# Matemaatiline maailmapilt

MTMM.00.342

Terje Hõim
Johann Langemets

2019/20 sügis

# Sisukord

***

# 1

# Sissejuhatus

***

*Jumal kirjutas universumi*
*matemaatika keeles – G. Galilei*



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 aastasadade 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 teadmistele, mida sa sellelt kursuselt 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 pingutamiseta, 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 tavapärases 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 suurusi 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 konkreetselt – 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 toredaid sõnamänge. Näiteks, Lewis Caroll loetleb üles aritmeetika neli tehet – kiitmine, nahutamine, jorutamine ja pragamine.

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 soovitused. Ole kursis sellega, mis toimub loengutes ja praktikumides. See eeldab kohal käimist ning igaks tunniks ettevalmistatud olemist. Pärast iga loengut käi materjal üle, kirjuta tähtsamad kohad oma sõnadega ümber või täida materjalis puuduolevad lüngad. Kui midagi jäi arusaamatuks, küsi kohe kas oma õppejõu või kursusekaaslase käest! Oleks väga hea, kui sul on kaaslane, kellega regulaarselt kursuse materjale arutada. Loe loengukonspekti hoolega ja hoia 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 üldomaksvõetud 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 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* $\geq 2$ *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 gruppi.
   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: $\Rightarrow$ *järeldub*, $\forall$ *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 1.1.** 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 $\leq -1$. $x = 0$ on ka sobiv.

(c) On olemas 3 sorti inimesi need, kes ei oska arvutada ja need, kes oskavad.

(d) Võrrandi $x^2 = 36$ lahendamiseks $\surd$ mõlemaid pooli.

(e) $f(x) = x^2$ ja $g(x) = 3x + 4$ tähendab $f(x) = g(x) = x = 4$.

# 2

# Mõiste, definitsioon, teoreem, eeldus ja väide

***

*Tervik on suurem kui tema osade summa – Aristoteles*



## 2.1 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 tunned 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 2.1.** Ahenda ja üldista järgmisi mõisteid:

(a) kolmnurk;

(b) geomeetria;

(c) ratsionaalarv;

(d) juur.

## 2.2 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 **definitsiooniks**.

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

1. **Definitsioon peab sisaldama ainult nii palju tunnuseid**, et ta täpselt piiritleks defineeritava mahu. Definitsioon „Kolmnurk on hulknurk" on liiga lai, aga definitsioon „Kolmnurk on hulknurk, millel on kolm võrdse pikkusega külge" jällegi liiga kitsas. (Seleta miks?) Liiga kitsas definitsioonis 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, definitsioon ei tohi sisaldada ringi. Kui sellest reeglist ei peeta kinni, saame **tautoloogia** ehk vea „idem per idem," mis tähendab ühe ja sama sõna kordumist definitsioonis.

3. **Definitsioon peab olema võimaluse korral jaatav**, sest eitava definitsiooni 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. Eitavaid definitsioone võib tarvitada ainult siis, kui defineeritav mõiste on ise eitavas laadis.

4. **Definitsioon peab olema selge ja arusaadav**, see tähendab, et definitsioonis ei tohi kasutada kahemõttelisi, metafoorseid ja segaseid väljendeid. Sellised väljendid nagu „lõvi on loomade kuningas“ ja „kordamine on tarkuse ema“ ei ole definitsioonid, aga neist võib olla abi mõistete sisu selgitamisel. Ka kuulus Hegeli poolt antud definitsioon riigile, “Riik on maailma vaimu poliitiline ilmutis” on ebakorrektne sel 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, sirget, tasandit, ruumi, hulka, arvu, 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. Inseneristkohtunik 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?)*

## 2.3 Liigitamine

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 võrdkülgseiks, võrdhaarseiks ja isekülgseiks. 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**.

## 2.4 Teoreem ja tõestus

Matemaatikas ei kontrollita tõele vastavust mitte eksperimenteerimise ja mõõtmise abil, vaid hoopis tõestades. **Teoreem** (kr. theóréma – vaadeldav, uuritav väide) on lause, mille õigsust tuleb tõestada arutluse kaudu, tuginedes aksioomidele ja varem tõestatud lausetele. Lauset, mille õigsust ei põhjendata teiste lausete abil, nimetatakse **aksioomiks** (kr. axióma – omaksvõetud 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) Iga kahe punkti $A$ ja $B$ korral $\overline{AB} = \overline{BA}$.

(d) **Paralleelide aksioom**: väljaspool sirget olevat punkti läbib ainult üks sirge, mis on paralleelne antud sirgega.

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, 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 järeldub, ehk mida on vaja tõestada.

**Näide 2.2.** „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 $A$ järeldub 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 järeldust üldise ilma puudutava väite kohta. Füüsikud ütlevad, et „Kui keha lastakse lahti maapinna lähedal, siis langeb see keha kiirendusega* $9,8\ m/s^2$ *.“ 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!*

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

Seega enamus 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 hüpotenuus, 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 mäeküljel musti lambaid. „Vaadake," hüüab insener. „Šotimaa selles osas on mustad lambad!" „Tõestitõesti," 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 poole pealt küll," pomiseb matemaatik oma nina alla.*

Vahetades teoreemis „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 2.3.** 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.

Seega, antud teoreemi kehtivusest ei järeldu pöördlause kehtivus. Kui aga pöördlause on tõene, siis nimetatakse seda **pöördteoreemiks**.

Asendades teoreemis „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 teoreemi **vastandlauseks**. Jällegi, antud teoreemi kehtivusest ei järeldu tema vastandlause kehtivus.

**Näide 2.4.** 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). Teoreemi „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 teoreemis „Kui $A$, siis $B$“ eeldus ja väide ning asendada nende eitustega, saame lause „Kui $\neg B$, siis $\neg A$.” Seda lauset nimetatakse antud teoreemi **pöördvastandlauseks**. Antud teoreemi kehtivusest järeldub alati selle teoreemi 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.

Teoreemis järeldub väide eeldusest. Sel juhul öeldakse, et eeldus on **piisav** väite tõestuseks. Kui kehtib teoreemi pöördteoreem, siis järeldub väitest eeldus. Sel juhul öeldakse, et eeldus on **tarvilik** väite tõestuseks. Kui koos teoreemiga kehtib ka pöördteoreem, siis võetakse tavaliselt need teoreemid kokku üheks lauseks, kasutades ühte väljenditest „on tarvilik ja piisav,” „siis ja ainult siis,” „parajasti siis, kui.”

**Näide 2.5.** „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 teoreemi, mis sisaldab tarvilikku ja piisavat tingimust, ümber sõnastada uuritava mõiste uueks definitsiooniks. Mõiste senine definitsioon muutub siis teoreemiks, mis sisaldab tarvilikku ja piisavat tingimust.

**Näide 2.6. Definitsioon**. Rööpkülikuks nimetatakse nelinurka, mille diagonaalid poolitavad teineteist. **Teoreem**. Nelinurk on rööpkülik siis ja ainult siis, kui ta vastasküljed on paralleelsed.

Märk $\square$ või $\blacksquare$ näitab teoreemi tõestuse lõppu.

Mõned teoreemid on huvitavamad ja tähtsamad kui teised. Seetõttu kasutavad matemaatikud sõna „teoreem“ asemel ka teisi alternatiivseid väljendeid. Sõna „teoreem“ kasutatakse vaid kõige tähtsamate ning üldistavamate tulemuste puhul. Muudel juhtudel kasutatakse akadeemilises tekstis järgnevaid nimetusi:

- **Lause** (ingl. k. *Proposition*) on väiksema tähtsusega teoreem.

- **Lemma** (*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** (*Corollary*) on lühikese ja lihtsa tõestusega tulemus, mille tõestuse olulisemaks osaks on eelnevalt tõestatud teoreem.

Mõnedes tekstides kasutatakse ka järgmisi nimetusi vahetulemuste väljatoomiseks:

- **Väide** (*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.

- **Tulemus** (*Result*) on väga tagasihoidlik ja üldine nimetus teoreemi kohta. Kõiki tähtsaid ja vähem tähtsaid teoreeme võib kutsuda tulemusteks.

- **Fakt** (*Fakt*) on väga väikese tähtsusega abitulemus.

## 2.5 Olemasolu ja üldisuse kvantorid

Järgmises konspekti peatükis näeme, kuidas matemaatikud kasutavad lausearvutuses spetsiaalseid loogikatehteid. Meie tutvume praeguses sissejuhatavas peatükis **kvantoritega** ja vastavate sümbolitega.

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 esitähti. 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 $x^3 - 27 = 0$." Üldkujul 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 väära lause $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R},\ x < y$, mida loetakse „leidub reaalarv $x$ nii, et iga reaalarvu $y$ korral $x < y$". Mõtle 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.

## 2.6 Kvantoreid sisaldavate lausete eitamine

Olgu antud järgmised kaks lauset:

- „Ei ole olemas täisarvu, mis on samaaegselt paaris ja paaritu."
- „Mitte kõik naturaalarvud ei ole algarvud."

Sümbolite abil saame need laused kirja panna järgmiselt:

- $\neg(\exists x \in \mathbb{Z}$, $x$ on paariarv ja $x$ on paaritu arv).
- $\neg(\forall x \in \mathbb{N}$, $x$ on algarv).

Mõeldes esimese lause peale, saame selle ümber sõnastada kujul „Kõik täisarvud ei ole samaaegselt paaris ja paaritud" ehk sümbolitega $\forall x \in \mathbb{Z}$, $\neg$($x$ on paarisarv ja $x$ on paaritu arv). Samamoodi on võimalik teine lause ümber sõnastada öeldes „Leidub naturaalarv, mis ei ole algarv" ehk matemaatika keeles $\exists x \in \mathbb{N}$, $\neg$($x$ on algarv).
Seega, väitmaks et $\exists x\ P(x)$ ei ole tõsi, väidame tegelikult, et $\forall x\ (\neg P(x))$.

**Näide 2.7.**

1. 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.

2. 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.

3. 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?

Väike spikker, mis aitab eituste moodustamist meeles pidada:

$$\neg(\forall x\ P(x)) \equiv \exists x(\neg P(x)), \quad \neg(\exists x\ P(x)) \equiv \forall x(\neg P(x))$$

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

Kas selliselt moodustatud laused on tõesed või mitte ja kuidas moodustada kvantoreid sisaldavate keerulisemate lausete eitusi, arutame järgmises peatükis.

# 3

# Lausearvutus

***

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



## 3.1 Matemaatiline loogika

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

Antiik-Kreeka mõtlejat **Aristotelest** (384–322 e.m.a.) 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.

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“. Tänaseks 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.

Traditsioonilise loogika aluseks on **mõtlemisseadused**, mida kutsutakse ka loogika aksioomideks. Mõtlemisseadusteks nimetame niisuguseid seadusi, millele peab alluma meie mõtlemine, et ta oleks loogiline ehk tõelevastav. Aristoteles sõnastas kolm mõtlemisseadust: samasuse seaduse, vasturääkivuste lubamatuse seaduse ja välistatud kolmanda seaduse. **W. G. Leibniz** (1646 – 1716) 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 vanasõna ütleb: „Üks räägib aiast ja teine aiaaugust.“ Matemaatikas on oluline jälgida, et mõisted, mida me arutluses kasutame, ei muutuks oma sisult arutluse käigus vaid, et 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“).

## 3.2 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. Matemaatilises loogikas nimetatakse **lauseks** 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 küsilaused ja paljud hüüdlaused, 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.

## 3.3 Tähtsamad lausearvutuse tehted

- **Eitus** (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 parjasti siis, kui lause $A$ on väär.
Kui lause sisaldab kvantorit, siis lause eitamine toimub järgmiselt:

$$\exists x\ P(x) \text{ eitus on } \forall x\ \neg P(x)$$

$$\forall x\ Q(x) \text{ eitus on } \exists x\ \neg Q(x)$$

Kvantoriga lause eitamisel tuleb vahetada kvantor ja eitada lauset.

**Näide 3.1.** $A =$ „Ühegi naturaalarvu logaritm pole null,“ $\neg A =$ „Vähemalt ühe naturaalarvu logaritm on null.“

**Näide 3.2.** $A =$ „Leidub reaalarv, millega ei saa jagada,“ $\neg A =$ „Iga reaalarvuga saab jagada.“

- **Konjunktsiooni** keeleliseks vasteks on sõnad „ja“ või „ning“. Tehtemärgina kasutatakse sümboleid $\wedge$ või &. Näiteks „Puhub tuul ja sajab vihma“ on valemkujul kirjutatuna $A \wedge B$ või $A\&B$, 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 komponentlaused $A$ ja $B$ on tõesed.

- **Disjunktsioon** (märk $\vee$) väljendab seost „või“. Näiteks „Helen laulab või Mart laulab“ on valemkujul $A \vee B$. 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.
Mittevälistava „või“ abil moodustatud liitlause on väär siis ja ainult siis, kui mõlemad komponentlaused on väärad.

- **Implikatsioon** (märk $\Rightarrow$ või $\rightarrow$ või $\supset$) 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 $A$ järeldub $B$.
  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** (märk $\Leftrightarrow$ või $\sim$ või $\leftrightarrow$) 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 valemkujul $A \Leftrightarrow B$.

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:

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

Eitus on ainus loogiline tehe, mida saab rakendada ainult ühele lausele. Ülejäänud loogiliste tehete – konjunktsioon, disjunktsioon, implikatsioon, ekvivalents – rakendamiseks peab olema vähemalt kaks komponenti.

Loogiliste tehete **prioriteedid** võimaldavad vähendada valemites kasutatavate sulgude arvu. Kõige kõrgema prioriteediga on eitusetehe 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

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

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.

## 3.4 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 3.3. Lausearvutuse valemid** 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 lõplikust 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 7.2).

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 valemeid 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 3.4.** Olgu antud valem

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

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 3.5.** Vaatleme taas valemit

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

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.

## 3.5 Valemite tõeväärtuse leidmine

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 3.6.** 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.

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

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 $Y = v$).

## 3.6 Muutujate väärtustused

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 $(1, 0, 1)$.

Olgu antud mingi lausearvutuse valem. Omistame kõigile selles valemis esinevatele lausemuutujatele tõeväärtused, s.o anname igale muutujale mingi tõeväärtuse. Valemi tõeväärtuse leidmiseks sellel väärtustusel tuleb sooritada kõik valemi tehted, milleks annab reeglid järgmine definitsioon.

**Definitsioon 3.7. Lausearvutuse valemi $\mathcal{F}$ tõeväärtus** etteantud väärtustusel leitakse järgmiste reeglite abil:

1. Kui $\mathcal{F} = \neg\mathcal{G}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{G} = 0$.
2. Kui $\mathcal{F} = \mathcal{G} \wedge \mathcal{H}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{G} = 1$ ja $\mathcal{H} = 1$.
3. Kui $\mathcal{F} = \mathcal{G} \vee \mathcal{H}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{G} = 1$ või $\mathcal{H} = 1$.
4. Kui $\mathcal{F} = \mathcal{G} \Rightarrow \mathcal{H}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{G} = 0$ või $\mathcal{H} = 1$.
5. Kui $\mathcal{F} = \mathcal{G} \Leftrightarrow \mathcal{H}$, siis $\mathcal{F} = 1$ parajasti siis, kui $\mathcal{G} = 1$ ja $\mathcal{H} = 1$ või $\mathcal{G} = 0$ ja $\mathcal{H} = 0$.

Eituse puhul on tegemist lihtsa postulaadiga, et teineteist eitavate lausete tõeväärtused on vastupidised. Konjunktsioon on tõene ainult juhul, kui mõlemad komponentlaused on tõesed. Disjunktsioon on tõene, kui on tõene vähemalt üks komponentlause. Seega realiseerib disjunktsioon sõna „või“ mittevälistavat tähendust. Implikatsioon on väär ainult siis, kui eesliige on tõene ja tagaliige väär. Kuigi tavakeeles kipume väära eesliikmega implikatsiooni (näiteks „Kui $1 = 2$, siis täna on tööpäev“) pidama rohkem vääraks kui tõeseks, peetakse tõeväärtuse arvutamise reeglites silmas pigem järeldumist matemaatilises mõttes. Näiteks pole meil mingit põhjust lugeda järeldust „Kui arv $x$ on positiivne, siis arvu $x$ ruut on positiivne“ vääraks juhul, kui vaadeldav arv on negatiivne või null. Lõpuks, ekvivalents kehtib siis, kui pooled on võrdse tõeväärtusega.

**Näide 3.8.** 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 $Z = 1$. Definitsiooni 3.7 esimese punkti põhjal saame, et $\neg X = 0$ ja $\neg Y = 1$ ning kolmanda punkti põhjal $Y \vee X = 1$. 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 kirjutatakse tehte tulemused iga tehtemärgi alla omaette veergu. Näites 3.8 konstrueeritud valemi tõeväärtustabeliks saame niiviisi

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

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 ($m$ tehtemärgi korral tuleb teha $2^n \cdot m$ tehet).

## 3.7 Valemite omadused

Järgnevas vaatleme lausearvutuse valemite „globaalseid“ omadusi, jälgides valemi tõeväärtust seal esinevate lausemuutujate erinevatel väärtustustel.

**Definitsioon 3.9.** Lausearvutuse valemit $\mathcal{F}$ nimetatakse **samaselt tõeseks** ehk **tautoloogiaks**, kui ta on igal väärtustusel tõene. Valemit $\mathcal{F}$ nimetatakse **samaselt vääraks** ehk **vastuoluliseks**, kui ta on igal väärtustusel väär.

Samaselt tõest valemit nimetatakse ka **loogiliselt tõeseks** valemiks ning samaselt väära valemit **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 ilmateates, 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 kanna, 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 väärad valemid esitavad väiteid, mis mingil tingimusel tõesed olla ei saa. Vaatleme näiteks valemit $X \wedge \neg X$ 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 homne ilm olema ühtaegu nii ilus kui ka halb. Seetõttu ka samaselt väära valemina esinev lause on infotühi.

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

**Näide 3.10.** Näidata, et valem $X \wedge Y \vee X \wedge \neg Y \vee \neg X \wedge Y \vee \neg X \wedge \neg Y$ on samaselt tõene. Koostame tõeväärtustabeli:

| $X$ | $Y$ | $X$ | $\wedge$ | $Y$ | $\vee$ | $X$ | $\wedge$ | $\neg Y$ | $\vee$ | $\neg X$ | $\wedge$ | $Y$ | $\vee$ | $\neg X$ | $\wedge$ | $\neg Y$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | | 1 | | 1 | | 0 | 0 | 1 | 0 | 0 | | 1 | 0 | 0 | 0 |
| 1 | 0 | | 0 | | 1 | | 1 | 1 | 1 | 0 | 0 | | 1 | 0 | 0 | 1 |
| 0 | 1 | | 0 | | 0 | | 0 | 0 | 1 | 1 | 1 | | 1 | 1 | 0 | 0 |
| 0 | 0 | | 0 | | 0 | | 0 | 1 | 0 | 1 | 0 | | 1 | 1 | 1 | 1 |

Et antud valemi tõeväärtuste veerus esinevad ainult tõesed väärtused, siis on valem samaselt tõene. Seda valemit võib pidada välistatud kolmanda seaduse üldistuseks kahe lausemuutuja juhule.

**Näide 3.11.** Näidata, et valem $\neg(X \vee Y) \wedge \neg(\neg X \vee \neg Y)$ on samaselt väär. Koostame tõeväärtustabeli:

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

Et antud valemi tõeväärtuste veerus esinevad ainult väärad väärtused, siis on valem samaselt väär.

Kui kaks valemit ei ole neis esinevate lausemuutujate ühelgi väärtustusel korraga tõesed, siis nimetatakse neid valemeid **vasturääkivateks**. Näite 3.11 põhjal võime öelda, et valemid $\neg(X \vee Y)$ ja $\neg(\neg X \vee \neg Y)$ on vasturääkivad. Analoogiliselt mõistetakse vasturääkivust kolme, nelja ja enama valemi puhul.

Vaatleme veel kahte valemiklassi.

**Definitsioon 3.12.** Lausearvutuse valemit $\mathcal{F}$ nimetatakse **kehtestatavaks**, kui ta on vähemalt ühel väärtustusel tõene. Valemit $\mathcal{F}$ nimetatakse **kummutatavaks**, kui ta on vähemalt ühe väärtustuse korral väär.

Näiteks valem $\neg(X \vee Y)$ on kehtestatav, sest tema tõeväärtuste veerus esineb 1 (vaata näite 3.11 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 3.13.** *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 ümberpöördult. □

**Lause 3.14.** *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. Ümberpöördult, 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 $\mathcal{F}$ 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.

# 4

# Valemite teisendamine

***

*Nägemusest, mida ei ole kontrollitud*
*ega tõestatud, ei piisa tõe tagamiseks*
*– B. Russel*



## 4.1 Järeldamine

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 4.1.** Öeldakse, et valemitest $\mathcal{F}_1, \ldots, \mathcal{F}_n$ **järeldub** valem $\mathcal{G}$, kui igal neis valemeis esinevate muutujate väärtustusel, millel $\mathcal{F}_1, \ldots, \mathcal{F}_n$ on tõesed, on ka $\mathcal{G}$ tõene.

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

$$\mathcal{F}_1, \ldots, \mathcal{F}_n \vDash \mathcal{G},$$

kus sümbolit $\vDash$ loetakse sõnaga „järeldub."

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

Järeldumist saab kindlaks teha tõeväärtustabeli abil. Valime tõeväärtustabelist välja read, milles valemid $\mathcal{F}_1, \ldots, \mathcal{F}_n$ 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 $\mathcal{F}_1, \ldots, \mathcal{F}_n$ on tõesed, kuid valem $\mathcal{G}$ on väär, siis oleme leidnud väärtustuse, mis väidetava järeldumise ümber lükkab.

