Peatükk 1

Arvu mõiste kujunemise alused

1.1 Lühiülevaade arvu mõiste kujunemise ajaloolistest aspektidest

- Tundub, et kõige lihtsam hulkade võrdlemise viis on üksühese vastavuse moodustamine.
- Hulga elementide loendamine nõuab loendamise võimalike tulemuste ehk **naturaalarvude** tähistamist. Kui hulga A elementide arv on m, siis hulk A on sama võimas kui kõik muud m-elemendilised hulgad.
- Naturaalarvude (mõistlik) ülesmärkimine nõuab **arvusüsteemi** olemasolu. Babüloonlased, egiptlased jt.
- Nulli loendamise teel otseselt ei saa saada. Babüloonlased (juba 8. saj. e.m.a.), olmeegid ja maiad (1. saj. m.a.j.), Brahmagupta (India, 628 m.a.j.) kasutasid nulli.
- Lihtsamad harilikud murrud kasutusel Egiptuses juba ca 1000 aastat e.m.a.
- Negatiivsed arvud võeti esimesena kasutusele Indias 6.–7. saj. m.a.j. ja pisut hiljem sõltumatult ka Hiinas. Kasutati võla tähisena. Euroopas läks kaua, enne kui negatiivsed arvud läbi lõid: alles 15. sajandil nad ilmusid kaupmeeste kasutusse ning matemaatikas murdsid läbi alles 17. sajandil. Newton („Üldine aritmeetika“, 1707): „Suurused võivad olla suuremad kui eimidagi või väiksemad kui eimidagi [null oli eimidagi].“
- Naturaalarvude aksiomaatika (Giuseppe Peano, 1889)

- Peano aksiomaatika mittetäielikkus (Kurt Gödel, 1931)
- Mõnede irratsionaalarvudeni jõuti juba antiik-Kreekas: pütagoorlased (5. saj. e.m.a.) olid raskustes $\sqrt{2}$ konstrueerimisel; tõestuseni jõudis Hippasus Metaphontumist (sünd. ca 500 e.m.a.). Põhjalik käsitlus irratsionaalarvude kohta sisaldub Eukleidese „Elementides“ (ca 300 e.m.a.).
- 18. ja 19. sajandil tehti palju tööd irratsionaalarvude ja transtsendentsete arvude vallas. Lambert (1761) ja Legendre (1794) näitasid, et π on irratsionaalarv. Ruffini (1799) ja Abel (1842) tõestasid Abel-Ruffini teoreemi (viienda ja kõrgema astme võrrandi üldine mittelahenduvus radikaalides). Hermite (1873) ja Lindemann (1882) tõestasid vastavalt, et e ja π on transtsendentsed.
- Reaalarvude esimese vettpidava definitsiooni andis Cantor aastal 1871.
- Esimesed viited negatiivsete arvude ruutjuurtele pärinevad antiik-Kreekast 1. saj. m.a.j.
- 16. sajandil, seoses kuup- ja neljanda astme võrrandite lahendivalemite tuletamisega, pöördus tähelepanu juurtele negatiivsetest arvudest. Geomeetrilise tõlgenduse idee esines juba Wallisel (1685), aga populaarseks sai ta pärast Wesseli (1799) tööd. Formaalne definitsioon reaalarvupaaridena anti kompleksarvude kohta alles 19. sajandil.
- Kvaternioonid defineeris esimesena Hamilton (1843).

1.2 Arvuhulkade $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ defineerimise erinevatest võimalustest

Moodustame hulga $\mathbb{N}$ kahel erineval viisil. Need viisid on kõige levinumad tänapäeval.

1.2.1 Peano aksiomaatika

Definitsioon. Vaatleme algebralist struktuuri $(N, 0, ', +, \cdot)$, millel on defineeritud 0-aarne tehe 0, unaarne tehe $'$ ning binaarsed tehted $+$ ja $\cdot$ selliselt, et

P1° $\vdash \forall x \in N\, x' \neq 0$,

P2° $\vdash \forall x, y \in N\, (x' = y' \Rightarrow x = y)$,

P3° $\vdash \forall x \in N\, (x + 0 = x)$,

P4° $\vdash \forall x, y \in N\,(x + y' = (x + y)')$,

P5° $\vdash \forall x \in N\,(x \cdot 0 = 0)$,

P6° $\vdash \forall x, y \in N\,(x \cdot y' = x \cdot y + x)$.

P7° kõik sekventsid kujul $\mathcal{A}(0)$, $\forall x \in N\,(\mathcal{A}(x) \Rightarrow \mathcal{A}(x')) \quad \vdash \quad \forall x \in N\,\mathcal{A}(x)$.

Ülaltoodud algebralist struktuuri, kus on valitud $N = \{0, 0', 0'', 0''', \dots\}$, nimetatakse **naturaalarvude hulgaks**, tähistatakse $\mathbb{N}$, selle elemente nimetatakse **(standardseteks) naturaalarvudeks** ning tähistatakse $1 = 0'$, $2 = 0''$, $3 = 0'''$ jne.

Aksioome P1°–P7° nimetatakse **Peano aritmeetika aksioomideks**.

On võimalik leida hulgast $\mathbb{N}$ erinevaid hulki, mis rahuldavad Peano aritmeetika aksioome. Sellistes, „mittestandardsetes“ naturaalarvude hulkades võib leiduda kõigist naturaalarvudest suuremaid elemente.

Kui töötada teist järku teoorias, st. lubada aksioomi P7° asemel aksioomi kujul

P7′ Iga predikaadi P jaoks kehtib: kui $P(0)$ ja $P(x)$-st järeldub $P(x + 1)$, siis $\forall x \in N\,P(x)$.

siis on ainus Peano aritmeetika aksioome rahuldav hulk $\mathbb{N}$. Aksioom P7° on aksioomist P7′ nõrgem selle poolest, et aksioomis P7° on sekventsi vasakul poolel $\mathcal{A}$ rollis võimalik kasutada ainult valemeid. Ent loenduval hulgal leidub predikaate, mida ei saa valemiga väljendada (kuna valemite hulk on loenduv, predikaatide hulk aga kontiinumi võimsusega).

Saab näidata, et Peano aritmeetika aksiomaatika hulgal $\mathbb{N}$ on **mittevasturäägiv**. See tähendab, hulgal $\mathbb{N}$ pole võimalik aksioomidest tuletada korraga valemit $\mathcal{A}$ ja valemit $\neg\mathcal{A}$.

Saksa matemaatik Kurt Gödel näitas 1931. aastal, et

1) leidub selliseid valemeid $\mathcal{A}$ struktuuris $\mathbb{N}$, et ei $\mathcal{A}$ ega $\neg\mathcal{A}$ pole Peano aksioomidest tuletatav;
2) punkt 1) kehtib ka juhul, kui aksioomidele P1° kuni P7° lisada mistahes lahenduv hulk aksioome.

Seega on Peano aritmeetika aksiomaatika **mittetäielik**, ja jääb selleks ka mistahes lahenduva hulga aksioomide lisamisel.

1.2.2 Hulgateoreetiline konstruktsioon

Peano aritmeetika aksioomid eriti ei tegele naturaalarvude hulga olemasolu ning naturaalarvude täpse „väljanägemise“ probleemidega. Pöörame nüüd nendele küsimustele oma tähelepanu.

Hulgateooria aksioomide seas (kasutame Zermelo-Fraenkeli aksiomaatikat) on *lõpmatuse aksioom*:

$$\exists X : \varnothing \in X \wedge (\forall x : x \in X \Rightarrow x \cup \{x\} \in X).$$

Sellist hulka, mis sisaldab tühja hulka ja rahuldab nõuet, et iga elemendi x korral sisaldab hulk elemendi $x \cup \{x\}$, nimetatakse tihti ka **induktiivseks**. Lõpmatuse aksioom väidab, et leidub induktiivne hulk. Meie jaoks on see aksioom töövahendiks, mis väidab naturaalarvude hulga olemasolu.

Tähistame $0 = \varnothing$ ning defineerime $x' = x \cup \{x\}$, kus x on mistahes hulk. Nüüd defineerime

$$\begin{array}{rcl} 1 & = & 0' = \varnothing' = \varnothing \cup \{\varnothing\} = \{\varnothing\}; \\ 2 & = & 1' = \{\varnothing\}' = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}; \\ 3 & = & 2' = \{\varnothing, \{\varnothing\}\}' = \{\varnothing, \{\varnothing\}\} \cup \{\{\varnothing, \{\varnothing\}\}\} = \\ & = & \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}; \\ \ldots & \ldots & \ldots \\ n & = & (n-1)' = (n-1) \cup \{n-1\} \end{array}$$

Olgu nüüd X induktiivne hulk, mille leidumine järeldub lõpmatuse aksioomist. Tähistame

$$\mathbb{N} = \bigcup \left\{ N \subset X : 0 \in N,\ \forall n \in N\, (n \in N \Rightarrow n' \in N) \right\}.$$

Naturaalarvude konkreetsete esituste kohta vt. `http://math.ut.ee/~zolki/math/ZF_nat.php`.

1.2.3 Tehetega seotud omadused. Naturaalarvude võrdlemine

Struktuur $\mathbb{N}$ on tehete $+$ ja $\cdot$ suhtes assotsiatiivne, kommutatiivne ja leidub nullelement/ühikelement. (Need on lihtsad järeldused Peano aksioomidest.) Niisiis on $(\mathbb{N}, 0, +)$ ja $(\mathbb{N}, 1, \cdot)$ kommutatiivsed monoidid.

Kehtib distributiivsusseadus

$$\vdash \forall x, y, z \in \mathbb{N}\, (x \cdot (y + z) = x \cdot y + x \cdot z).$$

Lihtsuse huvides tähistame edaspidi $x^n = \underbrace{x \cdot x \cdots x}_{n \text{ tegurit}}$. Rõhutame, et see *astendamistehe* ei ole algebraline tehe.

Definitsioon. Öeldakse, et naturaalarv m **pole suurem** kui naturaalarv n, kui predikaat $P(m, n) = \exists k \in \mathbb{N} : n = m + k$ on tõene. Seda kirjutatakse $m \leqslant n$.

Öeldakse, et naturaalarv m **pole väiksem** kui naturaalarv n, kui $n \leqslant m$. Seda kirjutatakse $m \geqslant n$.

Kirjutised $m < n$ ja $m > n$ on loogiliselt samaväärsed vastavalt kirjutistega $m \leqslant n \wedge m \neq n$ ning $m \geqslant n \wedge m \neq n$.

Lause 1. *Mistahes kahe naturaalarvu m ja n korral kehtib parajasti üks kolmest väitest $m < n$, $m = n$ ja $m > n$.*

Lause 2. *Seos $\leqslant$ on lineaarse järjestuse seos hulgal $\mathbb{N}$.*

1.3 Täis- ja ratsionaalarvud

1.3.1 Naturaalarvude laiendamine täisarvudeni

Viime hulka $\mathbb{N} \times \mathbb{N}$ sisse seose $\sim$ selliselt, et $(a, b) \sim (c, d)$ parajasti siis, kui $a + d = b + c$. Lihtne on näidata, et seos on ekvivalentsiseos. Tähistame $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$. Hulka $\mathbb{Z}$ nimetatakse **täisarvude hulgaks** ning selle elemente **täisarvudeks**.

Sisuliselt on täisarvud arvud, mis vastavad naturaalarvupaari komponentide võimalikele asenditele arvteljel üksteise suhtes.

Tehted hulgas $\mathbb{Z}$ defineerime järgmiselt:

- $\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}$;
- $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac+bd, ad+bc)}$.

Definitsioonide korrektsuse kontroll on vahetu.

Vaatleme kujutust $n \mapsto \overline{(n,0)}$, mis korraldab sisestuse $\mathbb{N} \subset \mathbb{Z}$. On lihtne kontrollida, et see sisestus säilitab tehted.

Tähistame $-n = \overline{(0,n)}$ ning sümboliga $-$ kujutuse, mis seab arvule n vastavusse arvu $-n$.

Lause. $(\mathbb{Z}, 0, -, +)$ on Abeli rühm. $(\mathbb{Z}, 1, \cdot)$ on kommutatiivne monoid. $(\mathbb{Z}, 0, 1, -, +, \cdot)$ on kommutatiivne ühikelemendiga ring.

Praktikas on otstarbekas võtta kasutusele täiendav binaarne tehe: **lahutamine**. See defineeritakse võrdusega

$$a - b = a + (-b), \qquad a, b \in \mathbb{Z}.$$

Lahutamine on võimalik defineerida ka selliste naturaalarvude a ja b jaoks, kus $a > b$. Nimelt, kui $a > b$, siis leidub nullist erinev naturaalarv c selliselt, et $a = b + c$. Näitame, et c on üheselt määratud ning tähistame $a - b := c$. Kui $a = b$, siis võtame $c = 0$. Juhul $a < b$ võime $a - b$ jätta määramata (siis pole lahutamine algebraline tehe) või deklareerida ka siis $a - b = 0$. Kui on defineeritud $a - b = 0$

kõigi $a \leqslant b$ korral, siis sellist lahutamist kutsutakse *lõigatud lahutamiseks* ning tähistatakse $\dot{-}$ märgiga.

Konstrueeritud $\mathbb{Z}$ elementide esitamiseks „tavalisel" kujul saab kasutada järgmist kirjeldust. Olgu antud täisarv $\overline{(a,b)}$, siis kehtib üks kolmest juhtumist $a < b$, $a = b$ või $a > b$. Esimesel juhul kirjutame $\overline{(a,b)} = -k$, kus $k \neq 0$ on selline naturaalarv, et $b = a + k$. Teisel juhul kirjutame $\overline{(a,b)} = 0$. Kolmandal juhul kirjutame $\overline{(a,b)} = k$, kus $k \neq 0$ on selline naturaalarv, et $a = b + k$.

Hulka $\mathbb{Z}$ viime sisse seose $\leqslant$:

$$\overline{(a,b)} \leqslant \overline{(c,d)} \quad \Leftrightarrow \quad a + d \leqslant b + c.$$

Samal moel nagu naturaalarvude korral toome sisse seosed $\geqslant$, $<$, $>$.

