

Algebra II

Praktikumid
sügis 2024

praktikumijuhendaja: Kristo Väljako

Sisukord

I	Algebraliste põhistruktuuride meeldetuletus. Alamstruktuurid	5
II	Homomorfismid ja isomorfismid	10
III	Faktorühmad. Faktoringid	15
IV	Otsekorrutised ja otsesummad	21
V	Mitme muutuja polünoomid. Sümmeetrilised polünoomid	27
VI	Mitme muutuja polünoomid. Polünoomide Juured. Algebra põhiteoreem	32
VII	Polünoomi lahutuskorpus	37
VIII	Matriksi Jordani normaalkuju	45
IX	(Bi)lineaarsed funktsionaalid. Kaasruum	58
X	Ruutvormid	68
XI	Tsüklilised rühmad	83
XII	Perioodilised ja vabad Abeli rühmad	91

Siia materjali olen kokku kogunud praktikumi ülesannete lahendused, mida kasutasin aine Algebra II (MTMM.00.040) praktikumide asemel 2021. aasta kevadel. See praktikumide materjal on mõeldud koos kasutamiseks Valdis Laane loengukonspektiga [1]. Teadupoolest valitses 2021 kevadel maailmas COVID-19 ning seetõttu oli Tartu Ülikoolis kogu õpe distantstil. Loodan, et need lahendused, mille kirjutamise vajadus tuli lohkavast viirushaigusest, on kasuks ka tulevikus selle aine lugemisel.

2021. aasta kevadel oli 12 alljärgnevat praktikumi. Lisaks toimus 2 auditoorset kontrolltööd, üks pärast IV praktikumi ja teine kõige lõpus. Lisaks oli 4 kodutööd praktikumide I ja II; V ja VI; VII ja VIII ning IX ja X teemade peale.

Sama materjali – väheste parandustega – kasutasin ka 2022. ja 2024. aasta sügissemestril.

Kristo Väljako

Praktikum I Algebraliste põhistruktuuride meeldetuletus. Alamstruktuurid

Ütleme, et poolrühm G on (mõlemapoolse) taandamisega, kui kehtivad

$$\forall a, b, c \in G: a * c = b * c \implies a = b,$$

$$\forall a, b, c \in G: c * a = c * b \implies a = b.$$

Kui eelnevatest tingimustest kehtib vaid üks, siis on tegemist kas vastavalt vasakpoolse või parempoolse taandamisega.

Edaspidi ma ei kirjuta ülesannete lahendustes tehtemärki $*$ välja ja kasutan korrutamise terminoloogiat.

Ülesanne I.1. Tõestada, et mittetühi lõplik (mõlemapoolse) taandamisega poolrühm on rühm.

Lahendus: Tähistame ülesandes antud poolrühma $G = \{a_1, \dots, a_n\}$. Valime elemendi $g \in G$. Vaatame kujutust $f_g: G \rightarrow G$, $a_k \mapsto ga_k$. Vastavalt taandamise nõudele kehtib $ga_k = ga_h$ parajasti siis, kui $k = h$, mistõttu on kujutus f_g injektiivne. Kuna G on lõplik, järeldeb f_g injektiivsusest ka tema surjektiivsus. Seega $\text{Im}(f_g) = \{ga_k | a_k \in G\} = G$. Seega leigub element $a_h \in G$ nii, et $g = ga_h$.

Olgu nüüd $b \in G$ suvaline. Vaatleme korrutist

$$gb = (ga_h)b = g(a_hb),$$

millest (vasakult) taandamisega saame $b = a_hb$. Nüüd vaatleme korrutist

$$bb = b(a_hb) = (ba_h)b,$$

kust (paremalt) paremalt taandamisega saame $b = ba_h$. Kokkuvõttes oleme näidanud, et $a_h =: \varepsilon$ on rühma G ühikelement.

Vaatleme taaskord elementi $g \in G$ ja bijektiivset kujutust f_g . Kuna $\varepsilon \in G = \text{Im}(f_g)$, siis leidub element $a_j \in G$ nii, et $\varepsilon = ga_j$. Analoogiliselt saame bijektiivse kujutuse $\hat{f}_g: G \rightarrow G$, $a_k \mapsto a_kg$ abil, et leidub ka element $\hat{a}_j \in G$ nii, et $\varepsilon = \hat{a}_jg$. Nüüd

$$a_j = \varepsilon a_j = (\hat{a}_jg)a_j = \hat{a}_j(ga_j) = \hat{a}_j\varepsilon = \hat{a}_j.$$

Järelikult leidub pöördelement $g^{-1} := a_j = \hat{a}_j$, mistõttu G on rühm. □

Ülesanne I.2. Tõestada, et kui rühma iga element on iseenda pöördelement, siis on tegu Abeli rühmaga.

Lahendus: Olgu G rühm, kus kehtib $aa = \varepsilon$ iga $a \in G$ korral. Olgu $a, b \in G$, vaatleme järgmist korrutist

$$ab = ab\varepsilon = ab((ba)(ba)) = a(bb)aba = a\varepsilon aba = (aa)ba = \varepsilon ba = ba.$$

Seega rühm G on kommutatiivne ehk Abeli rühm. □

Ülesanne I.3. Leida, mitmel eri viisil saab neljaelemendilise hulga rühmaks muuta.

Lahendus: Olgu $\{\varepsilon, a, b, c\}$ neljaelemendiline hulk. Hakkame täitma vastavat Cayley tabelit. Esiteks peab rühmas olema ühikelement, mida etteruttavalt tähistasin ε ; vastavalt sellele saame Cayley tabelis täita ühe rea ja veeru. Lisaks peab rühmas olema igal elemendil üheselt määratud pöördelement, seetõttu peab Cayley tabeli igas veerus ja igas reas leiduma iga element täpselt üks kord. Allpool toome välja Cayley tabeli, kus on täidetud kindlad kohad ja nendesse, mille täitmiseks on valik, on kirjutatud arv, mitu elementi sinna sobiks:

*	ε	a	b	c
ε	ε	a	b	c
a	a	3	1	1
b	b	1	2	1
c	c	1	1	1

Eelnevast võiks arvata, et selliseid 4 elemendilisi rühmi on kokku $3 \cdot 2 = 6$. Siiski, kui hakata eelnevat tabelit täitma, siis kaks tabelit langevad ära ja saame 4 erinevat tabelit, mis on ka allpool ära toodud:

*	ε	a	b	c
ε	ε	a	b	c
a	a	ε	c	b
b	b	c	ε	a
c	c	b	a	ε
G_1				
*	ε	a	b	c
ε	ε	a	b	c
a	a	ε	c	b
b	b	c	a	ε
c	c	b	ε	a
G_2				
*	ε	a	b	c
ε	ε	a	b	c
a	a	b	c	ε
b	b	c	ε	a
c	c	ε	a	b
G_3				
*	ε	a	b	c
ε	ε	a	b	c
a	a	c	ε	b
b	b	ε	c	a
c	c	b	a	ε
G_4				

Kui aga vaatame nüüd eelnevaid tabeleid hoolega, siis märkame, et kujutused

$$\begin{aligned} f: G_2 &\rightarrow G_3, & (f(\varepsilon), f(a), f(b), f(c)) &= (\varepsilon, b, a, c) \\ g: G_2 &\rightarrow G_4, & (g(\varepsilon), g(a), g(b), g(c)) &= (\varepsilon, c, b, a) \end{aligned}$$

osutuvad isomorfismideks, mitõttu $G_2 \cong G_3 \cong G_4$. Järelikult leidub isomorfismi täpsuseni ainult 2 erinevat neljaelemendilist rühma (G_1 ja G_2). $\square$

Ülesanne I.4. Olgu $G = \{a_1, \dots, a_n\}$ lõplik Abeli rühm ja $c = a_1 * \dots * a_n$. Tõestada, et $c * c = \varepsilon$, kus ε on rühma G ühikelement.

Lahendus: Kehtigu ülesande eeldused (G lõplikust on vaja, et leiduks $c \in G$). Olgu $a_h \in G$ ($h \in \{1, \dots, n\}$). Kuna G on rühm, siis pöördelement $a_h^{-1} = a_k \in G$. Kuna G on Abeli rühm, siis võime korrutises elemente ümberjärjestada. Seega kehtib

$$\begin{aligned} cc &= (a_1 \dots a_{h-1} a_h a_{h+1} \dots a_n)(a_1 \dots a_{k-1} a_k a_{k+1} \dots a_n) = \\ &= a_h a_k (a_1 \dots a_{h-1} a_{h+1} \dots a_n)(a_1 \dots a_{k-1} a_{k+1} \dots a_n) = \\ &= \varepsilon (a_1 \dots a_{h-1} a_{h+1} \dots a_n)(a_1 \dots a_{k-1} a_{k+1} \dots a_n) = \\ &= (a_1 \dots a_{h-1} a_{h+1} \dots a_n)(a_1 \dots a_{k-1} a_{k+1} \dots a_n). \end{aligned}$$

Analoogiliselt saame kõik elemendid viia kõrvuti oma pöördelemendiga, misjärel saamegi tulemuseks $cc = \varepsilon$. $\square$

Ülesanne I.5. Leida kõik $(\mathbb{Z}, +)$ alamrühmad. Kas nende alamrühmade ühisosa võtmine vastab mingile teisele algebralisele tehtele?

Lahendus: Olgu H suvaline rühma $(\mathbb{Z}, +)$ mittetriviaalne alamrühm (s.t. $H \neq \{0\}$ ja $H = \mathbb{Z}$). Tähistame sümboliga n alamrühma H vähimat positiivset elementi. Selline n leidub, kuna igas rühmas $\mathbb{Z}$ alamrühmas leidub positiivseid ja negatiivseid elemente ($z \in H \implies -z \in H$).

Olgu $h \in H$ suvaline. Kuna $(\mathbb{Z}; +, \cdot)$ on Eukleidese ring (kursusest Algebra I), saame elementi h jäägiga jagada elemendiga n , teisisõnu leiduvad täisarvud $q, r \in \mathbb{Z}$ nii, et $h = qn + r$, kus $0 \leq r < n$. Kuna alamrühma H on vastavalt definitsioonile liitmise suhtes kinnine kehtivad $qn \in H$ ja $r = h - qn \in \mathbb{Z}$. Teisest küljest, kuna $0 \leq r < n$ ja n on vähim positiivne element rühmas H , saame $r = 0$. Seega $h = qn$, $q \in \mathbb{Z}$ ehk $H = n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\}$.

Kokkuvõttes saime, et iga rühma $(\mathbb{Z}, +)$ pärisalamrühm on kujul $n\mathbb{Z}$, $n \in \mathbb{N}$.

Olgu meil kaks alamrühma $n\mathbb{Z}$ ja $m\mathbb{Z}$, $n, m \in \mathbb{N}$. Vaatleme nende ühisosa

$$n\mathbb{Z} \cap m\mathbb{Z} = \{z \mid (n \mid z) \& (m \mid z)\}.$$

Eelnevast näeme, et kehtib valem $n\mathbb{Z} \cap m\mathbb{Z} = \text{VÜK}(n, m)\mathbb{Z}$, kus $\text{VÜK}(n, m)$ on arvude n, m vähim ühiskordne. $\square$

Ülesanne I.6. Leidke ringide $\mathbb{Z}_{10}$ ja $\mathbb{Z}_7$ kõik pööratavad elemendid.

Lahendus: Ringi $\mathbb{Z}_{10}$ kõiki pööratavaid elemente on lihtsaim leida selle ringi korrutamise Cayley tabelist. (Selle Cayley tabeli välja kirjutamine on ka kasulik, et saada täielikku arusaama, mis selles ringis toimub.) Seega siin ta on:

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\bar{2}$	$\bar{5}$	$\bar{8}$	$\bar{1}$	$\bar{4}$	$\bar{7}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{2}$	$\bar{6}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{2}$	$\bar{6}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{8}$	$\bar{5}$	$\bar{2}$	$\bar{9}$	$\bar{6}$	$\bar{3}$
$\bar{8}$	$\bar{0}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{9}$	$\bar{0}$	$\bar{9}$	$\bar{8}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Siit tabelist on näha, et ringi $\mathbb{Z}_{10}$ pööratavad elemendid on $\bar{1}$ ($\bar{1}^{-1} = \bar{1}$), $\bar{3}$ ($\bar{3}^{-1} = \bar{7}$), $\bar{7}$ ($\bar{7}^{-1} = \bar{3}$) ja $\bar{9}$ ($\bar{9}^{-1} = \bar{9}$). Eelnev on kooskõlas Arvuteooria kursuses õpetatava tingimusega, et element $\bar{a}$ on ringis $\mathbb{Z}_n$ pööratav parajasti siis, kui $\text{SÜT}(a, n) = 1$.

Ringi $\mathbb{Z}_7$ korral võib ka Cayley tabeli teha, kuid mõistlikum oleks meenutada Algebra I kursusest, et ring $\mathbb{Z}_n$ on korpus parajasti siis, kui n on algarv. Kuna 7 on teadupoolest algarv, siis $\mathbb{Z}_7$ on korpus ning vastavalt korpuse definitsioonile on kõik nullist erinevad elemendid pööratavad. $\square$

Ülesanne I.7. Kas saab leida näidet ringist R ühikelemendiga $1 \neq 0$ ja tema alamringist A ühikelemendiga 1_A , kus $1_A \neq 0$ ja $1_A \neq 1$?

Lahendus: Vastavalt alamringi definitsioonile ei saa sellist olukorda olla. Alamring peab olema kooskõlas kõigi oma ülemringi tehetega, sealhulgas 0-aarse ühikelemendi fikseerimise tehetega. $\square$

Ülesanne I.8. Kas ring, mis ei ole korpus, võib sisaldada alamkorpust?

Lahendus: Jah. Näiteks polünoomide ring $K[X]$, kus K on mingi korpus. Ring $K[X]$ ei ole korpus, kuna ühelgi mittekonstantsel polünoomil (s.t. $\deg(f) \geq 1$) ei leidu pöördelementi. See asjaolu tuleb valemist

$$\forall f, g \in K[X]: \quad \deg(fg) = \deg(f) + \deg(g).$$

Samas ring $K[X]$ sisaldab korpust K alamkorpuseks, kui konstantsete polünoomide hulk:

$$K[X] \supset K \cong \{f \in K[X] \mid f = 0 \vee \deg(f) = 0\}.$$

(Sümbol $\supset$ tähistab range sisalduvusega ülemstruktuuri.) $\square$

Eelneva ülesande lahenduseks sobib ka näide $\mathbb{C} < \mathbb{H}$, kus $\mathbb{C}$ on kompleksarvude korpus ja $\mathbb{H}$ kvaternioonide ring. Kvaternioonid on kompleksarvude (ja seeläbi ka reaalarvude) üldistus. Kvaternioonid avalduvad kujul $z_1 + \mathbf{j}z_2$, kus $z_1, z_2 \in \mathbb{C}$ ja $\mathbf{j}$ on kvaternioonühik, mis rahuldab tingimusi $\mathbf{j}^2 = -1$ ja $i\mathbf{j} = -\mathbf{j}i$ (i on 'tavaline' kompleksarvudest tuntud imaginaarühik). Ainaüksi viimasest arvutuseeskirjast on näha, et kvaternioonide korrutamine ei ole üldjuhul kommutatiivne, mistõttu $\mathbb{H}$ ei ole korpus.

Ülesanne I.9. Olgu X mittetühi hulk ja $\mathcal{P}(X)$ tema alamhulkade hulk. Defineerime hulga X alamhulga A korrutised korpuse $\mathbb{Z}_2$ elementidega võrdustega $\bar{1}A = A$ ja $\bar{0}A = \emptyset$. Kas hulk $\mathcal{P}(X)$ on vektorruum üle $\mathbb{Z}_2$, kui liitmise osas vaadelda sümmeetrilist vahet Δ ?

Lahendus: Jah. Selles võib veenduda kontrollides vektorruumi aksioome, mis on väga lihtne. $\square$

Minu arust on eelmises ülesandes tegemist huvitava näitega vektorruumist.

Ülesanne I.10. Leidke vektorruumi $\mathbb{R}_6[X]$ vektorite süsteemi

$$f_1 = X^6 + X^4, \quad f_2 = X^6 + 3X^4 - X, \quad f_3 = X^6 - 2X^4 + X, \quad f_4 = X^6 - 4X^4 + 2X$$

lineaarse katte mõõde ja baas.

Lahendus: Uurime, mis on süsteemi $S := \{f_1, f_2, f_3, f_4\}$ astak. Kasutades ruumi $\mathbb{R}_6[X]$ kanoonilist baasi $\{X^6, X^5, X^4, X^3, X^2, X, 1\}$, saame esitada antud vektorid koordinaat-kujul. Kogume need kujud maatriksisse, kus igale veerule vastab üks vektor, ning teostame selle maatriksiga elementaarteisendusi:

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 0 & 0 & -1 & 0 \\ 1 & 0 & -2 & 0 & 0 & 1 & 0 \\ 1 & 0 & -4 & 0 & 0 & 2 & 0 \end{pmatrix} \xrightarrow{-I} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & -1 \\ 0 & -3 & 1 \\ 0 & -5 & 2 \end{pmatrix} \cdot (-1) \rightarrow \begin{pmatrix} 1 & 1 & 0 \\ 0 & -2 & 1 \\ 0 & -3 & 1 \\ 0 & -5 & 2 \end{pmatrix} \rightarrow$$

$$\rightarrow \begin{pmatrix} 1 & 1 & 0 \\ 0 & -2 & 1 \\ 0 & -3 & 1 \\ 0 & -3 & 1 \end{pmatrix} \xrightarrow{-\text{III}} \begin{pmatrix} 1 & 1 & 0 \\ 0 & -2 & 1 \\ 0 & -3 & 1 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{+\frac{3}{2}\text{II}} \begin{pmatrix} 1 & 1 & 0 \\ 0 & -2 & 1 \\ 0 & 0 & \frac{5}{2} \\ 0 & 0 & 0 \end{pmatrix}.$$

(Vahepeal jätsin välja null-veerud, kuna nad ei mängi lineaarse sõltumatuse uurimises mingit rolli). Eelnevast saame, et $\text{rank}(S) = 3$. (Alles jäänud matriksi determinant on võrdne $1 \cdot (-2) \cdot \frac{5}{2} = -5 \neq 0$, kuna tegemist on kolmnurkmatriksiga).

Kokkuvõttes näeme, et küsitud lineaarkatte mõõde ehk dimensioon

$$\dim \text{span}(S) = \text{rank}(S) = 3.$$

Antud matriksarvutusest on näha ka, et lineaarkatte baasiks sobib $\{f_1, f_2, f_3\}$. □

Eelmise ülesande juures muidugi ilmselt on võimalik ka näha, et $f_4 = f_1 - f_2 + f_3$ ning seejärel kontrollida, et $\{f_1, f_2, f_3\}$ on lineaarselt sõltumatu süsteem. See lahendus on muidugi siintoodust lühem. Kuid pedagoogilistel põhjustel tahtsin võimalikult üldise lahendusskeemi anda.

Ülesanne* I.11. Kas ring, milles kehtib samasus $x^3 = x$, on kommutatiivne?

Praktikum II Homomorfismid ja isomorfismid

Ülesanne II.1. Tõestage, et kujutus $\psi: \theta \mapsto \cos \theta + i \sin \theta$ on homomorfism rühmast $(\mathbb{R}; +)$ rühma $(\{z \in \mathbb{C} \mid |z| = 1\}; \cdot)$. Leidke homomorfismi ψ tuum $\text{Ker } \psi$.

Lahendus: Tähistame $S_1 := \{z \in \mathbb{C} \mid |z| = 1\}$ (tähistus tuleb sellest, et antud hulk on ühikringjoon komplekstasandil). Olgu $\theta_1, \theta_2 \in \mathbb{R}$, siis

$$\psi(\theta_1 + \theta_2) = \cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2) = e^{i(\theta_1 + \theta_2)} = e^{i\theta_1} e^{i\theta_2} = \psi(\theta_1) \psi(\theta_2).$$

Seega on ψ rühmade homomorfism. (Eelnevas leidis kasutust de Moivre valem).

Leiame tuuma $\text{Ker } \psi$. Olgu $\theta \in \text{Ker } \psi$, siis

$$1 = \psi(\theta) = \cos \theta + i \sin \theta = e^{i\theta} \implies \theta = 2\pi n, \quad (n \in \mathbb{Z}).$$

Järelikult $\text{Ker } \psi = \{2\pi n \mid n \in \mathbb{Z}\}$. Siit saame muuhulgas järeldada, et homomorfism ψ ei ole injektiivne. $\square$

Ülesanne II.2. Leida kõik rühma $(\mathbb{Z}, +)$ endomorfismid.

Lahendus: Olgu $\phi: \mathbb{Z} \rightarrow \mathbb{Z}$ aditiivne endomorfism (s.t. liitmise suhtes homomorfism, mille lähte- ja sihthulk langevad kokku). Tähistame $n := \phi(1) \in \mathbb{Z}$. Võtame suvalise $m \in \mathbb{N}_1$, siis

$$\phi(m) = \phi\left(\sum_{k=1}^m 1\right) = \sum_{k=1}^m \phi(1) = \sum_{k=1}^m n = n \sum_{k=1}^m 1 = nm.$$

Seega ahend $\phi|_{\mathbb{N}_1}: \mathbb{N}_1 \rightarrow \mathbb{Z}$ käitub kujul $m \mapsto nm$. Nüüd peame uurima, kuidas kujutus ϕ käitub hulgal $\{\dots, -2, -1, 0\}$. Kuna ϕ on endomorfism, siis

$$\begin{aligned} \phi(0) &= 0 = n0, \\ \phi(-m) &= -\phi(m) = -(nm) = n(-m), \quad (m \in \mathbb{N}_0). \end{aligned}$$

Seega endomorfism $\phi: \mathbb{Z} \rightarrow \mathbb{Z}$, avaldub kujul $z \mapsto nz$, kus $n \in \mathbb{Z}$. Vastavalt meie konstruktsioonile ei saa teistsuguseid endomorfisme $\mathbb{Z} \rightarrow \mathbb{Z}$ olla. Kokkuvõttes $\text{End}((\mathbb{Z}, +)) = \{z \mapsto nz \mid n \in \mathbb{Z}\}$. $\square$

Viisakusest võiks ka igaks juhuks kontrollida, kas eelnevalt konstrueeritud ϕ on ikka endomorfism. See järeldub eelnevast konstruktsioonist, kuid kontrolliks võib seda kontrollida. (See kontroll on väga lihtne.)

Ülesanne II.3. Tõestada, et rühm $(\mathbb{Q}, +)$ ei ole isomorfne rühmaga $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Lahendus: Vaatleme rühmi $(\mathbb{Q}, +)$ ja $(\mathbb{Q} \setminus \{0\}, \cdot)$. Oletame vastuväiteliselt, et eksisteerib rühmade isomorfism $\iota: \mathbb{Q} \rightarrow \mathbb{Q} \setminus \{0\}$. Kuna ι on bijektiivne, leidub ratsionaalarv $q \in \mathbb{Q} \setminus \{0\}$ nii, et $\iota(q) = -1$. Tulenevalt ι homomorfisusest, saame

$$-1 = \iota(q) = \iota\left(\frac{q+q}{2}\right) = \iota\left(\frac{1}{2}q + \frac{1}{2}q\right) = \iota\left(\frac{1}{2}q\right) \iota\left(\frac{1}{2}q\right) = \left(\iota\left(\frac{1}{2}q\right)\right)^2.$$

Kuna $\frac{1}{2}q$ on ilmselt ratsionaalarv, leidub ratsionaalarv $p := \iota(\frac{1}{2}q) \in \mathbb{Q}$ nii, et $p^2 = -1$. See on ilmselge vastuolu. $\downarrow$

Kokkuvõttes ei leidu isomorfismi $\iota: \mathbb{Q} \rightarrow \mathbb{Q} \setminus \{0\}$. $\square$

Ülesanne II.4. Olgu $f: G \rightarrow G'$ rühmade homomorfism. Tõestada, et $\text{Im } f$ on Abeli rühm parajasti siis, kui $xyx^{-1}y^{-1} \in \text{Ker } f$ iga $x, y \in G$ korral.

Lahendus: Olgu $f: G \rightarrow G'$ rühmade homomorfism. Loeme teadaolevaks, et homomorfismi f kujutus $\text{Im } f$ on alati rühm ning kehtib valem $(ab)^{-1} = b^{-1}a^{-1}$.

($\Rightarrow$) Olgu $\text{Im } f$ Abeli rühm ja $x, y \in G$. Paneme tähele, et

$$\begin{aligned} f(xyx^{-1}y^{-1}) &= f(x)f(y)f(x^{-1})f(y^{-1}) = f(x)f(y)(f(x))^{-1}(f(y))^{-1} = \\ &= f(y)(f(x)(f(x))^{-1})(f(y))^{-1} = f(y)\varepsilon(f(y))^{-1} = f(y)(f(y))^{-1} = \varepsilon. \end{aligned}$$

Seega $xyx^{-1}y^{-1} \in \text{Ker } f$.

($\Leftarrow$) Kehtigu iga $x, y \in G$ korral $xyx^{-1}y^{-1} \in \text{Ker } f$. Olgu $\xi, \eta \in \text{Im } f$, siis leiduvad $x, y \in G$ nii, et $f(x) = \xi$ ja $f(y) = \eta$. Paneme tähele, et

$$\begin{aligned} \varepsilon &= f(xyx^{-1}y^{-1}) = f(xy)f(x^{-1}y^{-1}) = f(xy)f((yx)^{-1}) = \\ &= f(xy)(f(yx)^{-1}) = f(x)f(y)(f(y)f(x))^{-1} = \xi\eta(\eta\xi)^{-1} = \xi\eta\xi^{-1}\eta^{-1}. \end{aligned}$$

Korrutades eelnevat võrdust paremalt elemendiga η ja seejärel elemendiga ξ , saamegi soovitud võrduse

$$\eta\xi = \xi\eta.$$

Järelikult on $\text{Im } f$ Abeli rühm. $\square$

Ülesanne II.5. Olgu G ja G' rühmad, kusjuures $G \cong G'$. Tõestage, et kui G on Abeli rühm, siis ka G' on Abeli rühm.

Tooge näide rühmadest G ja G' , kus G on Abeli rühm, aga G' ei ole, kuid leidub rühmade homomorfism $f: G \rightarrow G'$.

Lahendus: Olgu $\iota: G \rightarrow G'$ rühmade isomorfism ja G Abeli rühm. Võtame elemendid $\xi, \eta \in G'$. Kuna isomorfism ι on bijektiivne leiduvad $x, y \in G$ nii, et $\xi = \iota(x)$ ja $\eta = \iota(y)$. Paneme tähele, et

$$\xi\eta = \iota(x)\iota(y) = \iota(xy) = \iota(yx) = \iota(y)\iota(x) = \eta\xi.$$

Järelikult on G' samuti Abeli rühm.

Olgu G mittekommutatiivne rühm. Tsenter $\text{Cen}(G) = \{c \in G \mid cx = xc, \forall x \in G\}$ on alati Abeli rühm. Sisestus $f: \text{Cen}(G) \rightarrow G$ on homomorfism. (Ilmselgelt ei ole kujutus f sürjektiivne.)

Olgu S_3 substituutsioonide (ehk bijektiivsete kujutuste) $\{1, 2, 3\} \rightarrow \{1, 2, 3\}$ rühm (kompositsiooni tehaga $\circ$). On teada, et S_3 on mitte kommutatiivne (lihtne kontrollida). Kujutus

$$f: \mathbb{Z}_2 \rightarrow S_3, \quad \begin{cases} \bar{0} \mapsto \text{id} \\ \bar{1} \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \end{cases},$$

kus sümbol id tähistab samasusteisendust. Kujutus f on homomorfism:

$$\begin{aligned} f(\overline{0}) + f(\overline{0}) &= \text{id} \circ \text{id} = \text{id} = f(\overline{0}), \\ f(\overline{1}) + f(\overline{0}) &= f(\overline{1}) \circ \text{id} = f(\overline{1}), \\ f(\overline{1}) + f(\overline{1}) &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id} = f(\overline{0}). \end{aligned}$$

□

Eelmise ülesande teisel küsimusel leidub ka triviaalne vastus. Olgu G suvaline Abeli rühma ja suvaline G' mittekommutatiivne rühm ühikelemendiga ε . Siis kujutus $g \mapsto \varepsilon$ on homomorfism.

Ülesanne II.6. Olgu V_1 ja V_2 vektorruumid üle korpuse K . Defineerida tehted hulgal

$$\text{Hom}(V_1, V_2) := \{f: V_1 \rightarrow V_2 \mid f \text{ on lineaarkujutus}\}$$

nii, et tulemuseks oleks samuti vektorruum üle K .

Lahendus: Olgu V_1 ja V_2 vektorruumid üle korpuse K . Defineerime hulgas $\text{Hom}(V_1, V_2)$ tehted komponenthaaval, see tähendab, et iga $f, f_1, f_2 \in \text{Hom}(V_1, V_2)$ ja $k, x \in K$ korral

$$\begin{aligned} (f_1 + f_2)(x) &:= f_1(x) + f_2(x), \\ (kf)(x) &:= kf(x) = f(kx). \end{aligned}$$

On lihtne näha, et selliste tehetega osutub $\text{Hom}(V_1, V_2)$ vektorruumiks üle K . □

Vektorruum $\text{Hom}(V_1, V_2)$ on mitmetes matemaatika valdkondades väga oluline. Ei tohi segi ajada, et hulk $\text{Hom}(V_1, V_2)$ on lisaks ka rühm kompositsiooni tehte $\circ$ suhtes.

Ülesanne II.7. Olgu R ring ühikelemendiga ε . Tõestada, et kujutus $f: \mathbb{Z} \rightarrow R$, mis on defineeritud võrdusega $f(n) = n\varepsilon$, on ringide homomorfism. Leida ringi $\mathbb{Z}$ kujutus $f(\mathbb{Z}) := \text{Im } f$.

Lahendus: Olgu R ring ühikelemendiga ε . Olgu $n, m \in \mathbb{Z}$, siis

$$\begin{aligned} f(1) &= 1\varepsilon = \varepsilon, \\ f(nm) &= (nm)\varepsilon = \underbrace{\varepsilon + \dots + \varepsilon}_{nm} = \underbrace{(\varepsilon + \dots + \varepsilon)}_n \underbrace{(\varepsilon + \dots + \varepsilon)}_m = f(n)f(m), \\ f(n+m) &= (n+m)\varepsilon = \underbrace{\varepsilon + \dots + \varepsilon}_{n+m} = \underbrace{(\varepsilon + \dots + \varepsilon)}_n + \underbrace{(\varepsilon + \dots + \varepsilon)}_m = f(n) + f(m). \end{aligned}$$

Järelikult on f ringide homomorfism.

Vaatleme hulka $\text{Im } f = \{r \in R \mid \exists n \in \mathbb{Z}: r = f(n)\}$. See hulk on alamring, kuna f on homomorfism. Vaatleme alamringi H , mis rahuldab sisalduvust $\{0\} \subseteq H \subseteq \text{Im } f$. Kuna $\varepsilon \in H$, siis iga summa $\varepsilon + \dots + \varepsilon = n\varepsilon \in H$, mistõttu $H = \text{Im } f$. Seega on f kujutuseks ühikelemendi ε poolt tekitatud alamring $\text{Im } f = f(\mathbb{Z}) = \langle \varepsilon \rangle$. □

Ülesanne II.8. Olgu R_1 ja R_2 ringid ning $\varphi: R_1 \rightarrow R_2$ ringide homomorfism. Tõestada, et $\varphi(0) = 0$ ja $\varphi(-a) = -\varphi(a)$.

Lahendus: Olgu R_1 ja R_2 ringid ning $\varphi: R_1 \rightarrow R_2$ ringide homomorfism. Paneme tähele, et

$$\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0).$$

Liidame eelmisele võrdusele elemendi $-\varphi(0)$, saame võrduse $0 = \varphi(0)$. Nüüd saame $a \in R$ korral

$$\varphi(a) + \varphi(-a) = \varphi(a + (-a)) = \varphi(0) = 0,$$

kust saame tänu vastandelemendi definitsioonile, et $-\varphi(a) = \varphi(-a)$. □

Ülesanne II.9. Tõestage, et ringid $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ ja

$$R := \left\{ \begin{pmatrix} a & 3b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$$

on isomorfsed.

Lahendus: Vaatleme kujutust

$$\iota: \mathbb{Z}[\sqrt{3}] \rightarrow R, \quad a + b\sqrt{3} \mapsto \begin{pmatrix} a & 3b \\ b & a \end{pmatrix}.$$

Kujutus ι on ilmselt bijektiivne. Peame näitama, et ta on ringide homomorfism. Olgu $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Paneme tähele, et

$$\begin{aligned} \iota(1) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E, \\ \iota((a_1 + b_1\sqrt{3}) + (a_2 + b_2\sqrt{3})) &= \iota(a_1 + a_2 + (b_1 + b_2)\sqrt{3}) = \begin{pmatrix} a_1 + a_2 & 3(b_1 + b_2) \\ b_1 + b_2 & a_1 + a_2 \end{pmatrix} = \\ &= \begin{pmatrix} a_1 & 3b_1 \\ b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & 3b_2 \\ b_2 & a_2 \end{pmatrix} = \iota(a_1 + b_1\sqrt{3}) + \iota(a_2 + b_2\sqrt{3}). \end{aligned}$$

Kooskõla korrutamiseks näitamiseks leiame valemi ringi $\mathbb{Z}[\sqrt{3}]$ elementide korrutamiseks

$$(a_1 + b_1\sqrt{3})(a_2 + b_2\sqrt{3}) = (a_1a_2 + 3b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{3}.$$

Nüüd

$$\begin{aligned} \iota((a_1 + b_1\sqrt{3})(a_2 + b_2\sqrt{3})) &= \begin{pmatrix} a_1a_2 + 3b_1b_2 & 3(a_1b_2 + b_1a_2) \\ a_1b_2 + b_1a_2 & a_1a_2 + 3b_1b_2 \end{pmatrix} = \\ &= \begin{pmatrix} a_1 & 3b_1 \\ b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & 3b_2 \\ b_2 & a_2 \end{pmatrix} = \iota(a_1 + b_1\sqrt{3})\iota(a_2 + b_2\sqrt{3}). \end{aligned}$$

Kokkuvõttes on ι ringide isomorfism. □

Ülesanne II.10. Tõestada, et lõplikumõõtmelise vektorruumi iga sürjektiivne lineaarteisendus on selle vektorruumi automorfism. Kas sama väide kehtib ka lõpmatumõõtmelise ruumi korral?

Lahendus: Olgu V lõplikumõõtmeline vektorruum üle korpuse K (tähistame $n := \dim V$) ja $f: V \rightarrow V$ sürjektiivne lineaarteisendus (ehk homomorfism). Tähistame ruumi V baasi $B = \{\epsilon_1, \dots, \epsilon_n\}$. Kuna f on sürjektiivne, saame valida vektorid $e_1, \dots, e_n \in V$ nii, et $\epsilon_1 = f(e_1), \dots, \epsilon_n = f(e_n)$. Näitame, et vektorite süsteem $C := \{e_1, \dots, e_n\}$ on lineaarselt sõltumatu. Selleks valime $a_1, \dots, a_n \in K$ nii, et $a_1 e_1 + \dots + a_n e_n = 0$. Paneme tähele, et

$$0 = f(a_1 e_1 + \dots + a_n e_n) = a_1 f(e_1) + \dots + a_n f(e_n) = a_1 \epsilon_1 + \dots + a_n \epsilon_n,$$

seega $a_1 = \dots = a_n = 0$, kuna $\epsilon_1, \dots, \epsilon_n$ on lineaarselt sõltumatud. Järelikult on vektorite süsteem C lineaarselt sõltumatu, mistõttu ka ruumi V baas.

Võtame $v = (v_1, \dots, v_n)_C, w = (w_1, \dots, w_n)_C \in V$ nii, et $f(v) = f(w)$. Sel juhul

$$\begin{aligned} 0 &= f(v) - f(w) = f(v - w) = f((v_1 - w_1)e_1 + \dots + (v_n - w_n)e_n) = \\ &= (v_1 - w_1)f(e_1) + \dots + (v_n - w_n)f(e_n) = (v_1 - w_1)\epsilon_1 + \dots + (v_n - w_n)\epsilon_n. \end{aligned}$$

Järelikult $v_1 - w_1 = \dots = v_n - w_n = 0$, kust saame $v_1 = w_1, \dots, v_n = w_n$ ja seetõttu $v = w$. Kokkuvõttes oleme saanud, et f on ka injektiivne, mis teeb temast vektorruumi V automorfismi ($f \in \text{Aut}(V)$).

Lõpmatumõõtmelisel juhul juhul see väide ei kehti. Anname kontranäite. Vaatleme jadaruumi $\mathbb{R}^{\mathbb{N}} = \{(a_k)_{k \in \mathbb{N}} \mid a_k \in \mathbb{R}\}$. Ruum $\mathbb{R}^{\mathbb{N}}$ on lõpmatumõõtmeline vektorruum üle korpuse $\mathbb{R}$, kus tehted on defineeritud komponenthaaval. Kujutus

$$f: \mathbb{R}^{\mathbb{N}} \rightarrow \mathbb{R}^{\mathbb{N}}, \quad (a_1, a_2, a_3, \dots) \mapsto (a_2, a_3, a_4, \dots)$$

on sürjektiivne homomorfism, aga ilmselt ei ole ta injektiivne. □

Ülesanne* II.11. Tõestada, et iga vähemalt kolmeelemendiline lõplik rühm omab automorfismi, mis ei ole samasusteisendus. Kas sama väide kehtib ka lõpmatute rühmade korral?

Praktikum III Faktorrühmad. Faktorringid

Ülesanne III.1. Tõestada, et rühma G tsenter $\text{Cen}(G) = \{c \in G \mid cx = xc, \forall x \in G\}$ on selle rühma normaaljagaja.

Lahendus: Olgu G rühm. Kuna vastavalt rühma definitsioonile näeme, et ühikelement $\varepsilon \in \text{Cen}(G)$, siis tsenter $\text{Cen}(G)$ ei ole tühi. Kehtigu $h, h_1, h_2 \in \text{Cen}(G)$ ja $g \in G$, siis

$$\begin{aligned} h^{-1}g &= h^{-1}g\varepsilon = h^{-1}ghh^{-1} = h^{-1}hgh^{-1} = gh^{-1}, \\ (h_1h_2)g &= h_1(h_2g) = h_1(gh_2) = (h_1g)h_2 = (gh_1)h_2 = g(h_1h_2), \end{aligned}$$

mistõttu $h^{-1}, h_1h_2 \in \text{Cen}(G)$. Järelikult on tsenter $\text{Cen}(G)$ rühma G alamrühm.

Olgu $h \in \text{Cen}(G)$, siis vastavalt tsentri definitsioonile element h kommuteerub iga rühma G elemendiga. Olgu $g \in G$ suvaline, siis

$$g^{-1}hg = g^{-1}gh = h \in \text{Cen}(G).$$

Seega tsenter $\text{Cen}(G)$ on rühma G normaaljagaja. □

Ülesanne III.2. Leidke rühma $(\mathbb{C}^*, \cdot)$ kõrvalklassid alamrühma

$$U = \{z \in \mathbb{C} \mid |z| = 1\}$$

järgi. (Siin $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$.)

Tõestage, et rühma $\mathbb{C}^*$ faktorrühm U järgi on isomorfne rühmaga $(\mathbb{R}^+, \cdot)$.

Lahendus: Vaatleme rühma U rühma $(\mathbb{C}^*, \cdot)$ alamrühmana. Hulk U on tõesti alamrühm, kuna iga $z, z_1, z_2 \in U$ korral

$$\begin{aligned} |z^{-1}| &= |z|^{-1} = 1^{-1} = 1 \implies z^{-1} \in U, \\ |z_1z_2| &= |z_1||z_2| = 1 \cdot 1 = 1 \implies z_1z_2 \in U. \end{aligned}$$

Vastavalt loengukonspekti [1] lausele 1.42 teame, et $a, b \in \mathbb{C}^*$ korral $aU = bU$ parajasti siis, kui $a^{-1}b \in U$. Paneme tähele, et

$$a^{-1}b \in U \implies 1 = |a^{-1}b| = |a^{-1}| \cdot |b| = |a|^{-1} \cdot |b| \implies |a| = |b|.$$

Järelikult suvaline kõrvalklass alamrühma U järgi avaldub kujul

$$aU = \{z \in \mathbb{C} \mid |z| = |a|\}, \quad (a \in \mathbb{C}).$$

Teadupoolest saame nüüd rääkida faktorrühmast $\mathbb{C}^*/U = \{aU \mid a \in \mathbb{C}\}$. (Selle rühma ühikelement on $U = 1U$.)

Vaatleme nüüd rühma $(\mathbb{R}^+, \cdot)$ (positiivsete reaalarvude rühm). Defineerime kujutuse

$$\iota: \mathbb{R}^+ \rightarrow \mathbb{C}^*/U, \quad \iota(r) := rU.$$

Näitame, et ι on rühmade homomorfism ehk ta on kooskõlas selle rühma teh(e)tega, olgu $r_1, r_2 \in \mathbb{R}^+$

$$\begin{aligned}\iota(r_1 r_2) &= (r_1 r_2)U = (r_1 U)(r_2 U) = \iota(r_1)\iota(r_2), \\ (\iota(1) &= 1U = U).\end{aligned}\tag{1}$$

Uurime kujutuse ι injektiivsust. Olgu $r_1, r_2 \in \mathbb{R}^+$ sellised, et $r_1 \neq r_2$, sel juhul ka $|r_1| \neq |r_2|$. Järelikult

$$\iota(r_1) = r_1 U \neq r_2 U = \iota(r_2),$$

mistõttu ι on injektiivne.

Nüüd vaatleme suvalist kõrvalklassi $aU \in \mathbb{C}^*/U$. Vastavalt kompleksarvu moodulile $|a| \in \mathbb{R}^+$. Järelikult kehtib $aU = \iota(|a|)$, mistõttu ι on ka surjektiivne.

Kokkuvõttes oleme näidanud, et ι on bijektiivne rühmade homomorfism ehk rühmade isomorfism, mistõttu $(\mathbb{C}^*/U, \cdot) \cong (\mathbb{R}^+, \cdot)$.

Loodetavasti saate intuitiivselt sellest ülesandest aru, et ei kompleksarvule $z \in \mathbb{C}$ vastav ekvivalentsiklass on ringjoon komplekstasandil, mille keskpunkt on 0 ning, mis läbib kompleksarvu z . Isomorfism ι seab aga igale positiivsele reaalarvule $r \in \mathbb{R}^+$ vastavusse ringjoone komplekstasandil, mille keskpunkt on 0 ning raadius on r . $\square$

Märkus 1. Rühma puhul ei ole tegelikult vaja kontrollida homomorfismi kooskõla ühikelemendiga (rida (1)), kuna see järeldub kooskõlast rühma tehtega. Kuid universaalalgebra kontekstis (s.h. monoidide korral) on vaja kontrollida ka kooskõla kõikide null-aarsete tehetega.