**Näide 4.2.** Teha kindlaks, kas valemitest $\neg(X \wedge Y)$ ja $Y \Rightarrow X$ järeldub valem $\neg Y$. Koostame tõeväärtustabeli:

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

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

**Näide 4.3.** Näidata, et valemitest $X \Rightarrow Y$ 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 valemit järelduda ei saa on siis, kui mingil väärtustusel eeldused (s.t kaks esimest valemit) on tõesed, kuid väide (s.t 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 4.4.** Olgu antud lausemuutujad, mille tähendus on järgmine: $X =$ „Kiiruste liitmisseadus kehtib", $Y =$ „Valgus liigub kinnistähtedega 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 liitmisseadus kehtib ja valgus liigub kinnistähtedega seotud taustsüsteemis kõigis suundades sama kiirusega, siis pole Maal valguse liikumiskiirus kõigis suundades sama", sest Maa ilmselt liigub kinnistähtedega 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 liitmisseadus ei kehti".

**Näide 4.5.** Kontrollida, et kehtivad järgmised (kõige lihtsamad) lauseloogika järeldused:

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

Toome veel ühe näite lausearvutuse vahendite kasutamisest arutluse õigsuse kontrollimisel.

**Näide 4.6.** 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.*

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

*Tõestus.* Kui valemitest $\mathcal{F}_1, \ldots, \mathcal{F}_n$ järeldub valem $\mathcal{G}$, siis neil väärtustustel, millel valemid $\mathcal{F}_1, \ldots, \mathcal{F}_n$ on tõesed, on ka valem $\mathcal{G}$ tõene, mistõttu $\mathcal{F}_1 \wedge \ldots \wedge \mathcal{F}_n \Rightarrow \mathcal{G}$ on tõene. Väärtustustel, millel mõni valemitest $\mathcal{F}_1, \ldots, \mathcal{F}_n$ on väär, on valem $\mathcal{F}_1 \wedge \ldots \wedge \mathcal{F}_n \Rightarrow \mathcal{G}$ tõene seetõttu, et implikatsiooni eesliige on väär.
Ümberpöördult, kui valem $\mathcal{F}_1 \wedge \ldots \wedge \mathcal{F}_n \Rightarrow \mathcal{G}$ on samaselt tõene, siis igal väärtustusel, millel valemid $\mathcal{F}_1, \ldots, \mathcal{F}_n$ on tõesed, on ka $\mathcal{F}_1 \wedge \ldots \wedge \mathcal{F}_n$ tõene, mistõttu valem $\mathcal{G}$ on samuti tõene. $\square$

**Näide 4.8.** Kordame uuesti näites 4.2 toodud ülesannet, kus pidi kindlaks tegema, kas valemitest $\neg(X \wedge Y)$ ja $Y \Rightarrow X$ järeldub valem $\neg Y$. Kasutades teoreemi 4.7, kontrollime seega, kas valem

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

on samaselt tõene. Selleks koostame vastava tõeväärtustabeli:

| $X$ | $Y$ | $\neg(X \wedge Y)$ | $\wedge$ | $(Y \Rightarrow X)$ | $\Rightarrow$ | $\neg Y$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 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!

## 4.2 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 | 0 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 |
| 0 | 0 | 1 | 1 | 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 valemeid ei ole võimalik nende komponentlausete sisu järgi teineteisest eristada, ehkki neil võib olla erinev väliskuju. Niisugustest kaalutlustest lähtudes anname järgmise definitsiooni.

**Definitsioon 4.9.** Valemeid $\mathcal{F}$ ja $\mathcal{G}$ nimetatakse **loogiliselt samaväärseteks**, kui nende tõeväärtused on võrdsed igal neis valemeis esinevate muutujate väärtustusel.

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

**Näide 4.10.** 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 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 | 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 valemitena 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, s.t järeldus on mõlemapidine. Eeldusest järeldub tulem ja vastupidi.

**Teoreem 4.11.** *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 $\mathcal{G} \models \mathcal{F}$.
Ümberpöördult, kui $\mathcal{F} \models \mathcal{G}$ ja $\mathcal{G} \models \mathcal{F}$, siis ei saa leiduda 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 $\mathcal{F}$. $\square$

Niisugust omadust kasutatakse tihti valemite samaväärsuse tõestamisel.

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

**Teoreem 4.12.** *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 ümberpöördult, 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. □

## 4.3 Lausearvutuse põhisamaväärsused

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

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

Kuid nende samaväärsuste kehtivust võib tõestada ka otsese arutlemise teel.

**Näide 4.14.** 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.
Ümberpöördult, 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 järeldub, 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 järeldub, et $\mathcal{G} \vee \mathcal{H}$ on tõene. Ka sel juhul on vasakpoolne valem tõene. Niisiis oleme näidanud, et vasakpoolsest valemist järeldub parempoolne ning parempoolest vasakpoolne. See tähendab, et need valemid on samaväärsed. $\square$

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.

## 4.4 Otsustuse eitamine

Nagu varasemalt (vt peatükk 2) õpitud, seisneb otsustuse eitamine antud väitele vasturääkiva väite leidmises. Lihtotsustuse eitamise reeglid võib kokku võtta järgmises tabelis:

| **Otsustus** | **Otsustuse eitus** |
|---|---|
| Kõik S on P | Mõni S ei ole P |
| Mitte ükski S ei ole P | Mõni S on P |
| Mõni S on P | Mitte ükski S ei ole P |
| Mõni S ei ole P | Kõik S on P |

Tabeli esimesele reale vastab juba tuntud kvantori ja eituse vahetamisseadus

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

ning tabeli kolmandale reale vastab samaväärsus

$$\neg(\exists x\ P(x)) \equiv \forall x\ \neg P(x).$$

Liitotsustuse eitamise reeglid saab aga lausearvutuse põhisamaväärsuste abil kirja panna järgmiselt:

| **Otsustus** | **Otsustuse eitus** |
|---|---|
| $\neg A$ | $A$ |
| $A \wedge B$ | $\neg A \vee \neg B$ |
| $A \vee B$ | $\neg A \wedge \neg B$ |
| $A \Rightarrow B$ | $A \wedge \neg B$ |
| $A \Leftrightarrow B$ | $(A \wedge \neg B) \vee (\neg A \wedge B)$ |

Tabelis olevat viimast rida võime selgitada järgmise näite abil.

**Näide 4.15.** Lause: „Inimene tunneb tööst rõõmu siis ja ainult siis, kui ta töö eest korralikku palka saab“.
Lause eitus: „Mõni inimene tunneb tööst rõõmu, kuigi ei saa töö eest korralikku palka või saab korralikku palka, kuid ei tunne tööst rõõmu“.

Samaväärsuse 6. ehk De Morgani seaduste tundmine on abiks ka järgmise kvantoritega lause eitamisel.

**Näide 4.16.** Lause „Kõikide täisarvude a ja b korral, kui korrutis ab on paarisarv, siis a on paarisarv või b on paarisarv.“ eitus 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 eitus kirja panna kvantoreid kasutades.

## 4.5 Valemite teisendamine

Samaväärsused etendavad lausearvutuses samasugust rolli nagu samasused algebras. Nii nagu algebras kasutatakse samasusi avaldiste lihtsustamiseks, nii võib ka lausearvutuse valemeid teisendada ja lihtsustada lausearvutuse samaväärsustega, kusjuures tekkiv valem jääb igal sammul samaväärseks esialgsega. Üks teisendussamm tähendab valemi 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 valemi mingit osavalemit.

**Teoreem 4.17.** *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 ning loogilistest samaväärsustest 9. ja 11. □

**Näide 4.18.** 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 4.19.** 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 4.20.** 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 4.21.** *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).

□

## 4.6 Täielik disjunktiivne 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 4.22.** **Lihtkonjunktsiooniks** ehk **elementaarkonjunktsiooniks** 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 4.23.** Lihtkonjunktsiooni nimetatakse **täielikuks**, 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 4.24.** Lausearvutuse valemi $\mathcal{F}$ **disjunktiivseks normaalkujuks** nimetatakse valemiga $\mathcal{F}$ samaväärset valemit, mis kujutab endast erinevate lihtkonjunktsioonide disjunktsiooni.

Ühel valemil võib olla ka rohkem kui üks disjunktiivne normaalkuju.

**Näide 4.25.** 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 4.26.** Lausearvutuse valemi $\mathcal{F}$ **täielikuks disjunktiivseks normaalkujuks** nimetatakse valemiga $\mathcal{F}$ samaväärset valemit, mis kujutab endast erinevate täielike lihtkonjunktsioonide disjunktsiooni.

*Märkus.* Sarnaselt täieliku disjunktiivse normaalkujuga saab defineerida ka täieliku konjunktiivse normaalkuju, mis kujutab endast erinevate täielike lihtdisjunktsioonide konjunktsiooni.

**Näide 4.27.** Näite 4.25 põhjal on valemi $\mathcal{F} = X \Rightarrow Y$ täielik disjunktiivne 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 disjunktiivsel 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 üldtähisena $X^\alpha$, kus $\alpha = t$ või $\alpha = v$. On kerge veenduda, et $X^\alpha = t \Leftrightarrow X = \alpha$ (kontrolli!).

**Lause 4.28.** *Täielike lihtkonjunktsioonide disjunktsioon*

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

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

**Näide 4.29.** Valem $X \wedge Y \vee \neg X \wedge \neg Y$ on täielikul disjunktiivsel normaalkujul. See valem on tõene väärtustustel $(t, t)$ ja $(v, v)$ ning väär väärtustustel $(t, v)$ ja $(v, t)$.

**Näide 4.30.** 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 disjunktiivsel normaalkujul olev on tõene parajasti väärtustustel $(t, v, t)$, $(v, t, t)$ ja $(v, v, v)$.

**Ülesanne 4.31.** Leida kolme muutuja valem, mis on tõene parajasti siis, kui kaks muutujat on väärad.

**Teoreem 4.32.** *Valemil eksisteerib täielik disjunktiivne normaalkuju parajasti siis, kui ta on kehtestatav.*

Teoreemist 4.32 järeldub vahetult, et samaselt vääral valemil ei leidu täielikku disjunktiivset normaalkuju.

## 4.7 Täielikule disjunktiivsele normaalkujule teisendamine

Etteantud (kehtestatava) valemi saab teisendada disjunktiivsele 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.

2. 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.

3. Asendame disjunktsioonide konjunktsioonid distributiivsust kasutades konjunktsioonide disjunktsioonidega $\mathcal{F} \wedge (\mathcal{G} \vee \mathcal{H}) \equiv \mathcal{F} \wedge \mathcal{G} \vee \mathcal{F} \wedge \mathcal{H}$

4. Kui esineb samaselt vääraid konjunktsioone, st esinevad samaaegselt $X$ ja $\neg X$, siis võime ka need ära jätta. Võrdsetest konjunktsioonidest jätame idempotentsuse omaduse tõttu alles ainult ühe $\mathcal{F} \wedge \mathcal{F} \equiv \mathcal{F}$.

5. Täieliku disjunktiivse normaalkuju saamiseks tuleb iga lihtkonjunktsioon teha täielikuks: kui näiteks lihtkonjunktsioonis $K$ puudub muutuja $X$, siis samaväärsusega

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

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

Valemi täielikku disjunktiivset normaalkuju saab leida ka tõeväärtustabeli abil.

**Näide 4.33.** Leida valemi $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$ täielik disjunktiivne normaalkuju.

| $X$ | $Y$ | $Z$ | $X$ | $\wedge$ | $\neg Y$ | $\wedge$ | $(Z$ | $\Rightarrow$ | $\neg X)$ | $\Leftrightarrow$ | $Y$ | $\vee$ | $X$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | | 0 | 0 | 0 | | 0 | 0 | 0 | | 1 | |
| 1 | 1 | 0 | | 0 | 0 | 0 | | 1 | 0 | 0 | | 1 | |
| 1 | 0 | 1 | | 1 | 1 | 0 | | 0 | 0 | 0 | | 1 | |
| 1 | 0 | 0 | | 1 | 1 | 1 | | 1 | 0 | 1 | | 1 | |
| 0 | 1 | 1 | | 0 | 0 | 0 | | 1 | 1 | 0 | | 1 | |
| 0 | 1 | 0 | | 0 | 0 | 0 | | 1 | 1 | 0 | | 1 | |
| 0 | 0 | 1 | | 0 | 1 | 0 | | 1 | 1 | 1 | | 0 | |
| 0 | 0 | 0 | | 0 | 1 | 0 | | 1 | 1 | 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 $(0, 0, 0)$.

2. Nendele väärtustustele vastavad täielikud lihtkonjunktsioonid on vastavalt $X \wedge \neg Y \wedge \neg Z$, $\neg X \wedge \neg Y \wedge Z$ ja $\neg X \wedge \neg Y \wedge \neg Z$.

3. Seega valemi $X \wedge \neg Y \wedge (Z \Rightarrow \neg X) \Leftrightarrow Y \vee X$ täielik disjunktiivne normaalkuju on

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

# 5

# Hulga mõiste

***

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



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 defineeris 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 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 $A, B, C, X, Y, \ldots$, hulga elemente aga väikeste ladina tähtedega $a, b, c, x, y, \ldots$. 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 5.1.** 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 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 $A = B$.

## 5.1 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 $A = \{$Päts, Meri, Rüütel, Ilves, Kaljulaid$\}$ 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 $X = \{1, 3, 5, \ldots, 49\}$ on kõigi 50-st väiksemate positiivsete paaritute arvude hulk ning $Y = \{2, 4, 6, \ldots\}$ on kõigi positiivsete paarisarvude hulk. Antud kirjaviisis mõttepunktid (kolm punkti) tähendavad seda, et jätka 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 $S = \{x \colon p(x)\}$ või $S = \{x \mid p(x)\}$, kus $p(x)$ tähistab tingimust või tingimuste loetelu, mida vaadeldavasse 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, et 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 5.2.** 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 5.3.** 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 5.4. Tühjaks hulgaks** $\emptyset$ nimetatakse hulka, mis ei sisalda ühtegi elementi.

Hulga elementideks võivad olla ka hulgad ise.

**Näide 5.5.**

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; s.t $2 \notin T$.

Lõpliku hulga $S$ korral tähistame sümboliga $|S|$ hulgas $S$ olevate elementide arvu ja nimetatame seda **hulga võimsuseks** ehk **hulga kardinaalarvuks** ja mõnikord lühemalt **kardinaalsuseks**. Kui $A = \{1, 2\}$ ja $B = \{1, 2, \{1, 2\}, \emptyset\}$, siis $|A| = 2$ ja $|B| = 4$. Samuti $|\emptyset| = 0$. Lõpmatu hulga võimsuse juurde tuleme hiljem tagasi.

Vaatame veel näiteid.

**Näide 5.6.** Olgu $D = \{n \in \mathbb{N}, n \leq 9\}$, $E = \{x \in \mathbb{Q}, x \leq 9\}$, $H = \{x \in \mathbb{R}\colon x^2 - 2 = 0\}$ ja $J = \{x \in \mathbb{Q}\colon x^2 - 2 = 0\}$.

(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 5.7.** Millistesse järgmistesse hulkadesse kuulub arv $-2$?

(a) $S_1 = \{-1, -2, \{-1\}, \{-2\}, \{-1, -2\}\}$;

(b) $S_2 = \{x \in \mathbb{N}\colon -x \in \mathbb{N}\}$;

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

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

(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. $\square$

**Ülesanne 5.8.** Mõtle välja üks viietäheline sõna nii, et $|S| = 3$, kus $S$ on sõnas esinevate tähtede hulk.

## 5.2 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 5.9.** Hulka $A$ nimetatakse hulga $B$ **osahulgaks** ehk **alamhulgaks**, 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

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

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

**Näide 5.10.**

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

**Lause 5.11.** *Hulkade sisalduvusseosel $\subset$ järgmised omadused:*

1. ***Refleksiivsus**: Iga hulga $A$ korral $A \subset A$;*
2. ***Antisümmeetrilisus**: Kui $A$ ja $B$ on sellised hulgad, et $A \subset B$ ja $B \subset A$, siis $A = B$;*
3. ***Transitiivsus**: Kui $A, B$ ja $C$ on sellised hulgad, et $A \subset B$ ja $B \subset C$, siis $A \subset C$;*
4. *Tühi hulk $\emptyset$ on iga hulga osahulk.*

*Tõestus.* Tõestame kolmanda ja neljanda omaduse. Esimese kahe omaduse tõestuse jätame iseseisvaks tööks.
3. 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 $x \in A$ järeldub, 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 järeldame, et ka $x \in C$. Olemegi näidanud, et suvalise elemendi $x$ korral hulgast $A$ see element kuulub ka hulka $C$. Seega $A \subset C$.
4. Oletame väite vastaselt, 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. □

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

**Lause 5.13.** *Tühi hulk $\emptyset$ on üheselt määratud.*

*Tõestus.* Oletame vastuväiteliselt, et leiduvad kaks erinevat tühja hulka $\emptyset_1$ ja $\emptyset_2$. Nüüd lauses 5.11 toodud 4. 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 5.11 toodud 2. omaduse põhjal järeldub, et $\emptyset_1 = \emptyset_2$. Viimane on aga vastuolus meie eeldusega, et $\emptyset_1 \neq \emptyset_2$. Seega leidub täpselt üks tühi hulk. □

**Ülesanne 5.14.** 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 üheelemendilisest 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 5.15.** Hulka $A$ nimetatakse hulga $B$ **pärisosahulgaks** või **pärisalamhulgaks** 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 5.16.**

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 5.17.** 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 sümboolikat kasutades kirja panna järgmiselt:

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

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. $\square$

**Ülesanne 5.18.** Tõesta, et ratsionaalarvude hulk $\mathbb{Q}$ on reaalarvude hulga $\mathbb{R}$ pärisosahulk.

Hulga $A$ **kõigi osahulkade hulka** tähistatakse tavaliselt $\mathcal{P}(A) = \{X \mid X \subset A\}$.

**Ülesanne 5.19.** 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 $|\mathcal{P}(A)| = 8$.

$\square$

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

*Tõestus.* Iseseisvalt! $\square$

**Näide 5.21.** 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 $\{\{\emptyset\}\} \in \mathcal{P}(C)$.

# 6

# Tehted hulkadega

***

*Matemaatikas on küsimuste*
*püstitamise kunst väärtuslikum kui*
*probleemide lahendamine – G. Cantor*



## 6.1 Hulkade ühend

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 6.1.** Hulkade $A$ ja $B$ **ühendiks** nimetatakse hulka $A \cup B$, mille moodustavad kõik elemendid, mis kuuluvad vähemalt ühte hulkadest $A$ või $B$, s.t

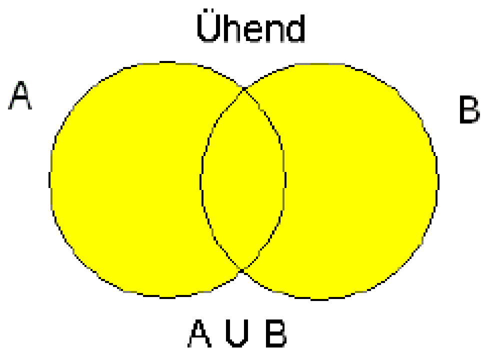
$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

Sidesõna „või“ kasutatakse siin jällegi mittevälistavas tähenduses, s.t 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 6.2.**

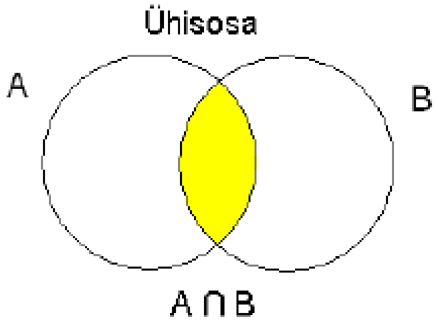
1. Kui $A = \{a, b, c\}$ ja $B = \{a, c, d, e\}$, siis $A \cup B = \{a, b, c, d, e\}$;
2. $[0, 1) \cup (0, 1] = [0, 1]$;
3. $\mathbb{N} \cup \mathbb{Q} = \mathbb{Q}$.

## 6.2 Hulkade ühisosa

**Definitsioon 6.3.** Hulkade $A$ ja $B$ **ühisosaks** ehk **lõikeks** nimetatakse hulka $A \cap B$, mille moodustavad kõik elemendid, mis kuuluvad nii hulka $A$ kui ka hulka $B$, s.t

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

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




**Näide 6.4.**

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

*Tõestus.* 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 $B$. Üldisust kitsendamata vaatame hulka $A$ (me oleksime sama hästi võinud valida ka hulga $B$). 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 6.6.** Mida saab öelda hulkade $A$ ja $B$ kohta, kui $A \cap B = \emptyset$? Kui $A \cap B = A$? Kui $A \cap B = B$? Joonista vastavad Venni diagrammid.

**Ülesanne 6.7.** Tõesta, et kui element $x$ ei kuulu kahe hulga $A$ ja $B$ ühendisse, siis ei kuulu ta ka nende hulkade ühisossa.

**Teoreem 6.8.** *Hulkade ühendil ja ühisosal on järgmised omadused:*

1. ***Idempotentsus:*** $A \cup A = A$, $A \cap A = A$;
2. ***Kommutatiivsus:*** $A \cup B = B \cup A$, $A \cap B = B \cap A$;
3. ***Assotsiatiivsus:*** $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$;

*4.* ***Distributiivsus:*** $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$, $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

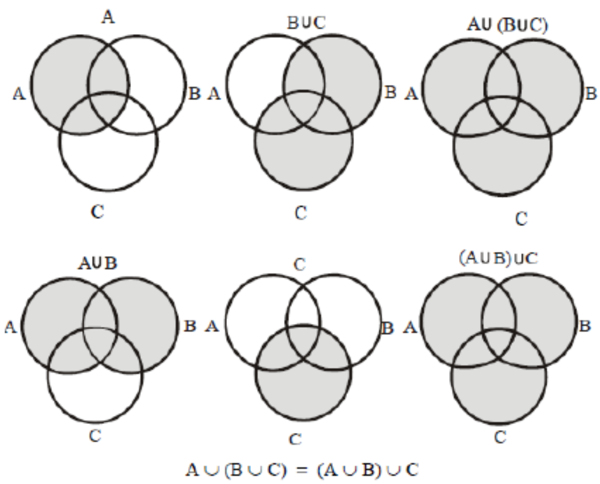
*Tõestus.* Omadused 1. – 3. järelduvad vahetult definitsioonidest ja on jäetud iseseisvaks tööks. Näitena tõestame teise distributiivsuse võrduse ehk $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

(i) Olgu $x \in (A \cap B) \cup C$. Siis $x \in A \cap B$ või $x \in C$. Kui $x \in C$, siis $x \in A \cup C$ ja $x \in B \cup C$, mistõttu $x \in (A \cup C) \cap (B \cup C)$. Kui aga $x \notin C$, siis $x \in A \cap B$ ehk $x \in A$ ja $x \in B$. Siis aga $x \in A \cup C$ ja $x \in B \cup C$, s.t $x \in (A \cup C) \cap (B \cup C)$. Sellega on näidatud, et $(A \cap B) \cup C \subset (A \cup C) \cap (B \cup C)$.