Osutub, et $\mathbb{Z}$ on lineaarselt järjestatud hulk seose $<$ suhtes, kusjuures kehtib

$$\cdots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \cdots$$

Järjestusseos $\leqslant$ on kooskõlas tehetega:

- $\vdash \forall a, b, c, d \in \mathbb{Z}\,(a \leqslant b \wedge c \leqslant d \Rightarrow a + c \leqslant b + d)$;
- $\vdash \forall a, b, c \in \mathbb{Z}\,(a \leqslant b \wedge 0 < c \Rightarrow ac \leqslant bc)$.

Siit teisest omadusest järeldub, et

$$\vdash \forall a, b, c \in \mathbb{Z}\,(a \leqslant b \wedge c < 0 \Rightarrow bc \leqslant ac).$$

Järjestus $<$ ei ole täielik.

Lause. Olgu $a \in \mathbb{Z}$ ja $b \in \mathbb{N}$, $b \neq 0$. Siis leiduvad üheselt määratud täisarvud q (jagatis) ja r (jääk) selliselt, et $a = bq + r$, kusjuures $0 \leqslant r < b$.

Definitsioon. Olgu $a, b \in \mathbb{Z}$. Öeldakse, et täisarv a jagab täisarvu b, kui leidub täisarv c selliselt, et $b = ac$.

Seos $|$ on osalise järjestuse seos.

Definitsioon. Olgu $a, b \in \mathbb{Z}$. Öeldakse, et a on b tegur, kui $a|b$. Öeldakse, et a on b kordne, kui $b|a$.

Definitsioon. Olgu $a, b, c \in \mathbb{Z}$. Öeldakse, et c on a ja b suurim ühistegur, kui

1) $c|a \wedge c|b$;
2) $\forall d \in \mathbb{Z}\,(d|a \wedge d|b \Rightarrow d|c)$.

Öeldakse, et c on a ja b vähim ühiskordne, kui

1) $a|c \wedge b|c$;
2) $\forall d \in \mathbb{Z}\,(a|d \wedge b|d \Rightarrow c|d)$.

Saab näidata, et nullist erinevate täisarvude a ja b korral kehtib võrdus $a \cdot b = \mathrm{SÜT}(a,b) \cdot \mathrm{VÜK}(a,b)$. Suurimat ühistegurit (aga selle võrduse kaudu siis ka vähimat ühiskordset) saab leida näiteks Eukleidese algoritmi abil.

1.3.2 Täisarvude laiendamine ratsionaalarvudeni

Viime hulka $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ seose $\sim$ sisse selliselt, et $(a,b) \sim (c,d)$ parajasti siis, kui $ad = bc$. On lihtne kontrollida, et $\sim$ on ekvivalentsiseos. Tähistame $\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})/\sim$. Hulka $\mathbb{Q}$ nimetatakse **ratsionaalarvude hulgaks** ja selle elemente **ratsionaalarvudeks**.

Meenutame, et algebralist struktuuri K, millel on defineeritud kaks 0-aarset tehet 0 ja 1, üks unaarne tehe $-$ ja kaks binaarset tehet $+$ ning $\cdot$ selliselt, et $(K, 0, -, +, \cdot)$ on ring ning hulgal $K\backslash\{0\}$ unaarne tehe $^{-1}$ selliselt, et $(K\backslash\{0\}, 1, ^{-1}, \cdot)$ on rühm, nimetatakse **korpuseks**. Kui sealjuures $(K\backslash\{0\}, 1, ^{-1}, \cdot)$ on Abeli rühm (st. kommutatiivne rühm), siis öeldakse, et K on **kommutatiivne korpus**.

Defineerime hulgas $\mathbb{Q}$ tehted järgmiste võrdustega.

- $\overline{(a,b)} + \overline{(c,d)} = \overline{(ad + bc, bd)}$;
- $\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac, bd)}$;
- $-\overline{(a,b)} = \overline{(-a,b)}$;
- $\overline{(a,b)}^{-1} = \overline{(b,a)}$.

On lihtne kontrollida, et tehete definitsioonid on korrektsed.

Defineerime kujutuse $\mathbb{Z} \to \mathbb{Q}$ kirjutisega $z \mapsto \overline{(z,1)}$. Niiviisi võime vaadelda $\mathbb{Z} \subset \mathbb{Q}$.

Lihtsuse huvides defineerime mistahes $x \in \mathbb{Q}$ ja $n \in \mathbb{N}$ korral $x^{-n} = (x^n)^{-1}$ (negatiivse astendajaga aste). Astendamistehe pole algebraline tehe.

Lause 3. *Algebraline struktuur* $(\mathbb{Q}, 0, 1, -, ^{-1}, +, \cdot)$ *on kommutatiivne korpus. Sealjuures säilitab sisestus* $z \mapsto \overline{(z,1)}$ *täisarvudel määratud tehted. Niisiis on* $\mathbb{Z}$ *kommutatiivse ühikelemendiga ringi* $\mathbb{Q}$ *alamring.*

Ratsionaalarvude hulgas vaadeldakse tavaliselt veel **jagamistehet** $\frac{q_1}{q_2} = q_1 \cdot q_2^{-1}$. Kuna nullelemendil pöördelement puudub, siis jagamistehe on kujutus ainult $\mathbb{Q} \times (\mathbb{Q}\backslash\{0\} \to \mathbb{Q}$ ega ole seetõttu algebraline tehe.

Defineerime hulgas $\mathbb{Q}$ seose $\leqslant$:

$$\overline{(a,b)} \leqslant \overline{(c,d)} \quad \Leftrightarrow \quad (bd > 0 \wedge ad \leqslant bc) \vee (bd < 0 \wedge ad \geqslant bc).$$

Saab näidata, et seos $\leqslant$ on lineaarne järjestus. Järjestus $\leqslant$ ei ole täielik.

Tavapäraselt on kombeks kirjutada $\overline{(a,b)} = \frac{a}{b}$. Lugejas ja nimetajas märgi täpsuseni on võimalik ratsionaalarv $\overline{(a,b)}$ viia *taandatud kujule*: $(a,b) \equiv (p,q)$, kus $a = p \cdot \text{SÜT}(a,b)$, $b = q \cdot \text{SÜT}(a,b)$. Garanteerinud veel, et $q > 0$ (vajadusel

muutes p märki), saab öelda, et kõik ratsionaalarvud on esitatavad hulga $\mathbb{Z} \times (\mathbb{N}\backslash\{0\})$ elementidena.

Lause 4. *Hulgad $\mathbb{N}$, $\mathbb{Z}$ ja $\mathbb{Q}$ on loenduvad.*

1.4 Reaalarvude teooria erinevaid käsitlusi

1.4.1 Järjestatud korpuse mõiste

Kõigepealt anname reaalarvude aksiomaatilise definitsiooni.

Lause 5. *Olgu K korpus. Siis*

1) $0a = 0$ *iga* $a \in K$ *korral;*
2) *kui* $ab = 0$, *siis* $a = 0$ *või* $b = 0$;
3) $(-a)b = -ab$ *iga* $a, b \in K$ *korral;*
4) $(-a)(-b) = ab$ *iga* $a, b \in K$ *korral.*

Definitsioon 6. Öeldakse, et kommutatiivne korpus K on **järjestatud korpus**, kui tema elementide vahel on defineeritud seos $<$ selliselt, et

1) iga kahe elemendi $a, b \in K$ korral kehtib täpselt üks tingimustest $a = b$, $a < b$, $b < a$;
2) kui $a < b$ ja $b < c$, siis $a < c$ iga $a, b \in K$ korral;
3) kui $a < b$, siis $a + c < b + c$ iga $a, b, c \in K$ korral;
4) kui $a < b$ ja $c > 0$, siis $ac < bc$ iga $a, b, c \in K$ korral.

Kirjutise $a > b$ loeme samaväärseks kirjutisega $b < a$. Kirjutise $a \leqslant b$ loeme samaväärseks kirjutisega $a < b$ või $a = b$.

Lause 7. *Olgu K järjestatud korpus. Siis*

1) $a < b$ *kehtib parajasti siis, kui* $-b < -a$;
2) $a \leqslant b$ *kehtib parajasti siis, kui* $-b \leqslant -a$;
3) *kui* $a < b$ *ja* $c < 0$, *siis* $ac > bc$;
4) $a^2 > 0$ *iga* $a \neq 0$ *korral;*
5) *kui* $a < c$ *ja* $b < d$, *siis* $a + b < c + d$;
6) *kui* $0 < a < b$, *siis* $0 < b^{-1} < a^{-1}$;
7) *kui* $ab > 0$, *siis kas* $a > 0$ *ja* $b > 0$ *või* $a < 0$ *ja* $b < 0$;

8) kui $ab < 0$, siis kas $a > 0$ ja $b < 0$ või $a < 0$ ja $b > 0$.

Lause 8. *Iga järjestatud korpus sisaldab endas isomorfismi täpsuseni naturaalarvude hulga.*

Isomorfismi rollis on siin hulkade isomorfism, mis säilitab tehted ja järjestuse.

Lause 9. *Iga järjestatud korpus sisaldab endas alamkorpust, mis on isomorfne ratsionaalarvude korpusega* $\mathbb{Q}$.

Definitsioon 10. Öeldakse, et hulk A järjestatud korpuses K on *ülalt tõkestatud*, kui leidub element $M \in K$ selliselt, et $\forall x \in K\, x \leqslant M$. Öeldakse, et hulk $A \subset K$ on *alt tõkestatud*, kui leidub $m \in K$ selliselt, et $\forall x \in K\, x \geqslant m$. Öeldakse, et hulk $A \subset K$ on *tõkestatud*, kui A on alt ja ülalt tõkestatud.

Olgu K järjestatud korpus. Tähistame $|x| = x$, kui $x \geqslant 0$, ning $|x| = -x$ vastasel korral. Tehet $|\cdot|$ nimetatakse *absoluutväärtuseks*.

Lause 11. *Hulk A järjestatud korpuses K on tõkestatud parajasti siis, kui leidub $M \in K$, $M > 0$, selliselt, et $|x| \leqslant M$ iga $x \in A$ korral.*

Definitsioon 12. Olgu K järjestatud korpus ja $A \subset K$. Öeldakse, et a on hulga A *ülemine raja* ja tähistatakse $\sup A$, kui

1) $\forall x \in A\, x \leqslant a$;
2) $\forall \varepsilon \in K\, (\varepsilon > 0 \Rightarrow \exists x \in A\, :\, x > a - \varepsilon)$.

Öeldakse, et a on hulga A *alumine raja* ja tähistatakse $\inf A$, kui

1) $\forall x \in A\, x \geqslant a$;
2) $\forall \varepsilon \in K\, (\varepsilon > 0 \Rightarrow \exists x \in A\, :\, x < a + \varepsilon)$.

Definitsioon 13. Järjestatud korpust K nimetatakse **täielikuks**, kui igal ülalt tõkestatud mittetühjal hulgal $X \subset K$ leidub ülemine raja.

Lause 14. *Täielikus järjestatud korpuses K leidub igal alt tõkestatud mittetühjal hulgal alumine raja.*

1.4.2 Täieliku järjestatud korpuse olemasolu ja ühesus

Järgmised teoreemid näitavad, et täielikke järjestatud korpusi on täpselt üks.

Teoreem 15. *Kaks täielikku järjestatud korpust K_1 ja K_2 on isomorfsed.*

Tähistame tähega $\mathbb{R}$ hulga $\mathbb{Q}$ selliste alamhulkade hulga, mis rahuldavad tingimusi

1) kui $q \in A$ ja $p < q$, siis $p \in A$;
2) hulgas A ei ole suurimat elementi;
3) $A \neq \varnothing$, $A \neq \mathbb{Q}$.

Siis iga $A \in \mathbb{R}$ on järjestatud korpuses $\mathbb{Q}$ ülalt tõkestatud alamhulk. Olgu $\tilde{A}$ hulga A kõigi ülemiste tõkete hulk, millest on välja jäetud vähim ülemine tõke, kui see eksisteerib.

Defineerime hulgas $\mathbb{R}$

- järjestuse seosega $A < B \Leftrightarrow A \subsetneq B$,
- liitmise $A + B = \{a + b : a \in A, b \in B\}$,
- nullelemendi $\overline{0} = \{p \in \mathbb{Q} : p < 0\}$,
- ühikelemendi $\overline{1} = \{p \in \mathbb{Q} : p < 1\}$,
- elemendi A vastandelemendi $-A = \{-q : q \in \tilde{A}\}$.
- Defineerime elementide A ja B korrutise.
  - Kui $A > \overline{0}$ ja $B > \overline{0}$, siis defineerime $A \cdot B = \{ab : a \in A, a \geqslant 0, b \in B, b \geqslant 0\} \cup \overline{0}$.
  - Kui $A > \overline{0}$ ja $B < \overline{0}$, siis $A \cdot B = -(A \cdot (-B))$.
  - Kui $A < \overline{0}$ ja $B > \overline{0}$, siis $A \cdot B = -((-A) \cdot B)$. Kui $A < \overline{0}$ ja $B < \overline{0}$, siis $A \cdot B = (-A) \cdot (-B)$.
  - Lõpuks, defineerime $\overline{0} \cdot B = B \cdot \overline{0} = \overline{0}$ iga B korral.
- Defineerime elemendi A pöördelemendi.
  - Elemendi $A > \overline{0}$ pöördelemendi defineerime $A^{-1} = \{\frac{1}{q} : q \in \tilde{A}\} \cup \{q \in \mathbb{Q} : q \leqslant 0\}$.
  - Kui $A < \overline{0}$, siis defineerime $A^{-1} = -((-A)^{-1})$.

Teoreem 16. *Hulk $\mathbb{R}$ koos ülal defineeritud tehetega 0, 1, $-$, $+$, $\cdot$ ja $^{-1}$ on täielik järjestatud korpus.*

Definitsioon 17. Hulka $\mathbb{R}$ nimetatakse **reaalarvude hulgaks** ja selle elemente **reaalarvudeks**.

Lause 18. *Hulgad* $2^{\mathbb{N}}$ *ja* $\mathbb{R}$ *on võrdse võimsusega ja mitteloenduvad hulgad.*

Hulgateoorias tõestatakse, et hulgad $\mathbb{R}^n$, $n \in \mathbb{N}$, $n \geqslant 1$, on kõik võrdse võimsusega. Samuti on $\mathbb{R}$ ja mistahes vahemik, lõik, poollõik ning poolsirge sama võimsusega.

