

Matemaatiline maailmapilt

MTMM.00.342

Lektor: Julia Polikarpus

Konspekt: Terje Hill ja Johann Langemets

2023/24 sügis

Sisukord

1	Sissejuhatuse	1
1.1	Kursuse eesmärk	2
1.2	Matemaatika kui keel	2
1.3	Miks õppida matemaatikat?	3
1.4	Kuidas õppida matemaatikat?	3
1.5	Matemaatiline maailmapilt	5
1.6	Mõiste	5
1.7	Defineerimine	6
1.8	Teoreem ja tõestus	7
1.9	Sümbolitest ja matemaatika õigekirjutamisest	11
2	Matemaatilise loogika alused	13
2.1	Matemaatiline loogika	13
2.2	Lausearvutuse põhimõisted	15
2.3	Predikaadid ja kvantorid	16
2.4	Lausearvutuse tehted	17
2.5	Lausearvutuse valemid	20
2.6	Valemi tõeväärtuse leidmine	21
2.7	Valemite omadused	23
2.8	Järeldumine	25
2.9	Samaväärsus	28
2.10	Valemite teisendamine	31
2.11	Täielik disjunktiiivne normaalkuju	33
3	Hulgateooria	37
3.1	Hulga kirjeldamine	38
3.2	Osahulk	41
3.3	Hulkade ühend ja ühisosa	44
3.4	Hulkade vahe ja sümmeetriline vahe	48
3.5	Hulga täiend	50
3.6	Lõplikud ja lõpmatud ühendid ja ühisosad	52
3.7	Hulkade otsekorrutis	54

4	Arvuteooria elemente ja matemaatiline induktsioon	57
4.1	Jaguvus ja algarvud	57
4.2	Matemaatiline induktsioon	60
4.3	Tugev matemaatiline induktsioon	67
5	Tõestamise erinevad meetodid	73
5.1	Pólya printsiibid	75
5.2	Induktiivne ja deduktiivne järeldamine	75
5.3	Tõestamine	76
5.4	Otsene tõestus	77
5.5	Tõestus alamjuhtude põhjal	78
5.6	Kontrapositiivne tõestus	79
5.7	Vastuväiteline tõestus	79
5.8	Samaväärsete tingimuste ehk ekvivalentsi tõestamine	81
5.9	Mitme samaväärse tingimuse tõestamine	82
5.10	Olemasolu ja ühesuse tõestus	83
5.10.1	Konstruktiivne olemasolu tõestus	83
5.10.2	Mittekonstruktiivne olemasolu tõestus	84
5.11	Oletused ehk hüpoteesid	85
5.12	Ümberlükkamised ehk kontranäited	86
5.13	Miks õpetada tõestamist?	87
5.14	Näpunäiteid tõestuse kirjutamiseks	87
6	Funktsioonid	91
6.1	Funktsiooni definitsioon	92
6.2	Hulga karakteristik funktsioon	93
6.3	Hulga kujutis ja tema omadused	96
6.4	Hulga originaal ja tema omadused	98
6.5	Hulga kujutise originaal ja originaali kujutis	100
6.6	Injektiivsed, sürjektiivsed ja bijektiivsed funktsioonid	101
6.7	Dirichlet' printsiip	103
6.8	Funktsioonide kompositsioon	103
6.9	Pöördfunktsioon	106
7	Hulga võimsus	109
7.1	Hulkade ekvivalentsus	109
7.2	Loenduvad hulgad	112
7.3	Cantor–Bernsteini teoreem	116
7.4	Kontiinumi võimsusega hulgad	117
8	Seosed	121
8.1	Seose mõiste	122
8.2	Seose esitusviise	126
8.3	Seose omadused	127
8.4	Tehted seostega	129
8.5	Ekvivalentsusseos	132

8.6	Ekvivalentsiklassid ja faktorhulk	133
8.7	Klassijaotus	134
8.8	Järjestusseos	137
9	Lisad	141
9.1	Valikuaksioom ja sellega ekvivalentsed väited	141
	Kirjandus	144

Sissejuhatus

*Jumal kirjutas universumi
matemaatika keeles – G. Galilei*

1.1	Kursuse eesmärk	2
1.2	Matemaatika kui keel	2
1.3	Miks õppida matemaatikat?	3
1.4	Kuidas õppida matemaatikat?	3
1.5	Matemaatiline maailmapilt	5
1.6	Mõiste	5
1.7	Defineerimine	6
1.8	Teoreem ja tõestus	7
1.9	Sümbolitest ja matemaatika õigekirjutamisest	11

Tõenäoliselt on sinu kokkupuude matemaatikaga kuni praeguse hetkeni suuresti koosnenud ülesannete lahendamisest, kasutades teatud selgeksõpitud lahendusviise ja tehnikaid. Näiteks oled sa õppinud, kuidas lahendada algebralisi võrrandeid ja võrrandisüsteeme, kuidas lihtsustada avaldisi või kontrollida trigonomeetriliste seoste kehtivust. Kasutades teatud reegleid ja lihtsustamist, oled õppinud leidma funktsiooni tuletist ja integraali ning nende abil uurinud funktsiooni käitumist või arvutanud pindalasid ja ruumalasid. Enamasti nõuab selliste ülesannete lahendamine vaid piisavalt harjutamist.

Kõik need meetodid ja tulemused, mida sa koolimatemaatikas õppinud oled, on kunagi ammu teiste inimeste poolt avastatud ning aastate kui mitte aastasade jooksul nende õigsus kontrollitud. Sinu jaoks on see matemaatika muidugi uus olnud ja nagu iga uue asjaga, oled sa selle omandamisel palju õppinud ja vaeva näinud. Uue tarkuse omandamine võiks ja peaks aga huvitav olema! Oled nõus? Nii tore oleks avastada matemaatikas midagi uut, mida me enne ei teadnud, ja näidata, et see uus tulemus kehtib. Aga kuidas seda tehakse? Kuidas tullakse välja uute tulemustega? Kuidas avastatakse uusi seoseid ja uusi meetodeid? Üheks võimaluseks on vaadelda erinevaid näiteid ja leida nende näidete vahel mõni ühine omadus. Vaadeldud näidetele toetudes sõnastatakse teatud hüpotees ehk

väide, mille kohta usutakse, et see võiks kehtida. Esimeseks sammuks tuleb aga iseennast veenda, et see, mida me väidame, on tegelikult ka tõene. Matemaatikas tähendab veenmine tõestuse konstrueerimist. Kuna iseendale lisaks peame ka kõiki teisi oma tulemuse õigsuses veenma, siis peab meie tõestus olema nii selgelt ja loogiliselt kirjutatud, et inimesed, kes tunnevad vastavaid matemaatilisi meetodeid, meid usuksid. Siinkohal tuleks ära märkida ka seda, et kui matemaatikas on väitele esitatud korrektne tõestus, siis ei kahtle enam keegi selle tulemuse õigsuses. Kokkuvõttes tähendab see seda, et sinu tulemus on tõestatud – järelikult see kehtib. Jutu lõpp. Ei ole mingisugust muud alternatiivi. Ja just selle poolest erinebki matemaatika teistest distsipliinidest.

1.1 Kursuse eesmärk

See kursus on üpris erinev sinu senistest kursustest. Meie kõige suuremaks eesmärgiks on arendada matemaatilise tõestuse konstrueerimise ja kirjutamise oskust nii, et sinu kirjutatud tõestused oleksid selged ja arusaadavad ka teistele. Matemaatilise sisu kõrval pöörame suurt tähelepanu ka matemaatilise mõtlemise protsessile ja selle arendamisele. Seega teeme üheskoos läbi arengu, kus sa muutud inimesest, kes matemaatikat kasutab, inimeseks, kes seda ka sügavamalt mõistab. Võib-olla saab see sinu esimeseks sammuks teel, kus sa ühel päeval ise uut matemaatikat ja uusi teadmisi lood. See kõik on saavutatav, kui sa vaid ise seda soovid. Suur osa matemaatikast, mida sa oma järgnevates kursustes kohtad, põhineb teadmiste, mida sa sellelt kursusest omandad. Mida tõsisemalt sa praegu materjali õpid ja matemaatilise mõtlemise protsessi arendad, seda kergem on sul hiljem matemaatikast aru saada. Tegelikult on ju nii, et iga ainet on meeldivam õppida, kui sa sellest ka aru saad. Selle saavutamiseks tuleb sul aga vaeva näha. Liiga tihti kuuleme lapsi või täiskasvanuid väitmas, et nad pole matemaatikas head. See on aga vaid nende väär alibi, mille taha peitu pugeda. Matemaatikat on võimalik selgeks õppida nagu iga teist ainet koolis. Teinekord kuuleme jällegi kedagi väitmas, et kuigi neil läheb matemaatikas hästi ja neile meeldib matemaatika, ei suuda nad kirja panna tõestuskäike. Ka see ei ole mingi argument, sest tõestustest arusaamiseks läheb vaja enesekindlust ja pingutust. See, et sa kontrolltöö või eksami tegid ära ilma suurema õppimiseta ja pingutamisetä, ei ole kindlasti kiitlemist väärt. Pigem on kiitlemist väärt see, kui saad öelda, et sul on hea matemaatiline ettevalmistus.

1.2 Matemaatika kui keel

Matemaatika aitab maailma kirjeldada nagu iga teinegi keel ning lubab seeläbi matemaatika keelt valdavatel inimestel omavahel suhelda ning informatsiooni vahetada. Siiski on matemaatika keel tavapärastest keeltest veidi erinev just selle poolest et, kui tavapärasel keeles võib sõna esineda kohati mitmes tähenduses, siis matemaatika kirjeldab objekte oluliselt täpsemalt ja seejuures üheselt mõistetavalt. Lisaks kasutavad matemaatikud mõistete kirjeldamiseks eraldiseisvat sõnavara, millega oled osaliselt juba koolipingis tutvunud, aga mida me selle kursuse jooksul pidevalt edasi arendame. Märkad peagi, et matemaatikat on tunduvalt raskem õppida siis, kui sa tema keelt ei valda.

Matemaatikud on nagu prantslased: mida sa neile ka ei ütleks, nad tõlgivad selle oma keelde ja edasine on juba midagi täielikult erinevat – Johann Wolfgang von Goethe.

1.3 Miks õppida matemaatikat?

Matemaatika arendab mõtlemist, mida läheb vaja pea igal erialal. Näiteks juristina töötades aitab matemaatika sul kindlasti kõige selgemalt oma argumente üles ehitada või teiste argumentidest vigu leida. Arstina töötades aitab statistika tundmine mõista ravimifirmade poolt välja hõisatud reklaamloosungite tegelikku sisu või aru saada, mida ikkagi tähendab, kui üks või teine DNA-s olev geen suurendab haigestumise riski. Arhitektina ja ehitajana pead oskama jooniseid teha ja nendelt infot lugeda, arvutada ruumide ja pindade suurus või teadma, kuidas leida tala kandevõimet. Arvuti leiutati matemaatikute poolt ning, kui sa äkki veel ei tea, siis mõistavad arvutid ainult matemaatikal põhinevat algoritmilist keelt, mis tähendab aga seda, et kui sa soovid, et arvuti sinu eest midagi ära teeks, pead talle seda ütlema täpselt ja konkreetset – matemaatiliselt.

Lisaks avaldab matemaatika suurt mõju ka kunstile, luulele ja muusikale. Kunstis ja arhitektuuris leiab sageli kuldlõikele põhinevate proportsioonide kasutamist, muusikalised helid koosnevad harmoonilistest võnkumistest ning matemaatikuharidusega on näiteks „Alice Imedemaal” ja „Karupoeg Puhhi” autorid. Viimastest raamatutest leiab ka toremaid sõnamänge. Näiteks, **Lewis Carroll** (1832–1898) loetleb üles aritmeetika neli tehet – kiitmine, nahutamine, jorutamine ja pragamine.

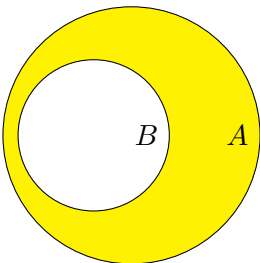


Charles Lutwidge Dodgson, kirjani-kunimega Lewis Carroll

Matemaatika aitab mõista ja kirjeldada meid ümbritsevat maailma. Kahekümnenda sajandi ühe suurima füüsiku Richard Feynman'i sõnul on matemaatika valdamine looduse kirjeldamiseks lausa möödapääsmatu. Matemaatiline bioloogia, matemaatiline füüsika ja teised matemaatikat otseselt kasutavad suunad pole tekkinud juhuslikult, vaid vajadusest kirjeldada meie ümber toimuvaid protsesse. Kindlasti pole siin loetletud näited ainsad, kus matemaatikat vaja läheb või kus ta kasuks võiks tulla – väike maadlus matemaatikaga on hea treening kogu eluks.

1.4 Kuidas õppida matemaatikat?

Matemaatika õppimine ei ole kerge. Ei ole olemas retsepti, kuidas õppida matemaatikat nii, et see oleks huvitav ja tulemused head. Võin aga anda mõned soovitusel. Ole kursis sellega, mis toimub loengutes ja praktikumides. See eeldab kaasa töötamist ning igaks tunniks ettevalmistatud olemist. Pärast iga loengut käi materjal üle, kirjuta tähtsamad kohad oma sõnadega ümber ja täida materjalis puuduolevad lüngad. Uue mõiste kohta koosta mõistekaart või tabel ning täienda seda kursuse jooksul. Siin on toodud näiteks alamhulga mõistekaart:

Definitsioon. Hulka B nimetatakse hulga A <i>osahulgaks</i> ehk <i>alamhulgaks</i> , kui hulga B kõik elemendid on hulga A elementideks. Tähistus. $B \subset A$.	Huvitavad faktid. • Tühi hulk on iga hulga osahulk. • Iga hulk on iseenda osahulk.
Näiteid. • $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ • $\{1, a\} \subset \{1, 2, 3, a, b\}$	Kontranäiteid. • $\{7, c\} \not\subset \{1, 2, 3, a, b\}$ • $7 \not\subset \{7\}$
Visuaal. 	Seotud mõisteid. • Element • Kõikide osahulkade hulk • Pärisosahulk • Venni diagramm • ...

Kui midagi jäi arusaamatuks, küsi kohe kas oma õppejõu või kursusekaaslane käest! Oleks väga hea, kui sul on kaaslane, kellega regulaarselt kursuse materjale arutada. Loe loengukonspekti hoolikalt ja hoi a paber ning pliiats käepärast. Teemat lugedes püüa leida sealt kõige olulisem. Lahenda iseseisvalt läbi kõik näidisülesanded ning tee nõutud kodutöö. Ole kindel, et sa ikka ise ka aru saad, mida kirjutad! Lahenda lisaks ka neid ülesandeid, mida kodutööks antud pole. Veelgi parem on, kui suudad ise mõne ülesande välja mõelda või kontrolltööks valmistumisel endale ise kontrolltöö kirjutada (miks mitte ka teistes ainetes). Seda tehes üllatad sa iseennastki, kui vilunuks sa võid saada! Loovus on matemaatikas väga oluline. Avastades ja luues midagi ise, ei aita sa kaasa ainult enda matemaatiliste teadmiste sügavamaks muutumisele, vaid võid panustada ka matemaatika valdkonna arengusse. Kui oled leidnud esimese seene või teinud oma esimese avastuse, siis vaata ringi: nad kasvavad kobaras. Rõhutan veelkord – matemaatika õppimiseks on vaja enesekindlust, eneseusku ja tugevat pingutust! Pea meeles järgmisi vanasõnu: „Usinus on õnne ema,” „Tamme ei langetata ühe hoobiga,” „Proovi kõiki kimbus olevaid võtmeid“ või „Kui sa ei saa teha seda, mida soovid, siis tee seda, mida suudad“ ning mõtle, mida need sinu jaoks tähendavad.

Üks sell olla otsustanud minna aju siirdamise kliinikusse, et oma aju suurendada. Sekretär seletas talle, et hetkel on saadaval vaid kolme sorti ajusid. Doktorite omad on 20 dollarit unts, advokaatide omad 30 dollarit unts ja matemaatikute omad 1000 dollarit unts. „1000 dollarit untsi eest!” karjus sell. „Miks nad nii kallid on?” „Sest ühe untsi saamiseks on nii palju matemaatikuid vaja.”

1.5 Matemaatiline maailmapilt

Miks just maailmapilt? Maailmapildiks on kombeks nimetada teadmiste süsteemi, mille abil inimene tunnetab teda ümbritsevat maailma ja suhestab end sellega. Maailmapilt on kogu süstematiseeritud info, mida indiviid vastava maailma kohta omab ning see kujuneb välja inimeste kogemuste, teadmiste, tõekspidamiste ja uskumuste baasil. Matemaatikas kujuneb maailmapilt välja aksioomide valiku ja teoreemide tõestamise baasil. Märkima peab ka seda, et erinevatel ajastutel ja erinevatel kultuuridel võib olla erinev maailmapilt. Tänapäeval on tähtis teaduslik maailmapilt, mis toetub teaduses üldomaks võetud seisukohtadele. Kuigi ühiskondlik maailmapilt on pidevas muutumises, on matemaatikas väljakujunenud maailmapilt tänu aluseks võetud aksioomidele ning rangele loogilisele ülesehitusele üpris kindlapiiriline. Matemaatiline maailmapilt tähendab meile matemaatiliste teadmiste konteksti, millesse uued lisanduvad teadmised hästi sobituvad.

1.6 Mõiste

Matemaatikat õppides oleme kokku puutunud paljude mõistetega. Meile on tuttavad näiteks geomeetria mõisted punkt, sirge, tasand, kolmnurk, vektor, risttahukas, kuup, aga ka paljud muud mõisted matemaatika teistest valdkondadest. Selleks, et õpitust aru saada ja oma teadmisi rakendada, tuleb kasutatavaid mõisteid tunda. Nii näiteks saad sa kindlasti aru lausest „EkspONENTfunktsiooni tuletis on võrdne funktsiooni enesega,” sest sa tunnud mõisteid ekspONENTfunktsioon ja tuletis. Seevastu sa arvatavasti ei saa aru sellise lause tähendusest: „Mis tahes mittetühja hulga kõigi ekvivalentsusseoste hulga ja kõigi klassijaotuste hulga vahel on olemas loomulik üksühene vastavus,” sest sa võib-olla pole veel õppinud mõisteid ekvivalentsusseos, klassijaotus või üksühene vastavus.

Nagu igapäevases mõtlemistegevuses, nii ka matemaatikas üldistatakse või ahendatakse mõisteid. Mõiste **üldistamine** tähendab siirdumist vähem üldiselt mõistelt üldisemale mõistele (generalisatsioon). Mõiste **ahendamine** tähendab siirdumist üldisemalt mõistelt vähem üldisele mõistele (determinatsioon). Selliseid mõistete ridu, milles mõisted on astmeliselt tuletatavad üldistamise või ahendamise teel, nimetatakse loogilisteks redeliteks. Näiteks loodusteadustes on kasutusel järgmine astmestik: riik, alamriik, hõimkond, klass, selts, sugukond, perekond, liik, alaliik. Matemaatikas võib näitena tuua astmestiku: nelinurk, kumer nelinurk, rööpkülik, ristkülik, ruut.

Ülesanne 1.1. Ahenda ja üldista järgmisi mõisteid:

- (a) kolmnurk;
- (b) silinder;
- (c) ratsionaalarv.

Liigitamine on teatava mõiste mahu täielik ja korrapärastatud avamine. Näiteks kolmnurki võime liigitada nurkade järgi nürinurkseiks, teravnurkseiks ja täisnurkseiks. Liigitades külgede järgi võime jaotada kolmnurki võrdhaarseiks ja isekülkseiks. Liigitus peab toimuma ühel alusel, see tähendab, et liigituse alus peab olema üks ja seesama kogu liigituses, siis

on ta selge ja järjekindel ning liigituse liikmed välistavad üksteist. Vastasel korral satub üks ja sama objekt kahe või enama liigituse liikme alla. Liigitus peab olema ka pidev, s.t liigituses ei tohi olla hüpet. Teaduslikku liigitust nimetatakse **klassifikatsiooniks**.

1.7 Defineerimine

Kui me kasutame mõnda mõistet ja tahame selle mõiste sisu seletada ka teistele, siis võime üles lugeda selle mõiste tunnuseid. Näiteks võime kirjeldada rööpkülikut järgnevalt: „Rööpkülik on tasandiline kujund; hulknurk; tal on neli külge ja neli nurka; tema vastasküljed on paralleelsed ja võrdsed; diagonaalid poolitavad teineteist; sisenurkade summa on 360° ; rööpküliku pindala leitakse kui aluse ja kõrguse korrutis.“ Selline kirjeldamisviis pole aga kuigi otstarbekas, sest osa loetletud omadustest on ülejäänutest järelduvad. Selleks, et täpselt ja lühidalt määratleda rööpkülikut, tuleb teda **defineerida**, tehes seda näiteks nii: „Rööpkülikuks nimetatakse nelinurka, mille vastasküljed on paralleelsed.“

Mõistete määratlemist lihtsamate ja tuntumate mõistete abil nimetatakse mõiste **defineerimiseks** ja mõiste määratlust nimetatakse **definiitsiooniks**.

Definiitsioon peab andma täpse ja lühikese vastuse küsimusele „Mida nimetatakse ...?“ või „Mis on ...?“ Selleks, et definiitsioon oleks täpne, peab ta alluma järgmistele reeglitele. Reeglite tundmine ja nendest kinnipidamine võimaldab vältida ebakorrektsust defineerimisel.

1. **Definiitsioon peab sisaldama ainult nii palju tunnuseid**, et ta täpselt piiritleks defineeritava mahu. Definiitsioon „Kolmnurk on hulknurk“ on liiga lai, aga definiitsioon „Kolmnurk on hulknurk, millel on kolm võrdse pikkusega külge“ jällegi liiga kitsas. (Seleta miks?) Liiga kitsas definiitsioonis on liigitunnuseid rohkem kui vaja.
2. **Defineeritavat mõistet ei tohi defineerida defineeritava mõiste enda**, mõne tema sünonüümi või mõne sellise mõiste kaudu, mis muutub mõistetavaks defineeritava mõiste abil. Seega, definiitsioon ei tohi sisaldada ringi. Kui sellest reeglist ei peeta kinni, saame **tautoloogia** ehk vea „idem per idem,“ mis tähendab ühe ja sama sõna kordumist definiitsioonis.
3. **Definiitsioon peab olema võimaluse korral jaatav**, sest eitava definiitsiooni juures jääb defineeritava sisu määramatuks. Näiteks, „punkt on see, millel ei ole osi ega mingisugust suurust“ või „kolmnurgal ei ole neli külge“ ei ava vastavate mõistete sisu. Eituse abil kirjeldatavaid definiitsioone võib tarvitada ainult siis, kui nad eitavad juba korrektselt defineeritud mõistet.
4. **Definiitsioon peab olema selge ja arusaadav**, see tähendab, et definiitsioonis ei tohi kasutada kahemõttelisi, metafoorseid ja segaseid väljendeid. Sellised väljendid nagu „lõvi on loomade kuningas“ ja „kordamine on tarkuse ema“ ei ole definiitsioonid, aga neist võib olla abi mõistete sisu selgitamisel. Ka kuulus Hegeli poolt antud definiitsioon riigile, „Riik on maailma vaimu poliitiline ilmutis“ on ebakorrektnel samal põhjusel.

Niisiis peab definitsioon mõiste täielikult määrama. Defineerimisel näidatakse hulk, millesse defineeritav objekt kuulub, ja lisatakse tingimus, mis eristab defineeritava objekti selle hulga kõigist teistest elementidest. Näiteks rööpküliku defineerimisel märgitakse, et ta kuulub nelinurkade hulka, ja lisatakse tunnus, mille poolest ta erineb kõigist teistest nelinurkadest.

Mõistet, mis määrab hulga, milles defineeritav objekt sisaldub, nimetatakse **soomõisteks**. Tingimust, mis eraldab defineeritava objekti selle hulga teistest elementidest, nimetatakse **liigitunnuseks**.

Sageli saab antud mõistet mitmel viisil defineerida. Näiteks rööpküliku defineerimisel võib võtta soomõisteks ka hulknurga või koguni tasapinnalise kujundi. Seejuures tuleb vastavalt muuta ka liigitunnust. Kuid ka siis, kui soomõisteks on võetud nelinurk, saab liigitunnust valida mitmeti; selleks võib võtta näiteks vastaskülgede võrdsuse või vastaskülgede paralleelsuse.

Mõisted, mida me mingi mõiste defineerimisel kasutame, peavad varasemast tuntud olema. Järelikult peavad need mõisted olema üldjuhul ise varem defineeritud. Nii tekivad teatavad mõistete astmestikud. Nende astmestike alguses on mõisted, mis jäetakse defineerimata ja mis on aluseks teiste mõistete defineerimisel. Neid mõisteid nimetatakse **algmõisteteks**. Matemaatikas kasutatakse algmõistetena näiteks punkti, ruumi, hulka, arvu, vastavust, suurust ja palju teisi.

Tüdrukute pesapalli mängus on kolm kohtunikku - üks insener, teine füüsik ja kolmas matemaatik. Viimane võistkonna mängija jõuab võistkonna plaadile palliga üheaegselt, kuid kõik kolm kohtunikku otsustavad, et võistleja on mängust väljas. Tüdruku vihane isa küsib, et miks kohtunikud nii otsustasid. Insenerist kohtunik vastab, „Ta on väljas, kuna ma usaldan vaid seda, mis on tegelikkuses toimunud.” Füüsikust kohtunik ütleb, „Ta on väljas, kuna ma usaldan ja kinnitan vaid seda, mida ma näen.” Matemaatik vastab, „Ta on väljas, kuna mina ütlen nii.” (Oskad sa matemaatiku vaatekohta kommenteerida?)

1.8 Teoreem ja tõestus

Matemaatikas ei kontrollita tõe vastavust mitte eksperimenteerimise ja mõõtmise abil, vaid hoopis tõestades. **Teoreem** (kr. theórēma – vaadeldav, uuritav väide) on lause, mille õigsust tuleb tõestada arutluse kaudu, tuginedes aksioomidele ja varem tõestatud lausele. Lauset, mille õigsust ei põhjendata teiste lausete abil, nimetatakse **aksioomiks** (kr. axiōma – omaks võetud lause) ehk **postulaadiks** (ld. postulátum – nõutav).

Aksioomidena vaadeldakse näiteks selliseid lauseid:

- (a) Igale naturaalarvule järgneb vahetult ainult üks naturaalarv.
- (b) Kaht erinevat punkti läbib ainult üks sirge.
- (c) **Paralleelide aksioom:** väljaspool sirget olevat punkti läbib ainult üks sirge, mis on paralleelne antud sirrega.



Eukleides (u 325 eKr–270 eKr). Tema 13 raamatust koosnev teos „Elemendid“ pani aluse Eukleidilisele geomeetriaale.

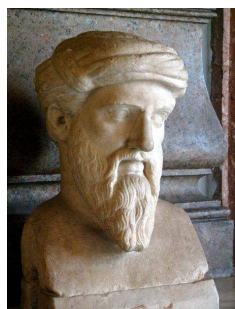
Ülejäänud valemid ja tulemused sõnastatakse lausetena, mida nimetataksegi teoreemideks. Kõigi teoreemide tõesus või väärus tuleneb aluseks võetud aksioomidest. Et aksioome ei tõestata, siis tekib küsimus, millest tuleneb nende tõesus. Aksioomide tõesuse üle otsustame nende alusel tõestatud teoreemide rakendamisel: iga teooriat kontrollib praktika. Aksioomid on õigupoolest vaid hüpoteesid.

Teoreem sõnastatakse tavaliselt kujul: „Kui A , siis B “. Teoreemi osa A , mis on seotud sõnaga kui, nimetatakse teoreemi **eelduseks**, ja osa B , mis on seotud sõnaga siis, **väiteks**. Eelduses öeldakse, millistest objektidest on teoreemis juttu, ehk mis on antud või mis on teada. Väites öeldakse, mis eeldusest järeldeb, ehk mida on vaja tõestada.

Näide 1.2. „Kui kaks vektorit on risti, siis on nende vektorite skalaarkorrutis null.“ Selle teoreemi eelduseks on kahe vektori ristseis ja väiteks see, et nende vektorite skalaarkorrutis on null.

Lühiduse mõttes sõnastatakse teoreeme mõnikord ka lihtlausetena. Väidet „Kõrvunurkade summa on 180° “ on võimalik ümber sõnastada liitlausena „Kui nurgad on kõrvunurgad, siis nende summa on 180° .“

Teoreemi tõestamine tähendab selle näitamist, et eeldusest A järeldeb väide B ; lühemalt $A \Rightarrow B$. Tõestamisel lähtutakse aksioomidest ja varem tõestatud teoreemidest.



Matemaatikas on väidete tõestamine palju rangem kui teistes distsipliinides. Kui me näiteks väidame, et „Juulikuus on Tartus palavad ilmad,“ siis oma viimaste aastate kogemustele tuginedes võime öelda, et see on tõsi, aga kas see tähendab ka seda, et igal aastal on iga juulikuu päev palav? Muidugi mitte! Ei ole kuigi tark tegu teha sellist kõikehõlmavat järelmust üldise ilma puudutava väite kohta. Füüsikud ütlevad, et „Kui keha lastakse lahti maapinna lähedal, siis langeb see keha kiirendusega $9,8 \text{ m/s}^2$.“ See lause on juba suurema tõenäosusega õige võrreldes Tartus juulikuist ilma puudutava lausega, aga ka see füüsika reegel ei ole absoluutselt korrektne. Esiteks, suurus $9,8$ on saadud ümardades. Teiseks, sõna „lähedal“ on väga ebamäärane. Galaktika mõõtmetes on ka Kuu Maale lähedal, aga see ei ole see sama „lähedal“ olemine, mida meie siin silmas peame. Me võiksime täpsustada öeldes, et „lähedal“ tähendab „100 meetri kõrgusel maapinnast,“ aga isegi sellise täpsustusega on probleem. Nimelt on isegi 100 meetri kõrgusel oleva keha gravitatsioonijõud pisut väiksem kui maapinnal oleval kehal. Ja ka maapinnal pole gravitatsioon ühe ja sama suurusega: Everesti mäe otsas on gravitatsioon väiksem kui merepinnal!

Pythagoras (u
570 eKr–490 eKr)

Et teoreemid tõestatakse loogilise arutlusega, siis tuleb uurida veel loogikat – õpetust õigest mõtlemisest. Ka loogikas eraldatakse välja aksioomid – õige mõtlemise põhiseadused.

Seega enamuse lauseid, mida me igapäevaselt ütleme ja väidame ning usume tõesed olevat, ei pruugi olla tõesed absoluutselt ja universaalselt. Matemaatikas aga sõna „tõene“ tähendab absoluutset, ilma igasuguste tingimusteta või erijuhtudeta tõeseks olemist.

Vaatame näitena Pythagorase teoreemi, mis väidab, et kui a ja b on täisnurkse kolmnurga kaks kaatetit ja c on sama kolmnurga hüpoteenus, siis kehtib võrdus $a^2 + b^2 = c^2$.

Loomulikult on see väide ilma igasuguste eranditeta tõene! Me teame seda sellepärast, et

sellele teoreemile on olemas tõestus (tegelikult palju erinevaid tõestusi). Sa võid muidugi küsida ja imestada, et kas see teoreem ikka tõesti kehtib, joonistades täisnurkse kolmnurga paberile ja mõõtes külgede pikkused tuhandiku millimeetri täpsuseni. Ilmneb, et Pythagorase teoreem sinu joonise puhul ei kehti, sest see kolmnurk, mille sa joonistasid ei ole täpne täisnurkne kolmnurk! Joonistamine on matemaatikas oluline abivahend vastava kontseptsiooni mõistmisel, aga tegelikult pole see muud kui vaid visand ehk tint paberil. „Tõeline“ täisnurkne kolmnurk saab vaid meie mõtetes eksisteerida.

Insener, füüsik ja matemaatik sõidavad rongiga läbi Šotimaa. Järsku märkavad nad mäe-küljel musti lambaid. „Vaadake,“ hüüab insener. „Šotimaa selles osas on mustad lambad!“ „Tõesti-tõesti,“ nähvab füüsik vastu. „Sa ei tohiks nii kiiresti järeldusi teha. Kõik, mis me öelda saame on see, et mõned lambad Šotimaa selles osas on mustad.“ „Nojah, ühe külje pealt küll,“ pomiseb matemaatik oma nina alla.

Vahetades lauses „Kui A , siis B “ eelduse ja väite, saame lause „Kui B , siis A .“ Seda lauset nimetatakse antud lause **pöördlauseks**. Kui lause kehtib, siis selle lause pöördlause ei pruugi kehtida.

Näide 1.3. Lause „Kui arv lõpeb nulliga, siis ta jagub viiega“ kehtib. Selle lause pöördlause „Kui arv jagub viiega, siis ta lõpeb nulliga“ ei kehti. Kui võtame aga näiteks lause „Kui kolmnurga küljed on võrdsed, siis on ta nurgad võrdsed“ ja moodustame pöördlause „Kui kolmnurga nurgad on võrdsed, siis ta küljed on võrdsed,“ siis kehtivad nii lause kui ka tema pöördlause.

Asendades lauses „Kui A , siis B “ eelduse ja väite nende eitustega (sümbolid $\neg A$ ja $\neg B$), saame lause „Kui $\neg A$, siis $\neg B$.“ Nii moodustatud lauset nimetatakse antud lause **vastandlauseks**. Jällegi, antud lause kehtivusest ei järeldu tema vastandlause kehtivus.

Näide 1.4. Lause „Kui kujund on kolmnurk, siis ta on hulknurk“ kehtib. Selle lause vastandlause on „Kui kujund ei ole kolmnurk, siis ta ei ole hulknurk.“ See lause ei ole tõene (näiteks nelinurk ei ole kolmnurk, aga hulknurk on ta ikkagi). Lause „Kui arv jagub üheksaga, siis ta ristsumma jagub üheksaga“ vastandlause on „Kui arv ei jagu üheksaga, siis ta ristsumma ei jagu üheksaga.“ Need laused on mõlemad tõesed.

Kui vahetada lauses „Kui A , siis B “ eeldus ja väide ning asendada nende eitustega, saame lause „Kui $\neg B$, siis $\neg A$.“ Seda lauset nimetatakse antud lause **pöördvastandlauseks**. Antud lause kehtivusest järeldub alati selle lause pöördvastandlause kehtivus ning vastupidi. Sümboleis: Kui A , siis $B \Leftrightarrow$ Kui $\neg B$, siis $\neg A$. Öeldakse ka, et need laused on loogiliselt samaväärsed.

Lausetega ning nende pöörd-, vastand- ja pöördvastandlausetega tegeleme lähemalt järgmises lausearvutuse peatükis.

Kui lauses järeldub väide eeldusest (konspektiivselt $A \Rightarrow B$), siis sel juhul öeldakse, et eeldus (A) on **piisav** väite (B) tõesuseks. Kui kehtib lause pöördlause ($B \Rightarrow A$), siis järeldub väitest eeldus. Sel juhul öeldakse, et eeldus on **tarvilik** väite tõesuseks. Kui koos lausega kehtib ka pöördlause, siis võetakse tavaliselt need laused kokku üheks lauseks,

kasutades ühte väljenditest: „on tarvilik ja piisav,” „siis ja ainult siis,” „parajasti siis, kui.”

Näide 1.5. „Selleks, et arv jaguks viiega, on tarvilik ja piisav, et ta lõpeb nulliga või viiega.“ „Arv jagub viiega siis ja ainult siis, kui ta lõpeb nulliga või viiega.“ „Arv jagub viiega parajasti siis, kui ta lõpeb nulliga või viiega.“

Sellised laused esitavad nn tarvilikke ja piisavaid tingimusi. Et korraga kehtivad nii $A \Rightarrow B$ kui ka $B \Rightarrow A$, siis võib seda märkida ka nii: $A \Leftrightarrow B$. Tarvilikke ja piisavaid tingimusi tõestades tõestatakse eraldi tarvilikkus ja piisavus.

Kui mõiste definitsioonis sisalduv liigitunnus on tarvilik ja piisav tingimus selleks, et soomõistega määratud hulga element on defineeritav objekt, siis saab näiteks lause, mis sisaldab tarvilikku ja piisavat tingimust, ümber sõnastada uuritava mõiste uueks definitsiooniks. Mõiste senine definitsioon muutub siis lauseks, mis sisaldab tarvilikku ja piisavat tingimust.

Näide 1.6. Definitsioon. Rööpkülikuks nimetatakse nelinurka, mille diagonaalid poollitavad teineteist. **Lause.** Nelinurk on rööpkülik siis ja ainult siis, kui ta vastasküljed on paralleelsed.

Märk $\square$ või $\blacksquare$ tähistab tavaliselt teoreemi tõestuse lõppu.

Mõned laused on huvitavamad ja tähtsamad kui teised. Seetõttu kasutavad matemaatikud sõna „lause“ asemel akadeemilises tekstis ka teisi alternatiivseid väljendeid:

- **Teoreem** (ingl *Theorem*) on akadeemilises tekstis kõige tähtsam või üldistavam lause.
- **Lause** (ingl *Proposition*) on väide, mis on väiksema tähtsusega kui teoreem.
- **Lemma** (ingl *Lemma*) on abitulemus, mille eesmärgiks on anda iseseiseva tähtsusega vahetulemus, mille abil tähtsamat teoreemi tõestada. Mõnedel teoreemidel on väga keerulised ja pikad tõestused, mis jagatakse osadeks ehk tükkideks. Lemma võibki olla üks selline osa või vahend, mille abil keerulisemat teoreemi tõestada.
- **Järeldus** (ingl *Corollary*) on lühikese ja lihtsa tõestusega tulemus, mille tõestuse olulisemaks osaks on eelnevalt tõestatud teoreem või lause.

Mõnedes tekstides kasutatakse ka järgmisi nimetusi vahetulemuste väljatoomiseks:

- **Väide** (ingl *Claim*) on sarnane lemmale, s.t esineb pikema teoreemi tõestuses ja aitab organiseerida tõestuses vajaminevaid samme. Võib sisaldada vaid vastava teoreemi tõestuse seisukohalt olulisi termineid.
- **Fakt** (ingl *Fact*) on väga väikese tähtsusega abitulemus.

1.9 Sümbolitest ja matemaatika õigekirjutamisest

Kuigi matemaatika on sümbolitele orienteeritud õppeaine, sisaldab matemaatiline tekst sümbolite kõrval ka sõnu. Järgnevalt vaatame üldtuntud soovitusi matemaatilise teksti kirjutamisel:

1. **Ära alusta sümboli, valemi või avaldisega.** Matemaatilise teksti kirjutamine järgib samu reegleid kui tavalise eestikeelse teksti kirjutamine. Näiteks peab lause alati algama suure tähega. Kui lause algab võrrandiga või sümboliga, tundub see suure algustähe puudumise tõttu ebatäiuslik. Samuti on lauset kergem lugeda, kui see algab sõnaga.

Näide. Selle asemel, et kirjutada: $x^2 - 6x + 8 = 0$ on kaks erinevat reaalarvulist lahendit.

Kirjuta: *Võrrandil $x^2 - 6x + 8 = 0$ on kaks erinevat reaalarvulist lahendit.*

2. **Eralda samasse loetelusse mittekuuluvad sümbolid sõnadega.** Ei ole soovitatav kirjutada kahte matemaatilist avaldist või sümbolit kõrvuti, kui nad ei kuulu samasse loetelusse. Selleks, et teha lause paremini loetavaks ning kergemini mõistetavamaks, peaks taolised sümbolid sobiva sõnaga eraldatud olema.

Näide. Lause: *Lisaks arvule a , b on samuti võrrandi $(x - a)(x - b) = 0$ lahendiks.*

Oleks palju selgem, kui lause kirjutada kujul: *Lisaks arvule a on arv b samuti võrrandi $(x - a)(x - b) = 0$ lahendiks.*

3. **Ära ühenda omavahel sõnu ja sümboleid.**

Näide. Selle asemel, et kirjutada: *Iga täisarv ≥ 2 on kas algarv või kordarv.*

Kirjuta: *Iga arvust kaks suurem või võrdne täisarv on kas algarv või kordarv.*

4. **Matemaatilistele sümbolitele ei lisata käändelõppe.** Näiteks, kirjuta *pideva funktsiooniga f* , mitte *pideva f -ga*.
5. **Kirjuta arv välja sõnadega, kui see kirjeldab nimisõna, kui arv on väike või kergesti sõnadega kirjeldatav. Arvulise väärtuse kirjeldamiseks kasuta numbreid.**

Näide. Leidub täpselt kaks 4. järku rühma.

Miljon eestlast ei saa kõik korraga eksida.

Arvust 101 väiksemaid positiivseid arve on 100.

Ühe pileti võid mulle ka anda!

6. **Jälgi, et valemite järel on punktid ja komad nii nagu vaja.**
7. **Väldi professionaalses matemaatilises tekstis sümboleid $\Rightarrow$, $\forall$, $\exists$, $\therefore$, välja arvatud kui kirjutad matemaatilise loogika tehteid.** Antud sümbolid on lühenditeks järgmistele väljenditele: $\Rightarrow$ *kui ..., siis*, $\forall$ *iga*, $\exists$ *leidub*, $\therefore$ *järelikult, seega*. Nende sümbolite teadmine tuleb kasuks, kui on vaja kiirelt loengus märkmeid teha või, kui visandad teoreemile selle tõestuse esimesi versioone. Paljud matemaatikud aga väldivad neid sümboleid oma lõplikus professionaalses tekstis.

Ülesanne 1.7. Kirjuta järgmised laused korrektselt ümber. Millist stiilireeglit on rikutud?

- (a) Liites 23-e ja 45-e, saame vastuseks kakskümmend kuus.
- (b) Olgu x positiivne reaalarv. x võib olla ka ≤ -1 . $x = 0$ on ka sobiv.
- (c) On olemas 3 sorti inimesi need, kes ei oska arvutada ja need, kes oskavad.
- (d) Võrrandi $x^2 = 36$ lahendamiseks $\sqrt{\quad}$ mõlemaid pooli.
- (e) $f(x) = x^2$ ja $g(x) = 3x + 4$ tähendab $f(x) = g(x) = x = 4$.

Matemaatilise loogika alused

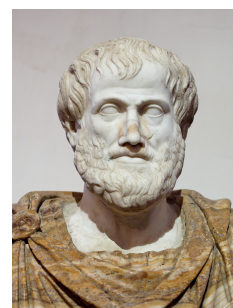
*Eksimine on inimlik, kuid
eksimuses kangekaelselt püsimine
on rumal – ladinakeelne vanasõna*

2.1	Matemaatiline loogika	13
2.2	Lausearvutuse põhimõisted	15
2.3	Predikaadid ja kvantorid	16
2.4	Lausearvutuse tehted	17
2.5	Lausearvutuse valemid	20
2.6	Valemi tõeväärtuse leidmine	21
2.7	Valemite omadused	23
2.8	Järeldumine	25
2.9	Samaväärsus	28
2.10	Valemite teisendamine	31
2.11	Täielik disjunkttiivne normaalkuju	33

2.1 Matemaatiline loogika

Loogika (kreeka keeles, *logiké techné* — mõtlemiskunst, logos – sõna, mõiste, mõistus) on teadus õigest mõtlemisest, selle vormidest ja struktuuridest.

Antiik-Kreeka mõtlejat **Aristotelest** peetakse loogikateaduse rajajaks. Kindlasti tunti ja kasutati mõningaid loogikareegleid juba enne Aristotelest, kuid Aristoteles oli esimene, kes rajas loogika süsteemse teadusena. Sõna „loogika” pärineb samuti kreeka keelest, kuid Aristoteles ise oma õpetust veel selle nimega ei kutsunud. Aristotelese loogikat ning selle edasiarendusi tuntakse ka nime all traditsiooniline loogika. 19. sajandi teisel poolel hakkas arenema kaasaegne loogika, mis tunneb rohkem loogikareegleid kui Aristotelese loogika. Kaasaegset loogikat tuntakse ka nime all matemaatiline loogika.



Aristoteles (u 384 eKr–322 eKr)

Matemaatiline loogika on loogika haru, milles loogikaprobleemide käsitlemiseks kasutatakse matemaatilisi meetodeid. Kirjeldades mingi valdkonna mõisteid ja väiteid, tuuakse sisse formaliseeritud keel, mis on matemaatiliseks uurimiseks piisavalt täpne, ühemõtteline ja lihtne.



Seejuures tehakse vahet keele süntaktilistel aspektidel, mis käsitlevad objekte kui teatavate reeglite järgi koostatud sümbolite järjendeid, ning semantilistel aspektidel, mis annavad süntaktilistele objektidele interpretatsiooni ehk „tähenduse“. Tänapäevaks on matemaatiline loogika jagunenud paljudeks harudeks. Et aga matemaatilises loogikas kasutatavad formaliseeritud keeled on osutunud väga sobivaks programmide koostamise ja analüüsimise juures, siis on kogu valdkonna areng üha tihedamini seotud arvutiteadusega.

Gottfried Wilhelm Leibniz
(1646–1716)

Traditsioonilise loogika aluseks on **mõtlemisseadused**, mida kutsutakse ka loogika aksioomideks. Mõtlemisseadusteks nimetame niisuguseid seadusi, millele peab alluma meie mõtlemine, et ta oleks loogiline ehk tõele vastav. Aristoteles sõnastas kolm mõtlemisseadust: samasuse seaduse, vasturääkivuste lubamatuse seaduse ja välistatud kolmanda seaduse. **G. W. Leibniz** lisas neile neljanda – küllaldase aluse seaduse.

1. **Samasuse seadus** väidab, et iga mõiste või väide peab ühe arutluse kestel jääma samaks. Selle seaduse rikkumine põhjustab asjatuid vaidlusi, mille kohta vanasõnagi ütleb: „Üks räägib aiast ja teine aiaaugust.“ Matemaatikas on oluline jälgida, et mõisted, mida me arutluses kasutame, ei muutuks oma sisult arutluse käigus, vaid me kasutaksime ühte mõistet ainult ühes tähenduses. Võimaluse piires tuleb vältida „igapäeva kõnekeelt“, sest kõnekeelele on omane mitmetähenduslikkus.
2. **Vasturääkivuse lubamatuse seadus** ütleb, et kaks teineteist eitavat lauset ei saa olla tõesed üheaegselt. Näiteks ei saa fikseeritud kordajatega ruutvõrrandi diskriminant olla samaaegselt negatiivne ja mittenegatiivne, või üks ja sama naturaalarv üheaegselt algarv ja kordarv. Kui mingi arutluse tulemusena oleme jõudnud selleni, et kehtivad korraga kaks teineteisele vasturääkivat lauset, siis on ilmselt arutluses tehtud viga. Kui viga on lihtne, siis saame ta hõlpsasti parandada. Kui viga on keerulisem ja peidetud, võib vea tekkepõhjuste uurimine pakkuda tööd matemaatikutele, loogikutele ja filosoofidele aastakümneteks või isegi sajanditeks. Selliseid vigu nimetatakse paradoksideks ehk antinoomiateks ning sofismideks.
3. **Välistatud kolmanda seadus** ütleb, et kahest teineteisele vasturääkivast väitest on üks tõene ja teine väär; kolmandat võimalust ei ole. Seega kaks arvu võivad olla võrdsed või mittevõrdsed; loomad võivad olla selgroolised või selgrootud, mingit kolmandat võimalust olla ei saa (*tetrium non datur*).
4. **Küllaldase aluse seadus** deklareerib, et igal otsustusel ning mõttel peab olema kindel alus, ehk iga väidet on vaja põhjendada mingi teise väitega, mille tõesus on kontrollitud. Näiteks, kui väidame, et trapetsi kesklõik on paralleelne trapetsi alustega ja võrdub aluste poolsummaga, siis tuleb seda väidet põhjendada tõestamise teel.

Matemaatilise loogika aluse moodustavad lausearvutus ja predikaatarvutus. Lausearvutuse eesmärk on uurida lausete omavahelist kombineerumist liitlauseks, näiteks kuidas

tekkinud liitlause tõeväärtus sõltub komponentlausete tõeväärtusest. Predikaatarvutus on lausearvutuse üldistus, kus fikseeritud tõeväärtusega lausete asemel vaadeldakse selliseid lauseid, mille tõeväärtus võib sõltuda argumentide väärtustest (näiteks laused „ $2x + 3 = 11$ ” ja „ x on algarv”).

2.2 Lausearvutuse põhimõisted

Lausearvutuse põhiliseks uuritavaks objektiks on lause, mis võib pärineda ükskõik millisest valdkonnast. Siiski, mitte iga keeleliselt korrektne lause ei ole matemaatilise loogika lause.

Definitsioon 2.1

Matemaatilises loogikas nimetatakse **lauseks** (ingl *proposition*) ainult niisugust väljendit (väidet, kõnekeele lauset), mille korral saab rääkida selle sisu vastavusest või mittevastavusest tegelikkusele.

Kui lause sisu vastab tegelikkusele, siis nimetatakse seda lauset **tõeseks**. Kui aga lause sisu ei vasta tegelikkusele, siis nimetatakse seda lauset **vääraks**. Seega on oluline, et igale lausele saab vastavusse seada tema **tõeväärtuse**, mis kirjeldab lause tegelikkusele vastavuse määra. Eeldame, et

- iga lause on kas tõene või väär (välistatud kolmanda seadus);
- ükski lause ei ole korraga tõene ja väär (mittevasturääkivuse seadus).

Seega vaatleme ainult niisugused lauseid, mis midagi väidavad, kusjuures igal väitel on olemas ühene tõeväärtus.

Näiteks laused „Abruka on üks Eesti saartest” ja „Arv 19 on algarv” on tõesed, aga laused „Hobune on kodulind”, „Kuu on üks suur kollane juustukera” ja „ $25 > 50$ ” on väärad. Lausete „Kas sul on iPad?”, „Tere päevast!” ja „ $x > 0$ ” kohta ei oska me öelda, kas nad on tõesed või väärad (viimasel juhul on tõesuse määramiseks vaja teada muutuja x väärtust arvuliselt). Välistatud kolmanda seaduse nõudel jäävad kõrvale kõik küsilauseid ja paljud hüüdlauseid, samuti kõik käsud ning mõttetud sõnaühendid. Mittevasturääkivuse seadus välistab mitmesugused paradoksid, näiteks „See lause siin on väär” või „Ma valetan praegu”, sest selliste väidete tõeväärtust pole võimalik üheselt määrata.

Kui lause on tõene, siis öeldakse, et selle tõeväärtus on t , ning kui lause on väär, siis selle tõeväärtus on v . Kasutatakse ka tähti t ja f (inglise keeles *true*, *false*) või numbreid 1 ja 0.

Lausearvutuse eesmärk ei ole uurida lausete sisulist tähendust, vaid antud lausetest uute lausete moodustamist. Loogiliste tehete abil saab lausetest moodustada **liitlauseid**. Lauseid, millest liitlause moodustatakse, nimetatakse **komponentlauseteks (lihtlauseteks)**. Liitlause nagu iga komponentlausegi, võib olla kas tõene või väär, kusjuures liitlause tõeväärtus sõltub ainult komponentlausete tõeväärtustest. Liitlausete moodustamiseks tuuakse sisse tähised komponentlausete ja seoste märkimiseks ning pannakse vaadeldav lause kirja sümbolkujul. Komponentlausete tähistamiseks kasutame suuri ladina tähti X , Y , Z

jne, mida nimetame **lausemuutujateks**, grammatilistele seostele aga vastavad lausearvutuse tehted. Kahte lauset, mis on sisu poolest identsed, aga vormilt erinevad, loetakse võrdseteks ja tähistatakse ühe ja sama tähega. Näiteks laused „Täisnurkse kolmnurga kõrgus on selle kolmnurga kaatetite projektsioonide geomeetriline keskmine“ ja „Täisnurkse kolmnurga kõrguse ruut võrdub selle kolmnurga kaatetite projektsioonide korrutisega“ väljendavad üht ja sama tõsiasja, on oma sisult võrdsed ja me võime neid tähistada ühe ja sama tähega. Sisu poolest erinevaid lauseid tähistatakse erinevate tähtedega.

2.3 Predikaadid ja kvantorid

Predikaadid on lausearvutuse lausete üldistused, kus fikseeritud tõeväärtusega lausete asemel vaadeldakse selliseid lauseid, mille tõeväärtus võib sõltuda argumentide väärtustest.