(ii) Olgu nüüd $x \in (A \cup C) \cap (B \cup C)$. Siis $x \in (A \cup C)$ ja $x \in (B \cup C)$. Kui $x \in C$, siis $x \in (A \cap B) \cup C$. Kui aga $x \notin C$, siis $x \in A$ ja $x \in B$ ehk $x \in A \cap B$ ning $x \in (A \cap B) \cup C$. Sellega on näidatud ka $(A \cup C) \cap (B \cup C) \subset (A \cap B) \cup C$ ning ühtlasi tõestatud teine distributiivsuse võrdus.

□

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




## 6.3 Hulkade vahe

**Definitsioon 6.9.** Hulkade $A$ ja $B$ **vaheks** nimetatakse hulka $A \setminus B$, mille moodustavad elemendid, mis kuuluvad hulka $A$, aga ei kuulu hulka $B$, s.t

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

**Näide 6.10.**

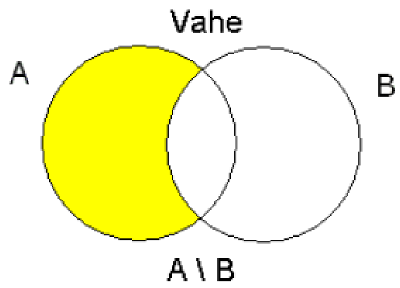
1. Kui $A = \{1, 2, 3, 4, 5\}$ ja $B = \{2, 4, 6\}$, siis $A \setminus B = \{1, 3, 5\}$ ja $B \setminus A = \{6\}$;

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 6.11.** Olgu antud hulgad $A = \{x \in \mathbb{R} \colon |x| \leq 3\}$, $B = \{x \in \mathbb{R} \colon |x| > 2\}$ ja $A = \{x \in \mathbb{R} \colon |x-1| \leq 4\}$.

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 6.12.** *Olgu $A, B$ ja $C$ hulgad. Siis*

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

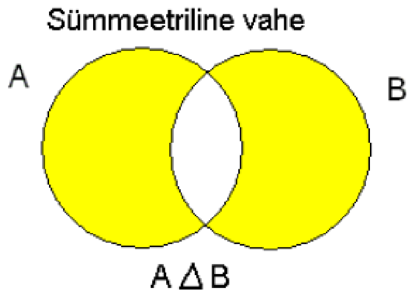
*Tõestus.* Iseseisvalt. □

## 6.4 Hulkade sümmeetriline vahe

**Definitsioon 6.13.** Hulkade $A$ ja $B$ **sümmeetriliseks vaheks** nimetatakse hulka $A \bigtriangleup B$, mille moodustavad elemendid, mis kuuluvad parajasti ühte kahest hulgast $A$ ja $B$, s.t

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

Sümmeetrilist vahet illustreerib järgmine Venni diagramm:




**Näide 6.14.** Kui $A = \{a, b, c\}$ ja $B = \{a, c, d, e\}$, siis $A \triangle B = \{b, d, e\}$.

**Lause 6.15.** *Olgu $A$ ja $B$ hulgad. Siis $A \triangle B = (A \cup B) \setminus (A \cap B)$.*

*Märkus.* Vaata ning võrdle seda tulemust sümmeetrilist vahet illustreeriva Venni diagrammiga.

*Lause 6.15 tõestus.* Peame tõestama, et kaks hulka $A \triangle B$ ja $(A \cup B) \setminus (A \cap B)$ on võrdsed. Selleks peame näitama mõlemapoolseid sisalduvusi ehk veenduma, et $A \triangle B \subset (A \cup B) \setminus (A \cap B)$ ja $(A \cup B) \setminus (A \cap B) \subset A \triangle B$.

1. Näitame esiteks, et kui $x \in A \triangle B$, siis $x \in (A \cup B) \setminus (A \cap B)$. Seega, olgu $x \in A \triangle B$. Hulkade sümmeetriline vahe on defineeritud ühendi kaudu, seega $x \in (A \setminus B) \cup (B \setminus A)$, mis omakorda tähendab, et $x \in A \setminus B$ või $x \in B \setminus A$. Kuna me ei tea, kumb kahest olukorrast aset leiab, vaatleme mõlemat juhtu eraldi. Seega jaguneb meie tõestus kahe alamjuhu vahel ning mõlemal korral peame näitama, et $x \in (A \cup B) \setminus (A \cap B)$.

   (a) Olgu $x \in A \setminus B$ , mis tähendab, et $x \in A$, kuid $x \notin B$. Kuna $x \in A$, siis võime öelda, et $x \in A \cup B$. Kuna $x \notin B$, siis ei ole element $x$ mõlemas hulgas, mis tähendab, et $x \notin A \cap B$. Kokkuvõtvalt $x \in (A \cup B) \setminus (A \cap B)$.

   (b) Olgu $x \in B \setminus A$, mis tähendab, et $x \in B$, kuid $x \notin A$. Sarnaselt eelneva aruteluga võime väita, et $x \in A \cup B$, kuid $x \notin A \cap B$. Seega taas $x \in (A \cup B) \setminus (A \cap B)$.

2. Teiseks peame näitama sisalduvust $(A \cup B) \setminus (A \cap B) \subset A \triangle B$. Oletame, et $x \in (A \cup B) \setminus (A \cap B)$. Selle kohaselt $x \in A \cup B$, kuid $x \notin A \cap B$. Eesmärgiks on näidata, et $x \in A \triangle B = (A \setminus B) \cup (B \setminus A)$ ehk meil oleks vaja näidata, et $x \in A \setminus B$ või $x \in B \setminus A$. Milline informatsioon meil hetkel teada on? Kuna $x \in (A \cup B) \setminus (A \cap B)$, siis $x$ kuulub ühte hulkadest $A$ või $B$, aga mitte mõlemasse. Ehk teisisõnu, kas $x \in A$ ja $x \notin B$ või et $x \in B$, kuid $x \notin A$. See aga tähendab, et $x \in A \setminus B$ või $x \in B \setminus A$, just täpselt, mida soovisimegi! Seega $x \in (A \setminus B) \cup (B \setminus A) = A \triangle B$. Kuna mõlemapoolsed sisalduvused on näidatud, oleme tõestanud, et $A \triangle B = (A \cup B) \setminus (A \cap B)$.

□

Lisaks just tõestatud lausele 6.15 on sümmeetrilisel vahel veel järgmised omadused.

**Lause 6.16.** *Olgu $A$, $B$ ja $C$ hulgad. Siis*

1. ***Kommutatiivsus:*** $A \triangle B = B \triangle A$;
2. ***Assotsiatiivsus:*** $(A \triangle B) \triangle C = A \triangle (B \triangle C)$;
3. ***Distributiivsus:*** $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$;
4. $A \triangle B = A \cup B \Leftrightarrow A \cap B = \emptyset$.

*Tõestus.* Iseseisvalt. □

**Ülesanne 6.17.** Kujuta Venni diagrammil hulgad $A \setminus (B \cup C)$, $A \cap (B \setminus C)$, $(A \setminus B) \setminus C$ ja $A \setminus (B \setminus C)$.

## 6.5 Hulga täiend

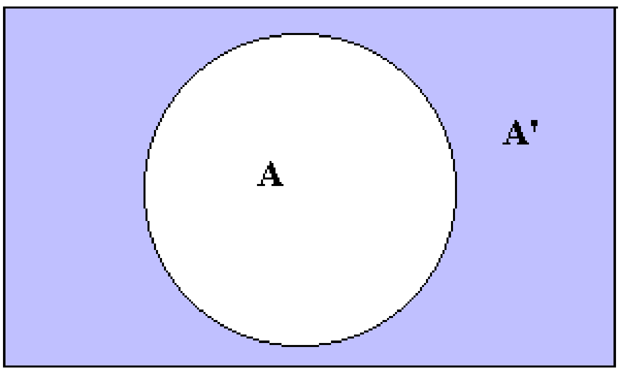
Koolimatemaatikas tegeletakse näiteks naturaalarvude hulgaga või täisarvude hulgaga, kusjuures uurimise objektideks on nii nende hulkade elemendid ja osahulgad kui ka elementide vahel defineeritud seosed, tehted ja funktsioonid. Hulgateoorias nimetatakse sellist hulka, mille uurimise objektideks on peamiselt 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 6.18.** Hulga $A$ **täiendiks** $A'$ nimetatakse hulka, mille moodustavad kõik need universaalse hulga $U$ elemendid, mis ei kuulu hulka $A$, s.t

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

Hulga $A$ täiendit saab Venni diagrammi abil kujutada järgmiselt:



**Näide 6.19.**

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

**Lause 6.20.** *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. Kahe hulga võrdsuse näitamiseks peame näitama mõlemad sisalduvused, esiteks $(A \cap B)' \subset A' \cup B'$ ja teiseks $A' \cup B' \subset (A \cap B)'$. Olgu $x \in (A \cap B)'$. Siis $x \notin A \cap B$. See aga tähendab, et $x \notin A$ või $x \notin B$. Seega peab kehtima, et $x \in A'$ või $x \in B'$ ehk teiste sõnadega, $x \in A' \cup B'$. Vastupidiselt, olgu nüüd $x \in A' \cup B'$. Siis $x \in A'$ või $x \in B'$, mis omakorda tähendab, et $x \notin A$ või $x \notin B$. Kuna $x$ ei kuulu vähemalt ühte hulkadest $A$ või $B$, siis ta ei saa olla nende ühisosas ehk $x \notin A \cap B$. See on aga sama mis $x \in (A \cap B)'$. Seega saame mõlemapidisest arutelust järeldada, et hulgad $(A \cap B)'$ ja $A' \cup B'$ on võrdsed. □

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 igaühte neist saab väljendada teiste kaudu. De Morgani seadustest järeldub 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 tõesest võrdusest niimoodi moodustatud hulkade vahel saame uue, samuti tõese võrduse, kui asendame kõik hulgad nende täiendhulkadega ning tehted $\cap$ ja $\cup$ vastavalt tehetega $\cup$ ja $\cap$.

Näiteks võime kirjutada $A \cap B = A \setminus (A \setminus B)$ ning eespool oli juba antud esitus $A \vartriangle B = (A \setminus B) \cup (B \setminus A)$.

**Ülesanne 6.21.**

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

**Ülesanne 6.22.** 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.

## 6.6 Tehete omadused – kokkuvõte

Oled kindlasti märganud, et avaldiste lihtsustamisel ja võrdlemisel on kasulik teada tehete algebralisi omadusi. Hulgateoreetilisi tehteid sisse tuues esitasime igas alapeatükis mõned lihtsamad omadused, mis tulenesid otseselt tehete definitsioonidest. Näiteks said sa teada, et ühend, ühisosa ja sümmeetriline vahe on kommutatiivsed tehted, aga vahe ei ole (too kontranäide!).

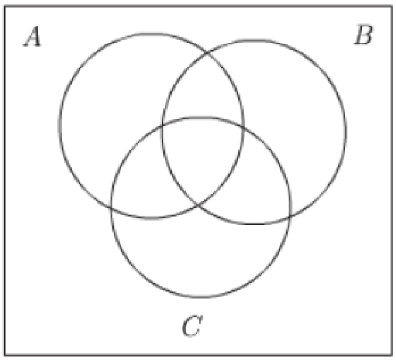
Mõned hulgateooria samasused saame lausearvutusest otse üle võtta. Ühend, ühisosa ja täiend on defineeritud vastavalt komponenthulkadesse kuulumise tingimuste disjunktsiooni, konjunktsiooni ja eituse abil. Seetõttu on neil tehetel nii ühekaupa kui ka omavahelistes seostes samad omadused, mis vastavatel lausearvutuse tehetel.

Nagu reaalarvude ja lausearvutuse jaoks, kehtivad ka hulgateoreetiliste tehete kohta mitmed keerulisemad samasused, kus esineb korraga mitu tehet. Peale idempotentsuse, kommutatiivsuse ja assotsiatiivsuse kehtivad mõned distributiivsuse seadused, ühtesid tehteid saab avaldada teiste kaudu jne. Esitame siin kokkuvõtvalt olulisemad samasused, millega mõnedest sa juba eespool tutvusid ja mida sagedasti kasutatakse.

1. Nagu lausearvutuses disjunktsiooni ja konjunktsiooni vahel, kehtivad ka ühendi ja ühisosa vahel kaks distributiivsuse seadust. Lisaks jaotub ühisosa võtmine ka hulkade vahele ja sümmeetrilisele vahele.
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$$
$$A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C), \qquad A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C).$$
2. Neelduvuse seadused
$$A \cup (A \cap B) = A, \qquad A \cap (A \cup B) = A.$$
3. De Morgani seadused
$$(A \cap B)' = A' \cup B', \qquad (A \cup B)' = A' \cap B'.$$
4. Vahe seosed teiste tehetega
$$A \setminus B = A \setminus (A \cap B), \qquad A \cup B = A \cup (B \setminus A), \qquad (A \setminus B) \setminus C = A \setminus (B \cup C).$$
5. Sümmeetriline vahe avaldub sümmeetriliselt $A$ ja $B$ suhtes:
$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

## 6.7 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 6.23.** 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 $\{A_i \colon i = 1, 2, 3, \dots\}$;
- 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

$$A_1 \cup A_2 \cup \ldots \cup A_n = \{x \mid x \in A_1 \vee x \in A_2 \vee \ldots \vee x \in A_n\},$$
$$A_1 \cap A_2 \cap \ldots \cap A_n = \{x \mid x \in A_1 \wedge x \in A_2 \wedge \ldots \wedge x \in A_n\}.$$

**Näide 6.24.** 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

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \ldots = \{x \mid \text{leidub } i \geq 1 \text{ nii, et } x \in A_i\},$$
$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cap \ldots = \{x \mid \text{iga } i \geq 1 \text{ korral } x \in A_i\}.$$

Olgu nüüd $\mathcal{I}$ mingi 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 6.25.** 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 6.26.** 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 6.27.**

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 $\cup_{a\in A}\{a\} = A$.

De Morgani seadused on üldistatavad mis tahes (isegi lõpmatu) arvu hulkade jaoks. Näiteks suvalistele ühisosadele ja ühenditele üldistuvad need järgmiselt:

$$\left(\bigcup_{\alpha\in\mathcal{I}} A_\alpha\right)' = \bigcap_{\alpha\in\mathcal{I}} A'_\alpha, \qquad \left(\bigcap_{\alpha\in\mathcal{I}} A_\alpha\right)' = \bigcup_{\alpha\in\mathcal{I}} A'_\alpha.$$

## 6.8 Hulkade otsekorrutis

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 6.28.** Hulkade $A$ ja $B$ **otsekorrutiseks** (või **kartesiuse** ehk **Descartes'i korrutiseks**) nimetatakse kõikide paaride $(a,b)$ hulka, kus $a\in A$ ja $b\in B$, seejuures elementide järjekord on oluline.

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

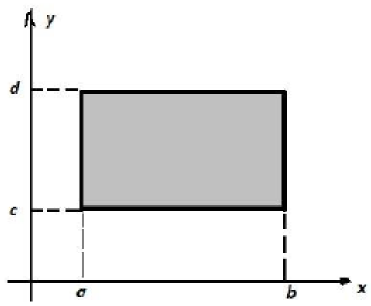
$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Öeldakse 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, s.t

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

Otsekorrutist $A \times A$ 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 6.29.** 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 6.30.** Kui $A = \{a, b, c, d, e, f, g, h\}$ ja $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$, siis otsekorrutist $A \times B = \{(a, 1), \ldots, (h, 8)\}$ võib vaadelda kui malelaua ruudustikku (males kirjutatakse lühemalt $a1, \ldots, h8$).

Peaks olema pikemata selge, et hulkade otsekorrutamine pole üldjuhul kommutatiivne, s.o 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 6.31.** *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 $w$ element hulgast $A \times C$. Peame näitama, et $w \in B \times D$. Kuna $w \in A \times C$, siis saame $w$ kirjutada kujul $(a, c)$, kus $a \in A$ ja $c \in C$ (otsekorrutise definitsiooni põhjal). Kuna element $a \in A$ ja hulk $A \subset B$, siis ka $a \in B$. Sarnaselt, kuna $c \in C$ ja $C \subset D$, siis $c \in D$. Kasutades uuesti otsekorrutise definitsiooni, võime väita, et $(a, c) \in B \times D$, mis aga tähendab seda, et $w \in B \times D$. Oleme seega näidanud, et iga hulga $A \times C$ element on ka hulga $B \times D$ element. Osahulga definitsiooni kohaselt tähendab see, et $A \times C \subset B \times D$. □

**Ülesanne 6.32.** Tõesta, et kui $A \neq \emptyset$ ja $B \neq \emptyset$, siis $A \times B = B \times A$ parajasti siis, kui $A = B$.

**Teoreem 6.33.** *Hulkade $A, B, C$ ja $D$ jaoks kehtivad järgmised võrdused:*

*1.* $A \times \emptyset = \emptyset$, $\emptyset \times A = \emptyset$*;*

*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:

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

Ülejäänud võrduste kontroll teosta iseseisvalt. □

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

$$A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \colon a_1 \in A_1, \ldots, a_n \in A_n\}.$$

Otsekorrutist $\underbrace{A \times \ldots \times A}_{n}$ 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 $A_1 \times \ldots \times A_n$ koosneb $m_1 \cdot \ldots \cdot m_n$ elemendist.

**Ülesanne 6.34.** Tõestada, et kui $A_i \neq \emptyset$ ja $B_i \neq \emptyset$ $(i = 1, \ldots, n)$, siis

1. $A_1 \times \ldots \times A_n \subset B_1 \times \ldots \times B_n$ parajasti siis, kui $A_1 \subset B_1, \ldots, A_n \subset B_n$;

2. $A_1 \times \ldots \times A_n = B_1 \times \ldots \times B_n$ parajasti siis, kui $A_1 = B_1, \ldots, A_n = B_n$.

# 7

# Arvuteooria elemente ja matemaatiline induktsioon

***

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



## 7.1 Jaguvus ja algarvud

**Definitsioon 7.1.** Öeldakse, et täisarv $a$ **jagab** täisarvu $b$ (ja tähistatakse $a \mid b$), kui leidub selline täisarv $c$, et $ac = b$.

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

**Näide 7.2.** $3 \mid 15$

Täisarvude jaguvusseosel on järgmised omadused.

**Lause 7.3.** *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 $a|b$ ja $a|c$, siis $a|(b \pm c)$*
4. *Kui $a \mid b$, siis $ac \mid bc$ iga $c \in \mathbb{Z}$ korral.*

5. *$a|1$ 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 $a \mid c$. □

**Lemma 7.4.** *Mis tahes täisarvu $a$ korral $a^2 + a \geq 0$.*

*Tõestus.* Iseseisvalt! □

**Teoreem 7.5.** *Olgu $a$ täisarv ja $b$ naturaalarv. Siis leiduvad üheselt määratud täisarvud $q$ (jagatis) ja $r$ (jääk) nii, et*

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

*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 7.4 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 7.6. Algarvuks** nimetatakse naturaalarvu $p > 1$, mille ainsad naturaalarvulised jagajad on 1 ja $p$. Naturaalarvu, mis on suurem kui 1 ja mis pole algarv, nimetatakse **kordarvuks**.

Sõnastame nüüd aritmeetika põhiteoreemi, millele tugineb suur osa naturaalarvude aritmeetikas tõestatavatest teoreemidest ja mis pärineb Eukleidese (u. 350 e.m.a.) „Elementide” IX raamatust. Teoreemi tõestuse jätame paragrahvi 7.3, sest see vajab (tugeva) matemaatilise induktsiooni meetodit.