Ülesanne III.3. Leida faktorühma $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(\bar{2}, \bar{0})\rangle$ Cayley tabel. Kas see meenutab mõne lihtsama rühma oma?¹

Lahendus: Meenutame, et vaatame siin ülesandes rühmi liitmise suhtes. Kõigepealt kirjutame välja antud alamrühma:

$$\langle(\bar{2}, \bar{0})\rangle = \{(\bar{2}, \bar{0}), (\bar{0}, \bar{0})\}.$$

Näitlikustamiseks kirjutame nüüd välja kõik faktorühma $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(\bar{2}, \bar{0})\rangle$ elemendid (kasutades standardset tähistust – kirjutades ekvivalentsiklassi esindaja kandiliste sulgude vahele)

$$\begin{aligned}[(\bar{0}, \bar{0})] &= (\bar{0}, \bar{0}) + \langle(\bar{2}, \bar{0})\rangle = \langle(\bar{2}, \bar{0})\rangle, \\ [(\bar{0}, \bar{1})] &= (\bar{0}, \bar{1}) + \langle(\bar{2}, \bar{0})\rangle = \{(\bar{2}, \bar{1}), (\bar{0}, \bar{1})\}, \\ [(\bar{1}, \bar{0})] &= (\bar{1}, \bar{0}) + \langle(\bar{2}, \bar{0})\rangle = \{(\bar{3}, \bar{0}), (\bar{1}, \bar{0})\}, \\ [(\bar{1}, \bar{1})] &= (\bar{1}, \bar{1}) + \langle(\bar{2}, \bar{0})\rangle = \{(\bar{3}, \bar{1}), (\bar{1}, \bar{1})\}, \\ [(\bar{2}, \bar{0})] &= (\bar{2}, \bar{0}) + \langle(\bar{2}, \bar{0})\rangle = \{(\bar{0}, \bar{0}), (\bar{2}, \bar{0})\} = [(\bar{0}, \bar{0})], \\ [(\bar{2}, \bar{1})] &= (\bar{2}, \bar{1}) + \langle(\bar{2}, \bar{0})\rangle = \{(\bar{0}, \bar{1}), (\bar{2}, \bar{1})\} = [(\bar{0}, \bar{1})], \\ [(\bar{3}, \bar{0})] &= (\bar{3}, \bar{0}) + \langle(\bar{2}, \bar{0})\rangle = \{(\bar{1}, \bar{0}), (\bar{3}, \bar{0})\} = [(\bar{1}, \bar{0})], \\ [(\bar{3}, \bar{1})] &= (\bar{3}, \bar{1}) + \langle(\bar{2}, \bar{0})\rangle = \{(\bar{1}, \bar{1}), (\bar{3}, \bar{1})\} = [(\bar{1}, \bar{1})].\end{aligned}$$

¹Rühmade otsekorrutist vaatleme täpsemalt järgmises praktikumis.

Nagu näha, siis faktorrühmas $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle(\bar{2}, \bar{0})\rangle$ on 4 elementi. Nüüd saame välja kirjutada selle faktorrühma Cayley tabeli

+	$[(\bar{0}, \bar{0})]$	$[(\bar{0}, \bar{1})]$	$[(\bar{1}, \bar{0})]$	$[(\bar{1}, \bar{1})]$
$[(\bar{0}, \bar{0})]$	$[(\bar{0}, \bar{0})]$	$[(\bar{0}, \bar{1})]$	$[(\bar{1}, \bar{0})]$	$[(\bar{1}, \bar{1})]$
$[(\bar{0}, \bar{1})]$	$[(\bar{0}, \bar{1})]$	$[(\bar{0}, \bar{0})]$	$[(\bar{1}, \bar{1})]$	$[(\bar{1}, \bar{0})]$
$[(\bar{1}, \bar{0})]$	$[(\bar{1}, \bar{0})]$	$[(\bar{1}, \bar{1})]$	$[(\bar{0}, \bar{0})]$	$[(\bar{0}, \bar{1})]$
$[(\bar{1}, \bar{1})]$	$[(\bar{1}, \bar{1})]$	$[(\bar{1}, \bar{0})]$	$[(\bar{0}, \bar{1})]$	$[(\bar{0}, \bar{0})]$

Nagu näha on see rühm isomorfne rühmaga $\mathbb{Z}_2 \times \mathbb{Z}_2$. □

Ülesanne III.4. Tõestage, et normaaljagajate ühisosa on normaaljagaja.

Lahendus: Olgu G rühm ning H_1 ja H_2 tema normaaljagajad. Uurime hulka $H_1 \cap H_2$. Kõigepealt veendume, et hulk $H_1 \cap H_2$ ei ole tühi. Kuna H_1 ja H_2 on rühma G alamrühmad, siis ühikelement ε kuulub mõlemasse alamrühma, mistõttu $\varepsilon \in H_1 \cap H_2$.

Veendume, et $H_1 \cap H_2$ rahuldab normaaljagaja tingimust. Olgu $h \in H_1 \cap H_2$ ja $g \in G$, siis

$$h \in H_1 \ \& \ h \in H_2 \xRightarrow{\text{normaaljagajad}} g^{-1}hg \in H_1 \ \& \ g^{-1}hg \in H_2 \implies g^{-1}hg \in H_1 \cap H_2.$$

Analoogilise argumendiga saab veenduda, et ühisosa $H_1 \cap H_2$ on alamrühm. Kokkuvõttes oleme näidanud, et $H_1 \cap H_2$ on G normaaljagaja. □

Tähistame järgmised ruutmaatriksite rühmad (korrutamise suhtes):

$$\begin{aligned} \text{GL}_n(\mathbb{R}) &:= \{A \in \text{Mat}_n(\mathbb{R}) \mid \det(A) \neq 0\} \quad (\text{regulaarsed maatriksid}), \\ \text{SL}_n(\mathbb{R}) &:= \{A \in \text{GL}_n(\mathbb{R}) \mid \det(A) = 1\}. \end{aligned}$$

Ülesanne III.5. Tõestage, et rühm $\text{SL}_n(\mathbb{R})$ on rühma $\text{GL}_n(\mathbb{R})$ normaaljagaja ja rühma $\text{GL}_n(\mathbb{R})$ faktorrühm normaaljagaja $\text{SL}_n(\mathbb{R})$ järgi on isomorfne rühmaga $(\mathbb{R}^*, \cdot)$, kus $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$.

Lahendus: Olgu $n \in \mathbb{N}_1$. Ilmselt leidub regulaarseid maatrikseid (näiteks ühikmaatriks), mistõttu $\text{SL}_n(\mathbb{R})$ ei ole tühi. Olgu $A, B \in \text{SL}_n(\mathbb{R})$, siis

$$\begin{aligned} \det(A^{-1}) &= (\det(A))^{-1} = 1^{-1} = 1 \implies A^{-1} \in \text{SL}_n(\mathbb{R}), \\ \det(AB) &= \det(A) \det(B) = 1 \cdot 1 = 1 \implies AB \in \text{SL}_n(\mathbb{R}). \end{aligned}$$

Järelikult on $\text{SL}_n(\mathbb{R})$ rühma $\text{GL}_n(\mathbb{R})$ alamrühm.

Olgu nüüd $A \in \text{SL}_n(\mathbb{R})$ ja $G \in \text{GL}_n(\mathbb{R})$ (regulaarsed maatriksid on parasjagu pööratavad maatriksid). Kasutades determinandi omadusi, saame

$$\det(G^{-1}AG) = \det(G^{-1}) \det(A) \det(G) = (\det(G))^{-1} \det(G) = 1.$$

Järelikult $G^{-1}AG \in \text{SL}_n(\mathbb{R})$. Kokkuvõttes on $\text{SL}_n(\mathbb{R})$ rühma $\text{GL}_n(\mathbb{R})$ normaaljagaja.

Nüüd anname faktorrühma $\text{GL}_n(\mathbb{R})/\text{SL}_n(\mathbb{R})$ suvalise elemendi kirjelduse:

$$[C] = C \text{SL}_n(\mathbb{R}) = \{A \in \text{Mat}_n(\mathbb{R}) \mid \det(A) = \det(C)\}, \quad (C \in \text{GL}_n(\mathbb{R})).$$

Defineerime kujutuse

$$\iota: \text{GL}_n(\mathbb{R})/\text{SL}_n(\mathbb{R}) \rightarrow \mathbb{R}, \quad \iota([C]) := \det(C).$$

Analoogiliselt ülesandega III.2 on lihtne näha, et kujutus ι on isomorfism. $\square$

Ülesanne III.6. Kas järgmiste ringide mittepööratavate elementide hulk on ideaal: a) $\mathbb{Z}$, b) $\mathbb{Z}_6$? Kas neid ringides leidub veel ideaale? Kui leidub, siis leida faktoring nende järgi.

Lahendus:

- a) Vaatleme ringi $\mathbb{Z}$. Selle ringi mittepööratavate elementide hulk on $\mathbb{Z} \setminus \{1, -1\}$. Võtame $2, -3 \in \mathbb{Z} \setminus \{1, -1\}$, vaatame nende summat

$$2 + (-3) = -1 \notin \mathbb{Z} \setminus \{1, -1\}.$$

Seega $\mathbb{Z} \setminus \{1, -1\}$ ei ole liitmise osas kinnine, järelikult pole see ka rühma $(\mathbb{Z}, +)$ alamrühm, seega pole $\mathbb{Z} \setminus \{1, -1\}$ ringi $\mathbb{Z}$ ideaal.

Paneme tähele, et ringi $\mathbb{Z}$ ideaalid on parajasti hulgad $n\mathbb{Z}$, kus $n \in \mathbb{Z}$. Eelnevast teame, et $\mathbb{Z} \setminus n\mathbb{Z} = \mathbb{Z}_n$.

- b) Vaatleme ringi $\mathbb{Z}_6$. Selle ringi mittepööratavate elementide hulk on $H := \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$. Kuna $\bar{2} + \bar{3} = \bar{5} \notin H$, siis hulk H ei ole ringi $\mathbb{Z}_6$ ideaal.

Paneme tähele, et ringil $\mathbb{Z}_6$ leidub kaks mittetriviaalset ideaali: $\bar{2}\mathbb{Z}_6 = \{\bar{0}, \bar{2}, \bar{4}\}$ ja $\bar{3}\mathbb{Z}_6 = \{\bar{0}, \bar{3}\}$. Vahetu kontroll näitab, et $\mathbb{Z}_6/(\bar{2}\mathbb{Z}_6) \cong \mathbb{Z}_2$ ja $\mathbb{Z}_6/(\bar{3}\mathbb{Z}_6) \cong \mathbb{Z}_3$.

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\square$

Ringi R ideaali I nimetatakse parempoolseks *peaideaaliks*, kui leidub element $a \in R$ nii, et $I = aR$. Vasakpoolne peaideaal defineeritakse analoogiliselt ($I = Ra$). Kommutatiivse ringi korral langevad need terminid kokku ja räägitakse lihtsalt peaideaalidest.

Ülesanne III.7. Leida Gaussi täisarvude ringi $G = \{a + bi \mid a, b \in \mathbb{Z}\}$ faktoring peaideaali $\langle 3 \rangle$ järgi.

Lahendus: Kirjutame välja elemendi 3 poolt tekitatud peaideaali

$$\langle 3 \rangle = 3G = \{3z \mid z \in G\} = \{3a + i3b \mid a, b \in \mathbb{Z}\}.$$

Näeme, et $\langle 3 \rangle$ on tõesti ideaal, sest suvaliste $a, a_1, a_2, b, b_1, b_2 \in \mathbb{Z}$ korral kehtivad

$$\begin{aligned} -(3a_1 + i3b_1) &= 3(-a_1) + i3(-b_1) \in \langle 3 \rangle, \\ (3a_1 + i3b_1) + (3a_2 + i3b_2) &= 3(a_1 + a_2) + i3(b_1 + b_2) \in \langle 3 \rangle, \\ (a + ib)(3a_1 + i3b_1) &= 3(aa_1 - bb_1) + i3(ab_1 + a_1b) \in \langle 3 \rangle. \end{aligned}$$

Vaatleme faktoringi $G/\langle 3 \rangle$. Urime, millal kehtib $[z_1] = [z_2]$, kus $[z_1], [z_2] \in G/\langle 3 \rangle$. Paneme tähele, et

$$[z_1] = [z_2] \iff z_1 + \langle 3 \rangle = z_2 + \langle 3 \rangle \iff z_1 - z_2 \in \langle 3 \rangle \iff \exists w \in G: z_1 - z_2 = 3w.$$

Tähistame $z_1 := a_1 + ib_1$, $z_2 := a_2 + ib_2$ ja $w = \alpha + i\beta$, kus $a_1, a_2, \alpha, b_1, b_2, \beta \in \mathbb{Z}$. Nüüd märkame, et eelneva põhjal

$$z_1 - z_2 = (a_1 - a_2) + i(b_1 - b_2) = 3\alpha + i3\beta = 3w \implies a_1 - a_2 = 3\alpha \text{ \& } b_1 - b_2 = 3\beta.$$

Järelikult kehtivad $3 \mid a_1 - a_2$ ja $3 \mid b_1 - b_2$. Märkame siin sarnasust jäägiklassiringidega ja järeldame, et

$$[z_1] = [z_2] \iff \operatorname{Re} z_1 \equiv \operatorname{Re} z_2 \text{ \& } \operatorname{Im} z_1 \equiv \operatorname{Im} z_2 \pmod{3}.$$

Kokkuvõttes näeme, et $G/\langle 3 \rangle \cong \mathbb{Z}_3 + i\mathbb{Z}_3$. □

Ülesanne III.8. Olgu $I = \langle X, 2 \rangle$ polünoomide X ja 2 poolt tekitatud ideaal ringis $\mathbb{Z}[X]$. Tõestage, et

1. I koosneb kõigist paarisarvulise vabaliikmega polünoomidest;
2. faktoring $\mathbb{Z}[X]/I$ on isomorfne jäägiklassikorpusega $\mathbb{Z}_2$.

Lahendus:

1. Vaatleme ringi $\mathbb{Z}[X]$. Vastavalt (universaal)algebra lineaarkatte definitsioonile kirjutame

$$\langle X, 2 \rangle = \{Xf + 2g \mid f, g \in \mathbb{Z}[X]\}.$$

Vaatleme suvalist elementi $Xf + 2g \in \langle X, 2 \rangle$. Ilmselt ei saa elemendi $Xf + 2g$ vabaliige sõltuda liidetavast Xf . Nagu näha, siis elemendi $Xf + 2g$ vabaliige on kujul $2g_0$, kus g_0 on polünoomi g vabaliige, ning $2g_0$ on ilmselt paarisarv. Olgu $z = z_n X^n + \dots + z_1 X + z_0 \in \mathbb{Z}[X]$ suvaline selline polünoom, kus z_0 on paarisarv, siis

$$z = X(z_n X^{n-1} + \dots + z_1) + 2 \frac{z_0}{2} \in \langle X, 2 \rangle.$$

Järelikult kuuluvad ideaali $\langle X, 2 \rangle$ parasjagu paarisarvulise vabaliikmega polünoomid.

2. Vaatleme faktoringi $\mathbb{Z}[X]/I$. Olgu $f, g \in \mathbb{Z}[X]$, siis

$$[f] = [g] \iff f - g \in \langle X, 2 \rangle.$$

Tingimus $f - g \in \langle X, 2 \rangle$ on samaväärne sellega, et polünoomi $f - g$ vabaliige on paarisarv, kusjuures polünoomi $f - g$ vabaliige avaldub $f_0 - g_0$, kus f_0 on polünoomi f vabaliige ja g_0 on polünoomi g vabaliige. Järelikult kehtib $[f] = [g]$ parajasti siis, kui $f_0 - g_0$ on paarisarv. Vahe $f_0 - g_0$ on paarisarv parajasti siis, kui arvud f_0 ja g_0 on mõlemad korraga kas paarisarvud või paaritud arvud. Järelikult kehtib

$$\mathbb{Z}[X]/\langle X, 2 \rangle = \left\{ \left\{ \sum_{k=0}^n g_k X^k \middle| g_0 \equiv 1 \pmod{2} \right\}, \left\{ \sum_{k=0}^n g_k X^k \middle| g_0 \equiv 0 \pmod{2} \right\} \right\}.$$

Defineerime kujutuse

$$\iota: \mathbb{Z}[X]/\langle X, 2 \rangle \rightarrow \mathbb{Z}_2, \quad \iota([g]) = g_0 \pmod{2}, \quad (g \in \mathbb{Z}[X]).$$

Lihtne on kontrollida, et ι on isomorfism. □

Ülesanne III.9. Olgu $\langle n \rangle$ naturaalarvu $n > 1$ poolt tekitatud peaideaal ringis $\mathbb{Z}[X]$. Tõestada, et faktoring $\mathbb{Z}[X]/\langle n \rangle$ on isomorfne ringiga $\mathbb{Z}_n[X]$.

Lahendus: Olgu $n > 1$ naturaalarv. Vaatleme arvu n poolt tekitatud peaideaali ringis $\mathbb{Z}[X]$

$$\langle n \rangle = n\mathbb{Z}[X] = \left\{ \sum_{k=0}^{k^*} na_k X^k \mid k^* \in \mathbb{N}, a_k \in \mathbb{Z} \right\}.$$

Taaskord uurime, millal kaks ekvivalentsiklassi $[f], [g] \in \mathbb{Z}[X]/\langle n \rangle$ on võrdsed:

$$[f] = [g] \iff f - g = \sum_{k=0}^{\max\{k_f, k_g\}} (f_k - g_k) X^k \in \langle n \rangle,$$

kus $f = \sum_{k=0}^{k_f} f_k X^k$ ja $g = \sum_{k=0}^{k_g} g_k X^k$ (kummaski polünoomis loeme puuduvad kordajad võrdseks nulliga). Analoogiliselt ülesandega III.7 saame, et $[f] = [g]$ kehtib parajasti siis kui iga indeksi k korral kehtib $n \mid f_k - g_k$. Siit saame tingimuse

$$[f] = [g] \iff \forall k \in \{0, \dots, \max\{k_f, k_g\}\}: \quad f_k - g_k \equiv 0 \pmod{n},$$

mistõttu $\mathbb{Z}[X]/\langle n \rangle \cong \mathbb{Z}_n[X]$. □

Ülesanne III.10. Tõestada, et korpuse K ainsad ideaalid on $\{0\}$ ja K .

Lahendus: Olgu K korpus ja H tema selline ideaal, et $\{0\} \subset H$. Olgu $k \in K$ suvaline. Võtame elementi $h \in H$ nii, et $h \neq 0$. Kuna K on korpus, leidub pöördelement $h^{-1} \in K$ ning $kh^{-1} \in K$. Kuna ideaal on suvalise skalaariga² korrutamise suhtes kinnine, saame

$$(kh^{-1})h = k(h^{-1}h) = k \in H.$$

Kuna k oli suvaline, siis saame võrduse $H = K$. □

Ülesanne* III.11. Olgu I kommutatiivse ringi R ideaal. Tõestada, et faktoring R/I on igal juhul kommutatiivne ja omab ühikelementi parajasti siis, kui leidub element $e \in R$ selliselt, et $er - r \in I$ iga $r \in R$ korral.

²Korpuse elemente nimetatakse vahel *skalaarideks*.

Praktikum IV Otsekorrutised ja otsesummad

Ülesanne IV.1. Tõestada, et kompleksarvude multiplikatiivne rühm $(\mathbb{C} \setminus \{0\}, \cdot)$ on positiivsete reaalarvude alamrühma $(\mathbb{R}^+, \cdot)$ ja alamrühma $U = \{z \in \mathbb{C} \mid |z| = 1\}$ otsekorrutis.

Lahendus: Kõigepealt meenutame, kuidas rühmas $(U, \cdot)$ toimub korrutamine. Olgu $z \in U$, saame selle esitada eksponentkujul $z = e^{i\theta}$, kus $\theta := \arg z$. Teadupoolest käib rühmas U korrutamine vastavalt valemile

$$z_1 z_2 = e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1 + \theta_2)}, \quad (z_1 = e^{i\theta_1}, z_2 = e^{i\theta_2} \in U).$$

Vaatleme nüüd otsekorrutist $\mathbb{R}^+ \times U$. Vastavalt otsekorrutise definitsioonile kehtib

$$(r_1, e^{i\theta_1}) \cdot (r_2, e^{i\theta_2}) = (r_1 r_2, e^{i\theta_1} e^{i\theta_2}) = (r_1 r_2, e^{i(\theta_1 + \theta_2)}), \quad (r_1, r_2 \in \mathbb{R}^+; e^{i\theta_1}, e^{i\theta_2} \in U).$$

Kui tähistada $(r, e^{i\theta}) =: re^{i\theta}$, siis oleme saanud vastavalt eelnevale reale täpselt nullist erinevate kompleksarvude korrutamise eksponentkujul, mistõttu kehtib $\mathbb{R}^+ \times U \cong \mathbb{C} \setminus \{0\}$. Kusjuures esimene otsekorrutise tegur $\mathbb{R}^+$ annab kompleksarvu mooduli ja teine tegur U annab sisuliselt kompleksarvu argumenti. $\square$

Märkus 2. Kui lubada eelmise ülesande otsekorrutise esimesse tegurisse ka reaalarvu 0 ning faktoriiseerides selliselt, et kõik mooduliga 0 olevad kompleksarvud on võrdsed, saame kogu kompleksarvude multiplikatiivse poolrühma $(\mathbb{C}, \cdot)$.

Vastavalt loengukonspekti [1] näitele 1.74, saab igat Abeli rühma vaadelda moodulina üle täisarvude ringi $\mathbb{Z}$. Seega saame rääkida ka Abeli rühmade otsesummast, kuigi loengukonspektis on see defineeritud vaid moodulite korral.

Ülesanne IV.2. Olgu B Abeli rühma A alamrühm. Tõestada, et selline alamrühm $C \leq A$, et $A = B \dot{+} C$, leidub parajasti siis, kui saab leida niisuguse homomorfismi $f: A \rightarrow B$, et $f(x) = x$ iga $x \in B$ korral.

Lahendus: Olgu A Abeli rühm ja $B \leq A$ alamrühm.

($\implies$) Leidugu alamrühm $C \leq A$ nii, et $A = B \dot{+} C$. Sel juhul leiduvad iga $a \in A$ korral üheselt määratud elemendid $b_a \in B$ ja $c_a \in C$ nii, et $a = b_a + c_a$. Defineerime kujutuse $f: A \rightarrow B$, $f(a) = f(b_a + c_a) := b_a$. Ilmselt iga $b \in B$ korral kehtib $b = b + 0$, seega $f(b) = b$ nagu tahetud. Olgu $a_1 = b_1 + c_1, a_2 = b_2 + c_2 \in A$, siis

$$\begin{aligned} f(a_1 + a_2) &= f((b_1 + c_1) + (b_2 + c_2)) = f((b_1 + b_2) + (c_1 + c_2)) = b_1 + b_2 = \\ &= f(b_1 + c_1) + f(b_2 + c_2) = f(a_1) + f(a_2). \end{aligned}$$

Järelikult on f homomorfism, mis rahuldab ülesande tingimusi.

($\impliedby$) Leidugu homomorfism $f: A \rightarrow B$ selline, et $f|_B(b) = b$, iga $b \in B$ korral. Sel juhul kehtib iga $a \in A$ korral $(f \circ f)(a) = f(f(a)) = f(a)$, kuna $f(a) \in B$. Tähistame hulga

$$C := \{c \in A \mid \exists a \in A: c = a - f(a)\}.$$

On selge, et kui $c_1, c_2 \in C$, siis leiduvad $a_1, a_2 \in A$ nii, et $c_1 = a_1 - f(a_1)$ ja $c_2 = a_2 - f(a_2)$. Paneme tähele, et

$$c_1 + c_2 = (a_1 - f(a_1)) + (a_2 - f(a_2)) = (a_1 + a_2) - (f(a_1) + f(a_2)) = (a_1 + a_2) - f(a_1 + a_2) \in C,$$

seega C alamrühm. Lisaks kehtib tingimus

$$f(c_1) = f(a_1 - f(a_1)) = f(a_1) - f(f(a_1)) = f(a_1) - f(a_1) = 0,$$

mistõttu $f(C) = \{0\}$.

Vaatleme summat $B + C$. Olgu $a \in A$, siis kehtib

$$a = a + f(a) - f(a) = f(a) + (a - f(a)) \in B + C,$$

järelikult kehtib $A = B + C$.

Olgu $a \in A$ ja kehtigu $a = b + c$, kus $b \in B$ ja $c \in C$. Peame näitama, et see esitus on ühene. Oletame vastuväiteliselt, et leiduvad veel elemendid $b_1 \in B$ ja $c_1 \in C$ nii, et $b_1 \neq b$, $c_1 \neq c$ ja $a = b_1 + c_1$. Paneme tähele, et

$$\begin{aligned} 0 &= f(0) = f(a - a) = f((b + c) - (b_1 + c_1)) = f((b - b_1) + (c - c_1)) = \\ &= f(b - b_1) + f(c - c_1) = b - b_1 + 0 = b - b_1, \end{aligned}$$

järelikult $b = b_1$. Seega $c = a - b = a - b_1 = c_1$. $\nmid$

Kokkuvõttes on esitus $a = b + c$ ühene, mistõttu $A = B + C$. $\square$

Kui R on ring, siis iga tema ideaal on – vastavalt definitsioonile – kinnine mõlemalt poolt ringi R elementidega korrutamise suhtes. Seega võib iga ideaali $I \trianglelefteq R$ vaadelda kui vasak- (või ka parempoolset) moodulit üle ringi R . Seetõttu võime rääkida ringi ideaalide otsesummast.

Ülesanne IV.3. Olgu R kommutatiivne ring, I , I_1 ja I_2 selle ideaalid. Tõestada, et kui $I = I_1 + I_2$, siis $I_1 I_2 = \{kh \mid k \in I_1, h \in I_2\} = \{0\}$.

Lahendus: Kehtigu ülesande eeldused ja $I = I_1 + I_2$. Kuna I_1 ja I_2 on ideaalid, on nad ringi R elementidega korrutamise suhtes kinnised. Olgu $k \in I_1$ ja $h \in I_2$, siis kehtivad

$$\begin{aligned} kh \in I_1 &\iff h \in I_2 \subseteq R, \\ kh \in I_2 &\iff k \in I_1 \subseteq R, \end{aligned}$$

seega $kh \in I_1 \cap I_2$, mistõttu $I_1 I_2 \subseteq I_1 \cap I_2$. Kuna ideaalid I_1 ja I_2 moodustavad otsesumma, siis, vastavalt loengukonspekti [1] teoreemile 1.81, teame, et $I_1 \cap I_2 = \{0\}$ ja järelikult ka $I_1 I_2 = \{0\}$. $\square$

Ülesanne IV.4. Esitada järgmised ringid pärisideaalide otsesummana (kui võimalik): a) $\mathbb{Z}_{10}$, b) $\mathbb{Z}_{12}$, c) $\mathbb{Z}$.

Lahendus:

- a) Vaatleme ringi $\mathbb{Z}_{10}$. Paneme tähele, et hulgad $2\mathbb{Z}_{10} = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ ja $5\mathbb{Z}_{10} = \{\bar{0}, \bar{5}\}$ on ringi $\mathbb{Z}_{10}$ pärisideaalid ning iga element ringist $\mathbb{Z}_{10}$ avaldub ideaalide $2\mathbb{Z}_{10}$ ja $5\mathbb{Z}_{10}$ elementide summana. Kuna $2\mathbb{Z}_{10} \cap 5\mathbb{Z}_{10} = \{\bar{0}\}$, siis kehtib $\mathbb{Z}_{10} = 2\mathbb{Z}_{10} \dot{+} 5\mathbb{Z}_{10}$.
- b) Vaatleme ringi $\mathbb{Z}_{12}$. Analoogiliselt ülesandega eelmise osaga saame võrduse $\mathbb{Z}_{12} = 3\mathbb{Z}_{12} \dot{+} 4\mathbb{Z}_{12}$, kus $3\mathbb{Z}_{12} = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$ ja $4\mathbb{Z}_{12} = \{\bar{0}, \bar{4}, \bar{8}\}$.
- c) Esimesest praktikumist teame, et ringi $\mathbb{Z}$ kõik aditiivsed alamrühmad peavad olema kujul $n\mathbb{Z}$, kus $n \in \mathbb{N}$. Oletame, et leiduvad ideaalid $n\mathbb{Z}$ ja $m\mathbb{Z}$ nii, et nende otsesumma on $\mathbb{Z}$. Siis peab nende ideaalide ühisosa olema $\{0\}$, see aga on võimatu kuna $V\ddot{U}K(n, m) \in n\mathbb{Z} \cap m\mathbb{Z}$. $\square$

Ülesanne IV.5. Tõestada, et n -mõõtmelise vektorruumi V iga alamruumi L_1 jaoks leidub täiend, s.t. selline alamruum L_2 , et $V = L_1 \dot{+} L_2$. Kas selline alamruum L_2 on üheselt määratud?

Lahendus: Olgu V vektorruum, $n = \dim V$ ja $L_1 \subseteq V$ alamruum. Olgu $\mathcal{B}_1 := \{\epsilon_1, \dots, \epsilon_k\}$, kus $k \leq n$ mingi ruumi L_1 baas. Täiendame selle ruumi V baasiks $\mathcal{B} := \{\epsilon_1, \dots, \epsilon_k, \epsilon'_{k+1}, \dots, \epsilon'_n\}$. (Seda saab alati teha, valides baasi eelnevatega lineaarselt sõltumatuid vektoreid.) Tähistame $L_2 := \text{span}(\epsilon'_{k+1}, \dots, \epsilon'_n)$, siis on ruumi L_2 baasiks $\mathcal{B}_2 := \{\epsilon'_{k+1}, \dots, \epsilon'_n\}$. Suvalise vektori $v \in V$ saame esitada baasis $\mathcal{B}$

$$v = (b_1\epsilon_1 + \dots + b_k\epsilon_k) + (b_{k+1}\epsilon'_{k+1} + \dots + b_n\epsilon'_n) \in L_1 + L_2.$$

Seega $V = L_1 + L_2$.

Nüüd olgu $w \in L_1 \cap L_2$, siis $w = (\beta_1, \dots, \beta_k)_{\mathcal{B}_1} = (\beta'_{k+1}, \dots, \beta'_n)_{\mathcal{B}_2}$. Järelikult

$$0 = w - w = \beta_1\epsilon_1 + \dots + \beta_k\epsilon_k + (-\beta'_{k+1})\epsilon'_{k+1} + \dots + (-\beta'_n)\epsilon'_n.$$

Kuna vektorid $\epsilon_1, \dots, \epsilon_k, \epsilon'_{k+1}, \dots, \epsilon'_n$ on kõik lineaarselt sõltumatud, siis $\beta_1 = \dots = \beta_k = -\beta'_{k+1} = \dots = -\beta'_n = 0$, mistõttu $w = 0$. Seega $L_1 \cap L_2 = \{0\}$ ja summa $L_1 + L_2$ on otsesumma.

Alamruumi L_1 täiend L_2 ei ole üheselt määratud, kuna ruumi L_1 baasi on mitmel viisil võimalik täiendada ruumi V baasiks. $\square$

Ülesanne IV.6. Olgu U ja W vektorruumi V alamruumid ja $U \cap W = \{0\}$. Tõestada, et $(U \dot{+} W)/W \cong U$.

Lahendus: Olgu V vektorruum üle korpuse K ja U, W alamruumid, mille korral $U \cap W = \{0\}$. Sel juhul saame konstrueerida otsesumma $U \dot{+} W$. Vaatleme faktorruumi $(U \dot{+} W)/W$. Selle ruumi suvaline element $[u + w] \in (U \dot{+} W)/W$ avaldub kujul

$$[u + w] = (u + w) + W = \{u + w + w_1 \mid w_1 \in W\}.$$

Urime, millal on elemendid $[u_1 + w_1], [u_2 + w_2] \in (U \dot{+} W)/W$ erinevad. Selleks paneme tähele, et

$$[u_1 + w_1] = [u_2 + w_2] \iff (u_1 + w_1) - (u_2 + w_2) = (u_1 - u_2) + (w_1 - w_2) \in W.$$

Kuna $w_1 - w_2 \in W$ kehtib alati, siis peab elementide $[u_1 + w_1]$ ja $[u_2 + w_2]$ võrdsuseks kehtima $u_1 - u_2 \in W$. Kuna aga ilmselt $u_1 - u_2 \in U$ ja $U \cap W = \{0\}$, siis $u_1 - u_2 = 0$ ehk $u_1 = u_2$. Seega elemendid $[u_1 + w_1]$ ja $[u_2 + w_2]$ on võrdsed parajasti siis, kui $u_1 = u_2$.

Defineerime kujutuse $\iota: (U \dot{+} W)/W \rightarrow U$, $[u + w] \mapsto u$. Võtame suvalised $k \in K$ ja $[u + w], [u_1 + w_1], [u_2 + w_2] \in (U \dot{+} W)/W$, siis

$$\begin{aligned}\iota(k[u + w]) &= \iota([ku + kw]) = ku = k\iota([u + w]), \\ \iota([u_1 + w_1] + [u_2 + w_2]) &= \iota([(u_1 + u_2) + (w_1 + w_2)]) = u_1 + u_2 = \\ &= \iota([u_1 + w_1]) + \iota([u_2 + w_2]).\end{aligned}$$

Seega on ι lineaarteisendus (ehk vektorruumide homomorfism). Võtame $u \in U$, siis $u = u + 0 = \iota([u + 0])$, mistõttu ι on sürjektiivne. Viimaseks võtame erinevad $[u_1 + w_1], [u_2 + w_2] \in (U \dot{+} W)/W$, siis vastavalt võrdsuse tingimusele faktorruumis $(U \dot{+} W)/W$ saame, et

$$\iota([u_1 + w_1]) = u_1 \neq u_2 = \iota([u_1 + w_2]),$$

mistõttu ι on injektiivne. Kokkuvõttes oleme saanud, et ι on vektorruumide isomorfism. $\square$

Ülesanne IV.7. Tõestada, et vektorruum $\mathbb{R}^n$ on alamruumide

$$\begin{aligned}L_1 &:= \{(a_1, a_2, \dots, a_n) \mid a_1 + a_2 + \dots + a_n = 0\}, \\ L_2 &:= \{(a_1, a_2, \dots, a_n) \mid a_1 = a_2 = \dots = a_n\}\end{aligned}$$

otsesumma.

Lahendus: Paneme tähele, et kuna $L_2 = \{(a, \dots, a) \mid a \in \mathbb{R}\}$, siis $\dim L_2 = 1$ (baasiks sobib $\{(1, 1, \dots, 1)\}$); ning

$$L_1 = \left\{ \left(a_1, \dots, a_{n-1}, -\sum_{k=1}^{n-1} a_k \right) \mid a_1, \dots, a_{n-1} \in \mathbb{R} \right\},$$

siis $\dim L_1 = n - 1$ (baasiks sobib $\{(1, 0, \dots, 0, -1), \dots, (0, 0, \dots, 1, -1)\}$). Siit saame, et

$$\dim L_1 + \dim L_2 = (n - 1) + 1 = n = \dim V.$$

Vaatleme ühisosa $L_1 \cap L_2$. Olgu $v \in L_1 \cap L_2$, siis leidub $a \in \mathbb{R}$ nii, et $v = (a, \dots, a)$. Teisest küljest $a + \dots + a = na = 0$, mistõttu $a = 0$ ja ka $v = 0$. Seega $L_1 \cap L_2 = \{0\}$ ja tänu teoreemile 1.86 saame, et $L_1 + L_2$ on otsesumma.

Tänu järeldusele 1.92 saame, et $\dim(L_1 \dot{+} L_2) = \dim L_1 + \dim L_2 = n$. Kuna V on ainus alamruum, mille dimensioon on n , saamegi siit, et $L_1 \dot{+} L_2 = V$. $\square$

Ülesanne IV.8. Tõestada, et n -mõõtmelise vektorruum on ühemõõtmeliste alamruumide $\langle a_1 \rangle, \langle a_2 \rangle, \dots, \langle a_n \rangle$ otsesumma, kus $a_1, a_2, \dots, a_n$ on selle vektorruumi mistahes baas.

Lahendus: Olgu V lõplikumõõtmeline vektorruum üle korpuse K ($\dim V =: n$) ja $\{a_1, \dots, a_n\}$ selle vektorruumi baas. Vaatleme alamruume

$$\langle a_h \rangle = \text{span}(a_h) = \{\kappa a_h \mid \kappa \in K\}, \quad (\text{ilmselt } \dim \langle a_h \rangle = 1),$$

kus $h \in \{1, \dots, n\}$. Olgu $v \in \langle a_1 \rangle \cap \sum_{h=2}^n \langle a_h \rangle$, siis $v = \kappa_1 a_1 = \sum_{h=2}^n \kappa_h a_h$, mistõttu

$$0 = v - v = (\kappa_2 a_2 + \dots + \kappa_n a_n) - \kappa_1 a_1.$$

Kuna $a_1, \dots, a_n$ on lineaarselt sõltumatud, siis saame, et $\kappa_1 = \kappa_2 = \dots = \kappa_n = 0$, mistõttu $v = 0$. Kuna $\langle a_1 \rangle \cap \sum_{h=2}^n \langle a_h \rangle = \{0\}$, siis summa $\sum_{h=1}^n \langle a_h \rangle$ on otsesumma. Tänu teoreemile 1.93 saame, et

$$\dim(\langle a_1 \rangle + \dots + \langle a_n \rangle) = \sum_{h=1}^n \dim \langle a_h \rangle = n.$$

Taaskord saime, et meie otsesumma dimensioon on n ja V ise on ainus selline alamruum, mistõttu saame $V = \langle a_1 \rangle + \dots + \langle a_n \rangle$. $\square$

Nimetame vektorruumi V lineaarteisenduse $P: V \rightarrow V$ projektoriks, kui kehtib $P \circ P = P$.

Ülesanne* IV.9. Olgu $P_i: V \rightarrow V$ lõplikumõõtmelise vektorruumi V projektorid, kus $i = 1, \dots, n$. Tõestada, et kui $P_i \circ P_j = 0$ iga $i \neq j$ korral, siis $V = \text{Im}(P_1) + \dots + \text{Im}(P_n) + \bigcap_{i=1}^n \text{Ker}(P_i)$. Näidata, et kehtib ka “vastupidine”, st kui $\sum_{i=1}^n P_i = 1_V$, siis $P_i \circ P_j = 0$ iga $i \neq j$ korral ja $V = \text{Im}(P_1) + \dots + \text{Im}(P_n)$.

Ülesanne lõpmatust otsekorruitisest ja otsesummast

Järgmine ülesanne tundus mulle esialgu pealevaadates triviaalne ja seepärast ma ta ka siia lisasin. Siiski juhtis tudeng U. Luhaäär minu tähelepanu asjaolule, et see pole nii lihtne kui alguses tundus. Siinkohal esitan selle ülesande täieliku lahenduse, kuid võite arvestada, et see tegelikult on selle aine mastaabist väljas. Üldse ei vaatle me siin aines eriti lõpmatumõõtmelisi vektorruume. Kõigepealt mõned märkused selle ülesande kohta.

Otsekorruitisse $\prod_{i=1}^{\infty} \mathbb{C}$ kuuluvad kõikvõimalikud kompleksarvuliste liikmetega jadad (seega tähistame $\prod_{i=1}^{\infty} \mathbb{C} = \mathbb{C}^{\mathbb{N}} = \{f: \mathbb{N} \rightarrow \mathbb{C}\}$). Väline otsesumma $\oplus \sum_{i=1}^{\infty} \mathbb{C}$ on aga jadaruumi $\mathbb{C}^{\mathbb{N}}$ alamruum, kuhu kuuluvad vaid sellised jadad, kus on lõplik arv nullist erinevaid liikmeid, seetõttu $\oplus \sum_{i=1}^{\infty} \mathbb{C} \subset \prod_{i=1}^{\infty} \mathbb{C}$.

Ülesande lahendamiseks kasutan Erdős–Kaplansky teoreemi. Selle teoreemi tõestus väljub selle aine raamidest. (See nõuab päris tõsiselt teadmisi hulgateooriast.) Tõestuse idee võib leida raamatust [4], peatükk 2 §7 ülesanne 3. Tähistame sümboliga $\#(A)$ hulga A võimsust.

TEOREEM 1 (Erdős–Kaplansky). *Olgu K korpus ja I mingi mingi lõpmatu hulk, siis kehtib*

$$\dim_K(K^I) = \#(K)^{\#(I)}. \quad (2)$$

Lisaks on meil vaja ka järgmist teoreemi, mille tõestus lõpmatul juhul kasutab Zorni lemmat. Aines “Sissejuhatus algebra struktuuridesse” vaadeldakse natuke taolisi teemasid, s.h. tõestatakse ära, et igas vektorruumis on baas. Võimsuste (kardinaalarvudega) tegeletakse aines “Matemaatika alused”.

TEOREEM 2. *Vektorruumi V iga baas on sama võimsusega.*

Ülesanne* IV.10.** Tõestada, et $\mathbb{C}$ kui vektorruumi üle iseenda loenduv väline otsesumma $\oplus \sum_{h=1}^{\infty} \mathbb{C}$ ei ole isomorfne otsekorruitisega $\prod_{h=1}^{\infty} \mathbb{C}$.

Lahendus: Näitamaks, et need vektorruumid ei ole isomorfsed, vaatleme nende baase. Otse-summa $\oplus \sum_{h=1}^{\infty} \mathbb{C}$ baasiks sobib hulk

$$\mathcal{B} := \{(1, 0, 0, \dots), (0, 1, 0, \dots), (0, 0, 1, \dots), \dots\}.$$

Kuna iga otse-summa $\oplus \sum_{h=1}^{\infty} \mathbb{C}$ element avaldub lõpliku summana hulga $\mathcal{B}$ elementidest. Märkame ka, et hulga $\mathcal{B}$ võimsus on loenduv ehk

$$\dim_{\mathbb{C}} \left(\oplus \sum_{h=1}^{\infty} \mathbb{C} \right) = \aleph_0.$$

Teisest küljest, kasutades Erdős–Kaplinsky teoreemi, saame

$$\dim_{\mathbb{C}} \left(\prod_{h=1}^{\infty} \mathbb{C} \right) = \dim_{\mathbb{C}} (\mathbb{C}^{\mathbb{N}}) = \#(\mathbb{C})^{\#(\mathbb{N})} = \mathfrak{c}^{\aleph_0} \geq \mathfrak{c} > \aleph_0,$$

kus $\mathfrak{c}$ tähistab kontiiniumi võimsust. Kuna nende vektorruumide dimensioonid on erinevad, siis ei saa need vektorruumid isomorfsed olla tänu teoreemile 2. $\square$

Lõpetuseks teen ühe märkuse lõpmatumõõtmeliste vektorruumide kohta.

Märkus 3. Lõpmatumõõtmeline vektorruum V võib olla isomorfne oma pärisalamruumiga. Olgu K korpus, vaatleme jadaruumi $K^{\mathbb{N}} = \prod_{h=1}^{\infty} K$ komponenthaval defineeritud tehetega. Kujutus

$$\iota: K^{\mathbb{N}} \rightarrow \{0\} \times K^{\mathbb{N}}, \quad (a_1, a_2, \dots) \mapsto (0, a_1, a_2, \dots)$$

on ilmselt isomorfism. Kuid hulk

$$\{0\} \times K^{\mathbb{N}} = \{(0, a_1, a_2, \dots) \mid a_1, a_2, \dots \in K\}$$

on selgelt vektorruumi $K^{\mathbb{N}}$ pärisalamruum, kuna koosneb kõigist jadadest, mille esimene liige on 0.

Praktikum V Mitme muutuja polünoomid. Sümmeetrilised polünoomid

Mitme muutuja polünoomi f *pealiikmeks* nimetame tema liiget m_f , mille korral iga teise liikme m korral $\deg(m_f) \geq \deg(m)$ ja $m_f \geq_{\text{lex}} m$. Ilmselt on selline pealiige üheselt määratud.

Üksliikmeid nimetatakse ka *monoomideks*. Ma vahel kasutan seda terminit.

Ülesanne V.1. Jagada polünoom $f = X^7Y^2 + X^3Y^2 - Y + 1$ jäägiga polünoomide paariga $g_1 = XY^2 - X$, $g_2 = X - Y^3$. Jäägiga jagamine tähendab selliste polünoomide q_1 , q_2 ja r leidmist, et

$$f = q_1g_1 + q_2g_2 + r,$$

kus kas $r = 0$ või r on üksliikmete “lineaarkombinatsioon” ja g_i pealiikmed ei jaga ühtegi neist üksliikmetest.