Definitsioon 2.2

Predikaat (ingl *predicate*) on lause, mis sisaldab vähemalt ühte muutujat ja millele saab omistada tõeväärtuse niipea, kui muutuja(te)le on omistatud väärtus(ed).

Näide 2.3. Olgu muutujate hulgaks M naturaalarvude hulk ja predikaadiks $P(n)$: „ n on algarv“, siis kehtib, et $P(1)$ on väär, $P(2)$ on tõene, $P(3)$ on tõene, $P(4)$ on väär jne.

Näide 2.4. Olgu muutujate hulgaks M kõigi Euroopa Liidu riikide hulk ja predikaadiks $R(x, y)$: „Riikidel x ja y on ühine maismaapiir“, siis kehtib, et $R(\text{Eesti}, \text{Läti})$ on tõene ja $R(\text{Saksamaa}, \text{Poola})$ on tõene, aga $R(\text{Rootsi}, \text{Hispaania})$ on väär.

Teine viis, kuidas saada predikaatidest lausearvutuse laused, on lisada nende ette kvantorid. Kui $P(x)$ on predikaat, siis $\exists x, P(x)$.

Paljudes matemaatika lausetes (teoreemides!) esinevad sõnad „kõik,“ „iga,“ „leidub,“ „eksisteerib,“ „on olemas,“ „vähemalt üks.“ Näiteks, „Kõik arvud jaguvad kahega,“ „On olemas lineaarseid funktsioone,“ „Vähemalt üks algarv on paarisarv,“ jne.

Osa neist lausetest on tõesed, osa väärad. Selliste lausete kirjutamisel kasutatakse loogikas kahte märki. Üks neist on **olemasolu kvantor** $\exists$ (loetakse „leidub“), teine **üldisuse kvantor** $\forall$ (loetakse „iga“). Need sümbolid kujutavad endast saksakeelsete sõnade „Existieren“ ja „Alle“ ümberpööratud esitähiti. Kvantori märgi taha tuleb alati kirjutada muutuja, millele see kvantor rakendub.

Kuidas siis neid sümboleid kasutatakse? Näiteks, kirjutusviis $\forall x \in \mathbb{R}, x^2 + 1 > 0$ tähendab iga reaalarvulise x korral on $x^2 + 1$ suurem nullist. Selle lause üldise kuju $\forall x P(x)$ võib kirja panna selliselt: „Mis tahes objekti või indiviidi x korral (antud objektide või indiviidide hulgast) on lause $P(x)$ tõene.“

Kirjutusviis $\exists x, x^3 - 27 = 0$ tähendab „leidub x , mille korral $x^3 - 27 = 0$.“ Üldkujuul siin $\exists x P(x)$ tähistab lauset „leidub x , mille korral kehtib $P(x)$ “ ehk „vähemalt ühel objektil

on omadus P ”. Sõna leiduma ei tähenda siin seda, et leidub üks ja ainult üks objekt, mis rahuldab antud tingimust, vaid et leidub vähemalt üks objekt (s.t võib leiduda ka mitu), mis rahuldavad antud tingimust.

Kui lauses kasutatakse üldisuse kvantorit, siis selle lausega väidetakse midagi kõigi antud liiki objektide kohta ja seetõttu peab neid väiteid tõestama ka üldkujul. Seevastu lause ümberlükkeks piisab ühest kontranäitest. Näiteks, Pierre Fermat’ esitas hüpoteesi, et iga naturaalarvu n korral $2^{2^n} + 1$ on algarv. Hüpotees peab paika $n = 0, 1, 2, 3$ ja 4 korral, aga $n = 5$ korral näitas Leonhard Euler, et saadud arv jagub arvuga 641. Sellega oli hüpotees ümber lükatud.

Kvantoreid $\forall$ ja $\exists$ võib omavahel kombineerida. Näiteks, $\forall x \in \mathbb{R} \exists y \in \mathbb{R}, x < y$ tähistab lauset „iga reaalarvu x korral leidub reaalarv y selliselt, et $x < y$ ”, mille me kõik teame õige olevat. Eelnevas lauses aga kvantorid ära vahetades, saame väärade lause $\exists x \in \mathbb{R} \forall y \in \mathbb{R}, x < y$, mida loetakse „leidub reaalarv x nii, et iga reaalarvu y korral $x < y$ ”. Mõtles viimasele lausele ise kontranäide!

Samuti võib kvantori märgi alla võtta rohkem kui ühe muutuja. Näiteks $\exists x, y, x + y = 5$ tähistab lauset „leiduvad arvud x ja y , mille korral kehtib $x + y = 5$ ”. Vahetades olemasolu kvantori üldisuse kvantori vastu, saame aga vale väite $\forall x, y, x + y = 5$ ehk „kõikide arvude x ja y korral kehtib $x + y = 5$ ”. Sarnaselt võime moodustada laused $\forall x \exists y, x + y = 5$ või $\exists x \forall y, x + y = 5$. Jällegi on üks nendest lausetest tõene (milline?) ja teine väär. Seega üldjuhul laused

$$\forall x \exists y, P(x, y) \text{ ja } \exists x \forall y, P(x, y)$$

ei ole samaväärsed.

2.4 Lausearvutuse tehted

- **Eitus** (ingl *negation*, märk $\neg$) on loogiline tehe, mida rakendatakse ainult ühele lausele. Igapäevakeeles väljendab eitus lause mittekehtimist, näiteks „Sidrun ei ole hapu”. Selle lause võib kirja panna valemiga $\neg A$, kus A = „Sidrun on hapu”.

Lause A **eituseks** nimetatakse lauset $\neg A$, mis on tõene parajasti siis, kui lause A on väär.

- **Konjunktsiooni** (ingl *conjunction*, märk $\wedge$) keeleliseks vasteks on sõnad „ja” või „ning”. Tehtemärgina kasutatakse kirjanduses ka sümbolit $\&$. Näiteks „Puhub tuul ja sajab vihma” on valemkuju kirjutatuna $A \wedge B$, kus A = “Puhub tuul” ning B = “Sajab vihma”. Konjunktsiooni nimetatakse vahel ka loogiliseks korrutiseks.

Lausete A ja B **konjunktsioon** $A \wedge B$ on tõene parajasti siis, kui mõlemad komponendilaused A ja B on tõesed.

- **Disjunktsioon** (ingl *disjunction*, märk $\vee$) väljendab seost „või”. Näiteks „Helen laulab või Mart laulab” on valemkuju $A \vee B$. Sidesõna „või” kasutatakse siin mittevälistavas tähenduses: „Kas A või B või mõlemad”. Igapäevases keeles on käibel ka

välistav „või“: „Kas A või B , aga mitte mõlemad“, näiteks „Ma külvan põllule rukist või panen põllule kartulid“. Disjunktsiooni all mõistame mittevälistavat „või“.

Lausete A ja B **disjunktsioon** $A \vee B$ on tõene parajasti siis, kui vähemalt üks komponentidest A või B on tõene.

- **Implikatsioon** (ingl *implication*, märk $\Rightarrow$) väljendab tingimuslikku konstruktsiooni „kui ..., siis ...“. Näiteks „Kui Sven terve aasta korralikult õpib, siis suudab ta kevadel eksamid hõlpsasti ära teha“ või „Kui kehtib teoreem A , siis kehtib teoreem B “. Mõlemad laused võib kirja panna valemiga $A \Rightarrow B$. Implikatsiooni saab sõnastada mitmel eri viisil. Näiteks:

1. Kui on A , siis on B .
2. Väitest A järelneb B .
3. A on B piisav tingimus.
4. B on A tarvilik tingimus.
5. A on ainult siis, kui on B .

Lausete A ja B **implikatsioon** $A \Rightarrow B$ on tõene parajasti siis, kui A on väär või B on tõene.

NB! Implikatsioon ei ole kommutatiivne tehe. Hoolikalt tuleb jälgida, milline avaldis on kirjutatud märgist $\Rightarrow$ vasakule poole, milline avaldis aga paremale poole.

- **Ekvivalents** (ingl *biconditional*, märk $\Leftrightarrow$) tähendab matemaatikas sagedasti kasutatavat seost „parajasti siis, kui“ ehk „siis ja ainult siis, kui“ ehk „on ekvivalentne sellega et“. Näiteks lause „arv r on ratsionaalarv parajasti siis, kui r esitub kas lõpliku või (lõpmatu) perioodilise kümnendmurruna“ on valemkuju $A \Leftrightarrow B$.

Lausete A ja B **ekvivalents** $A \Leftrightarrow B$ või $A \sim B$ on tõene parajasti siis, kui kas A ja B on mõlemad tõesed või mõlemad väärad.

Kõik toodud tehete definitsioonid saab esitada ühises tabelis:

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$	$\neg A$
t	t	t	t	t	t	v
t	v	v	t	v	v	v
v	t	v	t	t	v	t
v	v	v	v	t	t	t

Lausearvutuse tehete **prioriteetid** võimaldavad vähendada valemities kasutatavate sulgude arvu. Kõige kõrgema prioriteediga on eituse tehe ja kõige madalama prioriteediga ekvivalentsitehe. Teiste tehete prioriteet ehk tugevusjärjekord fikseeritakse nii, et see kahaneb järgmises tehete loetelus vasakult paremale:

$$\neg \wedge \vee \Rightarrow \Leftrightarrow$$

Olles seega piiritlenud lausearvutuse tehted, võime nüüd koostada lihtsamatest lausetest keerulisemaid, ühendades neid omavahel lausearvutuse tehete abil. Näiteks saame moodustada lause

$$((A \Leftrightarrow B) \Rightarrow (A \wedge C)) \vee \neg B.$$

Niisugustes operatsioonides eeldame endiselt järgmiste tingimuste täidetust:

- tehteid võib teostada ükskõik milliste lausetega (sisulist seost nende vahel ei nõuta);
- tehte tulemusena saadud lause tõeväärtus sõltub ainult komponentlausete tõeväärtustest, mitte nende sisust.

Nendest tingimustest järeldub vahetult, et lausetega tehete sooritamisel on oluline mitte lausete sisu, vaid tõeväärtus. Lausearvutuse üks põhilisi ülesandeid ongi liitlause tõeväärtuse leidmine.

Uurime nüüd, kuidas toimub kvantoriga lausete eitamine.

Definitsioon 2.5: Kvantoriga lause eitamise reeglid

1. lause " $\exists x P(x)$ " eitus on " $\forall x \neg P(x)$ ";
2. lause " $\forall x P(x)$ " eitus on " $\exists x \neg P(x)$ ".

Mitme kvantori puhul toimime analoogiliselt. Näiteks, valemi $\forall x \exists y P(x, y)$ eitus on

$$\neg(\forall x \exists y P(x, y))$$

on teise reegli tõttu

$$\exists x \neg(\exists y P(x, y))$$

ja esimese reegli tõttu

$$\exists x \forall y \neg P(x, y).$$

Sarnaselt saame, et valemi $\exists x \forall y P(x, y)$ eitus on $\forall x \exists y \neg P(x, y)$.

Näide 2.6.

1. Olgu antud lause „Mitte kõik naturaalarvud ei ole algarvud.“ Samamoodi on võimalik teine lause ümber sõnastada öeldes „Leidub naturaalarv, mis ei ole algarv“ ehk sümbolites $\exists x \in \mathbb{N}, \neg(x \text{ on algarv})$. Teisisõnu, leidub naturaalarv, mis pole algarv.
2. Olgu antud lause „Leidub reaalarv x selliselt, et $x^2 = 3$.“ Tähistades $P(x) : x^2 = 3$, saame lause kirjutada kujul $\exists x \in \mathbb{R}, P(x)$. See on tõene lause, sest näiteks $x = \sqrt{3}$ rahuldab antud tingimust. Eituseks on lause „Iga reaalarvu x korral $x^2 \neq 3$,“ mis on väär.
3. Vaatame nüüd lauset „Iga kahe reaalarvu x ja y korral $x^2 + y^2 \geq 0$ “ ehk sümbolkujul $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, P(x, y)$, kus $P(x, y)$ tähistab väidet $x^2 + y^2 \geq 0$. See on tõene lause. Tema eitus „Leiduvad reaalarvud x ja y nii, et $x^2 + y^2 < 0$ “ on aga selgelt väär.

4. Lause „Iga positiivse ratsionaalarvu a jaoks leidub positiivne ratsionaalarv b nii, et $ab = 1$ “ on tõene. Moodustame tema eituse: „Leidub positiivne ratsionaalarv a nii, et iga ratsionaalarvu b korral $ab \neq 1$,“ mis on väär. Miks?

Näide 2.7. Lause „Kõikide täisarvude a ja b korral, kui korrutis ab on paarisarv, siis a on paarisarv või b on paarisarv.“ eituse oleks järgmine: „Leiduvad sellised täisarvud a ja b , mille korral ab on paarisarv ja a ning b on mõlemad paaritud arvud.“

Proovi selle näite esialgne lause ja tema eituse kirja panna kvantoreid kasutades.

2.5 Lausearvutuse valemid

Kirjutades laused üles sümbolkujul, saamegi **lausearvutuse valemid**. Kui see on tehtud, siis võime edasise uurimise aluseks võtta valemid ja jätta kõrvale laused, millest need valemid saadi. Täpse eeskirja valemite kirjapanemiseks määrab kindlaks järgmine definitsioon.

Definitsioon 2.8

Lausearvutuse valemid (ingl *propositional formula*) on parajasti need, mida saab koostada järgmiste reeglite abil:

1. iga lausemuutuja on lausearvutuse valem;
2. tõeväärtused t ja v on valemid;
3. kui $\mathcal{F}$ on lausearvutuse valem, siis ka $\neg\mathcal{F}$ on lausearvutuse valem;
4. kui $\mathcal{F}$ ja $\mathcal{G}$ on lausearvutuse valemid, siis ka $\mathcal{F} \wedge \mathcal{G}$, $\mathcal{F} \vee \mathcal{G}$, $\mathcal{F} \Rightarrow \mathcal{G}$ ja $\mathcal{F} \Leftrightarrow \mathcal{G}$ on lausearvutuse valemid;
5. kui $\mathcal{F}$ on lausearvutuse valem, siis ka $(\mathcal{F})$ on lausearvutuse valem.

Näiteks kirjutis $(\mathcal{A} \vee \mathcal{B}) \wedge (\mathcal{C} \Rightarrow \mathcal{D})$ on valem, kui $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ on valemid.

Definitsioonist järeldub, et valem saab sõltuda lõplikult arvust muutujatest ning on antud eeskiri, kuidas lihtsamatest valemitest saab järk-järgult moodustada keerulisemaid. Niisugust tüüpi definitsioonid esinevad loogikas üsna sageli, neid nimetatakse **induktiivseteks**, sest vormi poolest meenutavad nad matemaatilise induktsiooni printsiipi. Tingimused 1) ja 2) kujutavad seejuures induktsiooni baasi, tingimused 3), 4) ja 5) aga induktsiooni sammu (induktsioonist räägime lähemalt paragrahvis 4.2).

Lähtudes lausemuutujatest, saame koostada valemid, mis sisaldavad ühte lausearvutuse tehet; lähtudes lausemuutujatest ja ühe tehtega valemitest, saame koostada kahe tehtega valemid jne. Kõiki antud valemi konstrueerimise käigus tekkinud vameid nimetatakse selle valemi **osavalemiteks**, konstrueerimise viimasel sammul kasutatud tehet aga valemi **peatehteks**. Kui lauses on mitu erinevat loogikatehet, siis tuleb arvestada sulgudega ja tehete järjekorraga (tuleta meelde: kõigepealt eitused, siis konjunktsioonid, siis disjunktsioonid, seejärel implikatsioonid ja ekvivalents). Kui mitme liikme konjunktsioonis või

disjunktsioonis sooritatakse tehteid vasakult paremale, siis võib tehete järjekorda täpsustavatest sulgudest loobuda. Samuti võib valemi välimised sulud ära jätta.

Näide 2.9. Olgu antud valem

$$\left(((X \wedge \neg Y) \wedge (Z \Rightarrow \neg X)) \Leftrightarrow (Y \vee X) \right).$$

Lausemuutujad X, Y, Z on lausearvutuse valemid definitsiooni esimese punkti põhjal. Kolmanda punkti põhjal on lausearvutuse valemid ka näiteks $\neg X$ ja $\neg Y$ ning neljanda punkti põhjal $Y \vee X$. Edasi on lausearvutuse valemid $X \wedge \neg Y$, $Z \Rightarrow \neg X$ ja $(X \wedge \neg Y) \wedge (Z \Rightarrow \neg X)$ ning samuti $((X \wedge \neg Y) \wedge (Z \Rightarrow \neg X)) \Leftrightarrow (Y \vee X)$. Viimase valemi peatehe on $\Leftrightarrow$ ja tema osavalemid on parajasti kõik loetletud valemid.

Näide 2.10. Vaatleme taas valemit

$$\left(((X \wedge \neg Y) \wedge (Z \Rightarrow \neg X)) \Leftrightarrow (Y \vee X) \right).$$

Jättes ära välimised sulud, saame

$$((X \wedge \neg Y) \wedge (Z \Rightarrow \neg X)) \Leftrightarrow (Y \vee X).$$

Tehete prioriteete arvestades võime loobuda sulgudest ümber valemi peatehte kummagi poole:

$$(X \wedge \neg Y) \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$$

Samuti pole tarvis ka esimesi sulge:

$$X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$$

Kokkuvõttes on valem omandanud hoopis ülevaatlikuma kuju.

2.6 Valemi tõeväärtuse leidmine

Iga lausemuutuja võib olla kas tõene või väär. Kui näiteks muutuja X on tõene, siis kirjutame $X = 1$ või $X = t$, vastasel korral, kui muutuja X on väär, kirjutame $X = 0$ või $X = v$. Juhul, kui me omistame tõeväärtuse igale vaatluse all olevale muutujale, siis nimetatakse sellist tõeväärtuste komplekti **muutujate väärtustuseks**. Näiteks muutujakomplekti X, Y, Z üks võimalik väärtustus on $X = 1, Y = 0, Z = 1$ ehk lühemalt $(1, 0, 1)$.

Valemi tõeväärtus määratakse muutujate tõeväärtuste kõikvõimalike kombinatsioonide korral. Seda on otstarbekas teha tabeli kujul, mida nimetatakse valemi **tõeväärtustabeliks**. Valemi tõeväärtuse leidmiseks tuleb muutujad asendada nende tõeväärtustega ning arvestada tehete järjekorda ja loogiliste tehete definitsioone.

Näide 2.11. Koostame näiteks valemi $(\neg X \Rightarrow Y) \vee (X \wedge Y)$ tõeväärtustabeli. Tabeli päisesse kirjutame muutujad X ja Y ning üksikud tehted nõutavas järjekorras. Kahe muutuja korral on 4 võimalikku tõeväärtuste kombinatsiooni. Nendega täidamegi muutujate X ja Y tõeväärtuste veerud ning seejärel täidame tabeli ülejäänud veerud, arvestades vastavaid loogilisi tehteid.

X	Y	$\neg X \Rightarrow Y$	$X \wedge Y$	$(\neg X \Rightarrow Y) \vee (X \wedge Y)$
t	t	t	t	t
t	v	t	v	t
v	t	t	v	t
v	v	v	v	v

Valemi $(\neg X \Rightarrow Y) \vee (X \wedge Y)$ tõeväärtused on tabeli viimases veerus. Näeme, et antud valem on väär vaid ühel juhul, ja nimelt siis, kui mõlemad muutujad on väärad ($X = v$ ja $Y = v$).

Näide 2.12. Leida valemi $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$ tõeväärtus muutujate X, Y, Z väärtustusel $(1, 0, 1)$.

Kõigepealt teame, et $X = 1$, $Y = 0$ ja $Z = 1$. Seega $\neg X = 0$ ja $\neg Y = 1$ ning $Y \vee X = 1$. Edasi leiame analoogilisel viisil, et $X \wedge \neg Y = 1$ ning $Z \Rightarrow \neg X = 0$, mistõttu $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) = 0$. Lõpuks näeme, et $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X = 0$. Vaadeldaval väärtustusel on valem järelikult väär.

Sarnaselt eespool antud tabelile on ka siin tark tegu tehete toimet ülevaatlikumalt kirjeldada tõeväärtustabeliga, mille vasakus osas on valemi argumentide kõikvõimalikud väärtustused, paremas osas aga tehete tulemused. Keerukama valemi tõeväärtustabelis võib kirjutada tehete tulemused iga tehtmärgi alla omaette veergu. Näites 2.12 konstrueeritud valemi tõeväärtustabeliks saame niiviisi

X	Y	Z	$X \wedge \neg Y$	$Z \Rightarrow \neg X$	$Y \vee X$	$X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$
1	1	1	0	0	1	0
1	1	0	0	1	1	0
1	0	1	1	0	1	0
1	0	0	1	1	1	1
0	1	1	0	1	1	0
0	1	0	0	1	1	0
0	0	1	0	1	0	1
0	0	0	0	1	0	1

Tõeväärtustabel on lausearvutuse valemi analüüsimise universaalne meetod. Enamiku ülesannetest, mis puudutavad lausearvutuse valemi tõesust või väärust, saab lahendada tõeväärtustabeliga, kuigi mõnede spetsiaalsete ülesannete lahendamiseks on olemas ka teisi meetodeid. Et aga n muutujaga valemi tõeväärtustabel sisaldab 2^n rida, siis kasvab tõeväärtustabeli maht muutujate arvu suurenedes väga kiiresti (m tehtmärgi korral tuleb teha $2^n \cdot m$ tehet).

2.7 Valemite omadused

Definitsioon 2.13

Lausearvutuse valemid $\mathcal{F}$ nimetatakse **samaselt tõeseks** ehk **tautoloogiaks** (ingl *tautology*), kui ta on igal väärtustusel tõene. Valemid $\mathcal{F}$ nimetatakse **samaselt vääraks** ehk **vastuoluliseks** (ingl *contradiction*), kui ta on igal väärtustusel väär.

Samaselt tõest valemid nimetatakse ka **loogiliselt tõeseks** valemiks ning samaselt väärade valemite **kontradiktsiooniks** või **loogiliselt vääraks** valemiks. Üks samaselt tõene valem on näiteks $X \vee \neg X$, mis väljendab välistatud kolmanda seadust. Mittevasturääkivuse seadust kirjeldab aga samaselt väär valem $X \wedge \neg X$.

Samaselt tõesed valemid väljendavad üldkehtivaid loogikaseadusi ning pakuvad seetõttu loogikas suurt huvi. Asendades niisuguses valemis kõik lausemuutujad mingite lausetega, saame liitlause, mis on alati tõene. Näiteks kui valemis $X \vee \neg X$ võtta $X =$ „Mul on õigus“, siis saame lause „Mul on õigus või mul ei ole õigus“, mis on tõene sõltumata sellest, kas mul õigus on või ei ole.

Et samaselt tõene valem on igas olukorras tõene, olenemata sellest, milline maailm tegelikult on, siis ei sisalda ta informatsiooni ja on seega sisutühi (ta ei ütle maailma kohta midagi). Kui näiteks lause „Homme on ilus ilm või homme ei ole ilus ilm“ esineks ilma teates, siis pole sellest homse ilma kohta võimalik midagi teada saada. Teinekord esineb taolise struktuuriga väiteid igapäevases keeles, näiteks „Seadus võetakse Riigikogus vastu või ei võeta“. Kuigi niisugune väide otsest informatsiooni ei kannu, saab järeldada lause esitamise faktist, et tegemist on mingi seadusega, mille vastuvõtmise suhtes pole kõik saadikud ühel meelel. Selline kaudne tõlgendamine jääb aga väljapoole lausearvutuse piire.

Samaselt väärade valemid esitavad väiteid, mis mingil tingimusel tõesed olla ei saa. Vaatleme näiteks valemid $X \wedge \neg X$ ja valime $X =$ „Homme on ilus ilm“. Saame lause „Homme on ilus ilm ja pole ilus ilm“, mis ei saa olla tõene, sest siis peaks homme ilm olema ühtaegu nii ilus kui ka halb. Seetõttu ka samaselt väärade valemite esinev lause on infotühi.

Üks võimalus valemite samaselt tõesuse kontrollimiseks on kasutada tõeväärtustabelit: valemite tõeväärtuste veerus peab esinema ainult väärtus 1. Et tõeväärtustabel on lõplik, siis saab lausearvutuse valemite samaselt tõesust alati kindlaks teha lõpliku arvu sammudega ehk, algoritmiteooria terminites, lausearvutuse samaselt tõeste valemite hulk on lahenduv. Analooilised märkused kehtivad samaselt väärade valemite kohta.

Näide 2.14. Näidata, et valem $\neg(X \vee Y) \wedge \neg(\neg X \vee \neg Y)$ on samaselt väär. Koostame tõeväärtustabeli:

Et antud valemite tõeväärtuste veerus esinevad ainult väärade väärtused, siis on valem samaselt väär.

Kui kaks valemid ei ole neis esinevate lausemuutujate ühelgi väärtustusel korraga tõesed, siis nimetatakse neid valemite **vasturääkivateks**. Näite 2.14 põhjal võime öelda, et valem

X	Y	$\neg(X \vee Y)$	$\neg(\neg X \vee \neg Y)$	$\neg(X \vee Y) \wedge \neg(\neg X \vee \neg Y)$
1	1	0	1	0
1	0	0	0	0
0	1	0	0	0
0	0	1	0	0

mid $\neg(X \vee Y)$ ja $\neg(\neg X \vee \neg Y)$ on vasturääkivad. Analoogiliselt mõistetakse vasturääkivust kolme, nelja ja enama valemi puhul.

Vaatleme veel kahte valemiklassi.

Definitsioon 2.15

Lausearvutuse valemid $\mathcal{F}$ nimetatakse **kehtestatavaks** (ingl *satisfiable*), kui ta on vähemalt ühel väärtustusel tõene. Valemid $\mathcal{F}$ nimetatakse **kummutatavaks** (ingl *refutable*), kui ta on vähemalt ühe väärtustuse korral väär.

Näiteks valem $\neg(X \vee Y)$ on kehtestatav, sest tema tõeväärtuste veerus esineb 1 (vaata näite 2.14 teise tehte tõeväärtuseid). Otse definitsioonist järeldub, et iga samaselt tõene valem on kehtestatav, sest selline valem on samuti vähemalt ühel väärtustusel tõene.

Sissetoodud valemiklasside vahel kehtivad järgmised seosed.

Lause 2.16

Valem $\mathcal{F}$ on samaselt tõene parajasti siis, kui tema eitus $\neg\mathcal{F}$ on samaselt väär.

Tõestus. Andes valemis $\mathcal{F}$ esinevatele lausemuutujatele suvalise väärtustuse, näeme, et valemite $\mathcal{F}$ ja $\neg\mathcal{F}$ tõeväärtused on vastupidised. Järelikult, kui $\mathcal{F}$ on igal väärtustusel tõene, siis $\neg\mathcal{F}$ on igal väärtustusel väär ja sama kehtib ka ümberpöörduvalt. ■

Lause 2.17

Valem $\mathcal{F}$ on kehtestatav parajasti siis, kui tema eitus $\neg\mathcal{F}$ ei ole samaselt tõene.

Tõestus. Kui $\mathcal{F}$ on kehtestatav, siis väärtustusel, kus $\mathcal{F}$ on tõene, on valem $\neg\mathcal{F}$ väär ja ei saa seetõttu olla samaselt tõene. Ümberpöörduvalt, kui $\neg\mathcal{F}$ ei ole samaselt tõene, siis leidub väärtustus, kus $\neg\mathcal{F}$ on väär ja $\mathcal{F}$ on järelikult tõene. ■

Analoogiat kasutades võime eelmisele kahele lausele lisaks väita, et valem $\mathcal{F}$ on samaselt väär parajasti siis, kui tema eitus $\neg\mathcal{F}$ on samaselt tõene, ning valem $\mathcal{F}$ on kummutatav parajasti siis, kui $\mathcal{F}$ ei ole samaselt tõene. Alati on neid omadusi võimalik kindlaks teha, koostades nende tõeväärtustabelid.

2.8 Järeldumine

Järeldamine ehk arutlus on mõtlemisprotsess, mille käigus ühele või mitmele otsustusele tuginedes jõutakse uue otsustuseni. Järeldamise tulemust nimetatakse **järelduseks**, otsustusi aga, millele tuginetakse – **eeldusteks**. Kui kõik eeldused on tõesed ning deduktiivne järeldus on õigesti tehtud, siis on ka järeldus tõene. Seega, loogika reeglite abil uute väidete tuletamine on ühtlasi nende väidete tõestamine. Meie uurime käesolevalt küsimust, millal on lausearvutuse valem tõene, kui mingite teiste lausearvutuse valemite tõesus on teada. Näitena vaatame kolme lauset:

1. Kui täna on 16. september, siis homme on 17. september.
2. Täna on 16. september.
3. Homme on 17. september.

Võime öelda, et lause 3 järeldub lausetest 1 ja 2. Samuti, olles õppinud, et lause ja tema pöördvastandlause on loogiliselt samaväärsed, võime väita, et lausest „Kui vihma sajab, siis katused on märjad“ järeldub „Kui katused ei ole märjad, siis vihma ei saja“.

Definitsioon 2.18

Öeldakse, et valemitest $\mathcal{F}_1, \dots, \mathcal{F}_n$ **järeldub** (ingl *derive*) valem $\mathcal{G}$, kui igal neis valemis esinevate muutujate väärtustusel, millel $\mathcal{F}_1, \dots, \mathcal{F}_n$ on tõesed, on ka $\mathcal{G}$ tõene.

Asjaolu, et valemitest $\mathcal{F}_1, \dots, \mathcal{F}_n$ järeldub valem $\mathcal{G}$, tähistatakse sümbolites nii:

$$\mathcal{F}_1, \dots, \mathcal{F}_n \models \mathcal{G},$$

kus sümbolit $\models$ loetakse sõnaga „järeldub.“

Eeldused on alati vasakul pool sümbolit $\models$. Kui vasakul on komadega eraldatud mitu valem, siis on mitu eeldust. Paremal pool $\models$ sümbolit on järeldus. Mõnikord kasutatakse sõna järeldus ka tähenduses järeldamine.

Järeldumist saab kindlaks teha tõeväärtustabeli abil. Valime tõeväärtustabelist välja read, milles valemid $\mathcal{F}_1, \dots, \mathcal{F}_n$ on kõik tõesed, ja selgitame, kas nendes ridades on ka valem $\mathcal{G}$ tõene. Kui on, siis järeldumine kehtib; kui aga leidub rida, milles valemid $\mathcal{F}_1, \dots, \mathcal{F}_n$ on tõesed, kuid valem $\mathcal{G}$ on väär, siis oleme leidnud väärtustuse, mis väidetava järeldumise ümber lükkab.

Näide 2.19. Teha kindlaks, kas valemitest $\neg(X \wedge Y)$ ja $Y \Rightarrow X$ järeldub valem $\neg Y$. Koostame tõeväärtustabeli:

Kaks esimest valem, on mõlemad tõesed ainult teises ja neljandas reas. Et ka kolmas valem on nendes ridades tõene, siis järeldumine leiab aset ehk $\neg(X \wedge Y), Y \Rightarrow X \models \neg Y$.

Näide 2.20. Näidata, et valemist $X \Rightarrow Y$ ja $Y \Rightarrow Z$ järeldub valem $X \Rightarrow Z$.

Seekord me tõeväärtustabelit välja ei kirjuta, vaid kontrollime järeldumise tõesust arutluse teel. Kõigepealt märkame, et ainukene olukord, kus kahest esimesest valemist kolmandat

X	Y	$\neg(X \wedge Y)$	$Y \Rightarrow X$	$\neg Y$
1	1	0	1	0
1	0	1	1	1
0	1	1	0	0
0	0	1	1	1

valemit järelduda ei saa on siis, kui mingil väärtustusel eeldused (st kaks esimest valemit) on tõesed, kuid väide (st kolmas valem) on väär. Teiste sõnadega, nii $X \Rightarrow Y$ on tõene, kui ka $Y \Rightarrow Z$ on tõene, kuid $X \Rightarrow Z$ on väär. Tuletades meelde, et implikatsioon saab väär olla ainult siis, kui eeldus on tõene ja väide väär, peab meie juhul järelikult kehtima, et X on tõene ja Z on väär. Esimese valemi $X \Rightarrow Y$ tõesusest järeldub seega, et Y peab olema tõene, kuid teine valem $Y \Rightarrow Z$ ei saa nüüd enam tõene olla, sest Y on tõene ja Z on väär.

Näide 2.21. Olgu antud lausemuutujad, mille tähendus on järgmine: X = „Kiiruste liitmiseseadus kehtib“, Y = „Valgus liigub kinnistähedega seotud taustsüsteemis kõigis suundades sama kiirusega“ ning Z = „Valgus liigub Maal kõigis suundades sama kiirusega“. Kehtib valem $X \wedge Y \Rightarrow \neg Z$ ehk tekstikujul „Kui kiiruste liitmiseseadus kehtib ja valgus liigub kinnistähedega seotud taustsüsteemis kõigis suundades sama kiirusega, siis pole Maal valguse liikumiskiirus kõigis suundades sama“, sest Maa ilmselt liigub kinnistähedega seotud taustsüsteemi suhtes. Peale selle kehtib valem Y , sest see on Einsteini relatiivsusteooria põhipostulaat, ja valem Z , sest see järeldub Michelson–Morley katsest (1887). Vaatleme niisiis kolme valemit

$$X \wedge Y \Rightarrow \neg Z, \quad Y \quad \text{ja} \quad Z.$$

Eeldame, et kõik need valemid on tõesed. Kuna Z on tõene, siis $\neg Z$ on väär ning esimeses valemis implikatsiooni tõesuse kehtimiseks peab osavalem $X \wedge Y$ olema väär. Et aga Y on tõene, siis peab X olema väär ja seega $\neg X$ tõene. Sellega oleme näidanud, et toodud kolmest valemist järeldub valem $\neg X$ ehk sõnades „Kiiruste liitmiseseadus ei kehti“.

Näide 2.22. Kontrollida, et kehtivad järgmised (kõige lihtsamad) lauseloogika järeldused:

1. *Modus ponens* (ld jaatav moodus): $X \Rightarrow Y, X \models Y$,
2. *Modus tollens* (ld eitav moodus): $X \Rightarrow Y, \neg Y \models \neg X$.

Toome veel ühe näite lausearvutuse vahendite kasutamisest arutluse õigsuse kontrollimisel.

Näide 2.23. Kontrollige, kas järgmine arutlus on õige.

Kui inimene on andekas ja auahne, siis ta teeb karjääri. Järelikult: kui inimene on auahne, kuid karjääri ei tee, siis ta ei ole andekas.

Olgu antud lausemuutujad, mille tähendus on järgmine: A = „Inimene on andekas“, B = „Inimene on auahne“ ja C = „Inimene teeb karjääri“. Kõigepealt paneme antud arutluse kirja loogiliste valemite abil:

$$A \wedge B \Rightarrow C \models B \wedge \neg C \Rightarrow \neg A.$$

Antud arutlus on õige siis, kui selline järeldus kehtib. Kuna ka paremal pool $\models$ märki on implikatsioon, alustame tegelikult kahe eeldusega: $A \wedge B \Rightarrow C$ ja $B \wedge \neg C$, ning eesmärgiks on näidata, et nendest järeldub $\neg A$. Oletame taas vastuväiteliselt, et antud arutelu andekuse ja auahnuse kohta on väär. See saab juhtuda vaid siis, kui eeldused on tõesed ja järeldus $\neg A$ on väär. Sellest järelduvalt peab A olema tõene. Teisest eelduse valemist saame, et kuna $B \wedge \neg C$ on tõene, siis peab B olema tõene ning ka $\neg C$ olema tõene, ehk C peab olema väär. Nüüd saime aga vastuolu eelduse esimese valemiga $A \wedge B \Rightarrow C$, sest see ei saa leitud A, B ja C väärtustel enam tõene olla. Seega arutlus on õige ja järeldumine leiab aset.

Teine võimalus järeldumist kindlaks teha on kasutada alljärgnevat teoreemi, mis taandab järeldumise kontrollimise üheainsa valemi samaselt tõesuse kontrollimisele. Niisugust lähenemist kasutatakse eriti siis, kui valemit analüüsitakse arvutil, sest lausearvutuse standardülesannete, nagu samaselt tõesuse kontroll, lahendamiseks on koostatud hulgaliselt tavalisi ja heuristilisi efektiivseid algoritme.

Teoreem 2.24

Valemitest $\mathcal{F}_1, \dots, \mathcal{F}_n$ järeldub valem $\mathcal{G}$ parajasti siis, kui valem $\mathcal{F}_1 \wedge \dots \wedge \mathcal{F}_n \Rightarrow \mathcal{G}$ on samaselt tõene.

Tõestus. Kui valemitest $\mathcal{F}_1, \dots, \mathcal{F}_n$ järeldub valem $\mathcal{G}$, siis neil väärtustustel, millel valemid $\mathcal{F}_1, \dots, \mathcal{F}_n$ on tõesed, on ka valem $\mathcal{G}$ tõene, mistõttu $\mathcal{F}_1 \wedge \dots \wedge \mathcal{F}_n \Rightarrow \mathcal{G}$ on tõene. Väärtustustel, millel mõni valemitest $\mathcal{F}_1, \dots, \mathcal{F}_n$ on väär, on valem $\mathcal{F}_1 \wedge \dots \wedge \mathcal{F}_n \Rightarrow \mathcal{G}$ tõene seetõttu, et implikatsiooni eesliige on väär.

Ümberpöörduvalt, kui valem $\mathcal{F}_1 \wedge \dots \wedge \mathcal{F}_n \Rightarrow \mathcal{G}$ on samaselt tõene, siis igal väärtustustel, millel valemid $\mathcal{F}_1, \dots, \mathcal{F}_n$ on tõesed, on ka $\mathcal{F}_1 \wedge \dots \wedge \mathcal{F}_n$ tõene, mistõttu valem $\mathcal{G}$ on samuti tõene. ■

Näide 2.25. Kordame uuesti näites 2.19 toodud ülesannet, kus pidi kindlaks tegema, kas valemitest $\neg(X \wedge Y)$ ja $Y \Rightarrow X$ järeldub valem $\neg Y$. Kasutades teoreemi 2.24, kontrollime seega, kas valem

$$\neg(X \wedge Y) \wedge (Y \Rightarrow X) \Rightarrow \neg Y$$

on samaselt tõene. Selleks koostame vastava tõeväärtustabeli:

X	Y	$\neg(X \wedge Y)$	$Y \Rightarrow X$	$\neg(X \wedge Y) \wedge (Y \Rightarrow X)$	$\neg(X \wedge Y) \wedge (Y \Rightarrow X) \Rightarrow \neg Y$
1	1	0	1	0	1
1	0	1	1	1	1
0	1	1	0	0	1
0	0	1	1	1	1

Viimasest implikatsiooni veerust näeme, et valem on samaselt tõene ja seega järeldus kehtib. Sarnaselt saab teistes näidetes antud järeldumist kontrollida vastavate valemite samaselt tõesust näidates. Proovi sama teha!

2.9 Samaväärsus

Koostades valemite $\neg(X \wedge Y)$ ja $\neg X \vee \neg Y$ tõeväärtustabelid, näeme, et valemite tõeväärtusveerud langevad kokku:

X	Y	$\neg(X \wedge Y)$	$\neg X \vee \neg Y$
1	1	0	0
1	0	1	1
0	1	1	1
0	0	1	1

Igapäevase keele abil on lihtne veenduda, et need valemid väljendavad ühte ja sama: esimene valem tähendab „Pole nii, et laused X ja Y on mõlemad tõesed“ ning teine valem „Vähemalt üks lausetest X või Y on väär“. Ühesuguse tõeväärtusveeruga valemid ei ole võimalik nende komponentlausete sisu järgi teineteisest eristada, ehkki neil võib olla erinev väliskuju. Niisugustest kaalutlustest lähtudes anname järgmise definitsiooni.

Definitsioon 2.26

Valemeid $\mathcal{F}$ ja $\mathcal{G}$ nimetatakse **loogiliselt samaväärseteks** (ingl *logically equivalent*), kui nende tõeväärtused on võrdsed igal neis valemis esinevate muutujate väärtustusel.

Asjaolu, et valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed, märgib kirjutis $\mathcal{F} \equiv \mathcal{G}$.

Näide 2.27. Näitame, et valemid $\neg(X \vee Y)$ ja $\neg X \wedge \neg Y$ on samaväärsed. Selleks võrdleme nende tõeväärtusi kasutades tõeväärtustabelit:

X	Y	$\neg(X \vee Y)$	$\neg X \wedge \neg Y$
1	1	0	0
1	0	0	0
0	1	0	0
0	0	1	1

Seega näeme, et kehtivad samaväärsused $\neg(X \wedge Y) \equiv \neg X \vee \neg Y$ ja $\neg(X \vee Y) \equiv \neg X \wedge \neg Y$. Neid samaväärsusi nimetatakse **De Morgani seadusteks**.

Samaväärsed võivad olla ka erinevaid muutujaid sisaldavad valemid. Näiteks, kui

$$\mathcal{F} = (Y \Rightarrow X) \wedge (\neg Y \Rightarrow X) \text{ ja } \mathcal{G} = (X \vee Z) \wedge (X \vee \neg Z),$$

siis $\mathcal{F} \equiv \mathcal{G}$ (kontrolli!). Kõik samaselt tõesed valemid on üksteisega samaväärsed, sest sellised valemid on igal väärtustusel tõesed. Analoogilisel põhjusel on omavahel samaväärsed kõik samaselt väärad valemid.

Loogiliselt samaväärsete valemitega esitatud väiteid võib teatud piires pidada sama mõtte või tähendusega väideteks, sest ükskõik, milline maailm ka poleks, kui üks neist väidetest

on tõene, on seda paratamatult ka teine ning vastupidi.

Järgmine teoreem näitab, et samaväärsete valemite puhul järeldub esimesest valemist teine ja teisest esimene, st järeldus on mõlemapidine.

Teoreem 2.28

Valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed parajasti siis, kui valemist $\mathcal{F}$ järeldub valem $\mathcal{G}$ ja valemist $\mathcal{G}$ järeldub valem $\mathcal{F}$.

Tõestus. Kui $\mathcal{F} \equiv \mathcal{G}$, siis suvalisel valemites $\mathcal{F}$ ja $\mathcal{G}$ esinevate lausemuutujate väärtustusel on need valemid kas mõlemad tõesed või mõlemad väärad. Seepärast kehtivad järeldused $\mathcal{F} \models \mathcal{G}$ ja $\mathcal{G} \models \mathcal{F}$.

Ümberpöörduvalt, kui $\mathcal{F} \models \mathcal{G}$ ja $\mathcal{G} \models \mathcal{F}$, siis ei saa leida väärtustust, kus $\mathcal{F}$ ja $\mathcal{G}$ tõeväärtused oleksid erinevad, mistõttu $\mathcal{F} \equiv \mathcal{G}$.

Seega, valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed parajasti siis, kui valemist $\mathcal{F}$ järeldub valem $\mathcal{G}$ ja valemist $\mathcal{G}$ järeldub valem $\mathcal{F}$. ■

Kahe valemi samaväärsuse kontrolli saab samuti taandada ühe valemi samaselt tõesuse kontrollile, nii nagu nägime järeldumise puhul.

Teoreem 2.29

Valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed parajasti siis, kui valem $\mathcal{F} \Leftrightarrow \mathcal{G}$ on samaselt tõene.

Tõestus. Eeldame, et valemid $\mathcal{F}$ ja $\mathcal{G}$ on samaväärsed. Valime valemites $\mathcal{F}$ ja $\mathcal{G}$ esinevatele muutujatele suvalise väärtustuse. Kui valitud väärtustusel valem $\mathcal{F}$ on tõene ja valem $\mathcal{G}$ on tõene, siis $\mathcal{F} \Leftrightarrow \mathcal{G}$ on samuti tõene, kui aga valitud väärtustusel valem $\mathcal{F}$ on väär ja valem $\mathcal{G}$ on väär, siis jällegi $\mathcal{F} \Leftrightarrow \mathcal{G}$ on tõene. Järelikult on valem $\mathcal{F} \Leftrightarrow \mathcal{G}$ tõene sõltumata väärtustusest ehk samaselt tõene.

Eeldame nüüd ümberpöörduvalt, et valem $\mathcal{F} \Leftrightarrow \mathcal{G}$ on samaselt tõene. Valime selles valemis esinevatele muutujatele suvalise väärtustuse. Et ekvivalents on tõene, siis kas $\mathcal{F}$ ja $\mathcal{G}$ on mõlemad tõesed või $\mathcal{F}$ ja $\mathcal{G}$ on mõlemad väärad. See tähendab, valemite $\mathcal{F}$ ja $\mathcal{G}$ tõeväärtused on suvalisel väärtustusel samad. Vastavalt definitsioonile on valemid $\mathcal{F}$ ja $\mathcal{G}$ samaväärsed. ■

On olemas hulk **lausearvutuse põhisamaväärsusi**, mida kasutatakse lausearvutuses teistest rohkem. Need on järgmised:

1. Idempotentsuse omadused:

- a) $\mathcal{F} \wedge \mathcal{F} \equiv \mathcal{F}$,
- b) $\mathcal{F} \vee \mathcal{F} \equiv \mathcal{F}$.

2. Kommutatiivsuse omadused:

- a) $\mathcal{F} \wedge \mathcal{G} \equiv \mathcal{G} \wedge \mathcal{F}$,
- b) $\mathcal{F} \vee \mathcal{G} \equiv \mathcal{G} \vee \mathcal{F}$.

3. Assotsiatiivsuse omadused:

a) $(\mathcal{F} \wedge \mathcal{G}) \wedge \mathcal{H} \equiv \mathcal{F} \wedge (\mathcal{G} \wedge \mathcal{H}),$

b) $(\mathcal{F} \vee \mathcal{G}) \vee \mathcal{H} \equiv \mathcal{F} \vee (\mathcal{G} \vee \mathcal{H}).$

4. Distributiivsuse omadused:

a) $\mathcal{F} \wedge (\mathcal{G} \vee \mathcal{H}) \equiv \mathcal{F} \wedge \mathcal{G} \vee \mathcal{F} \wedge \mathcal{H},$

b) $\mathcal{F} \vee (\mathcal{G} \wedge \mathcal{H}) \equiv (\mathcal{F} \vee \mathcal{G}) \wedge (\mathcal{F} \vee \mathcal{H}).$

5. Neelamisomadused:

a) $\mathcal{F} \wedge (\mathcal{F} \vee \mathcal{G}) \equiv \mathcal{F},$

b) $\mathcal{F} \vee \mathcal{F} \wedge \mathcal{G} \equiv \mathcal{F}.$

6. De Morgani seadused (duaalsus):

a) $\neg(\mathcal{F} \wedge \mathcal{G}) \equiv \neg\mathcal{F} \vee \neg\mathcal{G},$

b) $\neg(\mathcal{F} \vee \mathcal{G}) \equiv \neg\mathcal{F} \wedge \neg\mathcal{G}.$

7. Kahekordse eituse omadus: $\neg\neg\mathcal{F} \equiv \mathcal{F}.$ **8. Liikmete elimineerimise reeglid,** kus t on suvaline samaselt tõene valem ja v on suvaline samaselt väär valem:

a) $\mathcal{F} \wedge t \equiv \mathcal{F},$

b) $\mathcal{F} \vee t \equiv t,$

c) $\mathcal{F} \wedge v \equiv v,$

d) $\mathcal{F} \vee v \equiv \mathcal{F}.$

9. Implikatsiooni avaldis konjunktsiooni ja disjunktsiooni kaudu:

a) $\mathcal{F} \Rightarrow \mathcal{G} \equiv \neg(\mathcal{F} \wedge \neg\mathcal{G}),$

b) $\mathcal{F} \Rightarrow \mathcal{G} \equiv \neg\mathcal{F} \vee \mathcal{G}.$

10. Konjunktsiooni ja disjunktsiooni avaldis implikatsiooni kaudu:

a) $\mathcal{F} \wedge \mathcal{G} \equiv \neg(\mathcal{F} \Rightarrow \neg\mathcal{G}),$

b) $\mathcal{F} \vee \mathcal{G} \equiv \neg\mathcal{F} \Rightarrow \mathcal{G}.$

11. Ekvivalentsi avaldis teiste tehete kaudu:

a) $\mathcal{F} \Leftrightarrow \mathcal{G} \equiv \mathcal{F} \wedge \mathcal{G} \vee \neg\mathcal{F} \wedge \neg\mathcal{G},$

b) $\mathcal{F} \Leftrightarrow \mathcal{G} \equiv (\mathcal{F} \Rightarrow \mathcal{G}) \wedge (\mathcal{G} \Rightarrow \mathcal{F}).$

Kõiki neid samaväärsusi saab kontrollida tõeväärtustabeli abil.

Näide 2.30. Samaväärsus 9. b) $\mathcal{F} \Rightarrow \mathcal{G} \equiv \neg\mathcal{F} \vee \mathcal{G}$ tuleneb järgmisest tabelist:

Kuid nende samaväärsuste kehtivust võib tõestada ka otsese arutlemise teel.

$\mathcal{F}$	$\mathcal{G}$	$\mathcal{F} \Rightarrow \mathcal{G}$	$\neg \mathcal{F} \vee \mathcal{G}$
1	1	1	1
1	0	0	0
0	1	1	1
0	0	1	1

Näide 2.31. Tõestame näiteks esimese distributiivsuse seadustest $\mathcal{F} \wedge (\mathcal{G} \vee \mathcal{H}) \equiv \mathcal{F} \wedge \mathcal{G} \vee \mathcal{F} \wedge \mathcal{H}$ (punktis 4).

Tõestus. Kui $\mathcal{F} \wedge (\mathcal{G} \vee \mathcal{H})$ on tõene, siis see on nii ainult siis, kui $\mathcal{F}$ on tõene ja $\mathcal{G} \vee \mathcal{H}$ on tõene. Kui viimases seoses $\mathcal{G}$ on tõene, siis ka $\mathcal{F} \wedge \mathcal{G}$ on tõene. Kui aga $\mathcal{H}$ on tõene, siis on ka $\mathcal{F} \wedge \mathcal{H}$ tõene. Mõlemal juhul on tõestatava samaväärsuse parempoolne valem tõene, sest disjunktsioon on tõene, kui üks komponentidest on tõene.

Ümberpöörduvalt, olgu $\mathcal{F} \wedge \mathcal{G} \vee \mathcal{F} \wedge \mathcal{H}$ tõene. Kui $\mathcal{F} \wedge \mathcal{G}$ on tõene, siis $\mathcal{F}$ ja $\mathcal{G}$ on mõlemad tõesed, millest järelneb, et ka $\mathcal{G} \vee \mathcal{H}$ on tõene. Seetõttu on vasakpoolne valem tõene. Kui aga $\mathcal{F} \wedge \mathcal{H}$ on tõene, siis $\mathcal{F}$ ja $\mathcal{H}$ on mõlemad tõesed, millest omakorda järelneb, et $\mathcal{G} \vee \mathcal{H}$ on tõene. Ka sel juhul on vasakpoolne valem tõene. Niisiis oleme näidanud, et vasakpoolsest valemist järelneb parempoolne ning parempoolsest vasakpoolne. See tähendab, et need valemid on samaväärsed. ■

Et konjunktsiooni, disjunktsiooni ja ekvivalentsi tõeväärtus ei muutu komponentlausete järjekorra muutmisel, siis on need loogilised tehted kommutatiivsed. Implikatsioon aga ei ole kommutatiivne. Seepärast tuleb implikatsiooni korral silmas pidada komponentlausete järjekorda.

Samaväärsused 9. – 11. näitavad, et osa loogilisi tehteid on samaväärsed teiste loogiliste tehete kombinatsioonidega.

2.10 Valemite teisendamine

Samaväärsused etendavad lausearvutuses samasugust rolli nagu samasused algebras. Nii nagu algebras kasutatakse samasusi avaldiste lihtsustamiseks, nii võib ka lausearvutuse valemid teisendada ja lihtsustada lausearvutuse samaväärsustega, kusjuures tekkiv valem jääb igal sammul samaväärseks esialgsega. Üks teisendussamm tähendab valemiga enda või tema osavalemi asendamist teise, samaväärse valemiga. Kui asendame valemis $\mathcal{F}$ mingi osavalemi $\mathcal{F}_1$ samaväärse valemiga $\mathcal{F}_2$, siis tulemuseks saadav valem ja valem $\mathcal{F}$ on igal väärtustusel ühesuguse tõeväärtusega, sest uus osavalem $\mathcal{F}_2$ annab igal väärtustusel sama tõeväärtuse nagu osavalem $\mathcal{F}_1$.