**Teoreem 7.7** (Aritmeetika põhiteoreem). *Iga naturaalarvu $n > 1$ saab esitada algarvude korrutisena (st leiduvad $r \in \mathbb{N}$ ja algarvud $p_1, \ldots, p_r$ nii, et $n = p_1 \cdot \cdots \cdot p_r$) ning see esitus on ühene tegurite järjekorra täpsuseni.*

**Teoreem 7.8** (Eukleides). *Algarvude hulk on lõpmatu.*

*Tõestus.* Olgu algarvud tähistatud $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$. Oletame vastuväiteliselt, et leidub suurim algarv $p_n$. Vaatleme naturaalarvu $a = p_1 p_2 \ldots p_n + 1$. Et $a > 1$, siis aritmeetika põhiteoreemi põhjal leidub algarv, mis arvu $a$ jagab. Kuna oletasime, et $p_1, p_2, \ldots, p_n$ on ainsad algarvud, siis peab leiduma selline $i \in \{1, \ldots, n\}$, et $p_i \mid a$. Lause 7.3 omaduse 3 põhjal saame, et $p_i \mid a - p_1 p_2 \ldots p_n$ ehk $p_i \mid 1$, mis on vastuolus sellega, et $p_i > 1$. □

## 7.2 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 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 |
| $\vdots$ | $\vdots$ | $\vdots$ |
| $n$ | $1 + 3 + 5 + 7 + 9 + 11 + \cdots + (2n - 1) =$ | $n^2$ |
| $\vdots$ | $\vdots$ | $\vdots$ |

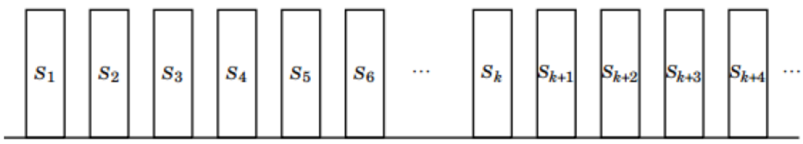
Pane tähele, et esimeses viies reas on tõesti nii, et $n$ esimese paaritu arvu summa on $n^2$. Samuti tasub märgata, et iga rea viimane liidetav on esitatav kujul $2n - 1$ (s.t, kui $n = 2$, siis teise rea viimane liidetav on $2 \cdot 2 - 1 = 3$; kui $n = 3$, kolmas paaritu arv summas on $2 \cdot 3 - 1 = 5$ jne). Aga siiski jääb õhku rippuma küsimus, et kas tõesti $1 + 3 + 5 + 7 + 9 + 11 + \ldots + (2n - 1)$ 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:

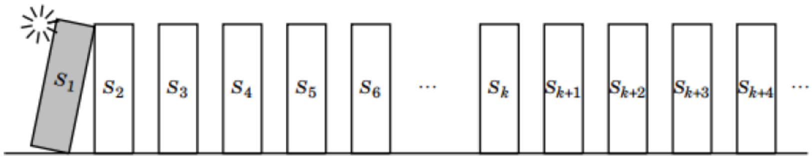
$$
\begin{aligned}
&S_1\colon 1 = 1^2\\
&S_2\colon 1+3 = 2^2\\
&S_3\colon 1+3+5 = 3^2\\
&\quad\vdots\\
&S_n\colon 1+3+5+7+\cdots+(2n-1) = n^2\\
&\quad\vdots
\end{aligned}
$$

Küsime: kas kõik need väited on tõesed?

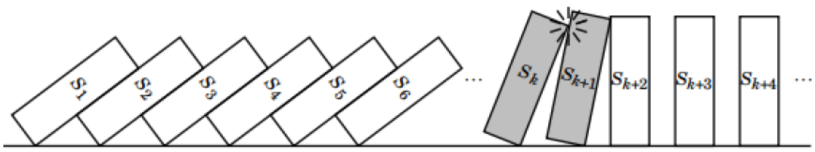
Matemaatiline induktsioon ongi mõeldud just seda tüüpi küsimuste vastamiseks, kus meil on antud terve hulk väiteid $S_1, S_2, \ldots, S_n, \ldots$ ja me peame tõestama, et kõik need väited on tõesed. Meetod on tegelikult väga lihtne ja meetodi iseloomustamiseks mõtle pikale reale doominotele, mis üksteise 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).



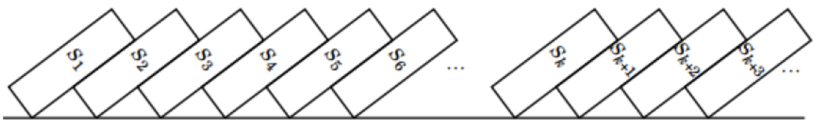

Joonis 7.1: Väited on reastatud nagu doominod.




Joonis 7.2: Oletame, et esimene väide on tõestatud (esimene doomino lükatakse ümber).




Joonis 7.3: Oletame, et doomino $S_k$ põhjustab alati doomino $S_{k+1}$ ümberkukkumise.




Joonis 7.4: Kõik doominod peavad kukkuma (ehk kõik väited peavad kehtima).

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

**Definitsioon 7.9. Matemaatilise induktsiooni meetod**. Olgu antud mingi seeria väiteid $S_1, S_2, \ldots, S_n, \ldots$. Antud seerias iga väide $S_n$ on tõene, kui

1. **Induktsiooni baas.** $S_1$ on tõene, s.t seerias esimene väide on tõene;
2. **Induktsiooni samm.** $S_k \Rightarrow S_{k+1}$, s.t oletusest, et suvaline väide $S_k$ on tõene, järeldub, et järgnev väide $S_{k+1}$ on tõene.

*Märkus.*

1. Pole oluline, et kõige esimene väide, mida kontrollitakse, vastab juhule $n = 1$. Piisab, kui väide kehtib mingi naturaalarvu korral ning üldistamine toimub sellele arvule järgnevatele arvudele.
2. Matemaatilise induktsiooniga tõestatavad valemid ja seosed kehtivad vaid naturaalarvude $n = 1, 2, 3, \ldots$ korral.
3. Matemaatilist induktsiooni saab rakendada ainult siis, kui mõlemad eeldused (induktsiooni baas ja induktsiooni samm) on rahuldatud.

**Näide 7.10.** Tõesta matemaatilise induktsiooni abil, et $n$ esimese naturaalarvu summa võrdub avaldise $\frac{n(n+1)}{2}$ väärtusega, s.o

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \quad n \geq 1.$$

*Tõestus.* Kuna valemi kehtivus sõltub naturaalarvust, saame tõestamiseks kasutame matemaatilist induktsiooni. Selleks kontrollime kõigepealt, kas valem kehtib $n = 1$ korral.

1. Induktsiooni baas. Kui $n = 1$, siis valemi vasak pool $vp = 1$ ja parem pool $pp = \frac{1(1+1)}{2} = 1$. Järelikult, $vp = pp$ ning valem kehtib, kui $n = 1$.
2. Induktsiooni samm. Eeldame, et valem kehtib $n = k$ korral, s.t $1+2+3+\cdots+k = \frac{k(k+1)}{2}$. Kontrollime, kas valemil on järgnevuse omadus, s.t kas valemi kehtivusest $k$ korral järeldub valemi kehtivus $k+1$ korral. Seega tuleb näidata, et $1+2+3+\cdots+k+k+1 = \frac{(k+1)(k+2)}{2}$. Selle võrduse tõestamiseks lähtume väite vasakust poolest ja püüame selle teisendada väite paremaks pooleks. Teisendamise käigus kasutame oma eeldust, et valem kehtib $k$ korral.

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

Seega näitasime, et esitatud valemil on järgnevuse omadus. Induktsiooni baasi ja induktsiooni sammu ühendamisest järeldub, et tõestatav valem kehtib iga naturaalarvu $n$ korral. □

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

**Näide 7.11.** Tõesta matemaatilise induktsiooni abil, et $n$ esimese paaritu naturaalarvu summa on $n^2$.

*Tõestus.*

1. Kui $n = 1$, siis valemi vasakpool $vp = 1$ ja parem pool $pp = 1^2 = 1$. Järelikult, $vp = pp$ ning valem kehtib, kui $n = 1$.

2. Eeldame, et valem kehtib $n = k$ korral, s.t $1 + 3 + 5 + \cdots + (2k - 1) = k^2$. Näitame, et sel juhul valem kehtib ka $n = k + 1$ korral, s.t näitame, et $S_k \Rightarrow S_{k+1}$.

$$\begin{aligned} vp &= \underbrace{1 + 2 + 3 + \cdots + (2k - 1)}_{eeldus} + (2(k + 1) - 1) = k^2 + (2(k + 1) - 1) \\ &= k^2 + 2k + 1 = (k + 1)^2 = pp. \end{aligned}$$

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

**Näide 7.12.** Tõesta, et kõigi naturaalarvude korral jagub avaldis $2^{2n} - 1$ kolmega.

*Tõestus.*

1. Tõestame, et tulemus kehtib $n = 1$ korral. Kuna $2^{2\cdot 1} - 1 = 4 - 1 = 3$, siis avaldis jagub kolmega $n = 1$ korral. Seega $S_1$ on tõene.

2. Eeldame, et väide kehtib $n = k$ korral, s.t $S_k = 2^{2k} - 1$ jagub kolmega. Tõestame, et väide kehtib siis ka $n = k + 1$ korral. Selleks arvutame

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

   Saadud avaldis jagub kolmega, kuna mõlemad liidetavad jaguvad kolmega (esimene liidetav $S_k$ jagub kolmega induktsiooni eelduse tõttu ja teises liikmes $2^{2k} \cdot 3$ on arv 3 kordajaks).

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

**Näide 7.13.** (Geomeetrilise jada $n$ esimese liikme summa valem.) Tõesta matemaatilise induktsiooni abil, et $a, r \in \mathbb{R}$ ja $|r| < 1$ korral

$$a + ar + ar^2 + ar^3 + \cdots + ar^n = \frac{a(1 - r^{n+1})}{1 - r}, \ n \geq 0.$$

*Tõestus.* Iseseisvalt. □

**Näide 7.14.** Tõesta, et $n \geq 1$ korral

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

*Tõestus.* Kasutame näidet 7.13 võttes seal $a = 1$ ja $r = \frac{1}{2}$. Siis

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

□

**Näide 7.15.** (Aritmeetilise jada $n$ esimese liikme summa valem). Tõesta matemaatilise induktsiooni abil, et

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

*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 7.16.** Iga naturaalarvu $n$ korral on $n^2+n+41$ algarv.

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 $n=1,2,\ldots,39$ 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.

**Näide 7.17.** Tõesta, et iga naturaalarv võrdub talle järgneva naturaalarvuga.

Alustame seekord järgnevuse omaduse (ehk induktsiooni sammu) kontrollimisega, kuna eelmises näites just selle puudumine osutus määravaks. Seega oletame, et väide on õige $n=k$ korral, s.t mingi naturaalarvu $k$ korral on see arv võrdne talle järgneva naturaalarvuga, s.t $k=k+1$. Näitame, et siis on väide õige ka $n=k+1$ korral. Selleks alustame vasakult poolelt

$$vp=\underbrace{k}_{eeldus}+1=(k+1)+1=k+2=pp,$$

kus näeme, et kasutades eeldust, saime tõese võrduse parema poolega. Seega induktsiooni samm kehtib. Kontrollime nüüd ka induktsiooni baasi, s.t püüame leida konkreetse näite mõne naturaalarvu korral, kus naturaalarv võrdub talle järgneva naturaalarvuga. Sellist näidet meil aga leida ei õnnestu, s.t meil ei õnnestu leida kahte järjestikust ja võrdset naturaalarvu. Väide on seega vale.

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

**Lause 7.18.** *Kõik hobused on ühte värvi.*

*„Tõestus“.*

1. **Induktsiooni baas**: Väide on õige $k=1$ puhul, sest üks hobune on iseendaga sama värvi.

2. **Induktsiooni samm**:

   Eeldame, et $n = k$ 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 7.19.** Kus on lause 7.18 tõestuses vigane arutlus?

## 7.3 Tugev matemaatiline induktsioon

Mõnikord võib ette tulla olukord, kus on raske otse tõestada, et väitest $S_k$ järeldub väide $S_{k+1}$. Pigem leiad, et on vajadus kasutada mõnda „madalamat“ väidet $S_i$ $(i < k)$, et näidata $S_{k+1}$ kehtivust. Sellistes olukordades on võimalik kasutada hariliku matemaatilise induktsiooni natukene muudetud varianti, mida kutsutakse tugevaks matemaatilise induktsiooni printsiibiks ja mis kõlab järgmiselt.

**Definitsioon 7.20. Tugeva matemaatilise induktsiooni meetod**. Olgu antud mingi seeria väiteid $S_1, S_2, \dots, S_n, \dots$. Antud seerias iga väide $S_n$ on tõene, kui

1. **Induktsiooni baas.** $S_1$ on tõene, s.t seerias esimene väide on tõene;

2. **Induktsiooni samm.** $S_1 \wedge S_2 \wedge \dots \wedge S_k \Rightarrow S_{k+1}$, s.t oletusest, et kõik eelnevad väited $S_1, \dots, S_k$ on tõesed, järeldub, et järgnev väide $S_{k+1}$ on tõene.

*Märkus.* Tugeva induktsiooni baasi kehtivuse kontrollimisel on mõnikord vaja tõestada lisaks esimesele väitele veel mõned järgnevad väited (vaata näiteks lause 7.25).

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 tõestamaks, 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 seda 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 7.21** (Aritmeetika põhiteoreem)**.** *Iga naturaalarvu $n > 1$ saab esitada algarvude korrutisena (st leiduvad $r \in \mathbb{N}$ ja algarvud $p_1, \ldots, p_r$ nii, et $n = p_1 \cdot \cdots \cdot p_r$) ning see esitus on ühene tegurite järjekorra täpsuseni.*

*Tõestus.* Näitame esmalt tugeva matemaatilise induktsiooniga, et iga naturaalarvu $n > 1$ saab esitada algarvude korrutisena. Arvu $n = 2$ puhul on see väide selge. 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 $d \mid n$, kusjuures $1 < d < n$. 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 $n$ saab algarvude korrutisena esitada kahel viisil:

$$n = p_1p_2 \ldots p_r = q_1q_2 \ldots q_s,$$

kus üldisust kitsendamata $r \leq s$ ja algarvud $p_i$ ja $q_j$ on mittekahanevas järjekorras, st $p_1 \leq p_2 \leq \cdots \leq p_r$ ja $q_1 \leq q_2 \leq \cdots \leq q_s$. Kuna $p_1 \mid q_1q_2 \ldots q_s$ ja $p_1$ on algarv, siis $p_1 = q_k$ mingi $k \in \{1, \ldots, s\}$ korral. Seega kehtib ka, et $p_1 \geq q_1$. Samamoodi arutledes saame, et $q_1 \geq p_1$ ning kokkuvõttes $p_1 = q_1$. Arvu $p_1$ taandades saame $p_2 \ldots p_r = q_2 \ldots q_s$. Korrates seda mõttekäiku saame $p_2 = q_2$ ja $p_3 \ldots p_r = q_3 \ldots q_s$. Kui $r < s$, siis niimoodi jätkates jõuame võrduseni $1 = q_{r+1}q_{r+2} \ldots q_s$, mis on aga võimatu, sest $q_i > 1$ iga $i \in \{1, \ldots, s\}$ korral. Seega $r = s$ ja $p_1 = q_1, \ldots, p_r = q_r$. □

**Näide 7.22.** Kastide virnadesse jagamise mäng. Oletame, et meil on ühes virnas (üksteise 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.*

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 valem on õige $n = 1$ korral.

2. Induktsiooni samm. Oletame, et väited $S_1, \dots, S_k$ on kõik tõesed mingi suvalise arvu $k$ korral. 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

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

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.

**Ülesanne 7.23.** Talunikul on üks paar vastsündinud jäneseid, isane ja emane. Ühe kuu pärast sünnist alates muutuvad jänesed paaritumisvõimeliseks ning kaks kuud pärast sündi 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?

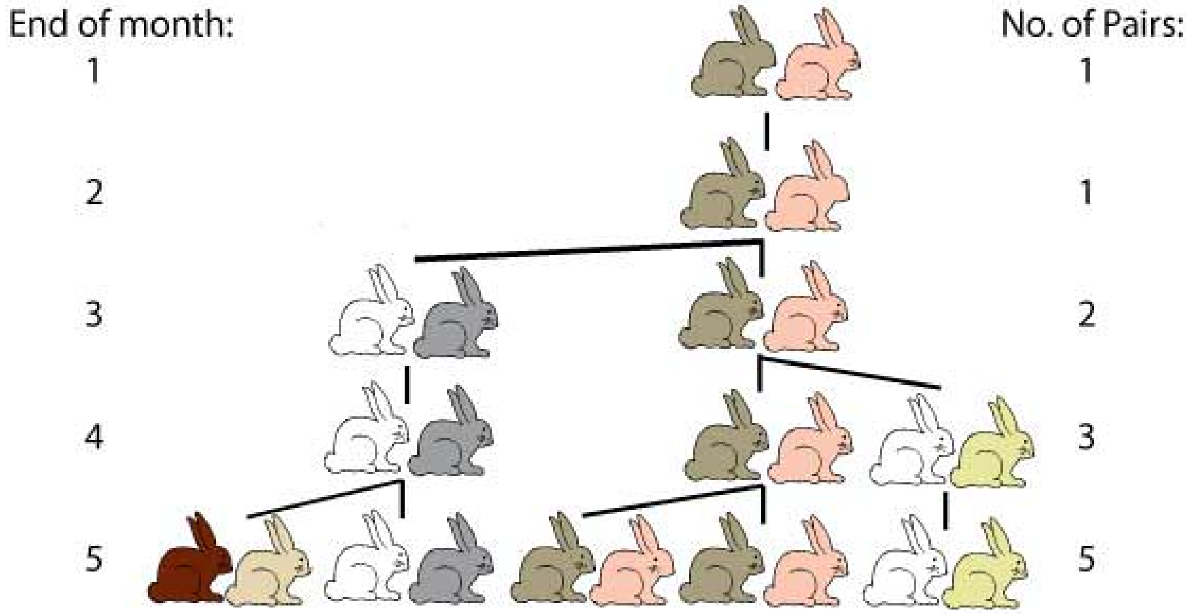
Olgu $F_n$ paaride arv $n$-ndal kuul. Siis järgmisel kuul on talunikul olemas kõik need jänesed, kes tal olid $n$-ndal kuul, uusi paare lisandub aga parajasti niipalju, kuipalju oli paare eelmisel, $(n-1)$-l kuul, sest need on järgmisel kuul kõik vähemalt kaks kuud vanad ja annavad igaüks ühe uue paari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

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

Lisaks teame, et $F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, \dots$.
Kasulik on defineerida veel $F_0 = 0$.

**Definitsioon 7.24.** 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**.

**Lause 7.25.** *Tõestada, et $F_n > 2n$ iga $n \geq 8$ korral.*




Joonis 7.5: https://learnodo-newtonic.com/wp-content/uploads/2015/09/Fibonacci-Sequence-in-the-Rabbit-Problem.jpg

*Tõestus.* Näitame selle väite kehtivust tugeva matemaatilise induktsiooni abil.

1. Induktsiooni baas. Kui $n = 8$, siis $F_8 = 21 > 2 \cdot 8 = 16$. Kui $n = 9$, siis $F_9 = 34 > 2 \cdot 9 = 18$. Seega väide kehtib, kui $n = 8$ ja $n = 9$.

2. Induktsiooni samm. Eeldame nüüd, et $F_m > 2m$ 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 $n \geq 8$.

$\square$

# 8

# Tõestamise erinevad meetodid

***

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



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 tolleaegse matemaatika. Eukleides esitas täpse ja loogiliselt terviklikku 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 postulaadi 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 eitus. Eukleidese 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 geomeetriat nimetatakse **mitteeukleidiliseks geomeetriaks**. Selle loomine näitas, et aksioome võib mõista lihtsalt kui eeldusi. Eukleidese „Elementides”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, s.t loogikareeglite abil saab tuletada ükskõik millise tõese matemaatikateoreemi. Frege süsteemi ja logitsistlikud 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**. Nimetatud 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 kasutud: reeglina piisab meile huvi pakkuvate väidete tõestamiseks siiski 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.

## 8.1 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 luiged 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.

## 8.2 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.

## 8.3 Otsene tõestus

Enamus tõestusi, millega sa siiamaani kokku puutunud oled (kui sa neid üldse näinud või teinud 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 üleüldine 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 8.1.** *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 8.2.** *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 teoreemis 8.1 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.

## 8.4 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. Kui teoreem väidab midagi kõigi reaalarvude kohta, on mõnikord abiks vaadelda kolme juhtu 1) $x < 0$, 2) $x = 0$ ja 3) $x > 0$.

**Lause 8.3.** *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. 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 $|x| = \max\{x, -x\}$. Veendu, et mõlemad definitsioonid on samaväärsed.

**Lause 8.4.** *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 $|x + y| = -(x + y) = (-x) + (-y) = |x| + |y|$.

□

## 8.5 Kontrapositiivne tõestus

Mõnikord on raske näidata otse, et väitest $P$ järeldub 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 8.5.** *Olgu $n$ täisarv. Kui $n^2$ on paaritu täisarv, siis $n$ on paaritu täisarv.*

*Tõestus.* Veendume antud lausega samaväärse lause kehtivuses: Kui $n$ on paaris täisarv, siis $n^2$ on paaris täisarv. 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. □

## 8.6 Vastuväiteline tõestus

Sageli juhtub, et otsene tõestus ei võimalda eesmärkideni jõuda kas siis detailide vähesuse tõttu või on eesmärgiks hoopis tõestada „negatiivne“ tulemus, s.t näidata, et teatud omadus ei kehti või mõnda elementi ei leidu, jne. 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. k. *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 8.6.** *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.* (vastuväiteliselt). 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 8.7.** *Naturaalarvude hulgas ei ole suurimat elementi.*

**Eeldus.** Vaadeldav hulk on naturaalarvude hulk.
**Väide.** Selles hulgas ei ole suurimat elementi.

*Tõestus.* Tõestame vastuväiteliselt. Oletame, et teoreemi väide ei pea paika ja on olemas niisugune naturaalarv $N$, et kõik ülejäänud naturaalarvud on sellest väiksemad. Vastavalt aksioomile on iga naturaalarvu $n$ korral ka $n+1$ naturaalarv. Seejuures on $n+1$ suurem kui $n$. Seega leidub ka arvu $N$ jaoks naturaalarv $N + 1$, mis on sellest suurem. See on aga vastuolus oletusega, et $N$ on suurim naturaalarv. Järelikult ei saa olla suurimat naturaalarvu. □

**Lause 8.8.** *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 $\cos y \geq 0$. □

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 $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$. Mõningase tööga peaksid sa olema võimeline tõestama, et arvud $\sqrt{7}$, $\pi$ ja $e^2$ on kõik irratsionaalsed.