Lahendus: Kõigepealt jagame polünoomi f polünoomiga g_1 . Selleks paneme tähele, et $g_1 = X(Y^2 - 1)$, jagame nende teguritega eraldi.

$$\begin{array}{r} X^7Y^2 + X^3Y^2 - Y + 1 \quad | X^6Y^2 + X^2Y^2 \\ \hline X^7Y^2 \quad \quad \quad \quad \quad | X \\ \hline X^3Y^2 - Y + 1 \\ \hline X^3Y^2 \quad \quad \quad \quad \quad \\ \hline -Y + 1 \end{array}$$

Seega oleme saanud jagatise $f = X(X^6Y^2 + X^2Y^2) + (-Y + 1)$. Nüüd jagame saadud jagatise läbi ka polünoomi g_1 teise teguriga.

$$\begin{array}{r} X^6Y^2 + X^2Y^2 \quad \quad \quad | X^6 + X^2 \\ \hline X^6Y^2 \quad \quad \quad -X^6 \quad | Y^2 - 1 \\ \hline X^2Y^2 + X^6 \\ \hline X^2Y^2 \quad \quad \quad -X^2 \\ \hline X^6 + X^2 \end{array}$$

Nüüd saame esitada polünoomi f järgnevalt:

$$f = X((Y^2 - 1)(X^6 + X^2) + (X^6 + X^2)) + (1 - Y) = (X^6 + X^2)g_1 + (X^7 + X^3 - Y + 1).$$

Jagame eelmise esituse jääki polünoomiga g_2 . Kuna see jagamine tuli päris pikk, siis see on ära toodud lahenduste lõpus eraldi leheküljel. Kokkuvõttes oleme saanud, et polünoom f avaldub kujul

$$\begin{aligned} f = & (X^6 + X^2)g_1 + \\ & + (X^6 + X^5Y^3 + X^4Y^6 + X^3Y^9 + X^2 + X^2Y^{12} + XY^3 + XY^{15} + Y^6 + Y^{18})g_2 + \\ & + (-Y + 1 + Y^9 + Y^{21}) \end{aligned}$$

Nagu näha, siis ükski “jäägi” liikmetest $-Y$, 1 , Y^9 ja Y^{21} ei jagu jagajate g_1 ja g_2 “leksikograafiliste” pealiikmetega XY^2 ja X . □

Mainin, et üldjuhul ei ole väga levinud defineerida mitme muutuja polünoomide jagamist, kuid nii illustratsiooniks mitme muutuja polünoomide erinevate rakenduste ja võimaluste kohta, sai eelmine ülesanne siia pandud. Järgmine ülesanne näitab, et taoline mitme muutuja polünoomide jagamise algoritm on vägagi sõltuv pealiikme definitsioonist.

Ülesanne V.2. Lahendada uuesti eelmine ülesanne:

1. vahetades ära g_1 ja g_2 järjekorra;
2. kasutades “pealiikme” definitsioonis leksikograafilise asemel “kõrgeima astme leksikograafilist” järjestust, nt $Y^2Z < X^3 < Y^2Z^2 < XY^3$.

Lahendus:

1. Vahetades polünoomide g_1 ja g_2 järjekorra, saame teistsuguse tulemuse. Jagamise protseduuri ennast pole siinkohal ära toonud. Jagades polünoomi f polünoomiga $g_2 = X - Y^3$, saame

$$f = (X^6Y^2 + X^5Y^5 + X^4Y^8 + X^3Y^{11} + X^2Y^2(1 + Y^{12}) + XY^5(1 + Y^{12}) + Y^8(1 + Y^{12}))g_2 + Y^{11}(1 + Y^{12}) - Y + 1.$$

Kuna polünoomi $Y^{11}(1 + Y^{12}) - Y + 1$ ei saa jagada enam polünoomiga $g_1 = XY^2 - X$, siis edasi enam “jagada” ei saa. Asjaolu, et see algoritm on selliselt ebasümmeetriline, näitab ka selle jagamise algoritmi puudusi.

2. Viime nüüd 1. ülesande jagamised läbi uue järjestusega. Jagades polünoomi f polünoomiga g_1 , ei ole mingit erinevust, kuna ka uue järjestuse korral on polünoomi $g_1 = XY^2 - X$ pealiikmeks XY^2 . Kui aga proovida jagada polünoomiga $g_2 = X - Y^3$, siis tuleb pealiikmeks võtta Y^3 . Polünoom f aga ei jagu sel viisil polünoomiga g_2 , kuna monoom X^7Y^2 ei jagu monoomiga Y^3 .

□

Ülesanne V.3. Tõestada, et kui R on kommutatiivne ühikuga ring, siis

$$R[X_1, \dots, X_k][X_{k+1}, \dots, X_n] \cong R[X_1, \dots, X_n].$$

Lahendus: Teadupoolest

$$R[X_1, \dots, X_k][X_{k+1}, \dots, X_n] = \left\{ \sum_{h=0}^m f_h X_{k+1}^{h_{k+1}} \dots X_n^{h_n} \mid m \in \mathbb{N}; f_1, \dots, f_m \in R[X_1, \dots, X_k] \right\}.$$

Olgu $f = \sum_{h=1}^m f_h X_{k+1}^{h_{k+1}} \dots X_n^{h_n} \in R[X_1, \dots, X_k][X_{k+1}, \dots, X_n]$. Ilmselt saame iga indeksi $h \in \{0, \dots, m\}$ korral esitada $f_h = \sum_{j=0}^{m_h} r_{hj} X_1^{j_{h1}} \dots X_k^{j_{hk}}$. Nüüd

$$\begin{aligned} f &= \sum_{h=0}^m f_h X_{k+1}^{h_{k+1}} \dots X_n^{h_n} = \sum_{h=0}^m \left(\sum_{j=0}^{m_h} r_{hj} X_1^{j_{h1}} \dots X_k^{j_{hk}} \right) X_{k+1}^{h_{k+1}} \dots X_n^{h_n} = \\ &= \sum_{h=0}^m \sum_{j=0}^{m_h} r_{hj} X_1^{j_{h1}} \dots X_k^{j_{hk}} X_{k+1}^{h_{k+1}} \dots X_n^{h_n}. \end{aligned}$$

Nagu näha esitub f üksliikmete kujul $rX_1^{k_1} \dots X_n^{k_n}$ lõpliku summana, kus $r \in R$ ja $k_1, \dots, k_n \in \mathbb{N}_0$, seega $f \in R[X_1, \dots, X_n]$.

Teisalt võttes $g \in R[X_1, \dots, X_n]$, siis

$$g = \sum_{h=0}^m r_h X_1^{h_1} \dots X_n^{h_n} = \sum_{n=0}^m (r_h X_1^{h_1} \dots X_k^{h_k}) X_{k+1}^{h_{k+1}} \dots X_n^{h_n}.$$

Kuna üksliikmed $r_h X_1^{h_1} \dots X_k^{h_k} \in R[X_1, \dots, X_k]$, siis vastavalt polünoomide definitsioonile $g \in R[X_1, \dots, X_k][X_{k+1}, \dots, X_n]$. Seega oleme näidanud, et kuigi formaalselt on need hulgad erinevad, siis praktiliselt kehtib $R[X_1, \dots, X_k][X_{k+1}, \dots, X_n] = R[X_1, \dots, X_n]$. Ilmselt on nendes hulkades ka liitmine ja korrutamine kooskõlas, mistõttu on need ringid võrdsed. $\square$

Ülesanne V.4. Olgu $n \in \mathbb{N}$, R ja S ringid, $s_1, \dots, s_n \in S$ ning $f : R \rightarrow S$ ringide homomorfism. Tõestada, et $\text{eval} : R[X_1, \dots, X_n] \rightarrow S$ on ringide homomorfism, kui $\text{eval}(p) = (f(p))(s_1, \dots, s_n)$. Siin $f(p) \in S[X_1, \dots, X_n]$ on polünoom, mille kordajateks on vastavate p kordajate f -kujutised.

Lahendus: Vaatleme “väärtustamisfunktsiooni” $\text{eval} : R[X_1, \dots, X_n] \rightarrow S$. Esiteks kirjutame välja, mida see väärtustamisfunktsioon tegelikult teeb. Selleks võtame polünoomi

$g = \sum_{h=0}^m r_h X_1^{h_1} \dots X_n^{h_n} \in R[X_1, \dots, X_n]$, siis

$$\text{eval}(g) = \left(\sum_{h=0}^m f(r_h) X_1^{h_1} \dots X_n^{h_n} \right) \Big|_{(X_1, \dots, X_n) = (s_1, \dots, s_n)} = \sum_{h=0}^m f(r_h) s_1^{h_1} \dots s_n^{h_n}.$$

Nüüd olgu $g_1 = \sum_{h=0}^{m_1} r_{1h} X_1^{h_1} \dots X_n^{h_n}$, $g_2 = \sum_{k=0}^{m_2} r_{2k} X_1^{k_1} \dots X_n^{k_n} \in R[X_1, \dots, X_n]$. Nüüd

$$\begin{aligned} \text{eval}(g_1 + g_2) &= \text{eval} \left(\sum_{j=0}^{\max\{m_1, m_2\}} (r_{1j} + r_{2j}) X_1^{j_1} \dots X_n^{j_n} \right) = \sum_{j=0}^{\max\{m_1, m_2\}} f(r_{1j} + r_{2j}) s_1^{j_1} \dots s_n^{j_n} = \\ &= \sum_{j=0}^{\max\{m_1, m_2\}} (f(r_{1j}) s_1^{j_1} \dots s_n^{j_n} + f(r_{2j}) s_1^{j_1} \dots s_n^{j_n}) = \\ &= \sum_{j=0}^{m_1} f(r_{1j}) s_1^{j_1} \dots s_n^{j_n} + \sum_{j=0}^{m_2} f(r_{2j}) s_1^{j_1} \dots s_n^{j_n} = \text{eval}(g_1) + \text{eval}(g_2), \\ \text{eval}(g_1 g_2) &= \text{eval} \left(\sum_{q=0}^{m_1 \cdot m_2} \left(\sum_{j=0}^q r_{1j} r_{2, q-j} \right) X_1^{q_1} \dots X_n^{q_n} \right) = \\ &= \sum_{q=0}^{m_1 \cdot m_2} f \left(\sum_{j=0}^q r_{1j} r_{2, q-j} \right) s_1^{q_1} \dots s_n^{q_n} = \\ &= \sum_{q=0}^{m_1 \cdot m_2} \left(\sum_{j=0}^q f(r_{1j}) f(r_{2, q-j}) \right) s_1^{q_1} \dots s_n^{q_n} = \text{eval}(g_1) \text{eval}(g_2). \end{aligned}$$

Eelnevas olid puuduvad tegurid r_{zj} , $z \in \{1, 2\}$, asendatud nullidega. Sellega oleme näidanud, et eval on ringide homomorfism. $\square$

Tähistame sümboliga $\sigma_k = \sigma_k(x_1, \dots, x_n)$ k -astme n -astme sümmeetrilise põhipolünoomi.

Ülesanne V.5. Avaldada järgmised sümmeetrilised polünoomid sümmeetriliste põhipolünoomide kaudu:

1. $f(X, Y, Z) = X^3YZ + XY^3Z + XYZ^3$;
2. $f(X, Y, Z) = X^3 + Y^3 + Z^3$;
3. $f(X, Y, Z) = (X + Y)(X + Z)(Y + Z)$.

Lahendus: See ülesanne põhineb Sümmeetriliste polünoomide põhiteoreemil.

1. Vaatleme polünoomi $f(X, Y, Z) = X^3YZ + XY^3Z + XYZ^3$. Leksikograafilise järjestuse mõttes on selle polünoomi pealiige X^3YZ . Vastavalt algoritmile moodustame polünoomi

$$\begin{aligned} g_1 &= \sigma_1^2 \sigma_2^0 \sigma_3 = (X + Y + Z)^2 XYZ = (X^2 + 2XY + 2XZ + Y^2 + 2YZ + Z^2)XYZ = \\ &= X^3YZ + 2X^2Y^2Z + 2X^2Z^2Y + Y^3XZ + 2Y^2Z^2X + Z^3YX. \end{aligned}$$

Nüüd saame

$$f_1 = f - g_1 = -2X^2Y^2Z - 2X^2Z^2Y - 2Y^2Z^2X.$$

Polünoomi f_1 kõrgemi liige on $2X^2Y^2Z$, selle liikme abil moodustame uue polünoomi

$$g_2 = -2\sigma_1^0 \sigma_2 \sigma_3 = -2(XY + XZ + YZ)XYZ = -2X^2Y^2Z - 2X^2YZ^2 - 2XY^2Z^2.$$

Paneme tähele, et $f_1 - g_2 = 0$, mistõttu saamegi polünoomi f avaldada järgnevalt

$$\begin{aligned} f &= g_1 + g_2 = \sigma_1^2 \sigma_3 - 2\sigma_2 \sigma_3 = \\ &= (X^2 + 2XY + 2XZ + Y^2 + 2YZ + Z^2)XYZ - 2(XY + XZ + YZ)XYZ. \end{aligned}$$

2. Vaatleme polünoomi $f(X, Y, Z) = X^3 + Y^3 + Z^3$. Selle polünoomi leksikograafiline pealiige X^3 . Selle abil moodustame polünoomi

$$\begin{aligned} g_1 &= \sigma_1^3 = (X + Y + Z)^3 = \\ &= X^3 + Y^3 + Z^3 + 3X^2Y + 3XY^2 + 3X^2Z + 3XZ^2 + 3Y^2Z + 3YZ^2 + 6XYZ. \end{aligned}$$

Moodustame vahe

$$f_1 = f - g_1 = -3X^2Y - 3XY^2 - 3X^2Z - 3XZ^2 - 3Y^2Z - 3YZ^2 - 6XYZ.$$

Eelneva polünoomi pealiige on $-3X^2Y$, selle järgi moodustame polünoomi

$$\begin{aligned} g_2 &= -3\sigma_1 \sigma_2 = -3(X + Y + Z)(XY + XZ + YZ) = \\ &= -3X^2Y - 3XY^2 - 3X^2Z - 3XZ^2 - 3Y^2Z - 3YZ^2 - 9XYZ. \end{aligned}$$

Nüüd moodustame nendest vahe

$$f_2 = f_1 - g_2 = 3XYZ.$$

Paneme tähele, et $f_2 = g_3 = 3\sigma_3$. Seega saame kirjutada

$$\begin{aligned} f &= g_1 + g_2 + g_3 = \sigma_1^3 - 3\sigma_1 \sigma_2 + 3\sigma_3 = \\ &= (X + Y + Z)^3 - 3(X + Y + Z)(XY + XZ + YZ) + 3XYZ. \end{aligned}$$

3. Vaatleme polünoomi $f(X, Y, Z) = (X + Y)(X + Z)(Y + Z)$. Korrutame selle polünoomi lahti

$$f(X, Y, Z) = X^2Y + X^2Z + XY^2 + XZ^2 + Y^2Z + YZ^2 + 2XYZ.$$

Moodustame pealiikme X^2Y abil polünoomi

$$\begin{aligned} g_1 &= \sigma_1\sigma_2 = (X + Y + Z)(XY + XZ + YZ) = \\ &= X^2Y + XY^2 + X^2Z + XZ^2 + Y^2Z + YZ^2 + 3XYZ. \end{aligned}$$

Selle abil moodustame polünoomi

$$f_1 = f - g_1 = -XYZ = -\sigma_3 = g_2.$$

Nüüd saame avaldada esitada

$$f = g_1 + g_2 = \sigma_1\sigma_2 - \sigma_3 = (X + Y + Z)(XY + XZ + YZ) - XYZ,$$

mis on ka tahetud esitus sümmeetriliste põhipolünoomide kaudu.

□

Ülesanne V.6. Avaldada avaldis

$$Q = \frac{(X - Y)^2}{XY} + \frac{(X - Z)^2}{XZ} + \frac{(Y - Z)^2}{YZ}$$

sümmeetriliste põhipolünoomide kaudu.

Lahendus: Kõigepealt peame esitama antud avaldise kahe polünoomi jagatisega. (Meenutada ratsionaalmurdude ringi Algebra I ainest.) Arvutame

$$\frac{(X - Y)^{2(Z)}}{XY} + \frac{(X - Z)^{2(Y)}}{XZ} + \frac{(Y - Z)^{2(X)}}{YZ} = \frac{Z(X - Y)^2 + Y(X - Z)^2 + X(Y - Z)^2}{XYZ}.$$

Nüüd avaldame lugeja ja nimetaja eraldi sümmeetriliste põhipolünoomide abil. Märkame, et nimetaja on juba kujul $XYZ = \sigma_3$.

Vaatleme nüüd lugejat. Kehtib

$$Z(X - Y)^2 + Y(X - Z)^2 + X(Y - Z)^2 = X^2Y + XY^2 + X^2Z + XZ^2 + Y^2Z + YZ^2 - 6XYZ.$$

Eelneva polünoomi pealiige on X^2Y , tema kaudu saame polünoomi $g_1 = \sigma_1\sigma_2$. Siit näeme, et $f_1 = -9XYZ = -9\sigma_3$. Järelikult saame lugeja esitada kujul

$$\sigma_1\sigma_2 - 9\sigma_3 = (X + Y + Z)(XY + XZ + YZ) - 9XYZ.$$

Seega saame avaldise Q avaldada kujul

$$Q = \frac{\sigma_1\sigma_2 - 9\sigma_3}{\sigma_3} = \frac{(X + Y + Z)(XY + XZ + YZ) - 9XYZ}{XYZ},$$

mis on tahetud esitus sümmeetriliste põhipolünoomide abil.

□

Ülesanne* V.7. Tõestada, et iga $k = 1, \dots, n$ ja $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in (\mathbb{R}^+)^n$ korral

$$\sqrt[k]{\sigma_k(\mathbf{x} + \mathbf{y})} \geq \sqrt[k]{\sigma_k(\mathbf{x})} + \sqrt[k]{\sigma_k(\mathbf{y})}.$$

Praktikum VI Mitme muutuja polünoomid. Polünoomide Juured. Algebra põhiteoreem

Enne 1. ülesande juurde asumist meenutame Eukleidese ringi definitsiooni ja tõestame ühe lemma. Nulliteguriteta kommutatiivset ringi R nimetatakse *Eukleidese ringiks*, kui leidub kujutus

$$\delta: R \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$$

nii, et

1. $\forall a, b \in R \setminus \{0\}: \delta(ab) \geq \delta(a);$
2. $\forall a \in R \forall b \in R \setminus \{0\} \exists q, r \in R: a = bq + r \quad \& \quad (r = 0 \quad \vee \quad \delta(r) < \delta(b)).$

Lemma 1. *Eukleidese ringi iga ideaal on peaideaal.*

Tõestus. Olgu $(R; +, \cdot)$ Eukleidese ring ja $I \trianglelefteq R$ nullist erinev ideaal. Olgu $d \in I$ selline, et $d \neq 0$ ja $\delta(d)$ on hulga $\delta[I]$ minimaalne element (s.t. $\forall a \in I: \delta(d) \leq \delta(a)$; selline d kindlasti leidub). Kuna I on ideaal ja $d \in I$, siis kehtib $dR \subseteq I$.

Olgu $a \in I$. Kuna R on Eukleidese ring, siis leiduvad elemendid $q, r \in R$ nii, et

$$a = dq + r, \quad (r = 0 \quad \vee \quad \delta(r) < \delta(d)). \quad (3)$$

Esitame $r = a - dq$, kuna $a, d \in I$ ja ideaalina on I liitmise ja ringi R elemendiga korrutamise suhtes kinnine, siis $r \in I$. Kuna d norm on minimaalne, siis kehtib $\delta(d) \leq \delta(r)$. Arvestades tingimust (3) saame, et $r = 0$. Järelikult $a = dq$, mistõttu $a \in dR$. Seega $I \subseteq dR$.

Kokkuvõttes oleme saanud, et $I = dR$ ehk I on elemendi d järgi tekitatud peaideaal. ■

Ringi, mille kõik vasakpoolsed ja kõik parempoolsed ideaalid on peaideaalid, nimetatakse *pea-ideaalringiks* (*principal ideal ring*). Peaideaalringid on moodsas ringiteoorias üllatavalt olulised.

Ülesanne VI.1. Tõestada, et polünoomide ring $K[X, Y]$ üle korpuse K ei ole Eukleidese ring

Lahendus: Teame, et $K[X, Y]$ on kommutatiivne ring. Vaatleme ringi $K[X, Y]$ ideaali $\langle X, Y \rangle$. Kõigepealt paneme tähele, et hulk

$$A := \left\{ \sum_{k=1}^n a_k X^{k_1} Y^{k_2} \mid n \in \mathbb{N}_1, a_1, \dots, a_n \in K; \forall k: k_1 + k_2 > 1 \right\} \cup \{0\} \subset K[X, Y]$$

on ideaal ringis $K[X, Y]$ (hulgas $A \setminus \{0\}$ on polünoomid, mille aste on vähemalt 1 ja vabaliige puudub). Lisaks on selge, et $\langle X, Y \rangle \subseteq A$.

Oletame vastuväiteliselt, et ideaal $\langle X, Y \rangle$ on peaideaal, ehk leidub polünoom $g \in K[X, Y]$ nii, et $\langle X, Y \rangle = gK[X, Y]$. Järelikult leiduvad polünoomid $f_1, f_2 \in K[X, Y]$ nii, et $X = gf_1$ ja $Y = gf_2$. Siit aga järeldub, et $g = 1$. Ilmselt aga $\langle X, Y \rangle \subseteq A \subset K[X, Y]$, kuna näiteks konstantsed polünoomid ei kuulu ideaali A . Vastuolu tuli sellest, et eeldasime g eksisteerimist.

Kokkuvõttes ei ole $K[X, Y]$ peaideaalring ning lemma 1 tõttu pole ta ka Eukleidese ring. □

Ülesanne VI.2. Leidke $a \in \mathbb{R}$ nii, et polünoomi $X^3 + 12X^2 + a$ kahe juure summa oleks võrdne kolmandaga.

Lahendus: Tähistame polünoomi $X^3 + 12X^2 + a$ juured c_1 , c_2 ja $c_3 = c_1 + c_2$. Kasutades Viete'i valemeid saame võrrandite süsteemi

$$\begin{aligned} 12 &= -c_1 - c_2 - (c_1 + c_2) = -2c_1 - 2c_2 \implies -6 = c_1 + c_2 \text{ \& } c_1 = -6 - c_2, \\ 0 &= c_1c_2 + c_1(c_1 + c_2) + c_2(c_1 + c_2), \\ a &= -c_1c_2(c_1 + c_2). \end{aligned}$$

Teisest võrrandist saame

$$0 = (-6 - c_2)c_2 - 6(-6 - c_2) - 6c_2 \implies c_2^2 + 6c_2 - 36 = 0.$$

Seega $(c_1, c_2) \in \{(3(\sqrt{5}-1), -3(1+\sqrt{5})), (-3(1+\sqrt{5}), 3(\sqrt{5}-1))\}$. Nagu näha, erinevad eelnevad paarid ainult järjekorra poolest. Nüüd leiame

$$a = 6 \cdot (3(\sqrt{5}-1)) \cdot (-3(1+\sqrt{5})) = -216.$$

Kontroll näitab, et arv -216 ka rahuldab ülesande tingimust. $\square$

Ülesanne VI.3. Leidke polünoomi

$$f(X) = X^3 - 9X^2 + 23X - 15$$

kõik juured, teades, et nad moodustavad aritmeetilise jada.

Lahendus: Olgu c_1 , c_2 ja c_3 polünoomi f juured. Kui nad moodustavad aritmeetilise jada, siis vastavalt aritmeetilise jada summa valemile kehtib

$$c_1 + c_2 + c_3 = 3c_1 + 3d,$$

kus d on antud aritmeetilise jada vahe. Lisaks $c_2 = c_1 + d$ ja $c_3 = c_1 + 2d$. Viete'i valemitest saame

$$9 = c_1 + c_2 + c_3 = 3c_1 + 3d \implies d = 3 - c_1.$$

Samuti saame Viete'i valemitest

$$\begin{aligned} 15 &= c_1c_2c_3 = c_1(c_1 + d)(c_1 + 2d) = c_1^3 + 3c_1^2d + 2c_1d^2 = \\ &= c_1^3 + 3c_1^2(3 - c_1) + 2c_1(3 - c_1)^2 = c_1^3 + 9c_1^2 - 3c_1^3 + 18c_1 - 12c_1^2 + 2c_1^3 \\ &= 18c_1 - 3c_1^2 \implies c_1^2 - 6c_1 + 5 = 0. \end{aligned}$$

Lahendades eelmise võrrandi saame

$$c_1 = 3 \pm \sqrt{9 - 5} = 3 \pm 2 = \begin{cases} 5, \\ 1. \end{cases}$$

Siit saame $d_1 = 3 - 5 = -2$ ja $d_2 = 2$. Vastavalt vahele d_1 saame $c_1 = 5$, $c_2 = 3$ ja $c_3 = 1$ ning vahe d_2 korral $c_1 = 1$, $c_2 = 3$ ja $c_3 = 5$. Kuna eelnevad lahendite komplektid erinevad ainult järjekorra poolest, siis oleme saanud üheselt määratud lahendid $(1, 3, 5)$. $\square$

Ülesanne VI.4. Leidke polünoomi

$$f(X) = X^4 - X^2 - 2X + 1$$

kompleksarvuliste juurte pöördarvude summa.

Lahendus: Tähistame tähtedega c_1, c_2, c_3 ja c_4 polünoomi $f \in \mathbb{C}[X]$ juured. Paneme tähele, et

$$(c_1)^{-1} + (c_2)^{-1} + (c_3)^{-1} + (c_4)^{-1} = \frac{c_2c_3c_4 + c_1c_3c_4 + c_1c_2c_4 + c_1c_2c_3}{c_1c_2c_3c_4} = \frac{\sigma_3(c_1, c_2, c_3, c_4)}{\sigma_4(c_1, c_2, c_3, c_4)},$$

kus σ_2 ja σ_3 on vastavad nelja muutuja sümmeetrilised põhipolünoomid. Ilmselt 0 ei ole polünoomi f juur, mistõttu on eelnevas reas jagamine lubatud. Viete'i valemitest saame, et

$$\begin{aligned}\sigma_3(c_1, c_2, c_3, c_4) &= (-1)^3 \cdot (-2) = 2, \\ \sigma_4(c_1, c_2, c_3, c_4) &= (-1)^4 \cdot 1 = 1.\end{aligned}$$

Seega $(c_1)^{-1} + (c_2)^{-1} + (c_3)^{-1} + (c_4)^{-1} = \frac{2}{1} = 2$. □

Ülesanne VI.5. Leidke kõigi n -nda astme kompleksarvuliste ühejuurte summa ja korrutis (kus $n \geq 2$).

Lahendus: Olgu $c_1, \dots, c_n$ kompleksarvulised n -nda astme ühejuured. Paneme tähele, et kompleksarvude korpuses avalduvad n -nda astme ühejuured täpselt polünoomi $X^n - 1 \in \mathbb{C}[X]$ juurtena. Vastavalt Viete'i valemitele saame, et

$$\begin{aligned}\sum_{k=1}^n c_k &= -1 \cdot 0 = 0, \\ \prod_{k=1}^n c_k &= (-1)^n(-1) = (-1)^{n+1}.\end{aligned}$$

Sellega oleme leidnud ühejuurte summa ja korrutise. □

Ülesanne VI.6. Lahendage järgmine võrrandisüsteem üle $\mathbb{C}$:

$$\begin{cases} x_1 + x_2 + x_3 = 0, \\ x_1^2 + x_2^2 + x_3^2 = 0, \\ x_1^3 + x_2^3 + x_3^3 = 24. \end{cases}$$

Lahendus: Eelmise praktikumi ülesandest V.5 on teada, et polünoom $X_1^3 + X_2^3 + X_3^3 \in \mathbb{C}[X_1, X_2, X_3]$ esitub 3 muutuja sümmeetriliste põhipolünoomide kaudu kujul

$$\sigma_1(X_1, X_2, X_3)^3 - 3\sigma_1(X_1, X_2, X_3)\sigma_2(X_1, X_2, X_3) + 3\sigma_3(X_1, X_2, X_3).$$

Esimesest võrrandist saame aga, et $\sigma_1(x_1, x_2, x_3) = 0$. Järelikult

$$24 = 0^3 + -3 \cdot 0 \cdot \sigma_2(x_1, x_2, x_3) + 3\sigma_3(x_1, x_2, x_3) = 3\sigma_3(x_1, x_2, x_3) = 3x_1x_2x_3.$$

Seega $x_1x_2x_3 = 8$.

Avaldame ka polünoomi $f(X_1, X_2, X_3) := X_1^2 + X_2^2 + X_3^2 \in \mathbb{C}[X_1, X_2, X_3]$ sümmeetriliste põhi-
 polünoomide kombinatsioonina. Pealiige on X^2 ja sealt saame

$$g_1 = \sigma_1^2 = (X_1 + X_2 + X_3)^2 = X_1^2 + X_2^2 + X_3^2 + 2X_1X_2 + 2X_1X_3 + 2X_2X_3.$$

Nüüd

$$f_1 = f - g_1 = -2(X_1X_2 + X_1X_3 + X_2X_3) = -2\sigma_2 = g_2.$$

Järelikult $f = \sigma_1^2 - 2\sigma_2$. Siit saame, et $-2\sigma_2(x_1, x_2, x_3) = 0$ ehk $\sigma_2(x_1, x_2, x_3) = 0$. Nüüdseks oleme
 saanud tingimused

$$\begin{cases} \sigma_1(x_1, x_2, x_3) = x_1 + x_2 + x_3 = 0, \\ \sigma_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3 = 0. \\ \sigma_3(x_1, x_2, x_3) = x_1x_2x_3 = 8. \end{cases}$$

Näeme, et vastavalt Viete'i valemitele on arvud x_1, x_2 ja x_3 polünoomi $X^3 - 8 \in \mathbb{C}[X]$ juured.
 Seega leiame polünoomi $X^3 - 8$ juured:

$$x_{1,2,3} = \sqrt[3]{8}, \\ x_1 = 2, \quad x_2 = 2e^{i\frac{2}{3}\pi}, \quad x_3 = 2e^{-i\frac{2}{3}\pi}$$

ehk otsitava võrrandite süsteemi lahenditeks on kompleksarvu 8 kuupjuured. □

Ülesanne VI.7. Olgu R kommutatiivne ring. Millistel tingimustel kehtib järgmine väide: igal
 n -nda astme polünoomil üle R on (kordsust arvestades) ülimalt n juurt?

Lahendus: Üldiselt on n -nda astme polünoomil $f \in R[X]$ ülimalt n juurt, kui R on kommuta-
 tiivne nulliteguriteta ring (integriteetkond). Kui ringis R on nullitegureid, s.t. leiduvad $a, b \in R$ nii,
 et $a \neq 0, b \neq 0$ ja $ab = 0$, siis on olukord keerulisem. Vaatleme näiteks lihtsat näidet $X^2 \in \mathbb{Z}_4[X]$.
 See tegurdub kujul $X^2 = X \cdot X$. Siit saame kahekordse juure $X = 0$, kui võrdsustame tegurid eraldi
 nulliga. Samas kehtib ringis $\mathbb{Z}_4$ võrdus $\bar{2}^2 = \bar{0}$, seega ka $\bar{2}$ on polünoomi X^2 juur. Seega on kordsusi
 arvestades polünoomil $X^2 \in \mathbb{Z}_4[X]$ kolm juurt.

Vaatleme nüüd ka näidet, kus on rohkem kui n juurt ka ilma kordsust arvestamata. Vaatleme
 näiteks polünoomi $X^2 - \bar{1} \in \mathbb{Z}_8[X]$. Kehtib

$$X^2 - \bar{1} = (X - \bar{1})(X - \bar{7}) = (X - \bar{3})(X - \bar{5}),$$

mistõttu $\bar{1}, \bar{7}, \bar{3}$ ja $\bar{5}$ on kõik polünoomi $X^2 - \bar{1}$ juured üle ringi $\mathbb{Z}_8$, mis on nulliteguritega ring.

Erandiks siin on 0-polünoom, aga ta on erandlik väga mitmes mõttes. Olemuslikult võib öelda,
 et nullpolünoomi $0 \in R[X]$ juurteks on kõik ringi R elemendid. Kuna me ei ole defineerinud 0
 polünoomi astet, siis ei ole ka 0 kunagi n -nda astme polünoom. (Tihti defineeritakse $\deg(0) = -\infty$.) □

Algebraalne arv on kompleksarv, mis on mingi polünoomi $0 \neq p(X) \in \mathbb{Q}[X]$ juureks. Kõigi
 algebraaliste arvude hulka tähistame $\mathbb{A}$. *Algebraalne täisarv* on selline algebraalne arv, mille korral
 $p(X) \in \mathbb{Z}[X]$ ja $p(X)$ pealiikme kordaja on 1.

Ülesanne VI.8. Tõestada, et algebraalse täisarvu ja tavalise täisarvu summa on algebraalne täisarv.

Lahendus: Olgu $z \in \mathbb{Z}$ ja a algebraline täisarv, siis leidub polünoom $p(X) = X^n + \alpha_1 X^{n-1} + \dots + \alpha_{n-1} X + \alpha_n \in \mathbb{Z}[X]$ nii, et a on polünoomi p juur. Ilmselt z on samuti algebraline täisarv, kuna on juureks polünoomile $X - z \in \mathbb{Z}[X]$. Vaatleme polünoomi

$$s(X) := (X - z)^n + \sum_{k=1}^n \alpha_k (X - z)^{n-k}.$$

Ilmselt kehtib

$$s(a + z) = (a + z - z)^n + \sum_{k=1}^n \alpha_k (a + z - z)^{n-k} = a^n + \sum_{k=1}^n \alpha_k a^{n-k} = p(a) = 0.$$

Kuna $X - z \in \mathbb{Z}[X]$ ja $\mathbb{Z}[X]$ on ring, siis iga $l \in \mathbb{N}$ korral $(X - z)^l \in \mathbb{Z}[X]$ ja iga $\alpha \in \mathbb{Z}$ korral $\alpha(X - z)^l \in \mathbb{Z}[X]$. Ka selliste polünoomide summa kuulub ringi $\mathbb{Z}[X]$. Vaatleme avaldist $s(X)$ lähemalt, avame seda Newtoni binoomvalemiga:

$$\begin{aligned} s(X) &= \sum_{h=0}^n (-1)^h \binom{n}{h} X^{n-h} z^h + \sum_{k=1}^n \alpha_k \sum_{j=0}^{n-k} (-1)^j \binom{n-k}{j} X^{n-k-j} z^j = \\ &= X^n + \sum_{h=1}^n (-1)^h \binom{n}{h} z^h X^{n-h} + \sum_{k=1}^n \alpha_k \sum_{j=0}^{n-k} (-1)^j \binom{n-k}{j} z^j X^{n-k-j}. \end{aligned}$$

Polünoomi $s(X)$ pealiikme kordaja on 1 (pealiige X^n on eelpool eraldatud; on lihtne näha, et teisest summast ei saa tulla X -i astmeks n). Seega s on vajalikele tingimustele vastav polünoom juurega $a + z$, mistõttu $a + z$ on algebraline täisarv. $\square$

Ülesanne VI.9. Tõestada, et kui ratsionaalarv on algebraline täisarv, siis ta on ka tavaline täisarv.

Lahendus: Olgu a ratsionaalne algebraline täisarv, siis leiduvad täisarvud $r, s \in \mathbb{Z}$, mille korral $\text{SÜT}(r, s) = 1$ ja $a = \frac{r}{s}$. Kuna a on algebraline täisarv, siis leidub polünoom $X^n + \alpha_1 X^{n-1} + \dots + \alpha_{n-1} X + \alpha_n \in \mathbb{Z}[X]$ nii, et

$$\left(\frac{r}{s}\right)^n + \alpha_1 \left(\frac{r}{s}\right)^{n-1} + \dots + \alpha_{n-1} \left(\frac{r}{s}\right) + \alpha_n = 0.$$

Korrutades eelneva võrduse pooli arvuga s^n , saame

$$\begin{aligned} r^n + \alpha_1 r^{n-1} s + \dots + \alpha_{n-1} r s^{n-1} + \alpha_n s^n &= 0 \\ \implies r^n &= (-\alpha_1 r^{n-1} - \dots - \alpha_n s^{n-1}) s, \end{aligned}$$

kus $-\alpha_1 r^{n-1} - \dots - \alpha_n s^{n-1}$ on täisarv. Siit saame jaguvuse $s \mid r^n$. Kuna aga $\text{SÜT}(r, s) = 1$, siis saame, et $s = \pm 1$. Järelikult $a = \pm r$ ehk $a \in \mathbb{Z}$ nagu tahetud. $\square$

Ülesanne* VI.10. Tõestada, et algebraliste täisarvude summa ja korrutis on samuti algebralised täisarvud.

Praktikum VII Polünoomi lahutuskorpus

Polünoomi $p(X) \in K[X]$ nimetatame *lahutuvaks* ringis $K[X]$, kui polünoom p on esitatav lineaarpolünoomide korrutisena ringis $K[X]$. (Inglise keeles *polynomial* $p(X) \in K[X]$ *splits in* $K[X]$.)

Ülesanne VII.1. Kas $X^4 - 11X^2 + 18$ on lahutuv ringis $\mathbb{Q}[X]$?

Lahendus: Vaatleme polünoomi $X^4 - 11X^2 + 18 \in \mathbb{Q}[X]$. Leiame selle polünoomi juured. Selleks vaatleme võrrandit

$$x^4 - 11x^2 + 18 = 0,$$

mis on biruutvõrrand. Seda saab lahendada asendusega $t := x^2$, misjärel

$$t^2 - 11t + 18 = 0,$$

$$t_{1,2} = 5, 5 \pm \sqrt{12, 25} = 5, 5 \pm 3, 5 = \{2; 9\}.$$

Seega $x \in \{-\sqrt{2}, \sqrt{2}, -3, 3\}$. Kuna $\pm\sqrt{2}$ ilmselt ei kuulu hulka $\mathbb{Q}$, siis polünoom $X^4 - 11X^2 + 18$ ei ole lahutuv ringis $\mathbb{Q}[X]$.

See polünoom on ringis $\mathbb{Q}[X]$ esitatav kujul

$$X^4 - 11X^2 + 18 = (X - 3)(X + 3)(X^2 - 2).$$

Kuna ruutpolünoom $X^2 - 2$ on taandumatu ringis $\mathbb{Q}[X]$, siis vähim ring, kus $p(X)$ lahutub on $K[X]$, kus $K \supset \mathbb{Q}$ on polünoomi $X^2 - 2$ lahutuskorpus. $\square$

Olgu K korpus ja $\alpha_1, \dots, \alpha_n \notin K$. Tähistame $K(\alpha_1, \dots, \alpha_n)$ korpust, mis on vähim korpus, mis sisaldab hulka $K \cup \{\alpha_1, \dots, \alpha_n\}$ ning K on korpuse $K(\alpha_1, \dots, \alpha_n)$ alamkorpus. Taandumatu polünoomi $p \in K[X]$ lahutuskorpuseks on korpus $K(\alpha_1, \dots, \alpha_n)$, kus $\alpha_1, \dots, \alpha_n$ on polünoomi p juured.

Ülesanne VII.2. Näidake, et polünoomidel $p(X) = (X^2 - 2X - 2)(X^2 + 1)$ ja $q(X) = X^5 - 3X^3 + X^2 - 3$ on sama lahutuskorpus üle $\mathbb{Q}$.

Lahendus: Kõigepealt leiame antud polünoomide lahutused (ringis $\mathbb{C}[X]$). Paneme tähele, et

$$p(X) = (X^2 - 2X - 2)(X^2 + 1) = (X - (1 + \sqrt{3}))(X - (1 - \sqrt{3}))(X + i)(X - i)$$

Kuna $1 \pm \sqrt{3}, i \notin \mathbb{Q}$, siis polünoomi p lahutuskorpus on $\mathbb{Q}(1 \pm \sqrt{3}, i)$. Ilmselt $\mathbb{Q}(1 \pm \sqrt{3}) = \mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$. Seega polünoomi $p(X)$ lahutuskorpus on $\mathbb{Q}(\sqrt{3}, i)$.

Tegurdame polünoomi q , kasutades selleks “rühmitamise” võtet (seda võtet õpetatakse põhikoolis). Tegurdame

$$\begin{aligned} q(X) &= X^5 - 3X^3 + X^2 - 3 = X^3(X^2 - 3) + X^2 - 3 = (X^2 - 3)(X^3 + 1) = \\ &= (X + \sqrt{3})(X - \sqrt{3})(X - 1)(X - e^{i\frac{2\pi}{3}})(X - e^{-i\frac{2\pi}{3}}), \\ e^{\pm i\frac{2\pi}{3}} &= \cos \frac{2\pi}{3} \pm i \sin \frac{2\pi}{3} = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2} = \frac{1}{2}(-1 \pm i\sqrt{3}). \end{aligned}$$

Seega polünoomi q lahutuskorpus on $\mathbb{Q}(\sqrt{3}, \frac{1}{2}(-1 + i\sqrt{3}))$. Paneme tähele, et

$$\frac{\sqrt{3}}{3} \left(2 \left(\frac{1}{2}(-1 + i\sqrt{3}) \right) + 1 \right) = i.$$

Järelikult $i \in \mathbb{Q}(\sqrt{3}, \frac{1}{2}(-1 + i\sqrt{3}))$, mistõttu $\mathbb{Q}(\sqrt{3}, i) \subseteq \mathbb{Q}(\sqrt{3}, \frac{1}{2}(-1 + i\sqrt{3}))$. Analoogiliselt saame näidata, et $\mathbb{Q}(\sqrt{3}, \frac{1}{2}(-1 + i\sqrt{3})) \subseteq \mathbb{Q}(\sqrt{3}, i)$, mistõttu kehtib $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3}, \frac{1}{2}(-1 + i\sqrt{3}))$. $\square$

Siinkohal tahaksin natuke selgitada, millised on ringi $K[X]/\langle f \rangle$ elemendid, kus $f \in K[X]$ (K on korpus). Teadupoolest $\langle f \rangle = fK[X] = \{fg \mid g \in K[X]\}$. Kuna $K[X]$ on Eukleidese ring, siis iga $h \in K[X]$ on esitatav kujul $h = gf + r$, kus $g, r \in K[X]$ ja $0 \leq \deg(r) < \deg(f)$, järelikult

$$[h] = [gf + r] = gf + r + \langle f \rangle = r + \langle f \rangle = [r] \in K[X]/\langle f \rangle.$$

Seega ring $K[X]/\langle f \rangle$ on isomorfne ringiga, kuhu kuuluvad vaid polünoomiga f jäägiga jagamise jäägid ehk polünoomid r nii, et $0 \leq \deg(r) < \deg(f)$.

Siit on näha, et ringid $K[X]/\langle f \rangle$ on analoogilised ringidega $\mathbb{Z}_n$, mis koosnevad naturaalarvuga n jäägiga jagamise jääkidest. Nii nagu ring $\mathbb{Z}_n$ on korpus parajasti siis, kui n on algarv; kehtib ka, et $K[X]/\langle f \rangle$ on korpus parajasti siis, kui f on taandumatu ringis $K[X]$. Täpsemalt ja põhjalikumalt vaadeldakse ringe kujul $K[X]/\langle f \rangle$ aines Lõplikud Korpused.

Ülesanne VII.3. Tehke kindlaks, kas järgmised korpuste laiendid on lahutuskorpused:

- 1) $\mathbb{Z}_3[X]/\langle X^5 + \bar{1} \rangle$ polünoomi $X^5 + \bar{1} \in \mathbb{Z}_3[X]$ suhtes;
- 2) korpus $\mathbb{Q}[\sqrt{2}] \supseteq \mathbb{Q}$ polünoomi $X^2 - 2$ suhtes.

Lahendus:

- 1) Vaatleme polünoomi $p(X) = X^5 + \bar{1} \in \mathbb{Z}_3[X]$. Uurime, kas polünoom $X^5 + \bar{1}$ on taandumatu ringis $\mathbb{Z}_3[X]$. Paneme tähele, et $\bar{2}$ on polünoomi p juur korpuses $\mathbb{Z}_3$. Seega p ei ole taandumatu ja $\mathbb{Z}_3[X]/\langle X^5 + \bar{1} \rangle$ ei ole korpus, ammugi siis lahutuskorpus. Kuid näitame seda asjaolu detailsemalt. Jagame polünoomi $X^5 + \bar{1}$ polünoomiga $X - \bar{2}$.

$$\begin{array}{r}
 \begin{array}{r}
 X^5 \\
 X^5 - \bar{2}X^4 \\
 \hline
 \bar{2}X^4 \\
 \bar{2}X^4 - \bar{2}X^3 \\
 \hline
 -\bar{2}X^3 \\
 -\bar{2}X^3 + X^2 \\
 \hline
 -X^2 \\
 -X^2 + \bar{2}X \\
 \hline
 -\bar{2}X \\
 -\bar{2}X + \bar{1} \\
 \hline
 \bar{1} \\
 \bar{1} - \bar{2} \\
 \hline
 0
 \end{array}
 \end{array}
 \begin{array}{r}
 +\bar{1} \\
 +\bar{1} \\
 +\bar{1} \\
 +\bar{1} \\
 +\bar{1} \\
 +\bar{1} \\
 +\bar{1}
 \end{array}
 \begin{array}{r}
 |X^4 + \bar{2}X^3 - \bar{2}X^2 - X - \bar{2} \\
 \hline
 |X - \bar{2}
 \end{array}$$

Seega

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

Ring $\mathbb{Z}_3[X]/\langle X^5 + \bar{1} \rangle$ ei ole korpus, kuna ekvivalentsiklassid $[X - \bar{2}]$ ning $[X^4 + \bar{2}X^3 - \bar{2}X^2 - X - \bar{2}]$ on selle ringi nullitegurid.