Tavaliselt on teisendamisel otstarbekas elimineerida kõik tehted peale eituse, konjunktsiooni ja disjunktsiooni, sest nende tehete vahel kehtivad kõige lihtsamad seosed. Mõnikord on parem enne tehete elimineerimist teisendada antud valemis mingit osavalemit.

Teoreem 2.32

Iga lausearvutuse valemi $\mathcal{F}$ jaoks leidub temaga loogiliselt samaväärne valem, mis ei sisalda loogilisi tehteid $\Rightarrow$ ja $\Leftrightarrow$.

Tõestus. Teoreem järeldub eelpool toodud arutelust ja põhisamaväärsustest 9. ja 11. ■

Näide 2.33. Teisenda valemit $\neg X \vee Y \Rightarrow X \wedge Y$.

Lahendus. Tähistame $\mathcal{F} = \neg X \vee Y \Rightarrow X \wedge Y$. Avaldades vaadeldavas valemis implikatsiooni eituse ja disjunktsiooni kaudu (9b), saame $\mathcal{F} \equiv \neg(\neg X \vee Y) \vee (X \wedge Y)$. De Morgani omaduse (6b) abil viime eituse sulgude sisse: $\mathcal{F} \equiv (\neg\neg X \wedge \neg Y) \vee (X \wedge Y)$. Kahekordse eituse ning tegelikult mittevajalikud sulud võime ära jätta: $\mathcal{F} \equiv X \wedge \neg Y \vee X \wedge Y$. Nüüd võime rakendada distributiivsuse omadust (4a) ja tuua muutuja X sulgude ette: $\mathcal{F} \equiv X \wedge (\neg Y \vee Y)$. Viimases valemis on liige $\neg Y \vee Y$ samaselt tõene ning me võime ta liikmete elimineerimise reegli (8a) põhjal välja jätta. Kokkuvõttes saame $\mathcal{F} \equiv X$. ■

Näide 2.34. Avalda $\neg(X \Leftrightarrow Y)$ eituse, disjunktsiooni ja konjunktsiooni abil.

Lahendus.

$$\begin{aligned}\neg(X \Leftrightarrow Y) &\equiv \neg((X \Rightarrow Y) \wedge (Y \Rightarrow X)) \\ &\equiv (\neg(X \Rightarrow Y)) \vee (\neg(Y \Rightarrow X)) \\ &\equiv (X \wedge \neg Y) \vee (Y \wedge \neg X).\end{aligned}$$

■

Näide 2.35. Teisenda valem $(X \Rightarrow (Y \Rightarrow Z)) \Leftrightarrow \neg(Y \Rightarrow X)$ selle valemiga loogiliselt samaväärseks valemiks nii, et saadud valemis puuduvad loogilised tehted $\Leftrightarrow$ ja $\Rightarrow$.

Lahendus.

$$\begin{aligned}(X \Rightarrow (Y \Rightarrow Z)) \Leftrightarrow \neg(Y \Rightarrow X) &\equiv (X \Rightarrow (\neg Y \vee Z)) \Leftrightarrow (\neg(\neg Y \vee X)) \\ &\equiv (\neg X \vee (\neg Y \vee Z)) \Leftrightarrow \neg(\neg Y \vee X) \\ &\equiv ((\neg X \vee (\neg Y \vee Z)) \wedge \neg(\neg Y \vee X)) \vee (\neg(\neg X \vee (\neg Y \vee Z)) \wedge \neg\neg(\neg Y \vee X)) \\ &\equiv ((\neg X \vee (\neg Y \vee Z)) \wedge (\neg X \wedge Y)) \vee ((X \wedge (Y \wedge \neg Z)) \wedge (\neg Y \vee X)) \\ &\equiv (\neg X \vee \neg Y \vee Z) \wedge (\neg X \wedge Y) \vee (X \wedge Y \wedge \neg Z \wedge (\neg Y \vee X)).\end{aligned}$$

■

Lisaks võime konkreetsemalt väita järgmist.

Lause 2.36

Iga valemi korral leidub temaga samaväärne valem, mis sisaldab ainult järgmisi tehteid:

- a) $\wedge$ ja $\neg$,
- b) $\vee$ ja $\neg$,
- c) $\Rightarrow$ ja $\neg$.

Tõestus.

- a) Esimese väite põhjendamisel kasutame samaväärsusi (9a), (11a) ja samaväärsusest (6) saadavat $X \vee Y \equiv \neg(\neg X \wedge \neg Y)$.
- b) Teise väite põhjendamisel kasutame samaväärsusi (9b), (11a) ja samaväärsusest (6) saadavat $X \wedge Y \equiv \neg(\neg X \vee \neg Y)$.
- c) Kolmanda väite põhjendamisel kasutame samaväärsusi (11b), (10a) ja (10b).

■

2.11 Täielik disjunktiiivne normaalkuju

Normaalkuju mõte on kahandada lausearvutuse valemite süntaktilist mitmekesisust, andes neile lihtsa väliskujuga ühtse vormi. Lisaks sellele on täielike normaalkujude puhul lihtne välja lugeda väärtustused, millal need valemid on tõesed.

Definitsioon 2.37

Lihtkonjunktsiooniks ehk **elementaarkonjunktsiooniks** (ingl *conjunction of literals*) nimetatakse muutujate või nende eituste konjunktsiooni.

Lihtkonjunktsioonid on näiteks $X \wedge Y$, $\neg X \wedge \neg Y$, X , $X \wedge \neg Y \wedge Z$, $X \wedge Y \wedge \neg Y$.

Definitsioon 2.38

Lihtkonjunktsiooni nimetatakse **täielikuks** (ingl *full*), kui vaadeldavatest muutujatest igaüks esineb täpselt ühe korra.

Pane tähele, et täielikkus sõltub siin vaadeldavate muutujate hulgast. Kui vaadeldakse muutujaid X, Y, Z , siis eelmistest näidetest on täielik lihtkonjunktsioon vaid $X \wedge \neg Y \wedge Z$.

Definitsioon 2.39

Lausearvutuse valemi $\mathcal{F}$ **disjunktiiivseks normaalkujuks** (ingl *disjunctive normal form*) nimetatakse valemiga $\mathcal{F}$ samaväärset valemite, mis kujutab endast erinevate lihtkonjunktsioonide disjunkttsiooni.

Ühel valemil võib olla ka rohkem kui üks disjunktiiivne normaalkuju.

Näide 2.40. Olgu $\mathcal{F} = X \Rightarrow Y$. Põhisamaväärsuste tõttu teame, et valemiga $\mathcal{F}$ samaväärne valem on $\neg X \vee Y$. Kuid ka $X \wedge Y \vee \neg X \wedge Y \vee \neg X \wedge \neg Y$ on valemiga $\mathcal{F}$ samaväärne (kontrolli tõeväärtustabeli abil!).

Definitsioon 2.41

Lausearvutuse valemi $\mathcal{F}$ **täielikuks disjunktiiivseks normaalkujuks** (ingl *full disjunctive normal form*) nimetatakse valemiga $\mathcal{F}$ samaväärset valemite, mis kujutab endast erinevate täielike lihtkonjunktsioonide disjunkttsiooni.

Märkus 2.42

Sarnaselt täieliku disjunktiiivse normaalkujuga saab defineerida ka täieliku konjunktiiivse normaalkuju, mis kujutab endast erinevate täielike lihtdisjunktsioonide konjunktsiooni.

Näide 2.43. Näite 2.40 põhjal on valemi $\mathcal{F} = X \Rightarrow Y$ täielik disjunktiiivne normaalkuju vaid $X \wedge Y \vee \neg X \wedge Y \vee \neg X \wedge \neg Y$. Valemiga $\mathcal{F}$ samaväärne valem $\neg X \vee Y$ ei ole täielikul disjunktiiivsel kujul, sest ta ei koosne täielikest lihtkonjunktsioonidest.

Võtame nüüd käsile normaalkujude tõesuse küsimuse. Täieliku normaalkuju hea omadus ja põhjus, miks teda üldse kasutatakse, seisneb selles, et tema puhul on kerge kindlaks teha, millistel väärtustustel on ta tõene ja millistel väär.

Järgnevates formaalsetes kirjutistes kasutame tähistust $X^t = X$ ja $X^v = \neg X$, samuti üldtähistena X^α , kus $\alpha = t$ või $\alpha = v$. On kerge veenduda, et $X^\alpha = t \Leftrightarrow X = \alpha$ (kontrolli!).

Lause 2.44

Täielike lihtkonjunktsioonide disjunktsioon

$$X_1^{\alpha_{11}} \wedge \dots \wedge X_n^{\alpha_{1n}} \vee X_1^{\alpha_{21}} \wedge \dots \wedge X_n^{\alpha_{2n}} \vee \dots \vee X_1^{\alpha_{m1}} \wedge \dots \wedge X_n^{\alpha_{mn}}$$

on tõene parajasti väärtustustel $(\alpha_{i1}, \dots, \alpha_{in})$, kus $i = 1, \dots, m$.

Näide 2.45. Valem $X \wedge Y \vee \neg X \wedge \neg Y$ on täielikul disjunktiiivsel normaalkujul. See valem on tõene väärtustustel (t, t) ja (v, v) ning väär väärtustustel (t, v) ja (v, t) .

Näide 2.46. Valem

$$X \wedge \neg Y \wedge Z \vee \neg X \wedge Y \wedge Z \vee \neg X \wedge \neg Y \wedge \neg Z$$

kui täielikul disjunktiiivsel normaalkujul olev on tõene parajasti väärtustustel (t, v, t) , (v, t, t) ja (v, v, v) .

Ülesanne 2.47. Leida kolme muutuja valem, mis on tõene parajasti siis, kui kaks muutajat on väärad.

Teoreem 2.48

Valemil eksisteerib täielik disjunktiiivne normaalkuju parajasti siis, kui ta on kehtestatav.

Teoreemist 2.48 järeldub vahetult, et samaselt vääral valemil ei leidu täielikku disjunktiiivset normaalkuju.

Etteantud (kehtestatava) valemi saab teisendada disjunktiiivsele normaalkujule järgmiste sammudega:

1. Elimineerime implikatsioonid ja ekvivalentsid, kasutades näiteks samaväärsusi $\mathcal{F} \Rightarrow \mathcal{G} \equiv \neg \mathcal{F} \vee \mathcal{G}$ ja $\mathcal{F} \Leftrightarrow \mathcal{G} \equiv \mathcal{F} \wedge \mathcal{G} \vee \neg \mathcal{F} \wedge \neg \mathcal{G}$. Tulemuseks saadud valem sisaldab ainult eitust, konjunktsiooni ja disjunktsiooni.

- Viime eitused vahetult lausemuutujate ette, kasutades De Morgani seadusi $\neg(\mathcal{F} \wedge \mathcal{G}) \equiv \neg\mathcal{F} \vee \neg\mathcal{G}$ ja $\neg(\mathcal{F} \vee \mathcal{G}) \equiv \neg\mathcal{F} \wedge \neg\mathcal{G}$. Kui kuskile tekib kahekordne eitus, siis jätame selle ära. Tulemuseks on valem, kus pole ühtegi eitust sulgude ees.
- Asendame disjunkttsioonide konjunkttsioonid distributiivsust kasutades konjunkttsioonide disjunkttsioonidega $\mathcal{F} \wedge (\mathcal{G} \vee \mathcal{H}) \equiv \mathcal{F} \wedge \mathcal{G} \vee \mathcal{F} \wedge \mathcal{H}$
- Kui esineb samaselt vääraid konjunkttsioone, st esinevad samaaegselt X ja $\neg X$, siis võime ka need ära jätta. Võrdsetest konjunkttsioonidest jätame idempotentsuse omaduse tõttu alles ainult ühe $\mathcal{F} \wedge \mathcal{F} \equiv \mathcal{F}$.
- Täieliku disjunkttiivse normaalkuju saamiseks tuleb iga lihtkonjunkttsioon teha täielikuks: kui näiteks lihtkonjunkttsioonis K puudub muutuja X , siis samaväärsusega

$$K \equiv K \wedge (X \vee \neg X) \equiv K \wedge X \vee K \wedge \neg X$$

oleme mõlemasse lihtkonjunkttsiooni $K \wedge X$ ja $K \wedge \neg X$ lisanud muutuja X . Vajadusel tuleb sellist võtet korrata ja lõpuks jätta omavahel võrdsetest täielikest lihtkonjunkttsioonidest alles ainult üks.

Valemi täielikku disjunkttiivset normaalkuju saab leida ka tõeväärtustabeli abil.

Näide 2.49. Leida valemi $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$ täielik disjunkttiivne normaalkuju.

X	Y	Z	$X \wedge \neg Y$	$Z \Rightarrow \neg X$	$Y \vee X$	$X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$
1	1	1	0	0	1	0
1	1	0	0	1	1	0
1	0	1	1	0	1	0
1	0	0	1	1	1	1
0	1	1	0	1	1	0
0	1	0	0	1	1	0
0	0	1	0	1	0	1
0	0	0	0	1	0	1

- Tõeväärtustabelist nägime, et valem $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$ on tõene ainult väärtustustel $(1, 0, 0)$, $(0, 0, 1)$ ja $(0, 0, 0)$.
- Nendele väärtustustele vastavad täielikud lihtkonjunkttsioonid on vastavalt $X \wedge \neg Y \wedge \neg Z$, $\neg X \wedge \neg Y \wedge Z$ ja $\neg X \wedge \neg Y \wedge \neg Z$.
- Seega valemi $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$ täielik disjunkttiivne normaalkuju on

$$(X \wedge \neg Y \wedge \neg Z) \vee (\neg X \wedge \neg Y \wedge Z) \vee (\neg X \wedge \neg Y \wedge \neg Z).$$

Hulgateooria

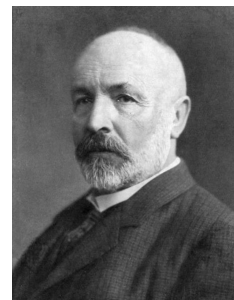
*Mitte keegi ei viska meid välja
paradiisist, mille Cantor on meie
jaoks loonud – D. Hilbert*

3.1	Hulga kirjeldamine	38
3.2	Osahulk	41
3.3	Hulkade ühend ja ühisosa	44
3.4	Hulkade vahe ja sümmeetriline vahe	48
3.5	Hulga täiend	50
3.6	Lõplikud ja lõpmatud ühendid ja ühisosad	52
3.7	Hulkade otsekorrutis	54

Selles peatükis räägime kõige fundamentaalsemast ideest matemaatikas – nimelt hulgast ja tutvustame hulgateooria algtõdesid. Kuna hulk on matemaatikas algmõiste, siis ei defineerita seda üldisemate mõistete kaudu. Hulkadest kui objektidest aga konstrueeritakse kõik matemaatilised struktuurid (näeme seda edasistes peatükkides tihti). Siinses kursuses ei ole meie eesmärgiks käsitleda hulgateooria aksiomaatilist ülesehitust, vaid anda mitteformaalsem ülevaade sellest, mis on hulk, kuidas matemaatikud hulki tähistavad ning millised olulised mõisted ja seosed on hulkade abil kirjeldatavad.

Hulki oled sa enda ümber näinud kogu aeg. Kõik järgnevad on näited hulkadest: üliõpilased siin kursusel kellel on oma iPad; sellel nädalal poest ostetud puuviljad; negatiivsed täisarvud jne. Lapsena õppisid sa valjult tähestikku pähe, tegelikult aga ütlesid tähti, mis kuuluvad spetsiaalsesse hulka nimega „Eesti tähestik“. Seega, hulk on mingite objektide kogu.

Täpsemalt sõnastas hulgateooria rajaja Georg Cantor hulga kui sellise omavahel erinevate objektide kogu, millest saab mõelda kui tervikust. Mida sellisest definitsioonist veel välja lugeda saab? Kõigepealt väidab eelnev lause, et hulka kuuluvad objektid on omavahel



Georg Cantor
(1845–1918)

erinevad. Teiseks peab olema võimalik üheselt otsustada, kas antud objekt kuulub vaadeldavasse hulka või mitte.

Hulga all mõistetakse üksteisest erinevate objektide kogumit, mida vaadeldakse ühe tervikuna ja kus iga objekti korral on võimalik üheselt kindlaks määrata, kas ta kuulub antud hulka.

Objekte, mis moodustavad hulga (kuuluvad hulka), nimetatakse **hulga elementideks**. Hulga element ja hulk ise loetakse alati erinevateks objektideks, seega hulk ei ole kunagi iseenda elemendiks.

Hulki tähistatakse tavaliselt suurte ladina tähtedega $A, B, C, X, Y, \dots$, hulga elemente aga väikeste ladina tähtedega $a, b, c, x, y, \dots$. Kui element a kuulub hulka A , siis kirjutame, et $a \in A$; kui a ei ole hulga A element, siis kirjutatakse $a \notin A$.

Näide 3.1. Olgu $A = \{1, 2, 3, 4, 5\}$. Siis $3 \in A$, aga $9 \notin A$.

Näide 3.2. Olgu $A = \{a \mid a \text{ on hulk}\}$. See oleks „kõikide hulkade hulk“. Kui A oleks hulk, siis ta oleks üks oma elementidest, seega $A \in A$. Viimane on aga võimatu, mistõttu A ei ole hulk. Antud juhul räägitakse **kõikide hulkade klassist** või **kõikide hulkade kogumist**.

Kahte hulka A ja B loetakse **võrdseteks** ja kirjutatakse $A = B$, kui hulgad A ja B koosnevad täpselt samadest elementidest. Viimase tingimuse võib kirja panna ka selliselt:

$$A = B \quad \Leftrightarrow \quad \forall x (x \in A \Leftrightarrow x \in B).$$

Näiteks, kui $A = \{x \mid x \in \mathbb{R}, x^2 - 3x + 2 = 0\}$ ja $B = \{1, 2\}$, siis annab ruutvõrrandi lahendamine tulemuseks, et $A = B$.

3.1 Hulga kirjeldamine

Hulkade kirjeldamisel on väga oluline täpselt kirja panna, millised elemendid antud hulka kuuluvad. Elementide *erinevuse* nõue hulga mõiste määrangus tähendab, et hulgas ei saa olla mitut elementi, mida loeme omavahel võrdseteks. Näiteks ei saa rääkida hulgast, mis koosneb kahest punasest ja kolmest sinisest kuulikesest, kusjuures punaseid kuule omavahel ja siniseid kuule omavahel loeksime ühesugusteks. Võrrandi $(x - 1)^2 = 0$ lahendite hulgas on üks element, mitte kaks võrdset arvu 1.

Kui hulk koosneb väikesest arvust elementidest, siis võib need elemendid looksulgude vahel komadega eraldatult üles loetleda. Näiteks $A = \{1, 2, 3\}$ on hulk, mis koosneb elementidest 1, 2 ja 3. Ei ole oluline, millises järjekorras hulga elemendid kirja pandud on. Seega $A = \{3, 2, 1\} = \{2, 1, 3\}$ tähistavad kõik eelpool mainitud hulka A . Eesti Vabariigi presidentide hulk on $A = \{\text{Päts, Meri, Rüütel, Ilves, Kaljulaid, Karis}\}$ ning kõigi arvust 20 väiksemate positiivsete paarisarvude hulk on $B = \{2, 4, 6, 8, 10, 12, 14, 16, 18\}$.

Mõnedes hulkades on aga liiga palju elemente, et neid kõiki üles loendada. Näiteks $X = \{1, 3, 5, \dots, 49\}$ on kõigi 50-st väiksemate positiivsete paaritute arvude hulk ning $Y = \{2, 4, 6, \dots\}$ on kõigi positiivsete paarisarvude hulk. Antud kirjaviisis mõttepunktid (kolm punkti) tähendavad seda, et jätkka loendust „samal viisil“.

Hulga elementide loendi esitamise asemel võib hulga määrata ka temasse kuulumise tingimuse abil, sest sageli kuuluvad samasse hulka elemendid, mis rahuldavad teatud tingimust või millel on mõni ühine omadus. Sellistel juhtudel kasutame kirjeldusviisi $S = \{x : p(x)\}$ või $S = \{x \mid p(x)\}$, kus $p(x)$ tähistab tingimust või tingimuste loetelu, mida vaadeldavas hulka kuuluvad elemendid x peavad rahuldama. (Erinevates allikates pannakse elemendi üldkuju ja tingimuste vahele kas püstkriips või koolon.) Näiteks, kui uurime võrrandi reaalarvulisi lahendeid, siis $S = \{x \in \mathbb{R} \mid (x-1)(x+2)(x+3) = 0\}$ on kõigi selliste reaalarvude x hulk, mis rahuldavad võrrandit $(x-1)(x+2)(x+3) = 0$ ehk S on selle võrrandi reaalarvuliste lahendite hulk. Me oleks võinud ka kirjutada, et $S = \{1, -2, -3\}$. Kuigi viimane kirjutusviis on palju lihtsam, ei anna see meile aga informatsiooni selle kohta, et algselt olime huvitatud teatud võrrandi lahenditest.

Mõned hulgad matemaatikas on kasutusel nii tihti, et nendele on antud omad tähistused. Tähtsamad arvuhulgad on

- **Naturaalarvude hulk** $\mathbb{N} = \{1, 2, 3, \dots\}$;
- **Täisarvude hulk** $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$;
- **Ratsionaalarvude hulk** $\mathbb{Q} = \{q \mid q = \frac{m}{n}, m \in \mathbb{Z}, n \in \mathbb{N}\}$;
- **Reaalarvude hulk** $\mathbb{R}$;
- **Irratsionaalarvude hulk** $\mathbb{I}$;
- **Kompleksarvude hulk** $\mathbb{C} = \{z \mid z = x + iy, x, y \in \mathbb{R}, i^2 = -1\}$.

Arvude intervallid saab samuti hulkadena kirja panna:

- **Lõik** $[a, b] = \{x \mid x \in \mathbb{R}, a \leq x \leq b\}$;
- **Vahemik** $(a, b) = \{x \mid x \in \mathbb{R}, a < x < b\}$;
- **Poollõigud** $[a, b) = \{x \mid x \in \mathbb{R}, a \leq x < b\}$ ja $(a, b] = \{x \mid x \in \mathbb{R}, a < x \leq b\}$.

Näide 3.3. Hulkade erinevaid kirjeldusviise:

1. $A = \{x \mid x \in \mathbb{R}, x^2 - 3x + 2 = 0\} = \{1, 2\}$;
2. $B = \{3n \mid n \in \mathbb{N}, n > 2\} = \{9, 12, 15, \dots\}$.

Ülesanne 3.4. Pane paaritute täisarvude hulk kirja kahel erineval viisil.

Hulgas ei pea aga olema ühtegi elementi. Tundub küll veider vaadelda hulki, milles elemendid puuduvad, kuid sellised hulgad kerkivad esile väga tihti ning väga erinevates olukordades. Näiteks, kui A on võrrandi $x^2 + 1 = 0$ reaalarvuliste lahendite hulk, siis hulgas A

ei ole ühtegi elementi. Matemaatikas on olemas vaid üks hulk, milles pole ühtegi elementi ja see on tühi hulk. Tühja hulka tähistatakse sümboliga $\emptyset$. Näiteks, kõigi reaalarvude x hulk, mis rahuldavad võrratust $x^2 < 0$, on samuti tühi hulk.

Definitsioon 3.5

Tühjaks hulgaks (ingl *empty set*) nimetatakse hulka, mis ei sisalda ühtegi elementi ja seda tähistatakse sümboliga $\emptyset$.

Hulga elementideks võivad olla ka hulgad ise.

Märkus. Lõpliku hulga A võimsuseks nimetatakse tema elementide arvu ning tähistatakse $|A|$. Vaata definitsiooni 7.2.

Näide 3.6.

1. Hulk $S = \{1, 2, \{1, 2\}, \emptyset\}$ koosneb neljast elemendist, millest kaks on ise hulgad, nimelt $\{1, 2\}$ ja $\emptyset$.
2. Hulk $T = \{0, \{1, 2, 3\}, 4, 5\}$ koosneb samuti neljast elemendist, nimelt kolmest täisarvust 0, 4 ja 5 ning ühest hulgast $\{1, 2, 3\}$. Kuigi $2 \in \{1, 2, 3\}$, ei ole arv 2 hulga T element, st $2 \notin T$.

Näide 3.7. Olgu $D = \{n \in \mathbb{N} : n \leq 9\}$, $E = \{x \in \mathbb{Q} : x \leq 9\}$, $H = \{x \in \mathbb{R} : x^2 - 2 = 0\}$ ja $J = \{x \in \mathbb{Q} : x^2 - 2 = 0\}$.

- (a) Kirjelda hulka D , loetledes üles kõik tema elemendid.
- (b) Nimeta kolm elementi, mis kuuluvad hulka E , aga ei kuulu hulka D .
- (c) Kirjelda hulka H , loetledes üles kõik tema elemendid.
- (d) Kirjelda hulka J mõnel muul viisil.
- (e) Leia hulkade D , H ja J võimsus.

Lahendus.

- (a) $D = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
- (b) $\frac{7}{5}, 0, -3$.
- (c) $H = \{\sqrt{2}, -\sqrt{2}\}$.
- (d) $J = \emptyset$.
- (e) $|D| = 9, |H| = 2$ ja $|J| = 0$.

■

Näide 3.8. Millistesse järgmistesse hulkadesse kuulub arv -2 ?

- (a) $S_1 = \{-1, -2, \{-1\}, \{-2\}, \{-1, -2\}\};$
- (b) $S_2 = \{x \in \mathbb{N} : -x \in \mathbb{N}\};$

$$(c) S_3 = \{x \in \mathbb{Z}: x^2 = 2^x\};$$

$$(d) S_4 = \{x \in \mathbb{Z}: |x| = -x\};$$

$$(e) S_5 = \{\{-1, -2\}, \{-2, -3\}, \{-1, -3\}\}.$$

Lahendus. Arv -2 kuulub hulkadesse S_1 ja S_4 . Hulga S_4 korral näeme, et $|-2| = 2 = -(-2)$. Hulk S_2 on tühi hulk, seega $-2 \notin S_2$. Kuna $(-2)^2 = 4$ ja $2^{-2} = \frac{1}{4}$, siis $-2 \notin S_3$. Ning viimaseks, kuna hulga S_5 kõikideks elementideks on hulgad, ei saa -2 hulga S_5 elemendiks olla, sest ta on arv, aga mitte hulk. ■

Ülesanne 3.9. Mõttele välja üks viietäheline sõna nii, et $|S| = 3$, kus S on sõnas esinevate tähtede hulk.

3.2 Osahulk

Järgnevalt uurime, millistel tingimustel saavad ühe hulga elemendid olla teise hulga elementideks. Ühe äärmusena võime vaadelda juhtu, kus kõik hulga A elemendid kuuluvad ka hulka B . Teise äärmusena aga juhtu, kus mitte ükski hulga A element ei kuulu hulka B .

Definitsioon 3.10

Hulka A nimetatakse hulga B **osahulgaks** ehk **alamhulgaks** (ingl *subset*), kui kõik hulga A elemendid on hulga B elementideks (ehk hulga A iga element kuulub hulka B).

Kui hulk A on hulga B osahulk, siis kirjutame $A \subset B$. Kui hulk A ei ole hulga B osahulk, siis kirjutame $A \not\subset B$. Kvantorite abil saame osahulgaks olemist ja mitteolemist kirja panna järgmiselt:

$$A \subset B \text{ tähendab, et } \forall x (x \in A \Rightarrow x \in B)$$

ja

$$\begin{aligned} A \not\subset B \text{ tähendab, et } & \neg(\forall x (x \in A \Rightarrow x \in B)) \\ & \equiv \exists x \neg(x \in A \Rightarrow x \in B) \\ & \equiv \exists x (x \in A \wedge x \notin B) \end{aligned}$$

Seega, $A \not\subset B$ tähendab seda, et peab leiduma selline hulga A element, mis ei kuulu hulka B .

Näide 3.11.

1. $(0, 1) \subset [0, 1]$.
2. Hulgal $\{a, b\}$ on järgmised osahulgad: $\emptyset, \{a\}, \{b\}, \{a, b\}$.

Lause 3.12: Osahulga omadused

1. Iga hulga A korral $A \subset A$ (*refleksiivsus*);
2. Iga hulga A korral $\emptyset \subset A$;
3. Kui A ja B on sellised hulgad, et $A \subset B$ ja $B \subset A$, siis $A = B$ (*antisümmeetrilisus*);
4. Kui A, B ja C on sellised hulgad, et $A \subset B$ ja $B \subset C$, siis $A \subset C$ (*transitiivsus*).

Tõestus. Tõestame 2. ja 4. omaduse. Ülejäänud kahe omaduse tõestuse jätame iseseisvaks tööks.

2. Oletame vastuväiteliselt, et leidub mittetühi hulk A nii, et $\emptyset \not\subset A$. Definitsiooni kohaselt peab siis leiduma element x hulgast $\emptyset$, mis ei kuulu hulka A . See on aga võimatu, sest hulgas $\emptyset$ ei leidu ühtegi elementi. Seega $\emptyset \subset A$ iga hulga A korral.

4. Eelduseks on, et $A \subset B$ ja $B \subset C$. Peame näitama, et $A \subset C$. Viimase väite tõestamiseks võtame suvalise elemendi x hulgast A ja näitame, et siis $x \in C$. Kuna esimesest eeldusest $A \subset B$, siis sellest, et $x \in A$ järelneb, et $x \in B$. Teise eelduse kohaselt $B \subset C$, seega iga hulga B element on ka hulga C elemendiks. Kuna meil $x \in B$, siis järelneb, et ka $x \in C$. Olemegi näidanud, et suvalise elemendi x korral hulgast A see element kuulub ka hulka C . Seega $A \subset C$. ■

Märkus. Sisalduvusseose teist omadust ehk antisümmeetrilisuse omadust kasutatakse sageli just siis, kui on vaja tõestada, et kaks hulka on võrdsed. Võrduse tõestamiseks näidatakse sel juhul, et kumbki hulkadest on teise hulga osahulk. Ehk siis võrdsuse $A = B$ tõestamiseks näidatakse, et $A \subset B$ ja $B \subset A$. Kui $A \neq B$, siis peab leiduma vähemalt üks element, mis kuulub ühte nendest hulkadest, aga mitte teise.

Näide 3.13. Transitiivsuse omadust illustreerivad kenasti arvuhulkade omavahelised seosed: kuna $\mathbb{Q} \subset \mathbb{R}$ ja $\mathbb{R} \subset \mathbb{C}$, siis loomulikult $\mathbb{Q} \subset \mathbb{C}$.

Lause 3.14

Tühi hulk $\emptyset$ on üheselt määratud.

Tõestus. Oletame vastuväiteliselt, et leiduvad kaks erinevat tühja hulka $\emptyset_1$ ja $\emptyset_2$. Nüüd lauses 3.12 toodud 2. omaduse põhjal $\emptyset_1 \subset \emptyset_2$ (sest $\emptyset_1$ on tühi hulk) ning $\emptyset_2 \subset \emptyset_1$ (sest $\emptyset_2$ on tühi hulk). Kuna $\emptyset_1 \subset \emptyset_2$ ja $\emptyset_2 \subset \emptyset_1$, siis lauses 3.12 toodud 3. omaduse põhjal järelneb, et $\emptyset_1 = \emptyset_2$. Viimane on aga vastuolus meie eeldusega, et $\emptyset_1 \neq \emptyset_2$. Seega leidub täpselt üks tühi hulk. ■

Ülesanne 3.15. Leia kaks hulka A ja B nii, et A on nii hulga B element kui ka osahulk.

Lahendus. Otsime kahte hulka A ja B nii, et $A \in B$ ja $A \subset B$. Alustame üheelemendilist hulgast, näiteks $A = \{1\}$. Kuna soovime, et $A \in B$, peab hulk B sisaldama hulka $\{1\}$ kui ühte oma elementi. Teisalt soovime aga, et $A \subset B$, mis tähendab definitsiooni järgi seda, et iga hulga A element peab olema ka hulga B elemendiks. Kuna arv 1 on hulga A

ainus element, peab arv 1 olema ka hulga B elemendiks. Seega üks võimalik valik hulgaks B on $B = \{1, \{1\}\}$, kuigi ka hulk $B = \{1, 2, \{1\}\}$ rahuldab nõutud tingimusi nagu ka veel paljud teised hulgad. ■

Definitsioon 3.16

Hulka A nimetatakse hulga B **pärisosahulgaks** või **pärisalamhulgaks** (ingl *proper subset*) ja kirjutatakse $A \subsetneq B$, kui hulk A on hulga B osahulk ja $A \neq B$.

Märkus. Seoste $A \subset B$ ja $A \subsetneq B$ vahekord on analoogiline arvude vahelise mitterange ja range võrratusega.

Näide 3.17.

1. Kui $S = \{4, 5, 7\}$ ja $T = \{3, 4, 5, 6, 7\}$, siis $S \subsetneq T$.
2. Arvuhulkade vahel kehtivad sisalduvused $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$.
3. Kui $a < b$, siis $(a, b) \subsetneq (a, b] \subsetneq [a, b]$.

Ülesanne 3.18. Tõesta, et täisarvude hulk $\mathbb{Z}$ on ratsionaalarvude hulga $\mathbb{Q}$ pärisosahulk.

Lahendus. Meil on vaja näidata kahte asja. Esiteks peame näitama, et kui element x kuulub täisarvude hulka $\mathbb{Z}$, siis kuulub ta ka ratsionaalarvude hulka $\mathbb{Q}$ (kuuluvuse ehk osahulgaks olemise tingimus). Teiseks peame näitama, et leidub selline element y , mis kuulub ratsionaalarvude hulka $\mathbb{Q}$, aga ei kuulu täisarvude hulka $\mathbb{Z}$ (pärisosahulgaks olemise tingimus). Need kaks väidet saame lausearvutuse sümbboolikat kasutades kirja panna järgmiselt:

$$\forall x (x \in \mathbb{Z} \Rightarrow x \in \mathbb{Q}) \quad \text{ja} \quad \exists y (y \in \mathbb{Q} \wedge y \notin \mathbb{Z}).$$

Esimese väite tõestus on lihtne. Olgu $x \in \mathbb{Z}$. Kuna iga täisarvu saab arvuga 1 jagada, võime kirjutada $x = \frac{x}{1}$. Nüüd on arv x esitatud kujul, kus lugejas ja nimetajas on täisarv. Ratsionaalarvu definitsiooni kohaselt on x seega ratsionaalarv ehk $x \in \mathbb{Q}$.

Teise osa tõestuseks on meil vaja leida ratsionaalarv, mis ei ole samal ajal täisarv. Võtame näiteks $y = \frac{1}{2}$ (selliseid arve on ju palju!). Definitsiooni kohaselt on y ratsionaalarv (esitatud kahe täisarvu suhtena), kuid y pole täisarv. Seega oleme leidnud vähemalt ühe arvu y , mis kuulub ratsionaalarvude hulka $\mathbb{Q}$, aga ei kuulu täisarvude hulka $\mathbb{Z}$. Sellega oleme näidanud, et täisarvude hulk $\mathbb{Z}$ on ratsionaalarvude hulga $\mathbb{Q}$ pärisosahulk. ■

Definitsioon 3.19

Olgu A hulk. Hulga A **kõigi osahulkade hulk** on $\mathcal{P}(A) = \{X \mid X \subset A\}$.

Ülesanne 3.20. Iga hulga korral leia tema kõigi osahulkade hulk. Samuti määra $|A|$ ja $|\mathcal{P}(A)|$.

1. $A = \emptyset$;
2. $A = \{a, b\}$;
3. $A = \{1, 2, 3\}$.

Lahendus.

1. $\mathcal{P}(A) = \{\emptyset\}$. Antud juhul $|A| = 0$ ja $|\mathcal{P}(A)| = 1$;
2. $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Seekord $|A| = 2$ ja $|\mathcal{P}(A)| = 4$;
3. $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$. Nüüd $|A| = 3$ ja $|\mathcal{P}(A)| = 8$.

■

Pane tähele, et eelmise näite iga hulga korral kehtib seos $|\mathcal{P}(A)| = 2^{|A|}$. Osutub, et see on alati nii ehk kui hulgas A on n elementi, siis sellel hulgal on 2^n erinevat osahulka.

Lause 3.21

Kui hulgas A on n elementi, siis hulgal A on 2^n erinevat osahulka.

Tõestus. Iseseisvalt!

■

Näide 3.22. Kui $C = \{\emptyset, \{\emptyset\}\}$, siis $\mathcal{P}(C) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$. Siinjuures on oluline mõista, et ükski hulkadest $\emptyset, \{\emptyset\}$ ja $\{\{\emptyset\}\}$ ei ole omavahel võrdsed. (Tühi kast ja kast, mille sees on tühi kast, ei ole samad asjad.) Antud hulga C korral on korrektne kirjutada

$$\emptyset \subset C, \quad \emptyset \subsetneq C, \quad \emptyset \in C, \quad \{\emptyset\} \subset C, \quad \{\emptyset\} \subsetneq C, \quad \{\emptyset\} \in C$$

samuti on korrektne ka $\{\{\emptyset\}\} \subset C$, $\{\{\emptyset\}\} \notin C$ ja $\{\{\emptyset\}\} \in \mathcal{P}(C)$.

3.3 Hulkade ühend ja ühisosa

Nii nagu saame omavahel täisarve kombineerides (liites, lahutades, korrutades ja mõnikord jagades) moodustada uusi täisarve, nii on võimalik kahe hulga ühendamisel moodustada uusi hulki.

Definitsioon 3.23

Hulkade A ja B **ühendiks** (ingl *union*) nimetatakse hulka $A \cup B$, mille moodustavad kõik elemendid, mis kuuluvad vähemalt ühte hulkadest A või B , st

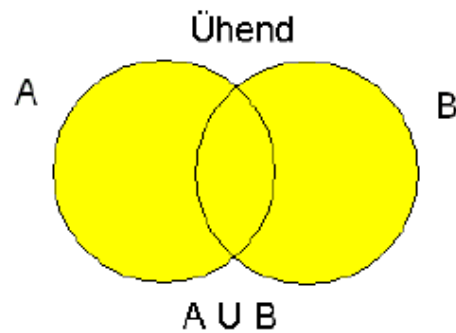
$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

Sidesõna „või“ kasutatakse siin jällegi mittevälistavas tähenduses, st element x võib kuuluda kas hulka A või hulka B või mõlemasse hulka korraga.

Ühiseid elemente arvestatakse vaid üks kord. Meelde jätmiseks ja segaduste vältimiseks tasub teada, et ühendi sümbol $\cup$ tuleneb inglisekeelsest sõnast *Union*.

Märgime, et alati $A \subset A \cup B$ ja $B \subset A \cup B$.

Tehete abil moodustatud hulkadest piltliku ettekujutuse saamiseks kasutatakse nn **Venni diagramme**. Kui hulgad A ja B on kujutatud ringidena, siis värvitud ala joonisel on nende ühend $A \cup B$.

**Näide 3.24.**

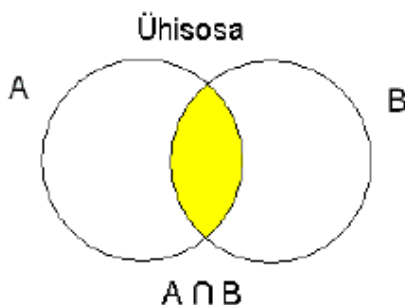
1. Kui $A = \{a, b, c\}$ ja $B = \{a, c, d, e\}$, siis $A \cup B = \{a, b, c, d, e\}$;
2. $[0, 1) \cup (0, 1] = [0, 1]$;
3. $\mathbb{N} \cup \mathbb{Q} = \mathbb{Q}$.

Definitsioon 3.25

Hulkade A ja B **ühisosaks** ehk **lõikeks** (ingl *intersection*) nimetatakse hulka $A \cap B$, mille moodustavad kõik elemendid, mis kuuluvad nii hulka A kui ka hulka B , st

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

Mis tahes hulkade korral $A \cap B \subset A$ ja $A \cap B \subset B$. Ühisosa on Venni diagrammi abil kujutatud värvitud osana järgmiselt:

**Näide 3.26.**

1. Kui $A = \{a, b, c\}$ ja $B = \{a, c, d, e\}$, siis $A \cap B = \{a, c\}$;
2. $[0, 1) \cap (0, 1] = (0, 1)$;
3. $\mathbb{N} \cap \mathbb{Q} = \mathbb{N}$.

Lause 3.27

Iga kahe hulga A ja B korral kehtib $A \cap B \subset A \cup B$.

Tõestus. Esiteks, kui $A \cap B = \emptyset$, siis $\emptyset = A \cap B \subset A \cup B$ lause 3.12 omaduse 2. põhjal. Seega vaatleme nüüd juhtu, kus $A \cap B \neq \emptyset$. Peame näitama, et kui $x \in A \cap B$, siis $x \in A \cup B$. Seega, olgu antud suvaline element $x \in A \cap B$. Ühisosa definitsiooni kohaselt kuulub element x mõlemasse hulka, nii hulka A kui ka hulka B . Kuna $x \in A$, siis kahe hulga ühendi definitsiooni kohaselt on õige ka väide, et $x \in A \cup B$. Seega oleme näidanud, et $A \cap B \subset A \cup B$. ■

Kui kahel hulgal A ja B ei ole ühiseid elemente, siis $A \cap B = \emptyset$ ning hulki A ja B nimetatakse **lõikumatuteks**. Näiteks, ratsionaalarvude ja irratsionaalarvude hulgad on lõikumatud.

Ülesanne 3.28. Mida saab öelda hulkade A ja B kohta, kui $A \cap B = A$ või kui $A \cap B = B$? Joonista vastavad Venni diagrammid.

Teoreem 3.29: Ühendi ja ühisosa omadusi

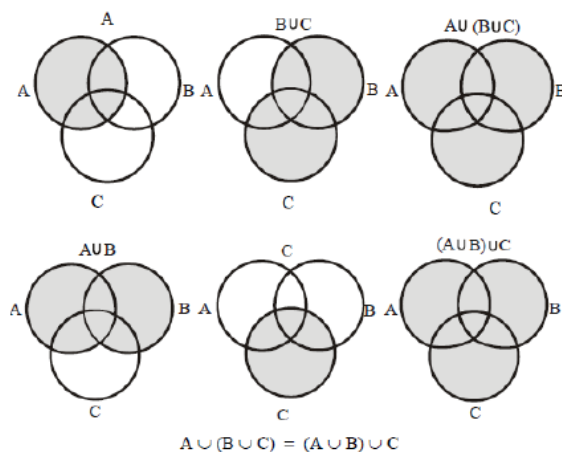
1. Iga hulga A korral $A \cup A = A$ ja $A \cap A = A$ (*idempotentsus*);
2. Mis tahes hulkade A ja B korral $A \cup B = B \cup A$ ja $A \cap B = B \cap A$ (*kommutiivsus*);
3. Mis tahes hulkade A , B ja C korral $(A \cup B) \cup C = A \cup (B \cup C)$ ja $(A \cap B) \cap C = A \cap (B \cap C)$ (*assotsiatiivsus*);
4. Mis tahes hulkade A , B ja C korral $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ ja $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ (*distributiivsus*).

Tõestus. Omadused 1. – 3. järelduvad vahetult definitsioonidest ja on jäetud iseseisvaks tööks. Näitena tõestame teise distributiivsuse võrduse ehk $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$. Kontrollime seda võrdust samaväärsuste ahela abil:

$$\begin{aligned}
 x \in (A \cup C) \cap (B \cup C) &\equiv x \in A \cup C \wedge x \in B \cup C \\
 &\equiv (x \in A \vee x \in C) \wedge (x \in B \vee x \in C) \\
 &\equiv (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \vee (x \in C \wedge x \in B) \vee (x \in C \wedge x \in C) \\
 &\equiv (x \in A \wedge x \in B) \vee (x \in A \vee x \in B \vee x \in C) \wedge x \in C \\
 &\equiv (x \in A \wedge x \in B) \vee x \in C \\
 &\equiv x \in A \cap B \vee x \in C \\
 &\equiv x \in (A \cap B) \cup C.
 \end{aligned}$$

Ülejäänud võrduste kontroll teosta iseseisvalt. ■

Assotsiatiivsuse omadust saab illustreerida Venni diagrammide abil järgmiselt: (Venni diagrammide joonistamine ei ole sama, mis tõestus!)



3.4 Hulkade vahe ja sümmeetriline vahe

Definitsioon 3.30

Hulkade A ja B **vaheks** (ingl *difference*) nimetatakse hulka $A \setminus B$, mille moodustavad elemendid, mis kuuluvad hulka A , aga ei kuulu hulka B , st

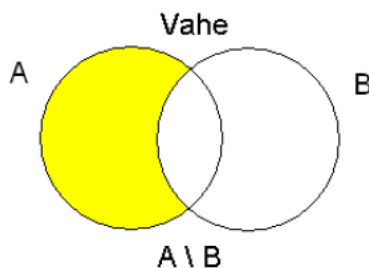
$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}.$$

Näide 3.31.

1. Kui $A = \{1, 2, 3, 4, 5\}$ ja $B = \{2, 4, 6\}$, siis $A \setminus B = \{1, 3, 5\}$ ja $B \setminus A = \{6\}$;
2. $[0, 1) \setminus (0, 1) = \{0\}$;
3. $\mathbb{N} \setminus \mathbb{Z} = \emptyset$.

Esimene nendest näidetest kinnitab ka asjaolu, et üldiselt $A \setminus B \neq B \setminus A$.

Venni diagrammil on kahe hulga vahe kujutatud järgmiselt:



Ülesanne 3.32. Olgu antud hulgad $A = \{x \in \mathbb{R} : |x| \leq 3\}$, $B = \{x \in \mathbb{R} : |x| > 2\}$ ja $C = \{x \in \mathbb{R} : |x - 1| \leq 4\}$.

1. Kirjelda hulki A , B ja C kasutades intervalli tähistusi;
2. Leia $A \cap B$, $A \setminus B$, $B \cap C$, $B \cup C$, $B \setminus C$ ja $C \setminus B$.

Lahendus.

1. $A = [-3, 3]$, $B = (-\infty, -2) \cup (2, \infty)$ ja $C = [-3, 5]$;
2. $A \cap B = [-3, -2) \cup (2, 3]$, $A \setminus B = [-2, 2]$, $B \cap C = [-3, -2) \cup (2, 5]$, $B \cup C = (-\infty, \infty)$, $B \setminus C = (-\infty, -3) \cup (5, \infty)$ ja $C \setminus B = [-2, 2]$.

■

Lause 3.33

Olgu A, B ja C hulgad. Siis

$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) \quad \text{ja} \quad A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C).$$

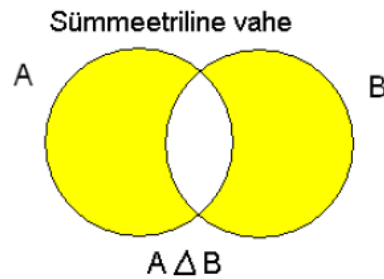
Tõestus. Iseseisvalt. ■

Definitsioon 3.34

Hulkade A ja B **sümmeetriliseks vaheks** (ingl *symmetric difference*) nimetatakse hulka $A \triangle B$, mille moodustavad elemendid, mis kuuluvad parajasti ühte kahest hulgast A ja B , st

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = \{x \mid (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\}.$$

Sümmeetrilist vahet illustreerib järgmine Venni diagramm:



Näide 3.35. Kui $A = \{a, b, c\}$ ja $B = \{a, c, d, e\}$, siis $A \triangle B = \{b, d, e\}$.

Lause 3.36

Olgu A ja B hulgad. Siis $A \triangle B = (A \cup B) \setminus (A \cap B)$.

Vaata ning võrdle seda tulemust sümmeetrilist vahet illustreeriva Venni diagrammiga.

Lause 3.36 tõestus. Peame tõestama, et kaks hulka $A \triangle B$ ja $(A \cup B) \setminus (A \cap B)$ on võrdsed. Kuna $A \triangle B = (A \setminus B) \cup (B \setminus A)$, siis peame näitama, et $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$. Tõepoolest,

$$\begin{aligned} x \in (A \cup B) \setminus (A \cap B) &\equiv x \in A \cup B \wedge x \notin A \cap B \\ &\equiv (x \in A \vee x \in B) \wedge \neg(x \in A \wedge x \in B) \\ &\equiv (x \in A \vee x \in B) \wedge (x \notin A \vee x \notin B) \\ &\equiv (x \in A \wedge x \notin A) \vee (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A) \vee (x \in B \wedge x \notin B) \\ &\equiv (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A) \\ &\equiv x \in A \setminus B \vee x \in B \setminus A \\ &\equiv x \in (A \setminus B) \cup (B \setminus A). \end{aligned}$$

Lisaks just tõestatud lausele 3.36 on sümmeetrilisel vahel veel järgmised omadused. ■

Lause 3.37: Sümmeetrilise vahe omadused

1. Mis tahes hulkade A ja B korral $A \triangle B = B \triangle A$ (*kommutatiivsus*);
2. Mis tahes hulkade A , B ja C korral $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ (*assotsiatiivsus*);
3. Mis tahes hulkade A , B ja C korral $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$ (*distributiivsus*);
4. Mis tahes hulkade A ja B korral $A \triangle B = A \cup B \Leftrightarrow A \cap B = \emptyset$.

Tõestus. Iseseisvalt. ■

Ülesanne 3.38. Kujuta Venni diagrammil hulgad $A \setminus (B \cup C)$, $A \cap (B \setminus C)$, $(A \setminus B) \setminus C$ ja $A \setminus (B \setminus C)$.

3.5 Hulga täiend

Koolimatemaatikas tegeletakse näiteks naturaalarvude hulgaga või täisarvude hulgaga, kusjuures uurimise objektideks on nii nende hulkade elemendid ja osahulgad kui ka elementide vahel defineeritud seosed, tehted ja funktsioonid. Hulgateoorias nimetatakse sellist hulka, mille uurimise objektideks on peamiselt selle hulga elemendid ja osahulgad ning nende vahel defineeritud seosed, tehted ja funktsioonid, **universaalhulgaks** ja tähistatakse tähega U .

Kui tegeletakse mingi universaalse hulga U elementidega, siis võivad iga konkreetse hulga $A \subset U$ puhul huvi pakkuda ka sellised universaalse hulga elemendid, mis hulka A ei kuulu. Näiteks, kui aritmeetikas on universaalseks hulgaks naturaalarvude hulk, siis koos paarisarvude hulgaga pakuvad huvi ka paaritud arvud.

Definitsioon 3.39

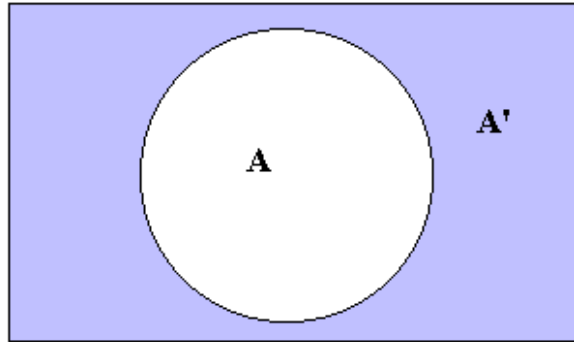
Olgu U universaalhulk ja $A \subset U$. Hulga A **täiendiks** A' (ingl *complement*) nimetatakse hulka, mille moodustavad kõik need universaalse hulga U elemendid, mis ei kuulu hulka A , st

$$A' = \{x \in U : x \notin A\} = U \setminus A.$$

Hulga A täiendit saab Venni diagrammi abil kujutada järgmiselt:

Näide 3.40.

1. Kui $U = \mathbb{Z}$, siis $\mathbb{N}' = \{0, -1, -2, \dots\}$;
2. Kui $U = \mathbb{R}$, siis $\mathbb{Q}' = \mathbb{I}$.


Lause 3.41: Täiendi omadused

Olgu U universaalhulk ja $A, B \subset U$. Hulga täiendi moodustamisel kehtivad järgmised omadused:

1. $\emptyset' = U$;
2. $U' = \emptyset$;
3. $A \cup A' = U$;
4. $A \cap A' = \emptyset$;
5. $A'' = A$;
6. $(A \cup B)' = A' \cap B'$;
7. $(A \cap B)' = A' \cup B'$.