**Lause 8.9.** *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 8.10.** *Kui positiivne reaalarv* $x$ *on irratsionaalarv, siis ka* $\sqrt{x}$ *on irratsionaalarv.*

*Tõestus.* Oletame vastuväiteliselt, et väide „Kui reaalarv $x$ on irratsionaalarv, siis ka $\sqrt{x}$ on irratsionaalarv“ ei kehti. Ehk oletame, 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 $x = (\sqrt{x})^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$. Saime, et $x$ on ratsionaalarv, mis on vastuolus meie oletusega, et $x$ on irratsionaalarv Järelikult peab kehtima meie esialgne väide: „Kui reaalarv $x$ on irratsionaalarv, siis ka $\sqrt{x}$ on irratsionaalarv“. □

**Teoreem 8.11.** *Kui $\alpha$ on irratsionaalarv, siis ka $3\alpha$ on irratsionaalarv.*

*Tõestus.* Viimast väidet on võimalik sõnastada eitavalt ehk soovime näidata, et $3\alpha$ ei ole ratsionaalarv. Seega, oletame vastuväiteliselt, et $3\alpha$ on tegelikult ratsionaalarv. Siis võime kirjutada $3\alpha = \frac{m}{n}$, kus $m$ ja $n$ on täisarvud ja $n \neq 0$. Jagades võrduse mõlemad pooled läbi arvuga 3, saame $\alpha = \frac{m}{3n}$, kus jällegi nii nimetaja kui ka lugeja on täisarvud. Oleme näidanud, et $\alpha$ on sellisel juhul ratsionaalarv, mis on aga vastuolus meie esialgse eeldusega, et $\alpha$ on irratsionaalarv. Seetõttu meie eeldus, et $3\alpha$ on ratsionaalarv, ei pea paika ja järelikult peab $3\alpha$ olema irratsionaalarv. □

**Näide 8.12.** Kõik positiivsed täisarvud on huvitavad. :)

*"Põhjendus".* Tõestame vastuväiteliselt ehk oletame, et leidub mittehuvitavaid arvusid. See tähendab, et mittehuvitavate arvude hulk ei ole tühi. Zermelo teoreemi (vt teoreem 11.77) põhjal teame, et siis see hulk on täielikult järjestatav ja saame leida vähima mittehuvitava positiivse täisarvu. Aga nüüd on juba päris huvitav, et mis arv see selline on!? Kõige Esimene Mittehuvitav Arv?... Huvitav-huvitav! Seega saime vastuolu. □

## 8.7 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 $(A \Rightarrow B) \land (B \Rightarrow A)$. 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 järeldub teisest. Seega, tõestamaks 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 8.13.** *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 8.13 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 8.14.** *Olgu $x$ ja $y$ reaalarvud. Siis $x^2 = y^2$ parajasti siis, kui $|x| = |y|$.*

*Tõestus.* Iseseisvalt! □

## 8.8 Mitme samaväärse tingimuse tõestamine

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

**Teoreem** (...eeldused...)**.** *Järgmised väited on samaväärsed:*

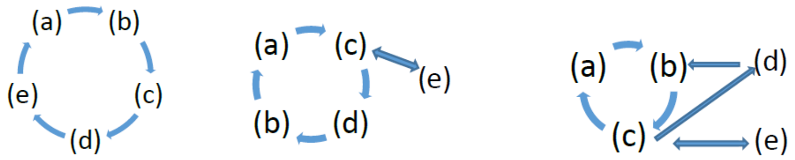
*(a)*

*(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 8.15.** *Olgu $n$ täisarv. Järgmised väited on samaväärsed:*

*(a)* $n$ *on paarisarv*

*(b)* $n+1$ *on paaritu arv*

*(c)* $n^2$ *on paarisarv*

*Tõestus.* Iseseisvalt! □

## 8.9 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.

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

**Näide 8.16.** Tõesta, et leidub täisarv, mille ruut on 81.

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

**Näide 8.17.** 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 $X \wedge \neg X$ järeldub valem $\neg(X \wedge \neg X)$. See tähendab, et valem $X \wedge \neg X$ on vajaliku omadusega. □

**Näide 8.18.** 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 $(a+b)^2 = (1+0)^2 = 1^2 = 1^2 + 0^2 = a^2 + b^2$. □

**Näide 8.19.** Koolimatemaatikast teame, et positiivsete reaalarvude $x$ ja $y$ korral kehtib üldjuhul võrratus $\frac{1}{2}(x+y) \geq \sqrt{xy}$. Kas on võimalik leida ka selliseid positiivseid reaalarve $x$ ja $y$, mille korral $\frac{1}{2}(x+y) \leq \sqrt{xy}$?

*Põhjendus.* Valime $x = y = 5$. Sellisel juhul $\frac{1}{2}(x+y) = 5 = \sqrt{xy}$. Parim, mis me siin teha saime oli kahe avaldise võrduma panemine, sest mitte ühegi arvupaari korral ei kehti ranget võrratust $\frac{1}{2}(x+y) < \sqrt{xy}$. □

**Mittekonstruktiivne 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 8.20.** *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.
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 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 eranditult väite vastaselt, s.t eeldame, et leidub kaks elementi, ütleme $x$ ja $y$, nõutud omadustega. Loogilise arutluse teel on meie eesmärgiks näidata, et siis $x = y$.

**Näide 8.21.** 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. Sajandeid tagasi püstitas Euler hüpoteesi, et kolme täieliku neljanda astme arvu summa ei ole kunagi võrdne mõne muu arvu neljanda astmega. Aga aastal 1986 (arvutite ajastul!) lükkas Noam Elkies Euleri väite ümber näidates, et

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

## 8.10 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.

| $2m^2 = n^2 \pm 1$ | $m$ | $n$ |
|---|---|---|
| $2 \cdot 1 = 1 + 1$ | 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 |

Tabelist märkame mitu toredat seost. Näiteks, igas reas liites $m$ ja $n$ väärtused, saame $m$ väärtuse järgmises reas. Proovi nüüd ise teha veel vähemalt kolm oletust erinevate seoste ja mustrite kohta samas tabelis. Oma tähelepanekute põhjal oleta järgmise kahe rea väärtused ning 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 ara 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'** 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 **Wiles** koos teiste matemaatikutega tõestas „Fermat' viimase teoreemi" näidates oletuse kehtivust kõigi täisarvuliste astendajate korral.

Veel üks kuulus hüpotees oli **Francis Guthrie** 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** ja **Wolfgang Hakeni** poolt kasutades arvutite abi. Nüüdseks on seega see hüpotees tõestatud ja temast on saanud teoreem.

## 8.11 Ümberlükkamised 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 8.22.** 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 8.23.** 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: $\exists n \in \mathbb{N}$, kui $n$ on algarv, siis $6n+1$ 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. □

**Näide 8.24.** Tõesta, et järgmine väide pole tõene:

$$\text{Kui } \alpha \text{ on reaalarv, siis } \tan^2 \alpha + 1 = \frac{1}{\cos^2 \alpha}.$$

*Põhjendus.* Kuna $\tan \alpha$ ja $\frac{1}{\cos \alpha}$ pole kumbki määratud punktis $\alpha = \frac{\pi}{2}$, siis sellel punktis neil väärtused puuduvad ja seega ei saa ka antud avaldis punktis $\frac{\pi}{2}$ kehtida. Seega, $\alpha = \frac{\pi}{2}$ on kontranäide antud avaldisele. □

## 8.12 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, s.t 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 konstanteerimine ise. Lisaks aitab tõestus süstematiseerida, ta seob erinevaid teadmisi ühtseks terviklikuks deduktiivseks arutlusahelaks, andes sel moel edasi intuitiivselt tajutud tõde. Sageli just selle funktsiooni kaudu tajumegi matemaatika ilu ja näeme seal kehtivaid seoseid.

## 8.13 Näpunäiteid tõestuse kirjutamiseks

Hea tõestuse kirjutamine eeldab harjutamist ja juhiste järgimist. Tuleb endale selgeks teha kehtivad tavad, kasutada sümboleid 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 järeldub. . . “ 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 ’järelikult’, ’niisiis’, ’seetõttu’, ’tähendab’, jt.

3. Matemaatilistes tekstides kasutatakse sõna ’mina’ asemel 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

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

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 $\blacksquare$ või täitmata $\square$ ruut.

# 9

# Funktsioonid

***

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



Funktsiooni mõiste on üks kesksetest matemaatikas. Pikka aega olid funktsioonid peamiselt matemaatilise analüüsi uurimisobjektid ja vaadeldi ainult reaal- 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 argumendi 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.

## 9.1 Funktsiooni definitsioon

**Definitsioon 9.1.** Olgu $X$ ja $Y$ hulgad. Kui on antud eeskiri, mis seab hulga $X$ igale elemendile vastavusse täpselt ühe hulga $Y$ elemendi, siis öeldakse, et on defineeritud **funktsioon** $f$, ja kirjutatakse $f\colon X \to Y$. Kui elemendile $x \in X$ seatakse vastavusse $y \in Y$, siis kasutatakse kirjutist $y = f(x)$ või $y = fx$ või $f\colon x \mapsto y$.

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

**Näide 9.2.**

1. Elementaarmatemaatikast tuntud lineaarne funktsioon $y = ax + b$ ($a \neq 0$), ruutfunktsioon $y = ax^2 + bx + c$ ($a \neq 0$) ja trigonomeetrilised funktsioonid $y = \sin x$ ning $y = \cos x$ on funktsioonid reaalarvude hulgast reaalarvude hulka: $f\colon \mathbb{R} \to \mathbb{R}$.

2. **Konstantne funktsioon** $f(x) = c$ seab igale hulga $X$ elemendile $x$ vastavusse ühe ja sama elemendi $c \in Y$.

3. **Samasus-** ehk **identsusfunktsiooniks** nimetatakse funktsiooni $f\colon X \to X$, kus $f(x) = x$ iga $x \in X$ korral.

4. Olgu funktsioon $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ antud võrdusega $f((x, y)) = (x, 0)$ iga $(x, y) \in \mathbb{R}^2$ korral, s.t $f$ 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.

5. Olgu $X \neq \emptyset$ hulk. Mis tahes bijektiivset funktsiooni $s\colon X \to X$ nimetatakse **substitutsiooniks** hulgal $X$. Olgu nüüd $X$ lõplik hulk. Käsitluse lihtsustamise huvides võime eeldada, et $X$ koosneb $n$ esimesest naturaalarvust ehk $X = \{1, 2, \ldots, n\}$. Substitutsiooni $s$ esitatakse tavaliselt tabelina:
$$s = \begin{pmatrix} 1 & 2 & \ldots & n \\ s(1) & s(2) & \ldots & s(n) \end{pmatrix},$$
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
$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

6. Funktsioon **põrand** $\lfloor x \rfloor \colon \mathbb{R} \to \mathbb{Z}$ seab reaalarvule $x$ vastavusse suurima temast väiksema või võrdse täisarvu ja funktsioon **lagi** $\lceil x \rceil \colon \mathbb{R} \to \mathbb{Z}$ seab reaalarvule $x$ vastavusse väikseima temast suurema või võrdse täisarvu, s.t

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

7. Reaalarvuliste liikmetega jada $a_1, a_2, a_3, \ldots$ on vaadeldav funktsioonina $f \colon \mathbb{N} \to \mathbb{R}$, kus igale naturaalarvule on seatud vastavusse kindel reaalarv, s.t $a_i = f(i)$ iga $i \in \mathbb{N}$ korral.

**Näide 9.3.** Olgu $U$ mingi universaalne hulk.

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

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

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

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

**Definitsioon 9.4.** Funktsioone $f \colon X \to Y$ ja $g \colon Z \to W$ nimetatakse **võrdseteks**, kui $X = Z$, $Y = W$ ja $f(x) = g(x)$ iga $x \in X (= Z)$ korral.

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

**Definitsioon 9.5.** Vaatleme funktsiooni $f \colon X \to Y$. Hulka

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

nimetatakse funktsiooni $f$ **graafikuks**.

**Ülesanne 9.6.** Olgu $f_1, f_2 \colon X \to Y$ funktsioonid. Tõesta, et $f_1 = f_2$ parajasti siis, kui $G(f_1) = G(f_2)$.

## 9.2 Hulga karakteristlik funktsioon

**Definitsioon 9.7.** Olgu $U$ universaalne hulk ja vaatleme tema osahulka $A \subset U$. Hulga $A$ **karakteristlikuks funktsiooniks** nimetatakse funktsiooni $\chi_A \colon U \to \{0, 1\}$, 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, s.t vastavus on injektiivne. Kas selline vastavus on ka sürjektiivne? Selle kontrollimiseks võtame ühe funktsiooni $\chi \colon U \to \{0, 1\}$ ja vaatleme hulka $A = \{x \in U \colon \chi(x) = 1\}$. 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 $\chi_A\colon U \to \{0,1\}$ 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, s.t

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

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

**Näide 9.8.**

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 9.9.** *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. $\chi_{A\triangle B}(x) = \chi_A(x) + \chi_B(x) - 2\chi_A(x) \cdot \chi_B(x)$;
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:

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

Siit järeldub, et

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

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 9.10.** 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 9.9 omadusi täiendi, ühisosa ja ühendi kohta saame,

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

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

**Ülesanne 9.11.** 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) $(A\cup B)\times C=(A\times C)\cup(B\times C)$.

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 $F$).

## 9.3 Hulga kujutis ja tema omadused

Olgu antud funktsioon $f\colon X \to Y$.

**Definitsioon 9.12.** Kui $x \in X$ ja $y \in Y$ on sellised, et $y = f(x)$, siis elementi $y$ nimetatakse **elemendi $x$ kujutiseks**.

Igal määramispiirkonna $X$ elemendil on parajasti üks kujutis.

**Näide 9.13.**

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

**Definitsioon 9.14.** Hulga $A \subset X$ **kujutiseks** nimetatakse hulga $Y$ osahulka $f(A)$, mis koosneb kõikide hulga $A$ elementide kujutistest, s.t

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

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

**Näide 9.15.**

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

**Teoreem 9.16.** *Olgu $f$ funktsioon hulgast $X$ hulka $Y$. 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.* Üldiselt 2. ja 5. omaduses võrdused ei kehti. Selleks vaatleme funktsiooni $f\colon X \to Y$, kus $X = Y = \mathbb{R}$ ja $f(x) = x^2$ iga $x \in \mathbb{R}$ korral. Nüüd $f(X) \neq Y$, sest

$$f(\mathbb{R}) = \{f(x)\colon x \in \mathbb{R}\} = \{x^2 \colon x \in \mathbb{R}\} = [0, \infty) \neq \mathbb{R}.$$

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 9.16 tõestus.*

1. Vastavalt hulga kujutise definitsioonile $f(\emptyset) = \{f(x) \colon x \in \emptyset\}$. 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 $f(X) = \{y \in Y \colon \exists x \ (x \in X \wedge f(x) = y)\}$. 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 kumbki võrduse pooltest on teise poole osahulk.

   (a) Olgu $y \in f(A \cup B)$. Siis hulga kujutise definitsiooni järgi eksisteerib $x \in A \cup B$, nii et $y = f(x)$. Ühendi definitsiooni järgi kehtib $x \in A$ või $x \in B$. Kui $x \in A$, siis hulga kujutise definitsiooni järgi $f(x) \in f(A)$, millest $y = f(x)$ tõttu saame $y \in f(A)$ ja lõpuks ühendi definitsiooni järgi $y \in f(A) \cup f(B)$. Kui $x \in B$, siis saame samal viisil $f(x) \in f(B)$, $y \in f(B)$ ja lõpuks $y \in f(A) \cup f(B)$. Seega kehtib mõlemal juhul $y \in f(A) \cup f(B)$, millega oleme tõestanud, et $f(A \cup B)$ on hulga $f(A) \cup f(B)$ alamhulk.

   (b) Teistpidi, olgu $y \in f(A) \cup f(B)$. Siis ühendi definitsiooni järgi kehtib $y \in f(A)$ või $y \in f(B)$. Kui $y \in f(A)$, siis hulga kujutise definitsiooni järgi leidub selline $x \in A$, et $f(x) = y$. Siis ühendi definitsioon järgi ka $x \in A \cup B$ ja järelikult hulga kujutise definitsiooni järgi $y \in f(A \cup B)$. Kui $y \in f(B)$, siis on tõestus analoogiline. Oleme jälle mõlemal juhul saanud $y \in f(A \cup B)$ ja seega on hulk $f(A) \cup f(B)$ hulga $f(A \cup B)$ osahulk.

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 9.16 omadused 4. ja 5. kehtivad ka suvalise arvu hulkade ühendi ja ühisosa korral (seejuures nende tõestused on analoogilised), s.t

$$f\Big(\bigcup_{\alpha \in \mathcal{I}} A_\alpha\Big) = \bigcup_{\alpha \in \mathcal{I}} f(A_\alpha) \quad \text{ja} \quad f\Big(\bigcap_{\alpha \in \mathcal{I}} A_\alpha\Big) \subset \bigcap_{\alpha \in \mathcal{I}} f(A_\alpha).$$

## 9.4 Hulga originaal ja tema omadused

Olgu antud funktsioon $f \colon X \to Y$.

**Definitsioon 9.17.** Kui $x \in X$ ja $y \in Y$ on sellised, et $y = f(x)$, siis elementi $x$ nimetatakse funktsiooni $f$ **elemendi** $y$ **originaaliks**.

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 $f(x) = x^2$, $f\colon \mathbb{R} \to \mathbb{R}$, siis arvu 1 originaalid on $-1$ ja 1, sest $f(-1) = 1$ ja $f(1) = 1$.

**Definitsioon 9.18.** Hulga $B \subset Y$ **originaaliks** nimetatakse hulka $f^{-1}(B)$, mis koosneb kõigist nendest hulga $X$ elementidest, mis kujutuvad hulga $B$ elemendiks, s.t

$$f^{-1}(B) = \{x \in X\colon f(x) \in B\}.$$

Tähistus $f^{-1}$ ei tähenda siin, et funktsioonil $f$ peaks leiduma pöördfunktsioon. Küll aga, kui funktsioonil $f$ leidub pöördfunktsioon, siis need mõisted – hulga $B$ originaal ja hulga $B$ kujutis pöördfunktsiooniga – ühtivad (vt paragrahv 9.10).

Teiseks, pane tähele, et $x \in f^{-1}(B) \Leftrightarrow f(x) \in B$. Seda lihtsat tähelepanekut on teinekord hea mõnes tõestuses kasutada.

**Näide 9.19.**

1. Vaatleme funktsiooni $f(x) = x^2$, $f\colon \mathbb{R} \to \mathbb{R}$. Siis $f^{-1}(\{1\}) = \{-1, 1\}$ ja $f^{-1}([-10, -5]) = \emptyset$.
2. Vaatleme funktsiooni $f(x) = 0$, $f\colon \mathbb{R} \to \mathbb{R}$. Siis $f^{-1}(\{0\}) = \mathbb{R}$.
3. Vaatleme funktsiooni $f(x) = x + 1$, $f\colon \mathbb{R} \to \mathbb{R}$. Siis $f^{-1}(\{0\}) = \{-1\}$.

**Teoreem 9.20.** *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 $f^{-1}(\emptyset) = \{x \in X\colon f(x) \in \emptyset\}$. Kuna pole selliseid hulga $X$ elemente, mis kujutuvad tühihulga elementideks, siis võrdus kehtib.
2. Vahetult originaali definitsioonist saame $f^{-1}(Y) = \{x \in X\colon f(x) \in Y\}$. 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 $x \in f^{-1}(A) \cup f^{-1}(B)$.

$$\begin{aligned} x \in f^{-1}(A \cup B) &\Leftrightarrow f(x) \in A \cup B \\ &\Leftrightarrow f(x) \in A \vee f(x) \in B \\ &\Leftrightarrow x \in f^{-1}(A) \vee x \in f^{-1}(B) \\ &\Leftrightarrow x \in f^{-1}(A) \cup f^{-1}(B). \end{aligned}$$

5. Näitame, et suvalise $x \in X$ korral kehtib $x \in f^{-1}(A \cap B)$ parajasti siis, kui $x \in f^{-1}(A) \cap f^{-1}(B)$.

$$\begin{aligned} x \in f^{-1}(A \cap B) &\Leftrightarrow f(x) \in A \cap B \\ &\Leftrightarrow f(x) \in A \wedge f(x) \in B \\ &\Leftrightarrow x \in f^{-1}(A) \wedge x \in f^{-1}(B) \\ &\Leftrightarrow x \in f^{-1}(A) \cap f^{-1}(B). \end{aligned}$$

6. Näitame, et suvalise $x \in X$ korral kehtib $x \in f^{-1}(Y \setminus B)$ parajasti siis, kui $x \in X \setminus f^{-1}(B)$.

$$\begin{aligned} x \in f^{-1}(Y \setminus B) &\Leftrightarrow f(x) \in Y \setminus B \\ &\Leftrightarrow f(x) \in Y \wedge \neg(f(x) \in B) \\ &\Leftrightarrow x \in f^{-1}(Y) \wedge \neg(x \in f^{-1}(B)) \\ &\Leftrightarrow x \in X \setminus f^{-1}(B), \end{aligned}$$

kusjuures viimane ekvivalents kehtib varem tõestatud seose $f^{-1}(Y) = X$ tõttu.

□

Teoreemi 9.20 omadused 4. ja 5. kehtivad ka suvalise arvu hulkade ühendi ja ühisosa korral (seejuures nende tõestused on analoogilised), s.t

$$f^{-1}\Big(\bigcup_{\alpha \in \mathcal{I}} A_\alpha\Big) = \bigcup_{\alpha \in \mathcal{I}} f^{-1}(A_\alpha) \quad \text{ja} \quad f^{-1}\Big(\bigcap_{\alpha \in \mathcal{I}} A_\alpha\Big) = \bigcap_{\alpha \in \mathcal{I}} f^{-1}(A_\alpha).$$

**Näide 9.21.** Hulkade kujutistel ei ole originaalide omadusega 6. analoogilist omadust. Kui näiteks $f\colon X \to Y$ 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 $f(X \setminus A) \supseteq Y \setminus f(A)$ (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.

## 9.5 Hulga kujutise originaal ja originaali kujutis

Kujutise ja originaali järjestikuse võtmise korral saame järgmised sisalduvused.

**Teoreem 9.22.** *Olgu $f: X \to Y$ funktsioon. Siis*

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.* Näidetes 9.23 ja 9.24 veendume, et üldiselt kummaski omaduses võrdused ei kehti.