2) Vaatleme polünoomi $X^2 - 2$. Ilmselt kehtib

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

Kuna polünoomid $X - \sqrt{2}$ ja $X + \sqrt{2}$ ei kuulu ilmselt ringi $\mathbb{Q}[X]$, on polünoom $X^2 - 2$ taandumatu selles ringis. Vastavalt loengukonspekti [1] teoreemile 2.23 on polünoomi $X^2 - 2$ lahutuskorpuseks $\mathbb{Q}[X]/\langle X^2 - 2 \rangle$. Hulga $\mathbb{Q}[X]/\langle X^2 - 2 \rangle$ elementide (ekvivalentsiklasside) esindajad on kõik polünoomid ringist $\mathbb{Q}[X]$, mille korral $\deg(p) < \deg(X^2 - 2) = 2$, seega oma vähimate astmetega esindajate kaudu saame esitada

$$\mathbb{Q}[X]/\langle X^2 - 2 \rangle = \{[bX + a] \mid a, b \in \mathbb{Q}\}.$$

Kuna $\mathbb{Q}[X]/\langle X^2 - 2 \rangle$ on faktoring, on seal tehted defineeritud esindajate kaudu. Liitmine on lihtne – analoogiline polünoomide tavalise liitmisega. Vaatleme aga täpsemalt korrutamist siin ringis. Olgu $[a_1 + b_1X], [a_2 + b_2X] \in \mathbb{Q}[X]/\langle X^2 - 2 \rangle$, siis

$$\begin{aligned} [a_1 + b_1X][a_2 + b_2X] &= [(a_1 + b_1X)(a_2 + b_2X)] = \\ &= [a_1a_2 + (a_1b_2 + b_1a_2)X + b_1b_2X^2]. \end{aligned}$$

Leidmaks ekvivalentsiklassi $[a_1a_2 + (a_1b_2 + b_1a_2)X + b_1b_2X^2]$ vähima astmega esindajat jagame polünoomi $a_1a_2 + (a_1b_2 + b_1a_2)X + b_1b_2X^2$ läbi polünoomiga $X^2 - 2$:

$$\begin{array}{r} \begin{array}{ccc} b_1b_2X^2 & (a_1b_2 + b_2a_2)X & +a_1a_2 \\ b_1b_2X^2 & & -2b_1b_2 \end{array} & \frac{|b_1b_2|}{|X^2 - 2|} \\ \hline (a_1b_2 + b_2a_2)X & a_1a_2 + 2b_1b_2 \end{array}$$

Järelikult

$$\begin{aligned} [a_1 + b_1X][a_2 + b_2X] &= [b_1b_2(X^2 - 2) + ((a_1b_2 + b_2a_2)X + (a_1a_2 + 2b_1b_2))] = \\ &= [(a_1b_2 + b_2a_2)X + (a_1a_2 + 2b_1b_2)]. \end{aligned}$$

Teisalt vaatleme nüüd ringi $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Defineerime kujutuse

$$\iota: \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[X]/\langle X^2 - 2 \rangle, \quad a + b\sqrt{2} \mapsto [a + bX].$$

Kujutus ι on ilmselt bijektiivne.

$$\begin{aligned} \iota((a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})) &= \iota((a_1 + a_2) + (b_1 + b_2)\sqrt{2}) = \\ &= [(a_1 + a_2) + (b_1 + b_2)X] = [(a_1 + b_1X) + (a_2 + b_2X)] = \\ &= [a_1 + b_1X] + [a_2 + b_2X] = \iota(a_1 + b_1\sqrt{2}) + \iota(a_2 + b_2\sqrt{2}), \\ \iota((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})) &= \iota((a_1a_2 + 3b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2}) = \\ &= [(a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)X] = [a_1 + b_1X][a_2 + b_2X]. \end{aligned}$$

Seega ι on ringide isomorfism. Tänu sellele, et $\mathbb{Q}[X]/\langle X^2 - 2 \rangle$ on korpus ja ι in isomorfism, siis ka $\mathbb{Q}[\sqrt{2}]$ on korpus. Kuna $\mathbb{Q}[\sqrt{2}]$ ja $\mathbb{Q}[X]/\langle X^2 - 2 \rangle$ on isomorfised, võib öelda, et $\mathbb{Q}[\sqrt{2}]$ on polünoomi $X^2 - 2$ lahutuskorpus üle korpuse $\mathbb{Q}$.

□

Analoogiliselt eelmise ülesande teisele punktile tõestatakse ka isomorfism

$$\mathbb{C} \cong \mathbb{R}[X]/\langle X^2 + 1 \rangle, \quad (X^2 + 1 \in \mathbb{R}[X]).$$

Seega kompleksarvud on polünoomi $X^2 + 1 \in \mathbb{R}[X]$ lahutuskorpus. Sisuliselt selliselt ka G. Cardano XVI sajandil kompleksarvud esimest korda kasutusele võttis. (Cardano kasutas teadaolevalt esimesena kompleksarvuseid, et lahendada ruutvõrrandeid.)

Ülesanne VII.4. Leida polünoomi $X^4 + X^2 - 1$ lahutuskorpus üle $\mathbb{Q}$. (Võtame teadaolevaks, et $X^4 + X^2 - 1$ on taandumatu ringis $\mathbb{Q}[X]$.)

Lahendus: Vaatleme polünoomi $p(X) = X^4 + X^2 - 1 \in \mathbb{Q}[X]$. Pannes tähele, et $x^4 + x^2 - 1 = 0$ on biruutvõrrand, saame leida polünoomi p juured. Arvutame

$$\begin{aligned} x^4 + x^2 + 1 &= 0, \\ x^2 &= -\frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} = -\frac{1}{2} \pm \frac{\sqrt{5}}{2}. \end{aligned}$$

Siit on näha, et polünoomil p kindlasti ei leidu ratsionaalarvulisi juuri. Siit näeme, et plünoom $X^4 + X^2 - 1$ on tõenäoliselt taandumatu ringis $\mathbb{Q}[X]$. Veenduda, et see polünoom tõepoolest on taandumatu, on üldiselt väga keeruline. Seepärast võtame teatavaks, et $X^4 + X^2 - 1$ on taandumatu ringis $\mathbb{Q}[X]$.

Seega polünoomi p lahutuskorpus on $\mathbb{Q}[X]/\langle p \rangle$. Kuna $\deg(p) = 4$, siis vastavalt ülesande 2 järel toodud kirjeldusele, võime esitada lahutuskorpuse

$$\mathbb{Q}[X]/\langle X^4 + X^2 - 1 \rangle = \{[aX^3 + bX^2 + cX + d] \mid a, b, c, d \in \mathbb{Q}\}.$$

Täiendava osana leiame korrutamise valemi selles korpuses. Olgu $[a_1X^3 + b_1X^2 + c_1X + d_1]$, $[a_2X^3 + b_2X^2 + c_2X + d_2] \in \mathbb{Q}[X]/\langle X^4 + X^2 - 1 \rangle$, siis

$$\begin{aligned} &[a_1X^3 + b_1X^2 + c_1X + d_1][a_2X^3 + b_2X^2 + c_2X + d_2] = \\ &= [a_1a_2X^6 + (a_1b_2 + b_1a_2)X^5 + (a_1c_2 + b_1b_2 + c_1a_2)X^4 + \\ &\quad + (a_1d_2 + b_1c_2 + c_1b_2 + d_1a_2)X^3 + (b_1d_2 + c_1c_2 + d_1b_2)X^2 + \\ &\quad + (c_1d_2 + d_2c_1)X + d_1d_2] = \\ &= [(a_1d_2 + b_1c_2 + c_1b_2 + d_1a_2 - a_1b_2 - b_1a_2)X^3 + \\ &\quad + (b_1d_2 + c_1c_2 + d_1b_2 - a_1c_2 - b_1b_2 - c_1a_2)X^2 + \\ &\quad + (-c_1d_2 - d_2c_1 + a_1b_2 + b_1a_2)X + (d_1d_2 + a_1c_2 + b_1b_2 + c_1a_2 - a_1a_2)]. \end{aligned}$$

Viimase võrduse saamiseks vajalikud jagamised on toodud ülesannete lahenduste lõpus, kuna on liialt pikad ning seepärast kirjutatud A3 paberile. □

Eelmises ülesandes vaadeldud korpuses $\mathbb{Q}[X]/\langle X^4 + X^2 - 1 \rangle$ võib korrutada ka, mitte tuletatud korrutamise valemit kasutades, vaid kasutades tähelepanekut $[X^4] = [1 - X^2]$. See järeldeb asjaolust, et ilmselt

$$[X^4 + X^2 + 1] = [X^4] + [X^2 - 1] = [0]$$

faktorkorpuses $\mathbb{Q}[X]/\langle X^4 + X^2 - 1 \rangle$.

Ülesanne VII.5. Leida polünoomi $X^3 + \bar{2}X^2 + \bar{2}$ lahutuskorpus üle $\mathbb{Z}_3$.

Lahendus: Vaatleme polünoomi $p(X) = X^3 + \bar{2}X^2 + \bar{2} \in \mathbb{Z}_3[X]$. Kontrollime, kas polünoomil p on juuri korpuses $\mathbb{Z}_3$. (Lõplikes korpustes on tihti optimaalseid võrrandit lahendada lihtsalt proovides, kas mõni element seda võrrandit rahuldab. Korpuses $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ on see lihtne.) Märkame, et $\bar{2}$ on polünoomi $X^3 + \bar{2}X^2 + \bar{2}$ juur. Jagame polünoomi p polünoomiga $X - \bar{2}$.

$$\begin{array}{r} X^3 + \bar{2}X^2 \qquad \qquad + \bar{2} \quad | X^2 + X + \bar{2} \\ X^3 - \bar{2}X^2 \qquad \qquad \qquad \quad | X - \bar{2} \\ \hline X^2 \qquad \qquad \qquad + \bar{2} \\ X^2 \qquad - \bar{2}X \qquad \qquad \qquad \quad \\ \hline \qquad \qquad \quad 2X \quad + \bar{2} \\ \qquad \qquad \quad \bar{2}X \quad + \bar{2} \\ \hline \qquad \qquad \qquad \qquad \qquad 0 \end{array}$$

Oleme saanud, et kehtib

$$X^3 + \bar{2}X^2 + \bar{2} = (X - \bar{2})(X^2 + X + \bar{2}).$$

Kontrollides potentsiaalseid lahendeid näeme, et polünoom $X^2 + X + \bar{2}$ on taandumatu ringis $\mathbb{Z}_3[X]$. Siit saame, et polünoomide p ja $q(X) = X^2 + X + \bar{2}$ lahutuskorpused langevad kokku. Seega tänu loengukonspekti [1] teoreemile 2.23 saame, et polünoomi $p(X) = X^3 + \bar{2}X^2 + \bar{2}$ lahutuskorpus on $\mathbb{Z}_3[X]/\langle X^2 + X + \bar{2} \rangle$. Kirjutame selle korpuse välja

$$\begin{aligned} \mathbb{Z}_3[X]/\langle X^2 + X + \bar{2} \rangle &= \{[aX + b] \mid a, b \in \mathbb{Z}_3\} = \\ &= \{[\bar{0}], [\bar{1}], [\bar{2}], [X], [\bar{2}X], [X + \bar{1}], [X + \bar{2}], [\bar{2}X + \bar{1}], [\bar{2}X + \bar{2}]\}. \end{aligned}$$

Kui tahame näha, kuidas toimub korrumine korpuses $\mathbb{Z}_3[X]/\langle X^2 + X + \bar{2} \rangle$, siis võime valemi leida jagades nagu eelmises ülesandes. Kuid võime kas kasutada tähelepanekut, et

$$[X^2 + X + \bar{2}] = [\bar{0}] \implies [X^2] = [X]^2 = -[X + \bar{2}] = [\bar{2}X + \bar{1}].$$

Siinkohal on see ülesanne lahendatud, kuid kuna ilmselt on polünoomide ringide faktorkorpustes arvutamine suhteliselt võõras, siis teeme veel mõningaid arvutusi, mis loodetavasti avavad natuke lahutuskorpuste olemust. Veendume, et $L = \mathbb{Z}_3[X]/\langle X^2 + X + \bar{2} \rangle$ on tõepoolest polünoomi $X^3 + \bar{2}X^2 + \bar{2}$ lahutuskorpus. Selleks peame veenduma, et polünoom $\tilde{p}(X) = X^3 + [\bar{2}]X^2 + [\bar{2}] \in L[X]$ on lahutuv. Eelnevast teame, et $[\bar{2}]$ ja $[X]$ on polünoomi $\tilde{p}$ juured korpuses L . Otsime ka 3. juure.

$$\begin{array}{r} X^2 + X \qquad \qquad + [\bar{2}] \quad | X + [X + \bar{1}] \\ X^2 - [X]X \qquad \qquad \quad | X - [X] \\ \hline [X + \bar{1}]X \quad + [\bar{2}] \\ [X + \bar{1}]X \quad + [\bar{2}] \\ \hline \qquad \qquad \qquad [\bar{0}] \end{array}$$

Seega viimane juur on $-[X + \bar{1}] = [\bar{2}X + \bar{2}]$. Nüüd näitame, et polünoom $\tilde{p}$ tõesti esitub lineaarpolünoomide korrutisena ringis $(\mathbb{Z}_3[X]/\langle X^2 + X + \bar{2} \rangle)[X]$. Paneme tähele

$$(X - [\bar{2}]) (X - [X]) (X - [\bar{2}X + \bar{2}]) =$$

$$\begin{aligned}
&= (X - [\bar{2}]) (X^2 - [\bar{2}X + \bar{2}] X - [X] X + [X] [\bar{2}X + \bar{2}]) = \\
&= (X - [\bar{2}]) (X^2 + [-\bar{2}X - \bar{2} - X] X + [\bar{2}X^2 + \bar{2}X]) = \\
&= (X - [\bar{2}]) (X^2 + X + [\bar{2}(\bar{2}X + \bar{1}) + \bar{2}X]) = \\
&= (X - [\bar{2}]) (X^2 + X + [X + \bar{2} + \bar{2}X]) = \\
&= (X - [\bar{2}]) (X^2 + X + [\bar{2}]) = \\
&= X^3 + X^2 + [\bar{2}] X - [\bar{2}] X^2 - [\bar{2}] X - [\bar{2}] [\bar{2}] = \\
&= X^3 + ([\bar{1}] + [\bar{1}]) X^2 + ([\bar{2}] - [\bar{2}]) X - [\bar{1}] = \\
&= X^3 + [\bar{2}] X^2 + [\bar{2}] = \tilde{p}(X).
\end{aligned}$$

Sellega ma loodan, et lahutuskorpuse olemus ja aritmeetika temas on natuke selgemaks saanud. $\square$

Siinkohal tahaksin toonitada, et kui polünoomi $p \in K[X]$ korral $\deg(p) > 3$, siis ei piisa selleks, et p oleks taandumatu, sellest kui tal ei leidu juuri korpuses K . Otsustamine, kas polünoom p on taandumatu, on üldiselt keeruline ülesanne (kui $\deg(p)$ on piisavalt suur).

Ülesanne VII.6. Tõestada, et $\sqrt{2} + \sqrt{3}$ on algebraline üle $\mathbb{Q}$, konstrueerides 4. astme polünoomi üle $\mathbb{Q}$, mille juureks ta on.

Lahendus: Kõigepealt leiame arvu $\sqrt{2} + \sqrt{3}$ astmed kuni 4.-ni Newtoni binoomvalemiga

$$\begin{aligned}
(\sqrt{2} + \sqrt{3})^4 &= (\sqrt{2})^4 + 4(\sqrt{2})^3\sqrt{3} + 6(\sqrt{2})^2(\sqrt{3})^2 + 4\sqrt{2}(\sqrt{3})^3 + (\sqrt{3})^4 = \\
&= 4 + 8\sqrt{6} + 36 + 12\sqrt{6} + 9 = 49 + 20\sqrt{6}, \\
(\sqrt{2} + \sqrt{3})^3 &= (\sqrt{2})^3 + 3(\sqrt{2})^2\sqrt{3} + 3\sqrt{2}(\sqrt{3})^2 + (\sqrt{3})^3 = \\
&= 2\sqrt{2} + 6\sqrt{3} + 9\sqrt{2} + 3\sqrt{3} = 11\sqrt{2} + 9\sqrt{3}, \\
(\sqrt{2} + \sqrt{3})^2 &= 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}.
\end{aligned}$$

Leidmaks polünoomi ringis $\mathbb{Q}[X]$, millele $\sqrt{2} + \sqrt{3}$ on juureks, peame leidma $a, b, c, d, e \in \mathbb{Q}$ nii, et

$$\begin{aligned}
0 &= a(49 + 20\sqrt{6}) + b(11\sqrt{2} + 9\sqrt{3}) + c(5 + 2\sqrt{6}) + d(\sqrt{2} + \sqrt{3}) + e = \\
&= (20a + 2c)\sqrt{6} + (9b + d)\sqrt{3} + (11b + d)\sqrt{2} + (49a + 5c + e).
\end{aligned}$$

Siit saame lineaarvõrranditesüsteemi

$$\left\{ \begin{array}{l} 20a + 2c = 0 \\ 9b + d = 0 \\ 11b + d = 0 \end{array} \right\} \implies 20b + 2d = 0 \implies d = -10b,$$

$$\left\{ \begin{array}{l} 49a + 5c + e = 0 \end{array} \right\} \implies 49a - 50a + e = 0 \implies e = a.$$

Kokkuvõttes $(a, b, c, d, e) \in \{(c_1, c_2, -10c_1, -10c_2, c_1) \mid c_1, c_2 \in \mathbb{Q}\}$. Võttes $c_1 = 1$ ja $c_2 = 0$, saame polünoomi

$$X^4 - 10X^2 + 1 \in \mathbb{Q}[X],$$

millele $\sqrt{2} + \sqrt{3}$ on juureks. Järelikult on $\sqrt{2} + \sqrt{3}$ algebraline arv. $\square$

Olgu korpus L korpuse K laiend. Elementi $\alpha \in L$ nimetatakse *algebraliseks* üle K , kui leidub polünoom $f \in K[X]$, mille korral $f(\alpha) = 0$. Algebralise elemendi $a \in L$ *minimaalne polünoom* üle K on vähima astmega polünoom $0 \neq p(X) \in K[X]$, mille pealiikme kordaja on 1 ja $p(a) = 0$.

Ülesanne VII.7. Tõestada, et algebralise elemendi minimaalne polünoom on taandumatu.

Lahendus: Olgu korpus L korpuse K laiend ja element $\alpha \in L$ algebraline üle K . Olgu $f \in K[X]$ elemendi α minimaalne polünoom. Oletame vastuväiteliselt, et leiduvad mittekonstantsed polünoomid $g_1, g_2 \in K[X]$ nii, et $\deg(g_1) < \deg(f)$, $\deg(g_2) < \deg(f)$ ja $f = g_1 g_2$. Vastavalt eeldusele on α polünoomi f juur, see tähendab et

$$f(\alpha) = g_1(\alpha)g_2(\alpha) = 0.$$

Ilmselt $g_1(\alpha), g_2(\alpha) \in L$. Kuna L on korpus, pole seal nullitegureid, ning seetõttu kehtib $g_1(\alpha) = 0$ või $g_2(\alpha) = 0$. See on aga vastuolu, kuna vastavalt eeldusele on f vähima astmega polünoom, mille korral $f(\alpha) = 0$. $\nmid$

Järelikult on minimaalne polünoom taandumatu. $\square$

Kehtib ka eelmise ülesande väite pöördväide.

Lemma 2. Olgu $K \subseteq L$ ja f taandumatu polünoom ringis $K[X]$. Kui algebralise elemendi $\alpha \in L$ korral $f(\alpha) = 0$, siis polünoom f on minimaalne polünoom.

Ülesanne VII.8. Leida $\sqrt{2} + i$ minimaalne polünoom 1) üle $\mathbb{R}$; 2) üle $\mathbb{Q}$.

Lahendus: Arvutame elemendi $\sqrt{2} + i$ astmed, kuni imaginaarühik, kõik irratsionaalarvud ja kõik imaginaarühiku ja irratsionaalarvu korrutised on esinenud kaks korda:

$$\begin{aligned}(\sqrt{2} + i)^1 &= \sqrt{2} + i, \\(\sqrt{2} + i)^2 &= 2 + i2\sqrt{2} - 1 = 1 + i2\sqrt{2}, \\(\sqrt{2} + i)^3 &= -\sqrt{2} + 5i, \\(\sqrt{2} + i)^4 &= -7 + 4i\sqrt{2}.\end{aligned}$$

- 1) Polünoomi $f \in \mathbb{R}[X]$, mille korral $f(\sqrt{2} + i) = 0$, minimaalne aste on 2. Kuna eelnevast on näha, et elemendi $\sqrt{2} + i$ kahe esimese astme korral on imaginaarühik i kaks korda esinenud, mistõttu tema saab välja taandada. Selleks on vaja leida $a, b, c \in \mathbb{R}$ nii, et

$$0 = a(1 + i2\sqrt{2}) + b(\sqrt{2} + i) + c = (a2\sqrt{2} + b)i + (a + b\sqrt{2} + c).$$

Siit saame lineaarvõrrandite süsteemi

$$\begin{cases} a2\sqrt{2} + b = 0 \implies b = -a2\sqrt{2}, \\ a + b\sqrt{2} + c = 0 \implies 0 = a - 4a + c \implies c = 3a. \end{cases}$$

Seega $(a, b, c) \in \{(c_1, -c_12\sqrt{2}, 3c_1) \mid c_1 \in \mathbb{R}\}$. Kuna minimaalse polünoomi pealiikme kordaja peab olema 1, siis võtame $c_1 = 1$ ja saamegi otsitud minimaalse polünoomi

$$f(X) = X^2 - 2\sqrt{2}X + 3 \in \mathbb{R}[X].$$

- 2) Et saada polünoomi $g \in \mathbb{Q}[X]$, millele $\sqrt{2} + i$ oleks juureks, on vaja võtta esimesed 4 astet. Kuna siin on vaja lahti saada lisaks imaginaarühikule i ka ratsionaalsust sisaldavatest liikmetest $\sqrt{2}$ ja $i\sqrt{2}$. Otsime ratsionaalarve $a, b, c, d, e \in \mathbb{Q}$ nii, et

$$\begin{aligned} 0 &= a(4i\sqrt{2} - 7) + b(5i - \sqrt{2}) + c(1 + i2\sqrt{2}) + d(\sqrt{2} + i) + e = \\ &= (4a + 2c)i\sqrt{2} + (5b + d)i + (d - b)\sqrt{2} + (c - 7a + e). \end{aligned}$$

Siit saame lineaarvõrrandite süsteemi (lahendamise järjekord on antud rea lõpus)

$$\begin{cases} 4a + 2c = 0 \implies c = -2a, & \text{(III),} \\ 5b + d = 0 \implies b = d = 0, & \text{(II),} \\ d - b = 0 \implies d = b, & \text{(I),} \\ c - 7a + e = 0 \implies -2a - 7a + e = 0 \implies e = 8a, & \text{(IV).} \end{cases}$$

Seega $(a, b, c, d, e) \in \{(c_1, 0, -2c_1, 0, 9c_1) \mid c_1 \in \mathbb{Q}\}$. Kuna minimaalse polünoomi polünoomi pealiikme kordaja peab jätkuvalt olema 1, siis võtame $c_1 = 1$ ja saame otsitud polünoomi

$$g(X) = X^4 - 2X^2 + 9 \in \mathbb{Q}[X].$$

Võib kontrollida, et polünoomid f ja g on mõlemad taandumatud vastavates ringides $\mathbb{R}[X]$ ja $\mathbb{Q}[X]$ ning seetõttu ka minimaalsed tänu lemmale 2. $\square$

Ülesanne* VII.9. Tõestada, et polünoomi $X^n - 1$, $n > 1$, lahutuskorpus üle $\mathbb{Q}$ on korpuse $\mathbb{Q}$ $\varphi(n)$. järku laiend (φ on Euleri φ -funktsioon).

Praktikum VIII Maatriksi Jordani normaalkuju

Ülesanne VIII.1. Leidke järgmiste maatriksite Jordani normaalkujud:

$$A = \begin{pmatrix} 3 & -1 & 1 & -7 \\ 9 & -3 & -7 & -1 \\ 0 & 0 & 4 & -8 \\ 0 & 0 & 2 & -4 \end{pmatrix}, \quad B = \begin{pmatrix} 4 & 1 & 1 & 1 \\ -1 & 2 & -1 & -1 \\ 6 & 1 & -1 & 1 \\ -6 & -1 & 4 & 2 \end{pmatrix},$$

$$C = \begin{pmatrix} 0 & -3 & 0 & 3 \\ -2 & -7 & 0 & 13 \\ 0 & -3 & 0 & 3 \\ -1 & -4 & 0 & 7 \end{pmatrix}, \quad D = \begin{pmatrix} 5 & 1 & -1 & -1 \\ 1 & 5 & -1 & -1 \\ 1 & 1 & 3 & -1 \\ 1 & 1 & -1 & 3 \end{pmatrix}.$$

Kas nende maatriksite hulgas leidub ka sarnaseid maatrikseid?

Lahendus: (Siin ülesandes kasutame algoritmi loengukonspekti [1] lk 66 all.)

A: Leiame maatriksi A omaväärtused. Selleks peame leidma maatriksi A karakteristliku polünoomi juured (kuna selles determinandis on piisavalt nulle saame ta leida otse determinandi definitsioonist):

$$\begin{aligned} 0 = \det(A - \lambda E) &= \begin{vmatrix} 3 - \lambda & -1 & 1 & -7 \\ 9 & -3 - \lambda & -7 & -1 \\ 0 & 0 & 4 - \lambda & -8 \\ 0 & 0 & 2 & -4 - \lambda \end{vmatrix} = \\ &= (3 - \lambda)(-3 - \lambda)(4 - \lambda)(-4 - \lambda) - (3 - \lambda)(-3 - \lambda)2(-8) - 9(-1)(4 - \lambda)(-4 - \lambda) + \\ &\quad + 9(-1)2(-8) = \\ &= (\lambda^4 - 25\lambda^2 + 144) - (144 - 16\lambda^2) - (144 - 9\lambda^2) + 144 = \lambda^4. \end{aligned}$$

Seega ainus omaväärtus $\lambda = 0$. Vastavalt algoritmile leiame arvud

$$u_j = \text{rank}((A - \lambda E)^j) = \text{rank}(A^j), \quad j = 1, 2, 3, 4.$$

Arvutame

$$\begin{pmatrix} 3 & -1 & 1 & -7 \\ 9 & -3 & -7 & -1 \\ 0 & 0 & 4 & -8 \\ 0 & 0 & 2 & -4 \end{pmatrix} - 3I \rightarrow \begin{pmatrix} 3 & -1 & 1 & -7 \\ 0 & 0 & -10 & 20 \\ 0 & 0 & 4 & -8 \\ 0 & 0 & 2 & -4 \end{pmatrix} \xrightarrow{\begin{matrix} +5IV \\ -2IV \end{matrix}} \begin{pmatrix} 3 & -1 & 1 & -7 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -4 \end{pmatrix}.$$

Seega $\text{rank}(A) = 2$.

Märkame, et $A^2 = 0$, mistõttu A on nilpotentne maatriks indeksiga 2. Tänu sellele võiks determinandi arvutamise ka vahele jätta ning järeldada nilpotentsusest, et ainus omaväärtus on $\lambda = 0$. Vastavalt teoreemile 3.22 saame lineaarvõrrandisüsteemi

$$\begin{cases} s_1 + s_2 = 4 - 2 = 2, \\ s_2 = 2. \end{cases}$$

Seega $s_2 = 2$ ehk Jordani normaalkujus on 2 Jordani kasti $J_2(0)$, mistõttu maatriksi A Jordani normaalkuju on

$$J(A) = \text{diag}(J_2(0), J_2(0)) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

B: Leiame maatriksi B omaväärtused. Taaskord arvutame neid kui karakteristliku polünoomi juuri:

$$\begin{aligned} 0 = \det(B - \lambda E) &= \begin{vmatrix} 4 - \lambda & 1 & 1 & 1 \\ -1 & 2 - \lambda & -1 & -1 \\ 6 & 1 & -1 - \lambda & 1 \\ -6 & -1 & 4 & 2 - \lambda \end{vmatrix} \begin{matrix} +\text{I} \\ +\text{IV} \end{matrix} = \\ &= \begin{vmatrix} 4 - \lambda & 1 & 1 & 1 \\ 3 - \lambda & 3 - \lambda & 0 & 0 \\ 0 & 0 & 3 - \lambda & 3 - \lambda \\ -6 & -1 & 4 & 2 - \lambda \end{vmatrix} = \\ &= -(3 - \lambda) \begin{vmatrix} 1 & 1 & 1 \\ 0 & 3 - \lambda & 3 - \lambda \\ -1 & 4 & 2 - \lambda \end{vmatrix} + (3 - \lambda) \begin{vmatrix} 4 - \lambda & 1 & 1 \\ 0 & 3 - \lambda & 3 - \lambda \\ -6 & 4 & 2 - \lambda \end{vmatrix} = \\ &= (3 - \lambda) \left(\begin{vmatrix} 4 - \lambda & 1 & 1 \\ 0 & 3 - \lambda & 3 - \lambda \\ -6 & 4 & 2 - \lambda \end{vmatrix} - \begin{vmatrix} 1 & 1 & 1 \\ 0 & 3 - \lambda & 3 - \lambda \\ -1 & 4 & 2 - \lambda \end{vmatrix} \right). \end{aligned}$$

Eraldi arvutades

$$\begin{aligned} \begin{vmatrix} 4 - \lambda & 1 & 1 \\ 0 & 3 - \lambda & 3 - \lambda \\ -6 & 4 & 2 - \lambda \end{vmatrix} &= (3 - \lambda) \left(\begin{vmatrix} 4 - \lambda & 1 \\ -6 & 2 - \lambda \end{vmatrix} - \begin{vmatrix} 4 - \lambda & 1 \\ -6 & 4 \end{vmatrix} \right) = \\ &= (3 - \lambda)((\lambda^2 - 6\lambda + 14) - (22 - 4\lambda)) = (3 - \lambda)(\lambda^2 - 2\lambda - 8), \\ \begin{vmatrix} 1 & 1 & 1 \\ 0 & 3 - \lambda & 3 - \lambda \\ -1 & 4 & 2 - \lambda \end{vmatrix} &= (3 - \lambda) \left(\begin{vmatrix} 1 & 1 \\ -1 & 2 - \lambda \end{vmatrix} - \begin{vmatrix} 1 & 1 \\ -1 & 4 \end{vmatrix} \right) = (3 - \lambda)((3 - \lambda) - 5) = \\ &= (3 - \lambda)(-2 - \lambda). \end{aligned}$$

Jätkates nüüd karakteristliku polünoomi juurte arvutamisega

$$0 = \det(B - \lambda E) = (3 - \lambda)^2(\lambda^2 - 2\lambda - 8 + 2 + \lambda) = (3 - \lambda)^2(\lambda^2 - \lambda - 6) = (\lambda - 3)^3(\lambda + 2).$$

Seega on maatriksi B omaväärtused $\lambda_1 = 3$ (algebraalse kordsusega 3) ja $\lambda_2 = -2$ (algebraalse kordsusega 1). (Determinandi arvutamine on eelnevalt tehtud selliselt, et vältida 4. astme võrrandi lahendamist.)

Vaatleme omaväärtust $\lambda_1 = 3$ ja arvutame talle vastava maatriksi

$$B_1 = B - 3E = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 6 & 1 & -4 & 1 \\ -6 & -1 & 4 & -1 \end{pmatrix} \begin{matrix} +I \\ \\ +III \\ \end{matrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 6 & 1 & -4 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} \\ -I \\ \\ \end{matrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 5 & 0 & -5 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Seega $u_1 = \text{rank}(B_1) = 2$. Edasi vaatleme eelneva maatriksi ruutu

$$B_1^2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 6 & 1 & -4 & 1 \\ -6 & -1 & 4 & -1 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -25 & 0 & 25 & 0 \\ 25 & 0 & -25 & 0 \end{pmatrix} \begin{matrix} \\ \\ +III \\ \end{matrix} \rightarrow \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -25 & 0 & 25 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Seega $u_2 = \text{rank}(B_1^2) = 1$. Kõrgemaid astmeid pole vaja vaadata kuna meil on 2 omaväärtust. Siit saame lineaarvõrrandisüsteemi

$$\begin{cases} s_1 + s_2 &= 4 - 2 = 2, \\ s_2 &= 2 - 1 = 1, \end{cases} \implies \begin{cases} s_1 = 1, \\ s_2 = 1. \end{cases}$$

Siit näeme, et Jordani normaalkujus leidub 1 Jordani blokk $J_1(3)$ ja 1 blokk $J_2(3)$. Vaatleme nüüd omaväärtust $\lambda_2 = -2$ ja arvutame talle vastava maatriksi

$$B_2 = B + 2E = \begin{pmatrix} 6 & 1 & 1 & 1 \\ -1 & 4 & -1 & -1 \\ 6 & 1 & 1 & 1 \\ -6 & -1 & 4 & 4 \end{pmatrix} \begin{matrix} +I \\ \\ -I \\ +I \end{matrix} \rightarrow \begin{pmatrix} 6 & 1 & 1 & 1 \\ 5 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 5 \end{pmatrix} \begin{matrix} \\ -I \\ \\ +I \end{matrix}.$$

Seega $v_1 = \text{rank}(B_2) = 3$. Vaatleme nüüd ka eelneva maatriksi ruutu

$$B_2^2 = \begin{pmatrix} 6 & 1 & 1 & 1 \\ -1 & 4 & -1 & -1 \\ 6 & 1 & 1 & 1 \\ -6 & -1 & 4 & 4 \end{pmatrix}^2 = 5 \begin{pmatrix} 7 & 2 & 2 & 2 \\ -2 & 3 & -2 & -2 \\ 7 & 2 & 2 & 2 \\ -7 & -2 & 3 & 3 \end{pmatrix} \begin{matrix} +I \\ \\ -I \\ +I \end{matrix} \rightarrow 5 \begin{pmatrix} 7 & 2 & 2 & 2 \\ 5 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 5 \end{pmatrix}$$

Seega $v_2 = \text{rank}(B_2^2) = 3$. Siit saame võrrandisüsteemi

$$\begin{cases} s_1 + s_2 &= 4 - 3 = 1, \\ s_2 &= 3 - 3 = 0, \end{cases} \implies \begin{cases} s_1 = 1, \\ s_2 = 0. \end{cases}$$

Siit loeme välja, et Jordani normaalkujus on üks blokk $J_1(-2)$. Kokkuvõttes saame nüüd maatriksi B Jordani normaalkuju välja kirjutada

$$J(B) = \text{diag}(J_2(3), J_1(3), J_1(-2)) = \begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}.$$

C: Leiame matriksi C omaväärtused, arvutades taaskord matriksi C karakteristliku polünoomi juured:

$$\begin{aligned} 0 = \det(C - \lambda E) &= \begin{vmatrix} -\lambda & -3 & 0 & 3 \\ -2 & -7-\lambda & 0 & 13 \\ 0 & -3 & -\lambda & 3 \\ -1 & -4 & 0 & 7-\lambda \end{vmatrix} = -\lambda \begin{vmatrix} -\lambda & -3 & 3 \\ -2 & -7-\lambda & 13 \\ -1 & -4 & 7-\lambda \end{vmatrix} = \\ &= -\lambda \left(-\lambda \begin{vmatrix} -7-\lambda & 13 \\ -4 & 7-\lambda \end{vmatrix} + 3 \begin{vmatrix} -2 & 13 \\ -1 & 7-\lambda \end{vmatrix} + 3 \begin{vmatrix} -2 & -7-\lambda \\ -1 & -4 \end{vmatrix} \right) = \\ &= -\lambda(-\lambda(\lambda^2 + 3) + 3(2\lambda - 1) + 3(1 - \lambda)) = -\lambda(-\lambda(\lambda^2 + 3) + 3\lambda) = \lambda^4. \end{aligned}$$

Nagu näha, on matriksi C ainus omaväärtus $\lambda = 0$. (Tegelikult on C nilpotentne matriks indeksiga 3.) Arvutame matriksi C astmete astakud

$$A = \begin{pmatrix} 0 & -3 & 0 & 3 \\ -2 & -7 & 0 & 13 \\ 0 & -3 & 0 & 3 \\ -1 & -4 & 0 & 7 \end{pmatrix} \xrightarrow{+I} \begin{pmatrix} 0 & -3 & 0 & 3 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ -1 & -4 & 0 & 7 \end{pmatrix} \xrightarrow{+3II} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ -1 & -4 & 0 & 7 \end{pmatrix},$$

$$A^2 = \begin{pmatrix} 3 & 9 & 0 & -18 \\ 1 & 3 & 0 & -6 \\ 3 & 9 & 0 & -18 \\ 1 & 3 & 0 & -6 \end{pmatrix} \xrightarrow{-I} \begin{pmatrix} 3 & 9 & 0 & -18 \\ 0 & 0 & 0 & 0 \\ 3 & 9 & 0 & -18 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{-3II} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & -6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A^3 = 0.$$

Seega $u_1 = \text{rank}(A) = 2$, $u_2 = \text{rank}(A^2) = 1$.

$$\begin{cases} s_1 + s_2 + s_3 &= 4 - 2 = 2, \\ s_2 + s_3 &= 2 - 1 = 1, \\ s_3 &= 1. \end{cases} \implies \begin{cases} s_1 = 1, \\ s_2 = 0, \\ s_3 = 1. \end{cases}$$

Järelikult on matriksi C Jordani normaalkujus üks Jordani blokk $J_3(0)$ ja üks blokk $J_1(0)$. Kokkuvõttes saame matriksi normaalkuju välja kirjutada

$$J(C) = \text{diag}(J_3(0), J_1(0)) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

D: Taaskord leiame matriksi D omaväärtused arvutades tema karakteristliku polünoomi juured:

$$0 = \det(D - \lambda E) = \begin{vmatrix} 5-\lambda & 1 & -1 & -1 \\ 1 & 5-\lambda & -1 & -1 \\ 1 & 1 & 3-\lambda & -1 \\ 1 & 1 & -1 & 3-\lambda \end{vmatrix} \xrightarrow{-II} \begin{vmatrix} 5-\lambda & 1 & -1 & -1 \\ 0 & 4-\lambda & 0 & 0 \\ 0 & 0 & 2-\lambda & -2 \\ 0 & 0 & -2 & 2-\lambda \end{vmatrix} \xrightarrow{-IV} \begin{vmatrix} 5-\lambda & 1 & -1 & -1 \\ 0 & 4-\lambda & 0 & 0 \\ 0 & 0 & 2-\lambda & -2 \\ 0 & 0 & 0 & 0 \end{vmatrix} =$$

$$\begin{aligned}
&= \begin{vmatrix} 4-\lambda & -4+\lambda & 0 & 0 \\ 1 & 5-\lambda & -1 & -1 \\ 0 & 0 & 4-\lambda & -4+\lambda \\ 1 & 1 & -1 & 3-\lambda \end{vmatrix} - IV = \begin{vmatrix} 4-\lambda & -4+\lambda & 0 & 0 \\ 0 & 4-\lambda & 0 & -4+\lambda \\ 0 & 0 & 4-\lambda & -4+\lambda \\ 1 & 1 & -1 & 3-\lambda \end{vmatrix} = \\
&= (4-\lambda) \begin{vmatrix} 4-\lambda & 0 & -4+\lambda \\ 0 & 4-\lambda & -4+\lambda \\ 1 & -1 & 3-\lambda \end{vmatrix} + (4-\lambda) \begin{vmatrix} 0 & 0 & -4+\lambda \\ 0 & 4-\lambda & -4+\lambda \\ 1 & -1 & 3-\lambda \end{vmatrix} = \\
&= (4-\lambda)((4-\lambda)^2(3-\lambda) - (4-\lambda)^2 - (4-\lambda)^2) + (4-\lambda)^2 = (4-\lambda)^4.
\end{aligned}$$

Järelikult on maatriksi D omaväärtus $\lambda = 4$ (algebraalse kordsusega 4). Leiame vastavad astakud:

$$A_1 = A - 4E = \begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} - I = \begin{pmatrix} 1 & 1 & -1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \implies u_1 = \text{rank}(A_1) = 1.$$

Kuna $A_1^2 = 0$, siis $u_2 = 0$. Siit saame lineaarvõrrandite süsteemi

$$\begin{cases} s_1 + s_2 = 4 - 1 = 3, \\ s_2 = 1, \end{cases} \implies \begin{cases} s_1 = 2, \\ s_2 = 1. \end{cases}$$

Siit on näha, et maatriksi D Jordani normaalkujus on 2 Jordani blokki $J_1(4)$ ja 1 blokk $J_2(4)$. Kokkuvõttes saame nüüd välja kirjutada maatriksi D Jordani normaalkuju

$$J(D) = \text{diag}(J_2(4), J_1(4), J_1(4)) = \begin{pmatrix} 4 & 1 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

Kuna sarnastel maatriksitel peavad olema samad karakteristikud polünoomid, siis võiksid maatriksid A ja C olla sarnased. Kuid kuna maatriksi A minimaalne polünoom on X^2 , aga maatriksi C minimaalne polünoom on X^3 , siis nad ei ole siiski sarnased. $\square$

Igaks juhuks mainin siin, et maatriksi (lineaarteisenduse) Jordani normaalkuju on määratud Jordani blokkide järjekorra täpsuseni.

Ülesanne VIII.2. Leidke maatriksi $(J_m(a))^2$ Jordani normaalkuju, kui $a \neq 0$.