Matemaatilise analüüsi arendamisel defineeritakse hulgas $\mathbb{R}$ *loomulik topoloogia*

$$\tau_{\mathbb{R}} = \left\{U \subset \mathbb{R} \,:\, \forall u \in U \exists \varepsilon > 0 \,\{r \in \mathbb{R} \,:\, |r-u| < \varepsilon\} \subset U\right\} \cup \varnothing.$$

ning sellest lähtuvalt saab sisse tuua funktsiooni piirväärtuse, tuletise, Riemanni integraali jm. mõisted.

Lause 19. *Iga reaalarvu* $b \geqslant 0$ *ja iga naturaalarvu* n *korral leidub üheselt määratud reaalarv* $x \geqslant 0$ *selliselt, et* $x^n = b$.

Lause 19 ratsionaalarvude vallas ei kehti, näiteks $\sqrt{2}$, $\sqrt{3}$ jne. ei ole ratsionaalarvud.

1.4.3 Cauchy meetod

Vaatleme nüüd alternatiivset, Cauchy meetodit reaalarvudeni jõudmiseks.

Tähistame tähega Q hulga $\mathbb{Q}$ kõigi selliste jadade (q_n) hulga, mis rahuldavad järgmist tingimust:

mistahes naturaalarvu K korral leidub selline indeks N, et

$$m, n \geqslant N \Rightarrow |q_m - q_n| < \frac{1}{K}.$$

Defineerime hulgal Q seose $\sim$ selliselt, et $(q_n) \sim (q'_n)$ parajasti sel juhul, kui mistahes naturaalarvu K korral leidub indeks N, et $n \geqslant N \Rightarrow |q_n - q'_n| < \frac{1}{K}$.

Lause 20. *Seos* $\sim$ *hulgal* Q *on ekvivalentsiseos.*

Teoreem 21. $Q/\sim$ *on täielik järjestatud korpus.*

Cauchy meetodi nime all tuntakse ka meetodit funktsionaalvõrrandite lahendamiseks. Näiteks saab selle meetodi abil leida pideva aditiivse funktsiooni või monotoonse aditiivse funktsiooni üldkuju.

1.4.4 Dedekindi lõiked

Kui on antud kaks reaalarvude hulka A ja B, mis rahuldavad tingimusi

1) $A \cup B = \mathbb{R}$;
2) $A \neq \emptyset$, $B \neq \emptyset$,
3) $\forall a \in A\, \forall b \in B\, (a < b)$,

siis öeldakse, et hulgad A ja B moodustavad kõigi reaalarvude hulgas *Dedekindi lõike* $A \mid B$. Kui leidub selline arv x, et $a \leqslant x \leqslant b$ kõikide $a \in A$ ja $b \in B$ korral, siis arvu x nimetame lõike $A \mid B$ *eraldusarvuks*.

Lause 22. *Dedekindi lõike $A \mid B$ eraldusarv (kui see eksisteerib) on üheselt määratud.*

Teoreem 23. *Järgmised väited on samaväärsed.*

i) Igal Dedekindi lõikel $A \mid B$ reaalarvude hulgas $\mathbb{R}$ on eraldusarv.

ii) Igal ülalt tõkestatud hulgal $A \subset \mathbb{R}$ leidub ülemine raja.

1.4.5 Irratsionaalarvud

Hulka $\mathbb{R} \backslash \mathbb{Q}$ nimetatakse *irratsionaalarvude hulgaks* ja tähistatakse $\mathbb{I}$. Kuna $\mathbb{Q}$ on loenduv, aga $\mathbb{R}$ on mitteloenduv, on ka $\mathbb{I}$ mitteloenduv.

Ülesanne 24. Kas leiduvad mittetäisruudud p ja q selliselt, et $\sqrt{p} + \sqrt{q}$ on ratsionaalarv?

Ülesanne 25. Kas leiduvad irratsionaalarvud a ja b selliselt, et a^b on ratsionaalarv?

Lause 26. *Arvud e ja π on irratsionaalarvud.*

Lahtised probleemid: ühegi $m, n \in \mathbb{Z}$, $m, n \neq 0$, korral pole teada, kas $m\pi + ne$ on irratsionaalarv või mitte. Samuti pole teada, kas 2^e, π^e ja $\pi^{\sqrt{2}}$ on irratsionaalarvud või mitte.

1.5 Kompleksarvud ja nende üldistused

Teoreem 27. *Hulk $\mathbb{C} = \{(a, b) : a, b \in \mathbb{R}\}$, kus on defineeritud 0-aarsed tehted $0 = (0, 0)$, $1 = (1, 0)$, elemendi $z = (a, b)$ korral unaarne tehe $-z = (-a, -b)$, nullist*

erinevate elementide $z = (a, b)$ *korral unaarne tehe* $z^{-1} = \left(\frac{a}{a^2+b^2}, \frac{b}{a^2+b^2}\right)$ *ning binaarsed tehted elementidel* $z_1 = (a_1, b_1)$, $z_2 = (a_2, b_2)$ *kujul*

$$z_1 + z_2 = ((a_1 + a_2), (b_1 + b_2)), \qquad z_1 \cdot z_2 = ((a_1a_2 - b_1b_2), (a_1b_2 + a_2b_1)),$$

on kommutatiivne korpus. Sealjuures leidub korpuste isomorfism hulkade $\mathbb{R}$ *ja* $\{(a, 0) : a \in \mathbb{R}\} \subset \mathbb{C}$ *vahel.*

Korpuse $\mathbb{C}$ elemente $z = (a, b)$ nimetatakse *kompleksarvudeks*.

Lause 27 mõttes loeme edaspidi $\mathbb{R} \subset \mathbb{C}$, kusjuures iga $r \in \mathbb{R}$ avaldub kujul $(r, 0) \in \mathbb{C}$. Korpusele $\mathbb{C}$ kanname üle varasemast tuntud kokkulepped tehete suhtes: $z_1 - z_2 = z_1 + (-z_2)$ (vahe), $\frac{z_1}{z_2} = z_1 \cdot z_2^{-1}$ (jagatis) ja $z_1^n = \underbrace{z_1 \cdot z_1 \cdots z_1}_{n}$ (aste). Kompleksarve (a, b) ja $(a, -b)$ nímetatakse üksteise kaaskompleksarvudeks ning kirjutatakse $\overline{(a, b)} = (a, -b)$ või $(a, b)^* = (a, -b)$.

Tähistame $i = (0, 1)$.

Lause 28. $i^2 = -1$.

Kompleksarvu $z = (a, b)$ võib esitada ka kujul $(a, b) = a \cdot (0, 1) + b \cdot (1, 0) = a + bi$. Sellist kuju nimetatakse kompleksarvu z *algebraliseks kujuks*, kusjuures liidetavat a nimetatakse *reaalosaks* ja liidetavat bi *imaginaarosaks*.

Kompleksarvude vallas defineeritakse reaalarvudega analoogiliselt *loomulik topoloogia*

$$\tau_{\mathbb{C}} = \left\{U \subset \mathbb{C} : \forall u \in U \exists \varepsilon > 0 \{r \in \mathbb{C} : |r - u| < \varepsilon\} \subset U\right\} \cup \varnothing.$$

Siin $|z|$ tähistab kompleksarvu z moodulit $|z| = \sqrt{a^2 + b^2}$. Reaalarvudega analoogiliste definitsioonide abil saab kompleksarvude valda sisse tuua funktsiooni piirväärtuse ja tuletise mõiste.

Ajalooliselt on kompleksarvudel olnud mitmeid erinevaid kujusid. Kompleksarvu $z = (a, b) = a \cdot 1 + b \cdot i$ kuju nimetatakse *algebraliseks kujuks*. Lisaks tuntakse veel *trigonomeetrilist*, *eksponentkuju* ja *maatrikskuju*.

Kompleksarvu $z = (a, b)$ trigonomeetriliseks kujuks nimetatakse esitust $z = r(\cos\varphi + i \sin\varphi)$, kus arv $r = |z|$ on kompleksarvu z moodul ja arvu φ nimetatakse kompleksarvu z argumendiks. Kompleksarvu võrduse definitsioonist saame, et $a = r\cos\varphi$ ja $b = r\sin\varphi$. Niisiis kehtib võrdus

$$a^2 + b^2 = r^2\cos^2\varphi + r^2\sin^2\varphi = r^2.$$

Seega, kui $z = 0$, siis $r = 0$ ja φ võime määrata suvalise. Kui aga $z \neq 0$, siis nõudega, et $r \geqslant 0$, saame määrata $r = +\sqrt{a^2 + b^2}$. Nüüd saab nurga φ leida trigonomeetrilisest võrrandist $\frac{a}{b} = \tan\varphi$.

Kompleksarvu $z = (a, b)$ eksponentkujuks nimetatakse esitust $z = re^{i\varphi}$. See kuju tekib otsekohe, kui defineerida kompleksarvulisest argumendist eksponentfunktsioon astmereaga

$$e^z = \sum_{k=0}^{\infty} \frac{z^k}{k!},$$

valides z rolli $i\varphi$ ning meenutades siinuse ja koosinuse astmeridu:

$$\sin x = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k+1}}{(2k+1)!}, \qquad \cos x = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k}}{(2k)!}.$$

Rea ümberjärjestamine on siin võimalik seetõttu, et kõik need kolm rida on absoluutselt koonduvad.

Kooliõpilasele mõistetavamalt saab tõestada funktsiooni $f(\varphi) = \dfrac{\cos\varphi + i\sin\varphi}{e^{i\varphi}}$ tuletise kaudu.

Valemit $e^{ix} = \cos x + i \sin x$ nimetatakse **Euleri valemiks**. Sellest saab lihtsasti tuletada **de Moivre'i valemi** $(\cos x + i \sin x)^n = \cos nx + i \sin nx$. De Moivre'i valem illustreerib trigonomeetrilise ja eksponentkuju populaarsuse põhjust – need kujud asendavad kompleksarvude korrutamise argumentide liitmisega.

Erinevalt reaalarvude korpusest ei saa kompleksarvude korpusse sisse viia järjestust nii, et ta oleks tehetega kooskõlas, st. et kehtiksid järjestusaksioomide analoogid.

Lause 29. *Kompleksarvude hulgal ei saa defineerida järjestusseost $>$, mis rahuldaks*

a) kui $z \neq 0$, siis kas $z > 0$ või $-z > 0$, kuid mitte mõlemad;
b) kui $z_1 > 0$ ja $z_2 > 0$, siis $z_1 z_2 > 0$.

Võrreldes reaalarvude hulgaga on kompleksarvudel määratud funktsioonid oma ehituselt keerukamad. Näiteks juba ruutfunktsioon $f(z) = z^2$ on kaheleheline funktsioon. n-astme juuri on mistahes kompleksarvust täpselt n tükki. (Seega juurfunktsioon pole rangelt võttes üldse funktsioon.)

Ka diferentseeruvuse mõiste tuleb teistsuguse, rangema sisuga. Ühese funktsiooni korral garanteerib diferentseeruvus mistahes järku tuletiste eksisteerimise. Samuti kehtib võrdlemisi üllatav tulemus.

Teoreem 30 (Liouville)**.** *Kui funktsioon $w = f(z)$ on ühene, diferentseeruv ja tõkestatud kogu komplekstasandil, siis on ta konstantne.*

Siit järeldub otsekohe algebra põhiteoreem.

Teoreem 31. *Igal komplekssete kordajatega mittekonstantsel polünoomil on vähemalt üks nullkoht kompleksarvude vallas.*

Kompleksarve kasutatakse elektroonikas, signaalitöötluses, reaalmuutuja integraalide leidmisel, geomeetrias jmt.

1.5.1 Kvaternioonid

Vaatleme kvaternioonide hulka $\mathbb{C} \times \mathbb{C} =: \mathbb{K}$ ja varustame ta tehetega:

$$\begin{aligned}(a,b)+(c,d) &= (a+c, b+d);\\ (a,b)\cdot(c,d) &= (ac-db^*, a^*d+cb);\\ (a,b)^* &= (a^*,-b).\end{aligned}$$

Sealjuures ülejäänud tehted defineeritakse loomulikul viisil, kusjuures kompleksarvud sisestuvad hulka $\mathbb{C} \times \mathbb{C}$ loomulikul viisil: $\mathbb{C} \ni z \mapsto (z,0) \in \mathbb{K}$. Eri tähised on mõeldud elementide $i = (i,0)$, $j = (0,1)$ ja $k = (0,i)$ jaoks. Lihtne on koostada kvaternioonide korrutustabel, sealhulgas $i^2 = j^2 = k^2 = ijk = -1$.

Osutub, et $(a,b)^*(a,b)$ on reaalarv (kvaterniooni (a,b) moodul).

Kvaternioonid moodustavad liitmise ja korrutamise suhtes mittekommutatiivse korpuse (ehk kaldkorpuse).

Samasugust, *Cayley-Dicksoni konstruktsiooni* saab jätkata, aga korrutamise omadused halvenevad. Nii moodustuvad oktonioonid, mis ei ole korrutamise suhtes assotsiatiivsed, ning edasi sedenioonid, kus korrutamise suhtes tekivad *nullitegurid* (nullist erinevad arvud, mille korrutis on null). Kõik need arvuhulgad on üksteisesse loomulikul viisil sisestatavad:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{K} \subset \mathbb{O} \subset \mathbb{S} \subset \dots$$

1.6 Algebralised ja transtsendentsed arvud

Definitsioon 32. Kompleksarvu nimetatakse **algebraliseks**, kui ta on mingi täisarvuliste kordajatega polünoomi nullkoht. Kui kompleksarv ei ole algebraline, siis öeldakse, et ta on **transtsendentne**.

On selge, et kõik ratsionaalarvud on algebralised. Samas, „suurem osa“ reaalarve on siiski transtsendentsed.

Lause 33. *Algebraliste arvude hulk on loenduv.*

Lause 34. *Transtsendentsete arvude hulk on kontiinumi võimsusega.*

Definitsioon 35. Öeldakse, et korpuse K alamhulk A on *algebraliselt sõltumatu* üle alamkorpuse L, kui mistahes lõpliku jada $\alpha_1, \dots, \alpha_n \in A$ korral, kus kõik arvud α_i on erinevad, ja mistahes mittetriviaalse polünoomi $P(x_1, \dots, x_n)$ korral, mille kordajad on alamkorpusest L, kehtib $P(\alpha_1, \dots, \alpha_n) \neq 0$.

