d(x) = x - \eta.$$

Polünoomide (20) kordajad kuuluvad korpusse $K(\Theta)$. Samasse korpusse peavad kuuluma ka suurima ühisteguri $d(x)$ kordajad, nii et eriti $\eta \in K(\Theta)$. Siis seose (19) tõttu ka $\xi \in K(\Theta)$ ja seega

$$K(\xi, \eta) \subset K(\Theta).$$

Teiselt poolt nähtub seosest (19), et

$$K(\Theta) \subset K(\xi, \eta).$$

Järelikult $K(\xi, \eta) = K(\Theta)$. Siinjuures on Θ algebraline element K suhtes, sest vastasel korral oleksid kõik $K(\Theta)$ elemendid, välja arvatud K elemendid, transtsendentsed (§ 25, art. 3), nende hulgas ka ξ ja η. Seega on teoreem 12 tõestatud kahe algebralise elemendi ξ ja η jaoks.

Rakendades täieliku induktsiooni printsiipi, oletame, et teoreem 12 on kehtiv $n-1$ algebralise elemendi puhul, s. o.

$$K(\xi_1, \xi_2, \ldots, \xi_{n-1}) = K(\bar{\Theta}),$$

ja näitame, et teoreem 12 jääb siis kehtima ka n algebralise elemendi korral. Tõepoolest:

$$K(\xi_1, \xi_2, \ldots, \xi_n) = K(\xi_1, \xi_2, \ldots, \xi_{n-1})(\xi_n) =$$

$$= K(\bar{\Theta}, \xi_n) = K(\Theta),$$

sest kahe elemendi $\bar{\Theta}$ ja ξ_n puhul on teoreem 12 kehtiv.

Vaatleme näitena laiendit $K(\sqrt{2}, i)$, kus K tähendab ratsionaalarvude korpust. Et $\sqrt{2}$ rahuldab ratsionaalarvude korpuses

taandumatut võrrandit $x^2 - 2 = 0$, siis on $(\sqrt{2} : K) = 2$ ja seega

$$K(\sqrt{2}) = \{a + b\sqrt{2}\},$$

kus a ja b tähendavad ratsionaalarve. Et i rahuldab võrrandit $x^2 + 1 = 0$, mis on taandumatu korpuses $K(\sqrt{2})$, siis

$$K(\sqrt{2}, i) = \{\alpha + \beta i\},$$

kus α ja β, kuuludes korpusse $K(\sqrt{2})$, omavad kuju

$$\alpha = a + b\sqrt{2}, \quad \beta = c + d\sqrt{2},$$

nii et

$$K(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}\, i\}.$$

Rakendame nüüd laiendile $K(\sqrt{2}, i)$ teoreemi primitiivsest elemendist, asendades elemendid $\sqrt{2}$ ja i üheainsa elemendiga $\Theta = \sqrt{2} + \lambda i$. Seejuures tuleb ratsionaalarv λ nii valida, et

$$\lambda \neq \frac{\xi_h - \xi}{\eta - \eta_j}, \quad h = 1, 2; \quad j = 2.$$

Antud juhul on $\xi_1 = \xi = \sqrt{2}$, $\xi_2 = -\sqrt{2}$; $\eta_1 = \eta = i$, $\eta_2 = -i$; seega saame vastavalt h väärtustele 1 ja 2:

$$\lambda \neq 0, \quad \lambda \neq \sqrt{2}\, i.$$

Et siin teine tingimus on iga λ kui ratsionaalarvu puhul täidetud, siis tuleb λ valiku puhul arvestada vaid esimest tingimust $\lambda \neq 0$. Võttes näiteks $\lambda = 1$, s. o. $\Theta = \sqrt{2} + i$, leiame kergesti, et Θ rahuldab neljanda astme taandumatut võrrandit $x^4 - 2x^2 + 9 = 0$. Seega $(\Theta : K) = 4$, nii et laiend $K(\Theta)$ koosneb kõigist elementidest kujul

$$a' + b'(\sqrt{2} + i) + c'(\sqrt{2} + i)^2 + d'(\sqrt{2} + i)^3 =$$
$$= (a' + c') + (b' - d')\sqrt{2} + (b' + 5d')i + 2c'\sqrt{2}\, i,$$

kus a', b', c' ja d' tähendavad mistahes ratsionaalarve. Märkides

$$a' + c' = a\,, \quad b' - d' = b\,, \quad b' + 5d' = c\,, \quad 2c' = d\,,$$

saame

$$K(\Theta) = \{a + b\sqrt{2} + ci + d\sqrt{2}\,i\},$$

nii et tõesti

$$K(\sqrt{2}\,,\ i) = K(\Theta).$$

Teoreemi 12 rakenduseks teeme sellest teoreemist ühe järelduse mistahes vahepealse korpuse Δ kohta, mis asetseb põhikorpuse K ja algebralise lihtlaiendi $K(\xi)$ vahel, s. o. kus

$$K \subset \Delta \subset K(\xi).$$

Olgu α maksimaalse astmega element vahepealses korpuses Δ ja β mistahes element selles korpuses. Vaatleme laiendit $K(\alpha\,,\ \beta)$. Toetudes teoreemile primitiivsest elemendist, võime leida niisuguse elemendi $\Theta = \alpha + \lambda\beta$, et oleks

$$K(\alpha\,,\ \beta) = K(\Theta).$$

Et Θ kuulub koos elementidega α ja β korpusse Δ, siis on α valiku kohaselt

$$(\Theta : K) \leqslant (\alpha : K).$$

Et aga α kuulub korpusse $K(\Theta)$, siis on teiselt poolt

$$(\alpha : K) \leqslant (\Theta : K)$$

ja seega

$$(\alpha : K) = (\Theta : K).$$

Teoreemi 8 järgi (§ 25, art. 3) on seega

$$K(\alpha) = K(\Theta),$$

millest nähtub, et Θ asetseb laiendis $K(\alpha)$. Järelikult asetseb laiendis $K(\alpha)$ ka element $\beta = \frac{\Theta - \alpha}{\lambda}$, s. o. Δ mistahes element, nii et

$$\Delta \subset K(\alpha).$$

Kuna teiselt poolt

$$K(\alpha) \subset \Delta ,$$

siis peab olema $\Delta = K(\alpha)$.

Tähendab, *kui põhikorpus K on karakteristikaga null, siis iga korpus Δ põhikorpuse K ja tema algebralise lihtlaiendi $K(\xi)$ vahel kujutab ka algebralist lihtlaiendit.* Seega kui korpuse K karakteristika on null, siis mitte ainult laiend $K(\xi_1 , \xi_2 , \ldots , \xi_n)$, vaid ka viimase alamkorpused kujutavad tegelikult lihtlaiendeid.

Harjutusülesandeid.

134. Leida

a) täisarvude 78, 96, 114;

b) polünoomide $x^4 - 4$, $x^4 + x^3 - 2x - 4$, $2x^4 - x^3 + 2x - 8$ poolt moodustatud ideaali kui peaideaali moodustav element.

135. Näidata, et integriteetkonnas $\{a + bi\sqrt{5}\}$, kus a ja b tähendavad täisarve, ideaal $(1 + i\sqrt{5},\ 1 - i\sqrt{5})$ ei ole peaideaal.

136. Analoogiliselt Gaussi täisarvude integriteetkonnaga näidata, et integriteetkond $\{a + b\sqrt{2}\}$, kus a ja b tähendavad täisarve, kujutab peaideaaliringi.

137. Leida jäägiklassikorpuses $R/(3 + \sqrt{2})$, kus R tähendab ülesande 136 integriteetkonda, elementide 5 ja $\sqrt{2}$ pöördelemendid.

138. Lahendada võrrandisüsteem

$$2x + 3iy = 2$$
$$3ix + 2y = 3$$

jäägiklassikorpuses $R/(1 + 2i)$, kus R tähendab Gaussi täisarvude integriteetkonda.

139. Leida jäägiklassikorpuste

a) $R/(1 + i)$; b) $R/(2 + i)$; c) $R/(1 + 2i)$

karakteristikad, kui R tähendab Gaussi täisarvude integriteetkonda.

140. Näidata, et peaideaaliringis need jäägiklassid ideaali (a) järgi, mille elemendid on a suhtes ühistegurita, moodustavad rühma korrutamise suhtes.

141. Leida laiendite

$$\text{a) } K\left(\sqrt{2-\sqrt[3]{2}}\right); \quad \text{b) } K\left(e^{\frac{2\pi i}{5}}\right)$$

määravad polünoomid, kui K tähendab ratsionaalarvude korpust.

142. Missugune on jäägiklassikorpuse $R/(7)$ aste tema algkorpuse suhtes, kui R tähendab Gaussi täisarvude integriteetkonda?

143. Mitu isesugust elementi on korpuses karakteristikaga p, kui selle korpuse aste tema algkorpuse suhtes on k?

144. Koostada nullist erinevate elementide korrutamistabel korpusele, mis saadakse jäägiklassikorpusest $R^{(2)}$ selles korpuses taandumatu ruutpolünoomi lahendi adjungeerimisel.

145. Adjungeerida ratsionaalarvude korpusele polünoomi x^4+1 mingi lahend ja lahutada siis see polünoom saadud laiendis taandumatute polünoomide korrutiseks.

146. Leida laiendi $K(\sqrt{2}, \sqrt[3]{2})$ aste, kui K on:

a) ratsionaalarvude korpus;

b) jäägiklassikorpus $R^{(7)}$.

147. Missugune on polünoomi x^8-1 lahutuskorpuse aste

a) ratsionaalarvude korpuse suhtes;

b) Gaussi ratsionaalarvude korpuse suhtes?

148. Näidata, et iga teise astme laiend kujutab põhikorpuse suhtes Galois korpust.

149. Näidata, et laiend, mis saadakse ratsionaalarvude korpusest polünoomi x^3+2 mingi lahendi adjungeerimisel, ei ole Galois korpus.

VIII. Galois teooria alused.

§ 27. Galois rühm.

1. Galois rühma mõiste. Suur edu, mida saavutas algebra tänu Galois uurimistele, põhineb ühelt poolt algebraliste lihtlaiendite uurimise taandamisel Galois korpuste uurimisele ja teiselt poolt rühmateooria meetodite rakendamisel korpuseteoorias. Seega panid Galois uurimused ühtlasi aluse rühmateooria arengule. Galois teooria sisuks on kommutatiivse korpuse algebraliste lihtlaiendite uurimine rühmateooria meetodite ja aparatuuriga. Galois teooria aluste arendamisel piirdume praktiliselt kõige sagedamini esineva juhuga, kus põhikorpuse K karakteristika on null.

Galois teooria põhimõisteteks on Galois korpus, missuguse mõistega tutvusime juba varem (§ 26, art. 2) ja Galois rühm, millega tutvume käesolevas artiklis.

Oletame, et vaadeldav algebraline lihtlaiend $K(\xi)$ kujutab Galois korpust. Olgu $p(x)$ laiendi $K(\xi)$ määrav polünoom, s. o. niisugune korpuses K taandumatu polünoom, mille lahendiks on ξ, ja olgu $\xi_1 = \xi$, ξ_2, ..., ξ_k polünoomi $p(x)$ lahendid, teiste sõnadega, ξ kaaselemendid. Seame $K(\xi)$ igale elemendile

$$f(\xi) = a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{k-1}\xi^{k-1}$$

vastavusse kaaslaiendi $K(\xi_i)$ elemendi

$$f(\xi_i) = a_0 + a_1\xi_i + a_2\xi_i^2 + \ldots + a_{k-1}\xi_i^{k-1}.$$

Võib kergesti veenduda, et korraldatud vastavus kujutab isomorfismi

$$K(\xi) \overset{+}{\longleftrightarrow} K(\xi_i).$$

Et aga $K(\xi)$ kui Galois korpus ühtib kõigi oma kaaslaienditega (§ 26, art. 2) ja seega $K(\xi_i) = K(\xi)$, siis taandub viimane isomorfism automorfismiks

$$K(\xi) \overset{+}{\underset{\cdot}{\longleftrightarrow}} K(\xi).$$

Selles automorfismis jäävad põhikorpuse K elemendid invariantseks, sest kui $f(\xi) = a_0$, siis ka $f(\xi_i) = a_0$. Seega, seades Galois korpuse $K(\xi)$ igale elemendile $f(\xi)$ vastavusse elemendi $f(\xi_i)$, saame korpuse $K(\xi)$ automorfismi, mis jätab põhikorpuse K elemendid invariantseks. Et elemendil ξ on k kaaselementi ξ_i, siis saame sel teel arvult k korpuse $K(\xi)$ automorfismi, mis jätavad K elemendid invariantseks.

Ei ole raske näha, et peale nende k automorfismi ei leidu teisi $K(\xi)$ automorfisme, mis jätaksid K elemendid invariantseks. Nimelt vastab iga niisuguse automorfismi s puhul võrdusele $p(\xi) = 0$ jälle võrdus $p(\bar{\xi}) = 0$, kus $\bar{\xi}$ tähendab ξ-le vastavat elementi automorfismis s. Seega $\bar{\xi} = \xi_i$, nii et s teisendab elemendi ξ kaaselemendiks ξ_i, missugust asjaolu märgime lühidalt sümboliga

$$\xi s = \xi_i.$$

Leiame elemendi $f(\xi)$ teisendi automorfismis s. Et automorfismis vastavus säilib tehete puhul, siis on

$$\begin{aligned} f(\xi)s &= (a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{k-1}\xi^{k-1})s = \\ &= a_0 s + (a_1\xi)s + (a_2\xi^2)s + \ldots + (a_{k-1}\xi^{k-1})s = \\ &= a_0 + a_1\xi_i + a_2\xi_i^2 + \ldots + a_{k-1}\xi_i^{k-1} = f(\xi_i), \end{aligned}$$

millest nähtub, et s kujutab varem vaadeldud automorfismi.

Niisiis leidub parajasti k korpuse $K(\xi)$ automorfismi, mis jätavad põhikorpuse K elemendid invariantseks. Märgime siin automorfismi, mis jätab ξ muutumatuks, s. o. identse automorfismi, tähega s_0, edasi automorfismi, mis teisendab ξ kaaselemendiks ξ_2, tähega s_1 jne., lõppeks automorfismi, mis teisendab ξ kaaselemendiks ξ_k, tähega s_{k-1}, nii et

$$\xi s_0 = \xi, \quad \xi s_1 = \xi_2, \quad \ldots, \quad \xi s_{k-1} = \xi_k.$$

Rakendame nüüd ξ-le järjest kahte automorfismi s_i ja s_j. Kõigepealt on $\xi s_i = \xi_{i+1}$. Rakendades elemendile ξ_{i+1} omakorda automorfismi s_j, saame tulemusena jälle mingi $p(x)$ lahendi, s. o. teatava ξ kaaselemendi ξ_h. Tähendab, $\xi_{i+1} s_j = \xi_h$ ehk

$$(\xi s_i) s_j = \xi_h .$$

Teiselt poolt on

$$\xi s_{h-1} = \xi_h .$$

Automorfismi s_{h-1}, mille toime on samaväärne automorfismide s_i ja s_j järjest rakendamisega, nimetatakse automorfismide s_i ja s_j korrutiseks ja märgitakse vastavalt sümboliga $s_i s_j$, nii et[1]

$$\xi(s_i s_j) = (\xi s_i) s_j .$$

Sümboli $\xi(s_i s_j)$ asemel kirjutame edaspidi lihtsalt $\xi s_i s_j$, sest sulgude ärajätmine ei saa siin tekitada arusaamatusi.

Näitame, et automorfismide hulk

$$\{s_0, s_1, s_2, \ldots, s_{k-1}\}$$

moodustab korrutamise suhtes rühma. Tõepoolest:

I. Korrutamise seadus on kehtiv, sest korrutis $s_i s_j$ kujutab automorfismi s_{h-1}, mis on automorfismidega s_i ja s_j üheselt määratud.

II. Assotsiatiivsuse seadus $s_i(s_j s_l) = (s_i s_j) s_l$ on kehtiv, sest

$$\xi s_i (s_j s_l) = [(\xi s_i) s_j] s_l = \xi (s_i s_j) s_l .$$

III. On olemas ühikautomorfism ehk identne automorfism $e = s_0$, mis rahuldab tingimust $s_i e = s_i$.

IV. Igal automorfismil s_i on olemas pöördautomorfism,

[1] Siit selgub ka põhjus, miks kirjutame ξs_i aga mitte $s_i \xi$, sest viimasel juhul saaksime korrutise $s_i s_j$ jaoks meile ebakohase valemi $(s_i s_j)\xi = s_j(s_i \xi)$.

nimelt automorfism s_i^{-1}, mis teisendab elemendi ξ_{i+1} elemendiks ξ, s. o. mille puhul [1] $\xi_{i+1}s_i^{-1} = \xi$, sest

$$\xi(s_i s_i^{-1}) = (\xi s_i)s_i^{-1} = \xi_{i+1}s_i^{-1} = \xi$$

ja seega $s_i s_i^{-1} = e$.

Definitsioon 1. Galois korpuse $\Sigma = K(\xi)$ nende automorfismide rühma, mis jätavad põhikorpuse K elemendid invariantseks, nimetatakse Σ Galois rühmaks K suhtes.

Galois korpuse $\Sigma = K(\xi)$ Galois rühma K suhtes märgime lühidalt sümboliga $\Sigma(K)$. Nagu nägime, on Galois rühma $\Sigma(K)$ järk võrdne laiendi Σ astmega $(\Sigma : K)$. Et saada kujutlust Galois rühma osast Galois korpuse omaduste uurimisel, tõestame järgmised kolm teoreemi.

Teoreem 1. *Põhikorpuse K ja tema Galois korpuse $\Sigma = K(\xi)$ vahel asetsevad korpused Δ ja $\bar{\Delta}$ kujutavad teineteise kaaslaiendeid K suhtes siis ja ainult siis, kui Galois rühmas $\Sigma(K)$ leidub niisugune automorfism, mis teisendab Δ korpuseks Δ.*

Teoreemi 1 tõestuseks oletame kõigepealt, et Δ ja $\bar{\Delta}$ on kaaslaiendid K suhtes. Siis on Δ ja $\bar{\Delta}$ ekvivalentsed, nii et nende vahel saab korraldada niisuguse isomorfismi $\Delta \overset{+}{\longleftrightarrow} \bar{\Delta}$, kus K elemendid jäävad invariantseks. Rakendame viimasele isomorfismile teoreemi 10 isomorfismi jätkust (§ 26, art. 1), mille järgi võib põhikorpuste isomorfismi jätkata vastavate polünoomide $f(x)$ ja $\bar{f}(x)$ lahutuskorpuste isomorfismini. Võttes $f(x) = p(x)$, kus $p(x)$ tähendab laiendi $\Sigma = K(\xi)$ määravat polünoomi, näeme, et ka $\bar{f}(x) = p(x)$. Et Σ on Galois korpus, siis $p(x)$, omades selles korpuses lahendit ξ, laguneb seal täielikult lineaartegurite korrutiseks. Seega osutub Σ polünoomi $p(x)$ lahutuskorpuseks K suhtes ja siis ammugi $p(x)$ lahutuskorpuseks nii Δ kui ka $\bar{\Delta}$ suhtes, mistõttu saab isomorfismi $\Delta \overset{+}{\longleftrightarrow} \bar{\Delta}$ jätkata

[1] Niisugune automorfism s_i^{-1} on olemas, sest iga automorfism, kujutades üksühest vastavust, on pööratav.

isomorfismini $\Sigma \overset{+}{\longleftrightarrow} \Sigma$. Viimane isomorfism kujutab aga Galois rühma $\Sigma(K)$ automorfismi[1] s, mis teisendabki korpuse Δ korpuseks $\bar{\Delta}$.

Teisendagu, ümberpöördult, Galois rühma $\Sigma(K)$ mingi automorfism s korpuse Δ korpuseks $\bar{\Delta}$. Paneme tähele, et automorfism s teisendab laiendi Σ mistahes elemendi Θ kaaselemendiks $\bar{\Theta}$, sest s teisendab võrduse $p(\Theta) = 0$ võrduseks $p(\bar{\Theta}) = 0$, kus $p(x)$ tähendab seda korpuses K taandumatut polünoomi, mille lahendiks on Θ. Olgu eriti Θ korpuse Δ moodustav element, s. o. kõrgeima astmega element korpuses Δ. Siis on $\bar{\Theta}$ kõrgeima astmega element korpuses $\bar{\Delta}$ ja kujutab seega viimase moodustavat elementi, nii et $\bar{\Delta} = K(\bar{\Theta})$, mis ütlebki, et $\bar{\Delta}$ on Δ kaaslaiend K suhtes.

Teoreem 2. *Galois korpuses $\Sigma = K(\xi)$ kujutavad elemendid Θ ja $\bar{\Theta}$ teineteise kaaselemente K suhtes siis ja ainult siis, kui Galois rühmas $\Sigma(K)$ leidub niisugune automorfism, mis teisendab elemendi Θ elemendiks $\bar{\Theta}$.*

Oletades, et Θ ja $\bar{\Theta}$ on kaaselemendid K suhtes, vaatleme vastavaid kaaslaiendeid $\Delta = K(\Theta)$ ja $\bar{\Delta} = K(\bar{\Theta})$. Teoreemi 1 esimese osa tõestuse puhul nägime, et niisugusel korral leidub Galois rühmas $\Sigma(K)$ automorfism s, mis kujutab isomorfismi $\Delta \overset{+}{\longleftrightarrow} \bar{\Delta}$ jätku. Et viimases isomorfismis Θ teisendub elemendiks $\bar{\Theta}$, siis teisendab ka s elemendi Θ elemendiks $\bar{\Theta}$.