Lahendus: Olgu $m \in \mathbb{N}$, $a \neq 0$ ja vaatleme Jordani blokki

$$J_m(a) = \begin{pmatrix} a & 1 & 0 & \dots & 0 \\ 0 & a & 1 & \dots & 0 \\ 0 & 0 & a & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a \end{pmatrix} \in \text{Mat}_m(\mathbb{C}).$$

Arvutame

$$(J_m(a))^2 = \begin{pmatrix} a^2 & 2a & 1 & 0 & \dots & 0 \\ 0 & a^2 & 2a & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & a^2 \end{pmatrix}$$

Leiame ma maatriksi $(J_m(a))^2$ omaväärtused ikka karakteristliku polünoomi abil

$$\begin{aligned} 0 = \det((J_m(a))^2 - \lambda E) &= \begin{vmatrix} a^2 - \lambda & 2a & 1 & 0 & \dots & 0 \\ 0 & a^2 - \lambda & 2a & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & a^2 - \lambda \end{vmatrix} = \\ &= (a^2 - \lambda) \begin{vmatrix} a^2 - \lambda & 2a & \dots & 0 \\ 0 & a^2 - \lambda & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a^2 - \lambda \end{vmatrix} - 2a \begin{vmatrix} 0 & 2a & \dots & 0 \\ 0 & a^2 - \lambda & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a^2 - \lambda \end{vmatrix} + \begin{vmatrix} 0 & a^2 - \lambda & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a^2 - \lambda \end{vmatrix} = \\ &= (a^2 - \lambda) \begin{vmatrix} a^2 - \lambda & 2a & 1 & 0 & \dots & 0 \\ 0 & a^2 - \lambda & 2a & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & a^2 - \lambda \end{vmatrix} = (a^2 - \lambda)^m. \end{aligned}$$

Järelikult on maatriksi $(J_m(a))^2$ ainsaks omaväärtuseks a^2 . Tähistame $B = J_m(a))^2 - a^2 E$ ja leiame arvud

$$u_j = \text{rank}((J_m(a))^2 - a^2 E)^j = \text{rank}(B^j),$$

kus $j \in \{1, \dots, m\}$. Selleks

$$\begin{aligned} B &= \begin{pmatrix} 0 & 2a & 1 & 0 & \dots & 0 \\ 0 & 0 & 2a & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}, & u_1 &= m - 1, \\ B^2 &= \begin{pmatrix} 0 & 2a & 1 & 0 & \dots & 0 \\ 0 & 0 & 2a & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 & 4a^2 & 4a & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 4a^2 & 4a & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}, & u_2 &= m - 2, \\ &\dots\dots\dots \\ B^{m-1} &= \begin{pmatrix} 0 & 2a & 1 & 0 & \dots & 0 \\ 0 & 0 & 2a & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}^m = \begin{pmatrix} 0 & \dots & 0 & (2a)^{m-1} \\ 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 \end{pmatrix}, & u_{m-1} &= 1, \\ B^m &= (0), & u_m &= 0. \end{aligned}$$

Siit saame lineaarvõrrandi süsteemi

$$\begin{cases} s_1 + s_2 + \dots + s_m &= m - (m - 1) = 1, \\ s_2 + \dots + s_m &= m - 1 - (m - 2) = 1, \\ \dots\dots\dots & \\ s_m &= u_{m-1} - u_m = 1, \end{cases}$$

järelikult $s_m = 1$ ja $s_1 = \dots = s_{m-1} = 0$. Seega oleme saanud, et Jordani normaalkuju koosneb ühest m -mndat järku Jordani kastist $J_m(a^2)$, mistõttu

$$J((J_m(a))^2) = J_m(a^2) = \begin{pmatrix} a^2 & 1 & 0 & \dots & 0 \\ 0 & a^2 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a^2 \end{pmatrix},$$

millega oleme soovitud Jordani normaalkuju kätte saanud. $\square$

Nüüd annan (suhteliselt) lihtsa algoritmi, kuidas lihtsustada lineaarteisenduse φ kanoonilise baasi leidmist üldistatud omavektori abil. Tähistame lineaarteisenduse φ maatriksit $A := A_\varphi$. Olgu λ lineaarteisenduse ψ omaväärtus algebraalse kordsusega n , s.t. $\det(A - \lambda E) = p(X)(\lambda - X)^n$, kus p on mingi polünoom. Tähistame $\psi_\lambda := \varphi - \lambda \text{id}$. Leiame vektori $w \in \text{Ker}(\psi_\lambda)^n$, mille korral $(\psi_\lambda)^{n-1}(w) \neq 0$. Seega kehtib $(A - \lambda E)^n w = 0$ ja $(A - \lambda E)^{n-1} w \neq 0$. Sellist vektorit w nimetatakse omaväärtusele λ vastavaks *üldistatud omavektoriks*. Nüüd avaldub kujutuse ψ_λ kanooniline baas kujul

$$\mathcal{B} = \{w, \psi_\lambda(w), \dots, \psi_\lambda^{n-1}(w)\} = \{w, (A - \lambda E)w, \dots, (A - \lambda E)^{n-1}w\}. \quad (4)$$

Järgmise ülesande idee seisneb tähelepanekus, et

$$A^n = (CJ(A)C^{-1})^n = (CJ(A)C^{-1})(CJ(A)C^{-1}) \dots (CJ(A)C^{-1}) = C(J(A))^n C^{-1}. \quad (5)$$

Eelnev valem on ka üks põhilisi põhjuseid, miks maatriksi Jordani normaalkujust räägitakse. Kuna Jordani maatriksitega on tehteid märgatavalt lihtsam teha, kui suvaliste maatriksitega.

Ülesanne VIII.3. Leida A^{2020} , kus

$$A = \begin{pmatrix} -2 & 5 & 9 \\ 1 & -20 & -22 \\ -1 & 15 & 17 \end{pmatrix}.$$

Lahendus: Taaskord on meil mõistlik üle minna maatriksile A vastava lineaarteisenduse $\varphi: \mathbb{R}^3 \rightarrow \mathbb{R}^3$, $(x, y, z) \mapsto (-2x + 5y + 9z, x - 20y - 22z, -x + 15y + 17z)$ kanoonilisele baasile kuna seal on võimalik märkimisväärselt lihtsamalt arvutada otsitud aste (seekord algoritmiga loengukonspekti [1] lk 65–66). Leiame maatriksi A omaväärtused, arvutades maatriksi A karakteristliku polünoomi juured:

$$0 = \det(A - \lambda E) = \begin{vmatrix} -2 - \lambda & 5 & 9 \\ 1 & -20 - \lambda & -22 \\ -1 & 15 & 17 - \lambda \end{vmatrix} + \text{III} = \begin{vmatrix} -2 - \lambda & 5 & 9 \\ 0 & -5 - \lambda & -5 - \lambda \\ -1 & 15 & 17 - \lambda \end{vmatrix} - 3\text{I} =$$

$$\begin{aligned}
&= \begin{vmatrix} -2-\lambda & 5 & 9 \\ 0 & -5-\lambda & -5-\lambda \\ 3\lambda+5 & 0 & -10-\lambda \end{vmatrix} = (5+\lambda) \left(\begin{vmatrix} -2-\lambda & 5 \\ 3\lambda+5 & 0 \end{vmatrix} - \begin{vmatrix} -2-\lambda & 9 \\ 3\lambda+5 & -10-\lambda \end{vmatrix} \right) = \\
&= (5+\lambda)(-(15\lambda+25) - (\lambda^2 - 15\lambda - 25)) = -\lambda^2(5+\lambda).
\end{aligned}$$

Seega maatriksi A omaväärtused on $\lambda_1 = 0$ (algebraalse kordsusega 2) ja $\lambda_2 = -5$.

Vaatleme omaväärtust $\lambda_1 = 0$. Tähistame $U_1 = \text{Ker } \varphi^2$, siis on kujutus $\varphi|_{U_1}: U_1 \rightarrow \mathbb{R}^3$ nilpotentne lineaarteisendus indeksiga 2. Otsime teisenduse $\varphi|_{U_1}$ kanoonilise baasi $\mathcal{B}_1$ (ruumis U_1). Selleks arvutame kõigepealt

$$A^2 = 25 \begin{pmatrix} 0 & 1 & 1 \\ 0 & 3 & 3 \\ 0 & -2 & -2 \end{pmatrix} \begin{matrix} -3I \\ +2I \end{matrix} \rightarrow \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Seega $\text{rank}(A^2) = 1$, millest saame, et $\dim U_1 = \dim \text{Ker } \varphi^2 = 3 - 1 = 2$ ning kergesti saame $U_1 = \text{span}\{(1, 0, 0), (0, 1, -1)\}$. Võtame vektori $(1, 0, 0)$ ja rakendame talle kujutust φ

$$\varphi(1, 0, 0) = (-2, 1, -1).$$

Kuna vektor $(-2, 1, -1)$ on nullist erinev, siis moodustab vektorite paar $\mathcal{B}_1 = \{(-2, 1, -1), (1, 0, 0)\}$ teisenduse $\varphi|_{U_1}$ kanoonilise baasi (rida (4)).

Vaatleme omaväärtust $\lambda_2 = -5$. Tähistame $A_2 = A + 5E$, millest saame

$$A_2 = \begin{pmatrix} 3 & 5 & 9 \\ 1 & -15 & -22 \\ -1 & 15 & 22 \end{pmatrix} \begin{matrix} \\ +II \end{matrix} \rightarrow \begin{pmatrix} 3 & 5 & 9 \\ 1 & -15 & -22 \\ 0 & 0 & 0 \end{pmatrix} \begin{matrix} -3II \\ \\ \end{matrix} \rightarrow \begin{pmatrix} 0 & 50 & 75 \\ 1 & -15 & -22 \\ 0 & 0 & 0 \end{pmatrix}.$$

Olgu maatriksile A_2 vastav lineaarteisendus $\psi: \mathbb{R}^3 \rightarrow \mathbb{R}^3$, $(x, y, z) \mapsto (3x + 5y + 9z, x - 15y - 22z, -x + 15y + 22z)$ ning tähistame $U_2 = \text{Ker } \psi$. Ruumi U_2 kirjeldab lineaarvõrrandite süsteemi

$$\begin{cases} 50y + 75z = 0 \\ x - 15y - 22z = 0 \end{cases} \implies \begin{cases} 2y + 3z = 0 \\ x = 15y + 22z \end{cases} \implies \begin{cases} y = -\frac{3}{2}z \\ x = (22 - 15\frac{3}{2})z = -\frac{1}{2}z \end{cases} \implies \begin{cases} x = -\frac{1}{2}c \\ y = -\frac{3}{2}c \\ z = c \end{cases}.$$

Siit saame ruumi U_2 baasi $\mathcal{B}_2 = \{(-1, -3, 2)\}$.

Võtame ühendi $\mathcal{B}_1 \cup \mathcal{B}_2 = \mathcal{B} = \{(-2, 1, -1), (1, 0, 0), (-1, -3, 2)\}$, mis ongi lineaarkujutuse φ kanooniline baas. Leiame siit üleminekumaatriksi

$$C = \begin{pmatrix} -2 & 1 & -1 \\ 1 & 0 & -3 \\ -1 & 0 & 2 \end{pmatrix}, \quad C^{-1} = \frac{1}{-1} \begin{pmatrix} 0 & -1 & 0 \\ 2 & 5 & 1 \\ 3 & 7 & 1 \end{pmatrix}^T = \begin{pmatrix} 0 & -2 & -3 \\ 1 & -5 & -7 \\ 0 & -1 & -1 \end{pmatrix}.$$

Nüüd saame välja arvutada maatriksi A Jordani normaalkuju.

$$J(A) = C^{-1}AC = \begin{pmatrix} 0 & -2 & -3 \\ 1 & -5 & -7 \\ 0 & -1 & -1 \end{pmatrix} \begin{pmatrix} -2 & 5 & 9 \\ 1 & -20 & -22 \\ -1 & 15 & 17 \end{pmatrix} \begin{pmatrix} -2 & 1 & -1 \\ 1 & 0 & -3 \\ -1 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -5 \end{pmatrix}.$$

Arvutame Jordani normaalkuju $J(A)$ 2020. astme

$$(J(A))^{2020} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -5 \end{pmatrix}^{2020} = \left(\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -5 \end{pmatrix}^2 \right)^{1010} = \left(5^2 \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right)^{1010} = 5^{2020} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Lähme tagasi maatriksi A peale

$$A^{2020} = C(J(A))^{2020}C^{-1} = 5^{2020} \begin{pmatrix} -2 & 1 & -1 \\ 1 & 0 & -3 \\ -1 & 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -2 & -3 \\ 1 & -5 & -7 \\ 0 & -1 & -1 \end{pmatrix} = 5^{2020} \begin{pmatrix} 0 & 1 & 1 \\ 0 & 3 & 3 \\ 0 & -2 & -2 \end{pmatrix}$$

ning sellega olemegi leidnud soovitud astme. $\square$

Analüüsist on teada, et eksponentfunktsiooni e^x Tayloriga avaldub kujul

$$e^x = \exp(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!}.$$

Asendades siin muutuja x mingi ruutmaatriksiga $A \in \text{Mat}_n(R)$, saame maatriksi A eksponentmaatriksi $\exp(A)$. Sõnastan siinkohal ühe lemma, mida järgmises ülesandes vaja läheb.

Lemma 3. Kui maatriksid $X, Y \in \text{Mat}_n(\mathbb{C})$ kommuteeruvad, siis kehtib

$$\exp(X + Y) = (\exp X) \cdot (\exp Y).$$

Selle lemma tõestus taandub asjaolule, et kui maatriksid X ja Y kommuteeruvad, siis kehtib Newtoni binoomvalemiga analoogiline valem.

Enne järgmise ülesande juurde pöördumist tõestame valemi (5) abil järgneva valemi

$$\begin{aligned} \exp(A) &= \exp(CJ(A)C^{-1}) = \sum_{k=0}^{\infty} \frac{1}{k!} (CJ(A)C^{-1})^k = \sum_{k=0}^{\infty} \frac{1}{k!} C(J(A))^k C^{-1} = \\ &= C \left(\sum_{k=0}^{\infty} \frac{1}{k!} (J(A))^k \right) C^{-1} = C \exp(J(A)) C^{-1}. \end{aligned} \quad (6)$$

Ülesanne VIII.4. Kasutades Jordani normaalkuju ja eksponentfunktsiooni Tayloriga leidke

$$\exp \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix}.$$

Lahendus: Teame, et maatriks $A = \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix}$ vastab lineaarteisendusele $\varphi: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $(x, y) \mapsto (3x - y, x + y)$. Leiame teisenduse φ kanoonilise baasi (algoritriga loengukonspekti [1] lk 55 – 56). Kõigepealt leiame maatriksi A omaväärtused

$$0 = \det(A - \lambda E) = \begin{vmatrix} 3 - \lambda & -1 \\ 1 & 1 - \lambda \end{vmatrix} = (3 - \lambda)(1 - \lambda) + 1 = 4 - 4\lambda + \lambda^2 = (\lambda - 2)^2.$$

Seega maatriksi A omaväärtus on $\lambda = 2$. Tähistame maatriksi $A_1 = A - 2E$. Maatriks A_1 on nilpotentne maatriks. Leiame tema indeksi:

$$A_1 = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}, \quad A_1^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

mistõttu nilpotentse maatriksi A_1 indeks on 2. Maatriksile A_1 vastab lineaarteisendus $\psi: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $(x, y) \mapsto (x - y, x - y)$. Vastavalt algoritmile enne rida (4) on vaja leida vektor $w \in \text{Ker } \varphi^2 = \mathbb{R}^2$ nii, et $\varphi(w) \neq 0$. Valime näiteks vektori $w = (1, 0)$. Arvutame

$$\psi((1, 0)) = (1, 1).$$

Paar $\mathcal{B} = \{(1, 1), (1, 0)\}$ on kujutuse ψ kanooniline baas, tema üleminekumaatriks on

$$C = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad C^{-1} = \frac{1}{-1} \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}^T = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}.$$

Esitame maatriksi A baasil $\mathcal{B}$ (ehk esitame tema Jordani normaalkujul $J(A)$):

$$J(A) = C^{-1}AC = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Nüüd arvutame maatriksi $J(A)$ liidetavate eksponentmaatriksid

$$\begin{aligned} \exp \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} &= \sum_{k=0}^{\infty} \frac{1}{k!} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}^k = \sum_{k=0}^{\infty} \frac{1}{k!} \begin{pmatrix} 2^k & 0 \\ 0 & 2^k \end{pmatrix} = \begin{pmatrix} e^2 & 0 \\ 0 & e^2 \end{pmatrix}, \\ \exp \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} &= \sum_{k=0}^{\infty} \frac{1}{k!} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \sum_{k=2}^{\infty} \frac{1}{k!} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^k = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Paneme tähele ka, et

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Kuna need maatriksid kommuteeruvad, siis lemmat 3 kasutades, saame

$$\exp(J(A)) = \exp \left(\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right) = \exp \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \cdot \exp \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} e^2 & 0 \\ 0 & e^2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} e^2 & e^2 \\ 0 & e^2 \end{pmatrix}.$$

Nüüd viime maatriksi $\exp(J(A))$ tagasi esialgsesse baasi, millega saamegi soovitud maatriksi kätte

$$\exp(A) = C \exp(J(A)) C^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} e^2 & e^2 \\ 0 & e^2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 2e^2 & -e^2 \\ e^2 & 0 \end{pmatrix},$$

mis on meie otsitud eksponentmaatriks. □

Ülesanne VIII.5. Leidke idempotentse maatriksi (s.o. maatriksi, mille korral $A^2 = A$) Jordani normaalkuju.

Lahendus: Olgu $A \in \text{Mat}_n(\mathbb{C})$ idempotentne maatriks ehk $A^2 = A$. Leiame maatriksi A omaväärtuse λ . Vastavalt definitsioonile on λ maatriksi A omaväärtus, kui leidub nullvektorist erinev vektor $v \in \text{Mat}_{n,1}(\mathbb{C})$ nii, et $Av = \lambda v$. Kehtib

$$\lambda v = Av = A^2 v = \lambda^2 v \implies (\lambda^2 - \lambda)v = 0 \implies \lambda^2 = \lambda,$$

millest $\lambda \in \{0, 1\}$. Järelikult võivad idempotentse maatriksi omaväärtused olla vaid 1 ja/või 0.

Kuna mingi pööratava maatriksi C korral $A = CJ(A)C^{-1}$, siis kehtib

$$A = A^2 = (CJ(A)C^{-1})^2 = CJ(A)C^{-1}CJ(A)C^{-1} = C(J(A))^2C^{-1}.$$

Järelikult $(J(A))^2 = J(A)$ ehk Jordani normaalkuju $J(A)$ on samuti idempotentne. Lihtne on kontrollida, et Jordani normaalkuju $J(A)$ on idempotentne parajasti siis, kui $J(A)$ on diagonaalne ehk koosneb vaid esimest järku Jordani blokkidest. Kuna A omaväärtused on 1 ja/või 0, siis avaldub Jordani normaalkuju

$$J(A) = \text{diag}(\underbrace{0, \dots, 0}_k, \underbrace{1, \dots, 1}_h),$$

kus $k + h = n$. □

Ülesanne VIII.6. Tooge näide kahest maatriksist, mis ei ole sarnased, aga mille karakteristikud polünoomid on võrdsed.

Lahendus: Näideteks sobivad näiteks kaks nilpotentset maatriksit $A, B \in \text{Mat}_n(K)$, mille indeksid on erinevad. Näiteks maatriksid A ja C esimesest ülesandest.

Siiski leidub ka mitte-nilpotentseid näiteid. Maatriksid, millel on samad omaväärtused, aga Jordani normaalkujud, mis erinevad Jordani blokkide arvult ja astmelt. (Kui Jordani normaalkujud erinevad vaid Jordani blokkide järjekorral, siis on tegemist sarnaste maatriksitega.) Näiteks

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

on sellised maatriksid. □

Ülesanne VIII.7. Olgu A regulaarne maatriks, mille Jordani normaalkuju on $J(A)$. Milline on maatriksi A^{-1} Jordani normaalkuju?

Lahendus: Olgu A regulaarne maatriks, siis leidub regulaarne C nii, et $A = CJ(A)C^{-1}$. Paneme tähele, et

$$A^{-1} = (CJ(A)C^{-1})^{-1} = (C^{-1})^{-1}(J(A))^{-1}C^{-1} = C(J(A))^{-1}C^{-1}.$$

Seega maatriksi A^{-1} Jordani normaalkuju on maatriksi $(J(A))^{-1}$ Jordani normaalkuju.

Vaatleme Jordani blokki $J_m(\lambda)$. Ilmselt on λ maatriksi $J_m(\lambda)$ omaväärtus, mistõttu leidub vektor v , mille korral $J_m(\lambda)v = \lambda v$. Paneme tähele, et

$$J_m(\lambda)(J_m(\lambda))^{-1}v = \lambda v = v,$$

millest saame, et $x = \frac{1}{\lambda}$ on matriksi $(J_m(\lambda))^{-1}$ omaväärtus. Siit järeldame, et

$$\text{Ker}(J_m(\lambda) - \lambda E) = \text{Ker} \left((J_m(\lambda))^{-1} - \frac{1}{\lambda} E \right),$$

millest saame $\dim(\text{Ker}((J_m(\lambda))^{-1} - \frac{1}{\lambda} E)) = \dim(\text{Ker}(J_m(\lambda) - \lambda E)) = 1$. Kasutades nüüd taaskord algoritmi loengukonspekti [1] leheküljelt 61 saame, et bloki $(J_m(\lambda))^{-1}$ Jordani normaalkuju on $J_m(\frac{1}{\lambda})$.

Tähistades $J(A) = \text{diag}(J_{k_1}(\lambda_1), \dots, J_{k_h}(\lambda_s))$. Kasutame blokk-diagonaalsete matriksite lihtsasti kontrollitavat omadust, et blokk-pöördmatriks koosneb esialgsete blokkide pöördblokkidest. Seega saame, et

$$J(A^{-1}) = \text{diag} \left(J_{k_1} \left(\frac{1}{\lambda_1} \right), \dots, J_{k_h} \left(\frac{1}{\lambda_s} \right) \right),$$

mis on tahetud Jordani normaalkuju. □

Matriksi A jäljeks $\text{trace}(A)$ nimetatakse tema peadiagonaali elementide summat. Seega kehtib matriksi $A = (a_{jh})_{j,h=1}^n$ korral $\text{trace}(A) = \sum_{j=1}^n a_{jj}$.

Tõestame järgneva lemma jälje kohta.

Lemma 4. Olgu R kommutatiivne ring ja $A, B \in \text{Mat}_n(R)$. Kehtib valem $\text{trace}(AB) = \text{trace}(BA)$.

Tõestus. Olgu R kommutatiivne ring ja $A = (a_{jh})_{j,h=1}^n, B = (b_{jh})_{j,h=1}^n \in \text{Mat}_n(R)$. Teadupoolest kehtivad

$$AB = \left(\sum_{k=1}^n a_{jk} b_{kh} \right)_{j,h=1}^n \quad \text{ja} \quad BA = \left(\sum_{k=1}^n b_{jk} a_{kh} \right)_{j,h=1}^n.$$

Nüüd

$$\text{trace}(AB) = \sum_{j=1}^n \sum_{k=1}^n a_{jk} b_{kj} = \sum_{j=1}^n \sum_{k=1}^n b_{kj} a_{jk} = \text{trace}(BA).$$

Eelneva rea viimases võrduses nimetasime lihtsalt summeerimisindeksid omavahel ümber. ■

Ülesanne VIII.8. Olgu $A \in \text{Mat}_n(K)$. Tõestada, et kui A on nilpotentne matriks, siis tema jälg $\text{trace } A = 0$.

Lahendus: Olgu $A \in \text{Mat}_n(K)$ nilpotentne, siis on tema ainus omaväärtus $\lambda = 0$. Teadupoolest on matriks A sarnane oma Jordani normaalkujuga $J(A)$. Algebra I konspektist [2] (lause 10.31) on teada, et sarnaste matriksite karakteristlikud polünoomid on võrdsed, seetõttu on neil ka samad omaväärtused. Jordani normaalkuju omaväärtused on alati tema peadiagonaalil, mistõttu $J(A)$ peadiagonaalil on kõik nullid, mistõttu $\text{trace}(J(A)) = 0$. Nüüd, tänu lemmale 4, kehtib

$$\text{trace } A = \text{trace}(CJ(A)C^{-1}) = \text{trace}(CC^{-1}J(A)) = \text{trace}(EJ(A)) = \text{trace}(J(A)) = 0$$

nagu tahetud. □

Ülesanne VIII.9. Olgu K algebraliselt kinnine korpus. Tõestada, et kui matriksi $A \in \text{Mat}_n(K)$ ainus omaväärtus on 0, siis A on nilpotentne.

Lahendus: Olgu K algebraliselt kinnine korpus ja $A \in \text{Mat}_n(K)$ maatriks, mille ainus omaväärtus on $\lambda = 0$. Sel juhul maatriksi A karakteristlik polünoom avaldub kujul

$$p(X) = \det(A - XE) = X^n.$$

Vastavalt Cayley-Hamiltoni teoreemile on maatriksile A vastava lineaarteisenduse karakteristlik polünoom ka tema annulleerivaks polünoomiks, mistõttu

$$p(A) = A^n = 0.$$

Järelikult on A nilpotentne maatriks. □

Koos loengukonspekti [1] lausega 3.14 saame eelmise ülesande sõnastada kasuliku lausena.

Lause. *Olgu K algebraliselt kinnine korpus. Maatriks $A \in \text{Mat}_n(K)$ on nilpotentne parajasti siis, kui tema ainus omaväärtus on 0.*

Ülesanne* VIII.10. Tõestada, et kui K on lõpmatu korpus, L tema laiend, $A, B \in \text{Mat}_n(K)$ on sarnased ringis $\text{Mat}_n(L)$, siis A ja B on sarnased juba ringis $\text{Mat}_n(K)$.

Praktikum IX (Bi)lineaarsed funktsionaalid. Kaasruum

Olgu V vektorruum üle korpuse K . Ruumi V kaasruumi tähistatakse

$$V^* := \text{Hom}(V, K).$$

Kaasruum V^* on kõigi lineaarsete funktsionaalide $V \rightarrow K$ hulk (vektorruum).

Ülesanne IX.1. Teha kindlaks, kas φ on lineaarne funktsionaal vektorruumil V üle korpuse K , kui

1. $\varphi((x_1, \dots, x_n)) = \sum_{k=1}^n c_k x_k$, kus $V = K^n$ ja $c_1, \dots, c_n \in K$ on fikseeritud;
2. $\varphi((x_1, \dots, x_n)) = 7x_2^3$, kus $K = \mathbb{Z}_3$ ja $V = \mathbb{Z}_3^n$;
3. $\varphi((x_1, \dots, x_n)) = a$, kus $V = K^n$ ja $a \in K \setminus \{0\}$ on fikseeritud;
4. $\varphi(f) = \int_a^b g(x)f(x)dx$, kus $K = \mathbb{R}$, $V = \mathcal{C}[a, b]$ (lõigul $[a, b]$ pidevad funktsioonid) ja $g \in \mathcal{C}[a, b]$ on fikseeritud.

Leida ruumil K^n lineaarseteks funktsionaalideks osutunud kujutuste maatriksid baasi $\{(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1)\}$ suhtes.

Lahendus:

1. Olgu $V = K^n$. Vaatleme kujutust $\varphi: K^n \rightarrow K$, $(x_1, \dots, x_n) \mapsto \sum_{k=1}^n c_k x_k$. Fikseerime $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in K^n$ ja $k \in K$, siis

$$\varphi(x + y) = \varphi((x_1 + y_1, \dots, x_n + y_n)) = \sum_{k=1}^n c_k (x_k + y_k) = \sum_{k=1}^n c_k x_k + \sum_{k=1}^n c_k y_k = \varphi(x) + \varphi(y),$$

$$\varphi(kx) = \varphi((kx_1, \dots, kx_n)) = \sum_{k=1}^n kx_k = k \left(\sum_{k=1}^n x_k \right) = k\varphi(x).$$

Seega $\varphi \in V^*$. Ilmselt avaldub kujutuse φ maatriks

$$(c_1 \ \dots \ c_n) \in \text{Mat}_{1,n}(K).$$

2. Olgu $V = \mathbb{Z}_3^n$. Kõigepealt paneme tähele, et iga $a \in \mathbb{Z}_3$ ja $n \in \mathbb{N}$ korral

$$na := \underbrace{a + \dots + a}_n = \bar{n}a.$$

Olgu $a, b \in \mathbb{Z}_3$, siis

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + b^3. \quad (7)$$

Tegelikult näeme kontrollimise teel, et kehtib isegi $a^3 = a$.

Vaatleme kujutust $\varphi: \mathbb{Z}_3^n \rightarrow \mathbb{Z}_3$, $(x_1, \dots, x_n) \mapsto 7x_2^3 = x_2$. Fikseerime $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{Z}_3^n$ ja $k \in \mathbb{Z}_3$, siis

$$\begin{aligned} \varphi(x + y) &= \varphi((x_1 + y_1, \dots, x_n + y_n)) = x_2 + y_2 = \varphi(x) + \varphi(y), \\ \varphi(kx) &= \varphi((kx_1, \dots, kx_n)) = kx_2 = k\varphi(x). \end{aligned}$$

Seega $\varphi \in (\mathbb{Z}_3^n)^*$. Ilmselt avaldub kujutuse φ maatriks

$$(0 \ 1 \ 0 \ \dots \ 0) \in \text{Mat}_{1,n}(\mathbb{Z}_3).$$

Siit näeme ka, et otseastme K^n projektsioon k -ndale koordinaadile on funktsionaal.

3. Olgu $V = K^n$ ja $a \in K \setminus \{0\}$. Vaatleme kujutust $\varphi: K^n \rightarrow K$, $(x_1, \dots, x_n) \mapsto a$. Fikseerime $x = (x_1, \dots, x_n) \in K^n$ ja $k \in K$, siis

$$\varphi(kx) = \varphi((kx_1, \dots, kx_n)) = a \neq k\varphi(x).$$

Seega φ ei ole lineaarne funktsionaal.

4. Olgu $K = \mathbb{R}$, $a, b \in \mathbb{R}$, $V = \mathcal{C}[a, b]$ ja $g \in \mathcal{C}[a, b]$. Vaatleme kujutust $\varphi: \mathcal{C}[a, b] \times \mathcal{C}[a, b] \rightarrow \mathbb{R}$. Kujutus φ on korrektselt defineeritud, kuna kahe pideva funktsiooni korrutis on pidev ja iga pidev funktsioon on (Riemanni mõttes) integreeruv. Fikseerime $f_1, f_2, f \in \mathcal{C}[a, b]$ ja $r \in \mathbb{R}$, siis

$$\begin{aligned} \varphi(f_1 + f_2) &= \int_a^b g(x)(f_1 + f_2)(x) \, dx = \int_a^b g(x)(f_1(x) + f_2(x)) \, dx = \\ &= \int_a^b (g(x)f_1(x) + g(x)f_2(x)) \, dx = \\ &= \int_a^b g(x)f_1(x) \, dx + \int_a^b g(x)f_2(x) \, dx = \varphi(f_1) + \varphi(f_2), \\ \varphi(kf) &= \int_a^b g(x)(kf)(x) \, dx = \int_a^b g(x)kf(x) \, dx = k \int_a^b g(x)f(x) \, dx = k\varphi(f). \end{aligned}$$

Seega $\varphi \in (\mathcal{C}[a, b])^*$. Lineaarfunktsionaali φ maatriksit me ei oska leida. Vektorruum $\mathcal{C}[a, b]$ on lõpmatumõõtmeline ruum. Valikuaksioomist järeldub, et tal leidub baas, mis on kontiiniumi võimsusega. Kuid seda baasi ei osata eksplitsiitselt esitada. (Kui uurite selle kohta lisainfot, siis meie vaatleme siin nn. Hameli baasi.)

□

Märkin, et analoogiliselt reaga (7), saab Newtoni binoomvalemit kasutades tõestada, et

$$\text{char}(K) = p \implies (a + b)^p = a^p + b^p, \quad (a, b \in K).$$

Seda valemit kutsutakse vahel, ilmselgetel põhjustel, “rebase unistuseks” (*freshman's dream*).

Ülesanne IX.2. Olgu V vektorruum üle $\mathbb{R}$. Näidata, et kujutus $\varphi: V \times V \rightarrow \mathbb{R}$ on bilineaarne funktsionaal ja leida tema maatriks, kui

1. $\varphi(x, y) = 0$;
2. $\varphi(\vec{x}, \vec{y}) = \langle \vec{x}, \vec{y} \rangle$, kus $V = \mathbb{E}_3$, ja baas on 1) $\{\vec{i}, \vec{j}, \vec{k}\}$, 2) $\{\vec{i} + \vec{j}, \vec{j} + \vec{k}, 2\vec{k}\}$;
3. $\varphi(f, g) = \int_0^1 f(x)g(x) \, dx$, kus $V = \mathbb{R}_2[X]$, ja baas on 1) $\{1, X, X^2\}$, 2) $\{1, X - 1, (X - 1)^2\}$;
4. $\varphi(z_1, z_2) = \text{Re}(z_1) \text{Re}(z_2) + \text{Im}(z_1) \text{Im}(z_2)$, kus $V = \mathbb{C}$, ja baas on 1) $\{1, i\}$, 2) $\{1 + i, 1 - i\}$;

Lahendus:

1. Olgu V vektorruum (üle K). Märkame, et kujutus $\varphi: V \times V \rightarrow K$, $(x, y) \mapsto 0$, rahuldab bilineaarsuse tingimusi. Näiteks, kui $x, y_1 + y_2 \in V$ ja $k \in K$, siis

$$\begin{aligned} \varphi(x, y_1 + y_2) &= 0 = 0 + 0 = \varphi(x, y_1) + \varphi(x, y_2) \\ \varphi(x, ky_1) &= 0 = k0 = k\varphi(x, y_1). \end{aligned}$$

Ilmselt on φ sümmeetriline. Lihtne on näha, et kui $\dim V = 0$, siis funktsionaali φ maatriks on nullmaatriks $0 \in \text{Mat}_n(K)$.

2. Olgu $V = \mathbb{E}_3$ (3-mõõtmeline eukleidiline ruum). Vaatleme funktsionaali $\varphi: \mathbb{E}_3 \times \mathbb{E}_3 \rightarrow \mathbb{R}$, $(\vec{x}, \vec{y}) \mapsto \langle \vec{x}, \vec{y} \rangle$. Kuna skalaarkorrutis (üle $\mathbb{R}$) on vastavalt definitsioonile kommutatiivne, siis järelikult on φ sümmeetriline. Seega piisab bilineaarsuseks, kui tõestame vaid esimesed kaks bilineaarsuse tingimust. Olgu $\vec{x}, \vec{x}_1, \vec{x}_2, \vec{y} \in \mathbb{E}_3$ ja $r \in \mathbb{R}$, siis vastavalt skalaarkorrutis definitsioonile

$$\begin{aligned}\varphi(\vec{x}_1 + \vec{x}_2, \vec{y}) &= \langle \vec{x}_1 + \vec{x}_2, \vec{y} \rangle = \langle \vec{x}_1, \vec{y} \rangle + \langle \vec{x}_2, \vec{y} \rangle = \varphi(\vec{x}_1, \vec{y}) + \varphi(\vec{x}_2, \vec{y}), \\ \varphi(r\vec{x}, \vec{y}) &= \langle r\vec{x}, \vec{y} \rangle = r\langle \vec{x}, \vec{y} \rangle = r\varphi(\vec{x}, \vec{y}).\end{aligned}$$

Seega φ on sümmeetriline bilineaarne funktsionaal.

Vaatleme ruumi $\mathbb{E}_3$ baasi $\mathcal{B}_1 = \{\vec{i}, \vec{j}, \vec{k}\}$ (see on standardne tähistus 3-mõõtmelise eukleidilise ruumi kanoonilisele reeperile). Baas $\mathcal{B}_1$ on ortonormaalne, seega näeme, et matriksi $A_\varphi^{\mathcal{B}_1} = (a_{hl})$ elemendid avalduvad

$$\begin{aligned}a_{11} &= \varphi(\vec{i}, \vec{i}) = \langle \vec{i}, \vec{i} \rangle = 1 = \langle \vec{j}, \vec{j} \rangle = \langle \vec{k}, \vec{k} \rangle = a_{22} = a_{33}, \\ a_{12} &= \varphi(\vec{i}, \vec{j}) = \langle \vec{i}, \vec{j} \rangle = 0 = a_{hl}, \quad h \neq l.\end{aligned}$$

Järelikult avaldub funktsionaali φ matriks baasi $\mathcal{B}_1$ suhtes

$$A_\varphi^{\mathcal{B}_1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \text{Mat}_3(\mathbb{R}).$$

Vaatleme ruumi $\mathbb{E}_2$ baasi $\mathcal{B}_2 = \{\vec{i} + \vec{j}, \vec{j} + \vec{k}, 2\vec{k}\}$. Vastavalt skalaarkorrutise definitsioonile arvutame matriksi $A_\varphi^{\mathcal{B}_2} = (a_{hl})$ elemendid

$$\begin{aligned}a_{11} &= \varphi(\vec{i} + \vec{j}, \vec{i} + \vec{j}) = \langle \vec{i} + \vec{j}, \vec{i} + \vec{j} \rangle = \langle \vec{i}, \vec{i} + \vec{j} \rangle + \langle \vec{j}, \vec{i} + \vec{j} \rangle = \\ &= \langle \vec{i}, \vec{i} \rangle + \langle \vec{i}, \vec{j} \rangle + \langle \vec{j}, \vec{i} \rangle + \langle \vec{j}, \vec{j} \rangle = 1 + 0 + 0 + 1 = 2, \\ a_{22} &= \varphi(\vec{j} + \vec{k}, \vec{j} + \vec{k}) = \langle \vec{j} + \vec{k}, \vec{j} + \vec{k} \rangle = \langle \vec{j}, \vec{j} + \vec{k} \rangle + \langle \vec{k}, \vec{j} + \vec{k} \rangle = \\ &= \langle \vec{j}, \vec{j} \rangle + \langle \vec{j}, \vec{k} \rangle + \langle \vec{k}, \vec{j} \rangle + \langle \vec{k}, \vec{k} \rangle = 1 + 0 + 0 + 1 = 2, \\ a_{33} &= \varphi(2\vec{k}, 2\vec{k}) = \langle 2\vec{k}, 2\vec{k} \rangle = 2\langle \vec{k}, 2\vec{k} \rangle = 4\langle \vec{k}, \vec{k} \rangle = 4, \\ a_{12} &= \varphi(\vec{i} + \vec{j}, \vec{j} + \vec{k}) = \langle \vec{i} + \vec{j}, \vec{j} + \vec{k} \rangle = \langle \vec{i}, \vec{j} + \vec{k} \rangle + \langle \vec{j}, \vec{j} + \vec{k} \rangle = \\ &= \langle \vec{i}, \vec{j} \rangle + \langle \vec{i}, \vec{k} \rangle + \langle \vec{j}, \vec{j} \rangle + \langle \vec{j}, \vec{k} \rangle = 0 + 0 + 1 + 0 = 1 = a_{21}, \\ a_{13} &= \varphi(\vec{i} + \vec{j}, 2\vec{k}) = \langle \vec{i} + \vec{j}, 2\vec{k} \rangle = \langle \vec{i}, 2\vec{k} \rangle + \langle \vec{j}, 2\vec{k} \rangle = 2\langle \vec{i}, \vec{k} \rangle + 2\langle \vec{j}, \vec{k} \rangle = \\ &= 0 + 0 = 0 = a_{31}, \\ a_{23} &= \varphi(\vec{j} + \vec{k}, 2\vec{k}) = \langle \vec{j} + \vec{k}, 2\vec{k} \rangle = \langle \vec{j}, 2\vec{k} \rangle + \langle \vec{k}, 2\vec{k} \rangle = 2\langle \vec{j}, \vec{k} \rangle + 2\langle \vec{k}, \vec{k} \rangle = \\ &= 0 + 2 = 2 = a_{32}.\end{aligned}$$

Järelikult avaldub funktsionaali φ matriks baasi $\mathcal{B}_2$ suhtes

$$A_\varphi^{\mathcal{B}_2} = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 2 \\ 0 & 2 & 4 \end{pmatrix} \in \text{Mat}_3(\mathbb{R}).$$

3. Olgu $V = \mathbb{R}_2[X]$. Vaatleme funktsionaali $\varphi: \mathbb{R}_2[X] \times \mathbb{R}_2[X] \rightarrow \mathbb{R}$, $(f, g) \mapsto \int_0^1 f(x)g(x) dx$. Olgu $f(X) = a_1X^2 + b_1X + c_1, g(X) = a_2X^2 + b_2X + c_2 \in \mathbb{R}_2[X]$, arvutame nende korrutise (selle eksplitsiitne kujuneb meile hiljem kasulikuks)

$$\begin{aligned} f(X)g(X) &= (a_1X^2 + b_1X + c_1)(a_2X^2 + b_2X + c_2) = \\ &= a_1a_2X^4 + (a_1b_2 + b_1a_2)X^3 + (a_1c_2 + c_1a_2 + b_1b_2)X^2 + (b_1c_2 + c_1b_2)X + c_1c_2. \end{aligned}$$

Kuna fg on polünoom (4. astme), siis funktsioon $fg: \mathbb{R} \rightarrow \mathbb{R}$ on pidev ja seetõttu ka integreeruv. Seega on funktsionaal φ korrektselt defineeritud. Kuna reaalarvuliste polünoomide korrutamine on kommutatiivne, siis on funktsionaal φ sümmeetriline, seepärast taaskord piisab vaid kahe esimese bilineaarsuse tingimuse näitamisest. Olgu $f, f_1, f_2, g \in \mathbb{R}_2[X]$ ja $r \in \mathbb{R}$, siis vastavalt (Riemanni) integraali omadustele kehtib

$$\begin{aligned} \varphi(f_1 + f_2, g) &= \int_0^1 (f_1 + f_2)(x)g(x) dx = \int_0^1 (f_1(x)g(x) + f_2(x)g(x)) dx = \\ &= \int_0^1 f_1(x)g(x) dx + \int_0^1 f_2(x)g(x) dx = \varphi(f_1, g) + \varphi(f_2, g), \\ \varphi(rf, g) &= \int_0^1 (rf)(x)g(x) dx = r \int_0^1 f(x)g(x) dx = r\varphi(f, g). \end{aligned}$$

Seega φ on sümmeetriline bilineaarne funktsionaal.

Vaatleme ruumi $\mathbb{R}_2[X]$ baasi $\mathcal{B}_1 = \{1, X, X^2\}$. Arvutame funktsionaali φ maatriksi $A_\varphi^{\mathcal{B}_1} = (a_{hk})$ elemendid

$$\begin{aligned} a_{11} &= \varphi(1, 1) = \int_0^1 1 dx = x \Big|_0^1 = 1, \\ a_{22} &= \varphi(X, X) = \int_0^1 x^2 dx = \frac{x^3}{3} \Big|_0^1 = \frac{1}{3}, \\ a_{33} &= \varphi(X^2, X^2) = \int_0^1 x^4 dx = \frac{x^5}{5} \Big|_0^1 = \frac{1}{5}, \\ a_{12} &= \varphi(1, X) = \int_0^1 x dx = \frac{x^2}{2} \Big|_0^1 = \frac{1}{2} = a_{21}, \\ a_{13} &= \varphi(1, X^2) = \int_0^1 x^2 dx = \frac{x^3}{3} \Big|_0^1 = \frac{1}{3} = a_{31}, \\ a_{23} &= \varphi(X, X^2) = \int_0^1 x^3 dx = \frac{x^4}{4} \Big|_0^1 = \frac{1}{4} = a_{32}. \end{aligned}$$

Järelikult avaldub funktsionaali φ maatriks baasi $\mathcal{B}_1$ suhtes

$$A_\varphi^{\mathcal{B}_1} = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} \end{pmatrix} \in \text{Mat}_3(\mathbb{R}).$$

Vaatleme ruumi $\mathbb{R}_2[X]$ baasi $\mathcal{B}_2 = \{1, X-1, (X-1)^2 = X^2-2X+1\}$. Arvutame funktsionaali φ maatriksi $A_\varphi^{\mathcal{B}_1} = (a_{hk})$ elemendid

$$a_{11} = \varphi(1, 1) = 1,$$

$$a_{22} = \varphi(X-1, X-1) = \int_0^1 (x^2 - 2x + 1) \, dx = \left(\frac{x^3}{3} - \frac{2x^2}{2} + x \right) \Big|_0^1 = \frac{1}{3},$$

$$\begin{aligned} a_{33} &= \varphi((X-1)^2, (X-1)^2) = \int_0^1 (x^4 - 4x^3 + 6x^2 - 4x + 1) \, dx = \\ &= \left(\frac{x^5}{5} - \frac{4x^4}{4} + \frac{6x^3}{3} - \frac{4x^2}{2} + x \right) \Big|_0^1 = \frac{1}{5}, \end{aligned}$$

$$a_{12} = \varphi(1, X-1) = \int_0^1 (x-1) \, dx = \left(\frac{x^2}{2} - x \right) \Big|_0^1 = -\frac{1}{2} = a_{21},$$

$$a_{13} = \varphi(1, (X-1)^2) = \int_0^1 (x^2 - 2x + 1) \, dx = \left(\frac{x^3}{3} - \frac{2x^2}{2} + x \right) \Big|_0^1 = \frac{1}{3} = a_{31},$$

$$\begin{aligned} a_{23} &= \varphi(X-1, (X-1)^2) = \int_0^1 (x^3 - 3x^2 + 3x - 1) \, dx = \\ &= \left(\frac{x^4}{4} - \frac{3x^3}{3} + \frac{3x^2}{2} - x \right) \Big|_0^1 = -\frac{1}{4} = a_{32}. \end{aligned}$$

Järelikult avaldub funktsionaali φ maatriks baasi $\mathcal{B}_2$ suhtes

$$A_\varphi^{\mathcal{B}_1} = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} & -\frac{1}{4} \\ \frac{1}{3} & -\frac{1}{4} & \frac{1}{5} \end{pmatrix} \in \text{Mat}_3(\mathbb{R}).$$

4. Olgu $V = \mathbb{C}$. Vaatleme funktsionaali

$$\varphi: \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{R}, \quad (z_1, z_2) \mapsto \text{Re}(z_1) \text{Re}(z_2) + \text{Im}(z_1) \text{Im}(z_2).$$

Kuna reaalarvude korrutamine on kommutatiivne, siis järelikult on φ sümmeetriline funktsionaal. Seetõttu piisab meil taaskord bilineaarsuse näitamiseks kontrollida vaid esimest kahte tingimust. Olgu $z = a + ib$, $z_1 = a_1 + ib_1$, $z_2 = a_2 + ib_2$, $w = c + id \in \mathbb{C}$ ja $r \in \mathbb{R}$, siis

$$\begin{aligned} \varphi(z_1 + z_2, w) &= (a_1 + a_2)c + (b_1 + b_2)d = (a_1c + b_1d) + (a_2c + b_2d) = \varphi(z_1, w) + \varphi(z_2, w), \\ \varphi(rz, w) &= (ra)c + (rb)d = r(ac + bd) = r\varphi(z, w). \end{aligned}$$

Seega φ on sümmeetriline bilineaarne funktsionaal.