Näiteks alamhulk $\{\sqrt[3]{e}, e+1\}$ ei ole algebraliselt sõltumatu üle $\mathbb{Q}$, kuna polünoomis $P(x_1,x_2) = x_1^3 - x_2 + 1$ võtame $x_1 = \sqrt[3]{e}$, $x_2 = e+1$ ja saame $P(x_1,x_2) = 0$.

Teoreem 36 (Lindemann-Weierstrassi teoreem)**.** *Kui $\alpha_1, \ldots, \alpha_n$ on algebralised arvud, mis on lineaarselt sõltumatud üle $\mathbb{Q}$, siis $e^{\alpha_1}, \ldots, e^{\alpha_n}$ on algebraliselt sõltumatud üle $\mathbb{Q}$.*

Lause 37. *Mistahes nullist erineva algebralise arvu α korral on e^{α} transtsendentne.*

Lause 38. *π on transtsendentne. Mistahes nullist erineva algebralise arvu α korral on $\sin\alpha$, $\cos\alpha$, $\tan\alpha$ transtsendentsed.*

Peatükk 2

Matemaatilised struktuurid

2.1 Binaarsed seosed

Olgu X ja Y mistahes hulgad.

Definitsioon 39. *Binaarseks seoseks*, edaspidi lihtsalt *seoseks*, hulkade X ja Y vahel nimetatakse otsekorrutise $X \times Y = \{(x, y) : x \in X, y \in Y\}$ mistahes alamhulka. Kui $R \subset X \times Y$ on seos, siis asjaolu, et $(x, y) \in R$, kirjutatakse ka xRy või $R(x, y)$.

Definitsioonist 39 järeldub, et $\varnothing$ ja $X \times Y$ on seosed hulkade X ja Y vahel. Sealjuures seost $\varnothing$ nimetatakse *tühjaks seoseks*.

Definitsioon 40. *Kujutuseks* hulgast X hulka Y nimetatakse eeskirja, mis hulga X iga elemendi korral seab temale vastavusse täpselt ühe elemendi hulgas Y. Kui f on kujutus hulgast X hulka Y, siis elemendile $x \in X$ kujutusega f vastavusse seatud elementi (ehk elemendi x *kujutist*) tähistatakse $f(x)$. Asjaolu, et f töötab hulgast X hulka Y, märgitakse kirjutisega $f : X \to Y$.

Võtame kasutusse mõned seost iseloomustavad mõisted.

Definitsioon 41. Öeldakse, et seos $R \subset X \times Y$ on

- *totaalne*, kui $\forall x \in X \, \exists y \in Y : xRy$;
- *sürjektiivne*, kui $\forall y \in Y \, \exists x \in X : xRy$;
- *ühene*, kui $\forall x \in X \, \forall y, z \in Y \; xRy \wedge xRz \Rightarrow y = z$;
- *injektiivne* ehk *üksühene*, kui $\forall y \in X \, \forall x, z \in Y \; xRy \wedge zRy \Rightarrow x = z$;
- *bijektiivne*, kui R on totaalne, sürjektiivne, ühene ja üksühene.

Ülesanne 42. Kontrolli, et seos on totaalne parajasti siis, kui tema pöördseos on sürjektiivne. Kontrolli, et seos on ühene parajasti siis, kui tema pöördseos on üksühene.

Seose ja kujutuse mõiste vahekorda iseloomustab järgmine

Lause 43. *Kui $R \subset X \times Y$ on totaalne ühene seos, siis võrdusega $f(x) = y$, kus xRy, on defineeritud kujutus $f : X \to Y$.*

Kui $f : X \to Y$ on kujutus, siis $R = \{(x, f(x)) : x \in X\}$ on totaalne ühene seos.

Ülesanne 44. Kontrolli, et kujutus f on injektiivne parajasti siis, kui temale vastav seos lause 43 mõttes on injektiivne.

Kontrolli, et kujutus f on sürjektiivne parajasti siis, kui temale vastav seos lause 43 mõttes on sürjektiivne.

Kontrolli, et kujutus f on bijektiivne parajasti siis, kui temale vastav seos lause 43 mõttes on bijektiivne.

Definitsioon 45. Öeldakse, et seos $R \subset X \times X$ on

- *refleksiivne*, kui $\forall x \in X : xRx$;
- *sümmeetriline*, kui $\forall x, y \in X : xRy \Rightarrow yRx$;
- *antisümmeetriline*, kui $\forall x, y \in X : xRy \wedge yRx \Rightarrow x = y$;
- *transitiivne*, kui $\forall x, y, z \in X : xRy \wedge yRz \Rightarrow xRz$;
- *lineaarne*, kui $\forall x, y \in X : xRy \vee yRx$;

Definitsioon 46. Öeldakse, et seos $R \subset X \times X$ on *ekvivalentsusseos*, kui ta on refleksiivne, sümmeetriline ja transitiivne.

Saab näidata, et ekvivalentsusseosed hulgal X on üksüheses vastavuses *klassijaotustega* hulgal X, st. selliste alamhulkade süsteemidega $X_\alpha \subset X$, $\alpha \in \mathfrak{A}$, kus $X_\alpha \neq \varnothing$ kõigi $\alpha \in \mathfrak{A}$ korral ning $\bigsqcup_{\alpha \in \mathfrak{A}} X_\alpha = X$. Sellele vastavusele tugineb hulkade ja struktuuride faktoriseerimine.

Definitsioon 47. Öeldakse, et seos $R \subset X \times X$ on *osalise järjestuse seos*, kui ta on refleksiivne, antisümmeetriline ja transitiivne.

Ülesanne 48. Kirjelda kõik seosed hulgal X, mis on korraga nii ekvivalentsusseosed kui ka osalise järjestuse seosed.

Teoreem 49. *Olgu $\leqslant$ osalise järjestuse seos. Defineerime seose $<$ selliselt, et $x < y \Leftrightarrow x \leqslant y \ \wedge \ x \neq y$. Seos $<$ on*

1° *irrefleksiivne:* $\forall x \in X \neg(x < x)$;

2° *asümmeetriline:* $\forall x, y \in X \, (x < y \Rightarrow \neg(y < x))$;

3° *transitiivne.*

Vastupidi, olgu seos $<$ irrefleksiivne, asümmeetriline ja transitiivne. Siis seos $\leqslant$, mis on defineeritud $x \leqslant y \Leftrightarrow x < y \vee x = y$, on osalise järjestuse seos.

Seose kohta, mis on irrefleksiivne, asümmeetriline ja transitiivne, öeldakse mõnikord ka *range osaline järjestus*.

Osaline järjestus on näiteks (kontrollida!)

- naturaal-, täis-, ratsionaal-, reaalarvud loomuliku järjestuse $\leqslant$ suhtes;
- naturaalarvud (aga mitte täisarvud!) jaguvusseose $x \mid y \Leftrightarrow \exists z : y = xz$ suhtes;
- antud hulga alamhulkade hulk sisalduvusjärjestuse suhtes;
- antud vektorruumi (normeeritud ruumi, Banachi ruumi jmt.) alamruumide hulk sisalduvusjärjestuse suhtes;
- antud osaliselt järjestatud hulga P jadaruum $\{(x_n) \subset P : n \in \mathbb{N}\}$ järjestuse $(x_n) \leqslant (y_n) \Leftrightarrow \forall n \in \mathbb{N}\,(x_n \leqslant y_n)$ suhtes;
- antud hulga X ja osaliselt järjestatud hulga P korral kujutuste ruum $P^X = \{f \mid f : X \to P\}$ järjestuse suhtes, kus $f \leqslant g \Leftrightarrow \forall x \in X\,(f(x) \leqslant g(x))$;
- suunatud tsükliteta graafi tipud seose R suhtes, kus xRy parajasti siis, kui leidub ahel tipust x tippu y;
- antud osaliselt järjestatud hulga P korral hulgal $P \times P$ *leksikograafiline* järjestus: $(x, y) \leqslant_L (u, v) \Leftrightarrow x < u \vee (x = u \wedge y \leqslant v)$;
- antud osaliselt järjestatud hulga P korral hulgal $P \times P$ järjestus: $(x, y) \leqslant_P (u, v) \Leftrightarrow x \leqslant u \wedge y \leqslant v$;
- antud osaliselt järjestatud hulga P korral hulgal $P \times P$ järjestus: $(x, y) \leqslant_{P^*} (u, v) \Leftrightarrow (x < u \wedge y < v) \vee (x = u \wedge y = v)$.

Kolme viimase näite kohta kehtib sisalduvusvahekord $\leqslant_{P^*} \subset \leqslant_P \subset \leqslant_L$.

Definitsioon 50. Osaliselt järjestatud hulga X (seose R suhtes) elementi $x \in X$ nimetatakse

- *vähimaks*, kui $\forall y \in X\,(x \leqslant y)$;
- *suurimaks*, kui $\forall y \in X\,(y \leqslant x)$;
- *minimaalseks*, kui $\forall y \in X\,(y \leqslant x \Rightarrow y = x)$;
- *maksimaalseks*, kui $\forall y \in X\,(x \leqslant y \Rightarrow x = y)$.

Ülesanne 51. Tõesta, et iga vähim element on minimaalne. Tõesta, et iga suurim element on maksimaalne.

Definitsioon 52. Öeldakse, et seos $R \subset X \times X$ on *lineaarse järjestuse seos*, kui ta on lineaarne osalise järjestuse seos. Lineaarselt järjestatud hulka nimetatakse *ahelaks*.

Ülesanne 53. Millised ülaltoodud osalistest järjestustest on lineaarsed järjestused?

Ülesanne 54. Tõesta teoreemiga 49 analoogiline teoreem *range lineaarse järjestuse* kohta, kus seda mõistet defineerivateks omadusteks on irrefleksiivsus, transitiivsus ja trihhotoomia (st. et suvaliste elementide a ja b korral kehtib täpselt üks lausetest $a < b$, $a = b$ või $a > b$.

Ülesanne 55. Tõesta, et lineaarselt järjestatud hulgal langevad vähima ja minimaalse ning suurima ja maksimaalse elemendi mõisted kokku. Leia näide osaliselt järjestatud hulgast ning tema elemendist, mis on minimaalne, kuid ei ole vähim, ning elemendist, mis on maksimaalne, kuid ei ole suurim.

Definitsioon 56. Öeldakse, et lineaarse järjestuse seos $R \subset X \times X$ on täieliku järjestuse seos, kui tema igal alamhulgal leidub vähim element.

Ülesanne 57. Tõesta, et osaliselt/lineaarselt/täielikult järjestatud hulga alamhulk on samuti osaliselt/lineaarselt/täielikult järjestatud hulk.

Ülesanne 58. Millised ülaltoodud lineaarsetest järjestustest on täielikud?

2.2 Aksiomaatilise hulgateooria elemendid

2.2.1 Zermelo-Fraenkeli aksiomaatika alused

Selles alapeatükis anname hulgateooria aksiomaatilise käsitluse alused. Kasutame Zermelo-Fraenkeli aksiomaatikat. Fikseerime signatuuri $(;;\in)$. Sealjuures kirjutame $\neg(x \in y)$ asemel $x \notin y$ ning $\exists x\,(\varphi(x) \wedge (\forall y\,(\varphi(y) \supset y = x)))$ asemel $\exists! x\,\varphi(x)$. (Selles peatükis võtame lausearvutuse implikatsiooni tähiseks $\supset$.)

ZF1° $\vdash \exists x\,\forall u\,(u \notin x)$.
See on *tühja hulga aksioom*, mis väidab, et leidub hulk, milles pole ühtegi elementi. Edaspidiseks tähistame selle hulga $\varnothing$.

ZF2° $\vdash \forall x\,\forall y\,(\forall u\,(u \in x \Leftrightarrow u \in y) \Leftrightarrow x = y)$.
See aksioom ütleb, et hulgad on võrdsed parajasti siis, kui neil on ühed ja samad elemendid.

ZF3° $\vdash \forall x\, \exists y\, \forall u\, (u \in y \Leftrightarrow \forall v\, (v \in u \supset v \in x))$.
See on *potentshulga aksioom*. Ta ütleb, et iga hulga jaoks leidub hulk, mille elementideks on antud hulga alamhulgad ja mitte midagi muud. Edaspidiseks tähistame selle hulga $\mathcal{P}(x)$.

ZF4° $\vdash \forall x\, \exists y\, \forall u\, (u \in y \Leftrightarrow \exists v\, (u \in v \ \wedge\ v \in x)$.
See on *ühendi aksioom*. Ta ütleb, et iga hulga jaoks leidub hulk, mille elementideks on antud hulga elementideks olevate hulkade elemendid. Sellist hulka tähistame edaspidi $\cup x$.

ZF5° $\vdash \exists x\, (\varnothing \in x \ \wedge\ \forall u\, (u \in x \supset \exists v\, (v \in x \ \wedge\ \forall w\, (w \in v \Leftrightarrow w \in u \ \vee\ w = u))))$.
See on *lõpmatu hulga aksioom*. Ta ütleb, et leidub hulk, mille elementideks on tühi hulk ja koos iga hulgaga u ka hulk $u \cup \{u\}$. Taolist hulka nimetatakse mõnikord ka *induktiivseks*.

ZF6° $\vdash \forall w_1 \cdots \forall w_n\, (\forall u\, \exists! v\, \varphi(u, v, w_1, \ldots, w_n) \supset$
$\forall x\, \exists! y\, \forall v\, (v \in y \Leftrightarrow \exists u\, (u \in x \ \wedge\ \varphi(u, v, w_1, \ldots, w_n))))$, kus $\varphi(u, v, w_1, \ldots, w_n)$ on suvaline valem, mille vabad muutujad on $u, v, w_1, \ldots, w_n$.
See on *asenduse aksioomiskeem*. Siin on kirjas üks aksioom iga valemi φ jaoks, kus on vähemalt kaks vaba muutujat. Tema sisuline tähendus on, et kui rakendada funktsiooni mingi hulga elementidele, siis ka saadud väärtused moodustavad hulga. Täpsemalt, kui mingite parameetrite $w_1, \ldots, w_n$ korral valem φ määrab funktsionaalse seose u ja v vahel (iga u jaoks leidub täpselt üks v nii, et kehtib $\varphi(u, v, w_1, \ldots, w_n)$), siis lastel u muutuda hulga x piires, moodustavad vastavad v väärtused hulga y.