Ümberpöördult, kui Galois rühma $\Sigma(K)$ automorfism s teisendab Θ elemendiks $\bar{\Theta}$, siis on $\bar{\Theta}$ elemendi Θ kaaselement K suhtes, nagu nägime teoreemi 1 teise osa tõestuse puhul.

Teoreem 3. *Kui Galois korpuses $\Sigma = K(\xi)$ jääb mingi element Θ invariantseks Galois rühma $\Sigma(K)$ iga automorfismi suhtes, siis kuulub Θ põhikorpusse K.*

Olgu tõestuseks $\bar{\Theta}$ elemendi Θ kaaselement. Teoreemi 2 järgi

[1] Kõneldes Galois rühma $\Sigma(K)$ automorfismidest, mõtleme rühma $\Sigma(K)$ kuuluvaid Σ automorfisme.

peab siis Galois rühmas $\Sigma(K)$ leiduma niisugune automorfism s, mis teisendab Θ elemendiks $\bar{\Theta}$. Et aga Θ peab jääma invariantseks s-i suhtes, siis peab olema $\bar{\Theta} = \Theta$, nii et elemendil Θ pole teisi kaaselemente peale iseenda. Seega peab Θ rahuldama esimese astme võrrandit, s. o.

$$c_0 + c_1\Theta = 0, \quad c_1 \neq 0,$$

kus kordajad c_0 ja c_1 kuuluvad põhikorpusse K. Siis kuulub aga ka $\Theta = -\frac{c_0}{c_1}$ põhikorpusse K.

Niisiis on põhikorpus K iseloomustatud sellega, et tema elemendid ja ainult need jäävad invariantseks Galois rühma $\Sigma(K)$ automorfismide puhul.

2. Võrrandi Galois rühm. Algebraliste võrrandite teoorias etendab tähtsat osa juhtum, kus Galois korpuseks Σ on polünoomi lahutuskorpus. Olgu antud võrrand $f(x) = 0$ üle korpuse K. Polünoomi $f(x)$ lahutuskorpuse $K(\xi_1, \xi_2, \ldots, \xi_n)$ Galois rühma nimetatakse *võrrandi $f(x) = 0$ Galois rühmaks*. Kuna meil on olemas menetlus polünoomi $f(x)$ kordsete lahendite eraldamiseks (§ 7, art. 3), siis võime üldsust kitsendamata eeldada, et siin lahendid $\xi_1, \xi_2, \ldots, \xi_n$ on kõik üksteisest erinevad. Teisendagu võrrandi $f(x) = 0$ Galois rühma mingi automorfism s elemendi ξ_i elemendiks $\bar{\xi}_i$. Et $f(x)$ kordajad kui K elemendid on s-i suhtes invariantsed, siis teisendab s võrduse $f(\xi_i) = 0$ võrduseks $f(\bar{\xi}_i) = 0$, mistõttu $\bar{\xi}_i$ kujutab teatavat võrrandi $f(x) = 0$ lahendit, s. o. $\bar{\xi}_i = \xi_{\alpha_i}$. Niisiis teisendab automorfism s lahendid

$$\xi_1, \xi_2, \ldots, \xi_n$$

lahenditeks

$$\xi_{\alpha_1}, \xi_{\alpha_2}, \ldots, \xi_{\alpha_n},$$

kutsudes seega esile lahendite $\xi_1, \xi_2, \ldots, \xi_n$ indeksite substitutsiooni

$$(1) \qquad \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}.$$

Seame võrrandi $f(x) = 0$ Galois rühma igale automorfismile s vastavusse selle automorfismi poolt esile kutsutud substitutsiooni (1). Siis vastavad erinevatele automorfismidele s ja t erinevad substitutsioonid. Tõepoolest, kui oleks

$$\xi_i s = \xi_{\alpha_i}, \quad \xi_i t = \xi_{\alpha_i},$$

siis, silmas pidades, et $f(x)$ lahutuskorpuse $K(\xi_1, \xi_2, \ldots, \xi_n)$ iga element Θ avaldub kujul

$$\Theta = R(\xi_1, \xi_2, \ldots, \xi_n),$$

kus R tähendab ratsionaalset avaldist üle K, saaksime

$$\Theta s = R(\xi_{\alpha_1}, \xi_{\alpha_2}, \ldots, \xi_{\alpha_n}), \quad \Theta t = R(\xi_{\alpha_1}, \xi_{\alpha_2}, \ldots, \xi_{\alpha_n}),$$

millest nähtub, et $\Theta s = \Theta t$ ja seega $s = t$, vastupidi eeldusele.

Niisiis on korraldatud vastavus võrrandi $f(x) = 0$ Galois rühma automorfismide ja nende poolt esile kutsutud substitutsioonide vahel üksühene:

$$s \leftrightarrow \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}.$$

Näitame, et see vastavus säilib korrutamise puhul ja kujutab seega isomorfismi. Nimelt kui t on mingi automorfism, mille korral $\xi_{\alpha_i} t = \xi_{\beta_i}$, nii et

$$t \leftrightarrow \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \beta_1 & \beta_2 & \ldots & \beta_n \end{pmatrix},$$

siis on

$$\xi_i st = (\xi_i s)\, t = \xi_{\alpha_i} t = \xi_{\beta_i},$$

mistõttu

$$st \leftrightarrow \begin{pmatrix} 1 & 2 & \ldots & n \\ \beta_1 & \beta_2 & \ldots & \beta_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix} \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \beta_1 & \beta_2 & \ldots & \beta_n \end{pmatrix}.$$

Tähendab, *võrrandi*[1] $f(x) = 0$ *Galois rühm on isomorfne selle*

[1] Eeldusel, et $f(x)$ ei oma kordseid lahendeid.

võrrandi lahendite indeksite $1, 2, \ldots, n$ *teatava substitutsioonirühmaga.* Viimane asjaolu lubab meil kõnelda võrrandi $f(x) = 0$ Galois rühma substitutsioonidest.

Leiame näitena võrrandi $x^4 - x^2 + 1 = 0$ Galois rühma, kui põhikorpuseks on ratsionaalarvude korpus. Jagades antud võrrandit x^2-ga, saame

$$x^2 - 1 + \frac{1}{x^2} = 0,$$

millest nähtub, et kui ξ_1 on selle võrrandi mingi lahend, siis avalduvad ülejäänud lahendid ξ_2, ξ_3, ξ_4 lahendi ξ_1 kaudu ratsionaalselt kujul

$$(2) \qquad \xi_2 = -\xi_1, \quad \xi_3 = \frac{1}{\xi_1}, \quad \xi_4 = -\frac{1}{\xi_1}.$$

Seepärast sisaldab laiend $K(\xi_1)$ juba kõiki lahendeid ξ_1, ξ_2, ξ_3, ξ_4 ja kujutab seega polünoomi $x^4 - x^2 + 1$ lahutuskorpust. Niisiis tuleb meil leida korpuse $K(\xi_1)$ Galois rühm K suhtes. Selleks paneme tähele, et ξ_1 kaaselementideks on kõik lahendid ξ_1, ξ_2, ξ_3, ξ_4, sest polünoom $x^4 - x^2 + 1$ on taandumatu ratsionaalarvude korpuses, nagu selles kergesti võib veenduda. Seega koosneb otsitav Galois rühm neljast automorfismist s_0, s_1, s_2, s_3, mis on määratud tingimustega

$$(3) \qquad \xi_1 s_0 = \xi_1, \quad \xi_1 s_1 = \xi_2, \quad \xi_1 s_2 = \xi_3, \quad \xi_1 s_3 = \xi_4.$$

Leiame neile automorfismidele vastavad substitutsioonid. Kõigepealt vastab identsele automorfismile s_0 identne substitutsioon e. Edasi, et saada automorfismile s_1 vastavat substitutsiooni, tuleb leida teisendid $\xi_i s_1$. Silmas pidades seoseid (2) ja (3), saame

$$\begin{aligned}
&\xi_1 s_1 = \xi_2 \\
&\xi_2 s_1 = (-\xi_1) s_1 = -(\xi_1 s_1) = -\xi_2 = \xi_1 \\
&\xi_3 s_1 = \left(\frac{1}{\xi_1}\right) s_1 = \frac{1}{\xi_1 s_1} = \frac{1}{\xi_2} = -\frac{1}{\xi_1} = \xi_4 \\
&\xi_4 s_1 = \left(-\frac{1}{\xi_1}\right) s_1 = -\frac{1}{\xi_1 s_1} = -\frac{1}{\xi_2} = \frac{1}{\xi_1} = \xi_3,
\end{aligned}$$

millest nähtub, et

$$s_1 \leftrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4).$$

Analoogiliselt leiame

$$s_2 \leftrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4),$$

$$s_3 \leftrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 4)(2\ 3).$$

Niisiis kujutab võrrandi $x^4 - x^2 + 1 = 0$ Galois rühm neljarühma (§ 20, art. 1).

Võrrandi $f(x) = 0$ Galois rühma võib defineerida ka vahetult substitutsioonirühmana, kasutamata $f(x)$ lahutuskorpuse automorfisme. Nimelt paneme tähele, et võrrandi $f(x) = 0$ lahendite $\xi_1, \xi_2, \ldots, \xi_n$ vahel kehtivad alati teatavad seosed

$$R(\xi_1, \xi_2, \ldots, \xi_n) = 0, \tag{4}$$

kus R tähendab ratsionaalset avaldist, mille kordajad kuuluvad põhikorpusse K. Niisugusteks seosteks on näiteks Vieta valemid (§ 9, art. 3), eriti aga võrrandi $x^4 - x^2 + 1 = 0$ puhul seosed (2). Olgu s mingi automorfism võrrandi $f(x) = 0$ Galois rühmas ja (1) temale vastav substitutsioon, nii et $\xi_i s = \xi_{\alpha_i}$. Siis teisendab s seose (4) seoseks

$$R(\xi_{\alpha_1}, \xi_{\alpha_2}, \ldots, \xi_{\alpha_n}) = 0,$$

s. o. seos (4) jääb kehtima, kui rakendada lahenditele $\xi_1, \xi_2, \ldots, \xi_n$ substitutsiooni (1) ehk, nagu öeldakse, substitutsioon (1) jätab seose (4) invariantseks. Näitame, ümberpöördult, et iga substitutsioon (1)

$$s = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix},$$

mis jätab kõik seosed võrrandi $f(x) = 0$ lahendite vahel invariantseks, kuulub selle võrrandi Galois rühma.

Selle väite tõestuseks seame $f(x)$ lahutuskorpuse $K(\xi_1, \xi_2, \ldots, \xi_n)$ igale elemendile $\Theta = F(\xi_1, \xi_2, \ldots, \xi_n)$ vastavusse elemendi $\overline{\Theta} = F(\xi_{\alpha_1}, \xi_{\alpha_2}, \ldots, \xi_{\alpha_n})$. Eriti kui $\Theta = \xi_i$, siis $\overline{\Theta} = \xi_{\alpha_i}$, millest nähtub, et korraldatud vastavus kutsub esile lahendite $\xi_1, \xi_2, \ldots, \xi_n$ indeksite substitutsiooni s. Näitame, et see vastavus kujutab teatavat võrrandi $f(x) = 0$ Galois rühma automorfismi.

Et siin võib elementi Θ väga mitmel viisil avaldada ratsionaalselt lahendite $\xi_1, \xi_2, \ldots, \xi_n$ kaudu, siis tuleb kõigepealt veenduda, et korraldatud vastavus on ühene. Nimelt kui Θ avaldub veel kujul $\Theta = G(\xi_1, \xi_2, \ldots, \xi_n)$, siis võrdus

$$F(\xi_1, \xi_2, \ldots, \xi_n) = G(\xi_1, \xi_2, \ldots, \xi_n)$$

kui ratsionaalne seos jääb substitutsiooni s puhul püsima, s. o.

$$F(\xi_{\alpha_1}, \xi_{\alpha_2}, \ldots, \xi_{\alpha_n}) = G(\xi_{\alpha_1}, \xi_{\alpha_2}, \ldots, \xi_{\alpha_n}),$$

millest ilmnebki vastavuse ühesus. Veel enam, korraldatud vastavus on üksühene. Tõepoolest, vastaku $f(x)$ lahutuskorpuse elementidele $F(\xi_1, \xi_2, \ldots, \xi_n)$ ja $G(\xi_1, \xi_2, \ldots, \xi_n)$ üks ja sama element

$$F(\xi_{\alpha_1}, \xi_{\alpha_2}, \ldots, \xi_{\alpha_n}) = G(\xi_{\alpha_1}, \xi_{\alpha_2}, \ldots, \xi_{\alpha_n}).$$

Olgu m substitutsiooni s järk, nii et $s^m = e$. Siis, rakendades viimasele võrdusele $m - 1$ korda substitutsiooni s, s. o. substitutsiooni $s^{m-1} = s^{-1}$, saame

$$F(\xi_1, \xi_2, \ldots, \xi_n) = G(\xi_1, \xi_2, \ldots, \xi_n).$$

Edasi pole enam mingit raskust näidata, et vastavus $\Theta \leftrightarrow \overline{\Theta}$ säilib tehete puhul ja jätab põhikorpuse K elemendid invariantseks.

Niisiis, *võrrandi $f(x) = 0$ Galois rühm K suhtes koosneb selle võrrandi lahendite nendest substitutsioonidest, mis jätavad invariantseks kõik lahenditevahelised ratsionaalsed seosed üle K.*

Vaatleme lõppeks juhtu, kus polünoom $f(x)$ on taandumatu korpuses K. Siis kujutavad lahendid $\xi_1, \xi_2, \ldots, \xi_n$ üksteise kaaselemente, mistõttu võrrandi $f(x) = 0$ Galois rühmas peavad leiduma teoreemi 2 järgi (art. 1) muu hulgas ka niisugused substitutsioonid, mis teisendavad ξ_1 vastavalt lahenditeks $\xi_1, \xi_2, \ldots, \xi_n$. Teiste sõnadega, võrrandi $f(x) = 0$ Galois rühm peab olema transitiivne.

Ümberpöördult, kui võrrandi $f(x) = 0$ Galois rühm K suhtes on transitiivne, siis saab näidata, et $f(x)$ on taandumatu korpuses K. Tõepoolest, kui $f(x)$ ei oleks taandumatu, siis peaks ta omama mittetriviaalset tegureiks lahutust $f(x) = \varphi(x)\psi(x)$. Olgu nüüd ξ_i polünoomi $\varphi(x)$ mingi lahend ja ξ_j $\psi(x)$ mingi lahend. Eeldades, et polünoomil $f(x)$ pole kordseid lahendeid, ei saa ξ_j olla ühtlasi polünoomi $\varphi(x)$ lahend. Seega on meil

$$\varphi(\xi_i) = 0, \quad \varphi(\xi_j) \neq 0.$$

Teiselt poolt peab võrrandi $f(x) = 0$ Galois rühmas leiduma transitiivsuse tõttu niisugune substitutsioon, mis teisendab selle võrrandi lahendi ξ_i lahendiks ξ_j ja seega võrduse $\varphi(\xi_i) = 0$ võrduseks $\varphi(\xi_j) = 0$, mis on vastuolus eelnenuga.

Tähendab, *kordsete lahenditeta polünoom $f(x)$ on taandumatu korpuses K siis ja ainult siis, kui võrrandi $f(x) = 0$ Galois rühm K suhtes on transitiivne.* Seega annab võrrandi $f(x) = 0$ Galois rühm tarviliku ja piisava tingimuse polünoomi $f(x)$ taanduvuse otsustamiseks. Praktiliselt kasutatakse seda tingimust sageli ümberpöördult võrrandi $f(x) = 0$ Galois rühma leidmiseks.

Leiame näitena võrrandi

$$x^5 - 4x - 2 = 0$$

Galois rühma ratsionaalarvude korpuse suhtes. Siin polünoom $x^5 - 4x - 2$ on Eisensteini kriteeriumi järgi taandumatu ratsionaalarvude korpuses, mistõttu vaadeldava võrrandi Galois rühm peab olema transitiivne. Teiselt poolt, rakendades Sturmi teo-

reemi, ei ole raske otsustada, et sel võrrandil on kolm reaallahendit ja seega kaks kaaskomplekslahendit, s. o.

$$\xi_1 = a + bi, \quad \xi_2 = a - bi, \quad \xi_3 = c, \quad \xi_4 = d, \quad \xi_5 = e,$$

kus a, b, c, d, e tähendavad reaalarve. Olgu nende lahendite vahel mingi ratsionaalne seos

$$R(\xi_1, \xi_2, \xi_3, \xi_4, \xi_5) = 0$$

ehk, pärast reaalosa ja imaginaarosa eraldamist,

$$P + Qi = 0.$$

Seega peab olema $P = 0$, $Q = 0$. Teostame nüüd lahendite indeksitega transpositsiooni (1 2), s. o. paigutame lahendid ξ_1 ja ξ_2 omavahel ümber. Et see transpositsioon on samaväärne i asendamisega $-i$-ga, siis

$$R(\xi_2, \xi_1, \xi_3, \xi_4, \xi_5) = P - Qi$$

ja järelikult

$$R(\xi_2, \xi_1, \xi_3, \xi_4, \xi_5) = 0,$$

sest $P = 0$, $Q = 0$. Seega transpositsioon (1 2), jättes invariantseks vaadeldava võrrandi lahenditevahelised seosed, peab kuuluma selle võrrandi Galois rühma. Kuid teoreemi 12 järgi (§ 23, art. 3) iga transitiivne rühm, mis sisaldab transpositsiooni, on kas sümmeetriline või imprimitiivne. Et aga viis numbrit 1, 2, 3, 4, 5 ei saa üldse jaguneda imprimitiivsuse klassideks, siis peab vaadeldava võrrandi Galois rühm kujutama sümmeetrilist rühma S_5.

3. Binoomvõrrandi Galois rühm. Vaatleme lähemalt lihtsaimat võrrandit

$$x^m - a = 0,$$

mille lahendid kujutavad m-astme juuri ja mis on tuntud binoomvõrrandi nime all. Eriti kui a on kompleksarv, siis nägime, et binoomvõrrandi kõik lahendid saab tuletada min-

gist ühest lahendist ξ korrutamisel vastavalt m-astme ühejuurtega

$$\varepsilon_0 = 1\,,\ \varepsilon_1\,,\ \varepsilon_2\,,\ \ldots\,,\ \varepsilon_{m-1}\,,$$

s. o. võrrandi $x^m - 1 = 0$ lahenditega (§ 1, art. 5). Ühejuurte kohta selgitasime, et nad moodustavad korrutamise suhtes tsüklilise rühma (§ 18, art. 3). Üldiselt saab ilmselt iga binoomvõrrandi $x^m - a = 0$ lahendeid tuletada mingist ühest lahendist ξ korrutamisel m-astme ühejuurtega, s. o. võrrandi

$$x^m - e = 0$$

lahenditega, kus e tähendab põhikorpuse K ühikelementi. Ei ole raske näha, et viimasel võrrandil pole kordseid lahendeid, kui põhikorpus K on karakteristikaga null. Tõepoolest, märkides $f(x) = x^m - e$, leiame $f'(x) = mx^{m-1}$, millest nähtub, et $f(x)$ ja $f'(x)$ on ühistegurita. Seega on võrrandil $x^m - e = 0$ m erinevat lahendit — m-astme ühejuurt

$$e\,,\ \varepsilon_1\,,\ \varepsilon_2\,,\ \ldots\,,\ \varepsilon_{m-1}\,,$$

mille kohta saab näidata, et nad moodustavad tsüklilise rühma korrutamise suhtes sõltumata põhikorpusest K. Et m-astme ühejuured moodustavad rühma, nähtub sellest, et nende hulk on kinnine korrutamise suhtes (§ 19, art. 2). Tõepoolest, kui ε_i ja ε_k on m-astme ühejuured, nii et $\varepsilon_i{}^m = e$, $\varepsilon_k{}^m = e$, siis

$$(\varepsilon_i\varepsilon_k)^m = \varepsilon_i{}^m\varepsilon_k{}^m = e\,,$$

s. o. korrutis $\varepsilon_i\varepsilon_k$ kujutab ka m-astme ühejuurt.