Tõestus. Omadused 1. – 5. järelduvad vahetult täiendi definitsioonist ja on jäetud iseseisvaks tööks. Omadusi 6. ja 7. nimetatakse De Morgani valemiteks. Antud valemid väljendavad ühendi ja ühisosa duaalsust täiendi võtmise suhtes. Meie tõestame vaid De Morgani valemi 7. (valemi 6. tõestus on analoogiline).

7. Kontrollime võrdust samaväärsuste ahela abil:

$$\begin{aligned}
 x \in (A \cap B)' &\equiv x \in U \wedge x \notin A \cap B \\
 &\equiv x \in U \wedge \neg(x \in A \wedge x \in B) \\
 &\equiv x \in U \wedge (x \notin A \vee x \notin B) \\
 &\equiv (x \in U \wedge x \notin A) \vee (x \in U \wedge x \notin B) \\
 &\equiv x \in A' \vee x \in B' \\
 &\equiv x \in A' \cup B'.
 \end{aligned}$$

Hulkade A ja B vahet $A \setminus B$ nimetatakse mõnikord ka **hulga B täiendiks hulga A suhtes**. Põhjuse selleks annab definitsioon $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$. ■

Neli hulgateoreetilist tehet (ühend, ühisosa, vahe ja sümmeetriline vahe) on omavahel seotud selles mõttes, et igähte neist saab väljendada teiste kaudu. De Morgani seadustest järeldeb lisaks nn **duaalsuse printsiip**, mis tähendab, et etteantud hulkadest, nt hulkadest X, Y, Z saab moodustada uusi hulki tehete $\cap$, $\cup$ ja $'$ abil. Seejuures igast tõest võrdusest niimoodi moodustatud hulkade vahel saame uue, samuti tõese võrduse, kui asendame kõik hulgad nende täiendhulkadega ning tehted $\cap$ ja $\cup$ vastavalt tehete $\cup$ ja $\cap$.

Näiteks võime kirjutada $A \cap B = A \setminus (A \setminus B)$ ning eespool oli juba antud esitus $A \Delta B = (A \setminus B) \cup (B \setminus A)$. Samuti võime kirjutada $(X' \cup Y) \cap X = (X \cap Y') \cup X' = (X \cup X') \cap (Y' \cup X') = U \cap (Y \cap X) = Y \cap X = X \cap Y$.

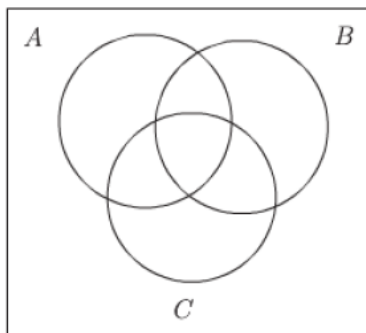
Ülesanne 3.42.

1. Avalda $A \cup B$ ja $A \setminus B$ tehete $\cap$ ja Δ abil;
2. Avalda $A \cap B$ ja $A \setminus B$ tehete $\cup$ ja Δ abil;
3. Avalda $A \cup B$ tehete $\setminus$ ja Δ abil.

Ülesanne 3.43. Tõesta, et $A \cup B$ ei ole võimalik avaldada tehete $\cap$ ja $\setminus$ abil ning $A \setminus B$ ei ole võimalik avaldada tehete $\cup$ ja $\cap$ abil.

3.6 Lõplikud ja lõpmatud ühendid ja ühisosad

Tihti seisame silmitsi olukorraga, kus hulgatehteid kasutades tuleb omavahel ühendada kolm või rohkem hulka. Tüüpiline Venni diagramm kolme hulga jaoks näeb välja selline:



Kolme hulga ühend defineeritakse kui $A \cup B \cup C = \{x \mid x \in A \vee x \in B \vee x \in C\}$. Jällegi, kui tahame, et element x kuuluks kolme hulga ühendisse, peab ta kuuluma vähemalt ühte nendest hulkadest.

Ülesanne 3.44. Oletame, et $x \in A \cup B \cup C$, kuid $x \notin A \cap B \cap C$. Millistesse hulkadesse saab element x kuuluda?

Kahe hulga ühendi ja ühisosa definitsioone saab üldistada:

- n hulga juhule, kus $n \in \mathbb{N}$;
- hulkade jadale $\{A_i : i = 1, 2, 3, \dots\}$;
- ja koguni suvalisele hulkade süsteemile.

Need üldised definitsioonid rakendavad sama ideed, nagu definitsioonid kahe komponendi puhul: ühendi moodustavad objektid, mis kuuluvad vähemalt ühte liidetavatest hulkadest, ja ühisosa need objektid, mis kuuluvad igasse vaadeldavasse hulka.

Nii saame n hulga ($n \in \mathbb{N}$) ühendi ja ühisosa defineerida võrdustega

$$A_1 \cup A_2 \cup \dots \cup A_n = \{x \mid x \in A_1 \vee x \in A_2 \vee \dots \vee x \in A_n\},$$

$$A_1 \cap A_2 \cap \dots \cap A_n = \{x \mid x \in A_1 \wedge x \in A_2 \wedge \dots \wedge x \in A_n\}.$$

Näide 3.45. Olgu $A_1 = \{0, 2, 5\}$, $A_2 = \{1, 2, 5\}$ ja $A_3 = \{2, 5, 7\}$. Siis

$$\bigcup_{i=1}^3 A_i = \{0, 1, 2, 5, 7\} \quad \text{ja} \quad \bigcap_{i=1}^3 A_i = \{2, 5\}.$$

Hulkade jada $A_1, A_2, A_3, \dots$ ühendi ja ühisosa saame defineerida võrdustega

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \dots = \{x \mid \exists i \in \mathbb{N} \text{ nii, et } x \in A_i\},$$

$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cap \dots = \{x \mid \forall i \in \mathbb{N} \text{ korral } x \in A_i\}.$$

Olgu nüüd $\mathcal{I}$ mingi mittetühi hulk ja vaatame hulkade süsteemi $(A_\alpha)_{\alpha \in \mathcal{I}}$, siis saame selle süsteemi hulkade ühendi ja ühisosa defineerida järgmiselt:

$$\bigcup_{\alpha \in \mathcal{I}} A_\alpha = \{x \mid \exists \alpha \in \mathcal{I} \text{ nii, et } x \in A_\alpha\},$$

$$\bigcap_{\alpha \in \mathcal{I}} A_\alpha = \{x \mid \forall \alpha \in \mathcal{I} \text{ korral } x \in A_\alpha\}.$$

Näiteks,

$$\bigcup_{i \in \{1, \dots, n\}} A_i = \bigcup_{i=1}^n A_i \quad \text{ja} \quad \bigcap_{i \in \{1, \dots, n\}} A_i = \bigcap_{i=1}^n A_i$$

ja

$$\bigcup_{i \in \mathbb{N}} A_i = \bigcup_{i=1}^{\infty} A_i \quad \text{ja} \quad \bigcap_{i \in \mathbb{N}} A_i = \bigcap_{i=1}^{\infty} A_i$$

Näide 3.46. Olgu iga $i \in \mathbb{N}$ korral $A_i = \{-i, 0, i\}$. Siis

$$\bigcup_{i=1}^{\infty} A_i = \mathbb{Z} \quad \text{ja} \quad \bigcap_{i=1}^{\infty} A_i = \{0\}.$$

Näide 3.47. Olgu $\mathcal{I} = [1, 4]$ ja iga $\alpha \in \mathcal{I}$ korral $A_\alpha = [0, \alpha]$. Siis näiteks $A_2 = [0, 2]$, $A_{\sqrt{2}} = [0, \sqrt{2}]$ ja $A_\pi = [0, \pi]$ ning

$$\bigcup_{\alpha \in \mathcal{I}} A_\alpha = \bigcup_{\alpha \in [1, 4]} A_\alpha = [0, 4] \quad \text{ja} \quad \bigcap_{\alpha \in \mathcal{I}} A_\alpha = \bigcap_{\alpha \in [1, 4]} A_\alpha = [0, 1].$$

Näide 3.48.

1. $\bigcup_{n \in \mathbb{Z}} [n - \frac{1}{2}, n + \frac{1}{2}) = \mathbb{R}$;
2. $\bigcap_{n=1}^{\infty} (0, \frac{1}{n}) = \emptyset$;
3. $\bigcup_{a, b \in \mathbb{Q}} (a, b) = \mathbb{R}$;
4. Iga hulga A korral $\bigcup_{a \in A} \{a\} = A$.

De Morgani seadused on üldistatavad mis tahes (isegi lõpmatu) arvu hulkade jaoks.

Ülesanne 3.49. Olgu U universaalhulk, $\mathcal{I} \neq \emptyset$ ja $A_\alpha \subset U$ iga $\alpha \in \mathcal{I}$ korral. Tõestada, et

$$\left(\bigcup_{\alpha \in \mathcal{I}} A_\alpha \right)' = \bigcap_{\alpha \in \mathcal{I}} A_\alpha' \quad \text{ja} \quad \left(\bigcap_{\alpha \in \mathcal{I}} A_\alpha \right)' = \bigcup_{\alpha \in \mathcal{I}} A_\alpha'.$$

3.7 Hulkade otsekorutis

Selleks, et defineerida keerulisemaid matemaatika struktuure, on tingimata vaja nn järjestatud paare (a, b) , kus $a \in A$ ja $b \in B$ ning A ja B võivad olla suvalised hulgad.

Definitsioon 3.50

Hulkade A ja B **otsekorutiseks** ehk **Descartes'i korutiseks** (ingl *Cartesian product*) nimetatakse kõikide paaride (a, b) hulka, kus $a \in A$ ja $b \in B$, seejuures elementide järjekord on oluline.

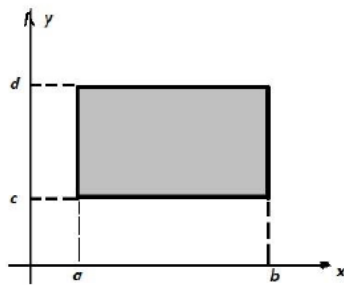
Hulkade A ja B otsekorutist tähistatakse sümboliga $A \times B$. Seega

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Õeldakse ka, et $A \times B$ on kõigi järjestatud paaride (a, b) hulk, kus $a \in A$, $b \in B$. Sõna „järjestatud” tähendab siin asjaolu, et kaht paari loetakse võrdseks siis ja ainult siis, kui nende vastavad elemendid on võrdsed, st

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d.$$

Otsekorutist $A \times A$ nimetatakse ka hulga A **otseruuduks** ja tähistatakse A^2 . Meile tuttavana võime ka koordinaattasandit vaadelda reaalarvude hulga $\mathbb{R}$ ruuduna: $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.



Näide 3.51. Ristkülikut $R = \{(x, y) : a \leq x \leq b, c \leq y \leq d\}$ võime esitada lõikude $[a, b]$ ja $[c, d]$ otsekorrutisena $R = [a, b] \times [c, d]$.

Näide 3.52. Kui $A = \{a, b, c, d, e, f, g, h\}$ ja $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$, siis otsekorrutist $A \times B = \{(a, 1), \dots, (h, 8)\}$ võib vaadelda kui malelaua ruudustikku (males kirjutatakse lühemalt $a1, \dots, h8$).

Peaks olema pikemata selge, et hulkade otsekorrutamine pole üldjuhul kommutatiivne, st kui $A \neq B$, siis $A \times B \neq B \times A$. Näiteks, $[1, 3] \times [4, 5] \neq [4, 5] \times [1, 3]$ (tee joonis!).

Lause 3.53

Hulkade A, B, C ja D korral, kui $A \subset B$ ja $C \subset D$, siis $A \times C \subset B \times D$.

Tõestus. Olgu A, B, C ja D sellised hulgad, et $A \subset B$ ja $C \subset D$. Peame tõestama, et $A \times C \subset B \times D$. Seega, olgu (a, c) suvaline element hulgast $A \times C$. Peame näitama, et $(a, c) \in B \times D$. Kuna $(a, c) \in A \times C$, siis $a \in A$ ja $c \in C$. Et $A \subset B$ ja $C \subset D$, siis $a \in B$ ja $c \in D$. Järelikult, $(a, c) \in B \times D$ ja seega olemegi näidanud, et $A \times C \subset B \times D$. ■

Ülesanne 3.54. Tõesta, et kui $A \neq \emptyset$ ja $B \neq \emptyset$, siis $A \times B = B \times A$ parajasti siis, kui $A = B$.

Teoreem 3.55: Otsekorrutise omadused

Hulkade A, B, C ja D jaoks kehtivad järgmised võrdused:

1. $A \times \emptyset = \emptyset$ ja $\emptyset \times A = \emptyset$;
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
3. $A \times (B \cap C) = (A \times B) \cap (A \times C)$;
4. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$;
5. $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

Tõestus. Kontrollime võrdust 2. samaväärsuste ahela abil:

$$\begin{aligned}
 (a, b) \in A \times (B \cup C) &\equiv a \in A \wedge b \in B \cup C \\
 &\equiv a \in A \wedge (b \in B \vee b \in C) \\
 &\equiv (a \in A \wedge b \in B) \vee (a \in A \wedge b \in C) \\
 &\equiv (a, b) \in A \times B \vee (a, b) \in A \times C \\
 &\equiv (a, b) \in (A \times B) \cup (A \times C).
 \end{aligned}$$

Ülejäänud võrduste kontroll teosta iseseisvalt. ■

Kahe hulga otsekorrutise mõiste on vahetult üldistatav mis tahes lõplikule arvule hulkadele. Tähistame sümboliga $(a_1, a_2, \dots, a_n)$ n -järjendit st n elemendi järjestatud hulka. Hulkade $A_1, \dots, A_n$ **otsekorrutiseks** $A_1 \times \dots \times A_n$ nimetatakse hulka kõigist n -järjenditest, mille elemendid on vastavatest hulkadest, st

$$A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) : a_1 \in A_1, \dots, a_n \in A_n\}.$$

Otsekorrutist $\underbrace{A \times \dots \times A}_n$ tähistatakse A^n ja nimetatakse hulga A **n -daks otseastmeks**.

Kui hulgas A on m elementi ja hulgas B on n elementi, siis hulgas $A \times B$ on $m \cdot n$ elementi. Üldisemalt, kui A_1 koosneb m_1 elemendist, ..., A_n koosneb m_n elemendist, siis $A_1 \times \dots \times A_n$ koosneb $m_1 \cdot \dots \cdot m_n$ elemendist.

Ülesanne 3.56. Olgu $n \in \mathbb{N}$. Tõestada, et kui $A_i \neq \emptyset$ ja $B_i \neq \emptyset$ ($i = 1, \dots, n$), siis

1. $A_1 \times \dots \times A_n \subset B_1 \times \dots \times B_n$ parajasti siis, kui $A_1 \subset B_1, \dots, A_n \subset B_n$;
2. $A_1 \times \dots \times A_n = B_1 \times \dots \times B_n$ parajasti siis, kui $A_1 = B_1, \dots, A_n = B_n$.

Arvuteooria elemente ja matemaatiline induktsioon

*Matemaatika nõuab kainet pead,
sest matemaatika on ju ise nagu
üks klaas viina teise järele –
A. H. Tammsaare*

4.1	Jaguvus ja algarvud	57
4.2	Matemaatiline induktsioon	60
4.3	Tugev matemaatiline induktsioon	67

4.1 Jaguvus ja algarvud

Definitsioon 4.1

Öeldakse, et täisarv a **jagab** (ingl *divides*) täisarvu b (ja tähistatakse $a \mid b$), kui leidub selline täisarv c , et $ac = b$.

Fakti, et $a \mid b$ võib tähistada ka kujul $b : a$ ehk arv b jagub arvuga a .

Näide 4.2. $3 \mid 15$, sest $3 \cdot 5 = 15$.

Täisarvude jaguvusseosel on järgmised omadused.

Lause 4.3: Jaguvuse omadused

Olgu a, b ja c täisarvud. Siis

1. $a \mid a$
2. Kui $a \mid b$ ja $b \mid c$, siis $a \mid c$.
3. Kui $a \mid b$ ja $a \mid c$, siis $a \mid (b \pm c)$
4. Kui $a \mid b$, siis $ac \mid bc$ iga $c \in \mathbb{Z}$ korral.
5. $a \mid 1$ parajasti siis, kui $a = 1$ või $a = -1$.

Tõestus. Tõestame omaduse 2., ülejäänud omadused saab tõestada analoogiliselt.

Olgu $a, b, c \in \mathbb{Z}$ sellised täisarvud, et $a \mid b$ ja $b \mid c$. Kuna $a \mid b$, siis leidub $m \in \mathbb{Z}$ nii, et $b = am$. Sarnaselt leidub $n \in \mathbb{Z}$ nii, et $c = bn$. Nüüd saamegi, et

$$c = bn = (am) \cdot n = a \cdot (mn).$$

Kuna $mn \in \mathbb{Z}$, siis olemegi näidanud, et $a \mid c$. ■

Järgnevalt esitame täisarvude jäägiga jaguvuse põhitulemuse.

Teoreem 4.4

Olgu a täisarv ja b naturaalarv. Siis leiduvad üheselt määratud täisarvud q (jagatis) ja r (jääk) nii, et

$$a = bq + r \quad \text{ja} \quad 0 \leq r < b.$$

Teoreemi tõestuses kasutame järgmist abitulemust

Lemma 4.5

Mis tahes täisarvu a korral $a^2 + a \geq 0$.

Tõestus. Olgu $a \in \mathbb{Z}$. Kuna a on täisarv, siis piisab vaadelda kahte juhtu, kui $a \geq 0$ ja kui $a < 0$. Esimesel juhul on selge, et $a^2 + a \geq 0$, sest $a \geq 0$ ja $a^2 \geq 0$. Teiseks, kui nüüd aga $a < 0$, siis $a \leq -1$, sest $a \in \mathbb{Z}$. Kuna $a + 1 \leq 0$, siis $a^2 + a = a(a + 1) \geq 0$. Kokkuvõttes olemegi näidanud, et iga täisarvu a korral $a^2 + a \geq 0$. ■

Nüüd oleme valmis esitama jäägiga jaguvuse tulemuse tõestuse.

Teoreemi tõestus. Olgu antud $a \in \mathbb{Z}$ ja $b \in \mathbb{N}$. Vaatleme hulka

$$A = \{a - bx \mid x \in \mathbb{Z}, a - bx \geq 0\} \subset \mathbb{N} \cup \{0\}.$$

Esmalt paneme tähele, et $A \neq \emptyset$. Tõepoolest,

$$a - b(-a^2) = a + ba^2 \geq a + a^2 \geq 0,$$

kus viimane võrratus kehtib lemma 4.5 põhjal ja seega $a - b(-a^2) \in A$. Kuna hulga $\mathbb{N} \cup \{0\}$ igas mittetühjas alamhulgas leidub vähim element, siis leidub ka hulga A vähim element $r = a - bq \in A$, kus $q \in \mathbb{Z}$.

Näitame, et $r < b$. Selleks oletame vastuväiteliselt, et $r \geq b$. Tähistame $r' := r - b$, siis

$$0 \leq r' = r - b = a - b(q + 1) \in A \quad \text{ja} \quad r' < r,$$

mis on vastuolus r valikuga. Niiviisi oleme leidnud sellised $q, r \in \mathbb{Z}$, et $a = bq + r$ ja $0 \leq r < b$.

Näitame, et q ja r on üheselt määratud. Selleks oletame, et leiduvad täisarvud q_1, q_2, r_1, r_2 nii, et

$$a = bq_1 + r_1 = bq_2 + r_2 \quad \text{ja} \quad 0 \leq r_1, r_2 < b.$$

Siis $b(q_1 - q_2) = r_2 - r_1$. Kuna $b \geq 1$, $|r_2 - r_1| < b$ ja $q_1 - q_2 \in \mathbb{Z}$, siis võrdusest $|r_2 - r_1| = |b| \cdot |q_1 - q_2|$ järeldub, et $q_1 - q_2 = 0$ ja seega ka $r_2 - r_1 = 0$. Sellega olemegi näidanud, et $q_1 = q_2$ ja $r_1 = r_2$. ■

Definitsioon 4.6

Algarvuks (ingl *prime*) nimetatakse ühest suuremat naturaalarvu p , mille ainsad naturaalarvulised jagajad on 1 ja p . Naturaalarvu, mis on suurem kui 1 ja mis pole algarv, nimetatakse **kordarvuks** (ingl *composite*).

Sõnastame nüüd aritmeetika põhiteoreemi, millele tugineb suur osa naturaalarvude aritmeetikas tõestatatavatest teoreemidest ja mis pärineb Eukleidese (u 350 eKr) „Elementide” IX raamatust. Teoreemi tõestuse jätame paragrahvi 4.3, sest see vajab (tugeva) matemaatilise induktsiooni meetodit.

Teoreem 4.7: Aritmeetika põhiteoreem

Iga naturaalarvu $n \geq 2$ saab esitada algarvude korrutisena (st leiduvad $r \in \mathbb{N}$ ja algarvud $p_1, \dots, p_r$ nii, et $n = p_1 \cdot \dots \cdot p_r$) ning see esitus on ühene tegurite järjekorra täpsuseni.

Teoreem 4.8: Eukleides

Algarvude hulk on lõpmatu.

Tõestus. Olgu algarvud tähistatud $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots$. Oletame vastuväiteliselt, et leidub suurim algarv p_n . Vaatleme naturaalarvu $a = p_1 p_2 \dots p_n + 1$. Et $a > 1$, siis aritmeetika põhiteoreemi põhjal leidub algarv, mis arvu a jagab. Kuna oletasime, et $p_1, p_2, \dots, p_n$ on ainsad algarvud, siis peab leiduma selline $i \in \{1, \dots, n\}$, et $p_i \mid a$. Et $p_i \mid a$ ja $p_i \mid p_i$, siis lause 4.3 omaduse 3 põhjal saame, et $p_i \mid a - p_1 p_2 \dots p_n$ ehk $p_i \mid 1$, mis on vastuolus sellega, et $p_i > 1$. ■

Järgnevalt sõnastame Eukleidese lemma ja selle järelduse, mida me ei tõesta.

Lemma 4.9: Eukleides

Mistahes $a, b, c \in \mathbb{Z}$ korral, kui $a \mid bc$ ja $\text{SÜT}(a, b) = 1$, siis $a \mid c$.

Järeldus 4.10

Kui $p, q_1, q_2, \dots, q_n$ on algarvud ja $p \mid q_1 q_2 \dots q_n$, siis leidub selline $k \in \{1, 2, \dots, n\}$, et $p = q_k$.

4.2 Matemaatiline induktsioon

Me kõik arvame, et tunneme naturaalarve hästi ja et meil on selged mitmed naturaalarvude omadused. Näiteks teame, et naturaalarve saab lahutada algtegurite korrutiseks või et summa ei sõltu liidetavate järjekorrast jne. Tegelikult on naturaalarvude hulk oma sisult aga palju rikkam ning isegi kaasaegsed matemaatikud ei tunne veel kõiki naturaalarvude omadusi. Näiteks pole teada, kas üle ühe paiknevate algarvude paaride, nn algarvude kaksikute hulk 3 ja 5, 5 ja 7, 11 ja 13, 17 ja 19, 29 ja 31, 41 ja 43, 59 ja 61, 71 ja 73, 101 ja 103 jne on lõplik või lõpmatu. Lahendamata probleeme naturaalarvude vallas võib välja tuua teisigi.

Meie tutvume siinses peatükis naturaalarvude järgnevuse omadusega, mis ütleb, et igale naturaalarvule järgneb naturaalarv. Täpsemalt, igale naturaalarvule saab vahetult järgneda ainult üks naturaalarv. Järgnevuse omadus on naturaalarvude suhtes üks olulisemaid omadusi ja seetõttu on järgnevuse omadus koos järgnevuse ühesusega naturaalarvude teooria ülesehitamisel üheks aksioomiks. See omadus väljendab naturaalarvude olemust, mis seisnebki järgnevuses. Lisaks peegeldab järgnevuse omadus ka naturaalarvude järjestatust suuruse järgi ja asjaolu, et naturaalarvude järjend on lõpmatu. Aksioomiks on ka naturaalarvu 1 olemasolu, sest järgnevuse omadust saab kasutada alles siis, kui midagi on algselt olemas, millest alustada.

Naturaalarvude kohta käivaid väiteid ei saa tõestada kontrollimise teel, sest naturaalarvude hulk on lõpmatu. Seega on vaja mingit tõestamismeetodit, mis naturaalarvudega tegelemisel nõuaks ja kasutaks järgnevuse omadust. Kehtib järgmine väide (aksioom): **kui mingi naturaalarvude hulk sisaldab arvu 1 ja selles kehtib järgnevuse omadus, siis see hulk sisaldab kõiki naturaalarve**. Tänu sellele väitele saame nüüd naturaalarvude kohta käivaid väiteid tõestada lõpliku arvu sammudega.

Esiteks, tuleb näidata, et väide kehtib naturaalarvu 1 korral. Seda saab teha kontrollimise teel.

Teiseks, tuleb näidata, et väitel on järgnevuse omadus. Kui see on näidatud, on meil õigus kolmandaks üldistada väide kõikidele naturaalarvudele.

Sageli ülesannete lahendamisel matemaatilise induktsiooni meetodi abil tuleb eelnevalt püstitada väidete seeria, lähtudes ülesande sisust.

Üldistamist üksikjuhult üldjuhule nimetatakse *induktsiooniks*. Filosoofias on induktsioon arutlemise viis, mille puhul sellest, et ühtedel asjadel on teatav omadus, järeldatakse, et see omadus on ka mõnel teisel asjal või isegi kõikidel samalaadsetel asjadel. Induktsiooniks nimetatakse seal ka induktiivse arutluse esitamist. Erinevalt deduktsioonist ei taga aga induktsioon üldjuhul seda, et kui eeldused on tõesed, siis ka järeldus on tõene, mis tähendab, et üldistuse õigsus jääb tõestamata. Meie jaoks on siiski väga oluline, et tõesed eeldused tagaksid ka tõese järelduse, ja seda võimaldab meile matemaatiline induktsioon. Käesolevas peatükis vaatamegi veel ühte tõestusmeetodit – *matemaatilist induktsiooni* – mis täiendab harilikku induktsiooni, vältides valesid üldistusi. Kuigi nimetus sisaldab sõna „induktsioon“, on siiski tegemist deduktiivse tõestamise vormiga.

Alustame näitega probleemist, mille tõestamiseks läheb vaja matemaatilist induktsiooni.

Väide. Esimese n paaritu arvu summa on n^2 .

Illustreerime seda väidet tabeliga:

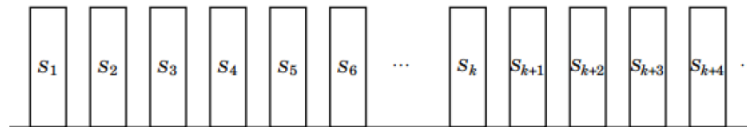
n	n esimese paaritu arvu summa	n^2
1	$1 =$	1
2	$1 + 3 =$	4
3	$1 + 3 + 5 =$	9
4	$1 + 3 + 5 + 7 =$	16
5	$1 + 3 + 5 + 7 + 9 =$	25
$\vdots$	$\vdots$	$\vdots$
n	$1 + 3 + 5 + 7 + 9 + 11 + \cdots + (2n - 1) =$	n^2
$\vdots$	$\vdots$	$\vdots$

Pane tähele, et esimeses viies reas on tõesti nii, et n esimese paaritu arvu summa on n^2 . Samuti tasub märgata, et iga rea viimane liidetav on esitatav kujul $2n-1$ (st, kui $n = 2$, siis teise rea viimane liidetav on $2 \cdot 2 - 1 = 3$; kui $n = 3$, kolmas paaritu arv summas on $2 \cdot 3 - 1 = 5$ jne). Aga siiski jääb õhku rippuma küsimus, et kas tõesti $1 + 3 + 5 + 7 + 9 + 11 + \cdots + (2n - 1)$ on võrdne arvuga n^2 ? Kas meie väide on tõene kõigi naturaalarvude korral? Sõnastame oma väite ümber järgmiselt. Iga naturaalarvu n korral (tabelis iga rea korral) olgu meil antud väited S_n järgmiselt:

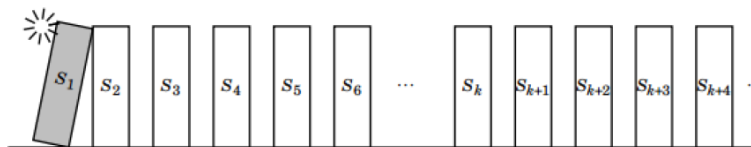
$$\begin{aligned}
 S_1: & 1 = 1^2 \\
 S_2: & 1 + 3 = 2^2 \\
 S_3: & 1 + 3 + 5 = 3^2 \\
 & \vdots \\
 S_n: & 1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2 \\
 & \vdots
 \end{aligned}$$

Küsimine: kas kõik need väited on tõesed?

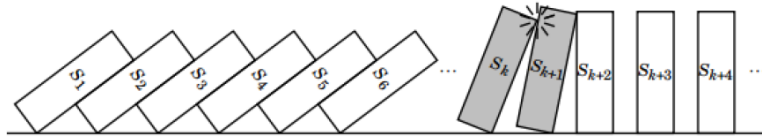
Matemaatiline induktsioon ongi mõeldud just seda tüüpi küsimuste vastamiseks, kus meil on antud terve hulk väiteid $S_1, S_2, \dots, S_n, \dots$ ja me peame tõestama, et kõik need väited on tõesed. Meetod on tegelikult väga lihtne ja meetodi iseloomustamiseks mõtle pikale reale doominotele, mis üksteise kõrvale püsti on laotud. Oletame, et sa suudad ära tõestada (kontrollida) esimese väite. Sellele vastab esimese doomino ümber lükkamine. Lisaks oletame, et sa suudad näidata, et kui väide S_k on tõene (vastav doomino kukub), siis see sunnib järgmise väite S_{k+1} olema tõene (järgmise doomino kukkuma). Seega, nüüd, kui doomino S_1 kukub, ajab ta ümber järgmise doomino S_2 , mis omakorda lükkab ümber doomino S_3 , kukkudes ajab doomino S_3 ümber doomino S_4 jne. Meil ei jää lõpuks midagi muud üle, kui tõdeda, et kõik väited on tõesed (ehk kõik doominod ümber lükatud).



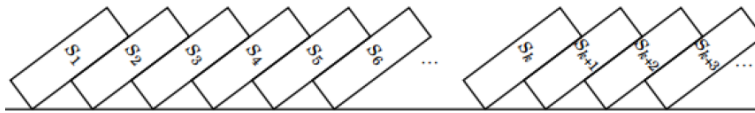
Joonis 4.1: Väited on reastatud nagu doominod.



Joonis 4.2: Oletame, et esimene väide on tõestatud (esimene doomino lükatakse ümber).



Joonis 4.3: Oletame, et doomino S_k põhjustab alati doomino S_{k+1} ümberkukkumise.



Joonis 4.4: Kõik doominod peavad kukkuma (ehk kõik väited peavad kehtima).

Eelnev arutelu annab meile sammud, mis on vajalikud matemaatilise induktsiooni tõestusmeetodi läbiviimiseks.

Teoreem 4.11: Matemaatilise induktsiooni printsiip

Olgu $S(n)$ predikaat, kus muutuja n saab naturaalarvulisi väärtusi. Kui

1. $S(1)$ on tõene (*induktsiooni baas*),
2. iga naturaalarvu k korral, kui $S(k)$ on tõene, siis ka $S(k + 1)$ on tõene (*induktsiooni samm*),

siis väide $S(n)$ on tõene iga naturaalarvu n korral.

Märkus 4.12

1. Pole oluline, et kõige esimene väide, mida kontrollitakse, vastab naturaalarvule 1. Piisab, kui väide kehtib mingi naturaalarvu korral ning üldistamine toimub sellele arvule järgnevatele arvudele.
2. Matemaatilist induktsiooni saab rakendada ainult siis, kui mõlemad eeldused (induktsiooni baas ja induktsiooni samm) on rahuldatud.

Näide 4.13. Tõesta matemaatilise induktsiooni abil, et n esimese naturaalarvu summa võrdub avaldise $\frac{n(n+1)}{2}$ väärtusega, so

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}, \quad \text{iga } n \geq 1 \text{ korral.}$$

Tõestus. Kuna valemi kehtivus sõltub naturaalarvust, saame tõestamiseks kasutada matemaatilist induktsiooni. Selleks tähistame sümboliga $S(n)$ predikaati $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$, kus $n \in \mathbb{N}$.

1. Induktsiooni baas. Kuna $1 = \frac{1(1+1)}{2}$, siis $S(1)$ on tõene.
2. Induktsiooni samm. Olgu $k \in \mathbb{N}$ ja oletame, et $S(k)$ on tõeneb. Peame näitama, et siis on tõene ka $S(k+1)$, st $1+2+3+\dots+k+k+1 = \frac{(k+1)(k+2)}{2}$. Selle võrduse tõestamiseks lähtume väite vasakust poolest ja püüame selle teisendada väite paremaks pooleks. Teisendamise käigus kasutame oma eeldust, et $S(k)$ kehtib.

$$\begin{aligned} \underbrace{1 + 2 + 3 + \dots + k}_{\text{eeldus}} + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}. \end{aligned}$$

Seega näitasime, et ka $S(k+1)$ kehtib. Matemaatilise induktsiooni printsiibi põhjal järeldub, et $S(n)$ kehtib iga naturaalarvu n korral. ■

Tõestame nüüd sissejuhatuses tutvustatud väite n esimese paaritu arvu summa kohta.

Näide 4.14. Tõesta matemaatilise induktsiooni abil, et n esimese paaritu naturaalarvu summa on n^2 .

Tõestus. Olgu $S(n)$ predikaat $1 + 3 + 5 + \dots + (2n-1) = n^2$, kus $n \in \mathbb{N}$.

1. Kuna $1 = 1^2$, siis $S(1)$ kehtib.
2. Olgu $k \in \mathbb{N}$. Eeldame nüüd, et $S(k)$ kehtib, st $1 + 3 + 5 + \dots + (2k - 1) = k^2$. Näitame, et siis ka $S(k + 1)$ kehtib. Tõepoolest,

$$\begin{aligned} & \underbrace{1 + 3 + 5 + \dots + (2k - 1)}_{\text{eeldus}} + (2(k + 1) - 1) = k^2 + (2(k + 1) - 1) \\ & = k^2 + 2k + 1 = (k + 1)^2. \end{aligned}$$

Seega oleme matemaatilise induktsiooni abil tõestanud, et valem kehtib kõigi naturaalarvude korral. ■

Näide 4.15. Tõesta, et kõigi naturaalarvude korral jagub avaldis $2^{2n} - 1$ kolmega.

Tõestus. Olgu $S(n)$ predikaat $3 \mid 2^{2n} - 1$, kus $n \in \mathbb{N}$.

1. Näitame esmalt, et $S(1)$ kehtib. Kuna $2^{2 \cdot 1} - 1 = 4 - 1 = 3$ ja $3 \mid 3$, siis $S(1)$ on tõene.
2. Olgu $k \in \mathbb{N}$. Eeldame, et $S(k)$ kehtib, st $3 \mid 2^{2k} - 1$. Tõestame, et siis kehtib ka $S(k + 1)$. Paneme tähele, et

$$\begin{aligned} 2^{2(k+1)} - 1 &= 2^{2k+2} - 1 = 2^{2k} \cdot 4 - 1 = 2^{2k} \cdot (1 + 3) - 1 \\ &= 2^{2k} \cdot 1 + 2^{2k} \cdot 3 - 1 = 2^{2k} \cdot 1 - 1 + 2^{2k} \cdot 3. \end{aligned}$$

Saadud avaldis jagub kolmega, sest eelduse põhjal $3 \mid 2^{2k} - 1$ ja $3 \mid 2^{2k} \cdot 3$. Järelikult, $3 \mid 2^{2(k+1)} - 1$ ehk kehtib ka $S(k + 1)$.

Oleme seega matemaatilise induktsiooni abil tõestanud, et kõigi naturaalarvude korral jagub avaldis $2^{2n} - 1$ kolmega. ■

Näide 4.16. (Geomeetrilise jada n esimese liikme summa valem.) Tõesta matemaatilise induktsiooni abil, et $a, r \in \mathbb{R}$ ja $|r| < 1$ korral

$$a + ar + ar^2 + ar^3 + \dots + ar^n = \frac{a(1 - r^{n+1})}{1 - r} \quad \text{iga } n \geq 0 \text{ korral.}$$

Tõestus. Iseseisvalt. ■

Näide 4.17. Tõesta, et $n \geq 1$ korral

$$1 + \frac{1}{2} + \dots + \frac{1}{2^{n-1}} < 2.$$

Tõestus. Kasutame näidet 4.16 võttes seal $a = 1$ ja $r = \frac{1}{2}$. Siis

$$1 + \frac{1}{2} + \dots + \frac{1}{2^{n-1}} = 1 \cdot \frac{1 - \left(\frac{1}{2}\right)^n}{1 - \frac{1}{2}} = 2 \cdot \left(1 - \left(\frac{1}{2}\right)^n\right) = 2 - \frac{1}{2^{n-1}} < 2.$$

Näide 4.18. (Aritmeetilise jada n esimese liikme summa valem.) Tõesta matemaatilise induktsiooni abil, et

$$\sum_{k=1}^n (a + (k - 1)d) = \frac{n}{2}(2a + (n - 1)d) \quad \text{iga } n \geq 1 \text{ korral.}$$

Tõestus. Iseseisvalt. ■

Peatüki alguse poole märkisime, et matemaatilist induktsiooni saab rakendada ainult siis, kui mõlemad eeldused (induktsiooni baas ja induktsiooni samm) on rahuldatud. Toome siinjuures kaks näidet olukordadest, kus ainult üks eeldustest on rahuldatud, mistõttu matemaatilist induktsiooni tulemuse tõestamiseks kasutada ei saa. Alustame meile juba tuttavast väitest.

Näide 4.19. Iga naturaalarvu n korral on $n^2 + n + 41$ algarv.

„**Tõestus**“. Alustame induktsiooni baasist ja kontrollime väidet $n = 1$ korral: $1^2 + 1 + 41 = 43$, mis on algarv. Veelgi enam osutub, et $n^2 + n + 41$ on algarv iga $n = 1, 2, \dots, 39$ korral. Järgmiseks oletame, et väide kehtib $n = k$ korral, s.t $k^2 + k + 41$ on algarv. Püüame tõestada, et siis ka $(k+1)^2 + (k+1) + 41$ on algarv. Sellega jääme aga jänni ning tõestamine ei õnnestu. Tegelikult teame, et juba väärtusel $n = 40$ on $40^2 + 40 + 41 = 40(40 + 1) + 41 = 41(40 + 1) = 41^2$ hoopis kordarv. Vaadeldud näide hoiatab kergekäeliste üldistuste tegemise eest. Siin küll kehtis induktsiooni baas, aga ei olnud võimalik näidata induktsiooni sammu kehtivust. Seega väide oli vale. ■



Järgmisena toome näite induktsiooni valest kasutamisest, mille autor on ungari matemaatik G. Pólya (1954).

Näide 4.20. Kõik hobused on ühte värvi.

„**Tõestus**“. Olgu $S(k)$ predikaat „igas karjas, kus on k hobust, on nad kõik sama värvi.“

1. **Induktsiooni baas:** Kuna üks hobune on iseendaga sama värvi, siis $S(1)$ kehtib.
2. **Induktsiooni samm:**

Eeldame, et $S(k)$ on tõene, st igas karjas, kus on k hobust, on nad sama värvi. Vaatleme nüüd karja, kus on $k + 1$ hobust. Eelduse kohaselt on esimesed k hobust sama värvi.

$$\underbrace{h_1, h_2, \dots, h_k}_{\text{sama värvi}}, h_{k+1}$$

Eelduse kohaselt on ka viimased k hobust sama värvi.

$$h_1, \underbrace{h_2, \dots, h_k, h_{k+1}}_{\text{sama värvi}}$$

Seega kõik hobused $h_1, h_2, \dots, h_k, h_{k+1}$ peavad olema sama värvi ehk $S(k) \Rightarrow S(k+1)$ on tõene.

Matemaatilise induktsiooni põhjal on kõik hobused ühte värvi. ■

Ülesanne 4.21. Kus on näite 4.20 tõestuses vigane arutlus?

Matemaatilise induktsiooni printsiipi saab rakendada ka predikaatidele, mille muutujad saavad väärtusi täisarvude hulgast.

George Pólya
(1887–1985)

Teoreem 4.22: Üldine matemaatilise induktsiooni printsiip

Olgu $S(k)$ predikaat, kus muutuja k saab täisarvulisi väärtusi. Kui

1. leidub $k_0 \in \mathbb{Z}$ nii, et $S(k_0)$ on tõene (*induktsiooni baas*),
2. iga $k \geq k_0$ korral, kui $S(k)$ on tõene, siis ka $S(k+1)$ on tõene (*induktsiooni samm*),

siis väide $S(k)$ on tõene iga $k \geq k_0$ korral.

4.3 Tugev matemaatiline induktsioon

Mõnikord võib ette tulla olukord, kus on raske otse tõestada, et väite $S(k)$ kehtivusest järeldub väide $S(k+1)$. Pigem leiad, et on vajadus kasutada mõnda varasemat väidet $S(i)$ ($i < k$), et näidata $S(k+1)$ kehtivust. Sellistes olukordades on võimalik kasutada hari-liku matemaatilise induktsiooni natukene muudetud varianti, mida kutsutakse tugevaks matemaatilise induktsiooni printsiibiks ja mis kõlab järgmiselt.

Teoreem 4.23: Tugeva matemaatilise induktsiooni printsiip

Olgu $S(n)$ predikaat, kus muutuja n saab naturaalarvulisi väärtusi. Kui

1. $S(1)$ on tõene (*induktsiooni baas*),
2. iga naturaalarvu m korral, kui iga $1 \leq k \leq m$ korral $S(k)$ on tõene, siis $S(m+1)$ on tõene (*induktsiooni samm*),

siis väide $S(n)$ on tõene iga naturaalarvu n korral.

Märkus 4.24

Tugeva induktsiooni baasi kehtivuse kontrollimisel on mõnikord vaja tõestada lisaks esimesele väitele veel mõned järgnevad väited (vaata näiteks lause 4.31).

Erinevus tavalise matemaatilise induktsiooni printsiibiga on selles, et nüüd järeldub $S(k+1)$ kehtimine kõigist eelnevatest väidetest $S(1), \dots, S(k)$, ehk meil on rohkem induktsiooni eeldusi, millest induktsiooni sammu tõestada. Kui tavalise matemaatilise induktsiooni korral me eeldasime, et $S(k)$ on tõene ja selle abil näitasime, et $S(k+1)$ peab olema tõene, siis nüüd võime eeldada, et $S(1), \dots, S(k)$ on kõik tõesed ja kasutada neid kõiki tõestamiseks, et $S(k+1)$ on tõene.

Hoolimata oma nimest, on tugev matemaatiline induktsioon tegelikult sama „tugev“ kui tavaline matemaatiline induktsioon. Iga väide, mis on tõestatav tugeva matemaatilise induktsiooni abil, on tehtav ka tavalise matemaatilise induktsiooniga. Ainuke erinevus on selles, et mõningad tõestused võivad tugeva matemaatilise induktsiooni abil olla lihtsamad. Samas, kui on võimalik ainult $S(k)$ kehtivusest tõestada $S(k+1)$ kehtivus, siis tuleks kasutada tavalist matemaatilist induktsiooni.

Nüüd oskame anda ka varem võlgu jäänud aritmeetika põhiteoreemi tõestuse.

Teoreem 4.25: Aritmeetika põhiteoreem

Iga naturaalarvu $n \geq 2$ saab esitada algarvude korrutisena (st leiduvad $r \in \mathbb{N}$ ja algarvud $p_1, \dots, p_r$ nii, et $n = p_1 \cdot \dots \cdot p_r$) ning see esitus on ühene tegurite järjekorra täpsuseni.

Märkus 4.26

Kokkuleppeliselt loetakse korrutiseks, milles tegureid pole, arvu 1. Korrutiseks, milles on vaid üks tegur, loetakse tegurit ennast. Analoogiliselt: summaks, milles on ainult üks liidetav, loetakse liidetavat ennast.

Märkus 4.27

Naturaalarvu n ühene esitus tegurite järjekorra täpsuseni algarvude korrutisena tähendab näiteks $n = 12$ puhul, et $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$ ning rohkem esitusi pole.

Teoreemi 4.25 tõestus. Näitame esmalt tugeva matemaatilise induktsiooniga, et iga naturaalarvu $n \geq 2$ saab esitada algarvude korrutisena.

Baas. Arvu $n = 2$ puhul on see väide selge. Vaata märkust 4.26.

Samm. Oletame, et $n > 2$ ja iga naturaalarvu $1 < m < n$ saab esitada algarvude korrutisena. Naturaalarv n peab olema kas algarv või kordarv. Esimesel juhul pole midagi tõestada. Kui aga n on kordarv, siis leidub naturaalarv d nii, et $d \mid n$, kusjuures $1 < d < n$ (Tõesta!). Olgu $n = da$, kus $a \in \mathbb{N}$, siis ka $1 < a < n$. Induktsiooni eelduse põhjal avalduvad d ja a algarvude korrutisena ning järelikult ka n avaldub algarvude korrutisena.

Ühesuse näitamiseks oletame, et naturaalarvu n saab algarvude korrutisena esitada kahel viisil:

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s,$$

kus üldisust kitsendamata $r \leq s$ ja algarvud p_i ja q_j on mittekahanevas järjekorras, st $p_1 \leq p_2 \leq \dots \leq p_r$ ja $q_1 \leq q_2 \leq \dots \leq q_s$. Kuna $p_1 \mid q_1 q_2 \dots q_s$ ja p_1 on algarv, siis Eukleidese lemma järelduse 4.10 põhjal $p_1 = q_k$ mingi $k \in \{1, \dots, s\}$ korral. Seega kehtib ka, et $p_1 \geq q_1$, sest $q_1 \leq q_k$. Samamoodi arutledes saame, et $q_1 \geq p_1$ ning kokkuvõttes $p_1 = q_1$. Arvu p_1 taandades saame $p_2 \dots p_r = q_2 \dots q_s$. Korrates seda mõttekäiku saame $p_2 = q_2$ ja $p_3 \dots p_r = q_3 \dots q_s$. Kui $r < s$, siis niimoodi jätkates jõuame võrduseni $1 = q_{r+1} q_{r+2} \dots q_s$, mis on aga võimatu, sest $q_i > 1$ iga $i \in \{1, \dots, s\}$ korral. Seega $r = s$ ja $p_1 = q_1, \dots, p_r = q_r$. ■

Näide 4.28. Kastide virnadesse jagamise mäng. Oletame, et meil on ühes virnas (üks-teise otsas) n kasti. Mängus teed rea samme, kus igal sammul jagad ühe virna kaheks mittetühjaks virnaks. Mäng lõpeb, kui igasse virna on jäänud vaid üks kast. Iga käigu eest saad punkte. Näiteks, kui jagad virna, milles oli $a + b$ kasti kahte virna, ühes a kasti ja

teises b kasti, siis saad selle käigu eest ab punkti. Lõplik punktisumma saadakse igal käigul kogutud punktide kokku liitmisel. Milline strateegia suurendaks sinu lõppsummat?

Teeme mängu läbi alustades 10 kastiga. Üks võimalik mängu käik oleks selline:

Virna kõrgus	Punkte
10	
5 5	25
5 3 2	6
4 3 2 1	4
2 3 2 1 2	4
2 2 2 1 2 1	2
1 2 2 1 2 1 1	1
1 1 2 1 2 1 1 1	1
1 1 1 1 2 1 1 1 1	1
1 1 1 1 1 1 1 1 1 1	1
Kokku punkte =	45 punkti

Kas sa suudaksid leida parema strateegia? Kasutame tugevat matemaatilist induktsiooni ja tõestame, et lõplik punktisumma sõltub ainult kastide arvust, mitte aga strateegiast!

Väide. Mis tahes viisil n kasti hunnikutesse jaotamisel on lõplik punktisumma alati $\frac{n(n-1)}{2}$.

Väite tõestus. Olgu $S(n)$ predikaat „ n kasti hunnikutesse jaotamisel on lõplik punktisumma alati $\frac{n(n-1)}{2}$ “.

1. Induktsiooni baas. Kui $n = 1$, siis on meil virnas vaid üks kast. Kuna mängus ühtegi sammu teha ei ole võimalik, siis on punktisummaks $\frac{1(1-1)}{2} = 0$. Seega $S(1)$ on tõene.
2. Induktsiooni samm. Olgu $k \in \mathbb{N}$. Oletame, et väited $S(1), \dots, S(k)$ on kõik tõesed. Näitame, et siis $S(k+1)$ on ka tõene. Seega, olgu meil virnas $k+1$ kasti ning esimese sammuna jagame need kastid kahte uude virna kõrgusega i ja $(k+1)-i$ kasti (mingi i korral, kus $1 \leq i \leq k$). Mängu lõppsumma moodustavad sellel esimesel käigul saadud punktide ja kõikide järgmiste käikude punktide summa. Seega

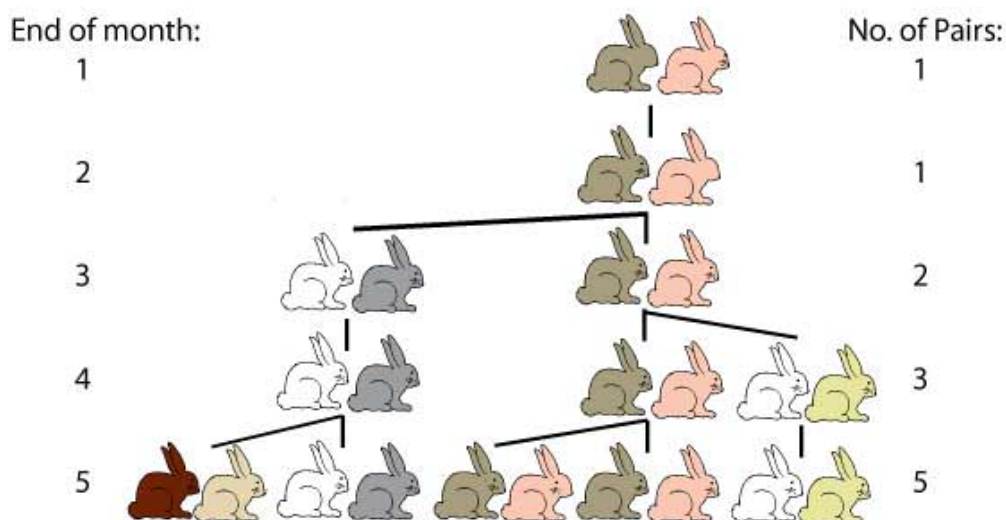
$$\begin{aligned}
 \text{lõppsumma} &= (1. \text{ käigu punktid}) + (i \text{ kasti jaotamise punktid}) \\
 &\quad + ((k+1-i) \text{ kasti jaotamise punktid}) \\
 &= i(k+1-i) + \frac{i(i-1)}{2} + \frac{(k+1-i)(k+1-i-1)}{2} \\
 &= \frac{k^2 + k}{2} = \frac{k(k+1)}{2}.
 \end{aligned}$$

Teisel sammul kasutasime eeldusi väidete $S(i)$ ja $S(k+1-i)$ kohta ning ülejäänud oli lihtsustamine. Seega näitasime, et suvalise k korral väidetest $S(1), \dots, S(k)$ järeldub väide $S(k+1)$, millega oleme tõestanud meie üldise väite tugeva matemaatilise induktsiooni abil. ■

Itaalia matemaatik Leonardo Fibonacci (u 1175 – u 1250), keda peetakse keskaja üheks silmapaistvaimaks matemaatikuks, vaatles oma 1202. aastal avaldatud teoses „Liber abaci“ järgmist ülesannet.



Leonardo Fibonacci (u 1170–1250)



Ülesanne 4.29. Talunikul on üks paar vastsündinud jäneseid, isane ja emane. Ühe kuu pärast sünnist alates muutuvad jäneseid paaritumisvõimeliseks ning kaks kuud pärast sünni annab emane jänes ühe paari järglasi. Eeldame, et ükski jänes ei sure ning et emane jänes annab uue paari, isase ja emase, igal kuul, alates kahe kuu vanuseks saamisest. Mitu paari jäneseid on talunikul n -ndal kuul?