*Teoreemi 9.22 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 9.20 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 saame, 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 9.23.** 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 $f(x) = x$, s.t $f(A) = A = \{1, 2, 3\}$. Teisalt,

$$f^{-1}(f(A)) = f^{-1}(A) = \{-3, -2, -1, 1, 2, 3\} \neq \{1, 2, 3\} = A.$$

**Näide 9.24.** 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

$$f(f^{-1}(B)) = f(\{-2, 0, 2\}) = \{0, 4\} \neq \{-1, 0, 4\} = B.$$

## 9.6 Funktsiooni paarsus

Olgu $X, Y \subset \mathbb{R}$ ja $f: X \to Y$ funktsioon.

**Definitsioon 9.25.** Funktsiooni $f: X \to Y$ nimetatakse **paarisfunktsiooniks**, kui iga $x \in X$ korral

1. $-x \in X$;
2. $f(-x) = f(x)$.

Paarisfunktsiooni graafik on sümmeetriline $y$-telje suhtes.

**Definitsioon 9.26.** Funktsiooni $f: X \to Y$ nimetatakse **paarituks funktsiooniks**, kui iga $x \in X$ korral

1. $-x \in X$;
2. $f(-x) = -f(x)$.

Paaritu funktsiooni graafik on sümmmeetriline koordinaatide alguspunkti suhtes.

**Näide 9.27.**

1. Kui $X = Y = \mathbb{R}$, siis funktsioonid $x$, $x^3$, $\sin x$ ja $\tan x$ on kõik paaritud fuktsioonid.
2. Kui $X = Y = \mathbb{R}$, siis funktsioonid $x^2$, $|x|$ ja $\cos x$ on kõik paaris fuktsioonid.
3. Kui $X = Y = \mathbb{R}$, siis funktsioon $x + x^2$ pole paaris ega paaritu.

## 9.7 Injektiivsed, sürjektiivsed ja bijektiivsed funktsioonid

**Definitsioon 9.28.** Funktsiooni $f\colon X \to Y$ nimetatakse

(a) **injektiivseks** ehk **üksüheseks**, 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**, kui iga $y \in Y$ jaoks leidub selline $x \in X$, et $y = f(x)$;

(c) **bijektiivseks** ehk **üksüheseks vastavuseks**, kui $f$ on nii injektiivne kui ka sürjektiive.

*Märkus.* Olgu $A\colon x_1 \neq x_2$ ja $B\colon f(x_1) \neq f(x_2)$. 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 9.29.**

1. Olgu $f(x) = x^2$. Vaatleme sellise avaldisega antud funktsiooni erinevatel hulkadel.

   Funktsioon $f\colon \mathbb{R} \to \mathbb{R}$ 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 $f\colon \mathbb{R} \to [0, \infty)$ on $x^2$ sürjektiivne, aga pole injektiivne.

   Funktsioonina $f\colon [0, \infty) \to [0, \infty)$ on $x^2$ injektiivne ja sürjektiivne, s.t on bijektiivne.

2. Funktsioon $\sin\colon \mathbb{R} \to \mathbb{R}$ ei ole injektiivne ega sürjektiivne. Miks?

   Funktsioon $\sin\colon \mathbb{R} \to [-1, 1]$ on sürjektiivne, aga pole injektiivne. Miks?

   Funktsioon $\sin\colon [-\pi/2, \pi/2] \to \mathbb{R}$ on injektiivne, aga pole sürjektiivne. Miks?

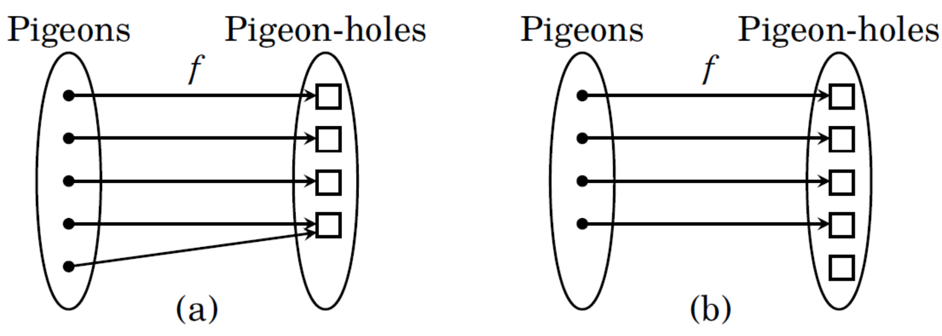
   Funktsioon $\sin\colon [-\pi/2, \pi/2] \to [-1, 1]$ on injektiivne ja sürjektiivne, s.t on bijektiivne.

3. Olgu meil kaks lõplikku hulka $X = \{x_1, \ldots, x_m\}$ ja $Y = \{y_1, \ldots, y_n\}$ , milles on vastavalt $m$ ja $n$ elementi. Uurime, millistel tingimustel leidub injektiivne/sürjektiivne/bijektiivne funktsioon $f\colon X \to Y$.
   (a) **Injektiivsus.** Kui $m > n$, siis iga funktsioon $f\colon X \to Y$ peab kujutama mingid hulga $X$ elemendid üheks ja samaks hulga $Y$ elemendiks. Järelikult ei leidu injektiivset funktsiooni $f\colon X \to Y$. 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 $Y$, s.t 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 $a_1, a_2, \ldots$ võime vaadelda kui funktsiooni $a\colon \mathbb{N} \to \mathbb{R}$. 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 $a\colon \mathbb{N} \to \mathbb{R}$ ei saa olla sürjektiivne.

**Ülesanne 9.30.** Tõesta, et funktsioon $f\colon X \to Y$ rahuldab tingimust $f(A \cap B) = f(A) \cap f(B)$ parajasti siis, kui ta on injektiivne.

## 9.8 Tuvipuuri printsiip

Olgu meil $A$ tuvide ja $B$ tuvipuuride hulk. Võime vaadelda funktsiooni $f\colon A \to B$, kus tuvi $x$ lendab puuri $f(x)$.




- Joonisel (a) on tuvisid rohkem kui tuvipuure, seega sel juhul vähemalt kaks tuvi peavad lendama ühte puuri. Teisisõnu, $f$ pole injektiivne.
- Joonisel (b) on tuvisid vähem kui tuvipuure, seega sel juhul jääb vähemalt üks puur tühjaks. Teisisõnu, $f$ pole sürjektiivne.

**Tuvipuuri printsiip 9.31.** *Olgu $A$ ja $B$ lõplikud hulgad ning $f\colon A \to B$ funktsioon.*

1. *Kui $|A| > |B|$, siis $f$ pole injektiivne.*
2. *Kui $|A| < |B|$, siis $f$ pole sürjektiivne.*

**Näide 9.32.** Tõestada, et leidub vähemalt kaks eestlast, kellel on täpselt sama palju juuksekarvu.

**Näide 9.33.** Kui valida juhuslikult kuus naturaalarvu, siis kaks neist annavad viiega jagades sama jäägi.

## 9.9 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 9.34.** Olgu $X, Y$ ja $Z$ mingid hulgad. Funktsioonide $f\colon X \to Y$ ja $g\colon Y \to Z$ **korrutiseks** ehk **kompositsiooniks** nimetatakse niisugust funktsiooni $g \circ f\colon X \to Z$, 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 kompositsioon $g \circ f$ on võimalik vaid siis, kui funktsiooni $g$ lähtehulk on sama mis funktsiooni $f$ sihthulk (vt näidet 9.35);
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, s.t üldjuhul $g \circ f \neq f \circ g$ (vt näidet 9.36). Seega, funktsioonide kompositsioon ei ole kommutatiivne.

**Näide 9.35.** 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 $g \circ f\colon \{a, b, c\} \to \{1, 2, 3\}$ 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 $\{1, 2, 3\}$. $\square$

**Näide 9.36.** 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 korrutamine on assotsiatiivne.

**Lause 9.37.** *Olgu $X, Y, Z$ ja $W$ hulgad. Kui $f\colon X \to Y$, $g\colon Y \to Z$ ja $h\colon Z \to W$, 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 muutumispiirkonnad on võrdsed, ning seejärel näitame, et iga elemendi $x$ korral nende ühisest määramispiirkonnast 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 muutumispiirkonnad on samad. Kuna $f\colon X \to Y$, $g\colon Y \to Z$ ja $h\colon Z \to W$, siis $g \circ f\colon X \to Z$ ja $h \circ g\colon Y \to W$. Seega $h \circ (g \circ f)\colon X \to W$ ja $(h \circ g) \circ f\colon X \to W$.
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 9.38.** *Kui $f\colon X \to Y$ ja $g\colon Y \to Z$ on injektiivsed, siis ka $g \circ f\colon X \to Z$ 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 9.39.** *Kui $f\colon X \to Y$ ja $g\colon Y \to Z$ on sürjektiivsed, siis ka $g \circ f\colon X \to Z$ on sürjektiivne.*

*Tõestus.* Valime vabalt $z \in Z$. Siis $g$ sürjektiivsuse tõttu leidub $y \in Y$ nii, et $g(y) = z$. Nüüd $f$ sürjektiivsuse 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 sürjektiivne. □

Lausetest 9.38 ja 9.39 järeldub vahetult järgmine tulemus.

**Järeldus 9.40.** *Kui $f\colon X \to Y$ ja $g\colon Y \to Z$ on bijektiivsed, siis ka $g \circ f\colon X \to Z$ on bijektiivne.*

**Definitsioon 9.41.** Olgu $X$ hulk. **Samasusteisenduseks** ehk **identsusteisenduseks** $I_X : X \to X$ nimetatakse funktsiooni, mis hulga $X$ igale elemendile seab vastavusse sama elemendi, s.t $I_X(x) = x$ iga $x \in X$ korral.

Kui kontekstist on selge, millise hulga samasusteisendust vaadeldakse, siis tavaliselt alumist indeksit ei lisata.

**Lause 9.42.** *Kui $f\colon X \to Y$, siis $f \circ I_X = I_Y \circ f = f$.*

*Tõestus.* Peame näitama, et kõik kolm funktsiooni on võrdsed. Tõestamisel kasutame sama taktikat kui lause 9.37 tõestamisel. Arutleme kõigepealt selle üle, et miks $f \circ I_X = f$. Kuna $f \circ I_X : X \to Y$ ja $f : X \to Y$, 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 9.43.** Olgu $f : X \to Y$ ja $g : Y \to X$ funktsioonid. Tõesta, et kui $g \circ f = I_X$, siis $f$ on injektiivne ja $g$ on sürjektiivne.

## 9.10 Pöördfunktsioon

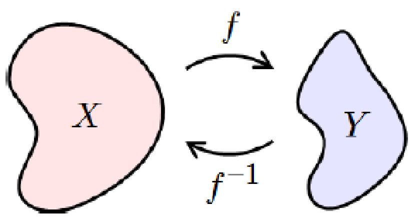
Olgu $f : X \to Y$ bijektiivne funktsioon. Kuna $f$ on sürjektiivne, siis igal elemendil hulgast $Y$ leidub originaal hulgas $X$. Veelgi enam, et $f$ on ka injektiivne funktsioon, siis igal elemendil hulgast $Y$ leidub täpselt üks originaal hulgas $X$. Järelikult, saame defineerida uue funktsiooni hulgast $Y$ hulka $X$, mis käitub vastupidiselt funktsiooni $f$ poolt antud vastavusega. See arutlus viibki meid pöördfunktsiooni mõiste juurde.

**Definitsioon 9.44.** Olgu $X$ ja $Y$ hulgad. Bijektiivse funktsiooni $f : X \to Y$ **pöördfunktsiooniks** nimetatakse funktsiooni $f^{-1} : Y \to X$, 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 $f^{-1} : Y \to X$ on funktsiooni $f : X \to Y$ 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 väljendid „funktsioon $f : X \to$

$Y$ on bijektsioon", „eksisteerib pöördfunktsioon $f^{-1}\colon Y \to X$", „funktsioon $f\colon X \to Y$ on pööratav" on kõik samaväärsed.

**Näide 9.45.** 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 9.46.** Olgu $f\colon \mathbb{Z} \to \mathbb{Z}$ 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 9.47.** *Olgu $X$ ja $Y$ hulgad ning $f\colon X \to Y$ bijektiivne funktsioon. Siis $f \circ f^{-1} = I_Y$ ja $f^{-1} \circ f = I_X$.*

*Tõestus.* Iseseisevaks tööks. □

**Teoreem 9.48.** *Kui $f\colon X \to Y$ ja $g\colon Y \to X$ 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 sürjektiivne, 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 9.37, 9.42 ja 9.47 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 9.49.** *Kui $f\colon X \to Y$ on pööratav, siis ka $f^{-1}\colon Y \to X$ on pööratav ja $(f^{-1})^{-1} = f$.*

*Tõestus.* Iseseivaks tööks. □

**Teoreem 9.50.** *Kui funktsioonidel $f\colon X \to Y$ ja $g\colon Y \to Z$ leiduvad pöördfunktsioonid, siis ka funktsioonil $g \circ f\colon X \to Z$ leidub pöördfunktsioon ja $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

*Tõestus.* Kõigepealt selleks, et funktsioonil $g \circ f\colon X \to Z$ leiduks pöördfunktsioon piisab veenduda, et ta on bijektiivne. Kuna funktsioonid $f$ ja $g$ on pööratavad, siis nad on bijektiivsed. Järelduse 9.40 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 9.48 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,

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ I \circ g^{-1} = g \circ g^{-1} = I$$

ja

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ I \circ f = f^{-1} \circ f = I.$$

□

Olgu $f\colon X \to Y$ funktsioon. Tähistust $f^{-1}$ kasutasime me eespool hulga $B \subset Y$ originaali jaoks, defineerides $f^{-1}(B) = \{x \in X\colon f(x) \in B\}$. 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.

$$\begin{aligned} &f^{-1}(B) \text{ (hulga } B \text{ kujutis funktsiooniga } f^{-1}) \\ &\qquad = \{f^{-1}(y) \in X\colon y \in B\} \\ &\qquad = \{x \in X\colon f(x) \in B\} \\ &\qquad = f^{-1}(B) \text{ (hulga } B \text{ originaal funktsiooniga } f), \end{aligned}$$

kus esimene ja viimane võrdus kehtivad vastavalt kujutise ja originaali definitsioonile ning keskmine võrdus $\{f^{-1}(y) \in X\colon y \in B\} = \{x \in X\colon f(x) \in B\}$ tänu tähistusele $f^{-1}(y) = x$ ehk $y = f(x)$.

# 10

# Hulga võimsus

***

*Matemaatik on masin, mis muudab*
*kohvi teoreemideks – P. Erdös*



## 10.1 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", s.t 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 $A = \{a_1, \ldots, a_n\}$ ja $B = \{b_1, \ldots, b_m\}$ 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 10.1.** Hulka $X$ nimetatakse **lõplikuks**, kui $X$ on tühi või leidub selline naturaalarv $n \geq 1$ nii, et $X$ saab seada üksühesesse vastavusse naturaalarvude hulga osahulgaga $\{1, \ldots, n\}$. Hulka $X$ nimetatakse **lõpmatuks**, 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 lõplikule hulgale vastavusse vaid ühe naturaalarvu – selle hulga elementide arvu.

**Definitsioon 10.2.** Lõpliku hulga $X$ **võimsuseks** nimetatakase tema elementide arvu ja tähistatakse sümboliga $|X|$.

**Lause 10.3.** *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 10.4.** Hulgad $X$ ja $Y$ on **ekvivalentsed** ehk **sama võimsusega**, kui leidub bijektsioon $f\colon X \to Y$.

Asjaolu, et hulgad $X$ ja $Y$ on ekvivalentsed tähistatakse tavaliselt kas $X \sim Y$ või $|X| = |Y|$.

Vaatame järgmiseks mõningaid üksüheseid vastavusi, mis annavad meile ekvivalentsete hulkade näiteid.

**Näide 10.5.** Kaks lõplikku hulka $X$ ja $Y$ on ekvivalentsed 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 10.6.** Olgu $X = \mathbb{N}$ ja $Y = \{x \in \mathbb{N}\colon\ x \text{ on paarisarv}\}$. Bijektsiooniks $f\colon X \to Y$ on $f(x) = 2x$ iga $x \in \mathbb{N}$ korral ning seega hulgad $X$ ja $Y$ on sama võimsusega ehk, teisisõnu, positiivseid paarisarve on täpselt sama palju kui naturaalarve.

**Näide 10.7.** Hulga $\mathbb{N}$ ja täisarvude hulga $\mathbb{Z}$ vahel saab üksühese vastavuse üles seada järgmise bijektsiooni $f\colon \mathbb{N} \to \mathbb{Z}$, 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 $f^{-1}\colon \mathbb{Z} \to \mathbb{N}$ 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 10.8.** 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 10.9.** Vahemik $(-\frac{\pi}{2}, \frac{\pi}{2})$ ja arvsirge $\mathbb{R}$ on sama võimsusega, sest funktsioon $\tan\colon (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$ on bijektsioon.

**Näide 10.10.** Reaalarvude paaride hulk $\mathbb{R}^2$ ja kompleksarvude hulk $\mathbb{C}$ on sama võimsusega, sest mõlemaid saab seada üksühesesse vastavusse tasandi kõigi punktide hulgaga. Otseselt saab selle vastavuse korraldada funktsiooniga $f\colon \mathbb{R}^2 \to \mathbb{C}$, kus $f((a, b)) = a + bi$ iga $(a, b) \in \mathbb{R}^2$, kus $i^2 = -1$.

Järgnevas loetleme üles olulisemad hulkade evivalentsuse seosed.

**Lause 10.11.** *Olgu $A, B$ ja $C$ hulgad. Siis*

1. *$A \sim A$;*
2. *Kui $A \sim B$, siis $B \sim A$;*
3. *Kui $A \sim B$ ja $B \sim C$, siis $A \sim C$.*

*Tõestus.*

1. Hulgal $A$ defineeritud samasusteisendus $I_A$ seab hulga $A$ üksühesesse vastavusse iseendaga;
2. Kui $A \sim B$, siis leidub bijektsioon $f\colon A \to B$. Funktsiooni $f$ pöördfunktsioon $f^{-1}\colon B \to A$ on siis samuti bijektsioon (kontrolli seda!);
3. Kui $A \sim B$ ja $B \sim C$, siis leiduvad bijektsioonid $f\colon A \to B$ ja $g\colon B \to C$. Nende kompositsioon $g \circ f\colon A \to C$ on siis samuti bijektsioon (miks?).

$\square$

## 10.2 Loenduvad hulgad

**Definitsioon 10.12.** Hulka $X$ nimetatakse **loenduvaks**, kui leidub bijektsioon hulga $X$ ja naturaalarvude hulga $\mathbb{N}$ vahel.

Seega loenduvad on parajasti need hulgad $X$, mida saab esitada kujul $X = \{x_1, x_2, \ldots, \}$. Tõestame selle väite allpool (vt lause 10.14), esialgu aga vaatame näiteid loenduvatest hulkadest.

**Näide 10.13.**

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 $\mathbb{Z}$.

   Intuitiivselt 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 lõpmatu 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 10.14.** *Hulk $X$ on loenduv parajasti siis, kui hulga $X$ elemendid saab esitada paarikaupa erinevate elementide lõpmatu jadana: $X = \{x_1, x_2, \ldots\}$.*

*Tõestus.* Kui hulk $X$ on loenduv, siis leidub paaride hulk $\{(1, x_1), (2, x_2), (3, x_3), \ldots\}$, mis seab hulgad $\mathbb{N}$ ja $X$ üksühesesse vastavusse. Selles paaride hulgas esineb iga naturaalarv täpselt ühe korra paari esimese komponendina ja hulga $X$ iga element täpselt ühe korra paari teise komponendina. Kui vaatleme paaride teistest komponentidest koostatud jada $\{x_1, x_2, \ldots\}$, siis selle jada elemendid on paarikaupa erinevad ja kehtib võrdus $X = \{x_1, x_2, \ldots\}$. Kui hulk $X$ on esitatud kujul $X = \{x_1, x_2, \ldots\}$, kus lõpmatu jada $\{x_1, x_2, \ldots\}$ on paarikaupa erinevate liikmetega, siis paaride hulk $\{(1, x_1), (2, x_2), (3, x_3), \ldots\}$ on üksühene vastavus $\mathbb{N}$ ja $X$ vahel (kontrollida!). $\square$

**Teoreem 10.15.** *Iga lõpmatu hulk sisaldab loenduva 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 10.16.** *Loenduva hulga iga lõpmatu osahulk on loenduv.*

*Tõestus.* Olgu $X$ loenduv hulk ja $Y$ tema lõpmatu osahulk. Lause 10.14 põhjal saame hulga $X$ elemendid esitada paarikaupa erinevate elementidega lõpmatu jadana: $X = \{x_1, x_2, \dots\}$. Kui jätame sellest jadast välja need liikmed, mis hulka $Y$ ei kuulu, siis saame lõpmatu osajada, mille elementide hulk on $X = \{x_{i_1}, x_{i_2}, \dots\}$. Jada liikmed $x_{i_j}$ on paarikaupa erinevad, sest see jada saadi erinevate liikmetega jadast elemente välja jättes. Lause 10.14 põhjal on hulk $Y$ loenduv. □

Teoreeme 10.15 ja 10.16 on loomulik mõista nii, et loenduv võimsus on vähim lõpmatu võimsus.

**Näide 10.17.** Naturaal-, täis- ja ratsionaalarvude hulga kõik lõpmatud osahulgad on loenduvad.

Järgmiseks teeme kindlaks rea loenduvuse omadusi, mis on seotud ühendi ja otsekorrutisega.