Jääb näidata, et m-astme ühejuurte rühm on tsükliline. Selleks tarvitseb vaid veenduda, et m-astme ühejuurte rühmas leidub vähemalt üks element ε, mille järk on m, sest siis astmed

$$\varepsilon^0 = e\,,\ \varepsilon\,,\ \varepsilon^2\,,\ \ldots\,,\ \varepsilon^{m-1}\,,$$

olles üksteisest erinevad, peavad kujutama kõiki m-astme ühejuuri. Lahutame arvu m korrutiseks

$$m = p_1{}^{\alpha_1}p_2{}^{\alpha_2}\ldots p_r{}^{\alpha_r}\,,$$

kus $p_1, p_2, \ldots, p_r$ on üksteisest erinevad algarvud. Ei ole raske näha, et ei leidu enam kui $\frac{m}{p_i}$ niisugust m-astme ühejuurt a, mille puhul

$$a^{\frac{m}{p_i}} = e,$$

sest võrrandil $x^{\frac{m}{p_i}} - e = 0$ ei saa olla korpuses enam kui $\frac{m}{p_i}$ lahendit. Seetõttu leidub alati niisuguseid m-astme ühejuuri a_i, mille puhul

$$a_i^{\frac{m}{p_i}} \neq e.$$

Vaatleme ühejuurt

$$\varepsilon_i = a_i^{mp_i^{-\alpha_i}}$$

ja leiame tema kui rühma elemendi järgu m_i. Et

$$\varepsilon_i^{p_i^{\alpha_i}} = a_i^m = e, \tag{5}$$

siis on ε_i järk ülimalt $p_i^{\alpha_i}$, s. o. $m_i \leqslant p_i^{\alpha_i}$. Jagades $p_i^{\alpha_i}$ arvuga m_i, saame

$$p_i^{\alpha_i} = qm_i + r,$$

kus $0 \leqslant r < m_i$ ja seega $\varepsilon_i^{m_i} = e$ tõttu

$$\varepsilon_i^{p_i^{\alpha_i}} = \varepsilon_i^{qm_i}\varepsilon_i^r = \varepsilon_i^r,$$

millest (5) järgi $\varepsilon_i^r = e$. Et aga m_i kui ε_i järk on väikseim naturaalarv, mille puhul $\varepsilon_i^{m_i} = e$, siis peab olema $r = 0$ ja järelikult

$$p_i^{\alpha_i} = qm_i,$$

mistõttu m_i kui $p_i^{\alpha_i}$ jagaja peab omama kuju

$$m_i = p_i^{\alpha},$$

kus $\alpha \leqslant \alpha_i$. Näitame, et $\alpha = \alpha_i$. Nimelt, kui oleks $\alpha < \alpha_i$, siis silmas pidades, et

$$\varepsilon_i^{m_i} = a_i^{mp_i^{-\alpha_i}} p_i^{\alpha} = a_i^{mp_i^{\alpha-\alpha_i}},$$

peaks $\varepsilon_i^{m_i} = e$ tõttu olema

$$\left(a_i^{mp_i^{\alpha-\alpha_i}}\right)^{p_i^{\alpha_i-\alpha-1}} = e$$

ehk

$$a_i^{\frac{m}{p_i}} = e,$$

vastuolus a_i valikuga. Seepärast on $\alpha = \alpha_i$ ja seega $m_i = p_i^{\alpha_i}$. Korrutise

$$\varepsilon = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_r$$

järk on siis

$$p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} = m,$$

sest järgud $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, ..., $p_r^{\alpha_r}$ on paarikaupa ühistegurita (§ 18, art. 3). Seega on m-astme ühejuurte rühm tõesti tsükliline, kusjuures ε kujutab algjuurt.

Ei ole raske näha, et ülaltoodud tõestuskäik jääb püsima ka korpuses karakteristikaga $p \geqslant 2$, kui ainult ühejuured on kõik üksteisest erinevad.

Piirdudes algarvulise astmega võrrandiga $x^p - e = 0$, tõestame järgmise teoreemi:

Teoreem 4. *Algarvulise p puhul on võrrandi $x^p - e = 0$ Galois rühm tsükliline, kusjuures tema järk on $p - 1$ jagajaks.*

Teoreemi 4 tõestuseks vaatleme algul juhtu, kus põhikorpuseks on mingi algkorpus P. Kui ε on mingi p-astme algjuur, siis laiend $P(\varepsilon)$ kujutab polünoomi $x^p - e$ lahutuskorpust. Siin elemendi ε aste P suhtes on $p - 1$, sest ε rahuldab võrrandit

$$x^{p-1} + x^{p-2} + \ldots + x + e = 0,$$

mis saadakse võrrandi $x^p - e = 0$ jagamisel lineaarteguriga $x - e$. Seejuures on polünoom $x^{p-1} + x^{p-2} + \ldots + x + e$ taan-

dumatu korpuses P, kuna P kui algkorpus karakteristikaga null on isomorfne ratsionaalarvude korpusega (§ 25, art. 1), ratsionaalarvude korpuses on aga vaadeldav polünoom taandumatu (§ 8, art. 2).

Niisiis koosneb võrrandi $x^p - e = 0$ Galois rühm algkorpuse P suhtes $p - 1$ automorfismist s_0, s_1, s_2, ..., s_{p-2}. Nende automorfismide leidmiseks vaatleme silmapilguks $(p-1)$-astme võrrandit

$$x^{p-1} - 1 = 0$$

üle jäägiklassikorpuse $R^{(p)}$. Selle võrrandi lahenditeks, s. o. $(p-1)$-astme ühejuurteks üle $R^{(p)}$ on $R^{(p)}$ nullist erinevad elemendid 1, 2, 3, ..., $p-1$, sest $R^{(p)}$ iga elemendi a puhul on Fermat' valemi järgi (I, § 8, art. 3)

$$a^p = a,$$

millest $a \neq 0$ korral

$$a^{p-1} = 1.$$

Et siin ühejuured 1, 2, 3, ..., $p-1$ on kõik üksteisest erinevad, siis moodustavad nad tsüklilise rühma. Seetõttu leidub niisugune $(p-1)$-astme ühejuur b, mille astmed

$$b^0 = 1,\ b,\ b^2,\ \ldots,\ b^{p-2}$$

kujutavad kõiki $(p-1)$-astme ühejuuri 1, 2, 3, ..., $p-1$.

Seega võime elemendi ε kaaselemendid ε, ε^2, ε^3, ..., ε^{p-1} esitada kujul

$$\varepsilon,\ \varepsilon^b,\ \varepsilon^{b^2},\ \ldots,\ \varepsilon^{b^{p-2}}$$

ja määrata võrrandi $x^p - e = 0$ Galois rühma automorfismid s_0, s_1, s_2, ..., s_{p-2} vastavalt tingimustega

$$\varepsilon s_0 = \varepsilon,\ \varepsilon s_1 = \varepsilon^b,\ \varepsilon s_2 = \varepsilon^{b^2},\ \ldots,\ \varepsilon s_{p-2} = \varepsilon^{b^{p-2}}.$$

Et

$$\varepsilon s_1^2 = (\varepsilon s_1) s_1 = (\varepsilon^b) s_1 = (\varepsilon s_1)^b = (\varepsilon^b)^b = \varepsilon^{b^2},$$

siis $s_1^2 = s_2$. Edasi on

$$\varepsilon s_1^3 = (\varepsilon s_1^2) s_1 = (\varepsilon^{b^2}) s_1 = (\varepsilon s_1)^{b^2} = (\varepsilon^b)^{b^2} = \varepsilon^{b^3}$$

ja seega $s_1^3 = s_3$. Üldiselt ei ole raske näha, et $\varepsilon s_1^k = \varepsilon^{b^k}$, millest $s_1^k = s_k$. Niisiis on võrrandi $x^p - e = 0$ Galois rühm algkorpuse P suhtes tsükliline, kusjuures tema järk on $p - 1$.

Juhul kui põhikorpus K ei ole algkorpus, vaatleme K-s sisalduvat algkorpust P. Olgu G_0 võrrandi $x^p - e = 0$ Galois rühm P suhtes ja G selle võrrandi Galois rühm K suhtes, s. o. $G_0 = P(\varepsilon)\,(P)$, $G = K(\varepsilon)\,(K)$. Küsime, kuidas on seotud rühmad G_0 ja G. Et $P \subset K$, siis $P(\varepsilon) \subset K(\varepsilon)$. Olgu s mingi automorfism rühmas G, s. o. niisugune korpuse $K(\varepsilon)$ automorfism, mis jätab K elemendid invariantseks. Automorfism s teisendab algjuure ε mingiks ühejuureks ε_i ja seega korpuse $P(\varepsilon)$ korpuseks $P(\varepsilon_i)$. Et ε ja ε_i on kaaselemendid P suhtes, siis $P(\varepsilon) = P(\varepsilon_i)$, sest $P(\varepsilon)$ kui polünoomi lahutuskorpus on Galois korpus. Seega iga automorfism s rühmas G kutsub esile korpuse $P(\varepsilon)$ automorfismi $\bar{s}$, mille puhul P elemendid jäävad invariantseks ja mis kuulub seega rühma G_0. Märkides G automorfismide s poolt esile kutsutud G_0 automorfismide $\bar{s}$ hulga tähega $\bar{G}$, võib kergesti veenduda, et leiab aset isomorfism

$$\bar{G} \longleftrightarrow G,$$

mis ütleb, et $\bar{G}$ on rühm ja nimelt G_0 alamrühm. G_0 on aga eelnenu põhjal tsükliline rühm järku $p - 1$. Siis on ka alamrühm $\bar{G}$ — ja ühes sellega G — tsükliline (§ 19, art. 2) ja tema järk on Lagrange'i teoreemi põhjal $p - 1$ jagajaks. Seega on teoreem 4 tõestatud.

Tuleme nüüd binoomvõrrandi

$$x^p - a = 0$$

juurde, kusjuures eeldame, et põhikorpus K sisaldab kõiki p-astme ühejuuri. Kui ξ tähendab mingit selle binoomvõrrandi

lahendit ja ε p-astme algjuurt, siis avalduvad kõik lahendid kujul

$$\xi\,,\ \xi\varepsilon\,,\ \xi\varepsilon^2,\ \ldots,\ \xi\varepsilon^{p-1},$$

millest nähtub, et binoomi $x^p - a$ lahutuskorpuseks on laiend $\Sigma = K(\xi)$. Tähendagu

$$\xi_1 = \xi\,,\ \xi_2 = \xi\varepsilon^{a_2},\ \xi_3 = \xi\varepsilon^{a_3},\ \ldots,\ \xi_k = \xi\varepsilon^{a_k}$$

ξ kaaselemente K suhtes. Binoomvõrrandi $x^p - a = 0$ Galois rühm $G = \Sigma(K)$ koosneb siis k automorfismist s_0, s_1, s_2, $\ldots$, s_{k-1}, mis on määratud tingimustega

$$\xi s_0 = \xi\,,\ \xi s_1 = \xi\varepsilon^{a_2},\ \xi s_2 = \xi\varepsilon^{a_3},\ \ldots,\ \xi s_{k-1} = \xi\varepsilon^{a_k}.$$

Seades siin igale automorfismile s_i vastavusse selle p-astme ühejuure ε^{a_i+1}, millega korrutub ξ automorfismi s_i rakendamisel, saame ilmselt üksühese vastavuse, kusjuures see vastavus säilib korrutamise puhul. Nimelt kui

$$s_i \longleftrightarrow \varepsilon^{a_i+1},\quad s_j \longleftrightarrow \varepsilon^{a_j+1},$$

siis

$$s_i s_j \longleftrightarrow \varepsilon^{a_i+1}\varepsilon^{a_j+1},$$

sest

$$\xi(s_i s_j) = (\xi s_i)s_j = (\xi\varepsilon^{a_i+1})s_j = \varepsilon^{a_i+1}(\xi s_j) = \varepsilon^{a_i+1}\varepsilon^{a_j+1},$$

kuna ε^{a_i+1} kui K element on invariantne s_j suhtes. Niisiis on k-st p-astme ühejuurest koosnev hulk

$$H = \{e\,,\ \varepsilon^{a_2},\ \varepsilon^{a_3},\ \ldots,\ \varepsilon^{a_k}\}$$

isomorfne Galois rühmaga G, mistõttu H osutub rühmaks. Et kõigi p-astme ühejuurte rühm on tsükliline, siis on ka H tsükliline (§ 19, art. 2), kusjuures H järk on Lagrange'i teoreemi põhjal p jagajaks, s. o. kas p või 1. Seega on ka Galois rühm G tsükliline, omades kas järku p või 1. Kui G järk on p, siis on ξ aste K suhtes p ja binoom $x^p - a$ on taandumatu korpuses K. Kui aga G järk on 1, siis on ξ aste K suhtes 1, nii et laiend

$K(\xi)$ langeb ühte K-ga ja binoom $x^p - a$ laguneb lineaartegurite korrutiseks juba põhikorpuses K.

Niisugust Galois korpust, mille Galois rühm on tsükliline, nimetatakse tsükliliseks korpuseks. Tähendab, *kui põhikorpus K sisaldab kõiki p-astme ühejuuri, siis on binoomi $x^p - a$ lahutuskorpus kas tsükliline korpus astmega p või langeb ühte K-ga.* On kehtiv ka ümberpöördud väide, mille sõnastame iseseisva teoreemina.

Teoreem 5. *Kui põhikorpus K sisaldab kõiki p-astme ühejuuri, siis võib iga tsüklilist p-astme Galois korpust $K(\xi)$ vaadelda teatava binoomi $x^p - a$ lahutuskorpusena.*

Teoreemi 5 eelduste kohaselt omab Galois korpuse $K(\xi)$ Galois rühm G kuju

$$G = \{e, s, s^2, \ldots, s^{p-1}\}.$$

Teisendagu G automorfismid elemendi ξ vastavalt kaaselementideks $\xi_1 = \xi, \xi_2, \xi_3, \ldots, \xi_p$, s. o.

$$\xi e = \xi, \quad \xi s = \xi_2, \quad \xi s^2 = \xi_3, \quad \ldots, \quad \xi s^{p-1} = \xi_p.$$

Moodustame avaldise

$$\xi + \varepsilon^\nu \xi_2 + \varepsilon^{2\nu} \xi_3 + \ldots + \varepsilon^{(p-1)\nu} \xi_p,$$

kus ε tähendab mingit p-astme algjuurt ja ν mingit täisarvu. Seda avaldist nimetatakse Lagrange'i resolvendiks ja märgitakse sümboliga (ξ, ε^ν). Näitame, et siin võib ν alati nii valida, et resolvent (ξ, ε^ν) kujutab mingit $K(\xi)$ elementi väljaspool põhikorpust K. Tõepoolest, vastasel korral kuuluksid resolvendid

$$\begin{aligned}
(\xi, \varepsilon^0) &= \xi + \xi_2 + \xi_3 + \ldots + \xi_p \\
(\xi, \varepsilon) &= \xi + \varepsilon\xi_2 + \varepsilon^2\xi_3 + \ldots + \varepsilon^{p-1}\xi_p \\
(\xi, \varepsilon^2) &= \xi + \varepsilon^2\xi_2 + \varepsilon^4\xi_3 + \ldots + \varepsilon^{2(p-1)}\xi_p \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
(\xi, \varepsilon^{p-1}) &= \xi + \varepsilon^{p-1}\xi_2 + \varepsilon^{2(p-1)}\xi_3 + \ldots + \varepsilon^{(p-1)^2}\xi_p
\end{aligned}$$

kõik põhikorpusse K ja seega kuuluks sinna ka nende summa

$$\sum_{\nu=0}^{p-1}(\xi\,,\ \varepsilon^\nu) = p\xi + \xi_2 \sum_{\nu=0}^{p-1}\varepsilon^\nu + \xi_3 \sum_{\nu=0}^{p-1}\varepsilon^{2\nu} + \ldots + \xi_p \sum_{\nu=0}^{p-1}\varepsilon^{(p-1)\nu}.$$

Nüüd on aga geomeetrilise rea summa valemi põhjal

$$\sum_{\nu=0}^{p-1}\varepsilon^{i\nu} = \frac{\varepsilon^{ip}-e}{\varepsilon-e} = \frac{e-e}{\varepsilon-e} = 0\,,$$

sest $\varepsilon^{ip} = (\varepsilon^p)^i = e^i = e$, ja seega

$$\sum_{\nu=0}^{p-1}(\xi\,,\ \varepsilon^\nu) = p\xi\,,$$

millest

$$\xi = \frac{1}{p}\sum_{\nu=0}^{p-1}(\xi\,,\ \varepsilon^\nu).$$

Järelikult peab ka ξ kuuluma põhikorpusse K. Siis aga langeks Galois korpus $K(\xi)$ ühte K-ga ega kujutaks üldse K laiendit. Seetõttu peab leiduma niisugune ν väärtus, mille puhul vastav resolvent $\Theta = (\xi\,,\ \varepsilon^\nu)$ ei kuulu põhikorpusse K.

Rakendame nüüd sel viisil valitud resolvendile Θ automorfismi s. Et

$$\xi s = \xi_2\,,\ \ \xi_2 s = (\xi s)s = \xi s^2 = \xi_3\,,\ \ldots\,,$$
$$\xi_{p-1}s = (\xi s^{p-2})s = \xi s^{p-1} = \xi_p\,,\ \ \xi_p s = (\xi s^{p-1})s = \xi s^p = \xi e = \xi\,,$$

siis

$$\begin{aligned}\Theta s &= \xi s + \varepsilon^\nu(\xi_2 s) + \varepsilon^{2\nu}(\xi_3 s) + \ldots + \\ &\quad + \varepsilon^{(p-2)\nu}(\xi_{p-1}s) + \varepsilon^{(p-1)\nu}(\xi_p s) = \\ &= \xi_2 + \varepsilon^\nu\xi_3 + \varepsilon^{2\nu}\xi_4 + \ldots + \varepsilon^{(p-2)\nu}\xi_p + \varepsilon^{(p-1)\nu}\xi = \\ &= \varepsilon^{-\nu}(\xi + \varepsilon^\nu\xi_2 + \varepsilon^{2\nu}\xi_3 + \ldots + \varepsilon^{(p-1)\nu}\xi_p) = \varepsilon^{-\nu}\,\Theta\,.\end{aligned}$$

Niisiis korrutub Θ automorfismi s toimel teguriga $\varepsilon^{-\nu}$. Rakendades automorfismi s resolvendile Θ järjest i korda, saame

$$\Theta s^i = \varepsilon^{-i\nu}\,\Theta$$

ja seega

$$\Theta^p S^i = (\Theta S^i)^p = (\varepsilon^{-i\nu}\Theta)^p = \varepsilon^{-i\nu p}\Theta^p = \Theta^p,$$

sest

$$\varepsilon^{-i\nu p} = (\varepsilon^p)^{-i\nu} = e^{-i\nu} = e\,.$$

Järelikult element Θ^p, jäädes invariantseks Galois rühma $G = \{e, s, s^2, \ldots, s^{p-1}\}$ iga automorfismi s^i suhtes, kuulub teoreemi 3 järgi (art. 1) põhikorpusse K, s. o.

$$\Theta^p = a\,, \quad a \in K\,.$$

Teiste sõnadega, Θ rahuldab binoomvõrrandit

$$x^p - a = 0\,.$$

Et põhikorpus K sisaldab eelduse kohaselt kõiki p-astme ühejuuri, siis on binoomi $x^p - a$ lahutuskorpuseks laiend $K(\Theta)$. Teoreemi 5 tõestuseks jääb näidata, et $K(\Theta) = K(\xi)$.

Kõigepealt on ilmne, et $\Theta = (\xi, \varepsilon^\nu)$, avaldudes ratsionaalselt $\xi_1 = \xi, \xi_2, \xi_3, \ldots, \xi_p$ kaudu, kuulub korpusse $K(\xi)$. Mis puutub Θ astmesse K suhtes, s. o. $x^p - a$ lahutuskorpuse astmesse, siis võib see eelnenu põhjal olla kas p või 1. Et teisel juhul langeb $K(\Theta)$ ühte K-ga, siis jääb see võimalus ära, kuna Θ ei kuulu valiku kohaselt põhikorpusse K. Seega peab olema $(\Theta : K) = p$. Et eelduse järgi ka $(\xi : K) = p$, siis

$$(\Theta : K) = (\xi : K),$$

kust teoreemi 8 põhjal (§ 25, art. 3)

$$K(\Theta) = K(\xi),$$

millega on teoreem 5 tõestatud.

§ 28. Galois teooria põhilause.

1. Alamkorpuste ja alamrühmade vastavus. Galois rühma tähtsus seisneb selles, et ta võimaldab selgitada Galois korpuse $\Sigma = K(\xi)$ struktuuri, lubades määrata kõik vahepealsed

korpused K ja Σ vahel koos nendevaheliste seostega. Nimelt leiab Galois korpuse alamkorpuste ja tema Galois rühma alamrühmade vahel aset üksühene vastavus, mis väljendub alljärgnevas Galois teooria põhilauses.