Olgu F_n paaride arv n -ndal kuul. Siis järgmisel kuul on talunikul olemas kõik need jäneseid, kes tal olid n -ndal kuul, uusi paare lisandub aga parajasti niipalju, kuipalju oli paare eelmisel, $(n - 1)$ -l kuul, sest need on järgmisel kuul kõik vähemalt kaks kuud vanad ja annavad igaüks ühe uue paari järglasi. Niisiis kehtib võrdus

$$F_{n+1} = F_n + F_{n-1}$$

Olgu $F_0 = 0$ ja $F_1 = 1$. Siis $F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, \dots$

Definitsioon 4.30

Arve $F_0, F_1, F_2, \dots$, kus $F_0 = 0$ ja $F_1 = 1$ ning iga naturaalarvu n korral $F_{n+1} = F_n + F_{n-1}$ nimetatakse **Fibonacci arvudeks** (ingl *Fibonacci numbers*).

Lause 4.31

Tõestada, et $F_n > 2n$ iga $n \geq 8$ korral.

Tõestus. Näitame selle väite kehtivust tugeva matemaatilise induktsiooni abil. Olgu $S(n)$ predikaat $F_n > 2n$, kus $n \geq 8$.

1. Induktsiooni baas. Kui $n = 8$, siis $F_8 = 21 > 2 \cdot 8 = 16$. Seega $S(8)$ kehtib. Kui $n = 9$, siis $F_9 = 34 > 2 \cdot 9 = 18$. Järelikult, ka $S(9)$ kehtib.

2. Induktsiooni samm. Eeldame nüüd, et $S(m)$ on tõene, st $F_m > 2m$, iga $m \in \{8, \dots, n\}$ korral. Me peame näitama, et $F_{n+1} > 2(n+1)$. Induktsiooni eelduse ja seose $F_{n+1} = F_n + F_{n-1}$ abil saame

$$F_{n+1} = F_n + F_{n-1} > 2n + 2(n-1) = 4n - 2.$$

Viimaks paneme tähele, et võrratus $4n-2 > 2n+2$ on samaväärne võrratusega $n > 2$, mis loomulikult kehtib, sest $n \geq 8$. Seega ka $S(n+1)$ on tõene ja matemaatilise induktsiooni printsiibi põhjal $S(n)$ kehtib iga $n \geq 8$ korral.

■

Ka tugevat matemaatilise induktsiooni printsiipi saab rakendada predikaatidele, mille muutujad saavad väärtusi täisarvude hulgast.

Teoreem 4.32: Üldine tugeva matemaatilise induktsiooni printsiip

Olgu $S(k)$ predikaat, kus muutuja k saab täisarvulisi väärtusi. Kui

1. leidub $k_0 \in \mathbb{Z}$ nii, et $S(k_0)$ on tõene (*induktsiooni baas*),
2. iga $k \geq k_0$ korral, kui iga $k_0 \leq l \leq k$ korral $S(l)$ on tõene, siis $S(k+1)$ on tõene (*induktsiooni samm*),

siis väide $S(k)$ on tõene iga $k \geq k_0$ korral.

Tõestamise erinevad meetodid

*Siin on minu tulemus, kuid ma ei
tea veel, kuidas temani jõuda –
C. F. Gauss*

5.1	Pólya printsiibid	75
5.2	Induktiivne ja deduktiivne järeldamine	75
5.3	Tõestamine	76
5.4	Otsene tõestus	77
5.5	Tõestus alamjuhtude põhjal	78
5.6	Kontrapositiivne tõestus	79
5.7	Vastuväiteline tõestus	79
5.8	Samaväärsete tingimuste ehk ekvivalentsi tõestamine	81
5.9	Mitme samaväärse tingimuse tõestamine	82
5.10	Olemasolu ja ühesuse tõestus	83
	5.10.1 Konstruktiivne olemasolu tõestus	83
	5.10.2 Mittekonstruktiivne olemasolu tõestus	84
5.11	Oletused ehk hüpoteesid	85
5.12	Ümberlükkamised ehk kontranäited	86
5.13	Miks õpetada tõestamist?	87
5.14	Näpunäiteid tõestuse kirjutamiseks	87

Kõikidele loodusteadustele on iseloomulik, et tulemuste saavutamiseks tehakse vaatlusi ja katseid. Matemaatikas ei tehta vaatlusi ega katseid, vaid tulemused saadakse rangete loogiliste arutluste abil, mida nimetatakse **tõestusteks**.

Matemaatikas on teatud arv põhimõisteid ja põhitõdesid, mida ei tõestata. Põhitõdesid, mida ei tõestata ja mida eeldatakse tõesed olevat, nimetatakse **aksioomideks**. Ülejäänud valemid ja tulemused sõnastatakse lausetena, mida nimetatakse teoreemideks. **Teoreem** on lause, mille õigsust tõestatakse range loogilise arutluse abil. Teoreemis esitatud väite õigsust tõestatakse aksioomidest ja varem tõestatud teoreemidest lähtudes.



Aksiomaatilise meetodi alusepanija on **Eukleides** (325 – 265 eKr), kes süstematiseeris oma teoses „Elemendid“ sellisel viisil toleaege matemaatika. Eukleides esitas täpse ja loogiliselt tervikliku geomeetrilise süsteemi, mida nimetatakse „eukleidiliseks geomeetriaks“. Selle süsteemi aluseks on definitsioonid ning aksioomid ja postulaadid (Eukleides eristas aksioome ja postulaate, kuid kaasaegses mõttes on need kõik aksioomid) ja nendest tuletas ta ülejäänud teoreemid. Aksioome pidas ta ilmseteks tõdedeks. Pikka aega (2000 aastat) tegelesid matemaatikud paralleelide aksioomi probleemiga, püüdes tõestada, et seda saab tuletada teistest aksioomidest. Paralleelide aksioom väidab, et

läbi punkti, mis ei asu antud sirgel, saab tõmmata ainult ühe sirge, mis on paralleelne selle sirgega.

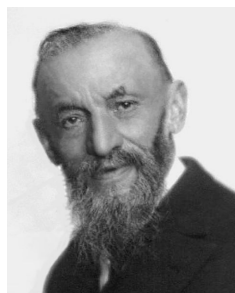
Alles XIX–XX saj. näidati, et see aksioom on tõepoolest sõltumatu teistest aksioomidest ning korrektne saab olla ka geomeetria, kus aluseks on võetud selle aksioomi eituse. Eukleidesi süsteem püsis 1820. aastani, mil silmapaistev vene matemaatik **Nikolai Lobatševski** (1792 – 1856) ja veidi hiljem ka ungari matemaatik **János Bolyai** (1802 – 1860) jõudsid paralleelide aksioomi muutes uue geomeetria avastamiseni. Teadmine, et võib üles ehitada geomeetria kui matemaatilise teooria, milles väljaspool sirget asuvat punkti läbib nendega samal tasandil rohkem kui üks sirge, mis ei lõika antud sirget või milles kolmnurkade sisenurkade summa on väiksem kui 180° , oli tollal isegi nimekatele matemaatikutele ootamatu. Tekkinud geomeetria nimetatakse **mitteeukleidiliseks geomeetriaks**. Selle loomine näitas, et aksioome võib mõista lihtsalt kui eeldusi. Eukleidesi „Elementide“ esinevate lünkade otsimine sai XIX sajandi lõpul matemaatikute üheks tähtsamaks ülesandeks. Selle ülesande lahendamise viis 1900. aastaks lõpule saksa matemaatik **David Hilbert** (1862 – 1943).

Gottlob Frege (1848 – 1925) lõi kaasaja loogika fundamentaalseima süsteemi, nn esimest järku predikaatarvutuse, mis baseerub lausearvutusel, predikaatidel ja kvantoritel. Frege kindel seisukoht oli, et kogu matemaatika saab taandada elementaarsetele loogikareeglitele, st loogikareeglite abil saab tuletada ükskõik millise tõese matemaatikateoreemi. Frege süsteemi ja logistsistlikud vaated võtsid oma töös aluseks 20. sajandi alguse mõjukaimad loogikud **Bertrand Russell** (1872 – 1970) ja **Alfred North Whitehead** (1861 – 1947), kes formaliseerisid oma teoses *Principia Mathematica* (1910 – 1913) suure osa matemaatika alustest. Matemaatika tuletamist loogikast alustasid Russell ja Whitehead täisarvude teooriast ehk aritmeetikast, võttes aluseks **Giuseppe Peano** (1858 – 1932) aritmeetika baastõed, millest loodeti tuletada aritmeetika ning seejärel ehitada sinna peale matemaatiline analüüs, algebra ja muud matemaatikaharud. Kolmekümnendatel aastatel tõestas **Kurt Gödel** (1906 – 1978), enamikule selleaja loogikutele ootamatult, ühe praeguseks kuulsaima loogikateoreemi üldse: **teoreemi mittetäielikkusest**. Nimestatud teoreem näitab, et aritmeetikat ei saa taandada loogikale, ehk konkreetsemalt, ei ole olemas lõplikku baasväidete (aksioomide) kogu, millest saaks tuletada kõiki aritmeetikateoreeme. Kui juba aritmeetikat ei saa lõpliku hulga baasväidete abil aksiomatiseerida, siis loomulikult ei saa seda teha ka enamike teiste matemaatikaharude jaoks. See ei tähenda samas, et loogikavahendid oleksid aritmeetika või muude keerulisemate valdkondade juures kasutatud: reeglina piisab meile huvi pakkuvate väidete tõestamiseks siiski

Nikolai
Lobatševski



David Hilbert



Giuseppe Peano



Kurt Gödel

suhteliselt väikesest hulgast harilikest elementaaraksioomidest. Gödeli teoreem kahandas huvi loogika vastu, kuid elektronarvutite leiutamine sajandi keskel ja majanduse, teaduse ning ühiskonna süvenev arvutiseerimine andsid loogikateadusele uue võimsa tõuke. Alates 1980. aastate lõpust on arendatud matemaatika formaliseerimist arvutil (nt interaktiivsed teoreemitõestajad), nende jaoks on loodud palju standardteoreemide teeke. Loogika ja teoreetiline arvutiteadus on muutunud vastastikku üksteisest sõltuvaks ning mitmete konkreetsete valdkondade puhul raskesti eristatavateks.

5.1 Pólya printsiibid

Tõestamisel võib kasu olla ungari matemaatiku Güorgy (inglise keeles George) Pólya (1887 - 1985) printsiipidest. Aastal 1945 ilmus tema populaarteadusliku raamatu *How to solve it* esmatrükk, mida on tõlgitud mitmetesse keeltesse. Eesti keeles ilmus raamat 1967. aastal Ülo Kaasiku tõlkes teosena *Kuidas lahendada ülesannet* ning 2001. aastal *Kuidas seda lahendada*.

Järgnevalt toome välja Pólya neli printsiipi.

1. Kõigepealt pead sa **probleemist aru saama**.

- Kas sa suudad probleemi sõnastada oma sõnadega?
- Kas sa suudad probleemi kirjeldada joonise või graafikuga?
- Kas on piisavalt informatsiooni, et leida lahendus/tõestus?

2. Kui oled aru saanud, siis **koosta plaan**.

- Katseta ja kontrolli.
- Välista variante.
- Vaatle erijuhte.

3. Vii plaan ellu.

- Jää oma plaanile kindlaks. Kui plaan ikka ei tööta, siis vali uus plaan.

4. **Vaata tehtule tagasi**.

- Kas saaks kuidagi paremini?
- Kas seda strateegiat saaks ka mõne muu probleemi jaoks kasutada?

Pólya: „Kui sa ikka ei oska esialgset probleemi lahendada, siis **kusagil on lihtsam või sarnane probleem**, mida sa oskad lahendada – **leia see üles!**”

5.2 Induktiivne ja deduktiivne järeldamine

Laias laastus saab mõtlemismehhanisme jagada kahte põhirühma: üldistuste tegemine ja järelduste tegemine.

Induktiivne järeldamine ehk üldistuste tegemine toimub siis, kui üksikjuhtudel selgunud omadus üldistatakse üldomaduseks. Nähes enda ümber ainult valgeid luiki, kipume üldistavalt uskuma, et kõik luigid maailmas on valged. Kui märkame, et asjad, millega me kokku puutume, esinevad kas enamasti või alati koos (leek = kuumus = valu), üldistame selle kokkusattumuse sageli reegliks. Kuid enamik igapäevaselt õpitud reegleist ei pruugi erandlikes olukordades kehtida, neil reeglitel on tavaliselt erandid. Üldistuste tegemine ehk induktsioon on seega mõtlemisprotsess, mis ei anna mingeid kindlaid teadmisi. Induktiivselt saab järeldada ainult millegi tõenäolisust, mitte tõesust ehk üldistuste edukus on statistiline: mida sagedamini selliselt leitud reegel kehtib, seda parem, aga ei maksa loota, et ta alati kehtib. Tuleb meeles pidada, et matemaatikas ei kasutata tõestamist kogemuse abil!

Loogikareeglite kasutamist uute väidete järeldamiseks nimetatakse aga nende väidete tuletamiseks ehk **deduktsiooniks** ehk tõestamiseks. Suur osa loogikas kasutatavatest reeglitest ongi esitatud järelduse vormis: ühe või mitme väite tõesusest järeldub uus väide. Teiste sõnadega, peetakse võimatuks, et eelduste tõesuse korral oleks järeldus väär. Erinevalt induktsioonist garanteerib õigete reeglite rakendamine õigetele faktidele alati ka õige tulemuse.

5.3 Tõestamine

Teoreemid esinevad sageli „Kui ..., siis ...“ kujul ehk matemaatiliselt kirjutatuna,

$$\forall x \in D, \text{ kui on tõene } P(x), \text{ siis on tõene ka } Q(x).$$

Tingimust $P(x)$ nimetatakse **eelduseks** ja tingimust $Q(x)$ **väiteks**. Võimsaim tõestuse meetod on selline, mis üldistab ehk laiendab väite kehtivuspiirkonda. Antakse ette suvaline x , mille korral eeldus $P(x)$ on tõene ja kasutades definitsioone, eelnevaid tulemusi ja reegleid järeldatakse, et $Q(x)$ on tõene.

Seega, teoreemi tõestamisel:

1. lähtutakse eeldusest;
2. viiakse läbi arutlus kasutades aksioome või varem tõestatud teoreemide väiteid;
3. loogilise arutluse käigus jõutakse lõpuks otsustuseni, et teoreemi väide tõesti kehtib.

Erinevad matemaatilised teooriad ei ole lihtsalt faktide kogumid, vaid loogilised süsteemid. Aksioomid, definitsioonid ja teoreemid ei ole mitte juhuslikus järjekorras loetletud, vaid on tavaliselt esitatud meisterlikus järjestuses. Iga teoreem peab olema paigutatud niisugusele kohale, et tema tõestus toetub varem esitatud aksioomidele, definitsioonidele ja teoreemidele. Eukleidese „Elemendid“ oli selliste rangelt loogiliste süsteemide esimene ning parim näide, mida teised teadused on püüdnud ja püüavad ikka veel jäljendada. Järgnevalt vaatamegi erinevaid tõestuse meetodeid.

5.4 Otsene tõestus

Enamik tõestusi, millega sa siia maani kokku puutunud oled, on olnud nn **otsesed tõestused**, mille korral iga järgmine samm toetub eelnevalt näidatud sammule või olemasolevale faktile. Loogiliselt õiges järjekorras arutledes jõutakse lõpuks tulemuseni.

Tähistades eelduse tähega P ning väite tähega Q , on eesmärk otseselt näidata, et $P \Rightarrow Q$.

Kuigi otsese tõestuse juures kasutatavad matemaatilised meetodid erinevad üksteisest vastavalt tõestamist vajavale väitele, on siiski üldine lähenemine alati sama: alusta nende andmetega, mis eelduses on antud ja loogilise arutluse tulemusena jõua väiteni, mida oli vaja tõestada.

Tõestuse üldise esitusega tutvumiseks vaatleme järgmist kahte näidet.

Lause 5.1

Olgu m ja n täisarvud. Kui m ja n on paarisarvud, siis on seda ka $m + n$.

Tõestus. Olgu m ja n paarisarvud. Siis saame nad esitada kujul $m = 2k_1$ ja $n = 2k_2$, kus k_1 ja k_2 on mingid täisarvud. Nende summa $m + n$ saame esitada kujul $m + n = 2k_1 + 2k_2 = 2(k_1 + k_2) = 2k$. Kuna $k := k_1 + k_2$ on täisarv, siis on $2k$ paarisarv ehk $m + n$ on paarisarv. ■

Lause 5.2

Iga paaritu täisarvu ruut annab 8-ga jagades jäägi 1.

Tõestus. Olgu n suvaline paaritu täisarv. Kuna n on paaritu, siis leidub täisarv k nii, et $n = 2k + 1$. Järelikult $n^2 = (2k + 1)^2$ ehk $n^2 = 4k^2 + 4k + 1$ ehk $n^2 = 4k(k + 1) + 1$. Kuna kahest järjestikusest arvust üks on alati paaris, siis $k(k + 1)$ on kindlasti paarisarv. Järelikult $4k(k + 1)$ jagub 8-ga ja seega oleme näidanud, et n^2 annab 8-ga jagades jäägi 1. ■

Mõned tüüpilised vead teoreemide tõestamisel:

- Argumenteeritakse näidetega. See, et mõne näite korral teoreem kehtib, ei tähenda veel selle üldist kehtimist.
- Samade tähistuste kasutamine erinevate terminite jaoks. Näiteks, kui lauses 5.1 tähistada kahte suvalist paarisarvu m ja n mõlemat kujul $m = 2k$ ja $n = 2k$, siis tekib arutluses viga, sest tekib seos $m = n$, mis suvaliste täisarvude korral ei kehti.
- Hüppeline üleminek tulemusele.
- Tulemust ennast kasutatakse tõestuse sees.

5.5 Tõestus alamjuhtude põhjal

Tegemist on meetodiga, kus väide tõestatakse kõigil võimalikel juhtudel.

Näiteks, kui teoreem väidab midagi kõikide täisarvude n kohta, siis võib vaadelda eraldi kahte juhtu: 1) n on paarisarv ja 2) n on paaritu arv. Või, kui teoreem väidab midagi kõigi reaalarvude kohta, on mõnikord abiks vaadelda kolme juhtu 1) $x < 0$, 2) $x = 0$ ja 3) $x > 0$.

Lause 5.3

Iga naturaalarvu n korral on $n^3 + n$ paarisarv.

Tõestus. Jaotame naturaalarvude hulga omakorda paaris- ja paarituteks arvudeks ehk saame kaks alamjuhtu, mille jaoks tõestuse läbi viime.

- a) Olgu n paarisarv ehk $n = 2k$, kus k on mingi naturaalarv. Kirjutades

$$n^3 + n = (2k)^3 + 2k = 8k^3 + 2k = 2(4k^3 + k) = 2l,$$

näeme, et $n^3 + n$ on paarisarv, sest $l = 4k^3 + k$ on naturaalarv.

- b) Olgu nüüd n paaritu arv ehk $n = 2k + 1$, kus k on mingi naturaalarv või null. Kirjutades

$$n^3 + n = (2k+1)^3 + (2k+1) = 8k^3 + 12k^2 + 6k + 1 + 2k + 1 = 2(4k^3 + 6k^2 + 4k + 1) = 2l,$$

näeme, et $n^3 + n$ on paarisarv, sest $l = 4k^3 + 6k^2 + 4k + 1$ on naturaalarv. ■

Selleks, et saaksime tõestada järgmise tulemuse, meenutame reaalarvu absoluutväärtuse definitsiooni. Reaalarvu x **absoluutväärtus** on

$$|x| := \begin{cases} x, & \text{kui } x \geq 0; \\ -x, & \text{kui } x < 0. \end{cases}$$

Vahest on kasulik reaalarvu x absoluutväärtus defineerida ka nii $|x| = \max\{x, -x\}$. Veen-du, et mõlemad definitsioonid on samaväärsed.

Lause 5.4

Mis tahes reaalarvude x ja y korral kehtib $|x + y| \leq |x| + |y|$.

Tõestus. Antud tõestuses vaatleme nelja alajuhtu.

- a) Olgu $x \geq 0$ ja $y \geq 0$. Siis $x + y \geq 0$ ning absoluutväärtuse definitsiooni kohaselt $|x + y| = x + y = |x| + |y|$.

- b) Olgu $x \geq 0$ ja $y < 0$. Siin on edasise vaatluse all omakorda kaks alamjuhtu.

- (i) Kui $x + y \geq 0$, siis $|x + y| = x + y < x + 0 < |x| + |y|$.

- (ii) Kui $x + y < 0$, siis $|x + y| = -(x + y) = (-x) + (-y) \leq 0 + (-y) = |y| \leq |x| + |y|$.
- c) Olgu $x < 0$ ja $y \geq 0$. Selle juhu tõestus viiakse läbi analoogiliselt juhule b). Proovi see ise kirja panna!
- d) Olgu $x < 0$ ja $y < 0$. Siis absoluutväärtuse definitsiooni põhjal $|x + y| = -(x + y) = (-x) + (-y) = |x| + |y|$.

■

5.6 Kontrapositiivne tõestus

Mõnikord on raske näidata otse, et väitest P järeljub väide Q ehk $P \Rightarrow Q$. Teame, et $P \Rightarrow Q$ on loogiliselt samaväärne oma pöördvastandlausega ehk kontrapositiiviga $\neg Q \Rightarrow \neg P$. Näitame hoopis, et kehtib $\neg Q \Rightarrow \neg P$.

Lause 5.5

Olgu n täisarv. Kui n^2 on paaritu täisarv, siis n on paaritu täisarv.

Esmalt veendume, et miks otse on seda raske tõestada. Nimelt, kui me alustame oma eeldusest, et n^2 on paaritu täisarv, siis järelikult leidub $k \in \mathbb{Z}$ nii, et $n^2 = 2k + 1$. Seega, $n = \pm\sqrt{2k+1}$, mis ei anna meile n paarsuse kohta mingit infot. Seega veendume hoopis antud lause kontrapositiivi kehtivuses: Kui n on paaristäisarv, siis n^2 on paaristäisarv.

Tõestus. Tõepoolest, kui n on paarisarv, siis leidub $k \in \mathbb{Z}$ nii, et $n = 2k$. Nüüd saame, et $n^2 = (2k)^2 = 4k^2$, mis on kindlasti paarisarv. ■

5.7 Vastuväiteline tõestus

Sageli juhtub, et otsene tõestus ei võimalda eesmärkideni jõuda kas siis detailide vähesuse tõttu või on eesmärgiks hoopis tõestada „negatiivne“ tulemus, st näidata, et teatud omadus ei kehti või mõnda elementi ei leidu. Sellisel juhul kasutatakse matemaatikas teoreemide tõestamisel sageli vastuväitelist tõestusviisi, mille aluseks on loogikaseadus: iga väite korral on tõene kas väide ise või selle eitus, kolmandat võimalust ei ole.

Vastuväiteline tõestus ehk absurdsusele taandamine (lad *reductio ad absurdum*) on kaudse tõestamise meetod, mille korral oletatakse, et väide on väär (ehk tõene on hoopis selle väite eitus), ning tehakse sellest oletusest järeldusi. Tõestus on edukas, kui jõuame vastuoluni kas teoreemi esialgse eeldusega või mõne teadaoleva tõega. Seega järeldame, et meie vastuväiteline oletus ei saa olla tõene ehk tõene saab olla vaid väide ise.

Vastuväitelist tõestust kasutatakse tihti siis, kui on vaja tõestada, et teatava omadusega objekti ei leidu või, et teataval objektil ei ole teatavat omadust. Seega, kui esialgne väide sisaldab eitust, siis eitades eitust saame alustada sobivama eeldusega. Järelikult, vastuväitelise tõestusviisi korral tuleb osata lauseid eitada.

Kui teoreemide tõestamisel üldiselt alustatakse eeldusest ja jõutakse loogilise arutelu käigus väite tõesuseni, siis vastuväitelise tõestuse puhul toimub kogu protsess vastupidi.

Vastuväitelise tõestuse korral:

1. alustatakse väitest ja oletatakse, et tõestatav väide on väär;
2. viiakse läbi arutlus, kasutades vajadusel aksioome või varem tõestatud teoreeme;
3. arutluse tulemusel jõutakse järelduseni, et väite eitamine on võimatu, sest viib vastuollu kas teoreemi eelduse või tuntud tõdedega;
4. tehakse kokkuvõte, et kuna väite eitus ei kehti, siis kehtib väide ise.

Lause 5.6

Kui tasandil kaks sirget a ja b on paralleelsed kolmanda sirgega c , siis need sirged a ja b on paralleelsed teineteisega.

Eeldus. $a \parallel c$ ja $b \parallel c$.

Väide. $a \parallel b$.

Tõestus. Eitame väidet ja oletame, et a ja b ei ole paralleelsed. Sellest oletusest järeldub, et need sirged peavad lõikuma mingis punktis P , sest tasandil kahe sirge kohta kolmandat võimalust ei ole. Sellisel juhul aga läbib punkti P kaks sirget, mis eelduse kohaselt on mõlemad paralleelsed sirgega c . See on aga vastuolus paralleelide aksioomiga, mis väidab, et väljaspool sirget asuvat punkti läbib ainult üks antud sirgega paralleelne sirge. Seega sirged a ja b ei saa lõikuda. Et kolmandat võimalust ei ole, siis järelikult $a \parallel b$. ■

Lause 5.7

Iga reaalarvu $x \in [0, \pi/2]$ korral $\sin x + \cos x \geq 1$.

Tõestus. Oletame vastuväiteliselt, et leidub reaalarv $y \in [0, \pi/2]$ nii, et $\sin y + \cos y < 1$. Kuna $y \in [0, \pi/2]$, siis $\sin y \geq 0$ ja $\cos y \geq 0$. Seega $0 \leq \sin y + \cos y < 1$, millest saame, et $0^2 \leq (\sin y + \cos y)^2 < 1^2$ ehk $0 \leq \sin^2 y + 2 \sin y \cos y + \cos^2 y < 1$. Järelikult $2 \sin y \cos y < 0$, mis on vastuolu sellega, et $\sin y \geq 0$ ja $\cos y \geq 0$. ■

Ülesanne 5.8. Olgu $x \in \mathbb{R}$. Tõestada, et kui iga $\varepsilon > 0$ korral $|x| < \varepsilon$, siis $x = 0$.

Ülesanne 5.9. Tõestada, et ei leidu täisarve m ja n nii, et $15m + 5n = 81$.

Väga tihti näeb vastuväitelise tõestuse kasutamist irratsionaalarvudega seotud väidete korral. Tuleta meelde, et **ratsionaalarvuks** nimetatakse reaalarvu r , mida saab kirjutada kujul $r = \frac{m}{n}$, kus m ja n on täisarvud ja $n \neq 0$. Näiteks $\frac{1}{3}$, $-7\frac{2}{5}$ ja 0 on ratsionaalarvud. Reaalarvu, mida ei saa kirjutada kahe täisarvu suhtena, nimetatakse **irratsionaalarvuks**. Kui reaalarve tähistada tähega $\mathbb{R}$ ja ratsionaalarve tähega $\mathbb{Q}$, siis irratsionaalarve tähistatakse tähega $\mathbb{I}$, kusjuures $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$.

Lause 5.10

Reaalarv $\sqrt{2}$ on irratsionaalarv.

Tõestus. Oletame vastuväiteliselt, et $\sqrt{2}$ on ratsionaalarv. Järelikult leiduvad täisarvud r ja $s \neq 0$ nii, et $\sqrt{2} = \frac{r}{s}$. Üldisust kitsendamata võime eeldada, et $\frac{r}{s}$ on taandumatu murd. Võttes selle võrduse ruutu saame $2 = \frac{r^2}{s^2}$, millest $2s^2 = r^2$. Seega on r^2 paarisarv, mistõttu on ka r paarisarv. Niisiis, leidub täisarv k nii, et $r = 2k$. Nüüd saame võrduse $2s^2 = r^2$ kirjutada kujul $2s^2 = 4k^2$, seega ka s on paarisarv. Et s ja r on mõlemad paarisarvud, siis nad sisaldavad tegurit 2, mis on vastuolus meie eeldusega, et $\frac{r}{s}$ on taandumatu murd. Järelikult on $\sqrt{2}$ irratsionaalarv. ■

Lause 5.11

Kui positiivne reaalarv x on irratsionaalarv, siis ka $\sqrt{x}$ on irratsionaalarv.

Tõestus. Oletame vastuväiteliselt, et x on irratsionaalarv ja $\sqrt{x}$ on ratsionaalarv. Kuna $\sqrt{x}$ on ratsionaalarv, siis leiduvad täisarvud a ja b , $b \neq 0$, nii, et $\sqrt{x} = \frac{a}{b}$. Seega $x = (\sqrt{x})^2 = (\frac{a}{b})^2 = \frac{a^2}{b^2}$. Saime, et x on ratsionaalarv, mis on vastuolus meie oletusega, et x on irratsionaalarv. Järelikult peab kehtima meie esialgne väide. ■

5.8 Samaväärsete tingimuste ehk ekvivalentsi tõestamine

Alustame kahe väite samaväärsusega, loogikas tähistatud kui $A \Leftrightarrow B$ ning loetud kui „ A siis ja ainult siis, kui B “ või „tingimus A on tarvilik ja piisav tingimuse B jaoks“ või „tingimus A on samaväärne tingimusega B “. Lausearvutuse peatükis näitasime ka, et $A \Leftrightarrow B$ on loogiliselt samaväärne valemiga $(A \Rightarrow B) \wedge (B \Rightarrow A)$. Viimane kirjutusviis annab meile aga selliste teoreemide tõestamise strateegia.

Selleks, et tõestada, et väited A ja B on samaväärsed (ekvivalentsed), tuleb näidata, et kumbki väide järelneb teisest. Seega, tõestamiseks teoreemi „ A siis ja ainult siis, kui B “, peame kõigepealt näitama, et $A \Rightarrow B$ ning seejärel näitama, et $B \Rightarrow A$, kasutades kummalgi juhul mis tahes sobilikku tõestamise meetodit.

Lause 5.12

Olgu a ja b täisarvud. Korrutis ab on paarisarv siis ja ainult siis, kui vähemalt üks arvudest a või b on paarisarv.

Arutelu. Kuna teoreemi sõnastuses esineb väljend „... siis ja ainult siis ...“, tuleb meil tõestada kaks implikatsiooni. Kõigepealt tuleb näidata, et 1) kui ab on paarisarv, siis vähemalt üks arvudest a või b on paarisarv, ning seejärel teistpidi, et 2) kui vähemalt üks arvudest a või b on paarisarv, siis ab on paarisarv. Ilma üldisust kitsendamata võime eeldada, et a on paarisarv. Me võiksime tõestuse anda ka alamjuhtude kaudu, kus kõigepealt on a paarisarv ja seejärel on b paarisarv, aga need tõestused saavad olema täpselt ühesugused ja seega võime lihtsalt valida ühe arvudest ja eeldada, et see on paarisarv. Teiseks

märkame, et kui sooviksime esimese implikatsiooni tõestamisel kasutada otsese tõestamise meetodit, siis alustaksime eeldusega, et $ab = 2k$, kus k on mingi täisarv. Edasi oleks meil aga väga raske öelda midagi arvude a ja b kohta eraldi. Seega on esimese implikatsiooni juures vaja teistsugust tõestusmeetodit. Püüame nüüd selle teoreemi ära tõestada.

Lause 5.12 tõestus.

1) $\Rightarrow$ 2). Tõestame selle implikatsiooni vastuväiteliselt. Selleks oletame väite vastaselt, et ab on paarisarv, aga mõlemad arvud a ja b on paaritud. Siis võime kirjutada, et $a = 2m + 1$ ja $b = 2n + 1$, kus m ja n on täisarvud. Saame

$$ab = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1.$$

Kuna $2mn + m + n$ on täisarv, oleme näidanud, et ab on paaritu arv, mis annab meile vastuolu eeldusega, et ab pidi olema paarisarv.

2) $\Rightarrow$ 1). Vastupidise implikatsiooni näitamiseks oletame, et kas a on paarisarv või b on paarisarv. Üldisust kitsendamata eeldame, et a on paarisarv ja seega kirjutatav kujul $a = 2k$, kus k on täisarv. Nüüd $ab = (2k)b = 2(kb)$ ja kuna kb on täisarv, oleme näidanud, et ab on paaris. ■

Lause 5.13

Olgu x ja y reaalarvud. Siis $x^2 = y^2$ parajasti siis, kui $|x| = |y|$.

Tõestus. Iseseisvalt! ■

5.9 Mitme samaväärse tingimuse tõestamine

Sageli on teoreemides samaväärseid tingimusi antud rohkem kui kaks ja teoreemi üldine sõnastus võib näha välja nii:

Teoreem 5.14

[...eeldused...] Järgmised väited on samaväärsed:

(a)

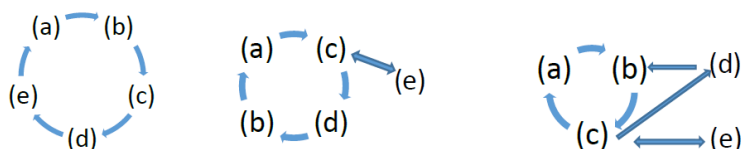
(b)

(c)

...

Sellistes teoreemides on erinevaid väiteid kolm või rohkem (ülemist piiri ei ole) ning eesmärgiks on näidata, et kõik need tingimused on samaväärsed. Samaväärsus antud olukorras tähendab seda, et kui üks väidetest on õige, siis on õiged ka kõik ülejäänud ja kui üks on vale, siis on samaväärsuse põhjal valed ka kõik ülejäänud väited. Kui samaväärseid väiteid on kolm, siis tuleks meil teha kolm ekvivalentsitõestust („... siis ja ainult siis...” tüüpi), kusjuures need oleksid $(a) \Leftrightarrow (b)$, $(b) \Leftrightarrow (c)$ ning $(a) \Leftrightarrow (c)$. Kui tõestatavaid väiteid on neli, siis tuleks teha 6 ekvivalentsitõestust ning üldjuhul n samaväärse väite tõestamiseks tuleks teha $\frac{n(n-1)}{2}$ ekvivalentsitõestust. Õnneks meil selliste teoreemide tõestamisel siiski

nii palju ekvivalentsitõestusi teha ei tule. Järgmine joonis annab kolm võimalust viie samaväärse tingimusega teoreemi tõestuskäigu planeerimiseks. Ühe otsaga nooled tähistavad vastavat implikatsiooni ning kahe otsaga nooled ekvivalentsi tõestamise vajadust.



Teoreem 5.15

Olgu n täisarv. Järgmised väited on samaväärsed:

- (a) n on paarisarv
- (b) $n + 1$ on paaritu arv
- (c) n^2 on paarisarv

Tõestus. Iseseisvalt! ■

5.10 Olemasolu ja ühesuse tõestus

Vaatleme nüüd selliseid tõestamise meetodeid, mida esitatakse kujul „ $\exists x$, mille korral $P(x)$ “. Sellised teoreemid tagavad, et eksisteerib vähemalt üks x , mille korral tingimus (omadus) $P(x)$ on õige. Sellist tõestust nimetatakse **olemasolu tõestuseks**.

Olemasolu tõestused jagunevad omakorda veel kaheks: konstruktiivseks ja mittekonstruktiivseks.

5.10.1 Konstruktiivne olemasolu tõestus

Konstruktiivse tõestuse läbiviimisel võime püüda elementi x otseselt konstrueerida või võtta abiks arvutid ja koostada algoritm otsitava elemendi x leidmiseks.

Näide 5.16. Tõesta, et leidub täisarv, mille ruut on 81.

Põhjendus. Selleks arvuks sobib 9, sest $9 \cdot 9 = 81$. ■

Näide 5.17. Tõesta, et leidub lausearvutuse valem, millest järeldub sama valemi eitus.

Põhjendus. Vaatleme valemit $X \wedge \neg X$. Tõeväärtustabeli põhjal on valem $X \wedge \neg X \Rightarrow \neg(X \wedge \neg X)$ samaselt tõene (Kontrolli!). Seega valemist $X \wedge \neg X$ järeljub valem $\neg(X \wedge \neg X)$. See tähendab, et valem $X \wedge \neg X$ on vajaliku omadusega. ■

Näide 5.18. Näita, et leiduvad reaalarvud a ja b nii, et $(a + b)^2 = a^2 + b^2$.

Põhjendus. Kuigi antud seos ei ole üldjuhul õige, saame leida arvupaare, mis ka sellist võrdust rahuldavad. Seega, olgu $a, b \in \mathbb{R}$ sellised, et $(a + b)^2 = a^2 + 2ab + b^2 = a^2 + b^2$. Siis peab $2ab = 0$. Üks võimalik lahend oleks $a = 1$ ja $b = 0$, sest siis $(a + b)^2 = (1 + 0)^2 = 1^2 = 1^2 + 0^2 = a^2 + b^2$. ■

5.10.2 Mittekonstruktivne olemasolu tõestus

Võib aga ka juhtuda, et olemasolevate tulemuste baasil on võimalik loogilise arutlemise teel otsitava objekti eksisteerimine kindlaks teha ilma seda objekti otseselt leidmata. Näiteks peaks sulle tuntud olema teoreem, mis väidab, et igal paarituastmelisel reaalarvuliste kordajatega polünoomil on vähemalt üks reaalne lahend. See teadmine aga ei aita sul iga sellise polünoomi korral seda lahendit leida. David Hilbert kasutas oma loengutes olemasolu tõestuse idee illustreerimiseks järgmist näidet:

Siin klassis on vähemalt üks üliõpilane, olgu ta nimi 'X', kelle kohta kehtib järgmine väide: Mitte ühelgi teisel üliõpilasel siin klassis ei ole rohkem juukseid peas kui üliõpilasel X. Kes see üliõpilane on? Seda ei saa me kunagi teada, aga tema olemasolus saame me absoluutselt kindlad olla.

Lause 5.19

Leiduvad irratsionaalarvud x ja y nii, et x^y on ratsionaalarv.

Tõestus. Teame, et $\sqrt{2}$ on irratsionaalarv. Uurime arvu $(\sqrt{2})^{\sqrt{2}}$. Vaatame nüüd kahte alamjuhtu:

1. Kui $(\sqrt{2})^{\sqrt{2}}$ on ratsionaalarv, siis olemegi oma väite tõestanud, sest võime võtta $x = y = \sqrt{2}$.
2. Kui $(\sqrt{2})^{\sqrt{2}}$ on irratsionaalarv, siis

$$((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2} \cdot \sqrt{2}} = (\sqrt{2})^2 = 2.$$

Seega sel juhul võime võtta $x = \sqrt{2}^{\sqrt{2}}$ ja $y = \sqrt{2}$.

Me ei tea kumb juht realiseerub, aga kindlasti leiduvad irratsionaalarvud x ja y nii, et x^y on ratsionaalarv. ■

Oma edasistes matemaatikaõpingutes kohtad sageli ka teoreeme, mis väidavad, et leidub **üks ja ainult üks** kindlaks määratud omadustega element. Selliste teoreemide tõestus hakkab tavaliselt väite vastaselt, st eeldame, et leidub kaks elementi, ütleme x ja y , nõutud omadustega. Loogilise arutluse teel on meie eesmärgiks näidata, et siis $x = y$.

Näide 5.20. Kui k ja b on reaalarvud ja $k \neq 0$, siis leidub üks ja ainult üks reaalarv x , mis rahuldab võrrandit $kx + b = 0$.

Põhjendus. Oletame väite vastaselt, et leiduvad kaks mittevõrdset reaalarvu x_1 ja x_2 , mis mõlemad rahuldavad antud võrrandit, s.t $kx_1 + b = 0$ ja $kx_2 + b = 0$. Pannes avaldised võrduma, saame $kx_1 + b = kx_2 + b$, millest pärast arvu b mõlemalt poolelt lahutamist saame, et $kx_1 = kx_2$. Kuna $k \neq 0$, siis pärast võrrandi mõlema poole arvuga k läbijagamist järeldub, et $x_1 = x_2$. Saime vastuolu eeldusega, et $x_1 \neq x_2$. Seega ei saa olla kahte erinevat lahendit ja on vaid üks. ■

Matemaatikud, olles huvitatud seostest ja seaduspärasustest, kalduvad tihti otsima mingite kindlate omadustega objekte, kas siis lihtsast uudishimust või vajadusest. Näiteks võivad nad küsida, et kas leiduvad täisarvud a, b ja c nii, et $a + b + c = 3$ ja $a^3 + b^3 + c^3 = 3$, lisaks triviaalsele lahendile $a = b = c = 1$? Või, kui tasandil on antud kaks suvalist ristkülikut, siis kas leidub selline sirge, mis jagab nende mõlema pindala täpselt pooleks? Tuleb välja, et mõlemale küsimusele saab jaatavalt vastata. Kas sa suudad lahenduse leida?

Pinnapealselt vaadatuna tundub, et olemasolu tõestusi on kergem teha kui muid tõestusi. Tuleb ju konstruktiivse tõestuse korral vaid üks teatud omadustega objekt leida ja vajadust pole tõestada, et mingi omadus kehtib hulga kõigi elementide jaoks. Sageli on aga selle ühe objekti leidmine väga raske. 1769. aastal püstitas **Euler** hüpoteesi, et kolme täisarvu neljanda astme arvu summa ei ole kunagi võrdne mõne muu arvu neljanda astmega. Aga aastal 1986 (arvutite ajastul!) lükkas **Noam Elkies** (sündinud 1966) Euleri väite ümber näidates, et

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$



Noam Elkies

5.11 Oletused ehk hüpoteesid

Üks põnevamaid asju, mida matemaatikaga teha saab, on otsida ja avastada uusi tulemusi. Seda pole aga kerge teha ja veelgi raskem on anda täpseid juhiseid, kuidas selline protsess toimuma peaks. Seoste ja mustrite leidmine on kunst, samamoodi nagu viljakate küsimuste küsimine. Vaatame järgmist täisruutude jada

$$0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324, 361, 400$$

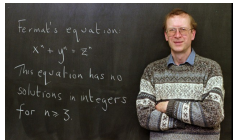
ja hakkame otsima mõnda kena seost nende arvude vahel. Näiteks märkame, et kahe täisruudu summa on alati täisruut, näiteks nagu $64 + 225 = 289$. Nüüd võiksime aga küsida, et kas kahe täisruudu summa on võrdne mõnede teiste täisruutude summaga? Aga mis juhtub, kui korrutada täisruutu arvuga 2?

Tuleb välja, et selline arv pole ise kunagi täisruuduks, küll aga võib olla täisruudule väga lähedal, nagu näiteks $2 \cdot 25 = 50 = 49 + 1$ või $2 \cdot 144 = 288 = 289 - 1$. Esitame oma leiud tabelina, et kergendada mustrite ja seoste leidmist.

Tabelist märkame mitu toredat seost. Näiteks, igas reas liites m ja n väärtused, saame m väärtuse järgmises reas. Proovi nüüd ise teha veel mõni oletus erinevate seoste ja mustrite kohta samas tabelis. Oma tähelepanekute põhjal oletage järgmise kahe rea väärtused ning



Pierre de Fermat



Andrew Wiles



Francis Guthrie



Kenneth Appel



Wolfgang Haken

$2m^2 = n^2 \pm 1$	m	n
$2 \cdot 1 = 1 + 1$	1	1
$2 \cdot 4 = 9 - 1$	2	3
$2 \cdot 25 = 49 + 1$	5	7
$2 \cdot 144 = 289 - 1$	12	17
$2 \cdot 841 = 1681 + 1$	29	41

kontrolli oma oletusi.

Pane tähele, et meie huvitav uurimus algas lihtsalt arvude ruutu tõstmisest, kuid siis küsisime hea küsimuse, et „mis juhtub, kui me täisruute kahega korrutame“, ja noppisime hulga vilju oma hästi organiseeritud tabelist. Sellised sammud ja tegemised kirjeldavad üpris hästi teed uute tulemuste avastamiseni.

Intrigeerivad oletused meelitavad ligi paljusid matemaatikuid ning tavaliselt leiavad need oletused kiiresti ka tõestuse või kontranäite. Vahetevahel aga juhtub, et mõned oletused püsivad tõestuseta mitmeid aastaid kuni uuem ja võimsam meetod või tõeliselt geniaalne idee need ära suudab lahendada. Üks kuulsamatest sellelaadsetest näidetest üldistab meie arvude ruutu tõstmise ideed ja väidab, et leiduvad täisarvud a, b ja c nii, et $a^2 + b^2 = c^2$. Esitame nüüd intrigeeriva küsimuse: Kas sarnane seos arvude a, b ja c vahel kehtib ka kõrgemate astendajate korral? See tähendab, et kas leiduvad täisarvud a, b ja c nii, et $a^3 + b^3 = c^3$ või $a^4 + b^4 = c^4$, jne? Aastal 1637 tegi **Pierre de Fermat** (1607 – 1665) oletuse, et arvust 2 suuremate astendajate puhul selline seos ei kehti, kuid suutis selle tõestada vaid neljanda astme jaoks. Rohkem kui sajand hiljem näitas **Euler**, et see seos ei kehti ka kuupide korral. Seejärel võttis aega kuni aastani 1990, mil **Andrew Wiles** (sündinud 1953) koos teiste matemaatikutega tõestas „Fermat’ viimase teoreemi“ näidates oletuse kehtivust kõigi täisarvuliste astendajate korral.

Veel üks kuulus hüpotees oli **Francis Guthrie** (1831 – 1899) poolt 1852. a. välja pakutud **nelja värvi probleem**, mis küsis, et kas iga maakaart on värvitav nelja värviga nii, et naabermaad on eri värvi. Guthrie püüdis ise Inglismaad värvida. Mitmed tolle aja kuulsad matemaatikud tegelesid selle probleemiga ja jõudsid hüpoteesi sõnastamiseni, et seda on võimalik teha. Tõestus tuli aga alles aastal 1976 **Kenneth Appeli** (1932 – 2013) ja **Wolfgang Hakeni** (sündinud 1928) poolt kasutades arvutite abi. Nüüdseks on seega see hüpotees tõestatud ja temast on saanud teoreem.

5.12 Ümberlökkamised ehk kontranäited

Tihti aga osutuvad oletused vääraks. Kui see väär oletus sisaldab väidet kõigi antud hulka või klassi kuuluvate elementide kohta, siis tuleb leida vaid üks näide, mille korral tulemus ei kehti. Seega tuleb leida kontranäide.

Näide 5.21. Tõesta, et järgmine väide pole tõene:

$$\forall a, b \in \mathbb{R} \text{ korral, kui } a < b, \text{ siis ka } a^2 < b^2.$$

Põhjendus. Piisab leida vaid üks paar arve a ja b , mille korral väide ei kehti. Valime selleks $a = -2$ ja $b = -1$. Siis $a < b$, sest $-2 < -1$, kuid $a^2 > b^2$, sest $(-2)^2 > (-1)^2$. Sellega on väide ümber lükatud. ■

Näide 5.22. Tõesta, et järgmine väide pole tõene:

$$\forall n \in \mathbb{N}, \text{ kui } n \text{ on algarv, siis } 6n + 1 \text{ on algarv.}$$

Põhjendus. Kontranäite leidmiseks eitame kõigepealt antud väidet: $\exists n \in \mathbb{N}$ nii, et n on algarv ja $6n + 1$ ei ole algarv. Seega peame järjest läbi proovima kõik algarvud ja leidma sellise algarvu n , mille korral $6n + 1$ ei ole algarv. Kannatlik töö viib sihile ja leiame, et $n = 19$ on selline algarv, mille korral $6n + 1 = 6 \cdot 19 + 1 = 115$ ei ole algarv. ■

5.13 Miks õpetada tõestamist?

Newtoni kohta räägitakse järgmist lugu. Noore üliõpilasena alustas ta geomeetria õppimist Eukleidese „Elementide“ lugemisest (nagu see tol ajal tavaline oli). Ta luges teoreeme, nägi, et need olid õiged ning jättis tõestused vahele. Ühtlasi ta imestas, miks peaks keegi sedavõrd ilmsete asjade tõestamisega nii palju vaeva nägema. Palju aastaid hiljem ta aga muutis oma seisukohta ja kiitis Eukleidest väga.

Miks peame õppima või õpetama tõestusi? Esimeseks vastuseks sellele küsimusele on muidugi tüüpiline väide, et tõestused on kesksel kohal matemaatikas ja seetõttu pole võimalik neid vältida ka matemaatikat õppides ja õpetades. Milleks matemaatikud üldse oma tulemusi tõestavad ja kolleegide tõestusi uurivad? Üheks põhjuseks on muidugi tulemuste üle kontrollimine – tõestus veenab meid väite paikapidavuses, st vastab küsimusele, „Kas on tõene?“. See ei ole matemaatikule aga ainuke ja kõige olulisem põhjus. Isegi professionaalsed matemaatikud on ilmselt valmis uskuma tarkades raamatutes või teadusajakirjades esitatud väiteid ilma tõestuseta. Miks nad siis ikkagi kolleegide tõestuskäike uurivad? Tähtsamaks põhjuseks on pigem selgitamine – tõestus viib meid sisulisele arusaamale väite olemusest, vastab küsimusele, „Miks on väide tõene?“. Ka matemaatikuid endid huvitab eelkõige just see aspekt ning küsimus „Miks?“, mitte pelgalt tõesuse konstateerimine ise. Lisaks aitab tõestus süstematiseerida, ta seob erinevaid teadmisi ühtseks terviklikuks deduktiivseks arutlusahelaks, andes sel moel edasi intuiitiivselt tajutud tõde. Sageli just selle funktsiooni kaudu tajumegi matemaatika ilu ja näeme seal kehtivaid seoseid.

5.14 Näpunäiteid tõestuse kirjutamiseks

Hea tõestuse kirjutamine eeldab harjutamist ja juhiste järgimist. Tuleb endale selgeks teha kehtivad tavad, kasutada sümboteid ja märgistusi korrektselt, kohaneda uue sõnavaraga, harjutada erinevaid tõestusmeetodeid, olla enda suhtes rangem ja nõudlikum, jne. Kõik see on saavutatav, kui sa seda soovid.

Iga tõestuse selgrooks on täiuslik „vettpidav“ argument. Kuna matemaatilised meetodid selle eesmärgi saavutamiseks sõltuvad etteantud probleemist, siis arutleme range tõestuse üle igal juhul eraldi. Siiski saame juba praegu öelda midagi tõestuses kasutatavate

detailide rohkuse üle. Üldine reegel ütleb, et peaksid kasutama piisaval hulgal detaile ja seletusi tõestuse iga sammu näitamisel, aga ei tohi detailidega ka üle pingutada, et lugejale koormavaks muutuda. Tõestuse kirjutamine on nagu luuletuse kirjutamine, kus hea poeet oskab öelda kõik mis vaja nii väheste sõnadega kui võimalik.

On mitmeid erinevaid võimalusi lühemate tõestuste saavutamiseks. Kindlasti aitab kaasa teadmine matemaatika sümbolitest ja keelest. Selle asemel, et öelda „Olgu x hulga A_1 või A_2 või A_3 element, välja arvatud see, et me ei taha, et $x = 0$ “ võime kohe kirjutada „Olgu $x \in (A_1 \cup A_2 \cup A_3) \setminus \{0\}$ “. On muidugi ka kartus minna teise äärmusesse ja liiga vähe kirjutada, kuid algajatel matemaatikutel nagu sina seda probleemi väga tihti ei juhtu. Kui võimalik, ehita oma tõestus üles olemasolevatele tulemustele, selle asemel, et iga olemasolevat tulemust jälle uuesti tõestada. Samuti, kui mitmes kohas tõestuse sees kasutatakse sarnast arutelu, siis pole vaja iga kord kõiki detaile välja tuua. Pigem ütle „Sarnaselt eelmisele juhule järeldeb...“ või „Samamoodi võime väita, et...“. Ning lõpetuseks, selleks, et paberile kirja panna kena tõestus, tuleb see ka matemaatiliselt hästi läbi mõelda. Ilusad matemaatilised tulemused väärivad ilusalt esitatud tõestusi.