Vaatleme ruumi $\mathbb{C}$ baasi $\mathcal{B}_1 = \{1, i\}$. Arvutame funktsionaali φ maatriksi $A_\varphi^{\mathcal{B}_1} = (a_{hk})$ elemendid

$$a_{11} = \varphi(1, 1) = 1^2 = 1,$$

$$a_{22} = \varphi(i, i) = -1^2 = -1,$$

$$a_{12} = \varphi(1, i) = \text{Re}(1) \text{Re}(i) - \text{Im}(1) \text{Im}(i) = 1 \cdot 0 - 0 \cdot 1 = 0 = a_{21}.$$

Järelikult avaldub funktsionaali φ maatriks baasi $\mathcal{B}_1$ suhtes

$$A_{\varphi}^{\mathcal{B}_1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \text{Mat}_2(\mathbb{R}).$$

Vaatleme ruumi $\mathbb{C}$ baasi $\mathcal{B}_2 = \{1+i, 1-i\}$. Arvutame funktsionaali φ maatriksi $A_{\varphi}^{\mathcal{B}_2} = (a_{hk})$ elemendid

$$\begin{aligned} a_{11} &= \varphi(1+i, 1+i) = 1^2 - 1^2 = 0, \\ a_{22} &= \varphi(1-i, 1-i) = 1^2 - (-1)^2 = 0, \\ a_{12} &= \varphi(1+i, 1-i) = 1^2 - (-1) \cdot 1 = 2 = a_{21}. \end{aligned}$$

Järelikult avaldub funktsionaali φ maatriks baasi $\mathcal{B}_1$ suhtes

$$A_{\varphi}^{\mathcal{B}_1} = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \in \text{Mat}_2(\mathbb{R}).$$

Siit ülesandest on muuhulgas näha, et kõikide sümmeetriliste bilineaarsete funktsionaalide maatriksid on sümmeetrilised. Kusjuures on sama funktsionaali maatriksid erineva baasi suhtes alati sarnased. $\square$

Enne järgmist ülesannet tõestame mõned lihtsad maatriksi jälje omadused (lisaks lemmale 4). Olgu R ring, $n \in \mathbb{N}_1$, $A = (a_{hk}), B = (b_{hk}) \in \text{Mat}_n(R)$ ja $c \in R$, siis

$$\begin{aligned} \text{trace}(A+B) &= \text{trace}((a_{hk} + b_{hk})_{h,k=1}^n) = \sum_{h=1}^n a_{hh} + b_{hh} = \sum_{h=1}^n a_{hh} + \sum_{h=1}^n b_{hh} = \text{trace}(A) + \text{trace}(B), \\ \text{trace}(cA) &= \text{trace}((ca_{hk})_{h,k=1}^n) = \sum_{h=1}^n ca_{hh} = c \sum_{h=1}^n a_{hh} = c \text{trace}(A). \end{aligned}$$

Siit on näha, et maatriksi jälg on mooduli $\text{Mat}_n(R)$ homomorfism.

Ülesanne IX.3. Olgu $V = \text{Mat}_n(\mathbb{C})$. Tõestada, et

$$f(A, B) := n \text{trace}(AB) - \text{trace}(A) \text{trace}(B)$$

on V bilineaarne funktsionaal. Kas f on sümmeetriline funktsionaal?

Lahendus: Olgu $n \in \mathbb{N}_1$. Vaatleme kujutust $f: \text{Mat}_n(\mathbb{C}) \times \text{Mat}_n(\mathbb{C}) \rightarrow \mathbb{C}$, mis on ülesande püstituses defineeritud. Fikseerime $A = (a_{hk}), B = (b_{hk}), \Gamma = (\gamma_{hk}) \in \text{Mat}_n(\mathbb{C})$ ja $c \in \mathbb{C}$.

$$\begin{aligned} f(A + \Gamma, B) &= n \text{trace}((A + \Gamma)B) - \text{trace}(A + \Gamma) \text{trace}(B) = \\ &= n \text{trace}(AB + \Gamma B) - (\text{trace}(A) + \text{trace}(\Gamma)) \text{trace}(B) = \\ &= (n \text{trace}(AB) - \text{trace}(A) \text{trace}(B)) + (n \text{trace}(\Gamma B) - \text{trace}(\Gamma) \text{trace}(B)) = \\ &= f(A, B) + f(\Gamma, B), \\ f(A, B + \Gamma) &= f(A, B) + f(A, \Gamma), \\ f(cA, B) &= n \text{trace}(cAB) - \text{trace}(cA) \text{trace}(B) = nc \text{trace}(AB) - c \text{trace}(A) \text{trace}(B) = \end{aligned}$$

$$= c(n \operatorname{trace}(AB) - \operatorname{trace}(A) \operatorname{trace}(B)) = cf(A, B),$$

$$f(A, cB) = cf(A, B).$$

Seega f on bilineaarne funktsionaal.

Kuna $\mathbb{C}$ on korpus, siis lemmast 4 järelneb funktsionaali f sümmeetrilisus, mistõttu f on sümmeetriline bilineaarne funktsionaal. $\square$

Ülesanne IX.4. Olgu V vektorruum üle korpuse K . Tõestada, et kui $\varphi: V \times V \rightarrow K$ on bilineaarne funktsionaal, siis iga $a \in V$ korral on $\psi: V \rightarrow K$, $\psi(v) = \varphi(v, a)$ lineaarne funktsionaal.

Lahendus: Olgu $\varphi: V \times V \rightarrow K$ bilineaarne funktsionaal. Fikseerime $a \in V$ ja vaatleme kujutust $\psi: V \rightarrow K$, $v \mapsto \varphi(v, a)$. Iga $v_1, v_2, v \in V$ ja $k \in K$ korral kehtib tänu bilineaarse funktsionaali definitsioonile

$$\begin{aligned}\psi(v_1 + v_2) &= \varphi(v_1 + v_2, a) = \varphi(v_1, a) + \varphi(v_2, a) = \psi(v_1) + \psi(v_2), \\ \psi(kv) &= \varphi(kv, a) = k\varphi(v, a) = k\psi(v).\end{aligned}$$

Seega $\psi \in V^*$. $\square$

Ülesanne IX.5. Olgu f bilineaarne funktsionaal vektorruumil V , kusjuures mistahes $0 \neq v \in V$ korral leidub $w \in V$ nii, et $f(v, w) \neq 0$. Tõestada, et iga $g \in V^*$ ja $w \in V$ jaoks leidub $v \in V$ nii, et $g(w) = f(v, w)$.

Lahendus: Olgu V vektorruum ja $f: V \times V \rightarrow K$ bilineaarne, kusjuures iga $0 \neq v \in V$ korral $\operatorname{Ker}(f(v, _)) \subset V$. Lisaks olgu $g \in V^*$ lineaarne funktsionaal. Fikseerime $w \in V$.

Kui $w = 0$, siis $g(w) = f(0, w) = 0$, mistõttu otsitud vektoriks sobib $0 \in V$.

Olgu $w \neq 0$. Vastavalt ülesande eeldustele saame valida $v \in V$ nii, et $f(v, w) \neq 0$. Kuna K on korpus, siis leidub $(f(v, w))^{-1} \in K$. Nüüd paneme tähele, et

$$f(g(w)(f(v, w))^{-1}v, w) = g(w)(f(v, w))^{-1}f(v, w) = g(w).$$

Seega otsitud vektoriks sobib $g(w)(f(v, w))^{-1}v \in V$. $\square$

Bilineaarset funktsionaali $\varphi: V \times V \rightarrow K$ nimetatakse *kaldsümmeetriliseks*, kui iga $x, y \in V$ korral kehtib

$$\varphi(x, y) = -\varphi(y, x).$$

Ülesanne IX.6. Olgu $V = K^2$, kus K on korpus. Näidata, et kujutus $\varphi: V \times V \rightarrow K$, mis on defineeritud võrdusega

$$\varphi((a_1, a_2), (b_1, b_2)) = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}$$

on kaldsümmeetriline bilineaarne funktsionaal. Leida selle funktsionaali maatriks baasi $\mathcal{B} = \{(1, 0), (0, 1)\}$ suhtes.

Lahendus: Olgu K korpus. Vaatleme funktsionaali $\varphi: K^2 \times K^2 \rightarrow K$, $((a_1, a_2), (b_1, b_2)) \mapsto a_1b_2 - b_1a_2$. Fikseerime $a = (a_1, a_2)$, $\alpha = (\alpha_1, \alpha_2)$, $b = (b_1, b_2)$, $\beta = (\beta_1, \beta_2) \in K^2$ ja $k \in K$, siis

$$\begin{aligned}\varphi(a + \alpha, b) &= \varphi((a_1 + \alpha_1, a_2 + \alpha_2), (b_1, b_2)) = \begin{vmatrix} a_1 + \alpha_1 & a_2 + \alpha_2 \\ b_1 & b_2 \end{vmatrix} = \\ &= (a_1 + \alpha_1)b_2 - b_1(a_2 + \alpha_2) = (a_1b_2 - b_1a_2) + (\alpha_1b_2 - b_1\alpha_2) = \\ &= \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} + \begin{vmatrix} \alpha_1 & \alpha_2 \\ b_1 & b_2 \end{vmatrix} = \varphi(a, b) + \varphi(\alpha, b), \\ \varphi(a, b + \beta) &= \begin{vmatrix} a_1 & a_2 \\ b_1 + \beta_1 & b_2 + \beta_2 \end{vmatrix} = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} + \begin{vmatrix} a_1 & a_2 \\ \beta_1 & \beta_2 \end{vmatrix} = \varphi(a, b) + \varphi(a, \beta), \\ \varphi(ka, b) &= \begin{vmatrix} ka_1 & ka_2 \\ b_1 & b_2 \end{vmatrix} = ka_1b_2 - ka_2b_1 = k(a_1b_2 - a_2b_1) = k \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = k\varphi(a, b), \\ \varphi(a, kb) &= \begin{vmatrix} a_1 & a_2 \\ kb_1 & kb_2 \end{vmatrix} = k \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = k\varphi(a, b).\end{aligned}$$

Seega funktsionaal φ on lineaarne. (Omadused, et determinandi ridade liitmisel liituvad determinandi ja, et determinandi korrutamisel skalaariga korrutub terve determinant, on teada Algebra I-st.)

Lisaks

$$\varphi(a, b) = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = a_1b_2 - b_1a_2 = -(b_1a_2 - a_1b_2) = - \begin{vmatrix} b_1 & b_2 \\ a_1 & a_2 \end{vmatrix} = -\varphi(b, a).$$

Seega φ on ka kaldsümmeetriline. (Ka see omadus, et detrimandi ridade vahetamisel ta korrutub -1 -ga, on Algebra I-s üldjuhul tõestatud.)

Leiame φ maatriksi $A_\varphi^B = (a_{hk}) \in \text{Mat}_2(K)$. Vastavalt bilineaarse funktsionaali baasi definitsioonile

$$\begin{aligned}a_{11} &= \varphi((1, 0), (1, 0)) = \begin{vmatrix} 1 & 0 \\ 1 & 0 \end{vmatrix} = 0, \\ a_{22} &= \varphi((0, 1), (0, 1)) = \begin{vmatrix} 0 & 1 \\ 0 & 1 \end{vmatrix} = 0, \\ a_{12} &= \varphi((1, 0), (0, 1)) = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1, \\ a_{21} &= \varphi((0, 1), (1, 0)) = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = -1.\end{aligned}$$

Järelikult

$$A_\varphi^B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Märkame, et $(A_\varphi^B)^T = -A_\varphi^B$. Järgnevalt näeme, et see on kooskõlas funktsionaali φ kaldsümmeetrilisusega. $\square$

Maatriksit $A \in \text{Mat}_n(R)$ nimetatakse *kaldsümmeetriliseks* (*skewsymmetric*), kui $A^T = -A$ (ehk $a_{hk} = -a_{kh}$). Tõestame lemma, mis on täpselt analoogiline loengukonspekti lausega 4.21. Kuigi meil otseselt seda lemmad vaja ei lähe, siis usutavasti annab see lemma parema arusaama kaldsümmeetrilistest funktsionaalidest.

Lemma 5. *Kaldsümmeetrilise bilineaarse funktsionaali maatriks mistahes baasi suhtes on kaldsümmeetriline. Kui mingi bilineaarse funktsionaali maatriks mingi baasi suhtes on kaldsümmeetriline, siis see funktsionaal on ka kaldsümmeetriline.*

Tõestus. ($\Rightarrow$) Olgu f kaldsümmeetriline bilineaarne funktsionaal ruumil V . Olgu $A_f^{\mathcal{B}} = (a_{hk})$, siis $a_{hk} = f(\epsilon_h, \epsilon_k) = -f(\epsilon_k, \epsilon_h) = -a_{kh}$, kus $\mathcal{B} = \{\epsilon_1, \dots, \epsilon_n\}$ on ruumi V suvaline baas. Järelikult f on kaldsümmeetriline.

($\Leftarrow$) Olgu bilineaarse funktsionaali f maatriks mingi baasi $\mathcal{B} = \{\epsilon_1, \dots, \epsilon_n\}$ suhtes kaldsümmeetriline. Siis iga $x, y \in V$ korral

$$f(x, y) = \sum_{h,k=1}^n f(\epsilon_h, \epsilon_k) x_h y_k = - \sum_{h,k=1}^n f(\epsilon_k, \epsilon_h) x_k y_h = -f(y, x).$$

Seega f on kaldsümmeetriline. ■

Ülesanne IX.7. Tõestada, et vektorruumi V (üle K) sümmeetriliste ja kaldsümmeetriliste bilineaarsete funktsionaalide hulga $\mathcal{S}$ ja $\mathcal{K}$ on $\mathcal{B}$ alamruumid, kus $\mathcal{B}$ on kõigi bilineaarsete funktsionaalide $V \times V \rightarrow K$ vektorruum. Millal kehtib $\mathcal{B} = \mathcal{S} + \mathcal{K}$?

Lahendus: Olgu V vektorruum üle korpuse K ja $\mathcal{B}$ kõigi bilineaarsete funktsionaalide $V \times V \rightarrow K$ vektorruum. Tähistame kõikide sümmeetriliste bilineaarfunktsionaalide hulka $\mathcal{S}$. Olgu $f, g \in \mathcal{S}$, $k \in K$ ja $x, y \in V$, siis

$$\begin{aligned} (f + g)(x, y) &= f(x, y) + g(x, y) = f(y, x) + g(y, x) = (f + g)(y, x), \\ (kf)(x, y) &= kf(x, y) = kf(y, x) = (kf)(y, x). \end{aligned}$$

Siit järeldub, et $\mathcal{S}$ on vektorruumi $\mathcal{B}$ alamruum.

Tähistame kõikide kaldsümmeetriliste bilineaarfunktsionaalide hulka $\mathcal{K}$. Olgu $f, g \in \mathcal{K}$, $k \in K$ ja $x, y \in V$, siis

$$\begin{aligned} (f + g)(x, y) &= f(x, y) + g(x, y) = -f(y, x) - g(y, x) = -(f(y, x) + g(y, x)) = -(f + g)(y, x), \\ (kf)(x, y) &= kf(x, y) = -kf(y, x) = -(kf)(y, x). \end{aligned}$$

Neist võrdustest järeldub, et ka $\mathcal{K}$ on vektorruumi $\mathcal{B}$ alamruum.

Uurime nüüd summat $\mathcal{S} + \mathcal{K}$. Vaatleme ühisosa $\mathcal{S} \cap \mathcal{K}$. Olgu $g \in (\mathcal{S} \cap \mathcal{K}) \setminus \{0_K\}$, kus $0_K: V \times V \rightarrow K$, $(x, y) \mapsto 0_K$ (ehk sümbolit 0_K kasutame kahes erinevas tähenduses: korpuse K ja vektorruumi $\mathcal{B}$ nullelemendina). Sel juhul leiduvad $x, y \in V$ nii, et $g(x, y) \neq 0_K$ ning kuna K korpus, siis leidub $(g(x, y))^{-1} \in K$. Kuna g on korruga sümmeetriline ja kaldsümmeetriline, siis

$$\begin{aligned} g(x, y) &= -g(x, y), \\ 2g(x, y) &= 0_K \quad | \cdot (g(x, y))^{-1}, \\ 2 \cdot 1_K &= 1_K + 1_K = 0_K. \end{aligned}$$

Viimane on samaväärne sellega, et $\text{char}(K) = 2$. Siit järeldame, et kui $\text{char}(K) \neq 2$, siis $\mathcal{S} \cap \mathcal{K} = \{0_K\}$, mistõttu summa $\mathcal{S} + \mathcal{K}$ on otsesumma.

Eeldame edaspidi, et $\text{char}(K) \neq 2$. Paneme tähele, et suvalise bilineaarse funktsionaali f saab iga $x, y \in V$ korral esitada kujul

$$f(x, y) = \mathbf{2}^{-1}(f(x, y) + f(y, x)) + \mathbf{2}^{-1}(f(x, y) - f(y, x)),$$

kus $\mathbf{2} := 1_K + 1_K$. Tähistame

$$\begin{aligned}\sigma_f(x, y) &:= \mathbf{2}^{-1}(f(x, y) + f(y, x)), \\ \kappa_f(x, y) &:= \mathbf{2}^{-1}(f(x, y) - f(y, x)).\end{aligned}$$

Ilmselt on σ_f ja κ_f bilineaarsed funktsionaalid. Paneme tähele, et

$$\begin{aligned}\sigma_f(y, x) &= \mathbf{2}^{-1}(f(y, x) + f(x, y)) = \mathbf{2}^{-1}(f(x, y) + f(y, x)) = \sigma_f(x, y), \\ \kappa_f(y, x) &= \mathbf{2}^{-1}(f(y, x) - f(x, y)) = -\mathbf{2}^{-1}(f(x, y) - f(y, x)) = -\kappa_f(x, y).\end{aligned}$$

Järelikult $\sigma_f \in \mathcal{S}$ ja $\kappa_f \in \mathcal{K}$. Siit näeme, et kuna iga bilineaarne funktsionaal f on esitatav sümmeetrilise σ_f ja kaldsümmeetrilise bilineaarse funktsionaali κ_f summana, siis $\mathcal{S} + \mathcal{K} = \mathcal{B}$.

Kokkuvõttes oleme näidanud, et kui $\text{char}(K) \neq 2$, siis kehtib $\mathcal{S} + \mathcal{K} = \mathcal{B}$. $\square$

Ülesanne* IX.8. Tõestada, et kui $A, B \in \text{Mat}_n(K)$ on diagonaliseeritavad ja $AB = BA$, siis leidub $C \in \text{Mat}_n(K)$ nii, et CAC^{-1} ja CBC^{-1} on mõlemad diagonaalmaatriksid. Kas väide kehtib ka juhul, kui $AB \neq BA$?

Praktikum X Ruutvormid

Ülesanne X.1. Viige ruutvorm $2X_1X_2 + 2X_2X_3$ kanoonilisele kujule.

Lahendus: Vaatleme ruutvormi $F = 2X_1X_2 + 2X_2X_3$, tema maatriks vaadeldaval baasil on

$$A_F := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Leiame ruutvormi F kanoonilise kuju. Selleks kasutame loengukonspekti teoreemi 4.34 tõestusest inspireeritud meetodit. Nimelt kirjutame maatriksi A_F alla ühikmaatriksi ning teisendame maatriksi A_F ridade ja veergude elementaarteisendustega diagonaalmaatriksiks, kusjuures pärast igat ridade elementaarteisendust teeme kohe ka sama elementaarteisenduse veergudega (ma märkin ainult ridade teisendust). Seega

$$\begin{aligned} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \text{II} &\rightarrow \begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ \hline 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \frac{1}{2}\text{I} \rightarrow \begin{pmatrix} 2 & 0 & 1 \\ 0 & -\frac{1}{2} & \frac{1}{2} \\ 1 & \frac{1}{2} & 0 \\ \hline 1 & -\frac{1}{2} & 0 \\ 1 & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} - \frac{1}{2}\text{I} \rightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} \\ \hline 1 & -\frac{1}{2} & -\frac{1}{2} \\ 1 & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix} + \text{II} \rightarrow \\ &\rightarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & -\frac{1}{2} & 0 \\ 0 & 0 & 0 \\ \hline 1 & -\frac{1}{2} & -1 \\ 1 & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} =: \begin{pmatrix} A'_F \\ C \end{pmatrix}. \end{aligned}$$

Siit näeme, et ruutvorm F avaldub kanoonilisel kujul

$$2Y_1^2 - \frac{1}{2}Y_2^2. \quad (8)$$

Kusjuures muutujad $X = (X_1 \ X_2 \ X_3)$ ja $Y = (Y_1 \ Y_2 \ Y_3)$ on omavahel seotud seostega

$$\begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} = X^T = CY^T = \begin{pmatrix} 1 & -\frac{1}{2} & -1 \\ 1 & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} = \begin{pmatrix} Y_1 - \frac{1}{2}Y_2 - Y_3 \\ Y_1 + \frac{1}{2}Y_2 \\ Y_3 \end{pmatrix}.$$

Kontrolliks näitame, et tegemist on tõesti sama ruutvormiga

$$\begin{aligned} F &= 2X_1X_2 + 2X_2X_3 = 2 \left(Y_1 - \frac{1}{2}Y_2 - Y_3 \right) \left(Y_1 + \frac{1}{2}Y_2 \right) + 2 \left(Y_1 + \frac{1}{2}Y_2 \right) Y_3 = \\ &= 2 \left(Y_1^2 + \frac{1}{2}Y_1Y_2 - \frac{1}{2}Y_2Y_1 - \frac{1}{4}Y_2^2 - Y_3Y_1 - \frac{1}{2}Y_3Y_2 \right) + 2 \left(Y_1Y_3 + \frac{1}{2}Y_2Y_3 \right) = 2Y_1^2 - \frac{1}{2}Y_2^2. \end{aligned}$$

Seega on (8) tõesti ruutvormi F kanooniline kuju. Samuti võib kontrollida, et kehtib võrdus $A'_F = C^T A_F C$, nagu tahtud oli. $\square$

Järgneviks ülesandeks tähistame muutujamaatriksid

$$\begin{aligned} X &:= (X_1 \ X_2 \ X_3), \\ Y &:= (Y_1 \ Y_2 \ Y_3), \\ \Xi &:= (\Xi_1 \ \Xi_2 \ \Xi_3), \quad (\text{kreeka täht "ksii"}), \\ \Upsilon &:= (\Upsilon_1 \ \Upsilon_2 \ \Upsilon_3), \quad (\text{kreeka täht "üpsilon"}). \end{aligned}$$

Ülesanne X.2. Viige järgmised ruutvormid normaalkujule a) üle $\mathbb{R}$, b) üle $\mathbb{C}$:

1. $F_1 = X_1^2 + 4X_2^2 + X_3^2 + 4X_1X_2 - 2X_1X_3$,
2. $F_2 = X_1^2 + 2X_2^2 - X_3^2 + 4X_1X_2 - 2X_1X_3 - 4X_2X_3$,
3. $F_3 = -4X_1^2 - X_2^2 - X_3^2 - 4X_1X_2 + 4X_1X_3 + 18X_2X_3$,
4. $F_4 = X_1^2 + 5X_2^2 - X_3^2 + 6X_1X_2 + 4X_2X_3$.

Millised nendest ruutvormidest on omavahel ekvivalentsed?

Lahendus:

1. Vaatleme ruutvormi $F_1 = X_1^2 + 4X_2^2 + X_3^2 + 4X_1X_2 - 2X_1X_3$, selle ruutvormi maatriks on

$$A_1 := \begin{pmatrix} 1 & 2 & -1 \\ 2 & 4 & 0 \\ -1 & 0 & 1 \end{pmatrix}.$$

Viime selle ruutvormi kõigepealt kanoonilisele kujule kasutades eelmises üleandes esitatud algoritmi:

$$\begin{aligned} \begin{pmatrix} 1 & 2 & -1 \\ 2 & 4 & 0 \\ -1 & 0 & 1 \end{pmatrix} &\xrightarrow{-2\text{I}} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 2 \\ -1 & 2 & 1 \end{pmatrix} \xrightarrow{+\text{I}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 2 & 0 \end{pmatrix} \xrightarrow{+\text{III}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix} \rightarrow \\ &\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 2 \\ 0 & 2 & 0 \end{pmatrix} \xrightarrow{-\frac{1}{2}\text{II}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & -1 \end{pmatrix} =: \begin{pmatrix} A'_1 \\ C_1 \end{pmatrix}. \end{aligned}$$

Seega ruutvormi F_1 kanooniline kuju on

$$F_1 = Y_1^2 + 4Y_2^2 - Y_3^2,$$

kusjuures $X^T = C_1 Y^T$. Nüüd viime normaalkujule üle korpuse $\mathbb{R}$, selleks peame matriksi A'_1 kõik read ja veerud, millele oleva elemendi absoluutväärtus on erinev 1-st läbi jagama selle elemendi ruutjuure absoluutväärtusega:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & -1 \\ \hline 1 & -1 & \frac{3}{2} \\ 0 & 1 & -\frac{1}{2} \\ 0 & 1 & \frac{1}{2} \end{pmatrix} \cdot \frac{1}{2} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \\ \hline 1 & -\frac{1}{2} & \frac{3}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \cdot \frac{1}{2} =: \begin{pmatrix} A''_1 \\ D_1 \end{pmatrix}.$$

Siit on näha, et üle korpuse $\mathbb{R}$ on ruutvormi F_1 normaalkuju

$$F_1 = \Xi_1^2 + \Xi_2^2 - \Xi_3^2,$$

kus

$$\begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} = X^T = D_1 \Xi^T = \begin{pmatrix} 1 & -\frac{1}{2} & \frac{3}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \Xi_1 \\ \Xi_2 \\ \Xi_3 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2\Xi_1 - \Xi_2 + 3\Xi_3 \\ \Xi_2 - \Xi_3 \\ \Xi_2 + \Xi_3 \end{pmatrix}.$$

Kuna korpuses $\mathbb{C}$ saame leida arvu i nii, et $i^2 = -1$, mille abil teisendame ka arvu -1 arvuks 1:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \\ \hline 1 & -\frac{1}{2} & \frac{3}{2} \\ 0 & \frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \cdot (-i) \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hline 1 & -\frac{1}{2} & -\frac{3i}{2} \\ 0 & \frac{1}{2} & \frac{i}{2} \\ 0 & \frac{1}{2} & -\frac{i}{2} \end{pmatrix} =: \begin{pmatrix} A'''_1 \\ D'_1 \end{pmatrix}.$$

Seega, üle korpuse $\mathbb{C}$, on ruutvormi F_1 normaalkuju

$$F_1 = \Upsilon_1^2 + \Upsilon_2^2 + \Upsilon_3^2,$$

kus

$$\begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} = X^T = D'_1 \Upsilon^T = \begin{pmatrix} 1 & -\frac{1}{2} & -\frac{3}{2}i \\ 0 & \frac{1}{2} & \frac{1}{2}i \\ 0 & \frac{1}{2} & -\frac{1}{2}i \end{pmatrix} \begin{pmatrix} \Upsilon_1 \\ \Upsilon_2 \\ \Upsilon_3 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2\Upsilon_1 - \Upsilon_2 - 3i\Upsilon_3 \\ \Upsilon_2 + i\Upsilon_3 \\ \Upsilon_2 - i\Upsilon_3 \end{pmatrix}.$$

2. Vaatleme ruutvormi $F_2 = X_1^2 + 2X_2^2 - X_3^2 + 4X_1X_2 - 2X_1X_3 - 4X_2X_3$, mille matriks on

$$A_2 := \begin{pmatrix} 1 & 2 & -1 \\ 2 & 2 & -2 \\ -1 & -2 & -1 \end{pmatrix}.$$

Viime selle ruutvormi normaalkujule, tehes ikka elementaarteisendusi ridade ja seejärel ka veergudega:

$$\begin{aligned}
 & \begin{pmatrix} 1 & 2 & -1 \\ 2 & 2 & -2 \\ -1 & -2 & -1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - 2I \rightarrow \begin{pmatrix} 1 & 0 & -1 \\ 0 & -2 & 0 \\ -1 & 0 & -1 \\ \hline 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + I \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \\ \hline 1 & -2 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{matrix} \cdot \frac{1}{\sqrt{2}} \\ \cdot \frac{1}{\sqrt{2}} \end{matrix} \rightarrow \\
 & \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \\ \hline 1 & -\sqrt{2} & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{matrix} \cdot (-i) \\ \cdot (-i) \end{matrix} =: D_2 \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hline 1 & i\sqrt{2} & -\frac{i}{\sqrt{2}} \\ 0 & -\frac{i}{\sqrt{2}} & 0 \\ 0 & 0 & -\frac{i}{\sqrt{2}} \end{pmatrix} =: \begin{pmatrix} A_2'' \\ D_2' \end{pmatrix}.
 \end{aligned}$$

Järelikult on ruutvormi F_2 normaalkujud

$$\begin{aligned}
 F_2 &= \Xi_1^2 - \Xi_2^2 - \Xi_3^2, & (\text{üle korpuse } \mathbb{R}), \\
 F_2 &= \Upsilon_1^2 + \Upsilon_2^2 + \Upsilon_3^2, & (\text{üle korpuse } \mathbb{C}),
 \end{aligned}$$

kus $X^T = D_2 \Xi^T = D_2' \Upsilon^T$.

3. Vaatleme ruutvormi $F_3 = -4X_1^2 - X_2^2 - X_3^2 - 4X_1X_2 + 4X_1X_3 + 18X_2X_3$, maatriksiga

$$A_3 := \begin{pmatrix} -4 & -2 & 2 \\ -2 & -1 & 9 \\ 2 & 9 & -1 \end{pmatrix}.$$

Viime selle ruutvormi normaalkujule:

$$\begin{aligned}
 & \begin{pmatrix} -4 & -2 & 2 \\ -2 & -1 & 9 \\ 2 & 9 & -1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \frac{1}{2} \rightarrow \begin{pmatrix} -1 & -1 & 1 \\ -1 & -1 & 9 \\ 1 & 9 & -1 \\ \hline \frac{1}{2} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - I \rightarrow \begin{pmatrix} -1 & 0 & 1 \\ 0 & 0 & 8 \\ 1 & 8 & -1 \\ \hline \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + I \rightarrow \\
 & \rightarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 8 \\ 0 & 8 & 0 \\ \hline \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + III \rightarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & 16 & 8 \\ 0 & 8 & 0 \\ \hline \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} - \frac{1}{2} II \rightarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & 16 & 0 \\ 0 & 0 & -4 \\ \hline \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & -\frac{1}{2} \\ 0 & 1 & \frac{1}{2} \end{pmatrix} \cdot \frac{1}{4} \rightarrow
 \end{aligned}$$

$$\rightarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -4 \\ \hline \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & \frac{1}{4} & -\frac{1}{2} \\ 0 & \frac{1}{4} & \frac{1}{2} \end{pmatrix} \cdot \frac{1}{2} \rightarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \\ \hline \frac{1}{2} & 0 & \frac{1}{4} \\ 0 & \frac{1}{4} & -\frac{1}{4} \\ 0 & \frac{1}{4} & \frac{1}{4} \end{pmatrix} \cdot (-i) \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hline -\frac{i}{2} & 0 & -\frac{i}{4} \\ 0 & \frac{1}{4} & \frac{i}{4} \\ 0 & \frac{1}{4} & -\frac{i}{4} \end{pmatrix} =: \begin{pmatrix} A_3'' \\ D_3' \end{pmatrix}.$$

Järelikult on ruutvormi F_3 normaalkujud

$$\begin{aligned} F_3 &= -\Xi_1^2 + \Xi_2^2 - \Xi_3^2, & (\text{üle korpuse } \mathbb{R}), \\ F_3 &= \Upsilon_1^2 + \Upsilon_2^2 + \Upsilon_3^2, & (\text{üle korpuse } \mathbb{C}), \end{aligned} \quad (9)$$

kus $X^T = D_3 \Xi^T = D_3' \Upsilon^T$. Ruutvormi F_3 normaalkujus (9) võib muutujate järjekorda muuta, muutes ka vastavat üleminekumaatriksi järjekorda. Selliselt saame normaalkuju

$$F_3 = (\Xi_1')^2 - (\Xi_2')^2 - \Xi_3^2,$$

kus $\Xi_1' = \Xi_2$ ja $\Xi_2' = \Xi_1$.

4. Vaatleme ruutvormi $F_4 = X_1^2 + 5X_2^2 - X_3^2 + 6X_1X_2 + 4X_2X_3$, maatriksiga

$$A_4 := \begin{pmatrix} 1 & 3 & 0 \\ 3 & 5 & 2 \\ 0 & 2 & -1 \end{pmatrix}.$$

Otsime ruutvormi F_4 normaalkuju:

$$\begin{aligned} \begin{pmatrix} 1 & 3 & 0 \\ 3 & 5 & 2 \\ 0 & 2 & -1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - 3I &\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 2 \\ 0 & 2 & -1 \\ \hline 1 & -3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + 2III \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & -1 \\ \hline 1 & -3 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix} \cdot \frac{1}{3} \rightarrow \\ &\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \\ \hline 1 & -1 & 0 \\ 0 & \frac{1}{3} & 0 \\ 0 & \frac{2}{3} & 1 \end{pmatrix} \cdot (-i) \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hline 1 & -1 & 0 \\ 0 & \frac{1}{3} & 0 \\ 0 & \frac{2}{3} & -i \end{pmatrix} =: \begin{pmatrix} A_4'' \\ D_4' \end{pmatrix}. \end{aligned}$$

Järelikult on ruutvormi F_4 normaalkujud

$$\begin{aligned} F_4 &= \Xi_1^2 + \Xi_2^2 - \Xi_3^2, & (\text{üle korpuse } \mathbb{R}), \\ F_4 &= \Upsilon_1^2 + \Upsilon_2^2 + \Upsilon_3^2, & (\text{üle korpuse } \mathbb{C}), \end{aligned}$$

kus $X^T = D_4 \Xi^T = D_4' \Upsilon^T$.

Nagu näha on kõik ruutvormid F_1, F_2, F_3 ja F_4 üle korpuse $\mathbb{C}$ omavahel ekvivalentsed. Üle korpuse $\mathbb{R}$ on omavahel ekvivalentsed F_1 ja F_4 ning F_2 ja F_3 , kuna nende ruutvormide paaride normaalkujud on samad. $\square$

Ülesanne X.3. Leidke, kui palju on erinevaid mitteekvivalentseid ruutvorme n muutujast a) üle $\mathbb{C}$, b) üle $\mathbb{R}$.

Lahendus:

- a) Vastavalt loengukonspekti lausele 4.37 on kõik ruutvormid üle korpuse $\mathbb{C}$ viidavad kujule $X_1^2 + \dots + X_r^2$, kus $r \leq n$ (seda kinnitab ka eelmine ülesanne). Seega leidub üle korpuse $\mathbb{C}$ täpselt n erinevat mitteekvivalentset $n+1$ muutuja ruutvormi (iga $r \in \{0, \dots, n\}$ kohta üks).
- b) Üle korpuse $\mathbb{R}$ on iga n muutuja ruutvorm viidav kujule $X_1^2 + \dots + X_k^2 - X_{k+1}^2 - \dots - X_r^2$, kus $r \leq n$. Võime kujutleda seda ülesannet, kus meil on $n+2$ kohta, kuhu tahame panna sümboleid 0, 1, -1 ja kaks “üleminekut” sümboliseerivat sümbolit |. Põhimõtteliselt peame valima, kuhu paneme sümboleid | ning enne esimest paneme kõik kordajad 1, kahe sümboli | kordajad -1 ja viimase järele kordajad 0. Näiteks, kui $n = 9$, siis

$$1 \ 1 \ 1 \ | \ -1 \ -1 \ -1 \ -1 \ | \ 0 \ 0$$

vastab ruutvormile $X_1^2 + X_2^2 + X_3^2 - X_4^2 - X_5^2 - X_6^2 - X_7^2$. Ühesõnaga peame leidma, kui mitmel moel on võimalik kahte “ülemineku” sümbolit paigutada $n+2$ koha vahel. See on teadupoolest võrdne arvuga

$$\binom{n+1}{2} = \frac{(n+1)!}{2!(n-1)!} = \frac{n(n+1)}{2} = \frac{n^2+n}{2}.$$

Täpselt nii palju on mitteekvivalentseid n muutuja ruutvorme üle korpuse $\mathbb{R}$. $\square$

Märgime, et eelmises ülesandes kasutasime tegelikult *kordumistega kombinatsioonide* arvutamise valemit. Olgu antud m -elemendiline hulk (eelmises ülesandes oli selleks $\{-1, 0, 1\}$). Vaatleme ülesannet, kus tahetakse teada saada, mitmel viisil on võimalik sealt valida k -elemendilisi kombinatsioone nii, et iga element võib kuitahes palju kordi korduda. Sellist ülesannet saab arvutada kordumistega kombinatsioonide arvuga:

$$\left(\binom{m}{k}\right) := \binom{m+k-1}{k} = \binom{m+k-1}{m-1}.$$

(Ülal tuleneb teine võrdus kombinatsioonide arvu sümmeetriast.)

Ülesanne X.4. Leidke kõik parameetri a reaalarvulised väärtused, mille korral ruutvorm $aX_1^2 + 2aX_2^2 + (a-3)X_3^2 + 2X_1X_2 + 2aX_1X_3 + 2X_2X_3$ on negatiivselt määratud.

Lahendus: Vaatleme ruutvormi $F := aX_1^2 + 2aX_2^2 + (a-3)X_3^2 + 2X_1X_2 + 2aX_1X_3 + 2X_2X_3$ üle korpuse $\mathbb{R}$. Ruutvormi F maatriks on

$$A := \begin{pmatrix} a & 1 & a \\ 1 & 2a & 1 \\ a & 1 & a-3 \end{pmatrix}.$$

Leiame ruutvormi F kanoonilise kuju (tegelikult pole siin üleminekumaatriksit vaja, aga harjutamiseks leiame siiski)

$$\begin{pmatrix} a & 1 & a \\ 1 & 2a & 1 \\ a & 1 & a-3 \end{pmatrix} - I \rightarrow \begin{pmatrix} a & 1 & 0 \\ 1 & 2a & 0 \\ 0 & 0 & -3 \end{pmatrix} - \frac{1}{a}I \rightarrow \begin{pmatrix} a & 0 & 0 \\ 0 & 2a - \frac{1}{a} & 0 \\ 0 & 0 & -3 \end{pmatrix}.$$

Seega F kanoonilisel kujul on

$$F = aY_1^2 + \left(2a - \frac{1}{a}\right)Y_2^2 - 3Y_3^2.$$

Et ruutvorm oleks negatiivselt määratud peavad tema kanoonilisel kujul kõik kordajad olema negatiivsed. Järelikult $a < 0$ ning

$$\begin{aligned} 2a - \frac{1}{a} &< 0, \\ 2a^2 - 1 &> 0, \\ a^2 &> \frac{1}{2} \\ a &\notin \left[-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right]. \end{aligned}$$

Teadupoolest $\{a \mid a < 0\} \cap \{a \mid a^2 > \frac{1}{2}\} = (-\infty, -\frac{1}{\sqrt{2}})$. Järelikult on ruutvorm F negatiivselt määratud, siis kui $a < -\frac{1}{\sqrt{2}}$. $\square$

Ülesanne X.5. Leidke kõik parameetri a reaalarvulised väärtused, mille korral ruutvorm $2X_1^2 - X_2^2 + 4X_3^2 + (2a-1)X_1X_2 + a^2X_2X_3$ on positiivselt määratud.

Lahendus: Vaatleme ruutvormi $F := 2X_1^2 - X_2^2 + 4X_3^2 + (2a-1)X_1X_2 + a^2X_2X_3$ üle korpuse $\mathbb{R}$. Ruutvormi F maatriks on

$$A := \begin{pmatrix} 2 & a - \frac{1}{2} & 0 \\ a - \frac{1}{2} & -1 & \frac{a^2}{2} \\ 0 & \frac{a^2}{2} & 4 \end{pmatrix}.$$

Seda ülesannet võib lahendada analoogiliselt eelmise ülesandega, kuid kasutame siin hoopis loengukonspekti teoreemi 4.46. Arvutame maatriksi A peamiinorid:

$$M_3 = \begin{vmatrix} 2 & a - \frac{1}{2} & 0 \\ a - \frac{1}{2} & -1 & \frac{a^2}{2} \\ 0 & \frac{a^2}{2} & 4 \end{vmatrix} = -8 - \frac{a^4}{2} - 2\left(a - \frac{1}{2}\right)^2 = -\left(8 + \frac{a^4}{2} + 2\left(a - \frac{1}{2}\right)^2\right).$$

Ilmselt kehtib iga $a \in \mathbb{R}$ korral $M_3 < 0$, mistõttu ei ole ruutvorm F kunagi positiivselt määratud. (Tegelikult kehtib ka $M_2 > 0$, mille arvutamine on lihtsam.) $\square$

Märgin siinkohal, et loengukonspekti teoreemil 4.46 leidub ka analoogiline versioon negatiivselt määratud ruutvormide jaoks. Esitan selle ilma tõestuseta.

TEOREEM 3. Ruutfunktsionaal vektorruumil üle $\mathbb{R}$ on negatiivselt määratud parajasti siis, kui tema maatriksi peamiinorid rahuldavad tingimusi

$$M_1 < 0, \quad M_2 > 0, \quad M_3 < 0, \quad \dots, \quad (-1)^n M_n > 0.$$

Eelnevat teoreemi koos loengukonspekti teoreemiga 4.46 nimetatakse tihti ruutvormide *Sylvesteri kriteeriumiks*. Seda olete ilmselt kasutanud Mitme muutuja analüüsis mitme muutuja funktsiooni ekstreemumite leidmisel.

Ülesanne X.6. Tõestage, et eukleidilise ruumi sümmeetrilise lineaarteisenduse erinevatele omaväärtustele vastavad omavektorid on ortogonaalsed.

Lahendus: Olgu $\mathcal{E}$ eukleidiline ruum ja $f: \mathcal{E} \rightarrow \mathcal{E}$ sümmeetriline lineaarteisendus. Fikseerime teisenduse f kaks omaväärtust λ_1 ja λ_2 , kus $\lambda_1 \neq \lambda_2$, ning $v_1, v_2 \in \mathcal{E}$ neile omaväärtustele vastavad omavektorid. Sel juhul kehtib

$$\begin{aligned} \lambda_1 \langle v_1, v_2 \rangle &= \langle \lambda_1 v_1, v_2 \rangle = \langle f(v_1), v_2 \rangle \stackrel{(*)}{=} \langle v_1, f(v_2) \rangle = \langle v_1, \lambda_2 v_2 \rangle = \lambda_2 \langle v_1, v_2 \rangle, \\ \lambda_1 \langle v_1, v_2 \rangle - \lambda_2 \langle v_1, v_2 \rangle &= (\lambda_1 - \lambda_2) \langle v_1, v_2 \rangle = 0, \end{aligned}$$

millest $\langle v_1, v_2 \rangle = 0$. Seega vektorid v_1 ja v_2 on ortogonaalsed. (Võrdus $(*)$ tuleb sümmeetrilise teisenduse definitsioonist.) $\square$

Tänu eelmisele ülesandele saame uue algoritmi, kuidas leida ruutvormi kanoonilist kuju, milles kasutatakse omaväärtusi. Järgmises ülesandes kasutame seda algoritmi.

Ülesanne X.7. Viige ruutvorm

1. $2X_1^2 + 5X_2^2 + 5X_3^2 + 4X_1X_2 - 4X_1X_3 - 8X_2X_3$,
2. $8X_1^2 - 7X_2^2 + 8X_3^2 + 8X_1X_2 - 2X_1X_3 + 8X_2X_3$,

kanoonilisele kujule ortogonaalse muutujate vahetusega (s.o. muutujate vahetusega, mille maatriks on ortogonaalmaatriks).