**Teoreem 10.18.**

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 otsekorrutis on loenduv.*
7. *Lõpliku arvu loenduvate hulkade otsekorrutis on loenduv.*

*Tõestus.* Tõestame 5. väite, ülejäänud väidete tõestused jäävad iseseisvaks tööks.
Üldisust kitsendamata võime eeldada, et hulgad $A_i$ on paarikaupa mittelõikuvad. Olgu

$$\begin{aligned} A_1 &= \{a_{11}, a_{12}, \dots, a_{1n}, \dots\} \\ A_2 &= \{a_{21}, a_{22}, \dots, a_{2n}, \dots\} \\ A_3 &= \{a_{31}, a_{32}, \dots, a_{3n}, \dots\} \\ &\dots \end{aligned}$$

Siis võime kirjutada, et $\bigcup_{i=1}^{\infty} A_i = \{a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \dots\}$ ehk $\bigcup_{i=1}^{\infty} A_i$ on loenduv. □

*Märkus.* Nii teoreemi 10.15 kui ka teoreemi 10.18 omaduse 5 tõestus sisaldab ilmutamata kujul valikuaksioomi kasutamist, mille kohta saab rohkem lugeda paragrahvist 11.9.

**Näide 10.19.** 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 $f\colon \mathbb{Q} \to A \subset \mathbb{Z} \times \mathbb{N}$, 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 10.18 seitsmenda väite põhjal $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N}$. Teisalt, et loenduva hulga lõpmatu osahulk on loenduv, siis ka $A \sim \mathbb{N}$. Seega oleme saanud, 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 määrang lõikavad 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 10.20.**

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.

## 10.3 Cantor–Bernsteini teoreem

**Definitsioon 10.21.** Ütleme, et hulga $A$ **võimsus ei ületa** hulga $B$ võimsust, kui leidub injektsioon $f\colon A \to B$.

Asjaolu, et hulga $A$ võimsus ei ületa hulga $B$ võimsust tähistatakse tavaliselt nii $|A| \leq |B|$.

Märgime, et injektsiooni $f\colon A \to B$ leidumine on samaväärne sellega, et leidub bijektsioon $f\colon A \to f(A) \subset B$.

**Näide 10.22.**

1. Vaatleme lõplikku hulka $A = \{a_1, \dots, a_n\}$. Funktsioon $f\colon A \to \mathbb{N}$, kus $f(a_k) = k$, $k = 1, \dots, n$, on injektsioon, seega hulga $A$ võimsus ei ületa hulga $\mathbb{N}$ võimsust.

2. Kui $A \subset B$, siis funktsioon $f\colon A \to B$, kus $f(a) = a$, $a \in A$, on injektsioon. 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 [4].

**Teoreem 10.23** (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 $f\colon A \to B$ ja $g\colon B \to A$, siis hulgad $A$ ja $B$ on sama võimsusega. Või veel lühemalt, kui $|A| \leq |B|$ ja $|B| \leq |A|$, siis $|A| = |B|$.

**Näide 10.24.** Tõesta, et $(0, 1) \sim (0, 1]$.

*Lahendus 1.* Kõigepealt märgime, et ei ole üldse ilmne, kuidas konstrueerida bijektsiooni hulkade $(0, 1)$ ja $(0, 1]$ vahel. Tänu Cantor–Bernsteini teoreemile piisab meil konstrueerida ainult kaks injektsiooni, mis on palju lihtsam ülesanne.
Esiteks, injektsiooniks hulgast $(0, 1)$ hulka $(0, 1]$ sobib $f(x) = x$ iga $x \in (0, 1)$ korral, sest $(0, 1) \subset (0, 1]$.
Teistpidi, injektsiooniks 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 injektsioonid $f\colon (0, 1) \to (0, 1]$ ja $g\colon (0, 1] \to (0, 1)$, siis teoreemi 10.23 põhjal $(0, 1) \sim (0, 1]$. □

Esitame nüüd ka alternatiivse lahenduse, kus konstrueerime konkreetse bijektsiooni $(0, 1)$ ja $(0, 1]$ vahel.

*Lahendus 2.* Olgu

$$A = \{\frac{1}{n+1} : n \in \mathbb{N}\} \subset (0, 1) \quad \text{ja} \quad B = \{\frac{1}{n} : n \in \mathbb{N}\} \subset (0, 1].$$

Siis $A \sim B$, sest $f\colon A \to B$, kus $f(\frac{1}{n}) = \frac{1}{n-1}$, $n \geq 2$, on bijektsioon (kontrolli!). Otsitavaks bijektsiooniks sobib (kontrolli!) $g\colon (0, 1) \to (0, 1]$, kus

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

□

**Ülesanne 10.25.** Tõesta, et $(0, 1) \sim [0, 2)$ ja $(0, 1) \sim [0, 3]$.

## 10.4 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 10.26.** *Vahemik* $(0,1)$ *ja naturaalarvude hulk* $\mathbb{N}$ *ei ole ekvivalentsed.*

*Tõestus.* Oletame vastuväiteliselt, et hulk $(0,1)$ on loenduv, s.t hulkade $\mathbb{N}$ ja $(0,1)$ vahel leidub üksühene vastavus. Sellisel juhul peab vahemik $(0,1)$ esituma loenduva hulgana: $(0,1) = \{x_1, x_2, x_3, \dots\}$. Kirjutame välja selle hulga kõik arvud järgmiselt:

$$\begin{aligned}
x_1 &= 0, a_{11}a_{12}a_{13}\dots a_{1j}\dots \\
x_2 &= 0, a_{21}a_{22}a_{23}\dots a_{2j}\dots \\
x_3 &= 0, a_{31}a_{32}a_{33}\dots a_{3j}\dots \\
&\dots\dots,
\end{aligned}$$

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 10.27.**

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 10.8 ja teine väide näidetest 10.8 ja 10.9, sest $(0,1) \sim (-\frac{\pi}{2}, \frac{\pi}{2}) \sim \mathbb{R}$. □

Seega leidub lõpmatuid hulki, mis ei ole võrdse võimsusega.

**Definitsioon 10.28.** Hulka, mis on ekvivalentne hulgaga $\mathbb{R}$ nimetatakse **kontiinumi võimsusega** hulgaks.

Niisiis, hulk $\mathbb{R}$ ja kõik vahemikud $(a,b)$ ning ka lõigud $[a,b]$, kus $a < b$, on kontiinumi võimsusega.

Kuna $\mathbb{Q}$ ja $\mathbb{I}$ on vastavalt kõigi ratsionaal- ja irratsionaalarvude hulgad, siis $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$. Et $\mathbb{Q}$ on loenduv hulk, siis $\mathbb{I}$ ei saa olla loenduv, sest vastasel juhul (vt teoreem 10.18, väide 2) oleks ka $\mathbb{R}$ loenduv hulk. Järelikult, irratsionaalarvude hulk $\mathbb{I}$ on kontiinumi võimsusega hulk.

Et iga lõpmatu hulk sisaldab loenduva osahulga (vt teoreem 10.15), siis võib arvata, et loenduva hulga võimsus on kõige väiksem lõpmatutest võimsustest. Sõnastame võimsuste võrdlemise printsiibi.

**Definitsioon 10.29.** 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 hulga $B$ võimsus (või hulga $B$ võimsus on suurem kui hulga $A$ võimsus).

Teisisõnu, kui leidub injektsioon $f\colon A \to B$ ja ei leidu sürjektsiooni $g\colon A \to B$, 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 9.29), kus ütlesime, et jada $a\colon \mathbb{N} \to \mathbb{R}$ ei saa olla sürjektiivne. Vaatleme hulka $a(\mathbb{N})$. Ta saab olla kas lõplik või loenduv olenevalt sellest, kas jadas $a(1), a(2), \ldots$ 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 11.49). Hulga $A$ võimsust tähistatakse sümboliga $|A|$ või card $A$ ning nimetatakse **kardinaalarvuks**. Kui $A = \{a_1, \ldots, a_n\}$, siis kirjutame $|A| = n$, samuti $|\emptyset| = 0$. Loenduva hulga võimsust tähistatakse sümboliga $\aleph_0$ (loe alef-null) ehk $|\mathbb{N}| = \aleph_0$. Kontiimnumi võimsusega hulki tähistatakse sümboliga $c$ ehk $|\mathbb{R}| = c$. Kokkuvõtvalt teame, et iga $n \in \mathbb{N}$ korral

$$n < \aleph_0 < c.$$

Nüüd tekib aga küsimus, et kas on olemas veel suurema võimsusega hulki, s.t kas on ka kontiinumist suurema võimsusega hulki? Jaatava vastuse viimasele küsimusele annab järgnev teoreem.

**Teoreem 10.30** (Cantori teoreem)**.** *Iga hulga $A$ kõigi osahulkade hulga $\mathcal{P}(A)$ võimsus on suurem kui hulga $A$ võimsus, s.t $|A| < |\mathcal{P}(A)|$.*

*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 kehtib kindlasti.
Esiteks, $|A| \leq |\mathcal{P}(A)|$, sest funktsioon $f\colon A \to \mathcal{P}(A)$, kus $f(a) = \{a\}$ iga $a \in A$ korral, on injektiivne.
Seose $|A| \neq |\mathcal{P}(A)|$ nägemiseks, oletame vastuväiteliselt, et $|A| = |\mathcal{P}(A)|$. Siis leidub bijektsioon $g\colon A \to \mathcal{P}(A)$. Olgu $g(a) = A_a \subset A$, $a \in A$. Seejuures kas $a \in A_a$ või $a \notin A_a$. Tähistame $A^* = \{a \in A\colon a \notin A_a\}$ ja tähistame veel $a^* = g^{-1}(A^*)$, siis $g(a^*) = A^*$. Kuna $g(a^*) = A_{a^*}$, siis $A^* = A_{a^*}$. Kas $a^* \in A_{a^*}$?

1. Kui oletada, et $a^* \in A_{a^*}$, siis saame hulga $A^*$ definitsiooni põhjal, et $a^* \notin A^*$ ehk $a^* \notin A_{a^*}$, vastuolu.

2. Kui aga oletada, et $a^* \notin A_{a^*}$, siis saame hulga $A^*$ definitsiooni põhjal, et $a^* \in A^*$ ehk $a^* \in A_{a^*}$, vastuolu.

Seega viivad mõlemad võimalused vastuoluni, mis näitab, et bijektsiooni $g\colon A \to \mathcal{P}(A)$ ei eksisteeri.

□

Järelikult on olemas hulk, mille võimsus on suurem kontiinumi võimsusest – näiteks hulga $\mathbb{R}$ kõigi osahulkade hulk $X = \mathcal{P}(\mathbb{R})$. Veel suurema võimsusega on hulk $\mathcal{P}(X)$ jne. 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.

Hulga võimsuse mõiste võttis kasutusele hulgateooria rajaja saksa matemaatik Georg Cantor 1878. aastal. Samal ajal püstitas ta ka nn **kontiinumi hüpoteesi**, mis ütleb, et ei leidu hulka, mis oleks võimsam kui $\mathbb{N}$, kuid vähem võimas kui $\mathbb{R}$. Tegemist ei ole teoreemiga. 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 $\aleph_0 < \aleph_1$ vahel), ja teist, milles kehtib kontiinumi hüpoteesi eitus (ehk leiduvad vahepealsed võimsused $\aleph_0 < \ldots < \aleph_1$).

Eeldusel, et kontiinuumi hüpotees on tõene, defineeritakse $\aleph_1$ hulga $\mathbb{R}$ võimsusena. See kardinaalarv on võimsuselt järgmine $\aleph_0$ järel. Sel juhul kehtib:

$$c = 2^{\aleph_0} = \aleph_1.$$

# 11

# Seosed

***

*Matemaatikud ei uuri mitte objekte*
*vaid nendevahelisi seoseid –*
*H. Poincaré*



Asjade ja sündmustega, mis on omavahel seoses, puutume me igapäevaelus tihti kokku. Näiteks on igal inimesel oma telefoni number, 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, täisarvu ja temale järgneva täisarvu vahel või kõrgemas matemaatikas argumendi väärtuse $x$ ja vastava funktsiooni 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.

## 11.1 Seose mõiste

**Definitsioon 11.1.** Olgu $A$ ja $B$ hulgad. **Seoseks** ehk **relatsiooniks** 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 $aRb$. Mõnikord öeldakse osahulga $R$ kohta, et see on seose graafik.

Seost $R = A \times B$ nimetatakse **universaalseks seoseks** ja seost $\emptyset \subset A \times B$ **tühiseoseks**.

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 $A_1, \ldots, A_n$ vahel nimetatakse vastavalt otsekorrutise $A_1 \times \ldots \times A_n$ 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: $=, <, \geq, \subset, \|$, jne. Tegelikkuses me mõtlemegi 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 nimekiri kõikidest objektide paaridest, mis antud seost rahuldavad. Vaatame nüüd näiteid, mis aitaksid sellest definitsioonist paremini aru saada.

**Näide 11.2.** 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 $R_2 = \{(2, 2), (2, 4), (2, 6), (3, 3), (3, 6)\}$.

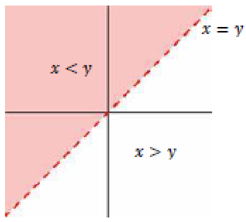
**Näide 11.3.** Olgu hulgaks $A$ kõigi naturaalarvude hulk $\mathbb{N}$ ning seoseks $R$ osahulk hulgas $\mathbb{N} \times \mathbb{N}$, mis koosneb kõikidest paaridest $(a, b)$, mille korral arv $a$ on arvu $b$ jagaja. Seega $R = \{(a, b) \colon a, b \in \mathbb{N}, a \mid b\}$. Seda seost $R$ nimetatakse **jaguvusseoseks**.

**Näide 11.4.** Olgu $A$ mis tahes hulk ja $R = \{(a, a) \colon a \in A\}$. 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 11.5.** 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 $A$.

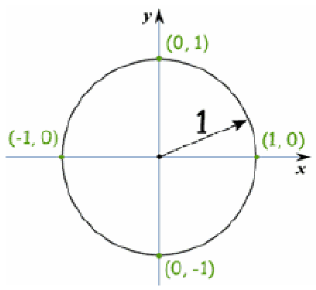
Kuidas kirjeldada antud seost siis, kui hulgaks $A$ oleks kõigi täisarvude hulk $\mathbb{Z}$? Paljud tuttavad matemaatilised seosed on esitatavad järjestatud paaride hulgana. Seost $<$ („väiksem”) täisarvudel võib esitada hulgana $R = \{(x, y) \colon x, y \in \mathbb{Z} \wedge y - x \in \mathbb{N}\}$, 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 $R = \{(x, y) \colon x < y\}$ reaalarvude hulgal? Antud juhul väljendab seos punktipaaride hulka tasandil ja see hulk on kujutatud järgmisel joonisel.




**Näide 11.6.** 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 11.7.** Olgu $A = B = \mathbb{R}$, $R = \{(x, y) \colon x^2 + y^2 = 1\}$. Seos $R$ on ringjoonel paiknevate punktipaaride hulk tasandil (ringjoon on keskpunktiga koordinaatide alguspunktis ning raadiusega 1).




**Näide 11.8.** 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 11.9.** Olgu $M$ maakeral elavate inimeste hulk. Siis $aRb$, kui inimestel $a$ ja $b$ on ühised vanemad.

**Näide 11.10. Funktsioon kui seose erijuht.** Olgu $f\colon X \to Y$ funktsioon. Defineerime $R = G(f)$, s.t $xRy$ parajasti siis, kui $(x, y) \in G(f) = \{(x, f(x))\colon x \in X\}$. 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 11.11.** Olgu $X$ ja $Y$ hulgad. Seost $R \subset X \times Y$ nimetatakse **funktsiooniks**, 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 mõtlemegi funktsioonidest kui kindlatest seostest. Anname uuest funktsiooni definitsioonist lähtuvalt ka injektiivsuse ja sürjektiivsuse uued definitsioonid.

**Definitsioon 11.12.** Olgu $R \subset X \times Y$ funktsioon. Siis $R$ on

1. **injektiivne**, 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**, kui iga $y \in Y$ korral leidub $x \in X$ nii, et $(x, y) \in R$.

**Ülesanne 11.13.** Olgu täisarvude hulgal $\mathbb{Z}$ antud järgmised seosed:

$$\begin{aligned} R_1 &= \{(a, b)\colon a \leq b\}, & R_4 &= \{(a, b)\colon a = b\}, \\ R_2 &= \{(a, b)\colon a > b\}, & R_5 &= \{(a, b)\colon a = b + 1\}, \\ R_3 &= \{(a, b)\colon a = b \vee a = -b\}, & R_6 &= \{(a, b)\colon a + b \leq 3\}. \end{aligned}$$

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 11.14.** 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 $2^{3^2} = 2^9 = 512$ seost. □

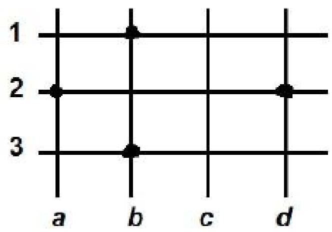
## 11.2 Seose esitusviise

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 11.2). Seost võib kujutada ka tabelina. Seos $R_1$ näites 11.2 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.



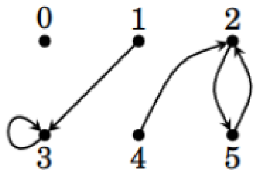

3. **Maatriksesitus**. Olgu $A = \{a_1, \ldots, a_n\}$ ja $B = \{b_1, \ldots, b_m\}$ ning $R$ seos hulkade $A$ ja $B$ vahel. Seame seosele $R$ vastavusse maatriksi $M_R = (m_{ij})$, kus $m_{ij} = 1$, kui $(a_i, b_j) \in R$ ja $m_{ij} = 0$, kui $(a_i, b_j) \notin R$, kus $i = 1, \ldots, n$ ja $j = 1, \ldots, m$.

   Näiteks, olgu $A = \{a, b, c, d\}$ ja $B = \{1, 2, 3\}$ ning $R = \{(a, 2), (b, 1), (b, 3), (d, 2)\}$. Siis

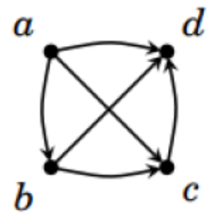
$$M_R = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

   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.

## 11.3 Seose omadused

Järgnevalt tutvustame seoste kirjeldamiseks ning klassifitseerimiseks vajaminevat sõnavara.

**Definitsioon 11.15.** Seost $R$ hulgal $A$ nimetatakse

(a) **refleksiivseks**, kui iga $a \in A$ korral $(a, a) \in R$;

(b) **irrefleksiivseks**, kui iga $a \in A$ korral $(a, a) \notin R$;

(c) **sümmeetriliseks**, kui iga $a, b \in A$ korral, kui $(a, b) \in R$, siis $(b, a) \in R$;

(d) **antisümmeetriliseks**, kui iga $a, b \in A$ korral kui $(a, b) \in R$ ja $(b, a) \in R$, siis $a = b$;

(e) **transitiivseks**, kui iga $a, b, c \in A$ korral, kui $(a, b) \in R$ ja $(b, c) \in R$, siis $(a, c) \in R$.

**Näide 11.16.** 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 11.17.** Kas jaguvusseos naturaalarvude hulgal on refleksiivne? Sümmeetriline? Antisümmeetriline?

*Lahendus.* Kuna $a|a$ mis tahes naturaalarvu korral, siis on jaguvusseos refleksiivne. (Kui me asendaksime naturaalarvude hulga täisarvude hulgaga, siis see seos enam refleksiivne ei oleks, sest nulli ei saa nulliga jagada.) Jaguvusseos naturaalarvude hulgal ei ole sümmeetriline, sest $1 \mid 2$, aga $2 \nmid 1$. Jaguvusseos naturaalarvude hulgal on aga antisümmeetriline, sest iga elemendi $a, b \in \mathbb{N}$ korral, kui $a \mid b$ ja $b \mid a$, siis $a = b$. $\square$

**Ülesanne 11.18.** Tõesta, et kui seos on sümmeetriline ja antisümmeetriline, siis ta on transitiivne.

**Näide 11.19.** Seos $<$ („väiksem“) reaalarvude hulgal on irrefleksiivne, antisümmeetriline ja transitiivne. Seos $\leq$ hulgal $\mathbb{R}$ on refleksiivne, antisümmetriline ja transitiivne.

**Näide 11.20.** Sirgete paralleelsuse seos $s \parallel t$ on sümmeetriline ja transitiivne, kuid ei ole refleksiivne, sest sirge ei saa olla iseendaga paralleelne (miks?). Sirgete paralleelsuse seos on samuti irrefleksiivne. Muid ülalnimetatud omadusi sellel seosel ei ole. Ent sirgete samasihilisus on sümmeetriline, transitiivne ja ka refleksiivne.
Sirgete ristioleku seos $s \perp t$ on irrefleksiivne, sümmeetriline, aga ei ole transitiivne.

**Näide 11.21.** Vaatleme hulga $E$ kõikide osahulkade hulka $X = \mathcal{P}(E)$ ja sisalduvuse seost $\subset$ hulgal $X$. See seos on refleksiivne, antisümmetriline ja transitiivne.

**Näide 11.22.** Olgu $A = \{a, b, c, d\}$ ja $R = \{(a, a), (a, b), (b, a), (b, c)\}$. Seosel $R$ pole ühtki varem nimetatud omadustest.

**Ülesanne 11.23.** Olgu $A$ hulk. Millised omadused on universaalsel seosel $R = A \times A$ ja tühiseosel $S = \emptyset$?

**Ülesanne 11.24.** Millised ülal nimetatud omadused on võrdusseosel?

**Ülesanne 11.25.** Too näide seosest, mis on sümmeetriline ja transitiivne, aga pole refleksiivne.

## 11.4 Pöördseos

**Definitsioon 11.26.** Seose $R \subset A \times B$ **pöördseoseks** nimetatakse seost $R^{-1} \subset B \times A$, mis määratakse samaväärsusega $bR^{-1}a \Leftrightarrow aRb$ ehk $R^{-1} = \{(b, a) \colon (a, b) \in R\}$.

Ülemine indeks „$-1$“ on siin ainult mugav ja kokkulepitud tähistus. See ei tähenda seose astmesse võtmist ega ka jagamist (mõlemad sellised tehted oleksid siinkohal absurdsed).

Igal seosel on olemas pöördseos. Kui $R$ on seos hulgal $A$, siis on seda ka $R^{-1}$. On ka lihtne näha, et $(R^{-1})^{-1} = R$, s.t pöördseose pöördseos ühtib esialgse seosega (Kontrolli!).