Teoreem 6. *Vastavalt Galois korpuse $\Sigma = K(\xi)$ igale alamkorpusele $\Delta \supset K$ leidub niisugune Galois rühma $G = \Sigma(K)$ alamrühm H, mis koosneb kõigist nendest G automorfismidest, mis jätavad Δ elemendid invariantseks ja ainult need. Ümberpöördult, vastavalt Galois rühma G igale alamrühmale H leidub Galois korpuse Σ niisugune alamkorpus $\Delta \supset K$, mis koosneb nendest Σ elementidest, mis jäävad invariantseks H automorfismide puhul ja ainult nende puhul.*

Teoreemi 6 esimese osa tõestuseks paneme tähele, et $\Sigma = K(\xi)$ on algebraline lihtlaiend ka iga vahepealse korpuse Δ suhtes, nimelt $\Sigma = \Delta(\xi)$. Tõepoolest, ühelt poolt on $\Delta \supset K$ tõttu

$$\Delta(\xi) \supset K(\xi)$$

ja teiselt poolt $\Delta \subset K(\xi)$ tõttu

$$\Delta(\xi) \subset K(\xi),$$

sest $\Delta(\xi)$ on väikseim korpus, mis sisaldab Δ-t ja ξ-d. Edasi saab näidata, et Σ on Galois korpus ka Δ suhtes. Tõepoolest olgu $q(x)$ mingi korpuses Δ taandumatu polünoom, mis omagu laiendis $\Sigma = \Delta(\xi)$ lahendit Θ. Kõik polünoomid üle Δ, mis omavad lahendit Θ, avalduvad siis kujul

$$q(x)r(x),$$

kus $r(x)$ tähendab mingit polünoomi üle Δ (§ 25, art. 3). Kuid Θ kui Σ element, olles algebraline K suhtes, rahuldab teatavat võrrandit

$$p(x) = 0,$$

kus $p(x)$ on korpuses K taandumatu polünoom. Et aga Σ on K suhtes Galois korpus, siis $p(x)$, omades laiendis Σ lahendit Θ, laguneb siin täielikult lineaartegurite korrutiseks. Vaadel-

des, teiselt poolt, $p(x)$-i kui polünoomi üle Δ ja pidades silmas, et $p(\Theta) = 0$, peab olema

$$p(x) = q(x)r(x),$$

mistõttu ka $q(x)$ laguneb laiendis Σ täielikult lineaartegurite korrutiseks. Tähendab, Σ on Galois korpus ka Δ suhtes.

Olgu nüüd H korpuse $\Sigma = \Delta(\xi)$ Galois rühm Δ suhtes, s. o. $H = \Sigma(\Delta)$. Galois rühma mõiste kohaselt koosneb H kõigist neist Σ automorfismidest, mis jätavad Δ elemendid invariantseks. Seega jätavad H automorfismid ammugi K elemendid invariantseks, mistõttu $H \subset G$. Teoreemi 3 järgi (§ 27, art. 1) jätavad H automorfismid ainult Δ elemendid invariantseks, millega on teoreemi 6 esimene osa tõestatud.

Ümberpöördult, kui on antud Galois rühma $G = \Sigma(K)$ mingi alamrühm H, siis märgime Δ-ga nende Σ elementide hulga, mis jäävad invariantseks kõigi H automorfismide puhul. Ei ole raske näha, et siin $\Delta \subset \Sigma$ kujutab korpust, sest kui $\alpha \in \Delta$ ja $\beta \in \Delta$, s. o. $\alpha s = \alpha$ ja $\beta s = \beta$ iga $s \in H$ puhul, siis

$$(\alpha - \beta)s = \alpha s - \beta s = \alpha - \beta, \quad \left(\frac{\alpha}{\beta}\right)s = \frac{\alpha s}{\beta s} = \frac{\alpha}{\beta},$$

ja seega on täidetud alamkorpuse tingimused

$$\alpha - \beta \in \Delta, \quad \frac{\alpha}{\beta} \in \Delta.$$

Jääb näidata, et Δ elemendid jäävad invariantseks a i n u l t H automorfismide puhul, nii et H sisaldab k õ i k i neid Σ automorfisme, mis jätavad Δ elemendid invariantseks ehk, teiste sõnadega, et H on Σ Galois rühm Δ suhtes, s. o. $H = \Sigma(\Delta)$. Olgu h rühma H järk ja h_1 Galois rühma $H_1 = \Sigma(\Delta)$ järk; siis on $h_1 \geqslant h$. Et $h_1 = (\Sigma : \Delta)$ ja $\Sigma = \Delta(\xi)$, siis $h_1 = (\xi : \Delta)$. Nüüd võib aga näidata, et $(\xi : \Delta) \leqslant h$, s. o. $h_1 \leqslant h$, mistõttu peab olema $h_1 = h$ ja siis ka $H_1 = H$.

Seose $(\xi : \Delta) \leqslant h$ tõestuseks vaatleme rühma

$$H = \{s_0, s_1, s_2, \ldots, s_{h-1}\},$$

mille automorfismid s_i teisendavad laiendi $\Sigma = \Delta(\xi)$ moodustava elemendi ξ kaaselementideks

$$\xi s_0 = \xi\,,\quad \xi s_1 = \xi_2\,,\quad \xi s_2 = \xi_3\,,\quad \ldots\,,\quad \xi s_{h-1} = \xi_h\,.$$

Moodustame h-astme polünoomi

$$g(x) = (x - \xi)(x - \xi_2)(x - \xi_3)\ldots(x - \xi_h) = \\ = x^h - \sigma_1 x^{h-1} + \sigma_2 x^{h-2} - \ldots + (-1)^h \sigma_h\,.$$

Siin kordajad

$$\sigma_1 = \xi + \xi_2 + \xi_3 + \ldots + \xi_h$$
$$\sigma_2 = \xi\xi_2 + \xi\xi_3 + \ldots + \xi_{h-1}\xi_h$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\sigma_h = \xi\xi_2\xi_3\ldots\xi_h$$

on invariantsed H automorfismide s_i suhtes. Nii on näiteks

$$\sigma_1 s_i = \xi s_i + \xi_2 s_i + \xi_3 s_i + \ldots + \xi_h s_i = \\ = \xi s_0 s_i + \xi s_1 s_i + \xi s_2 s_i + \ldots + \xi s_{h-1} s_i\,,$$

kus korrutised $s_0 s_i$, $s_1 s_i$, $s_2 s_i$, $\ldots$, $s_{h-1} s_i$ kujutavad jälle automorfisme s_0, s_1, s_2, $\ldots$, s_{h-1}, kuid mingis teises järjestuses, mistõttu $\sigma_1 s_i = \sigma_1$. Seepärast kordajad σ_i, olles invariantsed kõigi H automorfismide suhtes, kuuluvad Δ mõiste kohaselt korpusse Δ. Et $g(\xi) = 0$, siis ongi

$$(\xi : \Delta) \leqslant h\,,$$

millega on ka teoreemi 6 teine osa tõestatud.

Galois teooria põhilauset võime lühidalt sõnastada järgmiselt: Galois korpuse $\Sigma = K(\xi)$ alamkorpuste $\Delta \supset K$ ja vastava Galois rühma $G = \Sigma(K)$ alamrühmade H vahel valitseb üksühene vastavus

$$\Delta \longleftrightarrow H\,,$$

kus $H = \Sigma(\Delta)$. Eriti vastab põhikorpusele K Galois rühm $G = \Sigma(K)$ ja laiendile Σ Galois rühm $\Sigma(\Sigma)$, s. o. ühikrühm E.

Olgu Δ_1, Δ_2 kaks Σ alamkorpust, kusjuures $\Delta_1 \subset \Delta_2$, ja olgu H_1, H_2 neile vastavad Galois rühma $G = \Sigma(K)$ alamrühmad, nimelt

$$H_1 = \Sigma(\Delta_1), \quad H_2 = \Sigma(\Delta_2).$$

Siis on $H_1 \supset H_2$, sest need G elemendid, mis jätavad Δ_2 elemendid invariantseks, jätavad ammugi invariantseks Δ_1 elemendid. Seega vastab Galois korpuse alamkorpuste kasvavale jadale vastava Galois rühma alamrühmade kahanev jada ja ümberpöördult, s. o.

$$\begin{array}{ccccccc} K & \subset & \Delta_1 & \subset & \Delta_2 & \subset & \Sigma \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ G & \supset & H_1 & \supset & H_2 & \supset & E. \end{array}$$

Galois teooria põhilausega fikseeritud üksühene vastavus Galois korpuse alamkorpuste ja vastava Galois rühma alamrühmade vahel võimaldab tunduvalt lihtsustada Galois korpuse struktuuri uurimist, sest Galois rühm on oma lõplikkuse tõttu palju kergemini käsiteldav kui lõpmatu Galois korpus.

2. Järeldusi Galois teooria põhilausest. Olgu $G = \Sigma(K)$ Galois korpuse $\Sigma = K(\xi)$ Galois rühm, $\Delta \supset K$ mingi Σ alamkorpus ja H temale Galois teooria põhilause järgi vastav alamrühm, s. o. $H = \Sigma(\Delta)$. Rühma H järk on seega $(\Sigma : \Delta)$ (§ 27, art. 1). Tekib küsimus, missugune on H indeks (H, G), s. o. G kõrvalklasside arv H järgi. Selle küsimuse lahendamiseks selgitame kõigepealt, missugused G automorfismid kuuluvad kõrvalklassi Hs, kus s tähendab mingit G automorfismi.

Kõrvalklassi mõiste kohaselt koosneb Hs kõigist niisugustest automorfismidest $t = hs$, kus $h \in H$. Olgu Θ alamkorpuse Δ moodustav element (§ 26, art. 3), nii et $\Delta = K(\Theta)$. Rakendades elemendile Θ automorfismi $t = hs$, leiame

$$\Theta t = (\Theta h)s = \Theta s,$$

sest kuna H automorfismid jätavad Δ elemendid invariantseks, siis $\Theta h = \Theta$. Tähendab, kõrvalklassi Hs automorfismid teisen-

davad Θ ikka üheks ja samaks elemendiks Θs. Näitame, et Hs koosneb k õ i g i s t neist G automorfismidest, mis teisendavad Θ elemendiks Θs. Nimelt kui t on mingi G automorfism, mis teisendab Θ elemendiks Θs, siis, rakendades võrduse $\Theta t = \Theta s$ mõlemale poolele automorfismi s^{-1}, saame

$$\Theta t s^{-1} = \Theta .$$

Tulemusest nähtub, et automorfism ts^{-1} jätab laiendi $\Delta = K(\Theta)$ moodustava elemendi — ja seega selle laiendi iga elemendi — invariantseks, mistõttu ts^{-1} peab kuuluma alamrühma H, s. o.

$$ts^{-1} = h ,$$

kus $h \in H$. Viimasest võrdusest saame $t = hs$, mis ütleb, et t kuulub kõrvalklassi Hs. Niisiis koosneb kõrvalklass Hs kõigist neist G automorfismidest, mis teisendavad laiendi Δ moodustava elemendi Θ üheks ja samaks elemendiks Θs.

Et teoreemi 2 järgi (§ 27, art. 1) Θs kujutab Θ kaaselementi K suhtes, siis on G kõrvalklasside arv H järgi võrdne Θ kaaselementide arvuga, s. o. Θ astmega K suhtes, ehk, mis sama on, Δ astmega K suhtes. Seega

$$(H , G) = (\Delta : K). \tag{6}$$

Silmas pidades, et rühma G järgu $n = (\Sigma : K)$, alamrühma H järgu $m = (\Sigma : \Delta)$ ja indeksi $j = (H , G)$ vahel kehtib seos $n = mj$ (§ 19, art. 3), leiame

$$(\Sigma : K) = (\Sigma : \Delta)(\Delta : K). \tag{7}$$

Selgitame veel küsimuse, missugusel tingimusel osutub Galois korpuse Σ alamkorpus $\Delta \supset K$ ise ka Galois korpuseks. Vaatleme selleks algul peale Δ veel mingit tema kaaslaiendit $\bar{\Delta}$. Olgu H ja $\bar{H}$ korpustele Δ ja $\bar{\Delta}$ Galois teooria põhilause mõttes vastavad alamrühmad ja s automorfism, mis teisen-

dab laiendi Δ kaaslaiendiks $\bar{\Delta}$ (§ 27, art. 1). Rakendades $\bar{\Delta}$ mistahes elemendile $\bar{\Theta}$ automorfismi $s^{-1}hs$, kus $h \in H$, saame

$$\bar{\Theta} s^{-1}hs = (\bar{\Theta} s^{-1})hs = \Theta hs .$$

Siin element $\Theta = \bar{\Theta} s^{-1}$ kuulub korpusse Δ, sest automorfism s^{-1} teisendab korpuse $\bar{\Delta}$ korpuseks Δ. Et H automorfismid jätavad Δ elemendid invariantseks, siis

$$\Theta hs = (\Theta h)s = \Theta s = (\bar{\Theta} s^{-1})s = \bar{\Theta} ,$$

ja seega

$$\bar{\Theta} s^{-1}hs = \bar{\Theta} .$$

Järelikult automorfism $s^{-1}hs$, jättes $\bar{\Delta}$ iga elemendi $\bar{\Theta}$ invariantseks, kuulub alamrühma $\bar{H}$, s. o. $s^{-1}hs \in \bar{H}$ ja seega

$$s^{-1}Hs \subset \bar{H} .$$

Rakendades, ümberpöördult, Δ mistahes elemendile Θ automorfismi $s\bar{h}s^{-1}$, kus $\bar{h} \in \bar{H}$, leiame analoogiliselt eelnenuga, et $s\bar{H}s^{-1} \subset H$, millest

$$\bar{H} \subset s^{-1}Hs .$$

Järelikult

$$\bar{H} = s^{-1}Hs ,$$

mis ütleb, et $\bar{H}$ on H kaasalamrühm.

Näitame, et ümberpöördult, kui H ja $\bar{H}$ on Galois rühmas G teineteise kaasalamrühmad, siis kujutavad neile Galois teooria põhilause järgi vastavad Σ alamkorpused Δ ja $\bar{\Delta}$ teineteise kaaslaiendeid. Olgu nimelt $\bar{H} = s^{-1}Hs$ ja teisendagu automorfism s korpuse Δ korpuseks Δ_1. Kui korpusele Δ_1 vastab Galois teooria põhilause järgi alamrühm H_1, siis on eelnenu põhjal $H_1 = s^{-1}Hs$ ja seega $H_1 = \bar{H}$. Et aga vastavus Galois teooria põhilauses on

üksühene, siis ka $\Delta_1 = \bar{\Delta}$, nii et s teisendab korpuse Δ korpuseks $\bar{\Delta}$. Teoreemi 1 järgi (§ 27, art. 1) on siis Δ ja $\bar{\Delta}$ kaaslaiendid. Niisiis vastavad Galois teooria põhilause mõttes kaaslaienditele kaasalamrühmad ja ümberpöördult.

Eriti kui Δ on Galois korpus, siis ühtib ta kõigi oma kaaslaienditega (§ 26, art. 2), mistõttu Δ-le vastav alamrühm H ühtib kõigi oma kaasalamrühmadega ja kujutab seega normaaljagajat (§ 20, art. 4). Ümberpöördult, kui H on normaaljagaja, siis ühtib ta kõigi oma kaasalamrühmadega, mistõttu H-le vastav alamkorpus Δ ühtib kõigi oma kaaslaienditega ja kujutab seega Galois korpust. Tähendab, *Galois korpuse Σ alamkorpus Δ kujutab Galois korpust K suhtes siis ja ainult siis, kui Δ-le vastav alamrühm H on Galois rühma $\Sigma(K)$ normaaljagaja.*

Kui nüüd Δ osutub Galois korpuseks, siis tekib küsimus, kuidas avaldub tema Galois rühm $\bar{G} = \Delta(K)$. Selle küsimuse selgitamiseks vaatleme mingit $G = \Sigma(K)$ automorfismi s, mis teisendagu Δ kaaslaiendiks $\bar{\Delta}$. Et Δ on Galois korpus, siis $\bar{\Delta} = \Delta$, mistõttu s kutsub esile Δ automorfismi

$$\Delta \overset{+}{\longleftrightarrow} \Delta,$$

mille puhul põhikorpuse K elemendid jäävad invariantseks. Märkides s-i poolt esile kutsutud Δ automorfismi, s. o. selle osa automorfismist s, mis puudutab Δ elemente, tähega $\bar{s}$, korraldame vastavuse

$$s \longrightarrow \bar{s}.$$

Et $\Sigma = \Delta(\xi)$ (art. 1), siis võib iga Δ automorfismi jätkata teatavaks Σ automorfismiks (§ 26, art. 1), mistõttu rühm G teisendub vastavuses $s \longrightarrow \bar{s}$ rühmaks $\bar{G}$. Ei ole raske näha, et vastavus $s \longrightarrow \bar{s}$ säilib korrutamise puhul ja osutub seega homomorfismiks

$$G \longrightarrow \bar{G}.$$

Rakendades teoreemi rühma homomorfismidest (§ 21, art. 2), võime järelikult kirjutada

$$\overline{G} \longleftrightarrow G/H,$$

kus normaaljagaja H koosneb neist G automorfismidest, millele vastab $\overline{G}$ ühikelement, s. o. Δ identne automorfism. Teiste sõnadega, H koosneb neist G automorfismidest, mis jätavad Δ elemendid invariantseks, s. o. H on Δ-le Galois teooria põhilause järgi vastav alamrühm. Tähendab, *kui Galois korpuse Σ alamkorpus Δ on ka Galois korpus K suhtes, siis on Galois rühm $\Delta(K)$ isomorfne faktorrühmaga G/H, kus $G = \Sigma(K)$ ja H on alamkorpusele Δ vastav alamrühm.*

Uurime näitena polünoomi $x^3 - 2$ lahutuskorpuse Σ struktuuri, kui põhikorpuseks K on ratsionaalarvude korpus. Et polünoomi $x^3 - 2$ lahendid on

$$\xi_1 = \sqrt[3]{2}, \quad \xi_2 = \sqrt[3]{2}\,\varepsilon_1, \quad \xi_3 = \sqrt[3]{2}\,\varepsilon_2,$$

kus

$$\varepsilon_1 = \frac{-1 + i\sqrt{3}}{2}, \qquad \varepsilon_2 = \frac{-1 - i\sqrt{3}}{2},$$

siis avaldub siin lahutuskorpus Σ kujul

$$\Sigma = K(\xi_1, \varepsilon_1).$$

Leiame võrrandi $x^3 - 2 = 0$ Galois rühma $G = \Sigma(K)$. Kõigepealt korpuse $K(\xi_1)$ Galois rühm koosneb kolmest automorfismist, mis on määratud tingimustega

$$\xi_1 \longleftrightarrow \xi_1, \quad \xi_1 \longleftrightarrow \xi_2, \quad \xi_1 \longleftrightarrow \xi_3.$$

Korpus $K(\xi_1, \varepsilon_1)$ omab omakorda kahte automorfismi, mis jätavad $K(\xi_1)$ elemendid invariantseks ja mis on määratud tingimustega

$$\varepsilon_1 \longleftrightarrow \varepsilon_1, \quad \varepsilon_1 \longleftrightarrow \varepsilon_2.$$

Jätkates korpuse $K(\xi_1)$ iga automorfismi korpuse $K(\xi_1, \varepsilon_1)$ ühe või teise automorfismini, saame kogusummas 6 automorfismi

$$S_0, S_1, S_2, S_3, S_4, S_5,$$

mis on määratud tingimustega

$$\xi_1 s_0 = \xi_1,\ \xi_1 s_1 = \xi_2,\ \xi_1 s_2 = \xi_3,\ \xi_1 s_3 = \xi_1,\ \xi_1 s_4 = \xi_2,\ \xi_1 s_5 = \xi_3$$
$$\varepsilon_1 s_0 = \varepsilon_1,\ \varepsilon_1 s_1 = \varepsilon_1,\ \varepsilon_1 s_2 = \varepsilon_1,\ \varepsilon_1 s_3 = \varepsilon_2,\ \varepsilon_1 s_4 = \varepsilon_2,\ \varepsilon_1 s_5 = \varepsilon_2,$$

ja mis moodustavadki rühma G. Cayley teoreemi järgi (§ 20, art. 1) on G isomorfne teatava substitutsioonirühmaga numbritest 1, 2, 3. Et aga numbritest 1, 2, 3 saab moodustada üldse 6 substitutsiooni, siis on G isomorfne sümmeetrilise rühma S_3 endaga, kusjuures võib kergesti veenduda, et

$$s_0 = e,\ s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3),\ s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2),$$
$$s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3),\ s_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2),\ s_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3).$$

Galois teooria põhilause järgi taandub seega korpuse $\Sigma = K(\xi_1, \varepsilon_1)$ struktuuri uurimine sümmeetrilise rühma S_3 struktuuri uurimisele. Mis puutub rühmasse S_3, siis on tal peale ühikrühma E neli pärisalamrühma (§ 19, art. 3)

$$H = \{e, s_3\},\ H_1 = \{e, s_4\},\ H_2 = \{e, s_5\},\ H_3 = \{e, s_1, s_2\}.$$

Seetõttu omab Σ peale põhikorpuse K neli pärisalamkorpust

$$\Delta,\ \Delta_1,\ \Delta_2,\ \Delta_3,$$

mille astmed K suhtes on valemi (7) järgi vastavalt

$$3, 3, 3, 2.$$

Siinjuures ei ole raske näha, et

$$\Delta = K(\xi_1),$$

sest substitutsioonid e, s_3 jätavad ξ_1 ja ühes sellega laiendi $K(\xi_1)$ iga elemendi invariantseks. Analoogilistel kaalutlustel on

$$\Delta_1 = K(\xi_3),\ \Delta_2 = K(\xi_2),\ \Delta_3 = K(\varepsilon_1).$$

Alamkorpustest Δ, Δ_1, Δ_2, Δ_3 osutub ainult Δ_3 Galois korpuseks, sest vaid H_3 on normaaljagaja (§ 19, art. 4). Vastav Galois rühm $\Delta_3(K)$ on isomorfne faktorrühmaga

$$G/H_3 = (H_3, H_3 s_3),$$

kus $H_3 s_3 = \{s_3, s_4, s_5\}$.