ZF7° $\vdash \forall x\, (\exists u\, (u \in x) \supset \exists v\, (v \in x \ \wedge\ \forall w\, (\neg(w \in x \ \wedge\ w \in v))))$.
See on *regulaarsuse aksioom*. Ta nõuab, et igas mittetühjas hulgas peab leiduma element, mille ühisosa antud hulgaga on tühi. Selle aksioomi eesmärgiks on välistada ebameeldivad olukorrad, nagu näiteks $a \in a$ või $a \in b$ ja $b \in a$. Vt. ka lause 62.

Lause 59. *Leidub täpselt üks tühi hulk.*

Tõestus. Tühja hulga aksioomi põhjal leidub vähemalt üks tühi hulk.

Olgu x_1 ja x_2 sellised, et $\forall u\, (u \notin x_1)$, $\forall u\, (u \notin x_2)$. Siis on täidetud $\forall u\, (u \in x_1 \Leftrightarrow u \in x_2)$. Nüüd aksioomi 2 põhjal $x_1 = x_2$. Seega mistahes kaks tühja hulka võrduvad. □

Teoreem 60. *Kehtib* paari aksioom $\forall x\, \forall y\, \exists z\, \forall u\, (u \in z \Leftrightarrow u = x \ \vee\ u = y)$.

Tõestus. Olgu meil a ja b. Me tahame näidata, et leidub hulk y selliselt, et $v \in y \Leftrightarrow (v = a \ \vee\ v = b)$. Tühja hulga aksioomist tuntud tühjale hulgale $\varnothing$ rakendame

kaks korda potentshulga aksioomi. Siis saame (tavapärases tähistuses) hulga $x = \{\varnothing, \{\varnothing\}\}$. Valime nüüd

$$\varphi(q, v, w_1, w_2) \equiv (q = \varnothing \ \wedge \ v = w_1) \ \vee \ (q \neq \varnothing \ \wedge \ v = w_2).$$

Kui parameetrid w_1 ja w_2 on fikseeritud, on φ funktsionaalne seos: lastes q muutuma mistahes hulgas, kehtib alati täpselt üks $q = \varnothing$ või $q \neq \varnothing$, seetõttu on φ iga q korral tõene täpselt ühe v väärtuse korral (vastavalt kas $v = w_1$ või $v = w_2$ korral).

Rakendame nüüd asendusskeemi, võttes w_1 rolli a ja w_2 rolli b. Me saame, et leidub täpselt üks y selliselt, et tema iga elemendi v korral kehtib: $\exists u\,(u \in x \wedge \varphi(u, v, a, b))$. Aga valem $\varphi(u, v, a, b)$ kehtib kahel juhul: kui $u = \varnothing$ ja $v = a$ ning kui $u \neq \varnothing$ ja $v = b$. Seega leidub täpselt üks hulk y selliselt, et tema elemendid on parajasti a ja b. (Tavapärases tähistuses kirjutaksime $v = \{a, b\}$.) □

Järeldus 61. *Kehtib* $\forall x\, \exists z\, \forall u\, (u \in z \Leftrightarrow u = x)$.

Tõestus. Vahetu järeldus paari aksioomist, võttes seal $x = y$. □

Järeldus 61 väidab sisuliselt, et iga x korral leidub hulk $z = \{x\}$.

Lause 62. *Ei leidu hulka a, mille korral $a \in a$.*

Tõestus. Oletame, et mingi a korral $a \in a$. Valides paari aksioomis x ja y rolli a, saame, et leidub hulk $b = \{a\}$. Ühelt poolt $b \neq \varnothing$, sest $a \in b$. Teiselt poolt, kuna $a \in a$ ja $a \in b$, siis $a \in a \ \wedge \ a \in b$. Niisiis b ei täida regulaarsuse aksioomi nõuet (mittetühjas hulgas b peab leiduma element v, et iga w korral $w \in v \ \wedge \ v \in b$ on väär). Seega hulka b ei eksisteeri ja oleme jõudnud vastuolule. Järelikult oletus taolise a leidumisest peab olema väär. □

Lause 63. *Kehtib* alamhulga aksioom*: $\forall x\, \exists y\, \forall z\, (z \in y \Leftrightarrow z \in x \ \wedge \ \varphi(z))$, kus $\varphi(z)$ on suvaline valem, mille vaba muutuja on z.*

Tõestus. Vaatleme kõigepealt juhtu, kus iga $w \in x$ korral $\neg\varphi(w)$. Siis sobib y rolli $\varnothing$.

Eeldame nüüd, et leidub selline $w \in x$, et $\varphi(w)$. Tähistame

$$\psi(u, v, w_1) \equiv ((u = v) \ \wedge \ \varphi(u)) \ \vee \ ((u = w_1) \ \wedge \ \neg\varphi(u)).$$

Siis ψ sobib asenduse aksioomiskeemi (võttes seal w_1 rolli meie w), kuna iga u korral kehtib täpselt üks lausetest $\varphi(u)$ või $\neg\varphi(u)$. Asendusskeemi põhjal leidub (koguni täpselt üks) y selliselt, et y kõik elemendid v on kas sellised, mille korral $\varphi(v)$, või element w (ja w korral ka kehtib $\varphi(w)$). Tavalises keeles oleme saanud x sellise alamhulga y, kuhu kuuluvad täpselt need elemendid, millel φ on tõene. □

Järeldus 64. *Kehtib* $\forall x_1\, \forall x_2\, \exists y\, \forall z\, (z \in y \Leftrightarrow z \in x_1 \ \wedge \ z \in x_2)$.

Tõestus. Rakenda alamhulga aksioomi, kus x rollis on x_1 ja $\varphi(z) \equiv z \in x_2$. □

Järeldus 64 väidab sisuliselt, et mistahes kahe x_1 ja x_2 korral leidub nende ühisosa.

Paari aksioomi kasutades saame moodustada antud hulkadest a ja b *järjestatud paari* $(a, b) = \{\{a\}, \{a, b\}\}$.

Ülesanne 65. Veendu, et järjestatud paarid (a_1, b_1) ja (a_2, b_2) on võrdsed parajasti siis, kui $a_1 = a_2$ ja $b_1 = b_2$.

Ühtlasi saab järjestatud paari moodustamist üldistada, moodustades $(a, b, c) = ((a, b), c)$ jne.

Mistahes hulkade x ja y korral leidub hulk $\mathcal{P}(\mathcal{P}(\cup\{x, y\}))$, selle alamhulk on aga kõigi järjestatud paaride (a, b) hulk, kus $a \in x$ ja $b \in y$. Seda hulka nimetatakse hulkade x ja y *otsekorrutiseks* ja tähistatakse $x \times y$. Otsekorrutist saab samuti üldistada, võttes $x \times y \times z = (x \times y) \times z$ jne.

Otsekorrutise alamhulgana saab sisse tuua binaarsed seosed, nendest lähtuvalt omakorda funktsioonid jne, nagu me tegime seda eelmises alapeatükis.

2.2.2 Hulkade võrdlemine

Definitsioon 66. Öeldakse, et hulga x võimsus pole suurem kui hulga y võimsus, kui leidub injektsioon $x \to y$. Seda tähistatakse $\overline{\overline{x}} \leqslant \overline{\overline{y}}$.

Öeldakse, et hulga x võimsus pole väiksem kui hulga y võimsus, kui leidub sürjektsioon $x \to y$. Seda tähistatakse $\overline{\overline{y}} \leqslant \overline{\overline{x}}$.

Öeldakse, et hulgad x ja y on *sama võimsusega*, kui leidub bijektsioon $x \to y$. Seda tähistatakse $\overline{\overline{x}} = \overline{\overline{y}}$.

Teoreem 67 (Cantor-Bernstein-Schröderi teoreem)**.** *Kui* $\overline{\overline{x}} \leqslant \overline{\overline{y}}$ *ja* $\overline{\overline{y}} \leqslant \overline{\overline{x}}$, *siis* $\overline{\overline{x}} = \overline{\overline{y}}$.

Järeldus 68. *Hulkade võimsuse poolest võrdlemise seos* $\leqslant$ *(kus* $x \leqslant y$ *parajasti siis, kui* $\overline{\overline{x}} \leqslant \overline{\overline{y}}$*) on osalise järjestuse seos.*

Tõestus. Refleksiivsuse aksioomi realiseerib ühikteisendus. Sümmeetria aksioom tuleneb Cantor-Bernstein-Schröderi teoreemist. Transitiivsus järeldub sellest, et kahe injektsiooni korrutis on injektsioon. □

Vastavalt ülesandele 49 tekib automaatselt ka range osaline järjestus $<$ võimsuste võrdlemiseks.

Teoreem 69 (Cantori teoreem)**.** *Mistahes hulga* x *korral* $\overline{\overline{x}} < \overline{\overline{\mathcal{P}(x)}}$.

Moodustame nüüd seose $\sim$ selliselt, et $x \sim y$ parajasti siis, kui $\overline{\overline{x}} = \overline{\overline{y}}$. See tähendab, hulgad x ja y on seoses $\sim$ parajasti siis, kui nad on sama võimsusega.

Lause 70. *Seos $\sim$ on ekvivalentsusseos.*

Tõestus. Refleksiivsus järeldub sellest, et ühikteisendus on bijektsioon. Sümmeetrilisus järeldub sellest, et bijektsiooni pöördkujutus on ka bijektsioon. Transitiivsus järeldub sellest, et kahe bijektsiooni korrutis on bijektsioon. □

Kõik lõplikud hulgad saab nüüd jaotada sama võimsusega hulkade klassidesse ning lõpliku hulga x korral tähistada, et $\overline{\overline{x}} = n$, kui $x \sim \{1, 2, \ldots, n\}$.

Naturaalarvude hulga $\mathbb{N}$ võimsust tähistatakse $\aleph_0$. Vahetult saab näidata, et $\overline{\overline{\mathbb{Z}}} = \overline{\overline{\mathbb{Q}}} = \aleph_0$. Samuti on algebraliste arvude hulk võimsusega $\aleph_0$.

Reaalarvude hulga $\mathbb{R}$ võimsust tähistatakse c. Saab näidata, et mistahes lõik, vahemik, poollõik, poolsirge on võimsusega c. Samuti on kõigi pidevate reaalmuutuja funktsioonide hulk võimsusega c.

Teoreem 71 (Võimsuste aritmeetika põhiteoreem)**.** *Kui x on lõpmatu hulk, siis $\overline{\overline{x \times x}} = \overline{\overline{x}}$.*

Siit järeldub muuhulgas, et $\overline{\overline{\mathbb{R}^n}} = \overline{\overline{\mathbb{C}}} = \overline{\overline{\mathbb{K}}} = c$ (kus $n \geqslant 1$).

Teoreem 72 (Cantor)**.** *Kehtib seos $\overline{\overline{\mathcal{P}(\mathbb{N})}} = c$.*

2.2.3 Valikuaksioom

Tavaliselt võetakse aksioomide hulka veel üks aksioom. Kirjutise suure mahu tõttu eeldame, et meil on välja arendatud binaarsete seoste teooria kuni totaalse ühese seose (ehk sisuliselt kujutuse) mõisteni.

ZF8° $\vdash \forall x\, \exists R\, \forall y\, (y \in x \supset \exists! z\, (R \text{ totaalne } \wedge\ R \text{ ühene } \wedge\ yRz))$
See on *valikuaksioom*. Ta väidab, et eksisteerib kujutus, mis „valib“ antud hulga igast hulgast välja ühe elemendi.

Valikuaksioomi kasutades saab tõestada järgmised tähtsad tulemused.

- *Kuratowski-Zorni lemma:* Kui mittetühja osaliselt järjestatud hulga igal ahelal leidub ülemine tõke, siis sellel hulgal leidub ülemine raja.
- *Zermelo teoreem:* Iga hulk on täielikult järjestatav.
- *Zermelo teoreemi vahetu järeldus:* Hulkade võimsuse järjestuse seos on lineaarne. (Seega, mistahes kaks hulka on võimsuse poolest võrreldavad.)
- Igal mittetriviaalsel vektorruumil on olemas baas.

- Kui A on lõpmatu hulk, siis leidub injektsioon hulgast $\mathbb{N}$ hulka A. (Teisiti öeldes, iga lõpmatu hulk sisaldab loenduva osahulga.)
- *Hahn-Banachi teoreem:* Igal pideval lineaarsel funktsionaalil $f : U \to \mathbb{K}$, kus U on alamruum normeeritud ruumis X ja $\mathbb{K} = \mathbb{R}$ või $\mathbb{K} = \mathbb{C}$, leidub normi säilitav jätk kogu ruumile X.

Probleem valikuaksioomi juures on see, et nii aksioomis endas kui ka tulemustes öeldud eksisteeriva objekti kohta puudub informatsioon. Näiteks praeguseni ei osata leida täielikku järjestust juba hulgas $\mathbb{R}$, rääkimata keerukamatest hulkadest. Samas, näiteks valikuaksioomi eituse eeldamine tähendaks, et leiduvad hulgad, mis pole võimsuse poolest võrreldavad.

Kui Zermelo-Fraenkeli aksioomide seas on ka valikuaksioom, siis tähistatakse sellist aksiomaatikat ZFC.

Pikka aega oli lahtine küsimus, kas leidub hulk S, mille korral $\aleph_0 < \overline{\overline{S}} < c$. See, nn. *kontiinumihüpoteesi* (Ch) nime all tuntud probleem sai osalise lahenduse aastal 1940 (Gödel): aksioomide süsteem ZFC+Ch ei ole vasturääkiv. Täielik lahendus tuli aastal 1963 (Cohen): aksioomide süsteem ZFC+$\neg$Ch ei ole vasturääkiv. Seega on loenduva ja kontiinumi võimsuse vahepealse võimsusega hulga olemasolu sõltumatu Zermelo-Fraenkeli ülejäänud aksioomidest.