Veel mõningaid soovitusi hea stiili omandamiseks:

1. Liigenda oma tõestus sobiva pikkusega lõikudeks. Ei ole kohustuslik, et sa tõestuse alguses uuesti ütled, mida tõestada tuleb, aga kui sa seda teed, siis muudab see tõestuse kindlasti paremini loetavamaks. Sinu sõnastus peab selgelt väljendama, et väide tahab alles tõestamist, kirjutades näiteks, „Meil on vaja näidata, et $A \cap B \subset A \cup B$ “, selle asemel, et lihtsalt öelda „Hulkade A ja B jaoks kehtib $A \cap B \subset A \cup B$ “, nagu oleks see väide juba tõestatud. Järgmise lausena oleks alati hea anda väike suunajuhis, millise strateegia järgi sa seda väidet tõestama hakkad, näiteks „Selleks näitame, et kui $x \in A \cap B$, siis $x \in A \cup B$.“
2. Kasuta oma matemaatilise kirjakeele rikastamiseks võimalikke sünonüüme. Näiteks sõna 'tõestama' asemel kasuta sõnu 'näitama', 'põhjendama', 'argumenteerima', jne. Samuti on hea, kui sul on tagavaraks alternatiivid sõnale 'seega'. Võimalikud sünonüümid oleksid 'järelkult', 'niisiis', 'seetõttu', 'tähendab', jt.
3. Matemaatilistes tekstides kasutatakse sõna 'mina' asemel sageli sõna 'meie'. Kuna matemaatilise teksti lugemine peaks olema aktiivne tegevus ja mitte passiivne, siis kasutades sõna 'meie' püüab autor kaasata ka lugejat tõestuse tegemise juurde.
4. Ära alusta lauseid sümboliga või matemaatilise valemiga. Eelista kirjutada „Võrrand $x^2 + 2x - 2 = 0$ on oluline, sest...“, selle asemel, et kirjutada „ $x^2 + 2x - 2 = 0$ on oluline, sest...“. Sarnaselt, kirjuta „Me teame, et n ei ole algarv, sest n on paarisarv ja $n \geq 4$ “ selle asemel, et kirjutada „ n ei ole algarv, sest n on paarisarv ja $n \geq 4$ “.
5. Tõestuses eriti olulised matemaatilised avaldised tuleks kirjutada eraldi reale suurema tähelepanu, aga ka selguse saamiseks. Näiteks esita järgmine avaldis omaette real

$$\bigcap_{r \in J} B_r = \{x \mid -1 < x \leq 0\}$$

selle asemel, et ta teksti sisse peita.

6. Tõestuse lõppu võib kirjutada fraase „..., *nagu oligi soovitud näidata*“, „..., *mis oligi meie eesmärgiks*“ või lihtsalt „*Sellega on tõestus lõpetatud*.“ Traditsiooniliselt lisavad matemaatikud ka tõestuse lõppu sümboli, et visuaalselt eraldada tõestus ülejäänud tekstist ja edasisest diskussioonist. Populaarseteks sümboliteks on 'QED' (ladina keelsest väljendist *quod erat demonstratum* ehk '*mida oligi tarvis tõestada*'), täidetud ■ või täitmata □ ruut.

Funktsioonid

*Ainuke viis matemaatikat õppida
on teha matemaatikat – P. Halmos*

6.1	Funktsiooni definitsioon	92
6.2	Hulga karakteristiklik funktsioon	93
6.3	Hulga kujutis ja tema omadused	96
6.4	Hulga originaal ja tema omadused	98
6.5	Hulga kujutise originaal ja originaali kujutis	100
6.6	Injektiivsed, sürjektiivsed ja bijektiivsed funktsioonid	101
6.7	Dirichlet' printsiip	103
6.8	Funktsioonide kompositsioon	103
6.9	Pöördfunktsioon	106

Funktsiooni mõiste on üks kesketest matemaatikas. Pikka aega olid funktsioonid peamiselt matemaatilise analüüsi uurimisobjektid ja vaadeldi ainult reaali- või kompleksarvudel defineeritud funktsioone, mida saab esitada mingi (elementaarfunktsioonidest koostatud) avaldise abil. Uuriti funktsioonide pidevust, diferentseeruvust, integreeruvust jne.

Ühe muutuja elementaarfunktsioonid on näiteks $f(x) = 6$, $g(x) = 3x$, $h(x) = x^2$, $k(x) = \sin x$, $l(x) = e^x$, $m(x) = \ln x$. Reaalarvude aritmeetilised tehted ja astendamine annavad meile viis kahe muutuja funktsiooni $x + y$, $x - y$, $x \cdot y$, $x : y$ ja x^y .

Matemaatilise analüüsi alastes raamatutes kirjutatakse ka praegu mõnikord, et „Funktsiooniks nimetatakse eeskirja, mis seab hulga X igale elemendile vastavusse hulga Y mingi elemendi“. Informaatik võiks seda ilmselt mõista nii, et see eeskiri tähendab algoritmi (programmi), mille abil saab argumenti väärtuse järgi leida funktsiooni väärtuse. Avaldise kujul antud funktsioonide jaoks on sellised algoritmid tõesti olemas, aga matemaatikas vaadeldakse ka üldisemaid olukordi, kus funktsiooni ei saa avaldada elementaarfunktsioonide kaudu ega ole olemas ka tema arvutamise algoritmi. Tegelikult ei eelda ka matemaatilise

analüüsi teoreemid mingi eeskirja olemasolu, sest nende teoreemide tõestustes eeldust mingi eeskirja olemasolu kohta ei kasutata. Eeldatakse vaid seda, et igale argumendi väärtusele vastab mingi funktsiooni väärtus.

6.1 Funktsiooni definitsioon

Definitsioon 6.1

Olgu X ja Y mittetühjad hulgad. Kui on antud eeskiri, mis seab hulga X igale elemendile vastavusse täpselt ühe hulga Y elemendi, siis öeldakse, et on defineeritud **funktsioon** (ingl *function*) f , ja kirjutatakse $f: X \rightarrow Y$. Kui elemendile $x \in X$ seatakse vastavusse $y \in Y$, siis kasutatakse kirjutist $y = f(x)$ või $y = fx$ või $f: x \mapsto y$.

Hulka X nimetatakse funktsiooni f **lähtehulgaks** ehk **määramispiirkonnaks** ja hulka Y nimetatakse funktsiooni f **sihthulgaks**. Hulka $f(X) = \{f(x) : x \in X\}$ nimetatakse funktsiooni f **väärtuste piirkonnaks** ehk **muutumispiirkonnaks**. Funktsiooni asemel räägitakse abstraktsemate hulkade korral ka operaatorist või kujutusest. Kujutust $f: X \rightarrow X$ nimetatakse hulga X **teisenduseks**.

Toome järgnevas mõningaid näiteid funktsioonidest.

Näide 6.2.

1. Elementaararvemaatikast tuntud lineaarne funktsioon $f(x) = ax + b$ ($a \neq 0$), ruut-funktsioon $f(x) = ax^2 + bx + c$ ($a \neq 0$) ja trigonomeetrilised funktsioonid $f(x) = \sin x$ ning $f(x) = \cos x$ on funktsioonid reaalarvude hulgast reaalarvude hulka.
2. **Konstantne funktsioon** $f(x) = c$ seab igale hulga X elemendile x vastavusse ühe ja sama elemendi $c \in Y$.
3. Olgu funktsioon $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ antud võrdusega $f((x, y)) = (x, 0)$ iga $(x, y) \in \mathbb{R}^2$ korral, st f seab tasandi punktile $P(x, y)$ vastavusse tema esimese koordinaadi x -teljel. Sellist funktsiooni nimetatakse **projekteerimisteisenduseks** x -teljele ehk **projektoriks** x -teljele. Analoogiliselt võib vaadelda projektorit y -teljele.
4. Olgu $X \neq \emptyset$ hulk. Mis tahes bijektiivset funktsiooni $s: X \rightarrow X$ nimetatakse **substitutsiooniks** hulgal X . Olgu nüüd X lõplik hulk. Käsitluse lihtsustamise huvides võime eeldada, et X koosneb n esimesest naturaalarvust ehk $X = \{1, 2, \dots, n\}$. Substitutsiooni s esitatakse tavaliselt tabelina:

$$s = \begin{pmatrix} 1 & 2 & \dots & n \\ s(1) & s(2) & \dots & s(n) \end{pmatrix},$$

kus esimeses reas on hulga X elemendid ja iga elemendi alla teise ritta on aga kirjutatud selle elemendi kujutis substitutsiooni s korral. Näiteks, üks võimalik substitutsioon on

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

5. Funktsioon **põrand** $\lfloor x \rfloor : \mathbb{R} \rightarrow \mathbb{Z}$ seab reaalarvule x vastavusse suurima temast väiksema või võrdse täisarvu ja funktsioon **lagi** $\lceil x \rceil : \mathbb{R} \rightarrow \mathbb{Z}$ seab reaalarvule x vastavusse väikseima temast suurema või võrdse täisarvu, st

$$\lfloor x \rfloor = \max\{m \in \mathbb{Z} : m \leq x\} \quad \text{ja} \quad \lceil x \rceil = \min\{n \in \mathbb{Z} : x \leq n\}.$$

6. Reaalarvuliste liikmetega jada $a_1, a_2, a_3, \dots$ on vaadeldav funktsioonina $f : \mathbb{N} \rightarrow \mathbb{R}$, kus igale naturaalarvule on seatud vastavusse kindel reaalarv, st $f(i) = a_i$ iga $i \in \mathbb{N}$ korral.

Näide 6.3. Olgu U mingi universaalne hulk.

1. Funktsiooniks on $f : \mathcal{P}(U) \rightarrow \mathcal{P}(U)$, kus

$$f(A) = A' \quad \text{iga } A \in \mathcal{P}(U) \text{ korral.}$$

2. Funktsiooniks on $f : \mathcal{P}(U) \times \mathcal{P}(U) \rightarrow \mathcal{P}(U)$, kus

$$f((A, B)) = A \cap B \quad \text{iga } (A, B) \in \mathcal{P}(U) \times \mathcal{P}(U) \text{ korral.}$$

Definitsioon 6.4

Funktsioone $f : X \rightarrow Y$ ja $g : Z \rightarrow W$ nimetatakse **võrdseteks** (ingl *equal*), kui $X = Z$, $Y = W$ ja $f(x) = g(x)$ iga $x \in X (= Z)$ korral.

Seega näiteks funktsioonid $\sin : \mathbb{R} \rightarrow \mathbb{R}$, $\sin : [-\pi, \pi] \rightarrow \mathbb{R}$ ja $\sin : \mathbb{R} \rightarrow [-1, 1]$ on kõik teineteisest erinevad.

Definitsioon 6.5

Vaatleme funktsiooni $f : X \rightarrow Y$. Hulka

$$G(f) = \{(x, f(x)) \mid x \in X\} \subset X \times Y$$

nimetatakse funktsiooni f **graafikuks** (ingl *graph*).

Ülesanne 6.6. Olgu $f_1, f_2 : X \rightarrow Y$ funktsioonid. Tõesta, et $f_1 = f_2$ parajasti siis, kui $G(f_1) = G(f_2)$.

6.2 Hulga karakteristlik funktsioon

Definitsioon 6.7

Olgu U universaalne hulk ja vaatleme tema osahulka $A \subset U$. Hulga A **karakteristlikuks funktsiooniks** (ingl *indicator function*) nimetatakse funktsiooni $\chi_A : U \rightarrow \{0, 1\}$, kus

$$\chi_A(x) = \begin{cases} 1, & \text{kui } x \in A \\ 0, & \text{kui } x \in U \setminus A. \end{cases}$$

Karakteristliku funktsiooni väärtuse $\chi_A(x)$ leidmine tähendab otsustamist, kas element $x \in U$ kuulub hulka A või mitte. Seega, igale hulgale $A \subset U$ on seatud vastavusse tema karakteristlik funktsioon. Erinevatele hulkadele vastavad erinevad funktsioonid, st vastavus on injektiivne. Kas selline vastavus on ka surjektiivne? Selle kontrollimiseks võtame ühe funktsiooni $\chi: U \rightarrow \{0, 1\}$ ja vaatleme hulka $A = \{x \in U: \chi(x) = 1\}$. Kui nüüd $x \in A$, siis $\chi(x) = 1$, kui aga $x \in U \setminus A$, siis $\chi(x) = 0$ ning seepärast $\chi = \chi_A$. Selle aruteluga oleme näidanud, et vaadeldav vastavus hulkade $A \subset U$ ja funktsioonide $\chi_A: U \rightarrow \{0, 1\}$ vahel on bijektsioon.

On selge, et fikseeritud universaalse hulga U kaks alamhulka A ja B on võrdsed parajasti siis, kui neil on sama karakteristlik funktsioon, st

$$A = B \Leftrightarrow \chi_A(x) = \chi_B(x), \quad \forall x \in U.$$

Seega, võrdsete hulkade puhul on karakteristliku funktsiooni väärtused samad. Erinevad hulgad peavad erineva vähemalt ühe elemendi poolest ja sellel elemendil on siis ka karakteristlike funktsioonide väärtused erinevad.

Näide 6.8.

1. Tühja hulga karakteristlik funktsioon on konstantne funktsioon 0 ja universaalhulga U karakteristlik funktsioon on konstantne funktsioon 1;
2. Kui universaalne hulk on naturaalarvude hulk $\mathbb{N}$, siis paaritute arvude hulga karakteristlik funktsioon on arvu jääk arvuga 2 jagamisel;
3. Kui universaalne hulk on naturaalarvude hulk $\mathbb{N}$ ja A on algarvude hulk, siis hulga A karakteristlik funktsioon on

$$\chi_A(x) = \begin{cases} 1, & \text{kui } x \text{ on algarv} \\ 0, & \text{kui } x \text{ ei ole algarv.} \end{cases}$$

Karakteristlikul funktsioonil on hulgateoreetiliste tehete suhtes järgmised omadused.

Lause 6.9: Karakteristliku funktsiooni omadused

Olgu U universaalne hulk ja $A, B \subset U$. Siis iga $x, y \in U$ korral

1. $\chi_A(x) \cdot \chi_A(x) = \chi_A(x)$;
2. $\chi_{A'}(x) = \chi_{U \setminus A}(x) = 1 - \chi_A(x)$;
3. $\chi_{A \cap B}(x) = \chi_A(x) \cdot \chi_B(x) = \min\{\chi_A(x), \chi_B(x)\}$;
4. $\chi_{A \cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_A(x) \cdot \chi_B(x) = \max\{\chi_A(x), \chi_B(x)\}$;
5. $\chi_{A \setminus B}(x) = \chi_A(x) - \chi_A(x) \cdot \chi_B(x)$;
6. $\chi_{A \Delta B}(x) = \chi_A(x) + \chi_B(x) - 2\chi_A(x) \cdot \chi_B(x)$;
7. $\chi_{A \times B}((x, y)) = \chi_A(x) \cdot \chi_B(y)$.

Tõestus. Nende võrduste kontrolliks piisab, kui vaadatakse läbi kõik võimalused elemendi x jaoks (x kuulub mõlemasse hulka, ainult hulka A , ainult hulka B , mitte kumbagi hulka) ja võrreldakse paremal esitatud avaldise väärtust vajaliku väärtusega. Näiteks, võrdus 1) järeldub sellest, et $0 \cdot 0 = 0$ ja $1 \cdot 1 = 1$. Olgu $x \in U$. Omaduse 3) tõestamisel tuleb arvestada nelja erineva võimalusega:

$$\begin{aligned}\chi_A(x) = 0 \text{ ja } \chi_B(x) = 0, & \quad \chi_A(x) = 0 \text{ ja } \chi_B(x) = 1, \\ \chi_A(x) = 1 \text{ ja } \chi_B(x) = 0, & \quad \chi_A(x) = 1 \text{ ja } \chi_B(x) = 1.\end{aligned}$$

Siit järeldub, et

$$\begin{aligned}\chi_A(x) \cdot \chi_B(x) = 1 &\equiv \chi_A(x) = 1 \wedge \chi_B(x) = 1 \\ &\equiv x \in A \wedge x \in B \\ &\equiv x \in A \cap B \\ &\equiv \chi_{A \cap B}(x) = 1,\end{aligned}$$

millest omakorda saame, et $\chi_A(x) \cdot \chi_B(x) = 0 \Leftrightarrow \chi_{A \cap B}(x) = 0$. Ülejäänud omaduste tõestused on analoogilised ja jäetud iseseivaks tööks. ■

Kuna hulgad ja nende karakteristlikud funktsioonid on bijektiivses vastavuses, võimaldavad siintoodud valemid veel ühte viisi hulgateoreetiliste samasuste tõestamiseks. Saame tõestada hulkade vahelisi võrdusi, näidates vastavate karakteristlike funktsioonide võrdsust. Seega, samasuse kontrolliks võime avaldada kummagi hulga karakteristliku funktsiooni nende hulkade karakteristlike funktsioonide kaudu, mis avaldistes esinevad, ja korrutada kõik summad ja vahed läbi ning lihtsustada. Lihtsustamise juures on oluline, et astmenäitajad saab ära jätta, sest karakteristliku funktsiooni väärtuste (0 ja 1) jaoks kehtib $\chi_A(x) \cdot \chi_A(x) = \chi_A(x)$.

Näide 6.10. Olgu U universaalne hulk ja $A, B \subset U$. Tõesta, et $(A \cap B)' = A' \cup B'$.

Lahendus. Tõestuseks piisab näidata, et $\chi_{(A \cap B)'}(x) = \chi_{A' \cup B'}(x)$ iga $x \in U$ korral. Fikseerime $x \in U$. Rakendades lause 6.9 omadusi täiendi, ühisosa ja ühendi kohta saame, et

$$\begin{aligned}\chi_{(A \cap B)'}(x) &= 1 - \chi_{A \cap B}(x) \\ &= 1 - \chi_A(x) \cdot \chi_B(x) \\ &= (1 - \chi_A(x)) + (1 - \chi_B(x)) - (1 - \chi_A(x)) \cdot (1 - \chi_B(x)) \\ &= \chi_{A'}(x) + \chi_{B'}(x) - \chi_{A' \cap B'}(x) \\ &= \chi_{A' \cup B'}(x)\end{aligned}$$

Kuna vasakpoolse hulga ja parempoolse hulga karakteristlikud funktsioonid on võrdsed iga elemendi x korral, on ka vastavad hulgad ise võrdsed. ■

Ülesanne 6.11. Olgu $A, B, C \subset U$ hulgad. Karakteristlike funktsioonide abil tõestada, et

- (a) $(A \cap B) \cup (A \setminus B) = A$;
- (b) $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$;

$$(c) (A \cup B) \times C = (A \times C) \cup (B \times C);$$

$$(d) (A \triangle B) \triangle C = A \triangle (B \triangle C).$$

Karakteristliku funktsiooni arvutamise algoritm (alamprogramm/funktsioon/protseduur mingis programmeerimiskeeles) on üks võimalik viis hulga esitamiseks arvutis. Lihtsast võimalikust väärtusest (0 või 1) hoolimata võib karakteristliku funktsiooni arvutamine olla tõsine probleem. Ta võib

- nõuda palju aega (otsustamine, kas x on algarv või kordarv);
- koguni üldse mitte omada algoritmi (testimine, kas programm P arvutab funktsiooni F).

6.3 Hulga kujutis ja tema omadused

Olgu antud funktsioon $f: X \rightarrow Y$.

Definitsioon 6.12

Kui $x \in X$ ja $y \in Y$ on sellised, et $y = f(x)$, siis elementi y nimetatakse **elemendi x kujutiseks** (ingl *image of x*).

Igal määramispiirkonna X elemendil on parajasti üks kujutis.

Näide 6.13.

1. Vaatleme funktsiooni $f(x) = x^2$, $f: \mathbb{R} \rightarrow \mathbb{R}$. Siis arvu 0 kujutis on 0, sest $f(0) = 0$. Arvude -1 ja 1 kujutis on 1, sest $f(-1) = 1 = f(1)$.
2. Vaatleme funktsiooni $f(x) = \sqrt{x}$, $f: \mathbb{N} \rightarrow \mathbb{R}$. Siis arvu 4 kujutis on 2, sest $f(4) = 2$.
3. Vaatleme funktsiooni $f(x) = x + 1$, $f: \mathbb{R} \rightarrow \mathbb{R}$. Siis arvu 0 kujutis on 1, sest $f(0) = 1$.

Definitsioon 6.14

Hulga $A \subset X$ **kujutiseks** (ingl *image*) nimetatakse hulga Y osahulka $f(A)$, mis koosneb kõikide hulga A elementide kujutistest, st

$$f(A) = \{f(x) : x \in A\} = \{y \in Y : \exists x (x \in A \wedge f(x) = y)\}.$$

NB! Kujutis $\neq$ kujutus. Sõna „kujutus“ tähistab funktsiooni (kujutamise viisi), sõna „kujutis“ tähendab aga funktsiooni väärtust, st kujutamise tulemust.

Näide 6.15.

1. Vaatleme funktsiooni $f(x) = x^2$, $f: \mathbb{R} \rightarrow \mathbb{R}$. Siis $f([-10, 10]) = [0, 100]$ ja $f(\mathbb{R}) = [0, \infty)$.
2. Vaatleme funktsiooni $f(x) = \sin x$, $f: \mathbb{R} \rightarrow \mathbb{R}$. Siis $f(\mathbb{R}) = [-1, 1]$, aga ka $f([- \pi, \pi]) = [-1, 1]$.

3. Vaatleme funktsiooni $f(x) = \ln x$, $f: (0, \infty) \rightarrow \mathbb{R}$. Siis $f((0, 1]) = (-\infty, 0]$.

Teoreem 6.16: Kujutise omadused

Olgu f funktsioon hulgast X hulka Y ja $A, B \subset X$. Siis

1. $f(\emptyset) = \emptyset$;
2. $f(X) \subset Y$;
3. Kui $A \subset B$, siis $f(A) \subset f(B)$;
4. $f(A \cup B) = f(A) \cup f(B)$;
5. $f(A \cap B) \subset f(A) \cap f(B)$.

Märkus 6.17

Üldiselt 2. ja 5. omaduses võrdused ei kehti. Selleks vaatleme funktsiooni $f: X \rightarrow Y$, kus $X = Y = \mathbb{R}$ ja $f(x) = x^2$ iga $x \in \mathbb{R}$ korral. Nüüd $f(X) \neq Y$, sest

$$f(\mathbb{R}) = \{f(x) : x \in \mathbb{R}\} = \{x^2 : x \in \mathbb{R}\} = [0, \infty) \neq \mathbb{R}.$$

Teise võrduse mitte kehtimises veendumiseks vaatleme hulki $A = \{-1\}$ ja $B = \{1\}$. Siis $f(A) = \{1\} = f(B)$, kuid $f(A \cap B) = f(\emptyset) = \emptyset$. Järelikult,

$$\emptyset = f(A \cap B) \neq f(A) \cap f(B) = \{1\}.$$

Teoreemi 6.16 tõestus.

1. Vastavalt hulga kujutise definitsioonile $f(\emptyset) = \{f(x) : x \in \emptyset\}$. Kuna aga ükski x tühja hulka ei kuulu, siis pole paremal olev tingimus rahuldatud ühegi elemendi x korral. Seega on parempoolne hulk tühi.
2. Olgu $y \in f(X)$. Hulga kujutise definitsiooni põhjal $f(X) = \{y \in Y : \exists x (x \in X \wedge f(x) = y)\}$. Seega $y \in Y$.
3. Olgu $A, B \subset X$ ja $A \subset B$. Väite 3. tõestamiseks tuleb meil vastavalt osahulga definitsioonile näidata, et kui $y \in f(A)$, siis $y \in f(B)$. Olgu $y \in f(A)$. Siis hulga kujutise definitsiooni järgi eksisteerib $x \in A$, nii et $y = f(x)$. Kuna $A \subset B$, siis saame $x \in B$. Seega eksisteerib $x \in B$, nii et $y = f(x)$, mistõttu hulga kujutise definitsiooni järgi $y \in f(B)$.
4. Võrduse tõestamiseks näitame, et kehtib järgmine samaväärsuste ahel:

$$\begin{aligned}
y \in f(A \cup B) &\equiv \exists x (x \in A \cup B \wedge y = f(x)) \\
&\equiv \exists x ((x \in A \vee x \in B) \wedge y = f(x)) \\
&\equiv \exists x (x \in A \wedge y = f(x) \vee x \in B \wedge y = f(x)) \\
&\equiv y \in f(A) \vee y \in f(B) \\
&\equiv y \in f(A) \cup f(B).
\end{aligned}$$

5. Olgu $y \in f(A \cap B)$. Hulga kujutise definitsiooni järgi eksisteerib $x \in A \cap B$, nii et $y = f(x)$. Ühisosa definitsiooni järgi kehtib siis $x \in A$ ja $x \in B$. Et $y = f(x)$, siis hulga kujutise definitsiooni järgi saame konjunktsiooni esimesest poolest $y \in f(A)$ ja teisest poolest $y \in f(B)$. Siit saame hulkade ühisosa definitsiooni põhjal $y \in f(A) \cap f(B)$.

■

Teoreemi 6.16 omadused 4. ja 5. kehtivad ka suvalise arvu hulkade ühendi ja ühisosa korral.

Ülesanne 6.18. Olgu X, Y hulgad, $f: X \rightarrow Y$ funktsioon, $\mathcal{I} \neq \emptyset$ ja $A_\alpha \subset X$ iga $\alpha \in \mathcal{I}$ korral. Tõestada, et

$$f\left(\bigcup_{\alpha \in \mathcal{I}} A_\alpha\right) = \bigcup_{\alpha \in \mathcal{I}} f(A_\alpha) \quad \text{ja} \quad f\left(\bigcap_{\alpha \in \mathcal{I}} A_\alpha\right) \subset \bigcap_{\alpha \in \mathcal{I}} f(A_\alpha).$$

6.4 Hulga originaal ja tema omadused

Definitsioon 6.19

Olgu antud funktsioon $f: X \rightarrow Y$. Kui $x \in X$ ja $y \in Y$ on sellised, et $y = f(x)$, siis elementi x nimetatakse funktsiooni f **elemendi y originaaliks** (ingl *inverse image of y*).

Mõnel hulga Y elemendil võib originaale olla üks, mõnel rohkem ja mõnel mitte ühtegi. Näiteks, kui me vaatleme ruutfunktsiooni kui funktsiooni reaalarvude hulgast reaalarvude hulka, siis on igal positiivsel reaalarvul kaks originaali, arvul null on üks originaal ja negatiivsetel reaalarvudel pole mitte ühtegi originaali. Täpsemalt, kui $f(x) = x^2$, $f: \mathbb{R} \rightarrow \mathbb{R}$, siis arvu 1 originaalid on -1 ja 1 , sest $f(-1) = 1$ ja $f(1) = 1$.

Definitsioon 6.20

Hulga $B \subset Y$ **originaaliks** (ingl *inverse image*) nimetatakse hulka $f^{-1}(B)$, mis koosneb kõigist nendest hulga X elementidest, mis kujutuvad hulga B elemendiks, st

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

Tähistus f^{-1} ei tähenda siin, et funktsioonil f peaks leiduma pöördfunktsioon, vaid on lihtsalt sümbol. Küll aga, kui funktsioonil f leidub pöördfunktsioon, siis need mõisted –

hulga B originaal ja hulga B kujutis pöördfunktsiooniga – ühtivad (vt paragrahv 6.9).

Teiseks, pane tähele, et

$$x \in f^{-1}(B) \Leftrightarrow f(x) \in B.$$

Seda lihtsat tähelepanekut on teinekord hea mõnes tõestuses kasutada.

Näide 6.21.

1. Vaatleme funktsiooni $f(x) = x^2$, $f: \mathbb{R} \rightarrow \mathbb{R}$. Siis $f^{-1}(\{1\}) = \{-1, 1\}$ ja $f^{-1}([-10, -5]) = \emptyset$.
2. Vaatleme funktsiooni $f(x) = 0$, $f: \mathbb{R} \rightarrow \mathbb{R}$. Siis $f^{-1}(\{0\}) = \mathbb{R}$.
3. Vaatleme funktsiooni $f(x) = x + 1$, $f: \mathbb{R} \rightarrow \mathbb{R}$. Siis $f^{-1}(\{0\}) = \{-1\}$.

Teoreem 6.22: Originaali omadused

Olgu f funktsioon hulgast X hulka Y ja $A, B \subset Y$. Siis

1. $f^{-1}(\emptyset) = \emptyset$;
2. $f^{-1}(Y) = X$;
3. Kui $A \subset B$, siis $f^{-1}(A) \subset f^{-1}(B)$;
4. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$;
5. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$;
6. $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$.

Tõestus.

1. Vahetult originaali definitsioonist saame, et $f^{-1}(\emptyset) = \{x \in X : f(x) \in \emptyset\}$. Kuna pole selliseid hulga X elemente, mis kujutuvad tühihulga elementideks, siis võrdus kehtib.
2. Vahetult originaali definitsioonist saame, et $f^{-1}(Y) = \{x \in X : f(x) \in Y\}$. Funktsiooni definitsiooni järgi kujutub hulga X iga element mingiks hulga Y elemendiks. Seega võrdus kehtib.
3. Olgu $x \in f^{-1}(A)$. Originaali definitsioonist saame, et siis $f(x) \in A$. Eelduse kohaselt on hulk A hulga B osahulk, ehk siis ka $f(x) \in B$. Hulga originaali definitsiooni järgi kehtib $x \in f^{-1}(B)$.
4. Näitame, et suvalise $x \in X$ korral kehtib $x \in f^{-1}(A \cup B)$ parajasti siis, kui $x \in f^{-1}(A) \cup f^{-1}(B)$.

$$\begin{aligned} x \in f^{-1}(A \cup B) &\equiv f(x) \in A \cup B \\ &\equiv f(x) \in A \vee f(x) \in B \\ &\equiv x \in f^{-1}(A) \vee x \in f^{-1}(B) \\ &\equiv x \in f^{-1}(A) \cup f^{-1}(B). \end{aligned}$$

5. Näitame, et suvalise $x \in X$ korral kehtib $x \in f^{-1}(A \cap B)$ parajasti siis, kui $x \in f^{-1}(A) \cap f^{-1}(B)$.

$$\begin{aligned} x \in f^{-1}(A \cap B) &\equiv f(x) \in A \cap B \\ &\equiv f(x) \in A \wedge f(x) \in B \\ &\equiv x \in f^{-1}(A) \wedge x \in f^{-1}(B) \\ &\equiv x \in f^{-1}(A) \cap f^{-1}(B). \end{aligned}$$

6. Näitame, et suvalise $x \in X$ korral kehtib $x \in f^{-1}(Y \setminus B)$ parajasti siis, kui $x \in X \setminus f^{-1}(B)$.

$$\begin{aligned} x \in f^{-1}(Y \setminus B) &\equiv f(x) \in Y \setminus B \\ &\equiv f(x) \in Y \wedge \neg(f(x) \in B) \\ &\equiv x \in f^{-1}(Y) \wedge \neg(x \in f^{-1}(B)) \\ &\equiv x \in X \wedge x \notin f^{-1}(B) \\ &\equiv x \in X \setminus f^{-1}(B), \end{aligned}$$

kusjuures eelviimane samaväärsus kehtib varem tõestatud seose $f^{-1}(Y) = X$ tõttu. ■

Teoreemi 6.22 omadused 4. ja 5. kehtivad ka suvalise arvu hulkade ühendi ja ühisosa korral.

Ülesanne 6.23. Olgu X, Y hulgad, $f: X \rightarrow Y$ funktsioon, $\mathcal{I} \neq \emptyset$ ja $A_\alpha \subset Y$ iga $\alpha \in \mathcal{I}$ korral. Tõestada, et

$$f^{-1}\left(\bigcup_{\alpha \in \mathcal{I}} A_\alpha\right) = \bigcup_{\alpha \in \mathcal{I}} f^{-1}(A_\alpha) \quad \text{ja} \quad f^{-1}\left(\bigcap_{\alpha \in \mathcal{I}} A_\alpha\right) = \bigcap_{\alpha \in \mathcal{I}} f^{-1}(A_\alpha).$$

Näide 6.24. Hulkade kujutistel ei ole originaalide omadusega 6. analoogilist omadust. Kui näiteks $f: X \rightarrow Y$ on konstantne funktsioon, siis $f(A) = \{c\}$ (kui $A \neq \emptyset$), $f(X \setminus A) = \{c\}$ (kui $A \neq X$) ja $Y \setminus f(A) = Y \setminus \{c\}$ ning ei leia aset sisalduvused $f(X \setminus A) \subset Y \setminus f(A)$ ega ka $f(X \setminus A) \supset Y \setminus f(A)$ (kui $Y \neq \{c\}$).

Nagu näeme, on hulkade originaalide omadused paremad kui hulkade kujutiste omadused, mistõttu funktsioonide põhiomaduste määratlemisel teistes matemaatilistes distsipliinides kasutatakse rohkem hulkade originaale.

6.5 Hulga kujutise originaal ja originaali kujutis

Kujutise ja originaali järjestikuse võtmise korral saame järgmised sisalduvused.

Teoreem 6.25

Olgu $f: X \rightarrow Y$ funktsioon.

1. Kui $A \subset X$, siis $A \subset f^{-1}(f(A))$;
2. Kui $B \subset Y$, siis $f(f^{-1}(B)) \subset B$.

Märkus 6.26

Näidetes 6.27 ja 6.28 veendume, et üldiselt kummaski omaduses võrdused ei kehti.

Teoreemi 6.25 tõestus.

1. Olgu $A \subset X$ ja olgu $x \in A$. Meil on vaja näidata, et $x \in f^{-1}(f(A))$. Hulga kujutise definitsiooni põhjal võime kirjutada $f(x) \in f(A)$. Et saaksime kasutada hulga originaali omadusi, asendame elemendi $f(x) \in Y$ üheelemendilise hulgaga ja vastavalt seose „element“ seosega „osahulk“. Saame $\{f(x)\} \subset f(A)$. Nüüd rakendame sellele seosele teoreemi 6.22 omadust 3 ja saame: $f^{-1}(\{f(x)\}) \subset f^{-1}(f(A))$. Aga $x \in f^{-1}(\{f(x)\})$, sest $f(x) \in \{f(x)\}$ (vt hulga originaali definitsiooni). Kahest viimasest seosest saamegi, et $x \in f^{-1}(f(A))$.
2. Olgu $B \subset Y$ ja olgu $y \in f(f^{-1}(B))$. Meil on vaja näidata, et $y \in B$. Siis kujutise definitsiooni põhjal leidub $x \in f^{-1}(B)$, nii et kehtib $f(x) = y$. Seos $x \in f^{-1}(B)$ tähendab originaali definitsiooni põhjal, et $f(x) \in B$. Seega $y \in B$.

■

Näide 6.27. Veendume, et üldiselt $A \neq f^{-1}(f(A))$.

Olgu $X = Y = \mathbb{R}$, $f(x) = |x|$ ja $A = \{1, 2, 3\}$. Iga $x \in A$ korral kehtib $f(x) = x$, st $f(A) = A = \{1, 2, 3\}$. Teisalt,

$$f^{-1}(f(A)) = f^{-1}(A) = \{-3, -2, -1, 1, 2, 3\} \neq \{1, 2, 3\} = A.$$

Näide 6.28. Veendume, et üldiselt $f(f^{-1}(B)) \neq B$.

Olgu $X = Y = \mathbb{R}$, $f(x) = x^2$ ja $B = \{-1, 0, 4\}$. Funktsiooniga f kujutuvad hulka B hulga $f^{-1}(B) = \{-2, 0, 2\}$ elemendid, mida funktsiooniga f kujutades saame

$$f(f^{-1}(B)) = f(\{-2, 0, 2\}) = \{0, 4\} \neq \{-1, 0, 4\} = B.$$

6.6 Injektiivsed, sürjektiivsed ja bijektiivsed funktsioonid

Definitsioon 6.29

Funktsiooni $f: X \rightarrow Y$ nimetatakse

- (a) **injektiivseks** ehk **üksüheseks** (ingl *injective*), kui iga paari $x_1, x_2 \in X$, $x_1 \neq x_2$, korral $f(x_1) \neq f(x_2)$;
- (b) **sürjektiivseks** ehk **pealekujutuseks** (ingl *surjective*), kui iga $y \in Y$ jaoks leidub selline $x \in X$, et $y = f(x)$;
- (c) **bijektiivseks** ehk **üksüheseks vastavuseks** (ingl *bijective*), kui f on nii injektiivne kui ka sürjektiivne.

Märkus 6.30

Olgu $A: x_1 \neq x_2$ ja $B: f(x_1) \neq f(x_2)$. Eelnevast teame, et lausearvutuse valemid $A \Rightarrow B$ ja $\neg B \Rightarrow \neg A$ on samaväärsed. Järelikult, funktsiooni f injektiivsust saame samaväärselt defineerida ka nii: kui $f(x_1) = f(x_2)$, siis $x_1 = x_2$.

Injektiivsus tähendab, et ühelgi hulga Y elemendil pole rohkem kui üks originaal.

Sürjektiivsus tähendab, et igal hulga Y elemendil leidub vähemalt üks originaal.

Bijektiivsus tähendab, et igal hulga Y elemendil leidub täpselt üks originaal.

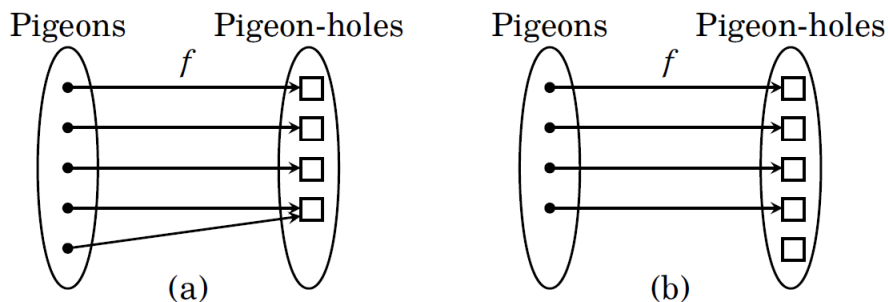
Näide 6.31.

1. Olgu $f(x) = x^2$. Vaatleme sellise avaldisega antud funktsiooni erinevatel hulkadel.
 Funktsioon $f: \mathbb{R} \rightarrow \mathbb{R}$ ei ole injektiivne ega sürjektiivne, sest igaks positiivseks reaalarvuks kujutatakse üks positiivne ja üks negatiivne arv. Negatiivseteks arvudeks ei kujutata ühtegi $\mathbb{R}$ elementi.
 Funktsioonina $f: \mathbb{R} \rightarrow [0, \infty)$ on x^2 sürjektiivne, aga pole injektiivne.
 Funktsioonina $f: [0, \infty) \rightarrow [0, \infty)$ on x^2 injektiivne ja sürjektiivne, st on bijektiivne.
2. Funktsioon $\sin: \mathbb{R} \rightarrow \mathbb{R}$ ei ole injektiivne ega sürjektiivne. Miks?
 Funktsioon $\sin: \mathbb{R} \rightarrow [-1, 1]$ on sürjektiivne, aga pole injektiivne. Miks?
 Funktsioon $\sin: [-\pi/2, \pi/2] \rightarrow \mathbb{R}$ on injektiivne, aga pole sürjektiivne. Miks?
 Funktsioon $\sin: [-\pi/2, \pi/2] \rightarrow [-1, 1]$ on injektiivne ja sürjektiivne, st on bijektiivne.
3. Olgu meil kaks lõplikku hulka $X = \{x_1, \dots, x_m\}$ ja $Y = \{y_1, \dots, y_n\}$, milles on vastavalt m ja n elementi. Uurime, millistel tingimustel leidub injektiivne/sürjektiivne/bijektiivne funktsioon $f: X \rightarrow Y$.
 - (a) **Injektiivsus.** Kui $m > n$, siis iga funktsioon $f: X \rightarrow Y$ peab kujutama mingid hulga X elemendid üheks ja samaks hulga Y elemendiks. Järelikult ei leidu injektiivset funktsiooni $f: X \rightarrow Y$. Kui $m \leq n$, siis saab konstrueerida injektiivse funktsiooni.
 - (b) **Sürjektiivsus.** Kui $m < n$, siis saavad hulga X elementide kujutisteks olla ainult m elementi hulgas Y , st ei leidu sürjektiivset kujutust. Kui $m \geq n$, siis leidub sürjektiivne kujutus.
 - (c) Bijektiivne kujutus leidub parajasti siis, kui $m = n$.
4. Iga reaalarvuliste liikmetega jada $a_1, a_2, \dots$ võime vaadelda kui funktsiooni $a: \mathbb{N} \rightarrow \mathbb{R}$. Kui kõik jada liikmed on erinevad, siis on funktsioon a injektiivne. Näiteks, kui $a_i = 2i$ iga $i \in \mathbb{N}$ korral. Hiljem tõestame, et ükski funktsioon $a: \mathbb{N} \rightarrow \mathbb{R}$ ei saa olla sürjektiivne.

Ülesanne 6.32. Tõesta, et funktsioon $f: X \rightarrow Y$ rahuldab tingimust $f(A \cap B) = f(A) \cap f(B)$ parajasti siis, kui ta on injektiivne.

6.7 Dirichlet' printsiip

Olgu meil A tuvide ja B tuvipuude hulk. Võime vaadelda funktsiooni $f: A \rightarrow B$, kus tuvi x lendab puuri $f(x)$.



- Joonisel (a) on tuvisid rohkem kui tuvipuuere, seega sel juhul vähemalt kaks tuvi peavad lendama ühte puuri. Teisisõnu, f pole injektiivne.
- Joonisel (b) on tuvisid vähem kui tuvipuuere, seega sel juhul jääb vähemalt üks puur tühjaks. Teisisõnu, f pole sürjektiivne.

Eelneva näite üldistus on Dirichlet' printsiip.

Teoreem 6.33: Dirichlet' printsiip

Olgu A ja B lõplikud hulgad ning $f: A \rightarrow B$ funktsioon.

1. Kui $|A| > |B|$, siis f pole injektiivne.
2. Kui $|A| < |B|$, siis f pole sürjektiivne.

Dirichlet' printsiibil on mitmeid huvitavaid rakendusi.

Näide 6.34. Tõestada, et leidub vähemalt kaks eestlast, kellel on täpselt sama palju juuksekarvu.

Näide 6.35. Kui valida juhuslikult kuus naturaalarvu, siis kaks neist annavad viiega jagades sama jäägi.

6.8 Funktsioonide kompositsioon

Täpselt samuti nagu on olemas aritmeetilised tehted (näiteks $+$ või $\cdot$) arvude kombineerimiseks ja hulgateoreetilised tehted (näiteks $\cup$ ja $\cap$) hulkade kombineerimiseks, on olemas ka tehted funktsioonide kombineerimiseks. Liitfunktsiooniks ehk funktsioonide (kujutuste) kompositsiooniks nimetatakse matemaatikas funktsiooni, mis saadakse kahe funktsiooni järjest rakendamisel.

Definitsioon 6.36

Olgu X, Y ja Z mingid hulgad. Funktsioonide $f: X \rightarrow Y$ ja $g: Y \rightarrow Z$ **kompositsiooniks** (ingl *composition*) nimetatakse niisugust funktsiooni $g \circ f: X \rightarrow Z$, et $(g \circ f)(x) = g(f(x))$ iga $x \in X$ korral.

Funktsiooni g nimetatakse siin **välimiseks** funktsiooniks, funktsiooni f **sisemiseks** funktsiooniks. Funktsioonide f ja g kompositsiooni $g \circ f$ nimetatakse ka liitfunktsiooniks. Funktsioonide f ja g liitfunktsiooni või nende liitfunktsiooni väärtuste leidmist nimetatakse ka funktsioonide f ja g järjest rakendamiseks.

Märkus.

1. Funktsioonide kompositsiooni $g \circ f$ on võimalik leida vaid siis, kui funktsiooni g lähtehulk on sama mis funktsiooni f sihthulk (vt näidet 6.37);
2. Kompositsiooni $g \circ f$ määramispiirkond on sama mis funktsiooni f määramispiirkond;
3. Võib juhtuda, et on võimalik defineerida nii $g \circ f$ kui ka $f \circ g$, kuid need kaks funktsiooni ei pruugi samad olla, st üldjuhul $g \circ f \neq f \circ g$ (vt näidet 6.38). Seega, funktsioonide kompositsioon ei ole kommutatiivne.

Näide 6.37. Olgu f selline funktsioon hulgast $\{a, b, c\}$ hulka $\{a, b, c\}$, et $f(a) = b$, $f(b) = c$ ja $f(c) = a$. Olgu g selline funktsioon hulgast $\{a, b, c\}$ hulka $\{1, 2, 3\}$, et $g(a) = 3$, $g(b) = 2$ ja $g(c) = 1$. Millised on $g \circ f$ ja $f \circ g$?

Lahendus. Kompositsioon $g \circ f: \{a, b, c\} \rightarrow \{1, 2, 3\}$ on defineeritud seostega $(g \circ f)(a) = g(f(a)) = g(b) = 2$, $(g \circ f)(b) = g(f(b)) = g(c) = 1$ ja $(g \circ f)(c) = g(f(c)) = g(a) = 3$. Kompositsioon $f \circ g$ ei ole defineeritud, sest funktsiooni f lähtehulk $\{a, b, c\}$ erineb funktsiooni g sihthulgast $\{1, 2, 3\}$. ■

Näide 6.38. Olgu f ja g sellised funktsioonid hulgast $\mathbb{Z}$ hulka $\mathbb{Z}$, et $f(x) = 2x + 3$ ja $g(x) = 3x + 2$ iga $x \in \mathbb{Z}$ korral. Millised on $g \circ f$ ja $f \circ g$?

Lahendus. Kõigepealt märkame, et seekord on mõlemad kompositsioonid $g \circ f$ ja $f \circ g$ defineeritud. Seega

$$(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$$

ja

$$(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11.$$

Pane tähele, et kuigi $g \circ f$ ja $f \circ g$ olid defineeritud, siis näeme, et antud juhul $g \circ f \neq f \circ g$. ■

Näitame nüüd, et funktsioonide kompositsioon on assotsiatiivne tehe.

Lause 6.39

Olgu X, Y, Z ja W hulgad. Kui $f: X \rightarrow Y$, $g: Y \rightarrow Z$ ja $h: Z \rightarrow W$, siis $h \circ (g \circ f) = (h \circ g) \circ f$.

Tõestus. Peame näitama, et kaks funktsiooni on võrdsed. Kuidas seda teha? Selleks näitame kõigepealt, et nende funktsioonide määramis- ja muutumiskiirkonnad on võrdsed, ning seejärel näitame, et iga elemendi x korral nende ühisest määramiskiirkonnast kummagi funktsiooni abil saadud kujutis on sama. Nendest kahest sammust saamegi siis järeldada, et antud funktsioonid on võrdsed.

Seega, kontrollime esiteks, et funktsioonide $h \circ (g \circ f)$ ja $(h \circ g) \circ f$ määramis- ja muutumiskiirkonnad on samad. Kuna $f: X \rightarrow Y$, $g: Y \rightarrow Z$ ja $h: Z \rightarrow W$, siis $g \circ f: X \rightarrow Z$ ja $h \circ g: Y \rightarrow W$. Seega $h \circ (g \circ f): X \rightarrow W$ ja $(h \circ g) \circ f: X \rightarrow W$.

Teiseks kontrollime, et iga $x \in X$ korral nende funktsioonide poolt saadud kujutised on võrdsed. Olgu x hulga X suvaline element. Siis $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$ ja $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$. Järelikult $h \circ (g \circ f) = (h \circ g) \circ f$. ■

Lause 6.40

Kui $f: X \rightarrow Y$ ja $g: Y \rightarrow Z$ on injektiivsed, siis ka $g \circ f: X \rightarrow Z$ on injektiivne.

Tõestus. Olgu $x_1, x_2 \in X$ sellised, et $x_1 \neq x_2$. Siis funktsiooni f injektiivsuse tõttu $f(x_1) \neq f(x_2)$. Viimasest aga järeldub funktsiooni g injektiivsuse tõttu, et $g(f(x_1)) \neq g(f(x_2))$ ehk $(g \circ f)(x_1) \neq (g \circ f)(x_2)$. Järelikult on $g \circ f$ injektiivne. ■

Lause 6.41

Kui $f: X \rightarrow Y$ ja $g: Y \rightarrow Z$ on surjektiivsed, siis ka $g \circ f: X \rightarrow Z$ on surjektiivne.

Tõestus. Valime vabalt $z \in Z$. Siis g surjektiivsuse tõttu leidub $y \in Y$ nii, et $g(y) = z$. Nüüd f surjektiivsuse tõttu leidub $x \in X$ nii, et $f(x) = y$. Seega $(g \circ f)(x) = g(f(x)) = g(y) = z$, mis ütleb, et $g \circ f$ on surjektiivne. ■

Lausetest 6.40 ja 6.41 järeldub vahetult järgmine tulemus.

Järeldus 6.42

Kui $f: X \rightarrow Y$ ja $g: Y \rightarrow Z$ on bijektiivsed, siis ka $g \circ f: X \rightarrow Z$ on bijektiivne.

Definitsioon 6.43

Olgu X hulk. **Samasusteisenduseks** ehk **identsusteisenduseks** (ingl *identity function*) $I_X: X \rightarrow X$ nimetatakse funktsiooni, mis hulga X igale elemendile seab vastavusse sama elemendi, st $I_X(x) = x$ iga $x \in X$ korral.

Kui kontekstist on selge, millise hulga samasusteisendust vaadeldakse, siis tavaliselt alustatakse indeksit ei lisata.

Lause 6.44

Kui $f: X \rightarrow Y$, siis $f \circ I_X = I_Y \circ f = f$.

Tõestus. Peame näitama, et kõik kolm funktsiooni on võrdsed. Tõestamisel kasutame

sama taktikat nagu lause 6.39 tõestamisel. Arutleme kõigepealt selle üle, et miks $f \circ I_X = f$. Kuna $f \circ I_X: X \rightarrow Y$ ja $f: X \rightarrow Y$, siis mõlema funktsiooni määramis- ja muutumispiirkonnad on samad.

Võtame nüüd suvalise elemendi $x \in X$ ja kontrollime $(f \circ I_X)(x) = f(I_X(x)) = f(x)$. Näeme, et elemendi x kujutis mõlema funktsiooniga on sama. Järelikult $f \circ I_X = f$. Tõestus, et $I_Y \circ f = f$ on analoogiline ja seepärast jäetud iseseisvaks tööks. ■

Ülesanne 6.45. Olgu $f: X \rightarrow Y$ ja $g: Y \rightarrow X$ funktsioonid. Tõesta, et kui $g \circ f = I_X$, siis f on injektiivne ja g on surjektiivne.

6.9 Pöördfunktsioon

Olgu $f: X \rightarrow Y$ bijektiivne funktsioon. Kuna f on surjektiivne, siis igal elemendil hulgas Y leidub originaal hulgas X . Veelgi enam, et f on ka injektiivne funktsioon, siis igal elemendil hulgas Y leidub täpselt üks originaal hulgas X . Järelikult, saame defineerida uue funktsiooni hulgas Y hulka X , mis käitub vastupidiselt funktsiooni f poolt antud vastavusega. See arutlus viibki meid pöördfunktsiooni mõiste juurde.

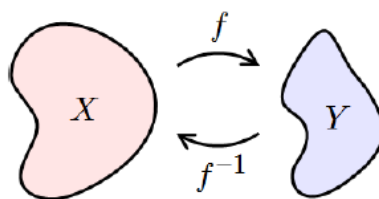
Definitsioon 6.46

Olgu X ja Y hulgad. Bijektiivse funktsiooni $f: X \rightarrow Y$ **pöördfunktsiooniks** (ingl *inverse function*) nimetatakse funktsiooni $f^{-1}: Y \rightarrow X$, mis seab igale $y \in Y$ vastavusse täpselt ühe elemendi $x \in X$, mille korral $f(x) = y$.

Seega, pöördfunktsiooni määramispiirkonnaks on Y ja muutumispiirkonnaks X . Pöördfunktsiooni tähistatakse $x = f^{-1}(y)$, kuid selle asemel kasutatakse pigem kuju $y = f^{-1}(x)$ (vahetatakse sõltuva ja sõltumatu muutuja tähistused).