§ 29. Galois teooria rakendusi.

1. Võrrandi lahenduvus radikaalides. Olgu antud n-astme algebraline võrrand $f(x) = 0$ üle korpuse K. Ütleme, et võrrand $f(x) = 0$ on lahenduv radikaalides üle K, kui leiduvad juured

$$\varrho_1 = \sqrt[p_1]{a_1}, \quad \varrho_2 = \sqrt[p_2]{a_2}, \quad \ldots, \quad \varrho_k = \sqrt[p_k]{a_k},$$

millede adjungeerimisel korpusele K saame niisuguse laiendi $K(\varrho_1, \varrho_2, \ldots, \varrho_k)$, mis sisaldab kõiki võrrandi $f(x) = 0$ lahendeid. Siinjuures tähendab a_1 mingit K elementi, a_2 laiendi $K(\varrho_1)$ elementi, a_3 laiendi $K(\varrho_1, \varrho_2)$ elementi jne., lõppeks a_k laiendi $K(\varrho_1, \varrho_2, \ldots, \varrho_{k-1})$ elementi. Teiste sõnadega, võrrand $f(x) = 0$ on radikaalides lahenduv, kui kõik selle võrrandi lahendid avalduvad ratsionaalselt lõpliku arvu juurte $\varrho_1, \varrho_2 \ldots, \varrho_k$ kaudu. Nii on näiteks kuupvõrrand

$$x^3 + px + q = 0$$

lahenduv radikaalides, kui põhikorpus, millesse kuuluvad kordajad p ja q, ei ole karakteristikaga 2 ega 3, sest siis on Cardano valemi järgi

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

ja seega avalduvad siin lahendid ratsionaalselt juurte

$$\varrho_1 = \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad \varrho_2 = \sqrt[3]{-\frac{q}{2} + \varrho_1}$$

kaudu kujul $x = \varrho_2 - \frac{p}{3\varrho_2}$ (§ 11, art. 2).

Puudutame kõigepealt lühidalt võrrandite radikaalides lahenduvuse küsimuse ajaloolist külge. Nimetatud küsimus kerkis üles pärast seda, kui Cardano 1545. a. publitseeris kolmanda ja neljanda astme võrrandite lahendused radikaalides. XVII ja

XVIII sajandi kõige silmapaistvamate matemaatikute Descartes'i, Tschirnhausi, Euleri, Bèzout' jt. korduvad katsed, leida kõrgema kui neljanda astme võrrandite lahendusi radikaalides, lõppesid eranditult tagajärjetult. Seepärast võttis Lagrange aastail 1770—1771 kõik seni tuntud menetlused võrrandite lahendamiseks radikaalides terava kriitika alla. Ta leidis, et need menetlused toetuvad kõik oluliselt ühele printsiibile. Olgu nimelt $\varphi(\xi_1, \xi_2, \ldots, \xi_n)$ mingi ratsionaalfunktsioon võrrandi $f(x) = 0$ lahendite $\xi_1, \xi_2, \ldots, \xi_n$ suhtes, mis omagu nende lahendite $n!$ võimaliku permutatsiooni puhul v erinevat väärtust. Siis saab näidata, et φ peab rahuldama v-astme võrrandit, kusjuures võrrandi $f(x) = 0$ lahendamiseks radikaalides tarvitseb vaid määrata $\varphi(\xi_1, \xi_2, \ldots, \xi_n)$ nõnda, et v tuleks väiksem kui n. Kasutades Lagrange'i resolventi, osutus niisuguse φ leidmine juhtudel $n = 2, 3, 4$ võimalikuks, kusjuures v omas vastavalt väärtusi $1, 2, 3$. Seevastu juhul $n > 4$ ei õnnestunud Lagrange'il leida niisugust φ-d, mille puhul oleks $v < n$.

Kuigi Lagrange ei suutnud lõplikult selgitada võrrandite radikaalides lahenduvuse küsimust, näitasid ometi tema uurimused, et selle asemel, et otsida üldise võrrandi lahendust radikaalides juhul $n > 4$, tuleks püüda tõestada niisuguse võrrandi radikaalides lahendamise võimatust. Aastal 1799 esitaski itaalia matemaatik Ruffini tõestuse kõrgema kui neljanda astme üldise võrrandi radikaalides lahenduvuse võimatuse kohta, kuid Ruffini tõestuskäik osutus puudulikuks ja täpsustati alles 1826. a. Abeli poolt. Ent Ruffini ja Abeli töödega polnud algebraliste võrrandite radikaalides lahenduvuse küsimus kaugeltki veel ammendavalt lahendatud. Sest kui ei leidu üldist lahendusvalemit radikaalides, mis oleks ühine kõigile n-astme võrranditele üle antud põhikorpuse, siis ei ole sellega veel öeldud, et vastavalt igale k o n k r e e t s e l e võrrandile ei võiks leiduda oma lahendusvalem radikaalides, nii nagu see esineb näiteks pöördvõrrandite puhul, mille aste ei ole suurem kui 9 (§ 11, art. 4). Võrrandite radikaalides lahenduvuse küsimuse lahendas lõplikult Évariste Galois (1811—1832), kes andis tarviliku ja piisava tingimuse antud võrrandi lahenduvuseks radikaalides, näidates ühtlasi, et

$n > 4$ puhul leidub konkreetseid võrrandeid, mis ei ole lahenduvad radikaalides. Galois erakordselt viljakad uurimused mitte ainult ei selgitanud algebralise võrrandi radikaalides lahenduvuse küsimust, vaid panid aluse ühele kaasaegse algebra tähtsale ja kiiresti arenevale harule — Galois teooriale, kus võrrandite radikaalides lahenduvuse küsimus on vaid üheks rakenduseks. Galois teooriat on arendanud edasi nõukogude matemaatikud Šatunovski, Tšebotarjov, Delone ja Faddejev. Delone rajas originaalse geomeetrilise teooria, mis kujutab Galois teooria üldistust. Seda geomeetrilist teooriat rakendas Delone koos Faddejeviga Galois teooria raskeimate probleemide lahendamiseks.

Galois isiksus, kelle lühike elukäik kulges äärmiselt tormiliselt, moodustab teatavas mõttes erandi teaduse ajaloos. Kukkunud kaks korda läbi sisseastumiseksameil kuulsasse Polütehnilisse Kooli Pariisis (École Polytechnique), astus Galois Normaalkooli (École Normale), kust ta kohe pärast 1830. a. juulirevolutsiooni välja heideti ülesastumise pärast direktori vastu. Võttes sügavalt veendunud tulise vabariiklasena aktiivselt osa prantsuse rahva poliitilisest elust, viibis Galois kaks korda vanglas revolutsioonilise tegevuse pärast. Enne veel, kui lõppes Galois 21. eluaasta, langes ta duellil põhjustel, mis on jäänud lõplikult selgitamata senini.

Vaatleme nüüd konkreetset võrrandit $f(x) = 0$ eeldades, et $f(x)$ on taandumatu korpuses K, kusjuures K karakteristika olgu null. Oletades, et siin mingi lahend ξ avaldub ratsionaalselt juurte

$$\varrho_1 = \sqrt[p_1]{a_1}, \quad \varrho_2 = \sqrt[p_2]{a_2}, \quad \ldots, \quad \varrho_k = \sqrt[p_k]{a_k}$$

kaudu, kus $a_1 \in K$, $a_2 \in K(\varrho_1)$, $\ldots$, $a_k \in K(\varrho_1, \varrho_2, \ldots, \varrho_{k-1})$, küsime, missugused kitsendused seab see oletus võrrandi $f(x) = 0$ Galois rühmale.

Kõigepealt võib üldsust kitsendamata eeldada, et juurijad $p_1, p_2, \ldots, p_k$ on kõik algarvud, sest iga liitarvulise juurijaga

radikaali võib asendada teatava arvu algarvuliste juurijatega radikaalidega. Nii on näiteks

$$\varrho = \sqrt[18]{a} = \sqrt{\sqrt[3]{\sqrt[3]{a}}} = \sqrt{\sqrt[3]{\varrho'}} = \sqrt{\varrho''},$$

kus $\varrho' = \sqrt[3]{a}$, $\varrho'' = \sqrt[3]{\varrho'}$.

Adjungeerime põhikorpusele K algul kõik p_1-astme, siis p_2-astme jne., lõppeks p_k-astme ühejuured. Selleks tarvitseb meil adjungeerida K-le vaid mingi p_1-astme algjuur, siis p_2-astme algjuur jne., lõppeks p_k-astme algjuur. Olgu näiteks ε' üks p_1-astme algjuur. Siis kujutab laiend $\Sigma_1 = K(\varepsilon')$ polünoomi $x^{p_1} - e$ lahutuskorpust K suhtes. Vastav Galois rühm $A = \Sigma_1(K)$, olles teoreemi 4 põhjal (§ 27, art. 3) tsükliline, on lahenduv (§ 22, art. 3), mistõttu tema kompositsioonijada

$$A \supset A_1 \supset A_2 \supset \ldots \supset A_l = E$$

omab algarvulisi indekseid

$$(A_1, A) = q_1, \quad (A_2, A_1) = q_2, \quad \ldots, \quad (A_l, A_{l-1}) = q_l.$$

Galois teooria põhilause järgi vastab igale alamrühmale A_i alamkorpus Δ_i, nii et $A_i = \Sigma_1(\Delta_i)$, kusjuures kahanevale alamrühmade jadale vastab kasvav alamkorpuste jada

$$K \subset \Delta_1 \subset \Delta_2 \subset \ldots \subset \Delta_l = \Sigma_1. \tag{8}$$

Et $A_{i-1} = \Sigma_1(\Delta_{i-1})$ ja A_i on A_{i-1} normaaljagaja, siis on Δ_i alamkorpuse Δ_{i-1} suhtes Galois korpus, kusjuures vastav Galois rühm $\Delta_i(\Delta_{i-1})$ on isomorfne faktorrühmaga (§ 28, art. 2)

$$A_{i-1}/A_i.$$

Viimane faktorrühm kui lahenduva rühma kompositsioonifaktor kujutab aga tsüklilist rühma järguga q_i (§ 22, art. 3). Siit järeldub, et jadas (8) on iga Δ_i eelneva alamkorpuse Δ_{i-1} suhtes tsükliline Galois korpus algarvulise astmega q_i.

Adjungeerides korpusele Σ_1 omakorda mingi p_2-astme algjuure ε'', saame laiendi $\Sigma_2 = \Sigma_1(\varepsilon'')$, mis kujutab polünoomi

$x^{p_2} - e$ lahutuskorpust Σ_1 suhtes. Vaadeldes vastavat Galois rühma $B = \Sigma_2(\Sigma_1)$, võime analoogiliselt eelnenuga jätkata jada (8) jadani

$$K \subset \Delta_1 \subset \Delta_2 \subset \ldots \subset \Delta_l = \Sigma_1 \subset \Delta_{l+1} \subset \ldots \subset \Delta_m = \Sigma_2,$$

ja korrates eelmist mõttekäiku k korda, jadani

$$(9) \quad K \subset \Delta_1 \subset \Delta_2 \subset \ldots \subset \Delta_l = \Sigma_1 \subset \Delta_{l+1} \subset \ldots \subset \Delta_m = \Sigma_2 \subset \\ \subset \Delta_{m+1} \subset \ldots \subset \Delta_t = \Sigma_k,$$

kus iga Δ_i on eelneva alamkorpuse Δ_{i-1} suhtes tsükliline Galois korpus algarvulise astmega. Siinjuures kujutab laiend Σ_k Galois korpust ka põhikorpuse K suhtes, sest Σ_k on polünoomi

$$(x^{p_1} - e)(x^{p_2} - e) \ldots (x^{p_k} - e)$$

lahutuskorpus K suhtes.

Adjungeerime nüüd korpusele Σ_k juured $\varrho_1, \varrho_2, \ldots, \varrho_k$, kusjuures koos iga juurega $\varrho_i = \sqrt[p_i]{a_i}$ adjungeerime ka p_i-astme juured kõigist a_i kaaselementidest K suhtes. Tulemusena saame tsüklilised korpused algarvulise astmega või ei saa üldse laiendit (§ 27, art. 3), mistõttu võime jätkata alamkorpuste jada (9) samasuguste omadustega jadani

$$(10) \quad K \subset \Delta_1 \subset \Delta_2 \subset \ldots \subset \Delta_t = \Sigma_k \subset \Delta_{t+1} \subset \ldots \subset \Delta_w = \Sigma,$$

kus laiend Σ sisaldab võrrandi $f(x) = 0$ lahendit ξ. Näitame, et Σ kujutab Galois korpust ka põhikorpuse K suhtes. Olgu nimelt Δ_u laiend, mille saame, adjungeerides korpusele Σ_k p_1-, p_2-, ..., p_i-astme juured, mis on võetud vastavalt elementidest a_1, a_2, ..., a_i ja kõigist viimaste kaaselementidest. Kasutades täieliku induktsiooni printsiipi, oletame, et Δ_u on Galois korpus K suhtes, ja näitame, et siis on seda ka laiend Δ_v, mis saadakse korpusest Δ_u elemendi a_{i+1} kaaselementidest

$$a_1 = a_{i+1}, a_2, \ldots, a_h$$

võetud p_{i+1}-astme juurte adjungeerimisel.

Olgu Θ laiendi Δ_u primitiivne element, nii et $\Delta_u = K(\Theta)$ (§ 26, art. 3). Vaatleme polünoomi

$$g(x) = (x-\Theta_1)(x-\Theta_2)\ldots(x-\Theta_j)(x^{p_{i+1}}-a_1)(x^{p_{i+1}}-a_2)\ldots(x^{p_{i+1}}-a_h),$$

milles $\Theta_1 = \Theta$, $\Theta_2, \ldots, \Theta_j$ tähendavad Θ kaaselemente K suhtes. Et Δ_u on induktsioonioletuse kohaselt Galois korpus, siis kuuluvad elemendid $\Theta_1, \Theta_2, \ldots, \Theta_j$ ja $a_1, a_2, \ldots, a_h$ korpusse Δ_u. Rakendades polünoomile $g(x)$ korpuse Δ_u Galois rühma mingit automorfismi, näeme, et selle mõjul võivad polünoomis $g(x)$ omavahel vahetuda vaid üksikud tegurid, mistõttu $g(x)$ kordajad jäävad invariantseks. Teoreemi 3 (§ 27, art. 1) järgi peavad seega $g(x)$ kordajad kuuluma põhikorpusse K. Et Σ_{i+1} ja siis ammugi Δ_v sisaldab kõiki p_{i+1}-astme ühejuuri, siis sisaldab Δ_v kõiki p_{i+1}-astme juuri elementidest $a_1, a_2, \ldots, a_h$. Seetõttu on Δ_v polünoomi $g(x)$ lahutuskorpus ja kujutab järelikult Galois korpust K suhtes. Kuna eriti $\Delta_t = \Sigma_k$ on Galois korpus K suhtes, siis on täieliku induktsiooni printsiibil seda ka $\Delta_w = \Sigma$.

Et Σ on Galois korpus K suhtes, siis korpuses K taandumatu polünoom $f(x)$, omades laiendis Σ lahendit ξ, laguneb seal täielikult lineaartegurite korrutiseks (§ 26, art. 2). Tähendab, kui võrrandi $f(x) = 0$ üks lahend avaldub radikaalides, siis avalduvad ka kõik tema teised lahendid radikaalides.

Vaatleme nüüd korpuse Σ Galois rühma $G = \Sigma(K)$. Galois teooria põhilause järgi vastab igale Σ alamkorpusele Δ_i rühma G alamrühm G_i, kusjuures kasvavale alamkorpuste jadale (10) vastab kahanev alamrühmade jada

$$(11) \qquad G \supset G_1 \supset G_2 \supset \ldots \supset G_t \supset G_{t+1} \supset \ldots \supset G_w = E.$$

Et jadas (10) on iga Δ_i eelneva alamkorpuse Δ_{i-1} suhtes Galois korpus algarvulise astmega, siis on jadas (11) iga alamrühm G_i eelneva G_{i-1} suhtes normaaljagaja algarvulise indeksiga, sest valemi 6 (§ 28, art. 2) järgi on

$$(G_i, G_{i-1}) = (\Delta_i : \Delta_{i-1}).$$

Seega on rühm G lahenduv.

Olgu Δ polünoomi $f(x)$ lahutuskorpus. Et $f(x)$ lahendid kuuluvad kõik korpusse Σ, siis on

$$K \subset \Delta \subset \Sigma.$$

Vaatleme võrrandi $f(x) = 0$ Galois rühma $\bar{G} = \Delta(K)$. Galois teooria põhilause järgi vastab Σ alamkorpusele Δ teatav G alamrühm H ja nimelt normaaljagaja, sest Δ on Galois korpus (§ 28, art. 2). Seega

$$\bar{G} \longleftrightarrow G/H.$$

Näitame, et G/H on lahenduv rühm. Paigutame selleks läbi H mingi G kompositsioonijada

$$G \supset H_1 \supset H_2 \supset \ldots \supset H \supset \ldots \supset H_w = E,$$

mille indeksid on Jordan-Hölderi teoreemi põhjal (§ 22, art. 2) võrdsed jada (11) indeksitega, kujutades seega algarve. Teoreemi 8 järgi (§ 21, art. 3) omab G/H kompositsioonijada kuju

$$G/H \supset H_1/H \supset H_2/H \supset \ldots \supset H/H = E.$$

Kui rühmade H_{i-1}, H_i, H järgud on vastavalt m_{i-1}, m_i, m, siis on

$$(H_i/H,\ H_{i-1}/H) = \frac{\frac{m_{i-1}}{m}}{\frac{m_i}{m}} = \frac{m_{i-1}}{m_i} = (H_i,\ H_{i-1}).$$

Et $(H_i,\ H_{i-1})$ kujutab algarvu, siis on faktorrühm G/H ja ühtlasi ka võrrandi $f(x) = 0$ Galois rühm $\bar{G}$ lahenduv. Niisiis, kui võrrand $f(x) = 0$ on lahenduv radikaalides, siis on selle võrrandi Galois rühm lahenduv.

Olgu nüüd, ümberpöördult, võrrandi $f(x) = 0$ Galois rühm $\bar{G}$ lahenduv, nii et tema kompositsioonijadal

$$\bar{G} \supset G_1 \supset G_2 \supset \ldots \supset G_k = E \tag{12}$$

on algarvulised indeksid

$$(G_1,\ \bar{G}) = p_1,\ (G_2,\ G_1) = p_2,\ \ldots,\ (G_k,\ G_{k-1}) = p_k.$$

Näitame, et siis võrrand $f(x) = 0$ on lahenduv radikaalides. Galois teooria põhilause järgi vastab kompositsioonijadale (12) polünoomi $f(x)$ lahutuskorpuse Δ alamkorpuste jada

$$K \subset \Delta_1 \subset \Delta_2 \subset \ldots \subset \Delta_k = \Delta,$$

kus, analoogiliselt jadaga (8), iga Δ_i on temale eelneva alamkorpuse Δ_{i-1} suhtes tsükliline Galois korpus algarvulise astmega p_i. Adjungeerides viimase jada igale korpusele kõik p_1-, p_2-, ..., p_k-astme ühejuured, saame jada

$$K' \subset \Delta_1' \subset \Delta_2' \subset \ldots \subset \Delta_k' = \Delta'. \tag{13}$$

Näitame, et siin iga Δ_i' kas langeb ühte temale eelneva alamkorpusega Δ'_{i-1} või on viimase suhtes tsükliline Galois korpus algarvulise astmega p_i. Piirdume tõestusel konkreetsuse mõttes korpustega Δ_1' ja K'. Kõigepealt ei ole raske näha, et Δ_1' on K' suhtes Galois korpus. Nimelt kui ε', ε'', ..., $\varepsilon^{(k)}$ tähendavad vastavalt p_1-, p_2-, ..., p_k-astme algjuuri, siis on

$$K' = K(\varepsilon', \varepsilon'', \ldots, \varepsilon^{(k)}), \quad \Delta_1' = \Delta_1(\varepsilon', \varepsilon'', \ldots, \varepsilon^{(k)}).$$

Olgu ξ korpuse Δ_1 moodustav element, nii et $\Delta_1 = K(\xi)$. Siis on

$$\Delta_1' = K(\xi)(\varepsilon', \varepsilon'', \ldots, \varepsilon^{(k)}) = K(\varepsilon', \varepsilon'', \ldots, \varepsilon^{(k)})(\xi) = K'(\xi),$$

millest nähtub, et ξ on ka Δ_1' moodustav element K' suhtes. Et Δ_1 on Galois korpus K suhtes, siis

$$K(\xi) = K(\xi_i),$$

kus ξ_i tähendab mingit ξ kaaselementi (§ 26, art. 2). Adjungeerides viimase võrduse kummalgi pool seisvatele korpustele algjuured ε', ε'', ..., $\varepsilon^{(k)}$, saame

$$K'(\xi) = K'(\xi_i),$$

mis ütlebki, et Δ_1' on Galois korpus K' suhtes.