2.3 Afiinne ruum

2.3.1 Afiinse ruumi mõiste ja tähtsamad omadused

Definitsioon 73. Mittetühja hulka $\mathcal{A}$ üle vektorruumi V nimetatakse *afiinseks ruumiks*, kui on antud kujutus $+ : \mathcal{A} \times V \to \mathcal{A}$ selliselt, et $(X, \vec{x}) \mapsto +(X, \vec{x}) := X + \vec{x}$, mis rahuldab kahte järgmist aksioomi:

$\mathrm{A1}^\circ \ \vdash \forall X \in \mathcal{A}\, \forall \vec{x}, \vec{y} \in V\, (X + (\vec{x} + \vec{y}) = (X + \vec{x}) + \vec{y})$;

$\mathrm{A2}^\circ \ \vdash \forall X, Y \in \mathcal{A}\, \exists! \vec{x} \in V\, (X + \vec{x} = Y)$.

Aksioomis $\mathrm{A2}^\circ$ iga kahe punkti X, Y korral tekkivat võrrandi $X + \vec{x} = Y$ ainsat lahendit tähistame sealjuures $\overrightarrow{XY}$.

Vektorruumi V nimetatakse afiinse ruumi $\mathcal{A}$ *sihiruumiks*.

Järeldus 74. *Iga punkti $X \in \mathcal{A}$ korral võrrandil $X + \vec{x} = X$ on üks ja sama lahend $\vec{x} = 0$.*

Järeldus 75. *Võrrandite $X + \vec{x} = Y$ ja $Y + \vec{x} = X$ lahendid on teineteise vastandvektorid, so. $\overrightarrow{YX} = -\overrightarrow{XY}$.*

Järeldus 76. *Iga kolme punkti $X, Y, Z \in \mathcal{A}$ korral $\overrightarrow{XY} + \overrightarrow{YZ} = \overrightarrow{XZ}$.*

Järeldus 77. *Võrdused $X + \vec{x} = Y$ ja $\overrightarrow{OX} + \vec{x} = \overrightarrow{OY}$ on samaväärsed.*

Järeldus 78. *Afiinne ruum on isomorfne oma sihiruumiga.*

Viimasest järeldusest saame, et kui fikseerime punkti $O \in \mathcal{A}$, siis $\mathcal{A} = \{O + \vec{x} : \vec{x} \in V\}$. Sealjuures punkti O võisime valida suvaliselt, mistõttu öeldakse, et afiinne ruum on homogeenne (ühetaoline) – ükski punkt pole teistega võrreldes „parem“.

Definitsioon 79. Afiinse ruumi *mõõtmeks* nimetatakse tema sihiruumi mõõdet: $\dim \mathcal{A} := \dim A$.

Afiinne ruum võib olla ka lõpmatumõõtmeline, kuna sihiruum võib olla suvaline vektorruum. Kui afiinne ruum $\mathcal{A}$ on n-mõõtmeline, siis tähistame seda afiinset ruumi ka $\mathcal{A}^n$.

Definitsioon 80. Afiinse ruumi $\mathcal{A}^n$ *reeperiks* nimetatakse hulka, mis koosneb selle ruumi mingist punktist O ja sihiruumi mingist baasist $\{\vec{e}_i\}$. Punkti O nimetame reeperi *alguspunktiks*. Reeperit tähistame $\{O; \vec{e}_i\}$.

Definitsioon 81. Punkti $X \in \mathcal{A}^n$ *kohavektoriks* reeperi $\{O; \vec{e}_i\}$ korral nimetatakse võrrandi $O + \vec{x} = X$ üheselt määratud lahendivektorit $\overrightarrow{OX}$. Punkti $X \in \mathcal{A}^n$ *koordinaatideks* reeperi $\{O; \vec{e}_i\}$ korral nimetatakse tema kohavektori $\overrightarrow{OX}$ koordinaate sihiruumi baasil $\{\vec{e}_i\}$.

Punkti X koordinaate x^i, mis on määratud seosest $\overrightarrow{OX} = \sum_{i=1}^{n} x^i \vec{e}_i$, kirjutatakse $X(x^1, x^2, \ldots, x^n)$ ehk lühidalt $X(x^i)$. Punkti koordinaadid on üheselt määratud, sest punkti kohavektor on üheselt määratud. Kuna afiinses ruumis puudub igasugune vektorruumi struktuur, siis ei ole otstarbekas kirjutada $X = (x^i)$, vastasel korral jääks mulje, et afiinne ruum on samastatav ruumiga $\mathbb{K}^n$. (Vektori koordinaatide korral küll kirjutame võrdusmärgi, sest see ühtlasi realiseeribki samastamise V ja $\mathbb{K}^n$ vahel, kus $\dim V = n$.)

Antud afiinse ruumi $\mathcal{A}$ reeperiteisendusi on võimalik kirjeldada reeperiteisendusmaatriksite

$$\overline{C} = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ c^1 & c^1_1 & c^1_2 & \ldots & c^1_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c^n & c^n_1 & c^n_2 & \ldots & c^n_n \end{pmatrix} \in GL(n+1, \mathbb{K}) \tag{2.1}$$

abil. Siin esimeses veerus (alates teisest elemendist) on uue reeperi $\{O', \vec{e}'_i\}$ alguspunkti O' koordinaadid vanas reeperis ning ülejäänud veergudes on uute

baasivektorite koordinaadid vanal baasil. Reeperiteisendusmaatriksi abil on võimalik kirjeldada, kuidas teisenevad punkti koordinaadid üleminekul ühelt reeperilt teisele.

Kujul (2.1) maatriksite $\overline{C}$ hulk moodustab maatriksite korrutamise suhtes pööratavate maatriksite $GL(n+1,\mathbb{K})$ alamrühma. Seda nimetatakse afiinseks rühmaks ja tähistatakse $\overline{GL}(n+1,\mathbb{K})$.

Fikseerides afiinse ruumi $\mathcal{A}^n$ kõigi reeperite hulgas $\mathcal{R}(\mathcal{A}^n)$ vabalt ühe reeperi $\{O_{(\circ)}, \vec{e}_i^{\,(\circ)}\}$ (nn. algreeperi), saame mistahes reeperi $\{O, \vec{e}_i\}$ avaldada algreeperi kaudu vastava teisendusmaatriksi $\overline{C} \in \overline{GL}(n+1,\mathbb{K})$ abil: $\{O_{(\circ)}, \vec{e}_i^{\,(\circ)}\} \xrightarrow{\overline{C}} \{O, \vec{e}_i\}$. Selliselt tekib kujutus $\varphi : \mathcal{R}(\mathcal{A}^n) \to \overline{GL}(n+1,\mathbb{R})$ võrdusega $\varphi(\{O, \vec{e}_i\}) = \overline{C}$. Osutub, et φ on isomorfism.

Teoreem 82. *Afiinse ruumi $\mathcal{A}^n$ reeperite hulk $\mathcal{R}(\mathcal{A}^n)$ on isomorfne afiinse rühmaga $\overline{GL}(n+1,\mathbb{K})$.*

Kui afiinse ruumi $\mathcal{A}$ sihiruum V on eukleidiline ruum (st. varustatud skalaarkorrutisega), siis nimetatakse afiinset ruumi $\mathcal{A}$ eukleidiliseks afiinseks ruumiks. Näiteks $\mathcal{A}$ sihiruumiga $\mathbb{R}^n$ on eukleidiline afiinne ruum. Koolis töötatakse eukleidiliste afiinsete ruumidega, kus sihiruumiks on $\mathbb{R}$, $\mathbb{R}^2$ ja $\mathbb{R}^3$. Skalaarkorrutise asemel võib vaadelda selle mõningaid variante, mis võimaldab saada näiteks pseudoeukleidilise või sümplektilise afiinse ruumi.

2.3.2 Afiinsed kujutused ja teisendused

Olgu $\mathcal{A}$ ja $\mathcal{A}'$ afiinsed ruumid vastavalt sihiruumidega V ja V' üle $\mathbb{R}$.

Definitsioon 83. Kujutust $f : \mathcal{A} \to \mathcal{A}'$ nimetatakse *afiinseks kujutuseks*, kui leidub selline lineaarkujutus $\varphi : V \to V'$, et iga punkti $X \in \mathcal{A}$ ja iga vektori $\vec{x} \in V$ korral kehtib $f(X + \vec{x}) = f(X) + \varphi(\vec{x})$. Lineaarkujutust φ nimetatakse afiinse kujutuse f *homogeenseks osaks*.

Afiinse kujutuse definitsioon on korrektne, sest kui $X + \vec{x} = Y + \vec{y}$, siis $X = Y + (\vec{y} - \vec{x})$. Niisiis

$$\begin{aligned} f(X+\vec{x}) &= f(X) + \varphi(\vec{x}) = f(Y + (\vec{y} - \vec{x})) + \varphi(\vec{x}) = \\ &= f(Y) + \varphi(\vec{y} - \vec{x})) + \varphi(\vec{x}) = f(Y) + \varphi(\vec{y}) - \varphi(\vec{x}) + \varphi(\vec{x}) = \\ &= f(Y) + \varphi(\vec{y}) = f(Y + \vec{y}). \end{aligned}$$

Tõestame, et afiinsed kujutused on parajasti need, mis säilitavad vektorite suhted. (Sealhulgas viivad sirged sirgeteks ja säilitavad sirgete paralleelsuse.)

Lause 84. *Olgu $\mathcal{A}$,$\mathcal{A}'$ afiinsed ruumid sihiruumidega V ja V'. Kui kujutus $f : \mathcal{A} \to \mathcal{A}'$ on afiinne, siis on täidetud tingimus*

$$\forall A, B, C \in \mathcal{A}\, \forall t \in \mathbb{R}\ \left(\overrightarrow{AB} = t\overrightarrow{AC} \Rightarrow \overrightarrow{f(A)\,f(B)} = t\overrightarrow{f(A)\,f(C)}\right). \qquad (2.2)$$

Tõestus. Olgu kujutus f afiinne homogeense osaga φ. Näitame, et kehtib nõutav tingimus. Olgu kolm punkti $A, B, C \in \mathcal{A}$ sellised, et leidub $t \in \mathbb{R}$, mille korral $\overrightarrow{AB} = t\overrightarrow{AC}$. Vaatleme võrrandeid $f(A) + \vec{x} = f(B)$ ja $f(A) + \vec{y} = \vec{C}$. Meil on vaja näidata, et $\vec{x} = t\vec{y}$. Näitame, et $\vec{x} = \varphi(\overrightarrow{AB})$ ja $\vec{y} = \varphi(\overrightarrow{AC})$, siis järeldub võrdus $\vec{x} = t\vec{y}$ homogeense osa φ lineaarsusest. Me saame seetõttu, et f on afiinne,

$$f(B) = f(A + \overrightarrow{AB}) = f(A) + \varphi(\overrightarrow{AB}), \qquad f(C) = f(A + \overrightarrow{AC}) = f(A) + \varphi(\overrightarrow{AC}),$$

millest lahendi ühesuse tõttu $\varphi(\overrightarrow{AB}) = \vec{x}$ ja $\varphi(\overrightarrow{AC}) = \vec{y}$. □

Lause 85. *Olgu $\mathcal{A}$,$\mathcal{A}'$ afiinsed ruumid sihiruumidega V ja V'. Kui kujutus $f : \mathcal{A} \to \mathcal{A}'$ on selline, et on täidetud tingimus (2.2), siis ta säilitab sirgete paralleelsuse, st. kui punktid $X, Y, Z, W \in \mathcal{A}$ on sellised, et $\overrightarrow{XY} = \overrightarrow{ZW}$, siis $\overrightarrow{f(X)\,f(Y)} = \overrightarrow{f(Z)\,f(W)}$.*

Tõestus. Olgu antud punktid $X, Y, Z, W \in \mathcal{A}$. Tähistame $O = X + \overrightarrow{ZX}$. Siis $\overrightarrow{XO} = \overrightarrow{ZX}$ ning seetõttu

$$\overrightarrow{OZ} = \overrightarrow{OX} + \overrightarrow{XZ} = \overrightarrow{OX} - \overrightarrow{ZX} = \overrightarrow{OX} - \overrightarrow{XO} = \overrightarrow{OX} + \overrightarrow{OX} = 2\overrightarrow{OX}.$$

Järelikult rahuldavad punktid O, Z, X tingimuse (2.2) eeldust, mistõttu ka $\overrightarrow{f(O)\,f(Z)} = 2\overrightarrow{f(O)\,f(X)}$.

Oletame nüüd, et kehtib $\overrightarrow{XY} = \overrightarrow{ZW}$ ning näitame, et sellest järeldub $\overrightarrow{f(X)\,f(Y)} = \overrightarrow{f(Z)\,f(W)}$. Tähistame $Q = X + \frac{1}{2}\overrightarrow{XY}$, siis $2\overrightarrow{XQ} = \overrightarrow{XY}$, mistõttu tingimuse (2.2) tõttu $2\overrightarrow{f(X)\,f(Q)} = \overrightarrow{f(X)\,f(Y)}$ ning samuti

$$2\overrightarrow{OQ} = 2\overrightarrow{OX} + 2\overrightarrow{XQ} = \overrightarrow{OZ} + \overrightarrow{XY} = \overrightarrow{OZ} + \overrightarrow{ZW} = \overrightarrow{OW},$$

millest järeldub tingimuse (2.2) tõttu, et $2\overrightarrow{f(O)\,f(Q)} = \overrightarrow{f(O)\,f(W)}$. On jäänud arvutada

$$\begin{aligned} \overrightarrow{f(X)\,f(Y)} &= 2\overrightarrow{f(X)\,f(Q)} = -2\overrightarrow{f(O)\,f(X)} + 2\overrightarrow{f(O)\,f(Q)} = \\ &= -\overrightarrow{f(O)\,f(Z)} + \overrightarrow{f(O)\,f(W)} = \overrightarrow{f(Z)\,f(W)}. \end{aligned}$$ □

Teoreem 86. *Olgu $\mathcal{A}$,$\mathcal{A}'$ afiinsed ruumid sihiruumidega V ja V'. Kujutus $f : \mathcal{A} \to \mathcal{A}'$ on afiinne parajasti siis, kui on täidetud tingimus (2.2).*

Tõestus. Kui f on afiinne, siis nõutava tingimuse täidetuse saame lausest 84.