Paneme tähele, et kui $f^{-1}: Y \rightarrow X$ on funktsiooni $f: X \rightarrow Y$ pöördfunktsioon, siis definitsioonist saame, et iga $x \in X$ ja iga $y \in Y$ korral kehtib

$$f(x) = y \Leftrightarrow f^{-1}(y) = x.$$



Pöördfunktsiooni definitsioonile eelnenud arutlus näitas seda, et funktsioonil f leidub pöördfunktsioon parajasti siis, kui f on bijektiivne. Mainime siinjuures ka ära, et väljen-

did „funktsioon $f: X \rightarrow Y$ on bijektsioon”, „eksisteerib pöördfunktsioon $f^{-1}: Y \rightarrow X$ ”, „funktsioon $f: X \rightarrow Y$ on pööratav” on kõik samaväärsed.

Näide 6.47. Olgu f selline funktsioon hulgast $\{a, b, c\}$ hulka $\{1, 2, 3\}$, et $f(a) = 3$, $f(b) = 2$ ja $f(c) = 1$. Kas leidub f^{-1} , kui jah, siis milline on f^{-1} ?

Lahendus. Esiteks, paneme tähele, et f on bijektiivne (kontrolli!) ja seega leidub f^{-1} . Teiseks, $f^{-1}(1) = c$, $f^{-1}(2) = b$ ja $f^{-1}(3) = a$. ■

Näide 6.48. Olgu $f: \mathbb{Z} \rightarrow \mathbb{Z}$ selline funktsioon, et $f(x) = x + 1$ iga $x \in \mathbb{Z}$ korral. Kas leidub f^{-1} , kui jah, siis milline on f^{-1} ?

Lahendus. Esiteks, paneme tähele, et f on bijektiivne (kontrolli!) ja seega leidub f^{-1} . Teiseks, tähistame esmalt $y = f(x)$. Siis saame, et $y = x + 1$ ehk $x = y - 1$. Viimane tähendab aga seda, et $y - 1$ on täpselt see element, mille f viib elemendiks y . Seega, $f^{-1}(y) = y - 1$. ■

Järgnevalt toome mõned pöördfunktsiooni omadused.

Lause 6.49

Olgu X ja Y hulgad ning $f: X \rightarrow Y$ bijektiivne funktsioon. Siis $f \circ f^{-1} = I_Y$ ja $f^{-1} \circ f = I_X$.

Tõestus. Iseseisevaks tööks. ■

Järgmine tulemus annab lihtsa meetodi, kuidas kahe suvalise funktsiooni puhul kontrollida, kas nad on teineteise pöördfunktsioonid.

Teoreem 6.50

Kui $f: X \rightarrow Y$ ja $g: Y \rightarrow X$ on sellised funktsioonid, et $g \circ f = I_X$ ja $f \circ g = I_Y$, siis eksisteerib f^{-1} ja $f^{-1} = g$.

Tõestus. Kõigepealt näitame, et eksisteerib f^{-1} . Selleks peame veenduma, et f on bijektiivne. Esiteks, f on injektiivne, sest kui $f(x_1) = f(x_2)$, siis

$$x_1 = I_X(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = I_X(x_2) = x_2.$$

Teiseks, f on surjektiivne, sest iga $y \in Y$ korral $f(g(y)) = (f \circ g)(y) = I_Y(y) = y$ ehk elemendil $y \in Y$ leidub originaal $g(y) \in X$. Niisiis, f on bijektiivne.

Viimaks, lausete 6.39, 6.44 ja 6.49 põhjal saame, et

$$f^{-1} = f^{-1} \circ I_Y = f^{-1} \circ (f \circ g) = (f^{-1} \circ f) \circ g = I_X \circ g = g.$$

■

Järeldus 6.51

Kui $f: X \rightarrow Y$ on pööratav, siis ka $f^{-1}: Y \rightarrow X$ on pööratav ja $(f^{-1})^{-1} = f$.

Tõestus. Iseseivaks tööks. ■

Teoreem 6.52

Kui funktsioonidel $f: X \rightarrow Y$ ja $g: Y \rightarrow Z$ leiduvad pöördfunktsioonid, siis ka funktsioonil $g \circ f: X \rightarrow Z$ leidub pöördfunktsioon ja $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Tõestus. Kõigepealt selleks, et funktsioonil $g \circ f: X \rightarrow Z$ leiduks pöördfunktsioon piisab veenduda, et ta on bijektiivne. Kuna funktsioonid f ja g on pööratavad, siis nad on bijektiivsed. Järelduse 6.42 põhjal saame nüüd, et $g \circ f$ on bijektiivne ehk ta on pööratav. Näitame, nüüd et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Teoreemi 6.50 põhjal piisab näidata, et $(g \circ f) \circ (f^{-1} \circ g^{-1}) = I$ ja $(f^{-1} \circ g^{-1}) \circ (g \circ f) = I$. Tõepoolest,

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ I \circ g^{-1} = g \circ g^{-1} = I_Z$$

ja

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ I \circ f = f^{-1} \circ f = I_X.$$

■

Olgu $f: X \rightarrow Y$ funktsioon. Tähistust f^{-1} kasutasime me eespool hulga $B \subset Y$ originaali jaoks, defineerides $f^{-1}(B) = \{x \in X: f(x) \in B\}$. Teisalt, pöördfunktsiooni definitsioon võimaldab aga mõista nüüd vasakul f^{-1} ka kui funktsiooni hulgast Y hulka X ja $f^{-1}(B)$ kui hulga B kujutist selle funktsiooniga. Veendume, et selline mõistmine on kooskõlas varasemaga.

$$\begin{aligned} f^{-1}(B) & \text{ (hulga } B \text{ kujutis funktsiooniga } f^{-1}) \\ &= \{f^{-1}(y) \in X: y \in B\} \\ &= \{x \in X: f(x) \in B\} \\ &= f^{-1}(B) \text{ (hulga } B \text{ originaal funktsiooniga } f), \end{aligned}$$

kus esimene ja viimane võrdus kehtivad vastavalt kujutise ja originaali definitsioonile ning keskmine võrdus $\{f^{-1}(y) \in X: y \in B\} = \{x \in X: f(x) \in B\}$ tänu tähistusele $f^{-1}(y) = x$ ehk $y = f(x)$.

Hulga võimsus

*Matemaatik on masin, mis muudab
kohvi teoreemideks – P. Erdős*

7.1	Hulkade ekvivalentsus	109
7.2	Loenduvad hulgad	112
7.3	Cantor–Bernsteini teoreem	116
7.4	Kontiinumi võimsusega hulgad	117

7.1 Hulkade ekvivalentsus

Hulkade võrdlemine seoste $A \subset B$, $A \neq B$ vms seisukohalt ei paku nii suurt huvi, sest hulgad võivad koosneda väga erinevatest elementidest. Huvitavam oleks võrrelda neid „kvantitatiivselt”, st vastata küsimusele „Kas nendes hulkades on ühepalju elemente?”

Selles peatükis defineerime, milliseid hulki loeme hulgateoorias ühesuurusteks. Lõplike hulkade jaoks on hulkade suuruse mõõduks elementide arv. Lõplike hulkade $A = \{a_1, \dots, a_n\}$ ja $B = \{b_1, \dots, b_m\}$ korral probleemi ei teki: loendame ära hulkade elemendid ja võrdleme arve m ja n . Kui $m = n$, siis on hulkadel ühepalju elemente.

Juba eelajaloolistel aegadel õppisid inimesed hulkade elemente loendama ja lõplikke hulki nende elementide arvu põhjal võrdlema. Anname kõigepealt lõpliku ja lõpmatu hulga definitsiooni ning vaatame üle, mida me teame hulkade suuruse võrdlemisest.

Definitsioon 7.1

Hulka X nimetatakse **lõplikuks** (ingl *finite*), kui X on tühi või leidub selline naturaalarv $n \geq 1$ nii, et X saab seada üksühesesse vastavusse naturaalarvude hulga osahulgaga $\{1, \dots, n\}$. Hulka X nimetatakse **lõpmatuks** (ingl *infinite*), kui ta ei ole lõplik.

On selge, et definitsioonis toodud üksühest vastavust ei saa konstrueerida mitme erineva n puhul ja järelikult seab lõpliku hulga definitsioon igale mittetühjale lõplikule hulgale vastavusse vaid ühe naturaalarvu – selle hulga elementide arvu.

Definitsioon 7.2

Lõpliku hulga X **võimsuseks** (ingl *cardinality*) nimetatakse tema elementide arvu. Hulga võimsust tähistatakse sümboliga $|X|$.

Näiteks, kui $A = \{1, 2\}$ ja $B = \{1, 2, \{1, 2\}, \emptyset\}$, siis $|A| = 2$ ja $|B| = 4$. Samuti $|\emptyset| = 0$.

Järgnevas toome välja lõplike hulkade võimsuste omadusi.

Lause 7.3

Olgu A ja B lõplikud hulgad. Siis

1. $|\mathcal{P}(A)| = 2^{|A|}$
2. $|A \cup B| = |A| + |B| - |A \cap B|$
3. $|A \setminus B| = |A| - |A \cap B|$
4. $|A \times B| = |A| \cdot |B|$

Tõestus. Iseseisvalt! ■

Elementide arvul lõpliku hulga suuruse mõõduna on järgmised omadused:

1. Hulkade X ja Y elementide arvud on võrdsed parajasti siis, kui X ja Y elementide vahel saab defineerida üksühese vastavuse;
2. Hulga X elementide arv on väiksem kui hulga Y elementide arv parajasti siis, kui ei leidu üksühest vastavust hulkade X ja Y vahel, aga leidub üksühene vastavus hulga X ja hulga Y mingi pärisosahulga $B \subsetneq Y$ vahel.

Omaduse 2 põhjal on loomulik lugeda ka iga lõpmatu hulk suuremaks igast lõplikust hulgast.

Omadusest 1 järeldub, et ühtegi lõplikku hulka ei saa seada üksühesesse vastavusse oma pärisosahulgaga. Lõpmatute hulkade puhul aga selline omadus ei kehti. Edasises näeme, et naturaalarvude hulga saab vastavusse seada paarisarvude hulgaga ning, et omavahel saab seada üksühesesse vastavusse suvalised positiivse pikkusega lõigud, näiteks $[0, 2]$ ja $[0, 1]$. Tegelikult saab oma pärisosahulgaga vastavusse seada koguni iga lõpmatu hulga. Neist näidetest esimene ja sellega sarnased olid tuntud juba Vana-Kreeka filosoofidele. Nemad käsitlesid sellist nähtust paradoksina, mille tõttu lõpmatute hulkade uurimisega ei tegeldud. Lõpmatus oli lihtsalt lõplikkuse eitus. Alles 19-nda sajandi teiseks pooleks oli matemaatika jõudnud selliste probleemide uurimiseni, mis tõid kaasa lõpmatuse mõiste liigendamise. Georg Cantor (1845–1918) üldistas elementide arvu mõiste ka lõpmatutele

hulkadele nn hulga võimsuse mõistena ja tulemuseks oli erinevate lõpmatute võimsuste avastamine.

Definitsioon 7.4

Hulgad X ja Y on **ekvivalent** ehk **sama võimsusega** (ingl *equivalent sets*), kui leidub bijektsioon $f: X \rightarrow Y$.

Asjaolu, et hulgad X ja Y on ekvivalentid tähistatakse tavaliselt kas $X \sim Y$ või $|X| = |Y|$.

Vaatame järgmiseks mõningaid üksüheseid vastavusi, mis annavad meile ekvivalentsete hulkade näiteid.

Näide 7.5. Kaks lõplikku hulka X ja Y on ekvivalentid parajasti siis, kui nende elementide arvud on võrdsed, ehk teisisõnu, kui hulgas X on k elementi, siis on hulk X ekvivalentne iga sellise hulgaga, milles on samuti k elementi.

Näide 7.6. Olgu $X = \mathbb{N}$ ja $Y = \{x \in \mathbb{N} : x \text{ on paarisarv}\}$. Bijektsiooniks $f: X \rightarrow Y$ on $f(x) = 2x$ iga $x \in \mathbb{N}$ korral ning seega hulgad X ja Y on sama võimsusega ehk positiivseid paarisarve on täpselt sama palju kui naturaalarve.

Näide 7.7. Hulga $\mathbb{N}$ ja täisarvude hulga $\mathbb{Z}$ vahel saab üksühese vastavuse üles seada järgmise bijektsiooni $f: \mathbb{N} \rightarrow \mathbb{Z}$, kui defineerida:

$$f(x) = \begin{cases} \frac{x-1}{2}, & \text{kui } x \text{ on paaritu arv} \\ -\frac{x}{2}, & \text{kui } x \text{ on paarisarv.} \end{cases}$$

Selle funktsiooni pöördfunktsioon $f^{-1}: \mathbb{Z} \rightarrow \mathbb{N}$ on kujul:

$$f^{-1}(x) = \begin{cases} 2x + 1, & \text{kui } x \geq 0 \\ -2x, & \text{kui } x < 0. \end{cases}$$

Seega, täisarve on sama palju kui naturaalarve.

Näide 7.8. Olgu $a, b, c, d \in \mathbb{R}$. Kui $a < b$ ja $c < d$, siis $[a, b] \sim [c, d]$, $(a, b) \sim (c, d)$ ja $[a, b) \sim [c, d)$. Bijektsiooniks kõigil juhtudel sobib lineaarne funktsioon

$$f(x) = \frac{(d-c)x + bc - ad}{b-a}, \quad x \in [a, b] \text{ (või } x \in (a, b) \text{ või } x \in [a, b)).$$

Näide 7.9. Vahemik $(-\frac{\pi}{2}, \frac{\pi}{2})$ ja arvsirge $\mathbb{R}$ on sama võimsusega, sest funktsioon $\tan: (-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R}$ on bijektsioon.

Näide 7.10. Reaalarvude paaride hulk $\mathbb{R}^2$ ja kompleksarvude hulk $\mathbb{C}$ on sama võimsusega, sest mõlemad saab seada üksühesesse vastavusse tasandi kõigi punktide hulgaga. Otseselt saab selle vastavuse korraldada funktsiooniga $f: \mathbb{R}^2 \rightarrow \mathbb{C}$, kus $f((a, b)) = a + bi$ iga $(a, b) \in \mathbb{R}^2$, kus $i^2 = -1$.

Järgnevas loetleme üles olulisemad hulkade ekvivalentsuse omadused.

Lause 7.11: Hulkade ekvivalentsuse omadused

Olgu A, B ja C hulgad. Siis

1. $A \sim A$ (*refleksiivsus*);
2. Kui $A \sim B$, siis $B \sim A$ (*sümmeetrilisus*);
3. Kui $A \sim B$ ja $B \sim C$, siis $A \sim C$ (*transitiivsus*).

Tõestus.

1. Hulgale A defineeritud samasusteisendus I_A seab hulga A üksühesesse vastavusse iseendaga;
2. Kui $A \sim B$, siis leidub bijektsioon $f: A \rightarrow B$. Funktsiooni f pöördfunktsioon $f^{-1}: B \rightarrow A$ on siis samuti bijektsioon (kontrolli seda!);
3. Kui $A \sim B$ ja $B \sim C$, siis leiduvad bijektsioonid $f: A \rightarrow B$ ja $g: B \rightarrow C$. Nende kompositsioon $g \circ f: A \rightarrow C$ on siis samuti bijektsioon (miks?).

■

7.2 Loenduvad hulgad**Definitsioon 7.12**

Hulka X nimetatakse **loenduvaks** (ingl *countably infinite*), kui leidub bijektsioon hulga X ja naturaalarvude hulga $\mathbb{N}$ vahel.

Seega loenduvad on parajasti need hulgad X , mida saab esitada kujul $X = \{x_1, x_2, \dots\}$. Tõestame selle väite allpool (vt lause 7.14), esialgu aga vaatame näiteid loenduvatest hulkadest.

Näide 7.13.

1. Täisarvude hulk ja paaris naturaalarvude hulk on loenduvad hulgad;
2. Igasugune hulga $\mathbb{N}$ lõpmatu osahulk on ise loenduv ning sama võimsusega kui naturaalarvude hulk $\mathbb{N}$.
3. Ratsionaalarvude hulk $\mathbb{Q}$ on loenduv ning sama võimsusega kui naturaalarvude hulk $\mathbb{N}$ või täisarvude hulk $\mathbb{Z}$.

Intuiitiivselt tundub meile, et ratsionaalarve peaks olema palju rohkem kui täisarve, sest iga kahe täisarvu vahel on lõpmata palju ratsionaalarve ning iga kahe ratsionaalarvu vahel omakorda lõpmata palju ratsionaalarve. Cantor oli aga see mees, kes esimesena näitas, et ratsionaalarvude hulk on loenduv ehk üksüheses vastavuses naturaalarvude hulgaga.

4. Saades nüüd teada, et ratsionaalarvude hulk on ka loenduv, võib loomulikult tekkida tunne, et kõik lõpmatud hulgad on loenduvad. Aga see ei ole nii. Taas oli selleks esimeseks meheks Cantor, kes näitas, et hulga $\mathbb{N}$ kõikide osahulkade hulk $\mathcal{P}(\mathbb{N})$ ei ole loenduv, täpselt samuti nagu ei ole loenduvad irratsionaalarvude hulk $\mathbb{I}$ või reaalarvude hulk $\mathbb{R}$. Veelgi põnevam, ka vahemik $(0, 1)$ ei ole loenduv.

Tõestame kõigepealt mõned üldised teoreemid loenduvate hulkade kohta.

Lause 7.14

Hulk X on loenduv parajasti siis, kui hulga X elemendid saab esitada paarikaupa erinevate elementide lõpmatu jadana: $X = \{x_1, x_2, \dots\}$.

Tõestus. Näitame esmalt, et kui X on loenduv, siis ta esitub paarikaupa erinevate elementide lõpmatu jadana. Kuna X on loenduv hulk, siis loenduvuse mõiste kohaselt leidub bijektsioon $f : \mathbb{N} \rightarrow X$. Tähistame iga $n \in \mathbb{N}$ korral $x_n := f(n)$. Kujutuse f injektiivsuse tõttu järeldub võrdusest $x_n = x_m$, et $n = m$, seega

$$X = \{f(n) \mid n \in \mathbb{N}\} = \{x_1, x_2, \dots\}$$

ehk hulga X elemendid on esitatavad paarikaupa erinevate elementide jadana, nagu tarvis. Teisalt, kehtigu

$$X = \{x_n \mid n \in \mathbb{N}\}$$

st oletame, et hulk X esitub paarikaupa erinevate elementide jadana. Näitame, et siis X on loenduv. Defineerime kujutuse $f : \mathbb{N} \rightarrow X$ võrdusega $f(n) = x_n$. Näitame, et f on bijektiivne. Esiteks, olgu $m, n \in \mathbb{N}$ valitud nii, et $m \neq n$. Kuna hulgas X on eelduse kohaselt paarikaupa erinevad elemendid, siis ka $x_m \neq x_n$. See tähendab, et f on injektiivne. Teiseks, olgu $y \in X$ suvaline. Eelduse kohaselt leidub $n \in \mathbb{N}$ nii, et $y = x_n = f(n)$. Järelikult on f surjektiivne. Kuna hulga X ja $\mathbb{N}$ on üksüheses vastavuses, siis X on loenduv hulk, nagu tarvis. ■

Teoreem 7.15

Iga lõpmatu hulk sisaldab loenduvat osahulga.

Tõestus. Olgu X suvaline lõpmatu hulk (seega ta pole lõplik, sealhulgas $X \neq \emptyset$). Seetõttu leidub temas elemente ja järgnevalt kirjeldamegi, kuidas hulga X elemente valides saab moodustada paarikaupa erinevate elementidega lõpmatu jada.

1. Valime elemendi $x_1 \in X$. See on võimalik, sest X ei ole tühi.
2. Valime elemendi $x_2 \in X \setminus \{x_1\}$. See on võimalik, sest kui hulk $X \setminus \{x_1\}$ oleks tühi, siis peaks kehtima, et $X = \{x_1\}$ ja seega olema lõplik.
3. Valime elemendi $x_3 \in X \setminus \{x_1, x_2\}$. See on võimalik, sest kui hulk $X \setminus \{x_1, x_2\}$ oleks tühi, siis peaks kehtima, et $X = \{x_1, x_2\}$ ja seega olema lõplik.

Seda valikut saab piiramatult jätkata ja tekib lõpmatu jada $Y = \{x_1, x_2, x_3, \dots\}$, mille elemendid on paarikaupa erinevad, sest konstruktsiooni järgi erineb iga valitud element kõigist eelmistest. Olemegi saanud loenduva osahulga $Y \subset X$. ■

Teoreem 7.16

Loenduva hulga iga lõpmatu osahulk on loenduv.

Tõestus. Olgu X loenduv ja $Y \subset X$ lõpmatu osahulk. Kuna X on loenduv, siis lause 7.14 põhjal

$$X = \{x_n \mid n \in \mathbb{N}\}.$$

Vaatleme hulga Y karakteristikku funktsiooni χ_Y hulga X suhtes st iga $x \in X$ korral

$$\chi_Y(x) = \begin{cases} 1, & x \in Y \\ 0, & x \in X \setminus Y \end{cases}.$$

Näeme, et kehtib

$$Y = \{x \in X \mid \chi_Y(x) = 1\}.$$

Hulk Y esitub paarikaupa erinevate elementide jadana, sest ta on lõpmatu hulk ning sisaldab üksnes hulga X elemente. Lause 7.14 põhjal on Y loenduv hulk. ■

Teoreeme 7.15 ja 7.16 on loomulik mõista nii, et loenduv võimsus on vähim lõpmatu võimsus.

Näide 7.17. Naturaal-, täis- ja ratsionaalarvude hulga kõik lõpmatud osahulgad on loenduvad.

Järgmiseks teeme kindlaks rea loenduvuse omadusi, mis on seotud ühendi ja otsekorruutisega.

Teoreem 7.18: Loenduvate hulkade omadused

1. Loenduva hulga ja lõpliku hulga ühend on loenduv.
2. Kahe loenduva hulga ühend on loenduv.
3. Lõpliku hulga loenduvate hulkade ühend on loenduv.
4. Loenduva hulga paarikaupa erinevate lõplike hulkade ühend on loenduv.
5. Loenduva hulga loenduvate hulkade ühend on loenduv.
6. Kahe loenduva hulga otsekorruutis on loenduv.
7. Lõpliku arvu loenduvate hulkade otsekorruutis on loenduv.

Tõestus. Tõestame 5. väite, ülejäänud väidete tõestused jäävad iseseisvaks tööks.

Üldisust kitsendamata võime eeldada, et hulgad A_i on paarikaupa mittelõikuvad. Olgu

$$A_1 = \{a_{11}, a_{12}, \dots, a_{1n}, \dots\}$$

$$A_2 = \{a_{21}, a_{22}, \dots, a_{2n}, \dots\}$$

$$A_3 = \{a_{31}, a_{32}, \dots, a_{3n}, \dots\}$$

...

Siis võime kirjutada, et $\bigcup_{i=1}^{\infty} A_i = \{a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \dots\}$ ehk lause 7.14 põhjal on $\bigcup_{i=1}^{\infty} A_i$ loenduv. ■

Märkus. Nii teoreemi 7.15 kui ka teoreemi 7.18 omaduse 5 tõestus sisaldab ilmutamata kujul valikuaksioomi kasutamist, mille kohta saab rohkem lugeda paragrahvist 9.1.

Näide 7.19. Saadud üldiste tulemuste abil saamegi nüüd näidata, et mitmed matemaatikast tuntud hulgad on loenduvad. Eelpool juba mainisime, et ratsionaalarvude hulk on loenduv. Tõepoolest, kuna kõik ratsionaalarvud on üheselt esitatavad taandumatu murru kujul $\frac{m}{n}$, kus $m \in \mathbb{Z}$ ja $n \in \mathbb{N}$, siis funktsioon $f: \mathbb{Q} \rightarrow A \subset \mathbb{Z} \times \mathbb{N}$, kus $f(\frac{m}{n}) = (m, n)$ ja A koosneb taandumatutest murdudest koosnevatest paaridest, on bijektsioon (kontrolli!). Näiteks, $(3, 4) \in A$, aga $(6, 8) \notin A$. Järelikult, $\mathbb{Q} \sim A$. Kuna $\mathbb{Z}$ ja $\mathbb{N}$ on loenduvad, siis teoreemi 7.18 seitsmenda väite põhjal $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N}$. Teisalt, teoreemi 7.16 põhjal saame, et $A \sim \mathbb{N}$. Seega oleme näidanud, et $\mathbb{Q} \sim A \sim \mathbb{N}$, teisisõnu ratsionaalarvude hulk on loenduv.

Samuti on loenduvad kahe- ja kolmemõõtmelise ruumi ratsionaalarvuliste koordinaatidega punktide hulk ning ka ratsionaalsete kordajatega polünoomide hulk jne.

Arvutite kasutamisel tegutseme me tegelikult loenduvate hulkade piirides. Kogu informatsioon esitatakse arvuti mälus naturaalarvude kujul. See tähendab, et fikseeritud viisil esitatavaid andmeid (reaalarve, programme, keele sõnu jm) on potentsiaalselt loenduv hulk. „Potentsiaalselt“ tähendab siin seda, et mälu suurus ja/või andmetüübi määrand loikavad sellest hulgast tegelikult lõpliku alamhulga, aga põhimõtteliselt on võimalik seda lõplikku osahulka kui tahes suureks teha (kasutades suurema mäluga arvutit, dünaamilisi andmestruktuure jms). Programmi kirjutades me enamasti mõtleme selle lõpmatu hulga elementidele (näiteks suvalistele täisarvudele). Aga mõnede probleemide juures arvestame ka piiranguid.

Järgmine näide väidab, et mitmed informaatika ja programmeerimise jaoks tähtsad hulgad on loenduvad.

Näide 7.20.

1. Kui A on lõplik tähestik $\{a_1, a_2, \dots, a_n\}$, siis kõigi (lõpliku pikkusega) sõnade hulk tähestikus A on loenduv.
2. Programmide hulk igas programmeerimiskeeles on loenduv.
3. Kui A on loenduv tähestik $\{a_1, a_2, \dots\}$, siis kõigi (lõpliku pikkusega) sõnade hulk tähestikus A on loenduv.

Ka need väited järelduvad üsna lihtsalt loenduvuse üldistest omadustest.

7.3 Cantor–Bernsteini teoreem

Definitsioon 7.21

Ütleme, et hulga A **võimsus ei ületa** (ingl *cardinality less than or equal*) hulga B võimsust, kui leidub injeksioon $f: A \rightarrow B$.

Asjaolu, et hulga A võimsus ei ületa hulga B võimsust tähistatakse tavaliselt nii $|A| \leq |B|$.

Märgime, et injeksiooni $f: A \rightarrow B$ leidumine on samaväärne sellega, et leidub bijeksioon $f: A \rightarrow f(A) \subset B$.

Näide 7.22.

1. Vaatleme lõplikku hulka $A = \{a_1, \dots, a_n\}$. Funktsioon $f: A \rightarrow \mathbb{N}$, kus $f(a_k) = k$, $k = 1, \dots, n$, on injeksioon, seega hulga A võimsus ei ületa hulga $\mathbb{N}$ võimsust.
2. Kui $A \subset B$, siis funktsioon $f: A \rightarrow B$, kus $f(a) = a$, $a \in A$, on injeksioon. Seepärast osahulga võimsus ei ületa hulga enda võimsust. Näiteks, hulga $\mathbb{N}$, aga ka $\mathbb{Q}$ võimsus, ei ületa hulga $\mathbb{R}$ võimsust.

Efektiivne vahend hulkade ekvivalentsuse tõestamiseks on järgmine tulemus, mille tõestuse võib leida näiteks õpikust [6].

Teoreem 7.23: Cantor–Bernsteini teoreem

Kui hulga A võimsus ei ületa hulga B võimsust ja hulga B võimsus ei ületa hulga A võimsust, siis hulgad A ja B on sama võimsusega.

Teisisõnu, Cantor–Bernsteini teoreem ütleb, et kui eksisteerivad injektiivsed funktsioonid $f: A \rightarrow B$ ja $g: B \rightarrow A$, siis hulgad A ja B on sama võimsusega. Või veel lühemalt, kui $|A| \leq |B|$ ja $|B| \leq |A|$, siis $|A| = |B|$.

Näide 7.24. Tõesta, et $(0, 1) \sim (0, 1]$.

Lahendus 1. Kõigepealt märgime, et ei ole üldse ilmne, kuidas konstrueerida bijeksiooni hulkade $(0, 1)$ ja $(0, 1]$ vahel. Tänu Cantor–Bernsteini teoreemile piisab meil konstrueerida ainult kaks injeksiooni, mis on palju lihtsam ülesanne.

Esiteks, injeksiooniks hulgast $(0, 1)$ hulka $(0, 1]$ sobib $f(x) = x$ iga $x \in (0, 1)$ korral, sest $(0, 1) \subset (0, 1]$.

Teistpidi, injeksiooniks hulgast $(0, 1]$ hulka $(0, 1)$ sobib $g(x) = \frac{x}{2}$ iga $x \in (0, 1]$ korral, sest g on injektiivne ja $g((0, 1]) = (0, \frac{1}{2}] \subset (0, 1)$.

Kuna oleme konstrueerinud injeksioonid $f: (0, 1) \rightarrow (0, 1]$ ja $g: (0, 1] \rightarrow (0, 1)$, siis teoreemi 7.23 põhjal $(0, 1) \sim (0, 1]$. ■

Esitame nüüd ka alternatiivse lahenduse, kus konstrueerime konkreetse bijeksiooni $(0, 1)$ ja $(0, 1]$ vahel.

Lahendus 2. Olgu

$$A = \left\{ \frac{1}{n+1} : n \in \mathbb{N} \right\} \subset (0, 1) \quad \text{ja} \quad B = \left\{ \frac{1}{n} : n \in \mathbb{N} \right\} \subset (0, 1].$$

Siis $A \sim B$, sest $f: A \rightarrow B$, kus $f(\frac{1}{n}) = \frac{1}{n-1}$, $n \geq 2$, on bijektsioon (kontrolli!). Otsitavaks bijektsiooniks sobib (kontrolli!) $g: (0, 1) \rightarrow (0, 1]$, kus

$$g(x) = \begin{cases} f(x), & \text{kui } x \in A \\ x, & \text{kui } x \in (0, 1) \setminus A. \end{cases}$$

■

Ülesanne 7.25. Tõesta, et $(0, 1) \sim [0, 2)$ ja $(0, 1) \sim [0, 3]$.

7.4 Kontiinumi võimsusega hulgad

Lõpmatute hulkade võrdlemisel poleks mõtet, kui nad kõik oleksid loenduvad. Hulgateooria looja G. Cantor kulutas palju aega, püüdes tõestada reaalarvude hulga $\mathbb{R}$ loenduvust. Oma üllatuseks ta avastas, et see hulk ja kõik tema lõigud ning vahemikud on mitteloenduvad.

Esimeseks sammuks lõpmatute võimsuste uurimisel on järgmine teoreem.

Teoreem 7.26

Vahemik $(0, 1)$ ja naturaalarvude hulk $\mathbb{N}$ ei ole ekvivalentsed.

Tõestus. Oletame vastuväiteliselt, et hulk $(0, 1)$ on loenduv, st hulkade $\mathbb{N}$ ja $(0, 1)$ vahel leidub üksühene vastavus. Sellisel juhul peab vahemik $(0, 1)$ esituma loenduva hulganäitega: $(0, 1) = \{x_1, x_2, x_3, \dots\}$. Kirjutame välja selle hulga kõik arvud järgmiselt:

$$\begin{aligned} x_1 &= 0, a_{11}a_{12}a_{13} \dots a_{1j} \dots \\ x_2 &= 0, a_{21}a_{22}a_{23} \dots a_{2j} \dots \\ x_3 &= 0, a_{31}a_{32}a_{33} \dots a_{3j} \dots \\ &\dots, \end{aligned}$$

kus a_{ij} on arvude kümnendnumbrid $(0, 1, 2, \dots, 9)$, kusjuures a_{ij} on arvu x_i j -s kümnendnumber. Moodustame nüüd uue arvu $y = 0, b_1b_2b_3 \dots b_j \dots$, kus $b_1 \neq a_{11}$, $b_2 \neq a_{22}$, $\dots$, $b_j \neq a_{jj}$ ning iga j korral $b_j \neq 9$ ja $b_j \neq 0$. Esimesed tingimused hoolitsevad selle eest, et see uus arv y ei kuulu ülaltoodud arvude loenduvasse „nimekirja“ (miks?), viimased kaks tingimust garanteerivad, et kümnendmurd kujutaks endast reaalarvu ja see arv poleks 0. Seega, saadud reaalarv y kuulub vahemikku $(0, 1)$ ja erineb kõigist paaride parempoolseteks komponentideks olevatest arvudest, mistõttu see paaride hulk ei saa olla üksühene vastavus $\mathbb{N}$ ja $(0, 1)$ vahel. ■

Järeldus 7.27

1. Iga vahemik (a, b) arvsirgel on ekvivalentne vahemikuga $(0, 1)$ ja seega ei ole loenduv;
2. $\mathbb{R}$ on ekvivalentne vahemikuga $(0, 1)$ ja seega ei ole loenduv.

Tõestus. Esimene väide järeldub vahetult näitest 7.8 ja teine väide näidetest 7.8 ja 7.9, sest $(0, 1) \sim (-\frac{\pi}{2}, \frac{\pi}{2}) \sim \mathbb{R}$. ■

Seega leidub lõpmatuid hulki, mis ei ole võrdse võimsusega.

Definitsioon 7.28

Hulka, mis on ekvivalentne hulgaga $\mathbb{R}$ nimetatakse **kontiinumi võimsusega** (ingl *cardinality of continuum*) hulgaks.

Niisiis, hulk $\mathbb{R}$ ja kõik vahemikud (a, b) ning ka lõigud $[a, b]$, kus $a < b$, on kontiinumi võimsusega.

Näide 7.29. Irratsionaalarvude hulk $\mathbb{I}$ on kontiinumi võimsusega. Tõepoolest, kuna $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$ ja $\mathbb{Q}$ on loenduv hulk, siis $\mathbb{I}$ ei saa olla loenduv, sest vastasel juhul (vt teoreem 7.18, väide 2) oleks ka $\mathbb{R}$ loenduv hulk. Järelikult, $\mathbb{I}$ on kontiinumi võimsusega hulk.

Et iga lõpmatu hulk sisaldab loenduva osahulga (vt teoreem 7.15), siis võib arvata, et loenduva hulga võimsus on kõige väiksem lõpmatutest võimsustest.

Definitsioon 7.30

Kui hulga A võimsus ei ületa hulga B võimsust ning A ja B ei ole ekvivalentsed, siis öeldakse, et hulga A **võimsus on väiksem kui** (ingl *cardinality strictly less than*) hulga B võimsus.

Teisisõnu, kui leidub injeksioon $f: A \rightarrow B$ ja ei leidu surjektsiooni $g: A \rightarrow B$, siis öeldakse, et hulga A võimsus on väiksem kui hulga B võimsus ja kirjutatakse $|A| < |B|$.

Näiteks, mis tahes lõpliku hulga A võimsus on väiksem kui naturaalarvude $\mathbb{N}$ võimsus. Samuti naturaalarvude $\mathbb{N}$ (või $\mathbb{Q}$ või $\mathbb{Z}$) võimsus on väiksem kui vahemiku $(0, 1)$ (või $\mathbb{R}$) võimsus.

Nüüd oleme ka võimelised põhjendama üht varem toodud väidet (vt näide 6.31), kus ütlesime, et jada $a: \mathbb{N} \rightarrow \mathbb{R}$ ei saa olla surjektiivne. Vaatleme hulka $a(\mathbb{N})$. Ta saab olla kas lõplik või loenduv olenevalt sellest, kas jadas $a(1), a(2), \dots$ on lõplik või lõpmatu hulk erinevaid liikmeid. Mõlemal juhul on hulga $a(\mathbb{N})$ võimsus väiksem kui hulga $\mathbb{R}$ võimsus, seega $a(\mathbb{N}) \neq \mathbb{R}$.

Siinkohal tasuks märkida, et seni me pole defineerinud, mis on hulga võimsus. Me oleme rääkinud ainult erinevate hulkade võimsuste võrdlemisest. Populaarselt võib öelda, et hulga

võimsus on temaga sama võimsate hulkade klass (täpse definitsiooni anname järgmises peatükis, vt definitsioon 8.70). Hulga A võimsust tähistatakse sümboliga $|A|$ või $\text{card } A$ ning nimetatakse **kardinaalarvuks**. Kui $A = \{a_1, \dots, a_n\}$, siis kirjutame $|A| = n$, samuti $|\emptyset| = 0$. Loenduva hulga võimsust tähistatakse sümboliga $\aleph_0$ (loe alef-null) ehk $|\mathbb{N}| = \aleph_0$. Kontiinummi võimsusega hulki tähistatakse sümboliga c ehk $|\mathbb{R}| = c$. Kokkuvõtvalt teame, et iga $n \in \mathbb{N}$ korral

$$n < |\mathbb{N}| < |\mathbb{R}|.$$

Nüüd tekib aga küsimus, et kas on olemas veel suurema võimsusega hulki, st kas on ka kontiinumist suurema võimsusega hulki? Jaatava vastuse viimasele küsimusele annab järgnev teoreem.

Teoreem 7.31: Cantori teoreem

Iga hulga A kõigi osahulkade hulga $\mathcal{P}(A)$ võimsus on suurem kui hulga A võimsus, st $|A| < |\mathcal{P}(A)|$.

Tõestus. Peame näitama, et $|A| \leq |\mathcal{P}(A)|$ ja $|A| \neq |\mathcal{P}(A)|$. Võime eeldada, et $A \neq \emptyset$, sest tühja hulga korral see väide kehtib kindlasti.

Esiteks, $|A| \leq |\mathcal{P}(A)|$, sest funktsioon $f: A \rightarrow \mathcal{P}(A)$, kus $f(a) = \{a\}$ iga $a \in A$ korral, on injektiivne.

Veendumaks, et $|A| \neq |\mathcal{P}(A)|$, oletame vastuväiteliselt, et $|A| = |\mathcal{P}(A)|$. Siis leidub bijektsioon $f: A \rightarrow \mathcal{P}(A)$. Defineerime hulga

$$B := \{x \in A : x \notin f(x)\}.$$

Kuna $B \subset A$ ja f on surjektiivne, siis leidub $a \in A$ nii, et $B = f(a)$. Uurime nüüd, kas $a \in B$. Paneme tähele, et

$$a \in B \Rightarrow a \notin f(a) \Rightarrow a \notin B$$

ja

$$a \notin B \Rightarrow a \in f(a) \Rightarrow a \in B.$$

Seega, $a \in B \Leftrightarrow a \notin B$, mis on vastuolu. Järelikult peab kehtima, et $|A| < |\mathcal{P}(A)|$. ■

Niisiis on olemas hulk, mille võimsus on suurem kontiinummi võimsusest – näiteks hulga $\mathbb{R}$ kõigi osahulkade hulk $\mathcal{P}(\mathbb{R})$. Veelgi enam, Cantori teoreemi korduval rakendamisel saame, et kehtib järgmine võrratuste ahel:

$$|\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{R})))| < \dots$$

Kokkuvõttes saame, et on olemas kui tahes suure võimsusega hulgad. Võimsuste teooria on teinud hulgateooriast (mis on ka mugav matemaatiline keel) matemaatika sisulise haru.

Cantori teoreemist järeldub, et ei ole olemas kõikide hulkade hulka ehk sellist kogumit ei saa vaadelda hulgana. Tõepoolest, selline „hulk” peaks sisaldama osahulgana ka oma kõikide osahulkade hulka, mis pole Cantori teoreemi kohaselt võimalik.

Et $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$, siis tekib loomulik küsimus, kas leidub selline hulk A nii, et $|\mathbb{N}| < |A| < |\mathcal{P}(\mathbb{N})|$. Cantor arvas, et sellist hulka A ei saa olemas olla, kuid ei suutnud seda tõestada. Seega püstitas ta 1878. aastal järgmise hüpoteesi.

Hüpotees 7.32: Kontiinumi hüpotees

Ei leidu sellist hulka X nii, et

$$|\mathbb{N}| < |X| < |\mathcal{P}(\mathbb{N})|.$$

Kontiinumi hüpoteesi võib sõnastada ka teisiti. Me teame juba, et ratsionaalarvude hulk on loenduv ehk $|\mathbb{Q}| = |\mathbb{N}|$. Teisalt teame, et $\mathbb{R}$ on kontiinumi võimsusega. Saab tõestada, et $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$ (vt [6, lk 50]). Seega kontiinumi hüpoteesi saame ümber sõnastada nii:

ei leidu sellist hulka $X \subset \mathbb{R}$ nii, et $|\mathbb{Q}| < |X| < |\mathbb{R}|$.

Tavaliste hulgateooria aksiomaatikate (näiteks Zermelo–Fraenkeli aksiomaatika koos valikuaksioomiga) puhul ei saa aksioomidest tuletada ei kontiinumhüpoteesi ega selle eitust. Aastal 1940 näitas Kurt Gödel, et harilikele hulgateooria aksioomidele valikuaksioomi ja kontiinumhüpoteesi lisamisega saadakse mittevasturääkiv aksioomide süsteem. Aga aastal 1963 näitas USA matemaatik Paul Cohen, et samadele aksioomidele lisades nii valikuaksioomi eituse kui ka kontiinumhüpoteesi eituse saadakse samuti mittevasturääkiv aksioomide süsteem. Lihtsustatult võib öelda, et saab vaadelda kahesugust hulgateooriat: üht, milles kontiinumi hüpotees kehtib (pole vahepealseid võimsusi $|\mathbb{N}| < |\mathbb{R}|$ vahel), ja teist, milles kehtib kontiinumi hüpoteesi eitus (ehk leiduvad vahepealsed võimsused $|\mathbb{N}| < \dots < |\mathbb{R}|$).

Eeldusel, et kontiinuumi hüpotees on tõene, defineeritakse $\aleph_1$ hulga $\mathbb{R}$ võimsusena. See kardinaalarv on võimsuselt järgmine $\aleph_0$ järel. Sel juhul kehtib:

$$\aleph_1 = 2^{\aleph_0} \text{ ehk } |\mathbb{R}| = 2^{|\mathbb{N}|}.$$

Seosed

*Matemaatikud ei uuri mitte objekte
vaid nendevahelisi seoseid –
H. Poincaré*

8.1	Seose mõiste	122
8.2	Seose esitusviise	126
8.3	Seose omadused	127
8.4	Tehted seostega	129
8.5	Ekvivalentsusseos	132
8.6	Ekvivalentsiklassid ja faktorhulk	133
8.7	Klassijaotus	134
8.8	Järjestusseos	137

Asjade ja sündmustega, mis on omavahel seoses, puutume me igapäevaelus tihti kokku. Näiteks on igal inimesel oma telefoninumber; töötamine võib olla seotud palga saamisega; sugulussidemete kaudu oled sa seotud teiste inimestega jne. Matemaatikas huvitume samuti mitmesugustest seostest, näiteks seosest arvu ja tema jagajate vahel; algarvu ja temale järgneva algarvu vahel või kõrgemas matemaatikas argumendi väärtuse x ja vastava funktsiooni tuletise väärtuse $f'(x)$ vahel. Geomeetrias on üheks seose näiteks kongruentsus, mida kasutatakse kolmnurkade uurimisel. Need näited kinnitavad, et matemaatikas leidub seoseid peaaegu igal sammul. Tüüpiliselt kasutame seoseid mingite objektide uurimiseks (kolmnurgad, täisarvud, maatriksid jne), selles peatükis on meie eesmärgiks aga seoseid endid uurida.

8.1 Seose mõiste

Definitsioon 8.1

Olgu A ja B hulgad. **Seoseks** ehk **relatsiooniks** (ingl *relation*) hulkade A ja B vahel nimetatakse otsekorrutise $A \times B$ mis tahes osahulka.

Seega, seos hulkade A ja B vahel on järjestatud paaride (a, b) hulk, kus $a \in A$ ja $b \in B$. Teisiti öeldes, seos on mingi osahulk $R \subset A \times B$. Paari $(a, b) \in R$ korral öeldakse, et **elemendid a ja b on seoses R** ning tähistatakse ka aRb .

Definitsioon 8.2

Seost $R = A \times B$ nimetatakse **universaalseks seoseks** (ingl *universal relation*) ja seost $\emptyset \subset A \times B$ **tühiseoseks** (ingl *empty relation*).

Kui $A = B$ ehk, kui $R \subset A \times A$, siis räägitakse **seosest hulgal A** .

Täpsem oleks ülal toodud definitsioonis rääkida binaarsest seosest ehk kahe hulga vahelisest seosest, sest n -aarseks seoseks hulkade $A_1, \dots, A_n$ vahel nimetatakse vastavalt otsekorrutise $A_1 \times \dots \times A_n$ mis tahes osahulka. Edaspidi vaatleme peamiselt just binaarseid seoseid.

Sageli määratakse seoseid hoopis mingi kirjelduse või omaduse abil ning märgitakse teatud spetsiaalsete sümbolite abil, näiteks: $=, <, \geq, \subset, \parallel$, jne. Tegelikult me mõtleme seosest harva kui järjestatud paaride hulgast. Pigem mõtleme seosest kui „testist“, mida arvupaar või objektide paar (a, b) peab rahuldama selleks, et aRb . Kui a ja b ei ole seoses R , siis tõmbame seost kirjeldavast märgist kriipsu läbi, nagu näiteks $a \neq b$ või $A \not\subset B$.

Kuidas siis mõista ülalpool antud seose definitsiooni kui mingit järjestatud paaride hulka? Mõtle nii, et seost kirjeldav järjestatud paaride hulk on täielik nimekirj kõikidest objektide paaridest, mis antud seost rahuldavad. Vaatame nüüd näiteid, mis aitaksid sellest definitsioonist paremini aru saada.

Näide 8.3. Olgu $A = \{2, 3\}$ ja $B = \{1, 2, 3, 4, 5, 6\}$. Siis $R_1 = \{(2, 2), (2, 3), (3, 1), (3, 5)\}$ on binaarne seos hulkade A ja B vahel. Samade hulkade A ja B korral võime vaadelda veel palju teisi seoseid, näiteks seost R_2 , mis on antud tingimusega, et see koosneb paaridest (a, b) , millede korral b jagub arvuga a . Siis $R_2 = \{(2, 2), (2, 4), (2, 6), (3, 3), (3, 6)\}$.

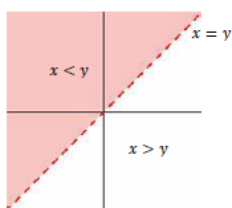
Näide 8.4. Olgu hulgaks A kõigi naturaalarvude hulk $\mathbb{N}$ ning seoseks R osahulk hulgas $\mathbb{N} \times \mathbb{N}$, mis koosneb kõikidest paaridest (a, b) , mille korral arv a on arvu b jagaja. Seega $R = \{(a, b) : a, b \in \mathbb{N}, a \mid b\}$. Seda seost R nimetatakse **jaguvusseoseks**.

Näide 8.5. Olgu A mis tahes hulk ja $R = \{(a, a) : a \in A\}$. Mis tahes elementide $a, b \in A$ korral $(a, b) \in R$ parajasti siis, kui $a = b$. Seda seost R nimetatakse **võrdusseoseks** hulga A elementide vahel.

Näide 8.6. Kui $A = \{1, 4, 5\}$, siis seoses $a < b$ („on väiksem kui”) on selle hulga elemendid 1 ja 4, 1 ja 5 ning 4 ja 5. Tegemist on seosega $R = \{(1, 4), (1, 5), (4, 5)\}$ hulgal A .

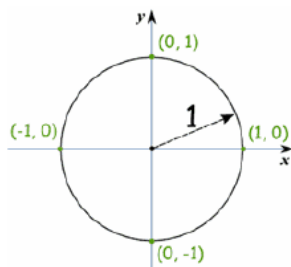
Kuidas kirjeldada antud seost siis, kui hulgaks A oleks kõigi täisarvude hulk $\mathbb{Z}$? Paljud tuttavad matemaatilised seosed on esitatavad järjestatud paaride hulgana. Seost $<$ („väiksem”) täisarvudel võib esitada hulgana $R = \{(x, y) : x, y \in \mathbb{Z} \wedge y - x \in \mathbb{N}\}$, mis annab meile teada, et (x, y) on omavahel seoses, kui $y - x$ on positiivne täisarv ehk kui $x < y$.

Olgu nüüd $A = \mathbb{R}$. Kuidas esitaksime või kujutaksime sama seost $R = \{(x, y) : x < y\}$ reaalarvude hulgal? Antud juhul väljendab seos punktipaaride hulka tasandil ja see hulk on kujutatud järgmisel joonisel.



Näide 8.7. Tasandi kõigi sirgete hulgal S võime vaadelda seost $s \parallel t$, mis tähendab, et sirged s ja t on paralleelsed. Samuti oleksime võinud vaadata seost $s \perp t$, mille korral sirge s on risti sirgega t .

Näide 8.8. Olgu $A = B = \mathbb{R}$, $R = \{(x, y) : x^2 + y^2 = 1\}$. Seos R on ringjoonel paiknevate punktupaaride hulk tasandil (ringjoon on keskpunktiga koordinaatide alguspunktis ning raadiusega 1).



Näide 8.9. Olgu K õppeaine „Matemaatiline maailmapilt” kuulajate hulk. Siis üheks seoseks hulgal K on $xRy \Leftrightarrow$ üliõpilane x on sümpaatne üliõpilasele y . Seega, seos R on teineteisele sümpaatsete üliõpilaste hulk.

Näide 8.10. Olgu M maakeral elavate inimeste hulk. Siis aRb , kui inimestel a ja b on ühised vanemad.

Näide 8.11. Funktsioon kui seose erijuht. Olgu $f: X \rightarrow Y$ funktsioon. Defineerime $R = G(f)$, st xRy parajasti siis, kui $(x, y) \in G(f) = \{(x, f(x)): x \in X\}$. Teisisõnu, funktsiooni f graafik on seos hulkade X ja Y vahel.

Eelmine näide õigustab mõtteviisi, et seosed on funktsioonide üldistus. Tihti leiab kirjandusest järgmise funktsiooni definitsiooni.

Definitsioon 8.12

Olgu X ja Y hulgad. Seost $R \subset X \times Y$ nimetatakse **funktsiooniks** (ingl *function*), kui

1. iga $x \in X$ korral leidub $y \in Y$ nii, et $(x, y) \in R$
2. kui $x \in X$ ja $y, z \in Y$ on sellised, et $(x, y) \in R$ ja $(x, z) \in R$, siis $y = z$.

Edaspidi mõtleme funktsioonidest kui kindlatest seostest. Anname uuest funktsiooni definitsioonist lähtuvalt ka injektiivsuse ja sürjektiivsuse uued definitsioonid.

Definitsioon 8.13

Olgu $R \subset X \times Y$ funktsioon. Siis R on

1. **injektiivne** (ingl *injective*), kui $x_1, x_2 \in X$ ja $y \in Y$ on sellised, et $(x_1, y) \in R$ ja $(x_2, y) \in R$, siis $x_1 = x_2$.
2. **sürjektiivne** (ingl *surjective*), kui iga $y \in Y$ korral leidub $x \in X$ nii, et $(x, y) \in R$.

Ülesanne 8.14. Olgu täisarvude hulgal $\mathbb{Z}$ antud järgmised seosed:

$$\begin{aligned} R_1 &= \{(a, b): a \leq b\}, & R_4 &= \{(a, b): a = b\}, \\ R_2 &= \{(a, b): a > b\}, & R_5 &= \{(a, b): a = b + 1\}, \\ R_3 &= \{(a, b): a = b \vee a = -b\}, & R_6 &= \{(a, b): a + b \leq 3\}. \end{aligned}$$

Millised seosed sisaldavad paare $(1, 1), (1, 2), (2, 1), (1, -1)$ ja $(2, 2)$?

Lahendus. Paar $(1, 1)$ kuulub seostesse R_1, R_3, R_4 ja R_6 . Paar $(1, 2)$ kuulub seostesse R_1 ja R_6 . Paar $(2, 1)$ kuulub seostesse R_2, R_5 ja R_6 . Paar $(1, -1)$ kuulub seostesse R_2, R_3 ja R_6 . Paar $(2, 2)$ kuulub seostesse R_1, R_3 ja R_4 . ■

Ülesanne 8.15. Kui palju erinevaid seoseid saab olla hulgal, milles on n elementi?