Vaatleme Galois rühmi $H = \Delta_1(K)$ ja $H' = \Delta_1'(K')$. Teisendagu rühma H' mingi automorfism s' korpuse Δ_1' moodustava elemendi ξ kaaselemendiks ξ_i. Et ξ on ka Δ_1 moodustav ele-

ment, siis s', teisendades Δ_1 moodustava elemendi ξ kaaselemendiks ξ_i, kutsub teoreemi 2 järgi (§ 27, art. 1) esile teatava korpuse Δ_1 automorfismi s, mis kuulub rühma H. Seame H' igale automorfismile s' vastavusse tema poolt esile kutsutud H automorfismi s ja märgime kõigi niisuguste automorfismide s hulga tähega $\bar{H}$. Ei ole raske näha, et korraldatud vastavus kujutab isomorfismi

$$H' \longleftrightarrow \bar{H},$$

mistõttu ka $\bar{H}$ osutub rühmaks — H alamrühmaks. Et $\bar{G}$ on lahenduv, siis on $H \longleftrightarrow \bar{G}/G_1$ tõttu H tsükliline rühm algarvulist järku p_1 (§ 22, art. 3) ja seega Lagrange'i teoreemi järgi kas $\bar{H} = E$ või $\bar{H} = H$. Esimesel juhul $\Delta_1' = K'$, teisel juhul kujutab Δ_1' K' suhtes tsüklilist Galois korpust algarvulise astmega p_1.

Kasutame nüüd teoreemi 5 (§ 27, art. 3), mille järgi iga tsüklilist p-astme Galois korpust võib vaadelda binoomi $x^p - a$ lahutuskorpusena, kui aga põhikorpus sisaldab kõiki p-astme ühejuuri. Selle teoreemi põhjal saadakse jadas (13) iga Δ_i' temale eelnevast korpusest Δ'_{i-1} teatava p_i-astme juure adjungeerimisel. Seega võib saada laiendi Δ' korpusest K' — aga siis ka põhikorpusest K — teatava arvu juurte adjungeerimisel. Et Δ' sisaldab kõiki võrrandi $f(x) = 0$ lahendeid, siis on võrrand $f(x) = 0$ radikaalides lahenduv.

Seega oleme jõudnud Galois teoreemi juurde, mis annab ammendava vastuse algebralise võrrandi radikaalides lahenduvuse küsimusele — ligi kolme sajandi vältel matemaatikute uurimiste tulipunktis püsinud küsimusele.

Teoreem 7. *Võrrand $f(x) = 0$, kus $f(x)$ on korpuses K taandumatu polünoom, on radikaalides lahenduv siis ja ainult siis, kui selle võrrandi Galois rühm K suhtes on lahenduv.*

Teoreemi 7 järgi ei ole näiteks viienda astme võrrand

$$x^5 - 4x - 2 = 0$$

ratsionaalarvude korpuses lahenduv radikaalides, sest tema

Galois rühmaks on sümmeetriline rühm S_5 (§ 27, art. 2), mis ei ole lahenduv (§ 23, art. 2).

Vaatleme lõppeks n-astme võrrandit

$$x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \ldots + (-1)^n \sigma_n = 0,$$

kus kordajad σ_1, σ_2, ..., σ_n tähendavad algebralisi muutujaid üle korpuse K. Niisugust võrrandit nimetatakse üldiseks n-astme võrrandiks. Üldise n-astme võrrandi kordajad kuuluvad ratsionaalfunktsioonide korpusse $K(\sigma_1, \sigma_2, \ldots, \sigma_n)$, mille võtame antud juhul põhikorpuseks. Et Vieta valemite järgi

$$\begin{aligned}
\sigma_1 &= \xi_1 + \xi_2 + \ldots + \xi_n \\
\sigma_2 &= \xi_1\xi_2 + \xi_1\xi_3 + \ldots + \xi_{n-1}\xi_n \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
\sigma_n &= \xi_1\xi_2 \ldots \xi_n,
\end{aligned}$$

kus ξ_1, ξ_2, ..., ξ_n on vaadeldava võrrandi lahendid, siis jätavad nende lahendite substitutsioonid kordajad σ_1, σ_2, ..., σ_n — ja seega ka põhikorpuse $K(\sigma_1, \sigma_2, \ldots, \sigma_n)$ kõik elemendid — invariantseks. Järelikult koosneb n-astme üldise võrrandi Galois rühm kõigist n-astme substitutsioonidest (§ 27, art. 2), kujutades sümmeetrilist rühma S_n. Et sümmeetriline rühm ei ole juhul $n > 4$ lahenduv (§ 23, art. 2), siis oleme seega tõestanud alljärgneva Ruffini-Abeli teoreemi.

Teoreem 8. *Kõrgema kui neljanda astme üldine võrrand ei ole radikaalides lahenduv.*

2. Geomeetrilised konstruktsioonid sirkli ja joonlaua abil. Geomeetriliste konstruktsioonide puhul pakub huvi küsimus, missugused neist konstruktsioonidest on teostatavad sirkli ja joonlaua abil, s. o. ainult ringide ja sirgete joonestamise teel. Kasutades Cartesiuse ristkoordinaadistikku, võime niihästi antud kui ka otsitava kujundi punkte esitada lõikude (arvude) abil. Olgu a, b, c, ... antud lõigud ja x otsitav lõik. Oletame, et lõiku x saab konstrueerida lõikudest a, b, c, ... ainult ringe ja sirgeid joonestades ja näitame, et siis x avaldub suuruste a, b, c, ... kaudu ratsionaaloperatsioonide ja ruutjuurte abil. Nimelt paneme tähele, et iga geomeetrilist konst-

ruktsiooni, mis on teostatav sirkli ja joonlaua abil, võime lahutada kolme liiki elementaarkonstruktsioonideks:

1^0 kahe sirge lõikepunkti leidmine;
2^0 sirge ja ringjoone lõikepunkti leidmine;
3^0 kahe ringjoone lõikepunkti leidmine.

Analüütiliselt avaldub igaüks neist elementaarkonstruktsioonidest kahest ülimalt ruutvõrrandist koosneva võrrandisüsteemi lahendamises ja taandub lõppude-lõpuks ühe lineaar- või ruutvõrrandi lahendamisele, mis on teostatav ratsionaaloperatsioonide ja ruutjuurte abil.

Ümberpöördult, kui lõik x saadakse antud lõikudest a, b, c, ... ratsionaaloperatsioonide ja ruutjuurte kaudu, siis ei ole raske veenduda, et x on konstrueeritav sirkli ja joonlaua abil. Et reaalkordajatega ruutvõrrandi lahendamisel võivad esineda ka kompleksarvud, siis tuleb viimase väite tõestuseks näidata, et kompleksarvude vallas on summa, vahe, korrutis, jagatis ja ruutjuur konstrueeritavad sirkli ja joonlaua abil. Kompleksarvude teooriast teame (§ 1, art. 3), et kompleksarvude summat, vahet, korrutist ja jagatist saab leida sirkli ja joonlaua abil. Mis puutub ruutjuure arvutamisse kompleksarvust $a = r(\cos\varphi + i\sin\varphi)$, siis on

$$\sqrt{a} = \pm\sqrt{r}\left(\cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2}\right),$$

kus ruutjuure leidmine positiivsest reaalarvust r ja nurga φ poolitamine on teostatavad sirkli ja joonlauaga.

Niisiis on lõik x konstrueeritav antud lõikudest a, b, c, ... sirkli ja joonlaua abil siis ja ainult siis, kui x saadakse lõikudest a, b, c, ... ratsionaaloperatsioonide ja ruutjuurte kaudu, s. o. kui võrrand $f(x) = 0$, mis seob lõiku x lõikudega a, b, c, ..., on lahenduv ruutjuurtes.

Leiame nüüd tingimuse võrrandi $f(x) = 0$ lahenduvuseks ruutjuurtes, kusjuures eeldame, et $f(x)$ on taandumatu põhikorpuses K. Oletades, et siin mingi lahend ξ avaldub ratsionaalselt ruutjuurte

$$\varrho_1 = \sqrt{a_1},\quad \varrho_2 = \sqrt{a_2},\quad \ldots,\quad \varrho_k = \sqrt{a_k}$$

kaudu, kus $a_1 \in K$, $a_2 \in K(\varrho_1)$, ..., $a_k \in K(\varrho_1, \varrho_2, \ldots, \varrho_{k-1})$, küsime, missugused kitsendused seab see oletus võrrandi $f(x) = 0$ Galois rühmale.

Analoogiliselt võrrandi $f(x) = 0$ lahenduvuse juhuga mistahes radikaalides (art. 1) adjungeerime korpusele K ruutjuured ϱ_1, ϱ_2, ..., ϱ_k, kusjuures koos iga ruutjuurega $\varrho_i = \sqrt{a_i}$ adjungeerime ka ruutjuured kõigist a_i kaaselementidest K suhtes. Tulemusena saame alamkorpuste jada

$$K \subset \Delta_1 \subset \Delta_2 \subset \ldots \subset \Delta_s = \Sigma,$$

kus iga Δ_i kujutab temale eelneva alamkorpuse Δ_{i-1} suhtes teise astme Galois korpust. Siinjuures osutub laiend Σ Galois korpuseks ka põhikorpuse K suhtes, mistõttu Σ peab sisaldama koos ξ-ga kõiki võrrandi $f(x) = 0$ lahendeid. Rakendades valemit (7) (§ 28, art. 2)

$$(\Sigma : K) = (\Sigma : \Delta)(\Delta : K)$$

üksteise järel laienditele Δ_2, Δ_3, ..., Δ_s, leiame

$$(\Sigma : K) = 2^s.$$

Olgu Δ polünoomi $f(x)$ lahutuskorpus. Kuna $f(x)$ lahendid kuuluvad kõik korpusse Σ, siis on

$$K \subset \Delta \subset \Sigma.$$

Et valemi (7) järgi

$$2^s = (\Sigma : \Delta)(\Delta : K),$$

siis peab $(\Delta : K)$, mis kujutab võrrandi $f(x) = 0$ Galois rühma $\Delta(K)$ järku (§ 27, art. 1), olema 2^s jagajaks, mistõttu

$$(\Delta : K) = 2^n,$$

kus $n \leqslant s$. Niisiis, kui võrrand $f(x) = 0$ on lahenduv ruutjuurtes, siis peab selle võrrandi Galois rühma järk kujutama kahe astet.

Olgu nüüd, ümberpöördult, võrrandi $f(x) = 0$ Galois rühma

$G = \Delta(K)$ järk 2^n. Teoreemi 10 järgi (§ 22, art. 3) on aga iga rühm, mille järk avaldub kujul p^n, lahenduv. Olgu

$$G \supset G_1 \supset G_2 \supset \ldots \supset G_n = E$$

rühma G kompositsioonijada ja

$$K \subset \Delta_1 \subset \Delta_2 \subset \ldots \subset \Delta_n = \Delta$$

Galois teooria põhilause mõttes vastav alamkorpuste jada. Valemi (6) (§ 23, art. 2) põhjal on

$$(\Delta_i : \Delta_{i-1}) = (G_i, G_{i-1}).$$

Et (G_i, G_{i-1}) kui lahenduva rühma kompositsiooni-indeks peab kujutama algarvu, teiselt poolt aga (G_i, G_{i-1}) peab olema 2^n jagajaks, siis $(G_i, G_{i-1}) = 2$ ja seega

$$(\Delta_i : \Delta_{i-1}) = 2 .$$

Tähendab, korpuse Δ_i iga element rahuldab ülimalt ruutvõrrandit üle Δ_{i-1} ja avaldub seega ülimalt ruutjuurtes Δ_{i-1} elementide kaudu. Siit nähtubki, et võrrand $f(x) = 0$ on lahenduv ruutjuurtes, kui selle võrrandi Galois rühma järk on 2^n. Kokku võttes oleme saanud järgmise tulemuse.

Teoreem 8. *Võrrand $f(x) = 0$, kus $f(x)$ on korpuses K taandumatu polünoom, on ruutjuurtes lahenduv siis ja ainult siis, kui selle võrrandi Galois rühm K suhtes omab järku 2^n.*

Vaatleme teoreemi 8 rakendamise näitena klassikalist nurga kolmeks võrdseks osaks jaotamise probleemi, mis juba neljandal sajandil enne meie ajaarvamise algust paelus kreeka geomeetrite tähelepanu ja mida tänapäevalgi püüavad asjatult lahendada mõned asjaarmastajad. Olgu antud nurk märgitud α-ga ja otsitav nurk φ-ga, nii et $\alpha = 3\varphi$. Siis on (§ 1, art. 4)

$$\cos\alpha = 4\cos^3\varphi - 3\cos\varphi ,$$

millest

$$(2\cos\varphi)^3 - 3 \cdot 2\cos\varphi - 2\cos\alpha = 0 .$$

Märkides $2\cos\varphi = x$, $2\cos\alpha = a$, saame nurga α kolmeks võrdseks osaks jaotamise probleemi taandada kuupvõrrandile

$$x^3 - 3x - a = 0 .$$

Eriti kui siin $a = \frac{1}{p}$ $\left(a = \arccos \frac{1}{2p}\right)$, kus p tähendab positiivset algarvu, saame võrrandi

$$x^3 - 3x - \frac{1}{p} = 0,$$

millel ei ole ratsionaallahendeid, mistõttu polünoom $x^3 - 3x - \frac{1}{p}$ on taandumatu ratsionaalarvude korpuses. Seetõttu peab selle võrrandi Galois rühma järk sisaldama tegurit 3 (art. 3), mis ütleb, et vaadeldav võrrand ei ole lahenduv ruutjuurtes. Teiste sõnadega, nurk $a = \arccos \frac{1}{2p}$ ei ole sirkli ja joonlaua abil jaotatav kolmeks võrdseks osaks. Niisiis pole vabalt etteantud nurga kolmeks võrdseks osaks jaotamise probleem sirkli ja joonlaua abil lahendatav.

3. Võrrandi lahenduvus reaalsetes radikaalides. Uurides reaalkordajatega kolmanda astme võrrandit $x^3 + px + q = 0$ üksteisest erinevate reaalsete lahendite korral, s. o. juhul $D > 0$ nägime, et Cardano valem lubab neid lahendeid leida vaid komplekssuuruste, nimelt komplekssete radikaalide kaudu (§ 11, art. 2). Toetudes Galois teooriale, saab kergesti selgitada selle nähtuse põhjust ja tõestada tema paratamatust mitte ainult kolmanda, vaid ka teatavate kõrgema astme võrrandite puhul. Selleks esitame järgmise, Hölderi poolt 1891. a. tõestatud teoreemi.

Teoreem 9. *Olgu reaalkordajatega võrrandi* $f(x) = 0$ *lahendid kõik reaalsed ja* $f(x)$ *taandumatu põhikorpuses* K. *Kui selle võrrandi Galois rühma järk sisaldab algtegurit* p, *kus* $p > 2$, *siis ei ole võrrand* $f(x) = 0$ *lahenduv reaalsetes radikaalides.*

Teoreemi 9 tõestuseks näitame kõigepealt, et kui mingi binoom $x^p - a$ on taanduv korpuses K, siis on $a = c^p$, kus $c \in K$. Tõepoolest, olgu

$$x^p - a = \varphi(x)\psi(x),$$

kus $\varphi(x)$ ja $\psi(x)$ on teatavad mittekonstantsed polünoomid üle K. Tähendagu ε p-astme algjuurt ja ξ mingit binoomvõrrandi $x^p - a = 0$ lahendit. Siis on

$$x^p - a = (x - \xi)(x - \xi\varepsilon) \ldots (x - \xi\varepsilon^{p-1})$$

ja seega

$$\varphi(x) = (x - \xi\varepsilon^{\alpha_1})(x - \xi\varepsilon^{\alpha_2}) \ldots (x - \xi\varepsilon^{\alpha_r}),$$

kus $0 < r < p$. Viimase võrduse järgi avaldub $\varphi(x)$ vabaliige (või selle vastandväärtus) kujul

$$b = \varepsilon^{\alpha_1+\alpha_2+\ldots+\alpha_r}\xi^r = \varepsilon'\xi^r,$$

milles ε' tähendab teatavat p-astme ühejuurt. Järelikult

$$b^p = (\varepsilon')^p\xi^{pr} = (\xi^p)^r = a^r.$$

Et $0 < r < p$, siis on p ja r ühistegurita, mistõttu leiduvad täisarvud u ja v, nii et (I, § 7, art. 2)

$$pu + rv = 1.$$

Seega võime kirjutada

$$a = a^{pu}a^{rv} = a^{pu}b^{pv} = (a^u b^v)^p$$

ehk

$$a = c^p,$$

kus $c = a^u b^v$ on teatav arv põhikorpuses K.

Olgu nüüd $\xi_1, \xi_2, \ldots, \xi_n$ võrrandi $f(x) = 0$ lahendid, nii et $\Delta = K(\xi_1, \xi_2, \ldots, \xi_n)$ kujutab polünoomi $f(x)$ lahutuskorpust, ja avaldugu need lahendid ratsionaalselt reaalsete juurte

$$\varrho_1 = \sqrt[p_1]{a_1}, \quad \varrho_2 = \sqrt[p_2]{a_2}, \quad \ldots, \quad \varrho_k = \sqrt[p_k]{a_k}$$

kaudu, kusjuures

$$a_1 \in K, \quad a_2 \in K(\varrho_1), \quad \ldots, \quad a_k \in K(\varrho_1, \varrho_2, \ldots, \varrho_{k-1}).$$

Siin võime üldsust kitsendamata eeldada, et iga binoom $x^{p_i} - a_i$ on taandumatu korpuses $K(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$, sest vastasel korral oleks eelnenu põhjal $a_i = c^{p_i}$, $c \in K(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$ ja seega $\varrho_i = c$ kui juur langeks välja. Selle eelduse tõttu on laiendi $K(\varrho_1, \varrho_2, \ldots, \varrho_i)$ aste $K(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$ suhtes p_i. Märkides $\Sigma = K(\varrho_1, \varrho_2, \ldots, \varrho_k)$, leiame valemi (6) (§ 28, art. 2) järgi

$$(\Sigma : K) = p_1 p_2 \ldots p_k$$

ehk, eraldades algarvude $p_1, p_2, \ldots, p_k$ hulgast need, mis on võrdsed 2-ga,

$$(14) \qquad (\Sigma : K) = 2^j p_{j+1} p_{j+2} \ldots p_k .$$

Adjungeerime nüüd polünoomi $f(x)$ lahutuskorpusele Δ juured $\varrho_1, \varrho_2, \ldots, \varrho_k$. Tulemusena saame reaalse korpuse

$$\Delta(\varrho_1, \varrho_2, \ldots, \varrho_k) = K(\xi_1, \xi_2, \ldots, \xi_n)(\varrho_1, \varrho_2, \ldots, \varrho_k) =$$
$$= K(\varrho_1, \varrho_2, \ldots, \varrho_k)(\xi_1, \xi_2, \ldots, \xi_n) = \Sigma(\xi_1, \xi_2, \ldots, \xi_n) = \Sigma ,$$

sest Σ sisaldab kõiki lahendeid $\xi_1, \xi_2, \ldots, \xi_n$. Et selgitada, missugune on Σ aste Δ suhtes, tarvitseb vaadelda vaid iga $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_i)$ astet eelneva laiendi $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$ suhtes. Silmas pidades, et korpus $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_i)$ saadakse korpusest $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$ reaalse juure ϱ_i, s. o. võrrandi $x^{p_i} - a = 0$ reaalse lahendi adjungeerimisel, on otsitava astme suhtes oluline, kas binoom $x^{p_i} - a_i$ on korpuses $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$ taanduv või taandumatu. Käsitleme eraldi kahte võimalust selle järgi, kas $p_i = 2$ või $p_i > 2$.

1^0 Kui $p_i = 2$, siis binoom $x^{p_i} - a_i = x^2 - a_i$ võib olla kas taanduv või taandumatu korpuses $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$. Esimesel juhul ei saa me üldse laiendit, sest siis on eelnenu põhjal $a_i = c^2$ ja seega $\varrho_i = c$, kus $c \in \Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$. Seevastu teisel juhul saame teise astme laiendi.

2^0 Kui $p_i > 2$, siis saab näidata, et binoom $x^{p_i} - a_i$ peab olema igal juhul taandumatu korpuses $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$.

Tõepoolest, kui binoom $x^{p_i} - a_i$ oleks taanduv, siis oleks eelnenu järgi $a_i = c^{p_i}$, $c \in \Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$ ja seega $\varrho_i = c$. Et aga

$$\Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1}) = K(\xi_1, \xi_2, \ldots, \xi_n)(\varrho_1, \varrho_2, \ldots, \varrho_{i-1}) = \\ = K(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})(\xi_1, \xi_2, \ldots, \xi_n),$$

siis kujutab korpus $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$ polünoomi $f(x)$ lahutuskorpust $K(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$ suhtes. Seepärast kuuluvad korpusse $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$ k õ i k võrrandi $x^{p_i} - a_i = 0$ lahendid. Et aga viimasel võrrandil on $p_i > 2$ tõttu ainult üks reaallahend, peab korpus $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$ sisaldama ka kompleksarve, vastuolus eeldusega, mille järgi $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$ oli reaalne korpus. Seega peab siin binoom $x^{p_i} - a_i$ olema taandumatu korpuses $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$, mistõttu $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_i)$ aste $\Delta(\varrho_1, \varrho_2, \ldots, \varrho_{i-1})$ suhtes tuleb p_i.