Lahendus:

1. Vaatleme ruutvormi $F := 2X_1^2 + 5X_2^2 + 5X_3^2 + 4X_1X_2 - 4X_1X_3 - 8X_2X_3$, mille maatriks on

$$A := \begin{pmatrix} 2 & 2 & -2 \\ 2 & 5 & -4 \\ -2 & -4 & 5 \end{pmatrix}.$$

Leiame selle maatriksi omaväärtused:

$$\begin{aligned} \det(A - \lambda E) &= \begin{vmatrix} 2 - \lambda & 2 & -2 \\ 2 & 5 - \lambda & -4 \\ -2 & -4 & 5 - \lambda \end{vmatrix} = \begin{vmatrix} 2 - \lambda & 2 & -2 \\ 2 & 5 - \lambda & -4 \\ 0 & 1 - \lambda & 1 - \lambda \end{vmatrix} = \\ &= (1 - \lambda) \left(\begin{vmatrix} 2 - \lambda & 2 \\ 2 & 5 - \lambda \end{vmatrix} - \begin{vmatrix} 2 - \lambda & -2 \\ 2 & -4 \end{vmatrix} \right) = \\ &= (1 - \lambda) \begin{vmatrix} 2 - \lambda & 4 \\ 2 & 9 - \lambda \end{vmatrix} = (1 - \lambda)(\lambda^2 - 11\lambda + 10). \end{aligned}$$

Järelikult on A omaväärtused $\lambda_1 = 1$ (algebraalse kordsusega 2) ja $\lambda_2 = 10$ (algebraalse kordsusega 1). Ruutvormi F kanooniline kuju on

$$F = Y_1^2 + Y_2^2 + 10Y_3^2. \quad (10)$$

Selle uskumiseks on meil vaja leida (ortogonaalne) üleminekumaatriks ruutvormi F viimasele kujule.

Fikseerime omaväärtuse $\lambda_1 = 1$. Leiame talle vastavaid ortogonaalsed omavektoreid, selleks lahendame järgneva lineaarvõrrandisüsteemi (Gaussi meetodiga)

$$\begin{cases} x_1 + 2x_2 - 2x_3 = 0, \\ 2x_1 + 4x_2 - 4x_3 = 0, \\ -2x_1 - 4x_2 + 4x_3 = 0, \end{cases}$$

$$\left(\begin{array}{ccc|c} 1 & 2 & -2 & 0 \\ 2 & 4 & -4 & 0 \\ -2 & -4 & 4 & 0 \end{array} \right) \xrightarrow[-2I]{+2I} \left(\begin{array}{ccc|c} 1 & 2 & -2 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right), \quad \begin{cases} x_1 = 2c_2 - 2c_1, \\ x_2 = c_1, \\ x_3 = c_2. \end{cases}$$

Selle lineaarvõrrandisüsteemi lahendite fundamentaalsüsteemiks valime $\{(-2, 1, 0), (2, 0, 1)\}$. Ortogonaliseerime selle süsteemi Gram-Schmidt ortogonaliseerimisalgoritmiga:

$$v_1 = (-2, 1, 0),$$

$$v_2 = (2, 0, 1) - \frac{\langle (2, 0, 1), (-2, 1, 0) \rangle}{\langle (-2, 1, 0), (-2, 1, 0) \rangle} (-2, 1, 0) = (2, 0, 1) + \frac{4}{5}(-2, 1, 0) = \left(\frac{2}{5}, \frac{4}{5}, 1 \right).$$

Seega sobib meie otsitavaks ortogonaalsete omavektorite süsteemiks vektorite paar $\mathcal{B} := \{(-2, 1, 0), (\frac{2}{5}, \frac{4}{5}, 1)\}$.

Fikseerime omaväärtuse $\lambda_2 = 10$. Leiame ühe talle vastava omavektori, selleks lahendame järgneva lineaarvõrrandisüsteemi

$$\begin{cases} -8x_1 + 2x_2 - 2x_3 = 0, \\ 2x_1 - 5x_2 - 4x_4 = 0, \\ -2x_1 - 4x_2 - 5x_3 = 0, \end{cases} \quad \left(\begin{array}{ccc|c} -8 & 2 & -2 & 0 \\ 2 & -5 & -4 & 0 \\ -2 & -4 & -5 & 0 \end{array} \right) \xrightarrow[+II]{+4II} \rightarrow$$

$$\rightarrow \left(\begin{array}{ccc|c} 0 & -18 & -18 & 0 \\ 2 & -5 & -4 & 0 \\ 0 & -9 & -9 & 0 \end{array} \right) \xrightarrow{-III} \left(\begin{array}{ccc|c} 0 & 0 & 0 & 0 \\ 2 & -5 & -4 & 0 \\ 0 & -9 & -9 & 0 \end{array} \right) \xrightarrow{-4III} \left(\begin{array}{ccc|c} 0 & 0 & 0 & 0 \\ 2 & -5 & -4 & 0 \\ 0 & -9 & -9 & 0 \end{array} \right) \xrightarrow{\cdot(-\frac{1}{9})} \left(\begin{array}{ccc|c} 0 & 0 & 0 & 0 \\ 2 & -1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{array} \right).$$

Seega, viimase lineaarvõrrandisüsteemi lahendite fundamentaalsüsteemiks sobib $\{(1, 2, -2)\}$. Vastavalt eelmisele ülesandele X.6 teame, et vektor $(1, 2, -2)$ on süsteemi $\mathcal{B}$ vektoritega ortogonaalne. Seega oleme leidnud 3 ortogonaalset omavektorit $\mathcal{B}_1 = \mathcal{B} \cup \{(1, 2, -2)\} = \{(-2, 1, 0), (\frac{2}{5}, \frac{4}{5}, 1), (1, 2, -2)\}$. Lõpetuseks normeerime süsteemi $\mathcal{B}_1$ vektorid

$$w_1 := \frac{1}{\|(-2, 1, 0)\|} (-2, 1, 0) = \frac{1}{\sqrt{5}} (-2, 1, 0) = \left(-\frac{2}{\sqrt{5}}, \frac{1}{\sqrt{5}}, 0 \right),$$

$$w_2 := \frac{1}{\|(\frac{2}{5}, \frac{4}{5}, 1)\|} \begin{pmatrix} 2 \\ 5 \\ 5 \end{pmatrix} = \frac{\sqrt{5}}{3} \begin{pmatrix} 2 \\ 5 \\ 5 \end{pmatrix} = \begin{pmatrix} \frac{2}{3\sqrt{5}} \\ \frac{4}{3\sqrt{5}} \\ \frac{\sqrt{5}}{3} \end{pmatrix},$$

$$w_3 := \frac{1}{\|(1, 2, -2)\|} (1, 2, -2) = \frac{1}{3} (1, 2, -2) = \begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \\ -\frac{2}{3} \end{pmatrix}$$

ning tähistame $\mathcal{B}' := \{(-\frac{2}{\sqrt{5}}, \frac{1}{\sqrt{5}}, 0), (\frac{2}{3\sqrt{5}}, \frac{4}{3\sqrt{5}}, \frac{\sqrt{5}}{3}), (\frac{1}{3}, \frac{2}{3}, -\frac{2}{3})\}$.
Nüüd saame otsitud üleminekumaatriksi välja kirjutada

$$C := \begin{pmatrix} -\frac{2}{\sqrt{5}} & \frac{2}{3\sqrt{5}} & \frac{1}{3} \\ \frac{1}{\sqrt{5}} & \frac{4}{3\sqrt{5}} & \frac{2}{3} \\ 0 & \frac{\sqrt{5}}{3} & -\frac{2}{3} \end{pmatrix}.$$

Kontroll näitab, et C on ilusti ortogonaalne (s.t. $C^{-1} = C^T$). Kontrollime, kas C ikka viib ruutvormi F kujule (10):

$$C^T A C = \begin{pmatrix} -\frac{1}{\sqrt{5}} & \frac{1}{\sqrt{5}} & 0 \\ \frac{2}{3\sqrt{5}} & \frac{4}{3\sqrt{5}} & \frac{\sqrt{5}}{3} \\ \frac{1}{3} & \frac{2}{3} & -\frac{2}{3} \end{pmatrix} \begin{pmatrix} 2 & 2 & -2 \\ 2 & 5 & -4 \\ -2 & -4 & 5 \end{pmatrix} \begin{pmatrix} -\frac{2}{\sqrt{5}} & \frac{2}{3\sqrt{5}} & \frac{1}{3} \\ \frac{1}{\sqrt{5}} & \frac{4}{3\sqrt{5}} & \frac{2}{3} \\ 0 & \frac{\sqrt{5}}{3} & -\frac{2}{3} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 10 \end{pmatrix},$$

mis on täpselt see, mida me tahtsime.

2. Vaatleme ruutvormi $F := 8X_1^2 - 7X_2^2 + 8X_3^2 + 8X_1X_2 - 2X_1X_3 + 8X_2X_3$, mille maatriks on

$$A := \begin{pmatrix} 8 & 4 & -1 \\ 4 & -7 & 4 \\ -1 & 4 & 8 \end{pmatrix}.$$

Leiame ruutvormi A kanoonilise kuju, mille üleminekumaatriks on ortogonaalne analoogiliselt osaga 1, kuid seekord vähemate selgitustega. Leiame maatriksi A omaväärtused:

$$\begin{aligned} \det(A - \lambda E) &= \begin{vmatrix} 8 - \lambda & 4 & -1 \\ 4 & -7 - \lambda & 4 \\ -1 & 4 & 8 - \lambda \end{vmatrix} = \begin{vmatrix} 8 - \lambda & 4 & -1 \\ 4 & -7 - \lambda & 4 \\ \lambda - 9 & 0 & 9 - \lambda \end{vmatrix} = \\ &= (9 - \lambda) \left(\begin{vmatrix} 8 - \lambda & 4 \\ 4 & -7 - \lambda \end{vmatrix} - \begin{vmatrix} 4 & -1 \\ -7 - \lambda & 4 \end{vmatrix} \right) = \\ &= (9 - \lambda) \left(\begin{vmatrix} 8 - \lambda & 4 \\ 4 & -7 - \lambda \end{vmatrix} + \begin{vmatrix} -1 & 4 \\ 4 & -7 - \lambda \end{vmatrix} \right) = \\ &= (9 - \lambda) \begin{vmatrix} 7 - \lambda & 4 \\ 8 & -7 - \lambda \end{vmatrix} = (9 - \lambda)(x^2 - 81). \end{aligned}$$

Järelikult on A omaväärtused $\lambda_1 = 9$ (algebraalse kordsusega 2) ja $\lambda_2 = -9$ (algebraalse kordsusega 1). Seega on ruutvormi F kanooniline kuju

$$F = 9Y_1^2 + 9Y_2^2 - 9Y_3^2. \quad (11)$$

Fikseerime omaväärtuse $\lambda_1 = 9$ ja leiame kaks lineaarselt sõltumatut omavektorit. Lahendame lineaarvõrrandisüsteemi

$$\begin{cases} -x_1 + 4x_2 - x_3 = 0, \\ 4x_1 - 16x_2 + 4x_3 = 0, \\ -x_1 + 4x_2 - x_3 = 0, \end{cases}$$

$$\begin{pmatrix} -1 & 4 & -1 & | & 0 \\ 4 & -16 & 4 & | & 0 \\ -1 & 4 & -1 & | & 0 \end{pmatrix} \xrightarrow[-I]{-4I} \begin{pmatrix} -1 & 4 & -1 & | & 0 \\ 0 & 0 & 0 & | & 0 \\ 0 & 0 & 0 & | & 0 \end{pmatrix}, \quad \begin{cases} x_1 = 4c_1 - c_2, \\ x_2 = c_1, \\ x_3 = c_2. \end{cases}$$

Siit valime eelneva lineaarvõrrandisüsteemi lahendite fundamentaalsüsteemi kujul $\{(4, 1, 0), (-1, 0, 1)\}$. Ortogonaliseerime need vektorid

$$v_1 := (-1, 0, 1),$$

$$v_2 := (4, 1, 0) - \frac{\langle (-1, 0, 1), (4, 1, 0) \rangle}{\langle (-1, 0, 1), (-1, 0, 1) \rangle} (-1, 0, 1) = (4, 1, 0) + \frac{4}{2}(-1, 0, 1) = (2, 1, 2).$$

Fikseerime omaväärtuse $\lambda_2 = -9$ ja leiame ühe omavektori. Lahendame lineaarvõrrandisüsteemi

$$\begin{cases} 17x_1 + 4x_2 - x_3 = 0, \\ 4x_1 + 2x_2 + 4x_3 = 0, \\ -x_1 + 4x_2 + 17x_3 = 0, \end{cases} \quad \begin{pmatrix} 17 & 4 & -1 & | & 0 \\ 4 & 2 & 4 & | & 0 \\ -1 & 4 & 17 & | & 0 \end{pmatrix} \xrightarrow{+I}$$

$$\rightarrow \begin{pmatrix} 17 & 4 & -1 & | & 0 \\ 4 & 2 & 4 & | & 0 \\ 16 & 8 & 16 & | & 0 \end{pmatrix} \xrightarrow[-4II]{-2II} \begin{pmatrix} 17 & 4 & -1 & | & 0 \\ 4 & 2 & 4 & | & 0 \\ 0 & 0 & 0 & | & 0 \end{pmatrix} \rightarrow$$

$$\rightarrow \begin{pmatrix} 9 & 0 & -9 & | & 0 \\ 4 & 2 & 4 & | & 0 \\ 0 & 0 & 0 & | & 0 \end{pmatrix} \xrightarrow[\cdot \frac{1}{2}]{\cdot \frac{1}{9}} \begin{pmatrix} 1 & 0 & -1 & | & 0 \\ 2 & 1 & 2 & | & 0 \\ 0 & 0 & 0 & | & 0 \end{pmatrix} \xrightarrow{+2I} \begin{pmatrix} 1 & 0 & -1 & | & 0 \\ 4 & 1 & 0 & | & 0 \\ 0 & 0 & 0 & | & 0 \end{pmatrix}.$$

Seega antud lineaarvõrrandi lahendiruum on $\{(c, -4c, c) \mid c \in \mathbb{R}\}$ ning tema fundamentaalsüsteemiks sobib $\{(1, -4, 1)\}$.

Nüüd oleme leidnud kolm ortogonaalset omavektorit $\mathcal{B} = \{(-1, 0, 1), (2, 1, 2), (1, -4, 1)\}$. Normeerime need vektorid

$$w_1 := \frac{1}{\|(-1, 0, 1)\|}(-1, 0, 1) = \frac{1}{\sqrt{2}}(-1, 0, 1) = \left(-\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right),$$

$$w_2 := \frac{1}{\|(2, 1, 2)\|}(2, 1, 2) = \frac{1}{3}(2, 1, 2) = \left(\frac{2}{3}, \frac{1}{3}, \frac{2}{3}\right),$$

$$w_3 := \frac{1}{\|(1, -4, 1)\|}(1, -4, 1) = \frac{1}{3\sqrt{2}}(1, -4, 1) = \left(\frac{1}{3\sqrt{2}}, -\frac{2\sqrt{2}}{3}, \frac{1}{3\sqrt{2}}\right).$$

Nüüd oleme saanud ka ortogonaalse üleminekumaatriksi

$$C := \begin{pmatrix} -\frac{1}{\sqrt{2}} & \frac{2}{3} & \frac{1}{3\sqrt{2}} \\ 0 & \frac{1}{3} & -\frac{2\sqrt{2}}{3} \\ \frac{1}{\sqrt{2}} & \frac{2}{3} & \frac{1}{3\sqrt{2}} \end{pmatrix},$$

mille abil saab ruutvormi F viia kanoonilisele kujule (11).

□

Täiendav, mittekohustuslik teema Järgnevat ülesannet võiks vaadelda kui teatavat tärnülesannet. Selle lahendamiseks on vaja arendada natuke ruutvormide teooriat rohkem juurde, kui loengus (ja loengukonspektis) tehtud on. Teeme seda siinkohal. Nimelt näitame, et kahel ruutvormil leidub ühine muutujavahetus, mis viib mõlemad ruutvormid kanoonilisele kujule, kui vähemalt üks neist on positiivselt määratud.

Olgu meil V vektorruum üle korpuse K , F ja G ruutfunktsionaalid vektorruumil V , kusjuures G olgu positiivselt määratud. Sel juhul leidub sümmeetriline bilineaarne funktsionaal $g: V \times V \rightarrow K$ nii, et

$$\forall x \in V: \quad g(x, x) = G(x) > 0.$$

Sel juhul saab vektorruumis V defineerida skalaarkorrutise võrdusega

$$\langle x, y \rangle := g(x, y), \quad (x, y \in V),$$

nii saame ruumi V vaadelda kui eukleidilist ruumi. Tänu loengukonspekti teoreemile 4.35 leidub ruutfunktsionaalil F eukleidilises ruumis V ortonormeeritud kanooniline baas $\mathcal{B}$. Ilmselt on $\mathcal{B}$ ka ruutfunktsionaalile G kanooniliseks baasiks, kuna $\mathcal{B}$ on ju ortonormeeritud funktsionaali g suhtes. Nüüd lahendame järgneva ülesanne, mis ilmselt selgitab eelnevat mõttekäiku.

Ülesanne X.8. Leidke muutujate vahetus, mis viib ruutvormid

$$\begin{aligned} F &= X_1^2 + 2X_2^2 + 3X_3^2 + 2X_1X_2 - 2X_1X_3, \\ G &= 2X_1^2 + 8X_2^2 + 3X_3^2 + 8X_1X_2 + 2X_1X_3 + 4X_2X_3 \end{aligned}$$

korraga kanoonilisele kujule üle korpuse $\mathbb{R}$.

Lahendus: Vaatleme ruutvorme F ja G vektorruumil V üle korpuse $\mathbb{R}$, mille maatriksid antud baasi $\mathcal{B} = \{\epsilon_1, \epsilon_2, \epsilon_3\}$ suhtes on

$$A_F := A := \begin{pmatrix} 1 & 1 & -1 \\ 1 & 2 & 0 \\ -1 & 0 & 3 \end{pmatrix}, \quad A_G := B := \begin{pmatrix} 2 & 4 & 1 \\ 4 & 8 & 2 \\ 1 & 2 & 3 \end{pmatrix}.$$

Paneme tähele, et ruutvorm F on positiivselt määratud, kuna maatriksi A peamiinorid

$$A_3 = \begin{vmatrix} 1 & 1 & -1 \\ 1 & 2 & 0 \\ -1 & 0 & 3 \end{vmatrix} = 1, \quad A_2 = \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} = 1, \quad A_1 = \det(1) = 1$$

on kõik positiivsed. Seega võtame aluseks ruutvormi F ja defineerime skalaarkorrutise

$$\langle v, w \rangle = f(v, w), \quad (v, w \in V), \quad (12)$$

kus f on ruutfunktsionaalile F vastav sümmeetriline bilineaarne funktsionaal, mille väärtused baasi $\mathcal{B}$ vektoritel on antud maatriksis A . See tähendab, et suvaliste $(a_1, a_2, a_3), (b_1, b_2, b_3) \in V$ (baasil $\mathcal{B}$) saab skalaarkorrutist arvutada

$$\begin{aligned} \langle a_1\epsilon_1 + a_2\epsilon_2 + a_3\epsilon_3, b_1\epsilon_1 + b_2\epsilon_2 + b_3\epsilon_3 \rangle &= a_1b_1\langle\epsilon_1, \epsilon_1\rangle + a_1b_2\langle\epsilon_1, \epsilon_2\rangle + a_1b_3\langle\epsilon_1, \epsilon_3\rangle + \\ &\quad + a_2b_1\langle\epsilon_2, \epsilon_1\rangle + a_2b_2\langle\epsilon_2, \epsilon_2\rangle + a_2b_3\langle\epsilon_2, \epsilon_3\rangle + \\ &\quad + a_3b_1\langle\epsilon_3, \epsilon_1\rangle + a_3b_2\langle\epsilon_3, \epsilon_2\rangle + a_3b_3\langle\epsilon_3, \epsilon_3\rangle = \\ &= a_1b_1 + a_1b_2 - a_1b_3 + a_2b_1 + 2a_2b_2 - a_3b_1 + 3a_3b_3. \end{aligned}$$

Leiame eukleidilise ruumi $(V; \langle, \rangle)$ ortonormeeritud baasi. Selleks ortonormeerime tavalise baasi $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ skalaarkorrutise $\langle, \rangle$ mõttes. Siis Gram-Schmidt'i ortogonaliseerimisprotsess:

$$\begin{aligned} v_1 &:= (1, 0, 0), \\ v_2 &:= (0, 1, 0) - \frac{\langle(1, 0, 0), (0, 1, 0)\rangle}{\langle(1, 0, 0), (1, 0, 0)\rangle}(1, 0, 0) = (0, 1, 0) - \frac{1}{1}(1, 0, 0) = (-1, 1, 0), \\ v_3 &:= (0, 0, 1) - \frac{\langle(1, 0, 0), (0, 0, 1)\rangle}{\langle(1, 0, 0), (1, 0, 0)\rangle}(1, 0, 0) - \frac{\langle(-1, 1, 0), (0, 0, 1)\rangle}{\langle(-1, 1, 0), (-1, 1, 0)\rangle}(-1, 1, 0) = \\ &= (0, 0, 1) + \frac{1}{1}(1, 0, 0) - \frac{1}{1}(-1, 1, 0) = (2, -1, 1) \end{aligned}$$

Paneme tähele, et vektorite v_1, v_2 ja v_3 pikkus on kõigil 1 (skalaarkorrutise (12) suhtes). Seetõttu on $\mathcal{B}' = \{v_1, v_2, v_3\}$ eukleidilise ruumi $(V; \langle, \rangle)$ ortonormeeritud baas üleminekumaatriksiga

$$U = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Leiame ruutvormi G maatriksi baasi $\mathcal{B}'$ suhtes

$$B' = U^T B U = \begin{pmatrix} 2 & 2 & 1 \\ 2 & 2 & 1 \\ 1 & 1 & 3 \end{pmatrix}.$$

Nüüd leiame ruutvormi G ortonormeeritud kanoonilise baasi skalaarkorrutise (12) kohta. (Kuna me nüüd opereerime baasil $\mathcal{B}'$, siis edaspidi arvutame skalaarkorrutist tavalisel viisil, mitte valemi (12) abil.) Leiame maatriksi B' omaväärtused

$$\begin{aligned} \det(B' - \lambda E) &= \begin{vmatrix} 2-\lambda & 2 & 1 \\ 2 & 2-\lambda & 1 \\ 1 & 1 & 3-\lambda \end{vmatrix} = \begin{vmatrix} 2-\lambda & 2 & 1 \\ \lambda & -\lambda & 0 \\ 1 & 1 & 3-\lambda \end{vmatrix} = \\ &= \lambda \left(\begin{vmatrix} 2 & 1 \\ 1 & 3-\lambda \end{vmatrix} + \begin{vmatrix} 2-\lambda & 1 \\ 1 & 3-\lambda \end{vmatrix} \right) = \lambda \begin{vmatrix} 4-\lambda & 1 \\ 2 & 3-\lambda \end{vmatrix} = \end{aligned}$$

$$= \lambda((4 - \lambda)(3 - \lambda) - 2) = \lambda(\lambda^2 - 7\lambda + 10).$$

Järelikult on maatriksi B omaväärtused $\lambda_1 = 0$, $\lambda_2 = 2$, $\lambda_3 = 5$ (kõik algebralise kordsusega 1). Nüüd peame leidma igale omaväärtusele vastava omavektori.

Fikseerime omaväärtuse $\lambda_1 = 0$. Lahendame lineaarvõrrandisüsteemi

$$\begin{pmatrix} 2 & 2 & 1 \\ 2 & 2 & 1 \\ 1 & 1 & 3 \end{pmatrix} - I \rightarrow \begin{pmatrix} 2 & 2 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 3 \end{pmatrix} - 2III \rightarrow \begin{pmatrix} 0 & 0 & -5 \\ 0 & 0 & 0 \\ 1 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 5 \\ 5 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} + 3I.$$

Seega, omaväärtuse $\lambda_1 = 0$ omavektorite ruum on $\{(c, -c, 0) \mid c \in \mathbb{R}\}$, millest valime vektori $(1, -1, 0)$.

Fikseerime omaväärtuse $\lambda_2 = 2$. Lahendame lineaarvõrrandisüsteemi

$$\begin{pmatrix} 0 & 2 & 1 \\ 2 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} - 2III \rightarrow \begin{pmatrix} 0 & 2 & 1 \\ 0 & -2 & -1 \\ 1 & 1 & 1 \end{pmatrix} + I \rightarrow \begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 0 \\ 1 & -1 & 0 \end{pmatrix} - I.$$

Seega, omaväärtuse $\lambda_2 = 2$ omavektorite ruum on $\{(c, c, -2c) \mid c \in \mathbb{R}\}$, millest valime vektori $(1, 1, -2)$.

Fikseerime omaväärtuse $\lambda_3 = 5$. Lahendame lineaarvõrrandisüsteemi

$$\begin{pmatrix} -3 & 2 & 1 \\ 2 & -3 & 1 \\ 1 & 1 & -2 \end{pmatrix} - I \rightarrow \begin{pmatrix} -3 & 2 & 1 \\ 5 & -5 & 0 \\ -5 & 5 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 5 \\ 5 \end{pmatrix} \rightarrow \begin{pmatrix} -3 & 2 & 1 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} + 2I \rightarrow \begin{pmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Seega, omaväärtuse $\lambda_3 = 5$ omavektorite ruum on $\{(c, c, c) \mid c \in \mathbb{R}\}$, millest valime vektori $(1, 1, 1)$.

Tulenevalt ülesandest X.6 on kõik valitud vektorid ortogonaalsed. Normeerime need vektorid

$$\begin{aligned} w_1 &:= \frac{1}{\|(1, -1, 0)\|} (1, -1, 0) = \frac{1}{\sqrt{2}} (1, -1, 0) = \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0 \right), \\ w_2 &:= \frac{1}{\|(1, 1, -2)\|} (1, 1, -2) = \frac{1}{\sqrt{6}} (1, 1, -2) = \left(\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, -\frac{2}{\sqrt{6}} \right), \\ w_3 &:= \frac{1}{\|(1, 1, 1)\|} (1, 1, 1) = \frac{1}{\sqrt{3}} (1, 1, 1) = \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}} \right). \end{aligned}$$

Sellega oleme saanud ruutvormi G kanoonilise baasi $\mathcal{B}_C = \{w_1, w_2, w_3\}$, mis on skalaarkorrutise (12) järgi ortonormeeritud. Üleminekumaatriks baasilt $\mathcal{B}'$ baasile $\mathcal{B}_C$ on

$$D := \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{3}} \\ 0 & -\frac{2}{\sqrt{6}} & \frac{1}{\sqrt{3}} \end{pmatrix}.$$

Maatriks $C := UD$ on nüüd otsitud üleminekumaatriks baasilt $\mathcal{B}$ baasile $\mathcal{B}_C$.

Kontrolliks arvutame, et

$$C^T AC = D^T U^T A U D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$C^T BC = D^T U^T B U D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}.$$

Siit on näha, et muutjatevahetus (üleminekumatriks) C viibki ruutvormid F ja G mõlemad ilusasti kanoonilisele kujule, nagu tahetud oli. $\square$

Ülesanne* X.9. Olgu $f(X_1, \dots, X_n)$ ja $g(X_1, \dots, X_n)$ ruutvormid, kusjuures g on positiivselt määratud. Tõestada, et kanooniline kuju $f = \lambda_1 Y_1^2 + \dots + \lambda_n Y_n^2$ on iga muutujavahetuse korral, mis viib g normaalkujule, määratud üheselt liidetavate järjekorra täpsuseni, kusjuures $\lambda_1, \dots, \lambda_n$ on nn λ -võrrandi $\det(A - \lambda B) = 0$ lahendid, kus A ja B on vormide f ja g matriksid.

Praktikum XI Tsüklilised rühmad

Olgu G lõplik rühm. Nagu loengukonspektist teada, siis tähistatakse elemendi $g \in G$ järku $\text{ord}(g)$. Vastavalt traditsioonile tähistan rühma G järku $\text{Ord}(G)$. Muidugi langeb (alam)rühma järgu mõiste kokku selle rühma alushulga võimsusega, siis

$$\text{Ord}(G) := \#(G) = |G|.$$

(Ω -algebra $(A; \Omega)$ *alushulgaks* nimetatakse hulka A).

Ülesanne XI.1. Leida substitutsioonide rühma S_3 kõigi elementide järgud.

Lahendus: Vaatleme substitutsioonide rühma $(S_3, \circ)$, kuhu kuuluvad kõik hulga $\{1, 2, 3\}$ bijektsioonid. Hulgaks S_3 on $3! = 6$ elementi. Vaatleme neid elemente, esitades neid kaherealiste maatriksitena. Esiteks ühikelement

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id},$$

ilmselt kehtib $\text{ord}(\text{id}) = 1$ nagu alati ühikelemendi korral. Vaatleme ülejäänud elemente ja arvutame nende astmed ning sellest järeldame nende järgud

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id}$$

$$\implies \text{ord} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = 2;$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id}$$

$$\implies \text{ord} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = 2;$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id}$$

$$\implies \text{ord} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = 3;$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id}$$

$$\implies \text{ord} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = 3;$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{id}$$

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

Sellega oleme leidnud substitutsioonide rühma S_3 kõikide elementide järgud. Paneme tähele, et meie tähistuses esitub tsükkel $(1, 3, 2)$ kujul $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ ning selle elemendi järk on tõesti 3 nagu ka loengukonspekti näites 5.8 (2).

Kuna suurim elemendi järk rühmas S_3 on 3, siis rühm S_3 ei ole tsükliline. $\square$

Olgu R ring. Tähistame sümboliga $U(R)$ kõigi ringi R pööratavate elementide (korrumise suhtes) rühma korrumise suhtes.

Ülesanne XI.2. Leida elementide $g \in G$ järk ning alamrühm $\langle g \rangle$, kus

1. $G = (\mathbb{Z}_{42}, +)$ ja $g \in \{\overline{12}, \overline{13}, \overline{14}\}$;
2. $G = \mathbb{C}$ ja $g \in \{\frac{1-i}{\sqrt{2}}, 1+i\}$;
3. $G = \mathbb{Z}_{15}$ ja $g = \overline{7}$;
4. $G = U(\mathbb{Z}_{15})$ ja $g = \overline{7}$;
5. $G = \mathbb{Z}_3 \oplus \mathbb{Z}_5$ ja $g = (\overline{1}, \overline{3})$.

Lahendus:

1. Vaatleme rühma $(\mathbb{Z}_{42}, +)$. Fikseerime elemendi $\overline{12} \in \mathbb{Z}_{42}$. Arvutame tema astmed (kuna meil on tegemist aditiivse rühmaga, siis aste on tegelikult korrumamine)

$$\begin{aligned} 2 \cdot \overline{12} &= \overline{24}, \\ 3 \cdot \overline{12} &= \overline{36}, \\ 4 \cdot \overline{12} &= \overline{48} = \overline{6}, \\ 5 \cdot \overline{12} &= \overline{18}, \\ 6 \cdot \overline{12} &= \overline{30}, \\ 7 \cdot \overline{12} &= \overline{42} = \overline{0}. \end{aligned}$$

Seega $\text{ord}_{\mathbb{Z}_{42}}(\overline{12}) = 7$ ning lisaks näeme, et

$$\langle \overline{12} \rangle = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}, \overline{30}, \overline{36}\}.$$

Fikseerime elemendi $\overline{13} \in \mathbb{Z}_{42}$. Paneme tähele, et $\text{SÜT}(13, 42) = 1$, siis loengukonspekti lause 5.12 põhjal saame, et $\overline{13}$ on rühma $\mathbb{Z}_{42}$ moodustaja (jätkuvalt meenutan, et aditiivses rühmas on korrumamine astendamise rollis ning ilmselt $\overline{13} = 13 \cdot \overline{1}$). Seega

$$\text{ord}_{\mathbb{Z}_{42}}(\overline{13}) = 42, \quad \langle \overline{13} \rangle = \mathbb{Z}_{42}.$$

Fikseerime elemendi $\overline{14} \in \mathbb{Z}_{42}$. Arvutame elemendi $\overline{14}$ astmed

$$\begin{aligned} 2 \cdot \overline{14} &= \overline{28}, \\ 3 \cdot \overline{14} &= \overline{42} = \overline{0}. \end{aligned}$$

Seega kehtib

$$\text{ord}_{\mathbb{Z}_{42}}(\overline{14}), \quad \langle \overline{14} \rangle = \{\overline{0}, \overline{14}, \overline{28}\}.$$

2. Vaatleme rühma $(\mathbb{C}, +)$ (ilmselt on siin mõeldud aditiivset rühma, kuna korrutamise suhtes ei moodusta $\mathbb{C}$ rühma). Vaatleme elemente $\frac{1-i}{\sqrt{2}}, 1+i \in \mathbb{C}$. Ilmselt ei teki kummagi elemendi iseendale liitmisel kunagi arvu 0. Järelikult kehtib

$$\begin{aligned} \text{ord}_{\mathbb{C}}\left(\frac{1-i}{\sqrt{2}}\right) &= \text{ord}_{\mathbb{C}}(1+i) = \infty, \\ \left\langle \frac{1-i}{\sqrt{2}} \right\rangle &= \left\{ \frac{z}{\sqrt{2}} - i \frac{z}{\sqrt{2}} \mid z \in \mathbb{Z} \right\}, \\ \langle 1+i \rangle &= \{z + iz \mid z \in \mathbb{Z}\}. \end{aligned}$$

3. Vaatleme rühma $(\mathbb{Z}_{15}, +)$ (sarnaselt eelmise punktiga, on siin ilmselt aditiivne rühm). Fikseerime elemendi $\bar{7} \in \mathbb{Z}_{15}$. Paneme tähele, et $\text{SÜT}(7, 15) = 1$, mistõttu taaskord loengukonspekti lause 5.12 järgi on $\bar{7}$ rühma $\mathbb{Z}_{15}$ moodustaja. Seega

$$\text{ord}_{\mathbb{Z}_{15}}(\bar{7}) = 15, \quad \langle \bar{7} \rangle = \mathbb{Z}_{15}.$$

4. Uurime, millised elemendid on ringis $(U(\mathbb{Z}_{15}), +, \cdot)$ pööratavad. Pööratavaid elemente võib leida lihtsalt kõigile elementidele pöördelemente leides. Loengukonspekti lausest 5.4 järeldub, et element $\bar{a} \in \mathbb{Z}_m$ on pööratav parajasti siis, kui $\text{SÜT}(a, m) = 1$ (see väide tõestatakse põhjalikult Arvuteoorias). Seega kirjutame välja hulga $U(\mathbb{Z}_{15})$ elemendid

$$U(\mathbb{Z}_{15}) = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\},$$

mistõttu

$$\text{Ord}(U(\mathbb{Z}_{15})) = \#(U(\mathbb{Z}_{15})) = 8.$$

Fikseerime elemendi $\bar{7} \in U(\mathbb{Z}_{15})$. Arvutame elemendi $\bar{7}$ astmed (kuna meil on praegu multiplikatiivne rühm, siis on astendamise rollis tavaline astendamine)

$$\begin{aligned} \bar{7}^2 &= \overline{49} = \bar{4}, \\ \bar{7}^3 &= \overline{28} = \bar{13}, \\ \bar{7}^4 &= \overline{91} = \bar{1}. \end{aligned}$$

Järelikult kehtib

$$\text{ord}_{U(\mathbb{Z}_{15})}(\bar{7}) = 4, \quad \langle \bar{7} \rangle = \{\bar{1}, \bar{4}, \bar{7}, \bar{13}\}.$$

5. Vaatleme rühma $\mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_5$ (välise otsesumma definitsiooni tõttu (loengukonspekt lk. 25)), mida vaatleme taaskord rühmana liitmise suhtes. Arvutame elemendi $(\bar{1}, \bar{3})$ astmed

$$\begin{aligned} 1 \cdot (\bar{1}, \bar{3}) &= (\bar{1}, \bar{3}), & 6 \cdot (\bar{1}, \bar{3}) &= (\bar{3}, \bar{3}) = (\bar{0}, \bar{3}), & 11 \cdot (\bar{1}, \bar{3}) &= (\bar{2}, \bar{3}), \\ 2 \cdot (\bar{1}, \bar{3}) &= (\bar{2}, \bar{6}) = (\bar{2}, \bar{1}), & 7 \cdot (\bar{1}, \bar{3}) &= (\bar{1}, \bar{6}) = (\bar{1}, \bar{1}), & 12 \cdot (\bar{1}, \bar{3}) &= (\bar{3}, \bar{6}) = (\bar{0}, \bar{1}), \\ 3 \cdot (\bar{1}, \bar{3}) &= (\bar{3}, \bar{4}) = (\bar{0}, \bar{4}), & 8 \cdot (\bar{1}, \bar{3}) &= (\bar{2}, \bar{4}), & 13 \cdot (\bar{1}, \bar{3}) &= (\bar{1}, \bar{4}), \\ 4 \cdot (\bar{1}, \bar{3}) &= (\bar{1}, \bar{7}) = (\bar{1}, \bar{2}), & 9 \cdot (\bar{1}, \bar{3}) &= (\bar{3}, \bar{7}) = (\bar{0}, \bar{2}), & 14 \cdot (\bar{1}, \bar{3}) &= (\bar{2}, \bar{7}) = (\bar{2}, \bar{2}), \\ 5 \cdot (\bar{1}, \bar{3}) &= (\bar{2}, \bar{5}) = (\bar{2}, \bar{0}), & 10 \cdot (\bar{1}, \bar{3}) &= (\bar{1}, \bar{5}) = (\bar{1}, \bar{0}), & 15 \cdot (\bar{1}, \bar{3}) &= (\bar{3}, \bar{5}) = (\bar{0}, \bar{0}). \end{aligned}$$

Eelnevast näeme, et

$$\text{ord}_{\mathbb{Z}_3 \times \mathbb{Z}_5}((\bar{1}, \bar{3})) = 15, \quad \langle (\bar{1}, \bar{3}) \rangle = \mathbb{Z}_3 \times \mathbb{Z}_5.$$

Vaadeldes hoolega eelnevalt arvutatud rühma $\mathbb{Z}_3 \times \mathbb{Z}_5$ näeme, et kehtib valem

$$\text{ord}_{G \times H}((a, b)) = \text{VÜK}(\text{ord}_G(a), \text{ord}_H(b)),$$

kus G ja H on lõplikud rühmad. Samuti näeme, et tsükliliste rühmade otsekorrutise element on selle rühma moodustaja parajasti siis, kui ta koosneb vastavate rühmade moodustajatest. $\square$

Ülesanne XI.3. Olgu $G = \langle g \rangle$, $|G| = 12$. Leida $G/\langle g^k \rangle$, kus $k = 6, 7, 8$.

Lahendus: Olgu G tsükliline rühm moodustajaga g , mille korral $\text{Ord}(G) = \#(G) = 12$ ja ε on rühma G ühikelement. Ilmselt kehtib $\text{ord}_G(g) = 12$. (Vastavalt loengukonspekti teoreemile 5.5 on rühm G isomorfne rühmaga $(\mathbb{Z}_{12}, +)$, mistõttu võiksime edasi arvestada $G = \mathbb{Z}_{12}$. Sel juhul $g \in \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$. Ma esitan vastused mõlemal juhul.)

$k = 6$: Paneme tähele, et $\text{SÜT}(6, 12) = 6$ ning $12 = 2 \cdot 6$. Tänu loengukonspekti lemmale 5.14 teame, et $\text{ord}(g^6) = 2$. Siit saame, et alamrühm $\langle g^6 \rangle$ on kaheelemendiline, mistõttu $\langle g^6 \rangle = \{\varepsilon, g^6\}$. Uurime faktorrühma $G/\langle g^6 \rangle$. Olgu $a \in G$, siis leidub $h \in \mathbb{N}$ nii, et $a = g^h$ ning

$$[a] = [g^h] = g^h \cdot \{\varepsilon, g^6\} = \{g^h, g^h g^6\} = \{g^h, g^{h+6}\}.$$

Seega

$$G/\langle g^6 \rangle = \{\{g^h, g^{h+6}\} \mid h \in \{0, 1, \dots, 5\}\} \implies \#(G/\langle g^6 \rangle) = 6.$$

(Kui $G = \mathbb{Z}_{12}$, siis kehtib $6g = \bar{6}$. Lisaks kehtivad $\langle 6g \rangle = \{\bar{0}, \bar{6}\}$ ja $\mathbb{Z}_{12}/\langle 6g \rangle = \{\{\bar{0}, \bar{6}\}, \{\bar{1}, \bar{7}\}, \{\bar{2}, \bar{8}\}, \{\bar{3}, \bar{9}\}, \{\bar{4}, \bar{10}\}, \{\bar{5}, \bar{11}\}\}$.)

$k = 7$: Märkame, et $\text{SÜT}(7, 12) = 1$. Järelikult g^7 on rühma G moodustaja, mistõttu $\langle g^7 \rangle = G$. Seega

$$G/\langle g^7 \rangle = G/G = \{G\} = \{[1_G]\}$$

ehk faktorrühm $G/\langle g^7 \rangle$ on triviaalne rühm ($\#(G/\langle g^7 \rangle) = 1$).

$k = 8$: Arvutame $\text{SÜT}(12, 8) = 4$ ning ilmselt $12 = 3 \cdot 4$. Kasutades taaskord loengukonspekti lemmat 5.14 ning saame, et $\text{ord}(g^8) = 3$. Oleme saanud, et alamrühm $\langle g^8 \rangle$ on kolmeelemendiline ning $\langle g^8 \rangle = \{\varepsilon, g^4, g^8\}$, kuna kehtib

$$g^8 g^8 = g^{16} = g^{12+4} = g^{12} g^4 = g^4.$$

Nüüd teame, et

$$G/\langle g^8 \rangle = \{\{g^h, g^{h+4}, g^{h+8}\} \mid h \in \{0, 1, 2, 3\}\} \implies \#(G/\langle g^8 \rangle) = 4.$$

(Kui $G = \mathbb{Z}_{12}$, siis $8g \in \{\bar{4}, \bar{8}\}$. Seetõttu $\langle 8g \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$ ning $\mathbb{Z}_{12}/\langle 8g \rangle = \{\{\bar{0}, \bar{4}, \bar{8}\}, \{\bar{1}, \bar{5}, \bar{9}\}, \{\bar{2}, \bar{6}, \bar{10}\}, \{\bar{3}, \bar{7}, \bar{11}\}\}$.)

$\square$

Toon siinkohal ära ühe lemma arvuteooriast. Toon siinkohal ära ka selle lemma tõestuse, kuid siin aines pole see kohustuslik.

Lemma 6. Olgu G rühm, $a \in G$ ja $\text{ord}(a) = m \in \mathbb{N}$ ning $k \in \mathbb{N}_1$. Siis kehtib $a^k = \varepsilon$ parajasti siis, kui $m \mid k$.

Tõestus. ($\implies$) Kehtigu $a^k = \varepsilon$. Tänu loengukonspekti lausele 5.3 leiduvad $q, r \in \mathbb{Z}$ nii, et $k = qm + r$ ja $0 \leq r < m$. Nüüd

$$\varepsilon = a^k = a^{qm+r} = a^{qm}a^r = (a^m)^qa^r = \varepsilon^qa^r = a^r.$$

Kuna m on vähim nullist erinev naturaalarv, mille korral $a^m = \varepsilon$, siis $r = 0$. Järelikult $k = qm$, mistõttu $m \mid k$.

($\impliedby$) Kehtigu $m \mid k$, mistõttu leidub $h \in \mathbb{Z}$ nii, et $k = hm$. Sel juhul kehtib $a^k = a^{hm} = (a^m)^h = \varepsilon^h = \varepsilon$ nagu tahetud. ■

Ülesanne XI.4. Tõestada, et n -dat järku tsüklilise rühma mistahes alamrühm on tsükliline ja iga $d \mid n$ korral leidub täpselt üks d -ndat järku alamrühm.

Lahendus: Olgu G tsükliline rühm moodustajaga $g \in G$ ja kehtigu tingimus $\text{Ord}(G) = \#(G) = n \in \mathbb{N}_1$.