Lahendus. Seos hulgal A on otsekorrutise $A \times A$ osahulk. Kui hulgas A on n elementi, siis otsekorrutises on n^2 elementi. Eelnevast teame, et kui hulgas on m elementi, siis on sellel hulgal 2^m osahulka. Seega, hulgal $A \times A$ on 2^{n^2} osahulka ja täpselt sama palju saab seal olla ka seoseid. Näiteks, hulgal $\{a, b, c\}$ on $2^{3^2} = 2^9 = 512$ erinevat seost. ■

Definitsioon 8.16

Seose $R \subset A \times B$ **pöördseoseks** (ingl *inverse relation*) nimetatakse seost $R^{-1} \subset B \times A$, mis määratakse samaväärsusega $bR^{-1}a \Leftrightarrow aRb$ ehk $R^{-1} = \{(b, a) : (a, b) \in R\}$.

Ülemine indeks „ -1 “ on siin ainult mugav ja kokkulepitud tähistus. See ei tähenda seose astmesse võtmist ega ka jagamist (mõlemad sellised tehted oleksid siinkohal absurdid).

Igal seosel on olemas pöördseos. Kui R on seos hulgal A , siis on seda ka R^{-1} . On ka lihtne näha, et $(R^{-1})^{-1} = R$, st pöördseose pöördseos ühtib esialgse seosega (Kontrolli!).

Näide 8.17. Kui $R = \{(1, 5), (2, 6), (3, 7), (3, 8)\}$, siis $R^{-1} = \{(5, 1), (6, 2), (7, 3), (8, 3)\}$.

Näide 8.18. Olgu $A = B = \mathbb{R}$ ja R reaalarvudel defineeritud range järjestuse seos $<$, so $R = \{(x, y) : x < y\}$. Siis $R^{-1} = \{(y, x) : (x, y) \in R\} = \{(y, x) : y > x\}$, st seose $<$ pöördseos on $>$.

Näide 8.19. Olgu $A = B = \mathbb{R}$ ja I reaalarvudel defineeritud võrdusseos ehk **ühikseos**, so $I = \{(x, y) : x = y\}$. Siis $I^{-1} = \{(y, x) : (x, y) \in I\} = \{(y, x) : y = x\}$, st võrdusseose pöördseos on ta ise.

Järgmisena uurime, **millal on funktsiooni pöördseos ise funktsioon**? Meenutame, et seos $R \subset X \times Y$ on funktsioon, kui

1. iga $x \in X$ korral leidub $y \in Y$ nii, et $(x, y) \in R$
2. kui $x \in X$ ja $y, z \in Y$ on sellised, et $(x, y) \in R$ ja $(x, z) \in R$, siis $y = z$.

Funktsiooni R pöördseos on $R^{-1} = \{(y, x) : (x, y) \in R\} \subset Y \times X$. Teeme nüüd kindlaks, millal on R^{-1} ise funktsioon:

1. Tahame, et iga $y \in Y$ korral leiduks $x \in X$ nii, et $(y, x) \in R^{-1}$ ehk $(x, y) \in R$. Seega R peab olema **sürjektiivne** funktsioon.
2. Tahame, et kui $y \in Y$ ja $x_1, x_2 \in X$ on sellised, et $(y, x_1) \in R^{-1}$ ja $(y, x_2) \in R^{-1}$, siis $x_1 = x_2$. Ehk, kui $(x_1, y) \in R$ ja $(x_2, y) \in R$, siis $x_1 = x_2$. Seega R peab olema **injektiivne**.

Kokkuvõttes oleme saanud, et pöördseose R^{-1} funktsiooniks olemiseks peab R olema **bijektiivne funktsioon**. Seega oleme näidanud, et kehtib järgmine tulemus.

Lause 8.20

Olgu $R \subset X \times Y$ funktsioon. Siis R on bijektiivne parajasti siis, kui tema pöördseos R^{-1} on funktsioon. Veelgi enam, pöördseos R^{-1} ongi funktsiooni R pöördfunktsioon.

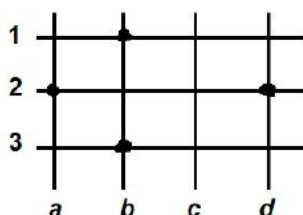
8.2 Seose esitusviise

Seoseid võib esitada väga mitmel viisil:

1. Kui hulgad A ja B on lõplikud ja ei sisalda väga palju elemente, siis võib seost R määrata lihtsalt temasse kuuluvate elemendipaaride loetelu teel (vt näide 8.3). Seost võib kujutada ka tabelina. Seos R_1 näites 8.3 esitub tabelina järgmiselt:

A	2	2	3	3
B	2	3	1	5

2. Kui otsekorrutist $A \times B$ kujutada ristkülikuna, siis seost hulkade A ja B vahel võime kujutada ükskõik millise kujundina selle ristküliku sees. Ka iga funktsiooni, nt $y = x^2$ graafik on osahulk „tõkestamatus” ristkülikus $\mathbb{R} \times \mathbb{R}$. Lõplike hulkade A ja B korral võib ristküliku asemel joonistada teatud ruudustiku, märkides ära sõlmed, mis vastavad seoses asuvatele elemendipaaridele. Joonisel on esitatud seos $R = \{(a, 2), (b, 1), (b, 3), (d, 2)\}$ hulkade $A = \{a, b, c, d\}$ ja $B = \{1, 2, 3\}$ vahel.



3. **Maatriksesitus.** Olgu $A = \{a_1, \dots, a_n\}$ ja $B = \{b_1, \dots, b_m\}$ ning R seos hulkade A ja B vahel. Seame seosele R vastavusse maatriksi $M_R = (m_{ij})$, kus $m_{ij} = 1$, kui $(a_i, b_j) \in R$ ja $m_{ij} = 0$, kui $(a_i, b_j) \notin R$, kus $i = 1, \dots, n$ ja $j = 1, \dots, m$.

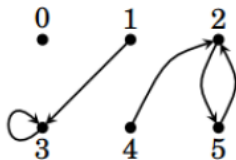
Näiteks, olgu $A = \{a, b, c, d\}$ ja $B = \{1, 2, 3\}$ ning $R = \{(a, 2), (b, 1), (b, 3), (d, 2)\}$. Siis

$$M_R = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

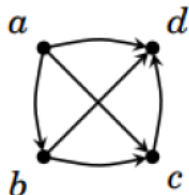
On kerge näha, et maatriksesitus on sisuliselt sama, mis eelmises punktis kirjeldatud „ruudustikuline” esitus. Maatriksite abil esitatud seose omadused on kergesti kindlaks tehtavad.

4. Seoseid võib kujutada ka mitmesuguste nooldiagrammide abil. Joonisel on kujutatud seos R hulga $A = \{0, 1, 2, 3, 4, 5\}$ elementide vahel, kus $(a, b) \in R$ on väljendatud

noolega elemendist a elementi b . Kui element on seoses iseendaga, siis seda väljendab ringnool algus- ja lõpp-punktiga sama elemendi juures. Seega antud juhul $R = \{(1, 3), (2, 5), (3, 3), (4, 2), (5, 2)\}$.



Tihti annabki seose graafiline kujutamine seosest palju parema ülevaate. Näiteks seos R hulgal $A = \{a, b, c, d\}$, kus xRy , kui x on tähestikus eespool kui y , on avaldatav hulgana $R = \{(a, b), (a, c), (a, d), (b, c), (b, d), (c, d)\}$ ning nooldiagrammina (vt joonis).



5. Eespool oli juba mainitud, et seost võib määrata ka sõnaliselt, mingi omaduse või tingimuse abil, valemina jms.

8.3 Seose omadused

Järgnevalt tutvustame seoste kirjeldamiseks ning klassifitseerimiseks vajaminevat sõnavara.

Definitsioon 8.21: Seose omadused

Olgu A hulk. Seost $R \subset A \times A$ nimetatakse

- (a) **refleksiivseks** (ingl *reflexive*), kui iga $a \in A$ korral $(a, a) \in R$;
- (b) **irrefleksiivseks** (ingl *irreflexive*), kui iga $a \in A$ korral $(a, a) \notin R$;
- (c) **sümmeetriliseks** (ingl *symmetric*), kui iga $a, b \in A$ korral, kui $(a, b) \in R$, siis $(b, a) \in R$;
- (d) **antisümmeetriliseks** (ingl *antisymmetric*), kui iga $a, b \in A$ korral kui $(a, b) \in R$ ja $(b, a) \in R$, siis $a = b$;
- (e) **transitiivseks** (ingl *transitive*), kui iga $a, b, c \in A$ korral, kui $(a, b) \in R$ ja $(b, c) \in R$, siis $(a, c) \in R$.

Näide 8.22. Olgu $A = \{1, 2, 3\}$ ja olgu antud hulgal A seosed $R_1 = \{(1, 1), (2, 1), (2, 2), (3, 3)\}$ ja $R_2 = \{(1, 1), (2, 1), (1, 2), (3, 3)\}$. Siis seos R_1 on refleksiivne, sest ta sisaldab kõiki paare kujul (a, a) ; nimelt, $(1, 1)$, $(2, 2)$ ja $(3, 3)$. Seos R_2 ei ole refleksiivne, sest ta ei sisalda paari $(2, 2)$. Seos R_2 ei ole samas ka irrefleksiivne, sest ta sisaldab paare $(1, 1)$ ja $(3, 3)$.

Märkus. Sümmeetrilisuse ja antisümmeetrilisuse omadused ei ole teineteise vastandid, sest seosel võivad olemas olla mõlemad omadused korraga või võib juhtuda, et ei ole kumbagi omadust. Samuti ei ole refleksiivsus ja irrefleksiivsus teineteise vastanditeks.

Ülesanne 8.23. Kas jaguvusseos täisarvude hulgal on refleksiivne? Sümmeetriline? Antisümmeetriline?

Lahendus. Kuna $a \mid a$ mis tahes täisarvu korral, siis on jaguvusseos refleksiivne. Jaguvusseos täisarvude hulgal ei ole sümmeetriline, sest $1 \mid 2$, aga $2 \nmid 1$. Täisarvude hulgal pole jaguvusseos antisümmeetriline, sest kui $a \mid b$ ja $b \mid a$, siis $|a| = |b|$. Kuid naturaalarvude hulgal on jaguvusseos antisümmeetriline, sest iga elemendi $a, b \in \mathbb{N}$ korral, kui $a \mid b$ ja $b \mid a$, siis $a = b$. ■

Ülesanne 8.24. Tõesta, et kui seos on sümmeetriline ja antisümmeetriline, siis ta on transitiivne.

Näide 8.25. Seos $<$ („väiksem“) reaalarvude hulgal on irrefleksiivne, antisümmeetriline ja transitiivne. Seos $\leq$ hulgal $\mathbb{R}$ on refleksiivne, antisümmeetriline ja transitiivne.

Näide 8.26. Sirgete samasihilisuse ehk paralleelsuse seos $s \parallel t$ on refleksiivne, sümmeetriline ja transitiivne.

Sirgete ristioleku seos $s \perp t$ on irrefleksiivne, sümmeetriline, aga ei ole transitiivne.

Näide 8.27. Vaatleme hulga E kõikide osahulkade hulka $X = \mathcal{P}(E)$ ja sisalduvuse seost $\subset$ hulgal X . See seos on refleksiivne, antisümmeetriline ja transitiivne.

Näide 8.28. Olgu $A = \{a, b, c, d\}$ ja $R = \{(a, a), (a, b), (b, a), (b, c)\}$. Seosel R pole ühtki varem nimetatud omadustest.

Ülesanne 8.29. Olgu A hulk. Millised omadused on universaalsel seosel $R = A \times A$ ja tühiseosel $S = \emptyset$?

Ülesanne 8.30. Millised üldnimetatud omadused on võrdusseosel?

Ülesanne 8.31. Too näide seosest, mis on sümmeetriline ja transitiivne, aga pole reflekstiivne.

Lause 8.32

Kui seos R on reflekstiivne, transitiivne, sümmeetriline või antisümmeetriline, siis ka tema pöördseos R^{-1} on vastava omadusega.

Tõestus. Iseseisvalt! ■

Ülesanne 8.33. Näita, et seos R hulgal A on sümmeetriline siis ja ainult siis, kui $R = R^{-1}$.

8.4 Tehted seostega

Kuna seos on teatav hulk, siis rakenduvad hulgateoreetilised tehted ka seostele. Näiteks saab rääkida seoste ühendist, ühisosast, vahest või täiendist.

Definitsioon 8.34

Olgu A ja B hulgad ning olgu antud seosed $R, S \subset A \times B$.

- (a) Seoste R ja S **ühendiks** (ingl *union*) nimetatakse seost $R \cup S$, mille korral $a(R \cup S)b \Leftrightarrow aRb \vee aSb$.
- (b) Seoste R ja S **ühisosaks** (ingl *intersection*) nimetatakse seost $R \cap S$, mille korral $a(R \cap S)b \Leftrightarrow aRb \wedge aSb$.
- (c) Seoste R ja S **vaheks** (ingl *difference*) nimetatakse seost $R \setminus S$, mille korral $a(R \setminus S)b \Leftrightarrow aRb \wedge \neg(aSb)$.
- (d) Seose R **täiendiks** (ingl *complement*) nimetatakse seost R' , mille korral $aR'b \Leftrightarrow \neg(aRb)$, kus universaalseks hulgaks on $A \times B$.

Nii defineeritud tehetele kanduvad mõistagi üle kõik suvaliste hulkade ühendi, ühisosa ja täiendi omadused.

Näiteks, seose $R = \{(a, b) : a \leq b\}$ täiendiks hulgal $\mathbb{R}$ on seos $R' = \{(a, b) : a > b\}$.

Ülesanne 8.35. Näita, et seos R hulgal A on antisümmeetriline siis ja ainult siis, kui $R \cap R^{-1} \subset I = \{(a, a) : a \in A\}$.

Definitsioon 8.36

Seoste $R \subset A \times B$ ja $S \subset B \times C$ **korrutiseks** ehk **kompositsiooniks** (ingl *composition*) nimetatakse seost $S \circ R \subset A \times C$, kus

$$S \circ R = \{(a, c) : \exists b \in B \text{ nii, et } (a, b) \in R \wedge (b, c) \in S\}.$$

Kasutatakse ka tähist SR . Sarnaselt eespool olevatele definitsioonidele, võime kahe seose korrutise definitsiooni tingimuse esitada ka kujul $a(S \circ R)c \Leftrightarrow \exists b \in B (aRb \wedge bSc)$.

Kui R on seos hulgal A , siis kasutame tähistusi $R^2 := R \circ R$, $R^3 := R^2 \circ R$ jne ehk üldiselt $R^n := R^{n-1} \circ R$ kui $n \geq 2$.

Näide 8.37. Olgu R selline seos hulgast $A = \{1, 2, 3\}$ hulka $B = \{1, 2, 3, 4\}$, kus

$$R = \{(1, 1), (1, 4), (2, 3), (3, 1), (3, 4)\}$$

ja S seos hulgast $B = \{1, 2, 3, 4\}$ hulka $C = \{0, 1, 2\}$, kus

$$S = \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\}.$$

Leidke $S \circ R$ ja $R \circ S$.

Lahendus. Näiteks, kuna element $(2, 3) \in R$ ja $(3, 1) \in S$, siis definitsiooni järgi saame, et $(2, 1) \in S \circ R$. Sarnaselt arutledes leiame, et

$$S \circ R = \{(1, 0), (1, 1), (2, 1), (2, 2), (3, 0), (3, 1)\}.$$

Teisalt, $R \circ S$ ei saa leida, sest $A \neq C$. ■

Ülesanne 8.38. Tõesta, et mis tahes seose $R \subset A \times B$ ja ühikseose $I \subset A \times A$ korral $R \circ I = R$ ning ühikseose $I \subset B \times B$ korral $I \circ R = R$.

Lause 8.39

Olgu A hulk ja R seos hulgal A . Tõestada, et R on transitiivne parajasti siis, kui $R^n \subset R$ iga $n \geq 2$ korral.

Tõestus. Vihje: matemaatiline induktsioon. ■

Märgime, et seoste korrutamisel võib juhtuda, et $R \neq \emptyset$ ja $S \neq \emptyset$, aga $S \circ R = \emptyset$. Too näide sellistest seostest!

Ülesanne 8.40. Olgu A , B ja C hulgad ning $R \subset A \times B$ ja $S \subset B \times C$. Tõestada, et

$$(S \circ R)^{-1} = \emptyset \Leftrightarrow R^{-1} \circ S^{-1} = \emptyset.$$

Ülesanne 8.41. Olgu A , B , C ja D hulgad ning $R \subset A \times B$, $S \subset B \times C$ ja $T \subset C \times D$. Tõestada, et

$$T \circ (S \circ R) = \emptyset \Leftrightarrow (T \circ S) \circ R = \emptyset.$$

Lause 8.42

Olgu A, B, C ja D hulgad. Kui $R \subset A \times B$, $S \subset B \times C$ ja $T \subset C \times D$, siis

1. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$;
2. $T \circ (S \circ R) = (T \circ S) \circ R$.

Tõestus.

1. Veendume väite kehtivuses samaväärsuste ahela abil:

$$\begin{aligned}
 (c, a) \in (S \circ R)^{-1} &\equiv (a, c) \in S \circ R \\
 &\equiv \exists b \in B ((a, b) \in R \wedge (b, c) \in S) \\
 &\equiv \exists b \in B ((b, a) \in R^{-1} \wedge (c, b) \in S^{-1}) \\
 &\equiv \exists b \in B ((c, b) \in S^{-1} \wedge (b, a) \in R^{-1}) \\
 &\equiv (c, a) \in R^{-1} \circ S^{-1}.
 \end{aligned}$$

2. Veendume väite kehtivuses samaväärsuste ahela abil:

$$\begin{aligned}
 (a, d) \in T \circ (S \circ R) &\equiv \exists c \in C ((a, c) \in S \circ R \wedge (c, d) \in T) \\
 &\equiv \exists c \in C (\exists b \in B ((a, b) \in R \wedge (b, c) \in S) \wedge (c, d) \in T) \\
 &\equiv \exists b \in B ((a, b) \in R \wedge (b, d) \in T \circ S) \\
 &\equiv (a, d) \in (T \circ S) \circ R.
 \end{aligned}$$

■

Ülesanne 8.43. Tõesta, et kui seosed R ja S on refleksiivsed, sümmeetrilised ja transitiivsed, siis $S \circ R$ on refleksiivne, sümmeetriline ja transitiivne parajasti siis, kui $S \circ R = R \circ S$. Leia näide refleksiivsetest, sümmeetrilistest ja transitiivsetest sesostest R ja S (samal hulgal A), kus $S \circ R \neq R \circ S$.

Järgnevalt uurime, kuidas teostada tehteid seostega kui nad on antud maatrikskujul. Osutub, et kui seosed on maatrikskujul, siis tehete $\vee$ ja $\wedge$ abil on võimalik kergesti leida seoste ühendi või ühisosa maatriksi. Nimelt, kui R ja S on seosed, mille maatrikskujud on M_R ja M_S , siis nende seoste ühendis on tõeväärtus 1 just nendel kohtadel, kus maatriksites M_R või M_S on samas kohas väärtus 1. Samade seoste ühisosas on tõeväärtus 1 just nendel kohtadel, kus maatriksites M_R ja M_S on samas kohas väärtus 1.

Näide 8.44. Olgu A ja B hulgad ning $R, S \subset A \times B$ seosed, mille esitused maatrikskujul on vastavalt

$$M_R = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{ja} \quad M_S = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

siis

$$M_{R \cup S} = M_R \vee M_S = \begin{pmatrix} 1 \vee 1 & 0 \vee 0 & 1 \vee 1 \\ 1 \vee 0 & 0 \vee 1 & 0 \vee 1 \\ 0 \vee 1 & 1 \vee 0 & 0 \vee 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

ja

$$M_{R \cap S} = M_R \wedge M_S = \begin{pmatrix} 1 \wedge 1 & 0 \wedge 0 & 1 \wedge 1 \\ 1 \wedge 0 & 0 \wedge 1 & 0 \wedge 1 \\ 0 \wedge 1 & 1 \wedge 0 & 0 \wedge 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Selleks, et seoseid R ja S korrutada maatrikskujul tuleb vastavad maatriksid M_R ja M_S korrutada **Boole'i mõttes**, see tähendab, et tavalise korrutamise $\cdot$ asendame konjunktsiooniga $\wedge$ ja liitmise $+$ asendame disjunktsiooniga $\vee$.

Näide 8.45. Olgu A hulk ja $R, S \subset A \times A$ seosed, mille esitused maatrikskujul on vastavalt

$$M_R = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{ja} \quad M_S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

siis

$$M_{S \circ R} = M_R \odot M_S = \begin{pmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 0) \vee (0 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 0) \vee (0 \wedge 1) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

8.5 Ekvivalentsusseos

Definitsioon 8.46

Olgu A hulk. Seost R hulgal A nimetatakse **ekvivalentsusseoseks** (ingl *equivalence relation*), kui ta on

- (a) refleksiivne, st kui aRa iga $a \in A$ korral;
- (b) sümmeetriline, st kui aRb , siis bRa ;
- (c) transitiivne, st kui aRb ja bRc , siis aRc .

Kui R on ekvivalentsusseos ja aRb , siis öeldakse, et elemendid a ja b on **ekvivalentsed** (seose R järgi). Sageli väljendatakse ekvivalentsusest kirjutades ka $a \sim b$.

Näide 8.47. Võrdsusseos $aRb \Leftrightarrow a = b$ on ilmselt ekvivalentsusseos suvalisel hulgal A . Tegemist on ühikseosega $R_A = I = \{(a, a) : a \in A\}$, mida mõnikord nimetatakse ka hulga A^2 diagonaaliks ja tähistatakse sel juhul $\triangle A$. Ühikseos ehk võrdsusseos on kõige kitsam ekvivalentsusseos, sest ta on iga ekvivalentsusseose (kui refleksiivse seose) osahulk. Ka seos $U = A \times A$ on ekvivalentsusseos hulgal A (nn universaalne seos). Seoseid I ja U nimetatakse **triviaalseteks seosteks** hulgal A .

Näide 8.48. Kujundite kongruentsus planimeetrias on ekvivalentsusseos tasandi kõikide kujundite hulgal. Kolmnurkade (või hulknurkade) sarnasuse seos on samuti ekvivalentsusseos. Olgu märgitud, et sel juhul kasutatakse just sümboolikat $\triangle ABC \sim \triangle DEF$.

Näide 8.49. Hulkade ekvivalentsus on ekvivalentsusseos (vt lause 7.11).

Näide 8.50. Sirgete samasihilisus on ekvivalentsusseos.

Näide 8.51. Kongruentsiseos täisarvude hulgal $\mathbb{Z}$ on samuti ekvivalentsusseos. Olgu m mingi fikseeritud naturaalarv. Täisarve a ja b nimetatakse **kongruentseteks mooduli m järgi**, kui vahe $a - b$ jagub arvuga m ja kirjutatakse $a \equiv b \pmod{m}$.

Näiteks, $25 \equiv 11 \pmod{7}$ ja $21 \equiv 13 \pmod{4}$.

Ülesanne 8.52. Näita, et kui ekvivalentsusseos on antisümmeetriline, siis on ta võrdus ehk ühikseos.

8.6 Ekvivalentsiklassid ja faktorhulk

Iga ekvivalentsusseose $R \subset A \times A$ abil saame hulga A jaotada nn ekvivalentsiklassideks.

Definitsioon 8.53

Ekvivalentsiklassiks (ingl *equivalence class*) elemendi $a \in A$ järgi (või ekvivalentsiklassiks seose R järgi esindajaga a) nimetatakse hulga A osahulka $[a]_R$, mis koosneb hulga A kõigist elementidest, mis on seoses R elemendiga a ehk

$$[a]_R = \{x \in A : aRx\}.$$

Niisiis, $x \in [a]_R$ tähendab seda, et aRx ja seose R sümmeetrilisuse tõttu ka seda, et xRa . Refleksiivsuse tõttu $a \in [a]_R$.

Näide 8.54. Olgu R selline seos hulgal $\mathbb{Z}$, et xRy parajasti siis, kui $x^2 = y^2$. Selline seos on ekvivalentsusseos (kontrolli!). Leiame ekvivalentisklassid $[0]$ ja $[4]$. Esiteks,

$$[0] = \{x \in \mathbb{Z} : 0Rx\} = \{x \in \mathbb{Z} : 0^2 = x^2\} = \{x \in \mathbb{Z} : 0 = x\} = \{0\}.$$

Analoogiliselt arutledes saame, et $[4] = \{-4, 4\}$.

Definitsioon 8.55

Olgu R ekvivalentsusseos hulgal A . Hulka, mille elementideks on seosele R vastava klassijaotuse kõik klassid, nimetatakse **hulga A faktorhulgaks ekvivalentsusseose R järgi** (ingl *quotient set*) ja tähistatakse A/R .

Seega, $A/R = \{[a]_R : a \in A\}$. Märgime, et erinevatele elementidele vastavad ekvivalentsiklassid võivad ühtida, st $a \neq b$ korral võib olla $[a]_R = [b]_R$. Faktorhulga elementideks võetakse võrdsete ekvivalentsiklasside seast ainult üks.

Näide 8.56. Kui hulgas A vaadelda ekvivalentsusseosena võrdusseost I , siis $A/I = \{\{a\} : a \in A\}$.

Näide 8.57. Loeme tasandi $X = \mathbb{R}^2$ punktid $x = (x_1, x_2)$ ja $y = (y_1, y_2)$ ekvivalentseteks, kui nad asuvad samal vertikaalsel sirgel. Siis $[x] = \{y \in X : y_1 = x_1\}$ on kõigi punktide hulk, mis asuvad punktiga x ühel ja samal vertikaalsel sirgel, ehk punkti x läbiv vertikaalne sirge. Faktorhulk X/R koosneb siin kõigist vertikaalsetest sirgetest.

Näide 8.58. Kui R on samasihilisuse seos tasandi (või ruumi) sirgete hulgal A , siis vastava faktorhulga elementideks on konkreetset sihid.

Näide 8.59. Kui R on vektorite võrdsuse seos $\vec{u} = \vec{v}$, siis iga ekvivalentsiklass koosneb samasuunalistest võrdse pikkusega vektoritest, mida vaadeldakse ühe ja sama vektorina. Seega faktorhulga elementideks on vabavektorid.

8.7 Klassijaotus

Definitsioon 8.60

Olgu A hulk, I (indeksite) hulk ja $K_i \subset A$ iga $i \in I$ korral. Öeldakse, et hulgal A on antud **klassijaotus** (ingl *partition*) $\mathcal{K} = \{K_i : i \in I\}$, kui

1. iga $i \in I$ korral $K_i \neq \emptyset$;
2. iga kaks erinevat hulka on mitteloikuvad, st iga $i, j \in I$ korral tingimusest $K_i \neq K_j$ järelneb, et $K_i \cap K_j = \emptyset$;
3. hulk A võrdub osahulkade K_i ühendiga, st $A = \bigcup_{i \in I} K_i$.

Hulki K_i , $i \in I$, nimetatakse selle klassijaotuse $\mathcal{K}$ *klassideks*.

Teiste sõnadega, klassijaotuse korral on hulk A jaotatud mitteloikuvateks mittetühjadeks osahulkadeks, mis moodustavadki hulkade süsteemi $\mathcal{K}$. Üldjuhul võib I olla ükskõik milline indeksite hulk (lõplik või lõpmatu).

Näide 8.61. Olgu G mingi gümnaasiumi kõikide õpilaste hulk ning K_{10} , K_{11} ja K_{12} vastavalt kõikide 10. klassi, 11. klassi ja 12. klassi õpilaste hulgad. Süsteem $\{K_{10}, K_{11}, K_{12}\}$ on klassijaotus hulgal G .

Näide 8.62. Hulga A kõik üheelemendilised osahulgad $\{a : a \in A\}$ moodustavad klassijaotuse, sest $\{a\} \neq \emptyset$, $\bigcup_{a \in A} \{a\} = A$ ja sellest, et $\{a\} \neq \{b\}$ (st $a \neq b$), järelneb, et $\{a\} \cap \{b\} = \emptyset$. See on kõige peenem klassijaotus hulgal A .

Näide 8.63. Ühest tervest hulgast A koosnev klassijaotus $\{A\}$ on kõige jämedam klassijaotus hulgal A .

Näide 8.64. Kui $A = \mathbb{R}$, siis moodustavad klassijaotuse poollõigud $K_i = [i, i + 1)$, $i \in \mathbb{Z}$. (Kontrolli ise, et tingimused oleksid täidetud!)

Hulga A klassijaotused $\{K_i\}$ ja $\{L_j\}$ loeme võrdseteks, kui iga K_i korral leidub L_j nii, et $L_j = K_i$, ja vastupidi, iga L_j korral leidub K_i nii, et $K_i = L_j$.

Lause 8.65

Klassijaotused $K = \{K_i : i \in I\}$ ja $L = \{L_j : j \in J\}$ ühtivad, kui iga K_i korral leidub L_j nii, et $K_i = L_j$.

Tõestus. Valime vabalt L_j . Olgu $a \in L_j$. Et $a \in A$, siis $A = \bigcup_{i \in I} K_i$ tõttu leidub K_i nii, et $a \in K_i$. Leiame $L_{j'}$ nii, et $L_{j'} = K_i$. Siis $a \in L_j \cap L_{j'}$, seega $L_j \cap L_{j'} \neq \emptyset$. Sellest järeldub, et $L_j = L_{j'}$ ehk $K_i = L_j$. ■

Näitame nüüd, et faktorhulk on klassijaotus.

Teoreem 8.66

Olgu R suvaline ekvivalentsusseos hulgal A . Siis faktorhulk A/R on klassijaotus hulgal A .

Tõestus. Selleks, et faktorhulk $A/R = \{[a]_R : a \in A\}$ oleks klassijaotus hulgal A peame kontrollima klassijaotuseks olemise kolme tingimust.

1. Näitame, et $[a]_R \neq \emptyset$ iga $a \in A$ korral. Tõepoolest, seose R refleksiivsuse tõttu iga $a \in A$ korral aRa , st iga $a \in A$ korral $a \in [a]_R$. Seega ei ole ükski klassijaotuse klassidest tühi.
2. Näitame, et kui $[a]_R \neq [b]_R$, siis $[a]_R \cap [b]_R = \emptyset$. Selle tingimuse kontrollimiseks veendume, et kehtib antud väite kontrapositiiv: kui $[a]_R \cap [b]_R \neq \emptyset$, siis $[a]_R = [b]_R$. Selleks võtame kaks osahulka $[a]_R$ ja $[b]_R$, kus $a, b \in A$, ning elemendi c nende ühisosast: $c \in [a]_R \cap [b]_R$. Et $c \in [a]_R$, siis on cRa , ning et $c \in [b]_R$, siis on cRb . Kuna cRa , siis saame seose R sümmeetria tõttu, et aRc . Kuna aRc ja cRb , siis seose R transitiivsuse tõttu aRb . Olgu nüüd x suvaline element osahulgast $[a]_R$. Siis xRa . Kuna aRb , siis järeldub sellest seose R transitiivsuse tõttu xRb . See tähendab, et $x \in [b]_R$ ehk $[a]_R \subset [b]_R$. Samasugune arutelu annab meile, et $[b]_R \subset [a]_R$. Järelikult, $[a]_R = [b]_R$.
3. Näitame, et $A = \bigcup_{a \in A} [a]_R$. Kuna $[a]_R \subset A$ iga $a \in A$ korral, siis on selge, et $A \supseteq \bigcup_{a \in A} [a]_R$. Vastupidi, kuna 1. osa põhjal $a \in [a]_R$ iga $a \in A$ korral, siis

$$A = \bigcup_{a \in A} \{a\} \subset \bigcup_{a \in A} [a]_R.$$

Seega $A = \bigcup_{a \in A} [a]_R$. ■

Teisalt osutub, et ka iga klassijaotus tekitab ühe ekvivalentsusseose.

Teoreem 8.67

Kui $K = \{K_i : i \in I\}$, on klassijaotus hulgal A , siis seos R , kus aRb tähendab, et elemendid a ja b kuuluvad ühte ja samasse klassi (mingisse hulka K_i), on ekvivalentsusseos hulgal A .

Tõestus. Olgu meil nüüd antud klassijaotus $K = \{K_i : i \in I\}$ hulgal A . Vaatleme seost R , mis on defineeritud tingimusega, et aRb siis, kui elemendid a ja b kuuluvad ühte ja

samasse klassi, ehk

$$aRb \Leftrightarrow \exists i \in I (a \in K_i \wedge b \in K_i).$$

Näitame, et selliselt defineeritud seos on ekvivalentsusseos.

1. Seos R on refleksiivne. Tõepoolest, iga $a \in A$ korral aRa , sest $A = \bigcup_{i \in I} K_i$ ning $a \in A$ tõttu peab element a vähemalt ühte hulka K_i kuuluma.
2. Seos R on sümmeetriline. Kui $a, b \in A$ korral aRb , siis $\exists i \in I (a \in K_i \wedge b \in K_i)$. On selge, et siis ka $b \in K_i \wedge a \in K_i$ ehk bRa .
3. Seos R on transitiivne. Kui $a, b, c \in A$ korral aRb ja bRc , siis vastavalt seose R definitsioonile leiduvad niisugused $i, j \in I$, et $a \in K_i$ ja $b \in K_i$ ning $b \in K_j$ ja $c \in K_j$. Kuna nüüd $b \in K_i \cap K_j$, siis järeldub klassijaotuse definitsiooni teisest tingimusest, et $K_i = K_j$. Järelikult $a, c \in K_i$, millest tuleneb, et aRc .

■

Teoreemidest 8.66 ja 8.67 järeldub, et **antud hulga kõigi ekvivalentsusseoste hulga ja sama hulga kõigi klassijaotuste hulga vahel on üksühene vastavus** (selles mõttes, et igale ekvivalentsusseosele vastab üks klassijaotus ja vastupidi, kui võtta ekvivalentsusseosele vastavale klassijaotusele vastav ekvivalentsusseos, siis see ekvivalentsusseos langeb kokku esialgse ekvivalentsusseosega).

Vaatleme juba näidetes esinenud ekvivalentsusseoseid ja klassijaotusi ning leiame neile loomulikult vastavad klassijaotused ja ekvivalentsusseosed.

Näide 8.68. Suvalises hulgas A antud võrdusseosele vastav klassijaotus koosneb hulkadest $[a]_R = \{b: b \in a \wedge bRa\} = \{b \in A: b = a\} = \{a\}$. Seega vastab võrdusele kui kõige kitsamale ekvivalentsusseosele kõige peenem klassijaotus $\{\{a\}: a \in A\}$.

Näide 8.69. Vaatleme hulgas A ühehulgalist klassijaotust $\{A\}$. Talle vastava ekvivalentsusseose R korral $aRb \Leftrightarrow a \in A \wedge b \in A \Leftrightarrow (a, b) \in A \times A$. Seega antud juhul $R = U = A \times A$, s.t kõige jämedamale klassijaotusele $\{A\}$ vastab kõige laiem ekvivalentsusseos ehk universaalne seos $A \times A$.

Eelmises peatükis ütlesime, et hulgad A ja B on ekvivalentsed ja tähistasime $A \sim B$, kui leidub bijektsioon hulgast A hulka B . Sõna „ekvivalentsed” kasutamine on õigustatud seetõttu, et hulkade võrdvõimsuse seosel on kõik ekvivalentsusseose omadused: refleksiivsus, sümmeetrilisus ja transitiivsus (vt lause 7.11).

Lause 7.11 põhjal saab hulgad jaotada ekvivalentsiklassidesse, kus igasse klassi kuuluvad hulgad on omavahel ekvivalentsed ehk sama võimsusega ja erinevatesse klassidesse kuuluvad hulgad ei ole ekvivalentsed. Hulga A ekvivalentsiklass koosneb kõigist hulgaga A ekvivalentsetest hulkadest. Sealjuures ei saa ekvivalentsiklasse lugeda hulkadeks, sest see tooks kaasa hulgateooria paradoksid.

Definitsioon 8.70

Hulga **võimsuseks** (ingl *cardinality*) nimetatakse tema ekvivalentsiklassi seose $\sim$ järgi.

Kuna hulkade ekvivalentsus on ekvivalentsusseos, siis fikseeritud hulga X kõik osahulgad jaotuvad mittelõikuvateks omavahel ekvivalentsete hulkade klassideks. Tühja hulga ekvivalentsiklass sisaldab vaid seda hulka ennast $\emptyset$, järgmine on üheelemendiliste osahulkade $\{a\}, \{b\}, \dots$ klass, seejärel kaheelemendiliste osahulkade klass jne. Vastavat ekvivalentsiklassi nimetataksegi hulga võimsuseks.

8.8 Järjestusseos

Definitsioon 8.71

Olgu A hulk. Seost R hulgal A nimetatakse **osalise järjestuse seoseks** (ingl *partial ordering*), kui ta on

- (a) refleksiivne, st kui aRa iga $a \in A$ korral;
- (b) antisümmeetriline, st kui aRb ja bRa , siis $a = b$;
- (c) transitiivne, st kui aRb ja bRc , siis aRc .

Kui R on järjestusseos, siis asjaolu aRb märgitakse $a \preceq b$ või samaväärselt $b \succeq a$. Öeldakse ka, et a **eelneb** elemendile b või b **järgneb** elemendile a .

Ülesanne 8.72. Tõesta, et kui R on järjestusseos, siis ka R^{-1} on järjestusseos.

Definitsioon 8.73

Hulka, millel on antud osalise järjestuse seos, nimetatakse **osaliselt järjestatud hulgaks** (ingl *partially ordered set*).

Kui hulgal A on antud osalise järjestuse seos R , siis tähistame seda tavaliselt paarina (A, R) . Näiteks, $(\mathbb{R}, \leq)$ ja $(\mathcal{P}(\{1\}), \subset)$ on osaliselt järjestatud hulgad.

Definitsioon 8.74

Olgu $(A, \preceq)$ osaliselt järjestatud hulk ja $a, b \in A$. Kui $a \preceq b$ või $b \preceq a$, siis öeldakse, et elemendid a ja b on **võrreldavad** (ingl *comparable*).

Definitsioon 8.75

Osaliselt järjestatud hulka nimetatakse **lineaarselt järjestatud hulgaks** ehk **ahelaks** (ingl *totally ordered*), kui iga kaks suvalist elementi sellest hulgast on omavahel võrreldavad.

Näide 8.76.

1. Võrratuse seos $\leq$ reaalarvude hulgal $\mathbb{R}$ on lineaarne järjestus, sest iga kaks arvu on võrreldavad.
2. Hulkade sisaldumise seos $\subset$ hulga X kõigi osahulkade hulgal $\mathcal{P}(X)$ on järjestusseos, aga ei ole lineaarne, sest kaks hulka $A, B \subset X$ ei pruugi olla võrreldavad. Tee joonis!
3. Jaguvusseos naturaalarvude hulgal $\mathbb{N}$ on järjestusseos, mis ei ole lineaarne.

Näide 8.77. Määrame tähestikus $\{a_1, \dots, a_n\}$ järjestuse $a_1 < a_2 < \dots < a_n$. Defineerime sõnade hulgas järjestuse

$$\begin{aligned} (x_1, \dots, x_m) \prec (y_1, \dots, y_l) \Leftrightarrow & (x_1 < y_1) \vee (x_1 = y_1 \wedge x_2 < y_2) \vee \\ & \vee (x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 < y_3) \vee \\ & \vee (x_1 = y_1 \wedge \dots \wedge x_m = y_m \wedge m < l). \end{aligned}$$

Taolist järjestust nimetatakse **alfabeetiliseks** ehk **leksikograafiliseks**, ta on lineaarne ning teda kasutatakse sõnaraamatutes.

Ülesanne 8.78. Olgu A kõigi lõigus $[a, b]$ määratud funktsioonide $f: [a, b] \rightarrow \mathbb{R}$ hulk. Defineerime seose $f \leq g \Leftrightarrow f(x) \leq g(x)$ iga $x \in [a, b]$ korral. Näita, et tegemist on järjestusseosega. Kas see järjestus on lineaarne?

Sageli vaadeldakse ka range järjestuse seost $\prec$, mida võib seosest $\preceq$ lähtudes defineerida järgmiselt: $x \prec y \Leftrightarrow x \preceq y$ ja $x \neq y$.

Definitsioon 8.79

Osaliselt järjestatud hulga A elementi a_0 nimetatakse **vähimaks** ehk **esimeseks** (ingl *least*), kui $a_0 \preceq a$ iga $a \in A$ korral. Analoogiliselt, elementi $a_0 \in A$ nimetatakse **suurimaks** ehk **viimaseks** (ingl *greatest*), kui $a \preceq a_0$ iga $a \in A$ korral.

Näide 8.80.

1. Hulgas $\mathbb{N}$ loomuliku järjestusega on vähim element 1, aga suurimat ei ole.
2. Reaalarvude vahemikus $(0, 1)$ ei ole vähimat ega suurimat elementi.
3. Hulgas $\mathcal{P}(X)$ sisalduvusjärjestusega on vähim element $\emptyset$ ja suurim X .

Lause 8.81

Osaliselt järjestatud hulgas ei ole üle ühe vähima ega üle ühe suurima elemendi.

Tõestus. Olgu a_0 ja a_1 vähimad elemendid. Siis $a_0 \preceq a_1$, sest a_0 on vähim element. Samuti $a_1 \preceq a_0$, sest a_1 on ka vähim element. Kuna osalise järjestuse seos on antisümmeetriline, siis $a_0 = a_1$. Suurima elemendi tõestus on analoogiline. ■

Definitsioon 8.82

Osaliselt järjestatud hulga A elementi a_0 nimetatakse **minimaalseks**, kui sellest, et $a \in A$ ja $a \preceq a_0$, järelneb, et $a = a_0$. (st hulgas A ei ole elemendist a_0 väiksemaid elemente). Analoogiliselt, elementi a_0 nimetatakse **maksimaalseks** (ingl *maximal*), kui sellest, et $a \in A$ ja $a_0 \preceq a$, järelneb, et $a = a_0$ (st hulgas A ei ole elemendist a_0 suuremaid elemente).

Definitsioonidest on näha, et vähima ja minimaalse elemendi põhiline erinevus seisneb selles, et vähima elemendi korral nõutakse, et kõik teised vaadeldava hulga elemendid on temaga võrreldavad, kuid minimaalse elemendi puhul seda ei nõuta.

Näide 8.83.

1. Reaalarvude hulgas, kus peetakse silmas loomulikku järjestust $\leq$, ei ole minimaalseid ega maksimaalseid elemente.
2. Osaliselt järjestatud hulgas $(\{1, 2, 3, 4\}, |)$ on vähim element (seega ka minimaalne) 1, maksimaalsed elemendid on 3 ja 4, kuid suurimat elementi ei ole.

Lause 8.84

Osaliselt järjestatud hulga vähim element on selle hulga ainus minimaalne element ja suurim element on selle hulga ainus maksimaalne element.

Tõestus. Olgu $a_0 \in A$ vähim element, st $a_0 \preceq a$ iga $a \in A$ korral. Kui mingi $b \in A$ korral kehtiks veel $b \preceq a_0$, siis järjestuse antisümmeetrilisuse tõttu $b = a_0$, mis tähendab, et a_0 on minimaalne element.

Viimaks veendume, et see element on ainus. Kui leiduks veel mingi minimaalne element $a_1 \in A$, siis $a_0 \preceq a_1$, sest a_0 on vähim element. Tingimuse $a_0 \neq a_1$ korral ei oleks a_1 minimaalne element, seepärast $a_0 = a_1$. ■

Lause 8.85

Lineaarselt järjestatud hulgas on minimaalne element vähim ja maksimaalne element suurim.

Tõestus. Olgu lineaarselt järjestatud hulgas A element a_0 minimaalne, st kui $a \preceq a_0$ iga $a \in A$ korral, siis $a = a_0$. Näitame, et $a_0 \preceq a$ iga $a \in A$ korral. Oletame vastuväiteliselt, et leidub $a_1 \in A$ nii, et ei kehti $a_0 \preceq a_1$. Lineaarse järjestuse tõttu $a_0 \preceq a_1$ või $a_1 \preceq a_0$, seega saab kehtida ainult $a_1 \preceq a_0$. Seejuures $a_1 \neq a_0$, sest $a_1 = a_0$ korral oleks $a_0 \preceq a_1$. Kuid $a_1 \neq a_0$ ja $a_1 \preceq a_0$ on vastuolus elemendi a_0 minimaalsusega. ■

Lausetest 8.84 ja 8.85 järelneb vahetult:

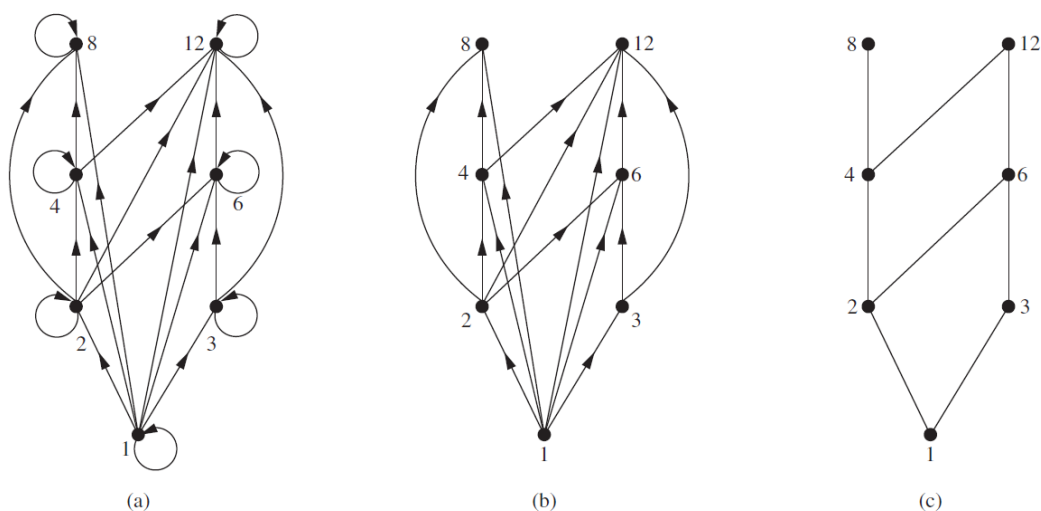
Järeldus 8.86

Lineaarselt järjestatud hulgas vähima ja minimaalse elemendi ning suurima ja maksimaalse elemendi mõisted ühtivad.

Lõplikku osaliselt järjestatud hulka saab esitada **Hasse diagrammina**. Selleks tuleb teha järgnevad sammud:

1. Esita järjestusseos $(R, \preceq)$ suunatud graafina
2. Kuna järjestusseos on refleksiivne, siis igas punktis (a, a) esineb silmus. Eemalda need silmused.
3. Järgmisena eemalda kõik servad, mis peavad seal olema transitiivsuse tõttu. Ehk eemalda kõik servad (a, c) , mille korral leidub $b \in R$ nii, et $a \preceq b$ ja $b \preceq c$.
4. Säti servad nii, et serva algpunkt oleks allpool lõpptippu.
5. Eemalda kõik suunad, sest kõik servad on nüüdseks juba suunatud üles.

Järgneval joonisel on samm-sammult kujutatud Hasse diagrammi tekkimine.



Joonis 8.1: Osaliselt järjestatud hulga $(\{1, 2, 3, 4, 6, 8, 12\}, |)$ Hasse diagramm

Hasse diagrammi kasulikkus seisneb selles, et sellelt on kerge leida minimaalseid ja maksimaalseid elemente. Nimelt, alumised elemendid on minimaalsed ja ülemised on maksimaalsed. Näiteks, ülemiselt jooniselt näeme, et vähim (seega ka minimaalne) element on 1 ja maksimaalsed elemendid on 8 ja 12 ning suurimat elementi ei ole.

Lisad

*Matemaatikas on küsimuste
püstitamise kunst väärtuslikum kui
probleemide lahendamine –
G. Cantor*

9.1	Valikuaksioom ja sellega ekvivalentssed väited	141
-----	--	-----

9.1 Valikuaksioom ja sellega ekvivalentssed väited

Aksioom 9.1: Valikuaksioom

Olgu H mittetühi hulk. Siis leidub funktsioon f , mis igale mittetühjale alamhulgale $X \subset H$ seab vastavusse elemendi samast hulgast $f(X) \in X$ (st, et kujutus f „valib” igast alamhulgast ühe elemendi).

Näide 9.2.

1. Kui H on naturaalarvude kõigi mittetühjade alamhulkade kogum, siis saame defineerida kujutuse f nii, et f seab igale alamhulgale vastavusse tema vähima elemendi.
2. Kui H on kõigi reaalarvuliste otspunktidega lõpliku pikkusega vahemike (a, b) , $a < b$, hulk, siis saame defineerida $f((a, b)) = \frac{a+b}{2}$.
3. Kui aga, H on reaalarvude hulga kõigi mittetühjade hulkade kogum, siis pole selge, kuidas sellist funktsiooni f leida. Tänapäevaks pole veel keegi sellist funktsiooni leidnud.

Kuratowski–Zorni lemmale tuginedes on võimalik tõestada mitmeid matemaatika fundamentaalseid teoreeme.

Definitsioon 9.3

Osaliselt järjestatud hulga mingi alamhulga **ülemine tõke** on element, mis on suurem või võrdne igast vaadeldavast elemendist.

Käesolevas kursuses ei esita me Kuratowski–Zorni lemma tõestust, kuid selle võib leida näiteks õpikust [6].

Lemma 9.4: Kuratowski–Zorni lemma

Kui osaliselt järjestatud hulga igal ahelal leidub ülemine tõke, siis selles hulgas leidub maksimaalne element.

Definitsioon 9.5

Hulka nimetatakse **täielikult järjestatuks**, kui ta on niiviisi lineaarselt järjestatud, et tema igal mittetühjal alamhulgal on olemas vähim element.

Näide 9.6.

1. Kõik lõplikud lineaarselt järjestatud hulgad on täielikult järjestatud.
2. Täielikult järjestatud hulk loomuliku järjestuse suhtes on näiteks $\mathbb{N} = \{1, 2, 3, \dots\}$.
3. Loomulik järjestus hulkades $\mathbb{Z}$, $\mathbb{Q}$ ja $\mathbb{R}$ ei ole täielik.
4. Täisarvude hulga saab muuta täielikult järjestatud hulgaks, järjestades tema elemendid järgmiselt:

$$1, 2, 3, \dots, 0, -1, -2, -3, \dots$$

5. Keegi pole aga seni osanud täielikult järjestada reaalarvude hulka $\mathbb{R}$.

Ülesanne 9.7. Kuidas täielikult järjestada kõiki ratsionaalarve?

Ka Zermelo teoreemi tõestust me antud kursus ei esita ja selle tõestuse võib jällegi leida õpikust [6].

Teoreem 9.8: Zermelo teoreem

Mis tahes mittetühja hulka on võimalik täielikult järjestada.

Järgmise teoreemi tulemuse võib leida näiteks õpikust [3].

Teoreem 9.9

Järgmised väited on samaväärsed:

- (i) **Kuratowski-Zorni lemma.** Kui osaliselt järjestatud hulga igal ahelal leidub ülemine tõke, siis selles hulgas leidub maksimaalne element.
- (ii) **Zermelo teoreem.** Mis tahes mittetühja hulka on võimalik täielikult järjestada.
- (iii) **Valikuaksioom.** Olgu H mittetühi hulk. Siis leidub funktsioon f , mis igale mittetühjale alamhulgale $X \subset H$ seab vastavusse elemendi samast hulgast $f(X) \in X$.

Kirjandus

- [1] F. Baudier, *Foundations of Mathematics*, Lecture notes at Texas A&M University, 2018.
- [2] R. Hammack, *Book of Proof*, Virginia Commonwealth University, 2013.
- [3] M. Kilp, *Algebra I*, Eesti Matemaatika Selts, Tartu, 2005.
- [4] V. Laan ja L. Tart, *Arvuteooria loengukonspekt*, TÜ, 2017.
- [5] T. J. Lakins, *The Tools of Mathematical Reasoning*, American Mathematical Society, 2016.
- [6] P. Oja, *Hulgateooria*, TÜ Kirjastus, 2006.
- [7] R. Palm, *Diskreetse matemaatika elemendid*, Tartu, 2009.
- [8] R. Palm ja R. Prank, *Sissejuhatus matemaatilisse loogikasse*, Tartu, 2004.
- [9] K. Rosen, *Discrete Mathematics and Its Applications*, Boston, McGraw-Hill, 2012.