Niisiis on

$$(\Sigma : \Delta) = 2^h p_{j+1} p_{j+2} \ldots p_k, \quad h \leqslant j. \tag{15}$$

Märkides $(\Delta : K) = m$, kus m kujutab võrrandi $f(x) = 0$ Galois rühma järku (§ 27, art. 1), võime valemi (7) põhjal (§ 28, art. 2) kirjutada

$$(\Sigma : K) = (\Sigma : \Delta) m$$

ehk (14) ja (15) tõttu

$$2^j p_{j+1} p_{j+2} \ldots p_k = 2^h p_{j+1} p_{j+2} \ldots p_k m,$$

millest

$$m = 2^{j-h},$$

vastuolus eeldusega, mille järgi m peab sisaldama algtegurit p, kus $p > 2$. Seega on teoreem 9 tõestatud.

Eriti järeldub teoreemist 9, et reaalkordajatega võrrand $f(x) = 0$, mille lahendid on kõik reaalsed ja kus $f(x)$ on taandumatu põhikorpuses K, ei ole lahenduv reaalsetes radikaalides, kui $f(x)$ aste n sisaldab mingit algtegurit p, kus $p > 2$. Tõepoolest, võrrandi $f(x) = 0$ Galois rühma järku m kui $f(x)$

lahutuskorpuse $\Delta = K(\xi_1, \xi_2, \ldots, \xi_n)$ astet K suhtes võib avaldada kujul

$$m = (\Delta : K) = (\Delta : \Delta_1)(\Delta_1 : K),$$

kus $\Delta_1 = K(\xi_1)$. Et $f(x)$ on taandumatu korpuses K, siis on $(\Delta_1 : K) = n$ ja seega

$$m = (\Delta : \Delta_1)n,$$

mistõttu ka m sisaldab algtegurit p, nagu seda eeldab teoreem 9.

Vaatleme näiteks reaalsete lahenditega kolmanda astme võrrandit

$$x^3 - 4x - 2 = 0.$$

Siin võib põhikorpuseks K valida ratsionaalarvude korpuse, milles polünoom $x^3 - 4x - 2$ on Eisensteini teoreemi põhjal taandumatu. Võttes $p = 3$ näeme seega, et vaadeldav võrrand ei ole lahenduv reaalsetes radikaalides. Ammugi pole siis üldine kolmanda astme võrrand

$$x^3 + px + q = 0$$

üksteisest erinevate reaalsete lahendite korral, s. o. juhul $D > 0$ lahenduv reaalsetes radikaalides (§ 11, art. 2).

Harjutusülesandeid.

150. Leida laiendi $K(\sqrt{2}, \sqrt{5})$ Galois rühm, kui K tähendab ratsionaalarvude korpust.

151. Leida võrrandite

a) $x^3 + 2x + 1 = 0$; b) $x^4 - 5x^2 + 6 = 0$;
c) $x^5 - 1 = 0$; d) $x^{12} - 1 = 0$

Galois rühmad ratsionaalarvude korpuse suhtes.

152. Leida võrrandite

a) $x^5 - 1 = 0$; b) $x^{12} - 1 = 0$

Galois rühmad reaalarvude korpuse suhtes.

153. Näidata, et võrrandi $f(x) = 0$ Galois rühma substitutsioonid on kõik paarissubstitutsioonid siis ja ainult siis, kui põhikorpus sisaldab suurust $\sqrt{D}$, kus D tähendab polünoomi $f(x)$ diskriminanti.

154. Leida laiendi $K(\sqrt{2}, \sqrt{5})$ alamkorpused, kui K tähendab ratsionaalarvude korpust. Missugused neist alamkorpustest on Galois korpused?

155. Näidata, et tsüklilise korpuse alamkorpused on ka tsüklilised.

156. Näidata, et võrrand $x^5 - p^2x - p = 0$ ei ole lahenduv radikaalides, kui p tähendab positiivset algarvu.

Harjutusülesannete vastuseid.

I. Kompleksarvud ja Hermite'i vormid. Algebrad.

1. a) 4; b) -2; c) $\frac{\sqrt{2}}{2}(1+i\sqrt{3})$;

d) $\pm(\sqrt{3}+i)$, $\pm(1-\sqrt{3}i)$; e) $\pm(|a+b|+i|a-b|)$, kui $|a| \geqslant |b|$ ja $\pm(|a+b|-i|a-b|)$, kui $|a| < |b|$.

2. a) $2+i$, $1-3i$; b) $\pm(4+i)$, $\pm(4-i)$; c) $3+4i$;

d) $\frac{1}{2}(\pm\sqrt{15}-i)$.

3. $x_1 = 3+11i$, $x_2 = -3+9i$, $x_3 = 1+7i$.

4. a) $2(\cos\frac{11}{6}\pi + i\sin\frac{11}{6}\pi)$; b) $\frac{1}{\cos\alpha}(\cos\alpha + i\sin\alpha)$.

6. $\frac{3\pm\sqrt{3}}{2} + i\frac{1\mp\sqrt{3}}{2}$.

7. Rööpküliku diagonaalide ruutude summa on võrdne külgede ruutude summaga.

8. $\cos 4\varphi = \cos^4\varphi - 6\cos^2\varphi\sin^2\varphi + \sin^4\varphi$,
$\sin 4\varphi = 4\cos^3\varphi\sin\varphi - 4\cos\varphi\sin^3\varphi$.

9. a) $2^9(1-\sqrt{3}i)$; b) $\pm\left(\sqrt{\frac{\sqrt{2}+1}{2\sqrt{2}}} + i\sqrt{\frac{\sqrt{2}-1}{2\sqrt{2}}}\right)$,

$\pm\left(\sqrt{\frac{\sqrt{2}-1}{2\sqrt{2}}} - i\sqrt{\frac{\sqrt{2}+1}{2\sqrt{2}}}\right)$.

10. a) $\frac{1}{i}$; b) 2^{-13}.

11. $\pm\frac{1}{\sqrt{2}}(1+i)$, $\pm\frac{1}{\sqrt{2}}(1-i)$.

12. $c_1 = \frac{2}{3}a$, $c_2 = -\frac{2}{3}ia$, $c_3 = \frac{1}{3}ia$, kus $|a| = 1$.

13. $x_k = \bar{a}_k \cdot b$.

14. -1, -2.

15. a) $|u_1|^2 + |u_2|^2 - 2|u_3|^2$,

$$x_1 = u_1 - iu_2 + u_3$$
$$x_2 = u_2 + iu_3$$
$$x_3 = u_3;$$

b) $2|u_1|^2 + 2|u_2|^2 - 2|u_3|^2 - 2|u_4|^2$,

$$x_1 = u_1 - u_4$$
$$x_2 = u_2 + u_3$$
$$x_3 = iu_2 - iu_3$$
$$x_4 = u_1 + u_4.$$

16. a) $|u_1|^2 + 2|u_2|^2 - 3|u_3|^2$,

$$x_1 = u_1$$
$$x_2 = \frac{2i}{\sqrt{5}} u_2 - \frac{i}{\sqrt{5}} u_3$$
$$x_3 = \frac{1}{\sqrt{5}} u_2 + \frac{2}{\sqrt{5}} u_3;$$

b) $2|u_1|^2 + \sqrt{2}|u_2|^2 - \sqrt{2}|u_3|^2$,

$$x_1 = \frac{1}{2} u_1 - \frac{\sqrt{2}+1}{2\sqrt{2+\sqrt{2}}} u_2 + \frac{\sqrt{2}-1}{2\sqrt{2-\sqrt{2}}} u_3 - \frac{1}{2} u_4$$

$$x_2 = -\frac{i}{2} u_1 - i\frac{\sqrt{2}+1}{2\sqrt{2+\sqrt{2}}} u_2 + i\frac{\sqrt{2}-1}{2\sqrt{2-\sqrt{2}}} u_3 + \frac{i}{2} u_4$$

$$x_3 = -\frac{i}{2} u_1 + i\frac{1}{2\sqrt{2+\sqrt{2}}} u_2 + i\frac{1}{2\sqrt{2-\sqrt{2}}} u_3 - \frac{i}{2} u_4$$

$$x_4 = \frac{1}{2} u_1 + \frac{1}{2\sqrt{2+\sqrt{2}}} u_2 + \frac{1}{2\sqrt{2-\sqrt{2}}} u_3 + \frac{1}{2} u_4.$$

17. $x_1 = u_1 - iu_2 - u_3$
$x_2 = u_1 + u_2 + iu_3$
$x_3 = iu_3$.

18. a) määramata;
b) positiivselt määratud;
c) negatiivselt määratud;
d) määramata.

19. $-2i + 2k$.

20. a) $\frac{1}{10}(1+2i+8j+k)$;

b) $\frac{a_1b_1+a_2b_2+a_3b_3+(a_2b_3-a_3b_2)i+(a_3b_1-a_1b_3)j+(a_1b_2-a_2b_1)k}{b_1^2+b_2^2+b_3^2}$;

c) $\xi = bi+cj+dk$, kus $b^2+c^2+d^2=1$.

21. a) määrab; b) määrab; c) ei määra.

22.

	b_1	b_2
b_1	b_1-b_2	b_1+b_2
b_2	b_1+b_2	b_2-b_1

23. $\begin{Vmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{Vmatrix}$; $\begin{Vmatrix} a_1 & 0 \\ a_2 & a_1 \end{Vmatrix}$; $\begin{Vmatrix} a_1 & a_2 & 0 \\ a_2 & a_1 & 0 \\ a_3 & -a_3 & a_1+a_2 \end{Vmatrix}$.

II. Polünoomid üle korpuse.

24. $a_1=0$, $b_1=2$, $a_{2,3}=\pm\frac{1}{2\sqrt{2}}$, $b_{2,3}=3$.

25. a) x^2-1; b) $x^2-2\sqrt{2}x-1$.

26. a) $X=i$, $Y=-ix$; b) $X=1-x$, $Y=2x^2-2x-3$.

27. a) $(x-1)(x+1)(x^2+1)(x^4+1)$;

b) $(x-1)(x+1)(x^2+1)(x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$;

c) $(x-1)(x+1)(x-i)(x+i)(x-\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i)(x-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i)(x+\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i)(x+\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i)$;

d) $(x-1)(x+1)(x^2+1)(x^2-3x+1)(x^2+3x+1)$.

28. a) $q(x)=2x^4-4x^3+3x^2-6x+4$, $r(x)=-8$;

b) $q(x)=2x^4+2ix^3-7x^2-7ix-1$, $r(x)=-i$.

29. $\sqrt{3}=2i$, $\sqrt{5}=3i$, kus $i^2=-1$.

30. $1+3j+4j^2$.

31. $(x-j)(x-j^2)(x-j-j^2)$, kus $j^3=-j-1$.

32. a) $\frac{x-1}{8(x^2+3)}-\frac{1}{8(x-1)}+\frac{1}{4(x-1)^2}$;

b) $\frac{\sqrt{3}+i}{16\sqrt{3}(x-\sqrt{3}i)}+\frac{\sqrt{3}-i}{16\sqrt{3}(x+\sqrt{3}i)}-\frac{1}{8(x-1)}+\frac{1}{4(x-1)^2}$;

c) $\frac{2x-2}{x^2+3}-\frac{2}{x-1}-\frac{1}{(x-1)^2}$.

33. a) $-1062+352(x+4)-70(x+4)(x+1)+$
$+14(x+4)(x+1)(x-1)+$
$+3(x+4)(x+1)(x-1)(x-3)+$
$+(x+4)(x+1)(x-1)(x-3)(x-4)$;

b) $-2787+927(x+4)-185(x+4)(x+1)+31(x+$
$+4)(x+1)(x-1)+3(x+4)(x+1)(x-1)(x-3)+$
$+2(x+4)(x+1)(x-1)(x-3)(x-4)$.

34. a) $24+73(x-2)+78(x-2)^2+40(x-2)^3+$
$+10(x-2)^4+(x-2)^5$;

b) $21+72(x-2)+90(x-2)^2+56(x-2)^3+$
$+17(x-2)^4+2(x-2)^5$.

35. a) $\frac{1}{(x+2)^2}-\frac{6}{(x+2)^3}+\frac{13}{(x+2)^4}-\frac{12}{(x+2)^5}$;

b) $\frac{1}{x+1}-\frac{4}{(x+1)^2}+\frac{7}{(x+1)^3}-\frac{6}{(x+1)^4}+\frac{1}{(x+1)^5}$.

36. a) $x^3-9x^2+21x-8$; b) $x^4+2x^3-3x^2+3$.

37. $f(0)=\frac{1}{n}(y_0+y_1+y_2+\ldots+y_{n-1})$.

38. $a=3$, $b=-4$.

39. $k=3$, $b=0$, $a\neq 0$.

40. $3x^4-4x^3-6x^2+12x+3$.

41. 5.

42. a) $(x-2)(x^2-2x+2)^2$; b) $(x^2+x+1)(x^2+2)^2$;
c) $(x^2+1)^2(x-1)^3$.

III. Polünoomid üle integriteetkonna.

44. a) $\xi_1=1$, $\xi_2=-2$, $\xi_3=3$, $\xi_{4,5}=\pm i$;

b) $\xi_1=\frac{1}{2}$, $\xi_{2,3}=-1\pm i\sqrt{3}$;

c) $\xi_1 = \frac{1}{2}$, $\xi_2 = -3$, $\xi_{3,4} = -\frac{1}{3}(1 \pm \sqrt{13})$.

47. $2x_1^3x_2 - 3x_1^3x_3 - 3x_1^2x_2^2 + 6x_1^2x_2x_3 + x_1^2x_3^2 - 2x_1x_2^3 + + 6x_1x_2^2x_3 - 13x_1x_2x_3^2 + 3x_1x_3^3 + 3x_2^3x_3 - x_2^2x_3^2 + + 3x_2x_3^3 - x_3^4$.

49. a) $\sigma_1^3 - 3\sigma_1\sigma_2$; b) $\sigma_1\sigma_2 - \sigma_3$; c) $\sigma_1^4 - 4\sigma_1^2\sigma_2 + 8\sigma_1\sigma_3 - 8\sigma_4$.

51. a) $x^5 - 4x^4 + 7x^3 - 8x^2 + 6x - 4$;

b) $x^4 - 2(a+b)x^2 + (a-b)^2$.

52. $\xi_1 = 4$, $\xi_{2,3} = \pm\frac{3}{2}$.

53. $\lambda = -2$; $\xi_{1,3} = -1 \pm \sqrt{3}$, $\xi_2 = -1$.

54. $\lambda = 8$; $\xi_{1,3} = \frac{1}{2}(1 \pm i\sqrt{15})$, $\xi_2 = -2$.

55. a) 2; b) 2 2 4.

56. 1, −1, 2.

57. $S = \frac{1}{4}\sqrt{a(-a^3 + 4ab - 8c)}$, $R = \frac{c}{\sqrt{a(-a^3 + 4ab - 8c)}}$.

59. $\xi = 1$.

60. $\lambda_1 = 3$, $\lambda_2 = -1$.

63. $-1 \pm \sqrt{2}$.

64. $\lambda_1 = 0$, $\lambda_2 = 1\,2\,5$, $\lambda_3 = -3$.

67. a) $x^6 - 4x^4 + 3x^2 - 12x + 12 = 0$;

b) $x^3 + 4x^2 - x - 4 = 0$.

IV. Algebralised võrrandid.

68. $\lambda = 78$.

69. a) $\xi_1 = 4$, $\xi_{2,3} = 1 \pm 4\sqrt{3}i$;

b) $\xi_1 = -2i$, $\xi_{2,3} = i$;

c) $\xi_{1,2} = -1 \pm i\sqrt{2}$, $\xi_{3,4} = -1 \pm i\sqrt{3}$;

d) $\xi_1 = 1$, $\xi_{2,3} = \frac{1}{4}(-1 + \sqrt{5} \pm i\sqrt{10 + 2\sqrt{5}})$,

$\xi_{4,5} = \frac{1}{4}(-1 - \sqrt{5} \pm i\sqrt{10 - 2\sqrt{5}})$;

e) $\xi_1 = -1$, $\xi_{2,3} = \frac{1}{2}(1 \pm i\sqrt{3})$,
$\xi_{4,5} = \frac{1}{2}(1 + \sqrt{3} \pm \sqrt{2\sqrt{3}})$,
$\xi_{6,7} = \frac{1}{2}(1 - \sqrt{3} \pm i\sqrt{2\sqrt{3}})$;

f) $\xi_1 = a$, $\xi_{2,3} = a \pm b$;

g) $\xi_{1,2} = -a \pm \sqrt{a^2 - 1}$, $\xi_{3,4} = \frac{1}{2}(-a \pm \sqrt{a^2 - 8})$.

70. a) $\xi_1 = 1$, $\xi_2 = 4$, $\xi_3 = 5$;
b) $\xi_1 = 3$, $\xi_2 = 6$, $\xi_{3,4} = -4 \pm 3i$;
c) $\xi_{1,2} = \pm 1$, $\xi_3 = 3 + 6i$, $\xi_4 = 2 + 5i$, $\xi_5 = 5 + i$, $\xi_6 = 1 + 4i$.

71. a) $\xi_1 = 1$, $\eta_1 = 0$; $\xi_2 = 0$, $\eta_2 = 1$; $\xi_{3,4} = \frac{1}{4}(1 \pm i\sqrt{3})$, $\eta_{3,4} = \frac{1}{4}(-3 \pm i\sqrt{3})$; $\xi_{5,6} = \frac{1}{4}(-3 \pm i\sqrt{3})$, $\eta_{5,6} = \frac{1}{4}(1 \pm i\sqrt{3})$;
b) $\xi_1 = 1$, $\eta_1 = 0$; $\xi_2 = 0$, $\eta_2 = 1$; $\xi_3 = 5$, $\eta_3 = 4$; $\xi_4 = 6$, $\eta_4 = 5$; $\xi_5 = 4$, $\eta_5 = 5$; $\xi_6 = 5$, $\eta_6 = 6$.

72. $\xi_2 = -i$, $\xi_{3,4} = -1 \pm i\sqrt{2}$, $\xi_{5,6} = -1 \pm i\sqrt{3}$.

73. a) $(x-1)(x+1)(x-i)(x+i)\left(x - \frac{1+i\sqrt{3}}{2}\right)\left(x - \frac{1-i\sqrt{3}}{2}\right)\left(x + \frac{1-i\sqrt{3}}{2}\right)\left(x + \frac{1+i\sqrt{3}}{2}\right)\left(x - \frac{\sqrt{3}+i}{2}\right)\left(x - \frac{\sqrt{3}-i}{2}\right)\left(x + \frac{\sqrt{3}-i}{2}\right)\left(x + \frac{\sqrt{3}+i}{2}\right)$;
b) $(x-1)(x+1)(x^2+1)(x^2-x+1)(x^2+x+1)(x^2-\sqrt{3}x+1)(x^2+\sqrt{3}x+1)$.

74. a) $\left(\frac{1}{2}, 1\right)$, $\left(-4, -\frac{1}{2}\right)$; b) $(1, 2)$, $(-2, -1)$.

75. a) $(-2, -1)$, $(-1, 0)$, $(0, 1)$, $(4, 5)$;
b) $\left(-2, -\frac{3}{2}\right)$, $\left(-\frac{3}{2}, -1\right)$, $\left(0, \frac{1}{2}\right)$, $\left(\frac{1}{2}, 1\right)$, $(1, 2)$.

76. 5, 3 või 1 selle järgi, kas $a^5 \gtreqless b^2$.

77. a) 3; b) 2; c) 1; d) 1.

78. $\lambda = -5$.

79. $0 \leqslant \lambda \leqslant 6$.

80. 1,6180341.

81. 0,34730.

82. $\xi_1 \approx 2{,}146$; $\xi_2 \approx -0{,}682$; $\xi_3 \approx -1{,}328$; $\xi_4 \approx -4{,}146$.

V. Polünoommaatriksid ja Jordani normaalkuju.

83. a) $\begin{Vmatrix} 1 & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x(x+1) \end{Vmatrix}$; b) $\begin{Vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x^2-3x+1 & 0 \\ 0 & 0 & 0 & 0 \end{Vmatrix}$.

84. a) $d_{1,2,3}(x) = 1$, $d_4(x) = x^4 + x - 1$;
b) $d_1(x) = 1$, $d_2(x) = x$, $d_3(x) = x^2(x+1)$,
$d_4(x) = x^4(x+1)^3(x-1)$;
c) $d_{1,2,3}(x) = 1$, $d_4(x) = [(x+a)^2 + b^2]^2$.

85. ei.

87. $d_1 = 1$, $d_2 = 2$, $d_3 = 4$, $d_4 = 16$; $e_1 = 1$, $e_{2,3} = 2$, $e_4 = 4$.

88. $U = \begin{Vmatrix} 2 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{Vmatrix}$, $V = \begin{Vmatrix} -4 & -7 & -5 \\ -7 & -12 & -9 \\ 1 & 1 & 1 \end{Vmatrix}$.