Olgu $H \subseteq G$ alamrühm. Kui H on triviaalne, s.t. $H = \{\varepsilon\}$, siis ilmselt on H tsükliline moodustajaga ε . Edaspidi oletame, et $\{\varepsilon\} \subset H$. Kuna g on rühma G moodustaja, siis iga elemendi $h \in H$ korral leidub naturaalarv $k \in \mathbb{N}$ nii, et $h = g^k$. Valime vähima $m \in \mathbb{N}_1$, mille korral $g^m \in H$. Olgu $h = g^k \in H \setminus \{\varepsilon\}$ suvaline. Saame jäägiga jagada ehk leiame arvud $q, r \in \mathbb{Z}$, kus $0 \leq r < m$ ja

$$k = qm + r.$$

Nüüd

$$h = g^k = g^{qm+r} = (g^m)^q g^r \implies g^r = g^k (g^m)^{-q}.$$

Vastavalt eeldusele $g^k, g^m \in H$ ning kuna H on rühm, siis ka $(g^m)^{-q}, g^k (g^m)^{-q} \in H$. Järelikult $g^r \in H$, kuna aga k on vähim nullist erinev naturaalarv, mille korral $g^k \in H$, peab kehtima $r = 0$. Seega $g^k = (g^m)^q g^0 = (g^m)^q \varepsilon = (g^m)^q$. Siit näeme, et $H = \langle g^m \rangle$, mistõttu H on tsükliline.

Tänu Lagrange'i teoreemile 1.46 teame, et iga alamrühma $H \subseteq G$ järk jagab arvu n ehk kehtib $\#(G) \mid n$.

Olgu $d \mid n$. Vaatleme alamrühma

$$\langle g^{\frac{n}{d}} \rangle = \{g^{\frac{n}{d}}, g^{2\frac{n}{d}}, \dots, g^{d\frac{n}{d}} = \varepsilon\} \implies \#(\langle g^{\frac{n}{d}} \rangle) = d.$$

Järelikult on alamrühma $\langle g^{\frac{n}{d}} \rangle$ järk d . Oletame vastuväiteliselt, et leidub alamrühm $H \subseteq G$ nii, et $\#(H) = d$ ja $H \neq \langle g^{\frac{n}{d}} \rangle$. Kuna H on tsükliline, siis saame valida alamrühma H moodustaja g^k , kusjuures $\text{ord}(g^k) = d$, mistõttu $g^{kd} = \varepsilon = g^n$. Järelikult tänu lemmale 6 leidub naturaalarv s nii, et $kd = sn$, kust $k = s\frac{n}{d}$. Olgu $h \in H$, siis leidub $q \in \mathbb{N}$ nii, et $h = (g^k)^q$ ning sel juhul

$$h = (g^k)^q = (g^{s\frac{n}{d}})^q = (g^{\frac{n}{d}})^{sq} \in \langle g^{\frac{n}{d}} \rangle.$$

Seega $H \subseteq \langle g^{\frac{n}{d}} \rangle$. Teisest küljest $\#(H) = \#(\langle g^{\frac{n}{d}} \rangle)$, millest saame $H = \langle g^{\frac{n}{d}} \rangle$. ✎

Eelmine ülesanne on väga kasulik. Selle kasulikkust demonstreerib järgmine ülesanne.

Ülesanne XI.5. Leida kõik 12-elemendilise tsüklilise rühma alamrühmad.

Lahendus: Loengukonspekti teoreemist 5.5 on teada, et kõik sama järku tsüklilised alamrühmad on isomorfsed, seepärast vaatleme siin ülesandes rühma $(\mathbb{Z}_{12}, +)$. Ülesandest XI.4 on teada, et $\mathbb{Z}_{12}$ kõik alamrühmad on tsüklilised, seega piisab meil kõiki alamrühmi otsides vaadelda alamrühmi $\langle a \rangle$, kus $a \in \mathbb{Z}_{12}$. Lisaks jäeldame loengukonspekti järelausest 5.15 ja eelmisest ülesandest, et kui $\text{SÜT}(b, 12) = \text{SÜT}(c, 12)$, siis $\langle \bar{b} \rangle = \langle \bar{c} \rangle$. Vaatleme kõik rühma $\mathbb{Z}_{12}$ elemendid läbi:

$$\begin{aligned}
& \langle \bar{0} \rangle = \{ \bar{0} \} \quad (\text{Ord}(\langle \bar{0} \rangle) = 1); \\
\text{SÜT}(1, 12) = 1: & \quad \langle \bar{1} \rangle = \mathbb{Z}_{12}, \quad (\text{Ord}(\langle \bar{1} \rangle) = 12); \\
\text{SÜT}(2, 12) = 2: & \quad \langle \bar{2} \rangle = \{ \bar{2}, 2 \cdot \bar{2} = \bar{4}, 3 \cdot \bar{2} = \bar{6}, 4 \cdot \bar{2} = \bar{8}, 5 \cdot \bar{2} = \bar{10}, 6 \cdot \bar{2} = \bar{0} \} = \\
& \quad = \{ \bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10} \}, \quad (\text{Ord}(\langle \bar{2} \rangle) = 6); \\
\text{SÜT}(3, 12) = 3: & \quad \langle \bar{3} \rangle = \{ \bar{3}, 2 \cdot \bar{3} = \bar{6}, 3 \cdot \bar{3} = \bar{9}, 4 \cdot \bar{3} = \bar{0} \} = \{ \bar{0}, \bar{3}, \bar{6}, \bar{9} \}, \quad (\text{Ord}(\langle \bar{3} \rangle) = 4); \\
\text{SÜT}(4, 12) = 4: & \quad \langle \bar{4} \rangle = \{ \bar{4}, 2 \cdot \bar{4} = \bar{8}, 3 \cdot \bar{4} = \bar{0} \} = \{ \bar{0}, \bar{4}, \bar{8} \}, \quad (\text{Ord}(\langle \bar{4} \rangle) = 3); \\
\text{SÜT}(5, 12) = 1: & \quad \langle \bar{5} \rangle = \mathbb{Z}_{12}; \\
\text{SÜT}(6, 12) = 6: & \quad \langle \bar{6} \rangle = \{ \bar{6}, 2 \cdot \bar{6} = \bar{0} \} = \{ \bar{0}, \bar{6} \}, \quad (\text{Ord}(\langle \bar{6} \rangle) = 2); \\
\text{SÜT}(7, 12) = 1: & \quad \langle \bar{7} \rangle = \mathbb{Z}_{12}; \\
\text{SÜT}(8, 12) = 4: & \quad \langle \bar{8} \rangle = \langle \bar{4} \rangle; \\
\text{SÜT}(9, 12) = 3: & \quad \langle \bar{9} \rangle = \langle \bar{3} \rangle; \\
\text{SÜT}(10, 12) = 2: & \quad \langle \bar{10} \rangle = \langle \bar{2} \rangle; \\
\text{SÜT}(11, 12) = 1: & \quad \langle \bar{11} \rangle = \mathbb{Z}_{12}.
\end{aligned}$$

Sellega oleme leidnud kõik rühma $\mathbb{Z}_{12}$ alamrühmad. Nagu näha leidub igale järgu 12 jagajale 1, 2, 3, 4, 6, 12 ka vastav alamrühm nagu oli tahetud. $\square$

Pannes ülesanded XI.3 ja XI.5 kokku näeme, et tegelikult on lõpliku tsüklilise rühma $\mathbb{Z}_n$ alamrühmad alati paaris. Nimelt iga $d \mid n$ korral kehtib

$$\begin{aligned}
\mathbb{Z}_n / \langle \bar{d} \rangle & \cong \left\langle \frac{n}{d} \right\rangle, \\
\mathbb{Z}_n / \left\langle \frac{n}{d} \right\rangle & \cong \langle \bar{d} \rangle.
\end{aligned}$$

Olgu G rühm. Lõpliku järku elemendi $g \in G$ (või alamrühma $\langle g \rangle$) *indeksiks* nimetatakse alamrühma $G/\langle g \rangle$ järku. Sümbolites

$$\text{ind}_G(g) = \text{ind}_G(\langle g \rangle) := \text{Ord}(G/\langle g \rangle) = \frac{\text{Ord}(G)}{\text{ord}(g)}.$$

Ülesanne XI.6. Tõestada, et rühma G mistahes elementide a , b ja c korral

1. elementidel ab ja ba on sama järk;
2. elementidel abc , bca ja cab on sama järk;
3. elementide abc ja cba järgud võivad olla erinevad.

Lahendus: Olgu G rühm ja $a, b, c \in G$.

1. Vaatleme elemente ab ja ba . Olgu $\text{ord}(ab) = n$, siis $(ab)^n = \varepsilon$. Paneme tähele, et

$$(ba)^n = (ba)^n bb^{-1} = b(\underbrace{ababab \dots ab}_{n-1})abb^{-1} = b(ab)^n b^{-1} = bb^{-1} = \varepsilon.$$

Seega $\text{ord}(ab) \mid n$. Analoogiliselt saame, et $\text{ord}(ba) \mid \text{ord}(ab)$, mistõttu kehtib $\text{ord}(ab) = \text{ord}(ba)$.

2. Vaatleme elemente abc , bca ja cab . Olgu $\text{ord}(abc) = n$, siis kehtib taaskord $(abc)^n = \varepsilon$. Paneme tähele, et analoogiliselt eelmise punktiga

$$\begin{aligned}(bca)^n &= (bca)^n (bc)(bc)^{-1} = bc(abc)^n (bc)^{-1} = bc(bc)^{-1} = \varepsilon, \\ (cab)^n &= (cab)^n cc^{-1} = c(abc)^n c^{-1} = cc^{-1} = \varepsilon.\end{aligned}$$

Seega $\text{ord}(bca) \mid n$ ja $\text{ord}(cab) \mid n$. Sarnaselt eelmise punktiga saame siit tahetud $\text{ord}(abc) = \text{ord}(bca) = \text{ord}(cab)$.

3. Selles osas vaatleme taaskord ülesandes XI.1 vaadeldud substitutsioonide rühma S_3 . Tähistame

$$a := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad b := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad c := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Arvutame

$$\begin{aligned}a \circ b \circ c &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \\ c \circ b \circ a &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.\end{aligned}$$

Ülesandest XI.1 saame nüüd, et

$$\begin{aligned}\text{ord}(a \circ b \circ c) &= 3, \\ \text{ord}(c \circ b \circ a) &= \text{ord}(\text{id}) = 1.\end{aligned}$$

See kontranäide lahendabki antud ülesande.

□

Mainin, et elementide järjestuse abc ümberjärjestusi bca ja cab nimetatakse *tsüklilisteks ümberjärjestusteks*.

Ülesanne XI.7. Tõestada, et kompleksarvu z järk rühmas $\mathbb{C} \setminus \{0\}$ on lõplik parajasti siis, kui $|z| = 1$ ja $\frac{1}{\pi} \arg z \in \mathbb{Q}$.

Lahendus: Vaatleme rühma $(\mathbb{C} \setminus \{0\}, \cdot)$ (ilmselt on siin mõeldud kompleksarvude multiplikatiivset rühma, kuna $(\mathbb{C} \setminus \{0\}, +)$ pole rühm).

($\implies$) Olgu $\text{ord}(z) = n \in \mathbb{N}$. Sel juhul kehtib

$$1 = z^n = (|z| \exp(i \arg z))^n = |z|^n \exp(in \arg z).$$

Siit järeldub, et $|z| = 1$ ja

$$\begin{aligned}\exists m \in \mathbb{Z}: \quad 2m\pi i &= in \arg z, \\ n &= \frac{2m\pi}{\arg z}.\end{aligned}$$

Kuna vastavalt eeldusele $n \in \mathbb{N}$, siis järelikult $\frac{\pi}{\arg z} \in \mathbb{Q}$ ning ilmselt ka

$$\frac{\arg z}{\pi} = \left(\frac{\pi}{\arg z} \right)^{-1} \in \mathbb{Q}.$$

($\Leftarrow$) Olgu $z \in \mathbb{C}$ selline, et $|z| = 1$ ja $\frac{\arg z}{\pi} \in \mathbb{Q}$, siis $\arg z = \pi \frac{m_1}{m_2}$ mingite $m_1, m_2 \in \mathbb{Z}$ korral. Sel juhul vastavalt tõestuse eelmisele osale

$$\text{ord}(z) = 2m_2$$

ehk z on ilmselt lõpliku järku. □

Kasutades eelmist ülesannet toon ära, et näiteks

$$\begin{aligned}\text{ord}_{\mathbb{C} \setminus \{0\}}(i) &= 4, \quad \langle i \rangle = \{1, i, -1, -i\}, \\ \text{ord}_{\mathbb{C} \setminus \{0\}}\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) &= 6, \quad \left(\arg\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = \frac{\pi}{3}\right), \\ \left\langle \frac{1}{2} + i\frac{\sqrt{3}}{2} \right\rangle &= \left\{1, \frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -1, -\frac{1}{2} - i\frac{\sqrt{3}}{2}, \frac{1}{2} - i\frac{\sqrt{3}}{2}\right\}.\end{aligned}$$

Aga näiteks $\text{ord}_{\mathbb{C} \setminus \{0\}}(\frac{3}{5} + i\frac{4}{5}) = \infty$, kuna $\arg(\frac{3}{5} + i\frac{4}{5}) = \arctan \frac{4}{3}$ pole ratsionaalarv.

Ülesanne XI.8. Leida kõik tsüklilise rühma endomorfismid.

Lahendus: Olgu G tsükliline rühm. Vastavalt loengukonspekti teoreemile 5.5 on G isomorfne kas rühmaga $(\mathbb{Z}, +)$ või $(\mathbb{Z}_n, +)$ mingi $n \in \mathbb{N}$ korral.

Kui $G \cong (\mathbb{Z}, +)$, siis seda juhtu vaatlesime II praktikumi ülesandes II.2. Meenutan, et

$$\text{End}((\mathbb{Z}, +)) = \{z \mapsto mz \mid m \in \mathbb{Z}\}.$$

Olgu $n \in \mathbb{N}$ ja eeldame, et $G \cong (\mathbb{Z}_n, +)$. Analoogiliselt ülesandega II.2 saame, et ka rühmas $(\mathbb{Z}_n, +)$ kehtib $\text{End}((\mathbb{Z}_n, +)) = \{z \mapsto mz \mid m \in \mathbb{Z}\}$. Samas on selge, et iga $z \in \mathbb{Z}_n$ korral

$$m_1 z = m_2 z \iff m_1 \equiv m_2 \pmod{n}, \quad (m_1, m_2 \in \mathbb{Z}).$$

Seepärast saame täpsustada, et

$$\text{End}((\mathbb{Z}_n, +)) = \{z \mapsto mz \mid m \in \mathbb{Z}_n\}.$$

Siit näeme, et leidub isomorfism $\iota: \mathbb{Z}_n \rightarrow \text{End}((\mathbb{Z}_n, +))$, $z \mapsto z_-$.

Kokkuvõttes näeme, et iga tsüklilise rühma G korral kehtib $G \cong \text{End}(G)$. □

Ülesanne* XI.9. Oletame, et mingis mittetriviaalses rühmas on kõik ühikelemendist erinevad elemendid p -ndat järku. Tõestada, et p on algarv.

Praktikum XII Perioodilised ja vabad Abeli rühmad

Ülesanne XII.1. Leida rühma $(\mathbb{Z}_{20}, +)$ kõik p -komponendid ($p \in \mathbb{P}$). Seejärel veenduge, et rühm $(\mathbb{Z}_{20}, +)$ tõesti avaldub oma p -komponentide otsesummana.

Lahendus: Leiame rühma $(\mathbb{Z}_{18}, +)$ kõikide elementide järgud. Arvutame

$$\begin{array}{ll}
 \text{ord}(\overline{0}) = 1; & \text{ord}(\overline{10}) = 2, \quad (2 \cdot \overline{10} = \overline{0}); \\
 \text{ord}(\overline{1}) = 20; & \text{ord}(\overline{11}) = 20; \\
 \text{ord}(\overline{2}) = 10, \quad (10 \cdot \overline{2} = \overline{0}); & \text{ord}(\overline{12}) = 5, \quad (5 \cdot \overline{12} = \overline{0}); \\
 \text{ord}(\overline{3}) = 20; & \text{ord}(\overline{13}) = 20; \\
 \text{ord}(\overline{4}) = 5, \quad (5 \cdot \overline{4} = \overline{0}); & \text{ord}(\overline{14}) = 10, \quad (10 \cdot \overline{14} = \overline{0}); \\
 \text{ord}(\overline{5}) = 4, \quad (4 \cdot \overline{5} = \overline{0}); & \text{ord}(\overline{15}) = 4, \quad (4 \cdot \overline{15} = \overline{0}); \\
 \text{ord}(\overline{6}) = 10, \quad (10 \cdot \overline{6} = \overline{0}); & \text{ord}(\overline{16}) = 5, \quad (5 \cdot \overline{16} = \overline{0}); \\
 \text{ord}(\overline{7}) = 20; & \text{ord}(\overline{17}) = 20; \\
 \text{ord}(\overline{8}) = 5, \quad (5 \cdot \overline{8} = \overline{0}); & \text{ord}(\overline{18}) = 10, \quad (10 \cdot \overline{18} = \overline{0}); \\
 \text{ord}(\overline{9}) = 20; & \text{ord}(\overline{19}) = 20.
 \end{array}$$

Siit näeme, et rühmal $(\mathbb{Z}_{20}, +)$ leidub kaks erinevat p -komponenti (mis erinevad triviaalsest rühmast), nimelt 2- ja 5-komponent. Seega

$$\begin{aligned}
 (\mathbb{Z}_{20})_2 &= \{a \in \mathbb{Z}_{20} \mid \exists k \in \mathbb{N}_0: \text{ord}(a) = 2k\} = \{a \in \mathbb{Z}_{20} \mid \text{ord}(a) \in \{1, 2, 4\}\} = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}\}, \\
 (\mathbb{Z}_{20})_5 &= \{a \in \mathbb{Z}_{20} \mid \exists k \in \mathbb{N}_0: \text{ord}(a) = 5k\} = \{a \in \mathbb{Z}_{20} \mid \text{ord}(a) \in \{0, 5\}\} = \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}\}, \\
 (\mathbb{Z}_{20})_q &= \{\overline{0}\}, \quad (q \in \mathbb{P} \setminus \{2, 5\}).
 \end{aligned}$$

Näitamaks asjaolu, et $\mathbb{Z}_{20} = (\mathbb{Z}_{20})_2 + (\mathbb{Z}_{20})_5$ esitame kõik elemendid vastavatesse p -komponentidesse kuuluvate elementide summana:

$$\begin{array}{llll}
 \overline{0} = \overline{0} + \overline{0}; & \overline{5} = \overline{5} + \overline{0}; & \overline{10} = \overline{10} + \overline{0}; & \overline{15} = \overline{15} + \overline{0}; \\
 \overline{1} = \overline{5} + \overline{16}; & \overline{6} = \overline{10} + \overline{16}; & \overline{11} = \overline{15} + \overline{16}; & \overline{16} = \overline{0} + \overline{16}; \\
 \overline{2} = \overline{10} + \overline{12}; & \overline{7} = \overline{15} + \overline{12}; & \overline{12} = \overline{0} + \overline{12}; & \overline{17} = \overline{5} + \overline{12}; \\
 \overline{3} = \overline{15} + \overline{8}; & \overline{8} = \overline{0} + \overline{8}; & \overline{13} = \overline{5} + \overline{8}; & \overline{18} = \overline{10} + \overline{8}; \\
 \overline{4} = \overline{0} + \overline{4}; & \overline{9} = \overline{5} + \overline{4}; & \overline{14} = \overline{10} + \overline{4}; & \overline{19} = \overline{15} + \overline{4}.
 \end{array}$$

Ilmselt on kõik eelnevalt toodud summad ühesed, mis tõestabki $\mathbb{Z}_{20} = (\mathbb{Z}_{20})_2 + (\mathbb{Z}_{20})_5$. □

Ülesanne XII.2. Esitage järgnevad rühmad oma mittetriviaalsete p -komponentide otsesummana:
a) $\mathbb{Z}_{10}$, b) $\mathbb{Z}_{25}$ c) $\mathbb{Z}_{60}$.

Lahendus:

- a) Paneme tähele, et $10 = 2 \cdot 5$. Seega tänu loengukonspekti teoreemile 5.22 esitub rühm $\mathbb{Z}_{10}$ otsesummana

$$\mathbb{Z}_{10} = (\mathbb{Z}_{10})_2 \dot{+} (\mathbb{Z}_{10})_5.$$

Kusjuures $(\mathbb{Z}_{10})_2 = \{\bar{0}, \bar{5}\}$ ja $(\mathbb{Z}_{10})_5 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$.

- b) Kuna $25 = 5^2$, siis kõikide rühma $\mathbb{Z}_{25}$ elementide järgud kuuluvad hulka $\{1, 5, 25\}$. Seega on kõikide elementide järk algarvu 5 aste. Kokkuvõttes on $\mathbb{Z}_{15}$ iseenda 5 komponent ehk $\mathbb{Z}_{15} = (\mathbb{Z}_{25})_5$.
- c) Paneme tähele, et $60 = 2^4 \cdot 3 \cdot 5$. Seega tänu loengukonspekti teoreemile 5.22 esitub rühm $\mathbb{Z}_{30}$ otsesummana

$$\mathbb{Z}_{60} = (\mathbb{Z}_{60})_2 \dot{+} (\mathbb{Z}_{60})_3 \dot{+} (\mathbb{Z}_{60})_5.$$

Kusjuures $(\mathbb{Z}_{60})_2 = \{\bar{0}, \bar{15}, \bar{30}, \bar{45}\}$, $(\mathbb{Z}_{60})_3 = \{\bar{0}, \bar{20}, \bar{40}\}$ ja $(\mathbb{Z}_{60})_5 = \{\bar{0}, \bar{12}, \bar{24}, \bar{36}, \bar{48}\}$.

□

Ülesanne XII.3. Leida rühma $(U(\mathbb{Z}_{21}), \cdot)$ p -komponendid ja esitada rühm $(U(\mathbb{Z}_{21}), \cdot)$ nende otse-summana.

Lahendus: Kõigepealt kirjutame välja hulga $U(\mathbb{Z}_{21})$. Selleks meenutame eelmise praktikumi ülesandest 2 asjaolu, et $\bar{a} \in \mathbb{Z}_n$ on pööratav parajasti siis, kui $\text{SÜT}(a, n) = 1$. Arvutame hulga

$$U(\mathbb{Z}_{21}) = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{8}, \bar{10}, \bar{11}, \bar{13}, \bar{16}, \bar{17}, \bar{19}, \bar{20}\}.$$

Näeme, et $\#(U(\mathbb{Z}_{21})) = \text{Ord}(U(\mathbb{Z}_{21})) = 12 = 2^2 \cdot 3$. Leiame nende elementide järgud:

$$\begin{array}{llll} \text{ord}(\bar{1}) = 1; & & \text{ord}(\bar{11}) = 6, & (11^6 \equiv 1 \pmod{21}); \\ \text{ord}(\bar{2}) = 6, & (2^6 \equiv 1 \pmod{21}); & \text{ord}(\bar{13}) = 2, & (13^2 \equiv 1 \pmod{21}); \\ \text{ord}(\bar{4}) = 3, & (4^3 \equiv 1 \pmod{21}); & \text{ord}(\bar{16}) = 3, & (16^3 \equiv 1 \pmod{21}); \\ \text{ord}(\bar{5}) = 6, & (5^6 \equiv 1 \pmod{21}); & \text{ord}(\bar{17}) = 6, & (17^6 \equiv 1 \pmod{21}); \\ \text{ord}(\bar{8}) = 2, & (8^2 \equiv 1 \pmod{21}); & \text{ord}(\bar{19}) = 6, & (19^6 \equiv 1 \pmod{21}); \\ \text{ord}(\bar{10}) = 6, & (10^6 \equiv 1 \pmod{21}); & \text{ord}(\bar{20}) = 2, & (20^2 \equiv 1 \pmod{21}). \end{array}$$

Kirjutame välja rühma $U(\mathbb{Z}_{21})$ p -komponendid:

$$\begin{aligned} (U(\mathbb{Z}_{21}))_2 &= \{a \mid \text{ord}(a) \in \{1, 2\}\} = \{\bar{1}, \bar{8}, \bar{13}, \bar{20}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2, \\ (U(\mathbb{Z}_{21}))_3 &= \{a \mid \text{ord}(a) \in \{1, 3\}\} = \{\bar{1}, \bar{4}, \bar{16}\} \cong \mathbb{Z}_3, \\ (U(\mathbb{Z}_{21}))_q &= \{\bar{0}\}, \quad (q \in \mathbb{P} \setminus \{2, 3\}). \end{aligned}$$

Lihtne kontroll näitab, et tõesti eelnevad isomorfsused kehtivad. Siit näeme, et

$$U(\mathbb{Z}_{21}) = (U(\mathbb{Z}_{21}))_2 \dot{+} (U(\mathbb{Z}_{21}))_3 = \{\bar{1}, \bar{8}, \bar{13}, \bar{20}\} \dot{+} \{\bar{1}, \bar{4}, \bar{16}\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Näitan, et eelnev summa on tõesti otsesumma, esitades kõik $U(\mathbb{Z}_{21})$ elemendi üheselt eelnevast otsesummat ning ka kolmikuna otsekorruutisest

$$\begin{array}{lll}
\bar{1} = \bar{1} \cdot \bar{1} \cong (\bar{0}, \bar{0}, \bar{0}), & \bar{8} = \bar{8} \cdot \bar{1} \cong (\bar{1}, \bar{0}, \bar{0}), & \bar{16} = \bar{1} \cdot \bar{16} \cong (\bar{0}, \bar{0}, \bar{2}), \\
\bar{2} = \bar{8} \cdot \bar{16} \cong (\bar{1}, \bar{0}, \bar{2}), & \bar{10} = \bar{13} \cdot \bar{4} \cong (\bar{0}, \bar{1}, \bar{1}), & \bar{17} = \bar{20} \cdot \bar{4} \cong (\bar{1}, \bar{1}, \bar{1}), \\
\bar{4} = \bar{1} \cdot \bar{4} \cong (\bar{0}, \bar{0}, \bar{1}), & \bar{11} = \bar{8} \cdot \bar{4} \cong (\bar{1}, \bar{0}, \bar{1}), & \bar{19} = \bar{13} \cdot \bar{16} \cong (\bar{0}, \bar{1}, \bar{2}), \\
\bar{5} = \bar{20} \cdot \bar{16} \cong (\bar{1}, \bar{1}, \bar{2}), & \bar{13} = \bar{13} \cdot \bar{1} \cong (\bar{0}, \bar{1}, \bar{0}), & \bar{20} = \bar{20} \cdot \bar{1} \cong (\bar{1}, \bar{1}, \bar{0}).
\end{array}$$

Nüüd oleme põhjalikult uurinud rühma $U(\mathbb{Z}_{21}) \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3 \cong \mathbb{Z}_{13} \setminus \{\bar{0}\}$. Loengukonspekti näites 5.30 vaadeldi rühma $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$. Need kaks on ka ainsad 12. järku Abeli rühmad. $\square$

Olgu A mingi Abeli rühm. Loengukonspekti järeltuse 5.29 põhjal teame, et Abeli rühm A esitub kujul $A \cong \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_s}$, kus $n_1, \dots, n_s \in \mathbb{N}$. Ilmselt kehtib

$$\#(A) = \text{Ord}(A) = \text{Ord}(\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_s}) = \prod_{k=1}^s n_k.$$

Iga lõplik Abeli rühm on perioodiline ning seetõttu tänu teoreemile 5.22 võrdne oma p -komponentide otsesummaga. Fikseerime Abeli rühma A p -komponendi A_p . Rühma A_p järk on $\text{Ord}(A_p) = p^k$ mingi $k \in \mathbb{N}$ korral. Tänu Lagrange'i teoreemile peab iga rühma A_p alamrühm jagama rühma A_p järku see tähendab, et iga rühma A_p alamrühm on järku p^h , kus $0 \leq h \leq k$. Tänu teoreemile 5.27 esitub A_p on tsükliliste alamrühmade otsesummana, aga kõikide nende alamrühmade järgud on mingid algarvu p astmed. Kuna nüüd esitus $A \cong \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_s}$ on saadud Abeli rühma A p -komponentide abil, siis näeme, et iga naturaalarv n_j , $j \in \{n_1, \dots, n_s\}$, on mingi algarvu aste.

Kokkuvõttes esitub iga Abeli rühm A kujul

$$A \cong \mathbb{Z}_{p_1^{a_1}} \times \dots \times \mathbb{Z}_{p_t^{a_t}}, \quad (13)$$

kus $p_1, \dots, p_t \in \mathbb{P}$ ja $a_1, \dots, a_t \in \mathbb{N}_0$ ning $p_1^{a_1} \cdot \dots \cdot p_t^{a_t} = \#(A)$. See esitus on otsetegurite järjekorra täpsuseni üheselt määratud. Antud esitus on arvude $n_1, \dots, n_s$ täpsustus, mis on mainitud loengukonspektis enne näidet 5.30.

Ülesanne XII.4. Leida kõik 36. ja 250. järku Abeli rühmad.

Lahendus:

- a) Paneme tähele, et $36 = 2^2 \cdot 3^2$. Tänu eelnevale mõttekäigule saame, et kõik 36. järku Abeli rühmad esituvad kujul $\mathbb{Z}_{p_1^{a_1}} \times \dots \times \mathbb{Z}_{p_t^{a_t}}$, kus $p_1, \dots, p_t \in \{2, 3\}$ ja $p_1^{a_1} \cdot \dots \cdot p_t^{a_t} = 36$. Selliseid Abeli rühmi leidub neli:

$$\begin{aligned}
\mathbb{Z}_{36} &\cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} = \mathbb{Z}_4 \times \mathbb{Z}_9, \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2} &= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9, \\
\mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3 &= \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3, \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 &.
\end{aligned}$$

- b) Paneme tähele, et $250 = 2 \cdot 5^3$. Analoogiliselt eelmise punktiga kirjutame välja kõik 250. järku Abeli rühmad. Need on

$$\begin{aligned}
\mathbb{Z}_{250} &\cong \mathbb{Z}_2 \times \mathbb{Z}_{5^3} = \mathbb{Z}_2 \times \mathbb{Z}_{125}, \\
\mathbb{Z}_2 \times \mathbb{Z}_{5^2} \times \mathbb{Z}_5 &= \mathbb{Z}_2 \times \mathbb{Z}_{25} \times \mathbb{Z}_5, \\
\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 &.
\end{aligned}$$

Sellelega oleme ammendanud kõik 250. järku Abeli rühmad.

□

Ülesanne XII.5. Leida rühmade $\mathbb{Z}_4 \oplus \mathbb{Z}_6$ ja $\mathbb{Z}_8 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{24}$ maksimaalset järku elemendid ning see maksimaalne järk.

Lahendus: Teadupoolest kehtib $\mathbb{Z}_4 \oplus \mathbb{Z}_6 \cong \mathbb{Z}_4 \times \mathbb{Z}_6$ ja $\mathbb{Z}_8 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{24} \cong \mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$. Leidmaks otsekorrutise maksimaalset järku elemendid, peame leidma vastavate otsetegurite kõrgeimat järku elemendid. Kuna rühm $\mathbb{Z}_n$ on iga $n \in \mathbb{Z}_1$ korral tsükliline rühm moodustajaga $\bar{1}$, siis on ka otsekorrutise $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_m}$ üheks maksimaalset järku elemendiks $(\bar{1}, \dots, \bar{1})$.

Järelikult on $(\bar{1}, \bar{1})$ rühma $\mathbb{Z}_4 \oplus \mathbb{Z}_6$ maksimaalset järku element, kusjuures

$$\text{ord}((\bar{1}, \bar{1})) = \text{VÜK}(4, 6) = 12.$$

Sama järku on kõik rühmade $\mathbb{Z}_4$ ja $\mathbb{Z}_6$ moodustajatest koosnevad paarid (rühma $\mathbb{Z}_4$ moodustajad: $\bar{1}, \bar{3}$; rühma $\mathbb{Z}_6$ moodustajad: $\bar{1}, \bar{5}$). Kuna $12 < \#(\mathbb{Z}_4 \oplus \mathbb{Z}_6) = 24$, siis rühm $\mathbb{Z}_4 \times \mathbb{Z}_6$ ei ole tsükliline rühm.

Analoogiliselt eelnevaga saame, et rühma $\mathbb{Z}_8 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{24}$ maksimaalset järku element on $(\bar{1}, \bar{1}, \bar{1})$, kusjuures

$$\text{ord}((\bar{1}, \bar{1}, \bar{1})) = \text{VÜK}(8, 10, 24) = 120.$$

Sama järku on kõik elemendid, mis koosnevad vastavate otsetegurite moodustajatest. Rühma $\mathbb{Z}_8$ moodustajad on $\bar{1}, \bar{3}, \bar{5}$ ja $\bar{7}$; rühma $\mathbb{Z}_{10}$ moodustajad on $\bar{1}, \bar{3}, \bar{7}, \bar{9}$; rühma $\mathbb{Z}_{24}$ moodustajad on $\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}, \bar{19}, \bar{23}$. Rühm $\mathbb{Z}_8 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{24}$ ei ole samuti tsükliline, kuna $120 < \#(\mathbb{Z}_8 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{24}) = 8 \cdot 10 \cdot 24 = 1920$. □

Ülesanne XII.6. Olgu A Abeli rühm. Tõestage, et rühma A kõigi lõplikku järku elementide rühm on A normaalne alamrühm.

Lahendus: Olgu A Abeli (aditiivne) rühm. Vaatleme alamrühma $H \subseteq A$, mis koosneb kõigist A elementidest, mis on lõpliku järku. Fikseerime $a, b \in H$, sel juhul leiduvad $n, m \in \mathbb{N}$ nii, et $n = \text{ord}(a)$ ja $m = \text{ord}(b)$. Paneme tähele, et

$$n(-a) = -(na) = -0 = 0,$$

$$\begin{aligned} \text{VÜK}(n, m)(a + b) &= \text{VÜK}(n, m)a + \text{VÜK}(n, m)b = \frac{\text{VÜK}(n, m)}{n}(na) + \frac{\text{VÜK}(n, m)}{m}(mb) = \\ &= \frac{\text{VÜK}(n, m)}{n}0 + \frac{\text{VÜK}(n, m)}{m}0 = 0 + 0 = 0. \end{aligned}$$

Seega leidub ka elementidel $-a$ ja $a + b$ lõplik järk. (Kusjuures $\text{ord}(-a) = \text{ord}(a)$ ja $\text{ord}(a + b) = \text{VÜK}(\text{ord}(a), \text{ord}(b))$, kuid eelnevad read ei ole piisavad selle tõestamiseks.) Teisisõnu $-a, a + b \in H$, mistõttu H on alamrühm.

Kuna A on Abeli rühm, siis iga alamrühm on ühtlasi ka normaalne (kuna kehtib $g + a + (-g) = (g - g) + a = 0 + a = a \in H$, kus $g \in A$ ja $a \in H$). □

Eelmises ülesandes vaadeldud alamrühma H nimetatakse rühma A *perioodiliseks alamrühmaks* ehk *väändega rühmaks* (*torsion subgroup*).

Ülesanne XII.7. Olgu A Abeli rühm kus iga elemendi järk on lõpmatu. Näidake, et lõplik hulk $\{a_1, \dots, a_n\}$ on vaba Abeli rühma A baas parajasti siis, kui $A = \langle a_1 \rangle \dot{+} \dots \dot{+} \langle a_n \rangle$.

Lahendus: ($\implies$) Olgu $\{a_1, \dots, a_n\}$ Abeli rühma A moodustajate süsteem. Sel juhul esitub iga $a \in A$ kujul

$$a = k_1 a_1 + \dots + k_n a_n \in \langle a_1 \rangle + \dots + \langle a_n \rangle,$$

kus $k_1, \dots, k_n \in \mathbb{Z}$. Seega $A \subseteq \langle a_1 \rangle + \dots + \langle a_n \rangle$. Kuna aga $\langle a_1 \rangle, \dots, \langle a_n \rangle$ on rühma A alamrühmad, siis ilmselt kehtib $\langle a_1 \rangle + \dots + \langle a_n \rangle \subseteq A$. Kokkuvõttes $A = \langle a_1 \rangle + \dots + \langle a_n \rangle$.

Nüüd, olgu $\{a_1, \dots, a_n\}$ lineaarselt sõltumatu ning $a \in \langle a_1 \rangle \cap (\langle a_2 \rangle + \dots + \langle a_n \rangle)$. Sel juhul leiduvad $h_1, \dots, h_n \in \mathbb{Z}$ nii, et $a = h_1 a_1$ ja $a = h_2 a_2 + \dots + h_n a_n$. Nüüd

$$h_2 a_2 + \dots + h_n a_n - h_1 a_2 = a - a = 0.$$

Kuna $a_1, \dots, a_n$ on lineaarselt sõltumatud, siis saame $-h_1 = h_2 = \dots = h_n = 0$, millest $a = 0$. Järelikult on summa $\langle a_1 \rangle + \dots + \langle a_n \rangle$ otsesumma.

($\impliedby$) Kehtigu $A = \langle a_1 \rangle + \dots + \langle a_n \rangle$. Sel juhul leiduvad iga $a \in A$ korral täisarvud $k_1, \dots, k_n \in \mathbb{Z}$ nii, et $a = k_1 a_1 + \dots + k_n a_n$. Järelikult on Abeli rühm A moodustatud süsteemi $\{a_1, \dots, a_n\}$ poolt.

Olgu $k_1, \dots, k_n \in \mathbb{Z}$ sellised, et $k_1 a_1 + \dots + k_n a_n = 0$. Vastavalt otsesumma definitsioonile, leiduvad iga elemendi, s.h. elemendi 0, liidetavad üheselt. Seega $k_h a_h = 0$ iga $h \in \{1, \dots, n\}$ korral. Kuna iga a_h järk on lõpmatu, saame $k_1, \dots, k_n = 0$ nagu soovitud. $\square$

Ülesanne XII.8. Olgu A vaba Abeli rühm baasiga B . Tõestage, et Abeli rühmade homomorfismi $f: A \rightarrow A$ üheseks määramiseks piisab, kui määrata tema ahend $f|_B$.

Lahendus: Olgu A vaba Abeli rühm baasiga B . Fikseerime elemendi $a \in A$. Vastavalt baasi definitsioonile leiduvad $k_1, \dots, k_n \in \mathbb{Z}$ nii, et $a = k_1 b_1 + \dots + k_n b_n$, kus $b_1, \dots, b_n \in B$. Vaatleme Abeli rühmade homomorfismi $f: A \rightarrow A$, sel juhul

$$f(a) = f(k_1 b_1 + \dots + k_n b_n) = k_1 f(b_1) + \dots + k_n f(b_n).$$

Järelikult on $f(a)$ üheselt määratud, kui on teada elemendid $f(b_1), \dots, f(b_n)$. $\square$

Eelnev ülesanne annab ilmselt kõige olulisema omaduse, miks rühma baasid kasutust leiavad.

Ülesanne* XII.9. Olgu $p > 2$ algarv. Leida isomorfismi täpsuseni kõik lõplikud (mitte tingimata Abeli) p^3 järku rühmad.

Kirjandus

- [1] V. Laan, *Algebra II*, loengukonspekt, Tartu Ülikool, 2021.
- [2] V. Laan, L. Tart, *Algebra I*, loengukonspekt, Tartu Ülikool, 2020.
- [3] M. Kilp, *Algebra I*, Eesti Matemaatika Selts, Tartu, 2005.
- [4] N. Bourbaki, *Elements of Mathematics, Algebra I* (2nd printing). Springer 1989.

Praktikumide lisad

Praktikum V Polünoomide jagamine ülesandes V.1

X^7				$+X^3$		$-Y+1$	$ X^6+X^5Y^3+X^4Y^6$	$+X^3Y^9+X^2(1+Y^{12})+XY^3(1+Y^{12})+Y^6(1+Y^{12})$
X^7	$-X^6Y^3$						$ X-Y^3$	
	X^6Y^3			$+X^3$		$-Y+1$		
	X^6Y^3	$-X^5Y^6$						
		X^5Y^6		$+X^3$		$-Y+1$		
		X^5Y^6	$-X^4Y^9$					
			X^4Y^9	$+X^3$		$-Y+1$		
			X^4Y^9	$-X^3Y^{12}$				
				$X^3(1+Y^{12})$		$-Y+1$		
				$X^3(1+Y^{12})$	$-X^2Y^3(1+Y^{12})$			
					$X^2Y^3(1+Y^{12})$	$-Y+1$		
					$X^2Y^3(1+Y^{12})$	$-XY^6(1+Y^{12})$		
						$XY^6(1+Y^{12})$	$-Y+1$	
						$XY^6(1+Y^{12})$	$-Y^9(1+Y^{12})$	
							$-Y+1$	$+Y^9(1+Y^{12})$

Praktikum VII Korrutamine korpuses $\mathbb{Q}[X]/\langle X^4+X^2-1\rangle$

$a_1a_2X^6$	$+(a_1b_2+b_1a_2)X^5$	$+(a_1c_2+b_1b_2+c_1a_2)X^4$	$+(a_1d_2+b_1c_2+c_1b_2+d_1a_2)X^3$	$+(b_1d_2+c_1c_2+d_1b_2)X^2$	$+(c_1d_2+d_2c_1)X$	$+d_1d_2$	$ a_1a_2X^2+(a_1b_2+b_1a_2)X+(a_1c_2+b_1b_2+c_1a_2-a_1a_2)$
$a_1a_2X^6$		$+a_1a_2X^4$		$-a_1a_2X^2$			$ X^4+X^2-1$
	$(a_1b_2+b_1a_2)X^5$	$(a_1c_2+b_1b_2+c_1a_2-a_1a_2)X^4$	$+(a_1d_2+b_1c_2+c_1b_2+d_1a_2)X^3$	$+(b_1d_2+c_1c_2+d_1b_2+a_1a_2)X^2$	$+(c_1d_2+d_2c_1)X$	$+d_1d_2$	
	$(a_1b_2+b_1a_2)X^5$		$+(a_1b_2+b_1a_2)X^3$		$-(a_1b_2+b_1a_2)X$		
		$(a_1c_2+b_1b_2+c_1a_2-a_1a_2)X^4$	$+(a_1d_2+b_1c_2+c_1b_2+d_1a_2-a_1b_2-b_1a_2)X^3$	$+(b_1d_2+c_1c_2+d_1b_2+a_1a_2)X^2$	$+(-c_1d_2-d_2c_1+a_1b_2+b_1a_2)X$	$+d_1d_2$	
		$(a_1c_2+b_1b_2+c_1a_2-a_1a_2)X^4$		$+(a_1c_2+b_1b_2+c_1a_2-a_1a_2)X^2$		$-a_1c_2-b_1b_2-c_1a_2+a_1a_2$	
			$(a_1d_2+b_1c_2+c_1b_2+d_1a_2-a_1b_2-b_1a_2)X^3$	$+(b_1d_2+c_1c_2+d_1b_2+2a_1a_2-a_1c_2-b_1b_2-c_1a_2)X^2$	$+(-c_1d_2-d_2c_1+a_1b_2+b_1a_2)X$	$+d_1d_2+a_1c_2+b_1b_2+c_1a_2-a_1a_2$	

Kokkuvõttes

$[a_1X^3+b_1X^2+c_1X+d_1][a_2X^3+b_2X^2+c_2X+d_2]=$
$$=[a_1a_2X^6+(a_1b_2+b_1a_2)X^5+(a_1c_2+b_1b_2+c_1a_2)X^4+(a_1d_2+b_1c_2+c_1b_2+d_1a_2)X^3+(b_1d_2+c_1c_2+d_1b_2)X^2+(c_1d_2+d_2c_1)X+d_1d_2]=$$
$$=[(a_1a_2X^2+(a_1b_2+b_1a_2)X+a_1c_2+b_1b_2+c_1a_2-a_1a_2)\cdot(X^4+X^2-1)+(a_1d_2+b_1c_2+c_1b_2+d_1a_2-a_1b_2-b_1a_2)X^3+(b_1d_2+c_1c_2+d_1b_2-a_1c_2-b_1b_2-c_1a_2)X^2+(-c_1d_2-d_2c_1+a_1b_2+b_1a_2)X+d_1d_2+a_1c_2+b_1b_2+c_1a_2-a_1a_2]=$$
$$=[(a_1d_2+b_1c_2+c_1b_2+d_1a_2-a_1b_2-b_1a_2)X^3+(b_1d_2+c_1c_2+d_1b_2+2a_1a_2-a_1c_2-b_1b_2-c_1a_2)X^2+(-c_1d_2-d_2c_1+a_1b_2+b_1a_2)X+d_1d_2+a_1c_2+b_1b_2+c_1a_2-a_1a_2].$$