Olgu nüüd kujutus $f : \mathcal{A} \to \mathcal{A}'$ selline, et kehtib tingimus (2.2). Näitame, et iga $X \in \mathcal{A}$ ja $\vec{x} \in V$ korral $f(X + \vec{x}) = f(X) + \varphi(\vec{x})$, kusjuures kujutus $\varphi : V \to V$ on lineaarne.

Fikseerime kõigepealt punkti $O \in \mathcal{A}$ ning defineerime vektori $\varphi(\vec{x})$ kui võrrandi $f(O) + \vec{y} = f(O + \vec{x})$ lahendi $\vec{y} \in V'$.

Olgu nüüd punkt $X \in \mathcal{A}$ ja vektor $\vec{x} \in V$ suvalised. Tähistame $Y = X + \vec{x}$ ning $W = O + \vec{x}$. Siis $\vec{x} = \overrightarrow{OW}$ ning lause 85 kohaselt $\overrightarrow{f(X)\,f(Y)} = \overrightarrow{f(O)\,f(W)} = \varphi(\overrightarrow{OW}) = \varphi(\vec{x})$. Järelikult

$$f(X + \vec{x}) = f(Y) = f(X) + \overrightarrow{f(X)\,f(Y)} = f(X) + \varphi(\overrightarrow{OW}) = f(X) + \varphi(\vec{x}).$$

Veendume, et φ on homogeenne. Fikseerime vektori $\vec{x} \in V$ ja arvu $t \in \mathbb{R}$. Siis punktid O, $O + t\vec{x}$ ja $O + \vec{x}$ rahuldavad tingimuse (2.2) eeldust, mistõttu võrrandite $f(O) + \vec{y} = f(O + t\vec{x})$ ja $f(O) + \vec{z} = f(O + \vec{x})$ lahendid ruumis V' on seoses $\vec{y} = t\vec{z}$. Homogeensus järeldub nüüd tähelepanekust, et $\vec{y} = \varphi(t\vec{x})$ ja $\vec{z} = \varphi(\vec{x})$.

Veendume, et φ on aditiivne. Fikseerime kaks vektorit $\vec{x}, \vec{y} \in V$. Siis

$$\begin{aligned} f(O) + (\varphi(\vec{x}) + \varphi(\vec{y})) &= (f(O) + \varphi(\vec{x})) + \varphi(\vec{y}) = f(O + \vec{x}) + \varphi(\vec{y}) = \\ &= f((O + \vec{x}) + \vec{y}) = f(O + (\vec{x} + \vec{y})). \end{aligned}$$

Kuna ka $f(O) + \varphi(\vec{x} + \vec{y}) = f(O + (\vec{x} + \vec{y}))$, siis $\varphi(\vec{x} + \vec{y}) = \varphi(\vec{x}) + \varphi(\vec{y})$. □

Afiinsete kujutuste tüüpilisteks näideteks on nihe, pööre, venitus jpm.

Märgime, et afiinsetest kujutustest üldisemad, projektiivsed kujutused, viivad küll sirged sirgeteks, aga ei säilita sirgete paralleelsust. Projektiivsete kujutuste omadusi uurib projektiivne geomeetria.

Järgmises lauses näeme, et afiinne kujutus on üheselt määratud, kui teame ühe punkti kujutist ja homogeenset osa.

Lause 87. *Iga lineaarkujutuse $\varphi : V \to V'$ ning iga kahe punkti $A \in \mathcal{A}$ ja $A' \in \mathcal{A}'$ korral leidub selline üheselt määratud afiinne kujutus $f : \mathcal{A} \to \mathcal{A}'$, mille homogeenseks osaks on φ ning mille korral $f(A) = A'$.*

Lause 88. *Olgu $f : \mathcal{A} \to \mathcal{A}'$ ja $g : \mathcal{A}' \to \mathcal{A}''$ afiinsed kujutused homogeensete osadega vastavalt $\varphi : V \to V'$ ja $\psi : V' \to V''$. Siis korrutis $gf : \mathcal{A} \to \mathcal{A}''$ on afiinne kujutus homogeense osaga $\psi\varphi : V \to V''$.*

Definitsioon 89. Afiinset kujutust $f : \mathcal{A} \to \mathcal{A}$ nimetatakse *afiinseks teisenduseks*. Bijektiivseid afiinseid teisendusi nimetatakse *automorfismideks* ehk *liikumisteks*.

Lause 90. *Afiinsete teisenduste hulk teisenduste korrutamise suhtes on monoid.*

Lause 91. *Afiinne teisendus $f : \mathcal{A} \to \mathcal{A}$ on automorfism parajasti siis, kui tema homogeenne osa $\varphi : V \to V$ on automorfism.*

Lause 92. *Afiinse ruumi $\mathcal{A}$ automorfismide hulk* Aut $\mathcal{A}$ *on kujutuste korrutamise suhtes rühm.*

Definitsioon 93. Fikseerime mingi vektori $\vec{a} \in V$ afiinse ruumi $\mathcal{A}$ sihiruumist. Teisendust $\tau_{\vec{a}} : \mathcal{A} \to \mathcal{A}$, mille korral $\tau_{\vec{a}}(X) = X + \vec{a}$, $X \in \mathcal{A}$, nimetatakse afiinse ruumi $\mathcal{A}$ *rööplükkeks* ehk *nihkeks* vektori $\vec{a}$ võrra.

Lause 94. *Iga $\vec{a} \in V$ korral rööplüke $\tau_{\vec{a}} : \mathcal{A} \to \mathcal{A}$ on afiinne teisendus, mille homogeenne osa on samasusteisendus vektorruumil V. Iga afiinne teisendus, mille homogeenne osa on samasusteisendus, on rööplüke.*

Lause 95. *Afiinse ruumi $\mathcal{A}$ kõigi rööplükete hulk on teisenduste korrutamise suhtes rühm, mis on isomorfne sihiruumiga V kui aditiivse rühmaga.*

Definitsioon 96. Olgu $f : \mathcal{A} \to \mathcal{A}$ afiinne teisendus. Kui leidub punkt $O \in \mathcal{A}$ selliselt, et $f(O) = O$, siis öeldakse, et f on *tsentroafiinne* teisendus punkti $O \in \mathcal{A}$ suhtes. Sealjuures nimetatakse punkti O afiinse teisenduse f *püsipunktiks*.

Lause 97. *Etteantud punkti $O \in \mathcal{A}$ ja etteantud lineaarteisenduse $\varphi : V \to V$ korral leidub üheselt määratud tsentroafiinne teisendus püsipunktiga O ja homogeense osaga φ.*

Teoreem 98. *Olgu O afiinse ruumi $\mathcal{A}$ vabalt fikseeritud punkt. Iga afiinse teisenduse $f : \mathcal{A} \to \mathcal{A}$ saab üheselt esitada rööplükke ja tsentroafiinse teisenduse püsipunktiga O korrutisena.*

Saab näidata, et afiinse ruumi $\mathcal{A}^n$ reeperite hulk $\mathcal{R}(\mathcal{A}^n)$ on isomorfne automorfismide rühmaga Aut $\mathcal{A}^n$. Seega teoreemi 82 tõttu on rühmad Aut $\mathcal{A}^n$ ja $\overline{GL}(n+1, \mathbb{R})$ isomorfsed. Selle fakti praktiline tähtsus seisneb asjaolus, et mistahes bijektiivse afiinse teisenduse saab kirjeldada maatriksina ruumist $\overline{GL}(n+1, \mathbb{R})$.

Definitsioon 99. Eukleidilise afiinse ruumi automorfismi nimetatakse *isomeetriliseks liikumiseks*, kui tema homogeenne osa on sihiruumi isomeetriline teisendus, st.

Teisiti öeldes, $f \in$ Aut $\mathcal{A}$ on isomeetriline liikumine, kui tema homogeenne osa φ rahuldab nõuet $\langle \varphi(\vec{x}), \varphi(\vec{y}) \rangle = \langle \vec{x}, \vec{y} \rangle$ mistahes vektorite $\vec{x}, \vec{y} \in V$ korral.

Näiteks rööplüke on isomeetriline liikumine, kuna tema homogeenne osa on samasusteisendus ning seega isomeetriline. Ka pööre on isomeetriline liikumine.

Lause 100. *Eukleidilise afiinse ruumi $\mathcal{A}$ isomeetriliste liikumiste hulk $I(\mathcal{A})$ on rühma* Aut $\mathcal{A}$ *alamrühm.*

Definitsioon 101. Eukleidilise afiinse ruumi mistahes kahe punkti $X, Y \in \mathcal{A}$ vaheliseks kauguseks $\rho(X, Y)$ nimetatakse vektori $\overrightarrow{XY}$ pikkust, st. $\rho(X, Y) = |\overrightarrow{XY}|$.

Lause 102. *Iga isomeetriline liikumine säilitab kahe punkti vahelise kauguse.*

Siit järeldub, et näiteks rööplüke ja pööre säilitavad punktidevahelised kaugused.

2.4 Võre

Definitsioon 103. Olgu X osaliselt järjestatud hulk seose R suhtes.

Öeldakse, et $z \in X$ on elementide $x, y \in X$ *alumine raja*, kui $z \leqslant x$, $z \leqslant y$ ning kehtib implikatsioon $\forall w \in X\,(w \leqslant x \wedge w \leqslant y \Rightarrow w \leqslant z)$. Alumist raja tähistatakse $\inf(x, y)$ või $x \wedge y$.

Öeldakse, et $z \in X$ on elementide $x, y \in X$ *alumine raja*, kui $x \leqslant z$, $y \leqslant z$ ning kehtib implikatsioon $\forall w \in X\,(x \leqslant w \wedge y \leqslant w \Rightarrow z \leqslant w)$. Ülemist raja tähistatakse $\sup(x, y)$ või $x \vee y$.

Definitsioon 104. Öeldakse, et osaliselt järjestatud hulk L on *võre*, kui tema mistahes kahel elemendil leidub ülemine ja alumine raja.

Võre on näiteks (kontrollida!)

- antud hulga kõigi alamhulkade hulk sisalduvusjärjestuse suhtes – sealjuures $X \wedge Y = X \cap Y$ ja $X \vee Y = X \cup Y$;
- antud topoloogilise ruumi lahtiste/kinniste hulkade hulk sisalduvusjärjestuse suhtes – sealjuures $X \wedge Y = X \cap Y$ ja $X \vee Y = X \cup Y$;
- antud vektorruumi (normeeritud ruumi, Banachi ruumi jmt.) alamruumide hulk sisalduvusjärjestuse suhtes – sealjuures $X \wedge Y = X \cap Y$ ja $X \vee Y = X + Y$;
- mistahes lineaarselt järjestatud hulk – sealjuures $x \wedge y = \min(x, y)$ ja $x \vee y = \max(x, y)$;
- naturaalarvude hulk jaguvusseose $x \mid y \Leftrightarrow \exists z : y = xz$ suhtes – sealjuures $x \wedge y = \text{SÜT}\,(x, y)$ ja $x \vee y = \text{VÜK}\,(x, y)$.

Ülesanne 105. Olgu L võre järjestusseosega R. Tõesta, et L on ahel parajasti siis, kui $\{x \vee y, x \wedge y\} = \{x, y\}$ kõigi $x, y \in L$ korral.

Võret võib defineerida ka algebraliselt. Teeme seda ning seejärel sõnastame teoreemi, mis väidab mõlema definitsiooni ekvivalentsust.

Definitsioon 106. *Võreks* nimetatakse kahe kahekohalise algebralise tehtega hulka $(L, +, \cdot)$, milles mistahes $x, y, z \in L$ korral

$$\begin{array}{rclcrcl} (a+b)+c & = & a+(b+c), & & (ab)c & = & a(bc), \\ a+b & = & b+a, & & ab & = & ba, \\ a+a & = & a, & & aa & = & a, \\ (a+b)a & = & a, & & ab+a & = & a. \end{array}$$

Teoreem 107. *Kui võres definitsiooni 104 mõttes defineerida $x + y = x \vee y$ ning $xy = x \wedge y$, siis see on võre definitsiooni 106 mõttes.*

Kui võres definitsiooni 106 mõttes defineerida $x \leqslant y \Leftrightarrow a = ab$, siis see on võre definitsiooni 104 mõttes.

Järeldus 108. *Mistahes naturaalarvude a, b, c korral kehtivad võrdused*

$$\begin{array}{rcl} V\ddot{U}K(V\ddot{U}K(a,b),c) & = & V\ddot{U}K(a,V\ddot{U}K(b,c)), \\ S\ddot{U}T(S\ddot{U}T(a,b),c) & = & S\ddot{U}T(a,S\ddot{U}T(b,c)), \\ V\ddot{U}K(a,b) & = & V\ddot{U}K(b,a), \\ S\ddot{U}T(a,b) & = & S\ddot{U}T(b,a), \\ S\ddot{U}T(a,a) & = & a, \\ V\ddot{U}K(a,a) & = & a, \\ S\ddot{U}T(V\ddot{U}K(a,b),a) & = & a, \\ V\ddot{U}K(S\ddot{U}T(a,b),a) & = & a. \end{array}$$

Lause 109. *Mistahes võre alamvõre on samuti võre.*

Definitsioon 110. Võret L nimetatakse *modulaarseks* ehk *Dedekindi võreks*, kui mistahes $a, b, c \in L$ korral kehtib implikatsioon $a \leqslant c \Rightarrow (a+b)c = a + bc$.

Modulaarsed on näiteks (kontrollida!)

- hulga kõigi alamhulkade võre;
- vektorruumi kõigi alamruumide võre;
- naturaalarvude võre jaguvusseose suhtes.

Definitsioon 111. Võret L nimetatakse *distributiivseks*, kui mistahes $a, b, c \in L$ korral $(a+b)c = ac + bc$.

Lause 112. *Iga distributiivne võre on modulaarne.*

Distributiivsed on näiteks (kontrollida!)

- hulga kõigi alamhulkade võre;
- naturaalarvude võre jaguvusseose suhtes.