89. a) 3; b) 1.

90. K_4; jah.

92. $\{(c_2,\ c_1 + 3c_2,\ c_1 + c_2,\ 2c_1 + 2c_2)\}$.

95. $\{(0,\ c_1,\ c_2,\ c_3)\}$.

97. $\{(c_1 + c_2 + c_3,\ c_1,\ c_2,\ c_3)\}$, $\{(-c,\ c,\ c,\ c)$

98. a) $\begin{Vmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{Vmatrix}$; b) $\begin{Vmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & \frac{1}{2}(1+i\sqrt{3}) & 0 \\ 0 & 0 & 0 & \frac{1}{2}(1-i\sqrt{3}) \end{Vmatrix}$.

c) $\begin{Vmatrix} 2 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{Vmatrix}$.

99. a) taandub; b) ei taandu.

101. a) ja c).

102. a) $\boldsymbol{b}_1 = (0, 0, 1)$, $\boldsymbol{b}_2 = (1, 1, -8)$, $\boldsymbol{b}_3 = (3, -6, 20)$;
b) $\boldsymbol{b}_1 = (0, -1, 1)$, $\boldsymbol{b}_2 = (0, 1, 0)$, $\boldsymbol{b}_3 = (1, 0, 0)$.

VI. Rühmateooria alused.

107.

	e	f_1	f_2	f_3	f_4	f_5
e	e	f_1	f_2	f_3	f_4	f_5
f_1	f_1	e	f_5	f_4	f_3	f_2
f_2	f_2	f_4	e	f_5	f_1	f_3
f_3	f_3	f_5	f_4	e	f_2	f_1
f_4	f_4	f_2	f_3	f_1	f_5	e
f_5	f_5	f_3	f_1	f_2	e	f_4

108. 1, 8, 4, 8, 2, 8, 4, 8.

109. $\{1, 3, 4, 5, 9\}$, $R^{(11)}$, $\{1, 10\}$.

111. $(A+B)^2 = \{e, f_2, f_3, f_4, f_5\}$.

112. $\{e, f_1\}$, $\{e, f_2\}$, $\{e, f_3\}$, $\{e, f_4, f_5\}$ (normaaljagaja).

113. $\left\{e, \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\right\}$, $\left\{e, \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}\right\}$,
$\left\{e, \begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}\right\}$, $\left\{e, \begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\right\}$.

114. $\{e, f_1\} + \{f_2, f_5\} + \{f_3, f_4\}$, $\{e, f_1\} + \{f_2, f_4\} + \{f_3, f_5\}$,
$\{e, f_2\} + \{f_1, f_4\} + \{f_3, f_5\}$, $\{e, f_2\} + \{f_1, f_5\} + \{f_3, f_4\}$,
$\{e, f_3\} + \{f_1, f_5\} + \{f_2, f_4\}$, $\{e, f_3\} + \{f_1, f_4\} + \{f_2, f_5\}$,
$\{e, f_4, f_5\} + \{f_1, f_2, f_3\}$.

115. $\{1, 5, 8, 12\} + \{2, 3, 10, 11\} + \{4, 6, 7, 9\}$.

119. a) $\left\{e, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$;

b) $\left\{e, \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}$.

122. $G \supset \{e, a^2, a^4, a^6, \ldots, a^{22}\} \supset$

$\supset \{e, a^4, a^8, a^{12}, a^{16}, a^{20}\} \supset \{e, a^8, a^{16}\} \supset E$,

$G \supset \{e, a^2, a^4, a^6, \ldots, a^{22}\} \supset$

$\supset \{e, a^4, a^8, a^{12}, a^{16}, a^{20}\} \supset \{e, a^{12}\} \supset E$,

$G \supset \{e, a^2, a^4, a^6, \ldots, a^{22}\} \supset$

$\supset \{e, a^6, a^{12}, a^{18}\} \supset \{e, a^{12}\} \supset E$,

$G \supset \{e, a^3, a^6, a^9, \ldots, a^{21}\} \supset$

$\supset \{e, a^6, a^{12}, a^{18}\} \supset \{e, a^{12}\} \supset E$.

123. 2, 2, 2, 3, 5.

125. (1 7 5 4)(2 3 6).

126. $\bar{s} = (7\ 3\ 8)(1\ 6)(5\ 2\ 4)$, $\bar{t} = (2\ 3\ 5)(8\ 6\ 4\ 7)$.

128. $\{e\} + \{(1\ 2)(3\ 4)\} + \{(1\ 3)(2\ 4), (1\ 4)(2\ 3)\} +$

$+ \{(1\ 2), (3\ 4)\} + \{(1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$,

$\{e, (1\ 2)(3\ 4)\}, \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$,

$\{e, (1\ 2)(3\ 4), (1\ 2), (3\ 4)\}$,

$\{e, (1\ 2)(3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$.

129. $H \supset \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \supset$

$\supset \{e, (1\,2)(3\,4)\} \supset E$,

$H \supset \{e, (1\ 2)(3\ 4), (1\ 2), (3\ 4)\} \supset \{e, (1\,2)(3\,4)\} \supset E$,

$H \supset \{e, (1\,2)(3\,4), (1\,3\,2\,4), (1\,4\,2\,3)\} \supset$

$\supset \{e, (1\,2)(3\,4)\} \supset E$.

130. $\{e, (1\ 3)(2\ 4)\}, \{e, (1\ 4)(2\ 3)\}$.

131. a) $\{e, (1\,2), (3\,4), (1\,2)(3\,4)\}$;

b) $\{e, (1\ 2)(3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$;

c) $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$; d) H.

133. $M_1 = \{1, 2\}$, $M_2 = \{3, 4\}$.

VII. Korpuseteooria alused.

134. a) 6; b) $x^2 - 2$.

137. $5^{-1} = 3$, $(\sqrt{2})^{-1} = 2$.

138. $x = 2$, $y = 3$.

139. a) 2; b) 3; c) 5.

141. a) $x^6 - 6x^4 + 12x^2 - 6$; b) $x^4 + x^3 + x^2 + x + 1$.

142. 2.

143. p^k.

144.

	e	a	b
e	e	a	b
a	a	$-e-a$	$-e$
b	b	$-e$	a

145. $(x - \xi)(x + \xi)(x - \xi^3)(x + \xi^3)$.

146. a) 6; b) 3.

147. a) 4; b) 2.

VIII. Galois teooria alused.

150. neljarühm.

151. a) S_3; b) $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$;

c) $\{e, (1\ 2\ 4\ 3), (1\ 3\ 4\ 2), (1\ 4)(2\ 3)\}$;

d) $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

152. a) $\{e, (1\ 2)\}$; b) $\{e, (1\ 2)\}$.

154. $K(\sqrt{2})$, $K(\sqrt{5})$, $K(\sqrt{10})$ (kõik Galois korpused).

Aineregister.

Aditiivne rühm 248
adjungeerimine 333
alamkorpus 328
alamring 313
alamruumi dimensioon 198
alamrühm e. jagaja 253
alamrühma indeks 258
— normalisaator 272
algebra e. hüperkomplekssüsteem 40
algebra järk 40
algebraline element 338
— laiend 339
— lihtlaiend 338
algebraliselt kinnine korpus 70
algelement 103
algjuur 25
algkorpus 329
algrühm 284
astmesummad 119

Baasielemendid 42
baasivektorid 199
Bezout' teoreem 62
binoomvõrrand 140, 371

Cardano valem 142

Descartes'i reegel 171
determinantjagajad 192
diferentseerimise ahelreegel 108
diskriminant 130

Eisensteini teoreem 97
ekvivalentsed laiendid 347
elemendi aste 339
— järk 249
— normalisaator 270
elementaarjagajad 192
elimineerimine 132
esimest liiki pöördvõrrand 150
eukleidiline ruum 30
Euleri valem 109

Faktorring e. jäägiklassiring ideaali järgi 318
faktorrühm 262

Galois korpus e. normaalkorpus 352
— rühm 363
— teooria põhilause 381
— teoreem 398
Gaussi ratsionaalarvud 320
— täisarvud 320

Hamilton-Cayley seos 212
Hermite'i bilineaarvorm 32
— maatriks e. enesekaasmaatriks 31
— ruutvorm 32
homomorfne vastavus e. homomorfism 275, 325
Horneri skeem 64
hüpertasand 200

Ideaal 314
identne automorfism 267
imaginaartelg 14
imaginaarühik 8
imprimitiivne substitutsioonirühm 306

imprimitiivsuse klassid 307
interpolatsiooniprobleem 80
invariantne alamruum 205
isobaarne polünoom 113
isomorfismi jätk 344
isomorfsed normaaljadad 286

Jagamisega algebra e. hüperkomplekskorpus 40
Jordan-Hölderi teoreem 286
Jordani kastike 210
— normaalkuju 225
jäägiklassikorpus polünoomi järgi 68
jäägiklassiring polünoomi järgi 66

Kaasalamrühmad 272
kaaselemendid (korpuses) 352
— (rühmas) 269
kaaskompleksid 9
kaaskvaternioonid 39
kaaslaiendid 352
kaasmaatriksid 27
kaaspolünoomid 159
kaassubstitutsioonid 299
kaasvektorid 28
karakteristlik maatriks 211
— polünoom 211
kast-diagonaalmaatriks 206
kommutatiivne e. Abeli rühm 240
kompleks e. osahulk 251
kompleksarv 8
kompleksarvu absoluutväärtus e. moodul 12
— argument e. amplituud 16
— imaginaarosa 8
— — kordaja 8
— reaalosa 8
— trigonomeetriline kuju 16
komplekside ühisosa 253
komplekstasand 14
kompositsioonifaktorid 289
kompositsiooni-indeksid 288
kompositsioonijada 284
kongruents ideaali järgi 317
kordne lahend 71
korpuse karakteristika 84
korrutamistabel 42
kvaternioon 38
kõrgeim liige 105
kõrvalklass 255
kõrvalklassi esindaja 255

Lagrange'i interpolatsioonivalem 80
— resolvent 378
— teoreem 258
lahenduv e. metatsükliline rühm 289
lahenduvus radikaalides 140, 390
leksikograafiline järjestus 105
lihtlaiend 335
lihtlaiendi aste 341
lihtmurd 73
liitelement 103
lineaarne alamruum 198
Lobatševski menetlus 181
lõplik rühm 242
lõpliku arvu moodustajatega rühm 293
lõpmata kõrge element 294
lõpmatut järku element 250

Maclaurini valem 163
maksimaalne normaaljagaja 284
m-dimensionaalne tasand 200
mittekommutatiivne korpus 38
mittelahutuv rühm 293
modulaarne rühm 295
Moivre'i valem 21
moodustav element 335
multiplikatiivne rühm 248
märgimuut 168
määramata kordajate meetod 57
määrav polünoom 339

Neljarühm 266
Newtoni interpolatsioonivalem 78
— lähendusvalem 175
— menetlus 174
— valemid 120

nilpotentne teisendus 207
normaaljada 284
— faktorid 284
— pikkus 284
normaaljagaja e. invariantne alamrühm 258, 273
normeeritud polünoom 56
normaalsuse tingimus 259
nullideaal 314
nullring 313

Osamurdudeks lahutamise valemid 75
osatuletis 108
otsekorrutis 292
otsesumma 203

Paaris-substitutsioon 300
paaritu substitutsioon 300
parempoolne kõrvalklass 255
— pöördelement 239
— ühikelement 239
peaideaal 314
peaideaaliring 320
polünoomi kaal 113
— lahutuskorpus 343
— liikme kaal 113
— pealiige 51
— tuletis 86
— tõus 81, 82
polünoomide algebra põhilause 69
polünoommaatriks 188
primaarne rühm 294
primitiivne element 353
— polünoom 95
puht-imaginaararv 8
pärisalamkorpus 328
pärisalamring 313
pärisalamrühm 253
pärisnormaaljagaja 259
pöördsubstitutsioon 242
pöördvõrrand 159

Ratsionaalfunktsioon 52
ratsionaalfunktsioonide korpus 52
reaaltelg 14
Remak-Schmidti teoreem 293
resultant 121
Ruffini-Abeli teoreem 399
rühm 239
rühma automorfism 267
— järk 242
— postulaadid 240
— tsenter 290
rühmade isomorfism 264

Siseautomorfism 268
Sturmi ahelik 167
— teoreem 168
substitutsioon 240
substitutsiooni aste 240
sümmeetrilised polünoomid 109
— põhipolünoomid 110
sümmeetriline rühm 242
sümmeetriliste polünoomide põhilause 110
Sylvesteri determinant 125

Taandumatu juhtum 147
— polünoom 60
taanduv polünoom 60
Taylori valem 79
teist liiki pöördvõrrand 150
teoreem isomorfismist 282
— primitiivsest elemendist 353
— ringi homomorfismidest 327
— rühma homomorfismidest 278
transitiivne substitutsioonirühm 305
transtsendentne element 338
— laiend 343
— lihtlaiend 338
Tschirnhausi teisendus 141
tsükkel 297
tsükliline alamruum 207
— baas 207
— korpus 378
— rühm 249
täisratsionaalne funktsioon e. polünoom 52

Unimodulaarmaatriks 195
unitaarmaatriks 28
unitaarne ruum 30
unitaarortogonaalsed vektorid 29
unitaarnormeeritud vektor 29
unitaarteisendus 30

Vabakorrutis 295
vahelduv e. alterneeruv rühm 301
vasakpoolne kõrvalklass 255
— pöördelement 244
— ühikelement 244
vektori kõrgus 221
vektoriruum e. lineaarne ruum 39, 198
Vieta valemid 116
välisautomorfism 268
võrrandi Galois rühm 365

Ühejuured 24
ühene vastavus 275
ühikideaal 314
ühikrühm 253
ühiksubstitutsioon e. identne substitutsioon 242
ühistegurita elemendid 322
— polünoomid 56
üldine võrrand 399
ülemkorpus e. laiend 69, 332

Sisukord.

Lk.

Eessõna 3

I. Kompleksarvud ja Hermite'i vormid. Algebrad.

§ 1. Kompleksarvud.

1. Kompleksarvude korpus 5
2. Kaaskompleksid ja kompleksarvu absoluutväärtus 10
3. Kompleksarvude geomeetriline interpretatsioon 13
4. Kompleksarvude astendamine ja juurimine 20
5. Ühejuured 24

§ 2. Hermite'i vormid.

1. Unitaarmaatriksid 27
2. Hermite'i vormid 30

§ 3. Algebrad.

1. Kvaternioonide korpus 37
2. Algebra mõiste 39
3. Algebra esitus maatriksite abil 44
Harjutusülesandeid (nr. 1—23) 47

II. Polünoomid üle korpuse.

§ 4. Polünoomide jaguvuse teooria.

1. Eukleidese algoritm 51
2. Võrrandi $f(x)X + g(x)Y = h(x)$ lahenduvus polünoomides 57
3. Taandumatud polünoomid 59

§ 5. Polünoomi lahendid.

1. Polünoomi jagumine lineaarteguriga 62
2. Jäägiklassiringid polünoomide järgi 65
3. Polünoomi lahendite olemasolu 69

Lk.

§ 6. Ratsionaalfunktsioonid ja interpolatsioonivalemid.

1. Ratsionaalfunktsioonide lahutamine osamurdudeks 72
2. Newtoni interpolatsioonivalem 78
3. Interpolatsiooniprobleem 80

§ 7. Polünoomi tuletis ja kordsed lahendid.

1. Korpuse karakteristika 84
2. Polünoomi tuletis 86
3. Kordsed lahendid 88
Harjutusülesandeid (nr. 24—42) 91

III. Polünoomid üle integriteetkonna.

§ 8. Polünoomi taanduvus täisarvude integriteetkonnas.

1. Algtegureiks lahutamise lause 94
2. Eisenstein'i teoreem 97
3. Ratsionaallahendite leidmine 99
4. Polünoomi taanduvus integriteetkonnas 102

§ 9. Sümmeetrilised polünoomid.

1. Mitme muutuja polünoomid 104
2. Sümmeetriliste polünoomide põhilause 109
3. Vieta valemid 115
4. Astmesummad 118

§ 10. Resultant ja diskriminant.

1. Resultant 121
2. Diskriminant 129
3. Eliminatsiooniprobleem 131
Harjutusülesandeid (nr. 43—67) 137

IV. Algebralised võrrandid.

§ 11. Võrrandite algebraline lahendus.

1. Tschirnhaus'i teisendus 140
2. Kolmanda astme võrrand 142
3. Neljanda astme võrrand 147
4. Pöördvõrrandid 150

§ 12. Kompleksarvude algebra põhilause.

1. Põhilause tõestus 154
2. Järeldusi põhilausest 158

Lk.

§ 13. Reaalkordajatega võrrandid.

1. Reaallahendite tõkked 162
2. Sturm'i lause 167
3. Descartes'i reegel 171
4. Newtoni menetlus 174
5. Lobatševski menetlus 181
Harjutusülesandeid (nr. 68—82) 185

V. Polünoommaatriksid ja Jordan'i normaalkuju.

§ 14. Polünoommaatriksid.

1. Polünoommaatriksi normaalkuju 187
2. Elementaarjagajad 192
3. Ekvivalentsed polünoommaatriksid 194

§ 15. Vektoriruumi lineaarsed alamruumid.

1. Lineaarse alamruumi mõiste 197
2. Alamruumide otsesumma 201
3. Invariantsed alamruumid 205

§ 16. Jordani normaalkuju.

1. Maatriksi karakteristliku võrrandi omadusi 210
2. Vektoriruumi lahutamine invariantsete alamruumide otsesummaks . 214
3. Jordani normaalkuju 220

§ 17. Polünoommaatriksite teooria rakendus Jordani normaalkujule.

1. Jordani normaalkuju kastikeste järgud 226
2. Järeldusi Jordani normaalkujust 230
3. Jordani normaalkujule vastava baasi leidmine 231
Harjutusülesandeid (nr. 83—102) 234

VI. Rühmateooria alused.

§ 18. Rühma mõiste.

1. Sümmeetriline rühm 239
2. Järeldusi rühma postulaatidest 243
3. Tsüklilised rühmad 248

§ 19. Alamrühmad.

1. Kompleksid 251
2. Alamrühma mõiste 253
3. Kõrvalklassid 255
4. Normaaljagaja 258

Lk.

§ 20. Isomorfism.

1. Isomorfismi mõiste 264
2. Automorfism 267
3. Kaaselemendid 268
4. Kaasalamrühmad 272

§ 21. Homomorfism.

1. Homomorfismi mõiste 274
2. Teoreem rühma homomorfismidest 277
3. Teoreem isomorfismist 281

§ 22. Kompositsioonijadad.

1. Maksimaalne normaaljagaja 284
2. Jordan-Hölder'i teoreem 286
3. Lahenduvad rühmad 288
4. Nõukogude matemaatikute osa kaasaegse rühmateooria arengus . . 292

§ 23. Substitutsioonirühmad.

1. Tsüklid 296
2. Vahelduv rühm 300
3. Transitiivsus ja imprimitiivsus 305
Harjutusülesandeid (nr. 103—133) 310

VII. Korpuseteooria alused.

§ 24. Ringiteooria alused.

1. Ideaali mõiste 313
2. Jäägiklassiringid ideaalide järgi 315
3. Peaideaaliringid 319
4. Ringide homomorfism 325

§ 25. Algkorpused ja lihtlaiendid.

1. Algkorpused 328
2. Korpuse laiendamine 332
3. Lihtlaiendid 336

§ 26. Polünoomi lahutuskorpus.

1. Lahutuskorpuse ühesus 343
2. Galois korpus 350
3. Teoreem primitiivsest elemendist 353
Harjutusülesandeid (nr. 134—149) 358

Lk.

VIII. Galois teooria alused.

§ 27. Galois rühm.

1. Galois rühma mõiste 360
2. Võrrandi Galois rühm 365
3. Binoomvõrrandi Galois rühm 371

§ 28. Galois teooria põhilause.

1. Alamkorpuste ja alamrühmade vastavus 380
2. Järeldusi Galois teooria põhilausest 384

§ 29. Galois teooria rakendusi.

1. Võrrandi lahenduvus radikaalides 390
2. Geomeetrilised konstruktsioonid sirkli ja joonlaua abil 399
3. Võrrandi lahenduvus reaalsetes radikaalides 403
Harjutusülesandeid (nr. 150—156) 407
Harjutusülesannete vastuseid 409
Aineregister 419

Vastutav toimetaja H. Keres.
Kaanejoonise valmistanud I. Linnat.
Keeleline toimetaja M. Tamm.
Tehniline toimetaja H. Seletus.

Ladumisele antud 24. II 1950. Trükkimisele antud 11. V 1950. Trükiarv 1200. Paber 61 × 86, 1/16. Trükipoognaid 26,75. Formaadile 60 × 92 kohaldatud trükipoognaid 25,41. Arvutuspoognaid 21,2. MB-03368.
Trükikoda „Hans Heidemann", Tartu, Vallikraavi 4. Tellimise nr. 663.

На эстонском языке.
Г. Кангро. Высшая алгебра II.

Hind rbl. 8.65

TÜ RAAMATUKOGU
1030001595949 9

A-17176

Rbl. 8.65