Ülesanne 113. Leida näide vektorruumist, mille alamruumide võre ei ole distributiivne. *Näpunäide: vaadelda tasandil asuvate vektorite ruumi.*

Teoreem 114. *Olgu L võre. Järgmised väited on samaväärsed.*

1) *Võre L on distributiivne.*

2) $\forall a, b, c \in L\,(ab + c = (a + c)(b + c))$.

3) $\forall a, b, c \in L\,(ab + bc + ca = (a + b)(b + c)(c + a))$.

4) $\forall a, b, c \in L\,((a + c = b + c) \wedge (ac = bc) \Rightarrow a = b)$.

Ülesanne 115. Kirjuta teoreemi 114 tingimused välja naturaalarvude võre korral.

2.5 Polünoomide ring

2.5.1 Polünoomide definitsioon ja nende mõned omadused

Olgu $R \neq 0$ kommutatiivne ring. Vaatleme kõikvõimalikke jadasid kujul $(a_0, a_1, \dots, a_n, 0, 0, \dots)$ (ülimalt lõplik arv nullist erinevaid elemente), kus $a_k \in R$, $k = 0, 1, \dots, n$. Tähistame kõigi selliste jadade hulga tähisega $R[X]$.

Defineerime hulgas $R[X]$ elementide liitmise ja korrutamise. Olgu $f, g \in R[X]$ sellised jadad, et $f = (a_0, a_1, a_2, \dots)$ ja $g = (b_0, b_1, b_2, \dots)$. Siis defineerime

$$\begin{aligned} f + g &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots), \\ fg &= (c_0, c_1, c_2, \dots), \qquad c_k = \sum_{i+j=k} a_i b_j, \quad k = 0, 1, 2, \dots \end{aligned}$$

Teoreem 116. *Jadade hulk $R[X]$ on kommutatiivne ühikelemendiga ring.*

Definitsioon 117. Ringi $R[X]$ nimetatakse *polünoomide ringiks* üle ringi R ning tema elemente *polünoomideks*.

Lause 118. *Polünoomide ringi $R[X]$ alamhulk $R' = \{(a, 0, 0, \dots) : a \in R\}$ on alamring ringis $R[X]$. Ringid R' ja R on isomorfsed.*

Ringi R' elemente lausest 118 nimetatakse *konstantseteks polünoomideks*.

Tähistame $X = (0,1,0,0,\dots)$. On lihtne veenduda, et $X^n = (\underbrace{0,0,\dots,0}_{n-1},1,0,0,\dots)$, kus $n = 1,2,\dots$. Kui $f = (a_0,a_1,a_2,\dots,a_n,0,0,\dots) \neq 0$ (siin element a_n olgu viimane nullist erinev komponent), siis võime ringi $R[X]$ tehteid kasutades esitada polünoomi f kujul

$$f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n. \tag{2.3}$$

Definitsioon 119. Liidetavaid a_iX^i polünoomi $f \in R[X]$, $f \neq 0$, esituses (2.3) nimetatakse tema *liikmeteks*, liiget a_0 *vabaliikmeks* ja liiget a_nX^n *pealiikmeks*. Polünoomi $X \in R[X]$ nimetatakse *tundmatuks* ehk *muutujaks*. Arvu n nimetatakse polünoomi f *järguks* ja tähistatakse $\deg f$.

Kui $f = (0,0,0,\dots)$, siis loetakse $\deg f = -\infty$.

Osutub, et mõningatel juhtudel saab polünoome jäägiga jagada nagu täisarvegi.

Definitsioon 120. Öeldakse, et ring R on *nulliteguriteta*, kui mistahes $a,b \in R$ korral kehtib implikatsioon $ab = 0 \Rightarrow a = 0 \vee b = 0$.

Teoreem 121. *Olgu R nulliteguriteta ring ning olgu f ja g kaks polünoomi ringist $R[X]$, kusjuures polünoomi g pealiikme kordaja on pööratav ringis R. Siis leiduvad üheselt määratud polünoomid $q,r \in R[X]$ nii, et $f = gq + r$, kusjuures* $\deg r \leqslant \deg g$.

Definitsioon 122. Elementi q teoreemist 121 nimetatakse polünoomide f ja g *jagatiseks* ning elementi r nimetatakse polünoomide f ja g jagamisel tekkivaks *jäägiks*.

Analoogiliselt täisarvudega defineerime jaguvusseose:

Definitsioon 123. Olgu R kommutatiivne nulliteguriteta ring. Öeldakse, et polünoom $f \in R[X]$ jagab polünoomi $g \in R[X]$ ja tähistatakse $f \mid g$, kui leidub polünoom $h \in R[X]$ selliselt, et $g = fh$.

2.5.2 Polünoomide juured

Definitsioon 124. Olgu R kommutatiivne nulliteguriteta ring ning $f = f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in R[X]$. Olgu $c \in R$. Elementi $a_0 + a_1c + a_2c^2 + \cdots + a_nc^n$ nimetatakse polünoomi f *väärtuseks* kohal c ja tähistatakse $f(c)$. Elementi c nimetatakse polünoomi f *juureks*, kui $f(c) = 0$.

Järgnevas on meie eesmärgiks selgitada välja, millal saab avaldada polünoomide juuri ning millised need avaldised on.

Teoreem 125 (Bezout' teoreem)**.** *Jääk, mis tekib polünoomi $f \in R[X]$ jagamisel polünoomiga $X - c$, võrdub $f(c)$.*

Järeldus 126. *Element $c \in R$ on polünoomi f juur parajasti siis, kui $X - c \mid f$.*

Polünoomi $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ ja polünoomi $X - c$ jagatist $g(X) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1}$ ja jääki r saab leida *Horneri skeemi* kasutades:

	a_n	a_{n-1}	a_{n-2}	$\dots$	a_1	a_0
c	a_n	$\underbrace{a_{n-1} + cb_{n-1}}$	$\underbrace{a_{n-2} + cb_{n-2}}$	$\dots$	$\underbrace{a_1 + cb_1}$	$\underbrace{a_0 + cb_0}$
	$\|\|$	$\|\|$	$\|\|$		$\|\|$	$\|\|$
	b_{n-1}	b_{n-2}	b_{n-3}		b_0	r

Ülesanne 127. Tõesta, et Horneri skeemi põhjal leitud $g \in R[X]$ ja $r \in R$ rahuldavad võrdust $f(X) = (X - c)g(X) + r$.

Definitsioon 128. Elementi $c \in R$ nimetatakse polünoomi $f \in R[X]$ *k-kordseks juureks*, kui $(X - c)^k \mid f(X)$, aga $(X - c)^{k+1} \nmid f(X)$.

Lause 129. *Olgu $f \in R[X]$, kus R on nulliteguriteta kommutatiivne ring. Olgu $c_1, c_2, \dots, c_m$ polünoomi f vastavalt $k_1, k_2, \dots, k_m$-kordsed juures, mis on paarikaupa erinevad. Siis*

$$f(X) = (X - c_1)^{k_1}(X - c_2)^{k_2} \cdots (X - c_m)^{k_m} g(X),$$

kusjuures ükski elementidest $c_1, c_2, \dots, c_m$ ei ole polünoomi $g \in R[X]$ juur.

Järeldus 130. *Olgu $f \in R[X]$, $R \neq 0$, kus R on nulliteguriteta kommutatiivne ring. Polünoomi f juurte koguarv (kordsust arvestades) ei ületa selle polünoomi astet.*

Lause 131. *Olgu R kommutatiivne korpus ning $f \in R[X]$, kujuures $n = \deg f$. Kui polünoomil f on korpuses R n juurt, siis f laguneb ringis $R[X]$ lineaartegurite korrutiseks. Vastupidi, kui f laguneb ringis $R[X]$ lineaartegurite korrutiseks, siis polünoomil f on korpuses R n juurt.*

Definitsioon 132. Olgu K korpus ja $f \in K[X]$ mittekonstantne polünoom. Korpust $\overline{K} \supset K$, mille korral polünoom f lahutub ringis $\overline{K}[X]$ lineaartegurite korrutiseks, nimetatakse polünoomi f *lahutuskorpuseks*.

Definitsioon 133. Olgu R kommutatiivne nulliteguriteta ring. Mittepööratavat elementi $p \in R$ nimetatakse *taandumatuks*, kui võrdusest $p = ab$, $a, b \in R$, järeldub, et kas a on pööratav või b on pööratav.

Osutub, et kommutatiivse nulliteguriteta ringi R korral ringi $R[X]$ pööratavad elemendid on parajasti ringi R pööratavad elemendid.

Lause 134. *Olgu K kommutatiivne korpus ja $p \in K[X]$, $\deg p \geqslant 2$, taandumatu polünoom. Siis ring $K_p = K[X]/pK[X]$ on korpus, mis sisaldab korpusega K isomorfset alamkorpust ning milles polünoomil p on olemas juur.*

Definitsioon 135. Mistahes mittekonstantsel polünoomil ringist $K[X]$, kus K on kommutatiivne korpus, leidub lahutuskorpus.

Definitsioon 136. Korpust K nimetatakse *algebraliselt kinniseks*, kui mistahes mittekonstantne polünoom ringist $K[X]$ laguneb selles ringis lineaartegurite korrutiseks.

Teoreem 137 (Algebra põhiteoreem)**.** *Korpus $\mathbb{C}$ on algebraliselt kinnine.*

Algebra põhiteoreemi pole võimalik tõestada ilma reaalarvude korpuse pidevuse aksioomi kasutamata. Samas leidub sellele elegantseid mittealgebralisi tõestusi kompleksarvude teoorias.

Teoreem 138 (Liouville'i teoreem)**.** *Kui kompleksmuutuja funktsioon $w = f(z)$ on diferentseeruv ja tõkestatud kogu komplekstasandil, siis f on konstantne.*

Lause 139 (Kasvulemma)**.** *Mistahes mittekonstantse polünoomi $f \in \mathbb{C}[X]$, $\deg f = n$, korral leidub reaalarv $r > 0$ selliselt, et*

$$|z| > r \quad \Rightarrow \quad \frac{1}{2}|z^n| < |f(z)| < \frac{3}{2}|z^n|.$$

Teoreem 140 (Algebra põhiteoreem)**.** *Mistahes mittekonstantsel polünoomil $f \in \mathbb{C}[X]$ on olemas juur.*

Tõestus. Olgu $f \in \mathbb{C}[X]$ mittekonstantne polünoom (siin: kompleksmuutuja funktsioon $f : \mathbb{C} \ni z \mapsto f(z) \in \mathbb{C}$). Oletame, et polünoomil f pole ühtki juurt korpuses $\mathbb{C}$, st. iga $z \in \mathbb{C}$ korral $|f(z)| > 0$. Olgu $n = \deg f$. Kasvulemmat kasutades leiame reaalarvu $r > 0$ selliselt, et kui $|z| > r$, siis $|f(z)| > \frac{1}{2}r^n$. Kuna komplekstasandi kinnine kera $rB_{\mathbb{C}}$ on kompaktne, siis leidub $u > 0$ selliselt, et $|f(z)| > u$, kui $|z| \leqslant r$. Tähistame $a = \min\left(u, \frac{1}{2}r^n\right)$, siis $|f(z)| > a > 0$ iga $z \in \mathbb{C}$ korral. Vaatleme kompleksmuutuja funktsiooni $g(z) = \frac{1}{f(z)}$, siis $|g(z)| = \frac{1}{|f(z)|} < \frac{1}{a}$. Liouville'i teoreemi põhjal on g konstantne, mistõttu ka f on konstantne. See on vastuolus eeldusega, järelikult leidub polünoomil f juur korpuses $\mathbb{C}$. □

Teoreemide 137 ja 140 väidete samaväärsuse tõestamiseks piisab näidata, et mõlemad väited on samaväärsed väitega: mistahes mittekonstantsel polünoomil $f \in \mathbb{C}[X]$ on (kordsust arvestades) $\deg f$ juurt.

Vahetult kompleksarvude omadustele tuginedes saab näidata, et polünoomi $X^n - c$, kus $c \in \mathbb{C}$, $c = r(\cos\varphi + i\sin\varphi)$, juured on arvud

$$\sqrt[n]{r}\left(\cos\frac{\varphi+2k\pi}{n} + i\sin\frac{\varphi+2k\pi}{n}\right), \qquad k = 0, 1, \ldots, n-1.$$

Lause 141. *Polünoomi $aX^2 + bX + c \in \mathbb{C}[X]$, $a \neq 0$, juurteks on kompleksarvud*

$$c_k = -\frac{b}{2a} + z_k, \qquad k = 1, 2,$$

kus z_1, z_2 on ruutjuured kompleksarvust $\left(\frac{b}{2a}\right)^2 - c$.

Leiame ka kuuppolünoomi juured. Üldisust kitsendamata võime eeldada, et pealiikme kordaja on võrdne arvuga 1.

Ülesanne 142. Kontrolli, et polünoom $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ saab muutuja vahetusega $X = Y - \frac{a_{n-1}}{n}$ (nn. *Tschirnhauseni teisendus*) kuju $f(X) = Y^n + b_{n-2}X^{n-2} + \cdots + b_0$.

Ülesanne 143. Kehtigu $p \neq 0$. Kontrolli, et polünoomi $f(X) = Y^3 + pY + q$ juurte leidmiseks piisab leida polünoomi $f(T) = T^6 + qT^3 - \frac{p^3}{27}$ juured, kus T rahuldab seost $3TY = 3T^2 - p$.

Ülesandega 143 on kuupvõrrand sisuliselt lahendatud, sest polünoomi $f(T) = T^6 + qT^3 - \frac{p^3}{27}$ kõik juured saame leida asendusest $T^3 = Z$, kus $f(Z) = Z^2 + qZ - \frac{p^3}{27}$.

Saab tuletada ka neljanda astme polünoomi juurte üldavaldised. Kõrgema astme polünoomide korral see pole võimalik, nagu väidab järgmine

Teoreem 144 (Abel-Ruffini teoreem)**.** *Mistahes naturaalarvu $n \geqslant 5$ korral leidub polünoom $f \in \mathbb{C}[X]$, $\deg f = n$, selliselt, et polünoomi f juuri ei saa avaldada nelja aritmeetikatehte ja juurimise kaudu.*

Abel-Ruffini teoreemi tõestus on võrdlemisi keeruline, nõudes korpuste teooria ja rühmateooria tundmist. Tähtsat rolli mängib siin Galois' rühma mõiste.