**Näide 11.27.** Kui $R = \{(1,5),(2,6),(3,7),(3,8)\}$, siis $R^{-1} = \{(5,1),(6,2),(7,3),(8,3)\}$.

**Näide 11.28.** Olgu $A = B = \mathbb{R}$ ja $R$ reaalarvudel defineeritud range järjestuse seos $<$, s.o $R = \{(x,y)\colon x < y\}$. Siis $R^{-1} = \{(y,x)\colon (x,y) \in R\} = \{(y,x)\colon y > x\}$, s.t seose $<$ pöördseos on $>$.

**Näide 11.29.** Olgu $A = B = \mathbb{R}$ ja $I$ reaalarvudel defineeritud võrdusseos ehk **ühikseos**, s.o $I = \{(x,y)\colon x = y\}$. Siis $I^{-1} = \{(y,x)\colon (x,y) \in I\} = \{(y,x)\colon y = x\}$, s.t võrdusseose pöördseos on ta ise.

**Lause 11.30.** *Kui seos $R$ on refleksiivne, transitiivne, sümmeetriline või antisümmeetriline, siis ka tema pöördseos $R^{-1}$ on vastava omadusega*

*Tõestus.* Iseseisvalt! □

**Ülesanne 11.31.** Näita, et seos $R$ hulgal $A$ on sümmeetriline siis ja ainult siis, kui $R = R^{-1}$.

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 $R^{-1} = \{(y,x)\colon (x,y) \in R\} \subset Y \times X$. 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 11.32.** *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.*

## 11.5 Ekvivalentsusseos

Olgu $A$ suvaline mittetühi hulk.

**Definitsioon 11.33.** Seost $R$ hulgal $A$ nimetatakse **ekvivalentsusseoseks**, kui ta on

(a) refleksiivne, s.t kui $aRa$ iga $a \in A$ korral;

(b) sümmeetriline, s.t kui $aRb$, siis $bRa$;

(c) transitiivne, s.t 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 ekvivalentsiseost kirjutades ka $a \sim b$.

**Näide 11.34.** Võrdsusseos $aRb \Leftrightarrow a = b$ on ilmselt ekvivalentsuseos suvalisel hulgal $A$. Tegemist on ühikseosega $R_A = I = \{(a, a)\colon a \in A\}$, mida mõnikord nimetatakse ka hulga $A^2$ diagonaaliks. Ühikseos ehk võrdusseos 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 11.35.** Kujundite kongruentsus nt planimeetrias on ekvivalentsuseos 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 11.36.** Sirgete samasihilisus ja vektorite kollineaarsus ning komplanaarsus on ekvivalentsuseosed.

**Näide 11.37.** Kongruentsiseos täisarvude hulgal $\mathbb{Z}$ on samuti ekvivalentsusseos. Olgu $m > 0$ 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 11.38.** Näita, et kui ekvivalentsusseos on antisümmeetriline, siis on ta võrdus ehk ühikseos.

## 11.6 Klassijaotus

Iga ekvivalentsuseose $R \subset A \times A$ abil saame hulga $A$ jaotada nn ekvivalentsiklassideks.

**Definitsioon 11.39. Ekvivalentsiklassiks** 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 $a$, s.t elementidest, mis on ekvivalentsed elemendiga $a$: $[a]_R = \{x\colon x \in A \text{ ja } aRx\}$.

Niisiis, $x \in [a]_R$ tähendab seda, et $aRx$ ja seose $R$ sümmetrilisuse tõttu ka seda, et $xRa$. Refleksiivsuse tõttu $a \in [a]_R$.

Ekvivalentsiklasside hulk on teatud omadustega. Seepärast toome sisse järgmise mõiste.

**Definitsioon 11.40.** Öeldakse, et hulgal $A$ on antud **klassijaotus** $K = \{K_i : i \in I\}$, kui

1. iga $i \in I$ korral $K_i \neq \emptyset$;

2. iga kaks erinevat hulka on mittelõikuvad, s.t iga $i, j \in I$ korral tingimusest $K_i \neq K_j$ järeldub, et $K_i \cap K_j = \emptyset$;

3. hulk $A$ võrdub osahulkade $K_i$ ühendiga, s.t $A = \bigcup_{i \in I} K_i$.

Hulki $K_i$, $i \in I$, nimetatakse selle klassijaotuse $K$ **klassideks**.

Teiste sõnadega, klassijaotuse korral on hulk $A$ jaotatud mittelõikuvateks mittetühjadeks osahulkadeks, mis moodustavadki hulkade süsteemi $K$. Üldjuhul võib $I$ olla ükskõik milline indeksite hulk (lõplik või lõpmatu).

**Näide 11.41.** 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 11.42.** Hulga $A$ kõik üheelemendilised osahulgad $\{a : a \in A\}$ moodustavad klassijaotuse, sest $\{a\} \neq \emptyset$, $\bigcup_{a \in A} \{a\} = A$ ja sellest, et $\{a\} \neq \{b\}$ (s.t. $a \neq b$), järeldub, et $\{a\} \cap \{b\} = \emptyset$. See on kõige peenem klassijaotus hulgal $A$.

**Näide 11.43.** Ühest tervest hulgast $A$ koosnev klassijaotus $\{A\}$ on kõige jämedam klassijaotus hulgal $A$.

**Näide 11.44.** Kui $A = \mathbb{R}$, siis moodustavad klassijaotuse poollõigud $K_i = [i, i + 1)$, $i \in Z$. (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 11.45.** *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 mingi 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 ekvivalentsuseosele vastavale klassijaotusele vastav ekvivalentsusseos, siis see ekvivalentsusseos langeb kokku esialgse ekvivalentsusseosega).

**Teoreem 11.46.**

1. *Olgu $R$ suvaline ekvivalentsusseos hulgal $A$. Siis ekvivalentsiklasside süsteem $\{[a]_R : a \in A\}$ on klassijaotus hulgal $A$.*

2. *Vastupidi, 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.*

1. Näitame, et osahulkade süsteem $\{[a]_R \colon a \in A\}$ on klassijaotus hulgal $A$. Tõepoolest, seose $R$ refleksiivsuse tõttu iga $a \in A$ korral $aRa$, s.t iga $a \in A$ korral $a \in [a]_R$. Seega ei ole ükski klassijaotuse klassidest tühi ning iga element kuulub vähemalt ühte klassidest $[a]_R$. See viimane väide aga tähendab ka seda, et iga $a \in A$ korral $a \in \bigcup_{a\in A}[a]_R$, s.t $A \subset \bigcup_{a\in A}[a]_R$. Et vastupidine sisalduvus $A \supseteq \bigcup_{a\in A}[a]_R$ on ilmne (miks?), siis oleme tõestanud, et $A = \bigcup_{a\in A}[a]_R$. Seega on klassijaotuse definitsiooni kolmas tingimus täidetud. Teise tingimuse kontrollimiseks näitame, et 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 $[b]_R \subset [a]_R$. Järelikult $[a]_R = [b]_R$. Kokkuvõttes oleme näidanud, et ekvivalentsiklasside süsteem $\{[a]_R \colon a \in A\}$ on klassijaotus hulgal $A$.

2. Olgu meil nüüd antud klassijaotus $K = \{K_i \colon i \in I\}$ 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. Seos $R$ on refleksiivne: 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. Seos $R$ on sümmeetriline: kui $aRb$, s.t $\exists i \in I\ (a \in K_i \wedge b \in K_i)$, siis ka $b \in K_i \wedge a \in K_i$, s.t $bRa$. 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 $aRc$. Kokkuvõtvalt oleme näidanud, et seos $R$ on refleksiivne, sümmeetriline ja transitiivne ning järelikult ekvivalentsusseos.

□

Vaatleme juba näidetes esinenud ekvivalentsusseoseid ja klassijaotusi ning leiame neile loomulikult vastavad klassijaotused ja ekvivalentsusseosed.

**Näide 11.47.** Suvalises hulgas $A$ antud võrdusseosele vastav klassijaotus koosneb hulkadest $[a]_R = \{b \colon b \in a \wedge bRa\} = \{b \in A \colon b = a\} = \{a\}$. Seega vastab võrdusele kui kõige kitsamale ekvivalentsusseosele kõige peenem klassijaotus $\{\{a\} \colon a \in A\}$.

**Näide 11.48.** 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 10.11).

Lause 10.11 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 11.49.** Hulga **võimsuseks** 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 $\{a\}, \{b\}, \ldots$ klass, seejärel kaheelemendiliste osahulkade klass jne. Vastavat ekvivalentsiklassi nimetataksegi hulga võimsuseks.

## 11.7 Faktorhulk

**Definitsioon 11.50.** Olgu $R$ ekvivalentsuseos hulgal $A$. Hulka, mille elementideks on seosele $R$ vastava klassijaotuse kõik klassid, nimetatakse **hulga $A$ faktorhulgaks ekvivalentsuseose $R$ järgi** ja tähistatakse $A/R$.

Seega, $A/R = \{[a]_R \colon a \in A\}$. Märgime, et erinevatele elementidele vastavad ekvivalentsiklassid võivad ühtida, s.t $a \neq b$ korral võib olla $[a]_R = [b]_R$. Faktorhulga elementideks võetakse võrdsete ekvivalentsiklasside seast ainult üks.

**Näide 11.51.** Kui hulgas $A$ vaadelda ekvivalentsusseosena võrdusseost $I$, siis $A/R = \{\{a\} \colon a \in A\}$.

**Näide 11.52.** 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 $[x] = \{y \in X \colon y_1 = x_1\}$ 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 11.53.** Kui $R$ on samasihilisuse seos tasandi (või ruumi) sirgete hulgal $A$, siis vastava faktorhulga elementideks on konkreetsed sihid.

**Näide 11.54.** 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.

## 11.8 Järjestusseos

**Definitsioon 11.55.** Seost $R$ hulgal $A$ nimetatakse **osalise järjestuse seoseks**, kui ta on

(a) refleksiivne, s.t kui $aRa$ iga $a \in A$ korral;

(b) antisümmeetriline, s.t kui $aRb$ ja $bRa$, siis $a = b$;

(c) transitiivne, s.t kui $aRb$ ja $bRc$, siis $aRc$.

Kui $R$ on järjestusseos, siis asjaolu $aRb$ märgitakse $a \leq b$ või samaväärselt $b \geq a$. Öeldakse ka, et $a$ **eelneb** elemendile $b$ või $b$ **järgneb** elemendile $a$.

**Ülesanne 11.56.** Tõesta, et kui $R$ on järjestusseos, siis ka $R^{-1}$ on järjestusseos.

**Definitsioon 11.57.** Hulka, millel on antud osalise järjestuse seos, nimetatakse **osaliselt järjestatud hulgaks**.

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 11.58.** Osaliselt järjestatud hulka nimetatakse **lineaarselt järjestatud hulgaks** ehk **ahelaks**, kui iga elementide paari $a$ ja $b$ korral $a \leq b$ või $b \leq a$, s.t kaks suvalist elementi on omavahel võrreldavad.

**Näide 11.59.**

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 11.60.** Määrame tähestikus $\{a_1, \dots, a_n\}$ järjestuse $a_1 < a_2 < \dots < a_n$. Defineerime sõnade hulgas järjestuse

$$\begin{aligned}(x_1, \dots, x_m) < (y_1, \dots, y_l) \Leftrightarrow\ & (x_1 < y_1) \vee (x_1 = y_1 \wedge x_2 < y_2) \vee \\ & \vee (x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 < y_3) \vee \\ & \vee (x_1 = y_1 \wedge \dots x_m = y_m \wedge m < l).\end{aligned}$$

Taolist järjestust nimetatakse **alfabeetiliseks** ehk **leksikograafiliseks**, ta on lineaarne ning teda kasutatakse sõnaraamatutes.

**Ülesanne 11.61.** Olgu $A$ kõigi lõigus $[a, b]$ määratud funktsioonide $f\colon [a, b] \to \mathbb{R}$ 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 $<$, mida võib seosest $\leq$ lähtudes defineerida järgmiselt: $x < y \Leftrightarrow x \leq y$ ja $x \neq y$.

**Definitsioon 11.62.** Osaliselt järjestatud hulga $A$ elementi $a_0$ nimetatakse **vähimaks** ehk **esimeseks**, kui $a_0 \leq a$ iga $a \in A$ korral. Analoogiliselt, elementi $a_0 \in P$ nimetatakse **suurimaks** ehk **viimaseks**, kui $a \leq a_0$ iga $a \in A$ korral.

**Näide 11.63.**

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 11.64.** *Osaliselt järjestatud hulgas ei ole üle ühe vähima ega üle ühe suurima elemendi.*

*Tõestus.* Olgu $a_0$ ja $a_1$ vähimad elemendid. Siis $a_0 \leq a_1$, sest $a_0$ on vähim element. Samuti $a_1 \leq a_0$, sest $a_1$ on ka vähim element. Kuna osalise järjestuse seos on antisümmeetriline, siis $a_0 = a_1$. Suurima elemendi tõestus on analoogiline. □

**Definitsioon 11.65.** Osaliselt järjestatud hulga $A$ elementi $a_0$ nimetatakse **minimaalseks**, kui sellest, et $a \leq a_0$ ja $a \in A$ korral järeldub, et $a = a_0$ (st hulgas $A$ ei ole elemendist $a_0$ väiksemaid elemente). Analoogiliselt, elementi $a_0$ nimetatakse **maksimaalseks**, kui sellest, et $a_0 \leq a$ ja $a \in A$ korral järeldub, 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 11.66.**

1. Reaalarvude hulgas, kus peetakse silmas loomulikku järjestust, 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 11.67.** *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 $a_0 \leq a$ iga $a \in A$ korral. Kui mingi $b \in A$ korral kehtiks veel $b \leq a_0$, 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 $a_0 \leq a_1$, 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 11.68.** *Lineaarselt järjestatud hulgas on minimaalne element vähim ja maksimaalne element suurim.*

*Tõestus.* Olgu lineaarselt järjestatud hulgas $A$ element $a_0$ minimaalne, st kui $a \leq a_0$ iga $a \in A$ korral, siis $a = a_0$. Näitame, et $a_0 \leq a$ iga $a \in A$ korral. Oletame vastuväiteliselt, et leidub $a_1 \in A$ nii, et ei kehti $a_0 \leq a_1$. Lineaarse järjestuse tõttu $a_0 \leq a_1$ või $a_1 \leq a_0$, seega saab kehtida ainult $a_1 \leq a_0$. Seejuures $a_1 \neq a_0$, sest $a_1 = a_0$ korral oleks $a_0 \leq a_1$. Kuid $a_1 \neq a_0$ ja $a_1 \leq a_0$ on vastuolus elemendi $a_0$ minimaalsusega. □

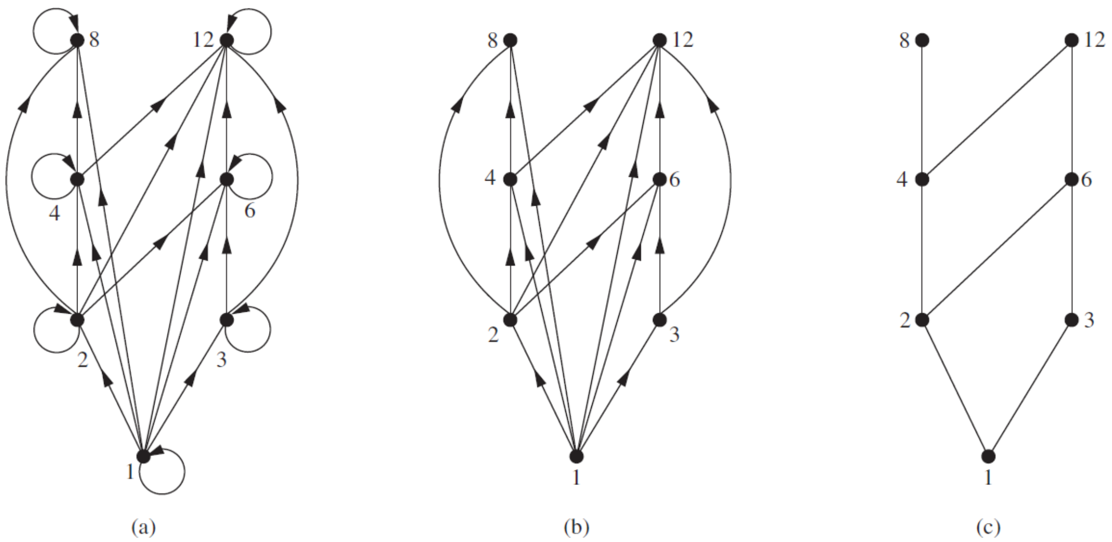
Lausetest 11.67 ja 11.68 järeldub vahetult:

**Järeldus 11.69.** *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 $(R, \leq)$ 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 $a \leq b$ ja $b \leq c$.
4. Säti servad nii, et graafi algtipp 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 11.1: 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.

## 11.9 Valikuaksioom ja sellega ekvivalentsed väited*

**Aksioom 11.70** (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 11.71.**

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. Tänaseks päevaks pole veel keegi sellist funktsiooni leidnud.

Kuratowski–Zorni lemmale tuginedes on võimalik tõestada mitmeid matemaatika fundamentaalseid teoreeme.

**Definitsioon 11.72.** 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 [4].

**Lemma 11.73** (Kuratowski–Zorni lemma)**.** *Kui osaliselt järjestatud hulga igal ahelal leidub ülemine tõke, siis selles hulgas leidub maksimaalne element.*

**Definitsioon 11.74.** Hulka nimetatakse **täielikult järjestatuks**, kui ta on niiviisi lineaarselt järjestatud, et tema igal mittetühjal alamhulgal on olemas vähim element.

**Näide 11.75.**

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 11.76.** Kuidas täielikult järjestada kõiki ratsionaalarve?

Ka Zermelo teoreemi tõestust me antud kursus ei esita ja selle tõestuse võib jällegi leida õpikust [4].

**Teoreem 11.77** (Zermelo teoreem)**.** *Mis tahes mittetühja hulka on võimalik täielikult järjestada.*

Järgmise teoreemi tulemuse võib leida näiteks õpikust [2].

**Teoreem 11.78.** *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 $f(X) \in X$.*

## 11.10 Tehted seostega*

Kuna seos on teatav hulk, siis rakenduvad hulgateoreetilised tehted ka seostele. Näiteks saab rääkida seoste ühendist, ühisosast, vahest või täiendist.

**Definitsioon 11.79.** Olgu $A$ ja $B$ hulgad ning olgu antud seosed $R, S \subset A \times B$.

(a) Seoste $R$ ja $S$ **ühendiks** nimetatakse seost $R \cup S$, mille korral $a(R \cup S)b \Leftrightarrow aRb \vee aSb$.

(b) Seoste $R$ ja $S$ **ühisosaks** nimetatakse seost $R \cap S$, mille korral $a(R \cap S)b \Leftrightarrow aRb \wedge aSb$.

(c) Seose $R$ **täiendiks** nimetatakse seost $R'$, mille korral $aR'b \Leftrightarrow \neg(aRb)$.

Nii defineeritud tehetele kanduvad mõistagi üle kõik suvaliste hulkade ühendi, ühisosa ja täiendi omadused. Universaalse hulga rollis on siin universaalne seos $U = A \times B$.

Näiteks, seose $R = \{(a, b) \colon a \leq b\}$ täiendiks hulgal $\mathbb{R}$ on seos $R' = \{(a, b) \colon a > b\}$.

**Ülesanne 11.80.** Näita, et seos $R$ hulgal $A$ on antisümmeetriline siis ja ainult siis, kui $R \cap R^{-1} \subset I = \{(a, a) \colon a \in A\}$.

**Definitsioon 11.81.** Seoste $R \subset A \times B$ ja $S \subset B \times C$ **korrutiseks** ehk **kompositsiooniks** nimetatakse seost $S \circ R \subset A \times C$, kus

$$S \circ R = \{(a, c) \colon \exists b \in B \text{ nii, et } (a, b) \in R \wedge (b, c) \in S\}.$$

Kasutatakse ka tähist $SR$. Sarnaselt eespool olevatele definitsioonidele, võime kahe seose korrutise definitsiooni tingimuse esitada ka kujul $a(S \circ R)c \Leftrightarrow \exists b \in B\ (aRb \wedge bSc)$.

Erijuhul, kui $R$ ja $S$ mõlemad on seosed hulgal $A$, on ka nende korrutis $S \circ R$ seos samal hulgal $A$.

**Näide 11.82.** 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 11.83.** 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 $I \circ R = R$.

Märgime, et seoste korrutamisel võib juhtuda, et $R \neq \emptyset$ ja $S \neq \emptyset$, aga $S \circ R = \emptyset$.

**Lause 11.84.** *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.* Tõestuseks on järgmised samaväärsuste ahelad:

1.

$$\begin{aligned}(c,a) \in (S \circ R)^{-1} &\Leftrightarrow (a,c) \in S \circ R \\ &\Leftrightarrow \exists b \in B\ (a,b) \in R \land (b,c) \in S \\ &\Leftrightarrow \exists b \in B\ (b,a) \in R^{-1} \land (c,b) \in S^{-1} \\ &\Leftrightarrow \exists b \in B\ (c,b) \in S^{-1} \land (b,a) \in R^{-1} \\ &\Leftrightarrow (c,a) \in R^{-1} \circ S^{-1}.\end{aligned}$$

2.

$$\begin{aligned}(a,d) \in T \circ (S \circ R) &\Leftrightarrow \exists c \in C\ (a,c) \in S \circ R \land (c,d) \in T \\ &\Leftrightarrow \exists c \in C\ \exists b \in B\ (a,b) \in R \land (b,c) \in S \land (c,d) \in T \\ &\Leftrightarrow \exists b \in B\ (a,b) \in R \land (b,d) \in T \circ S \\ &\Leftrightarrow (a,d) \in (T \circ S) \circ R.\end{aligned}$$

□

**Ülesanne 11.85.** Tõesta, et kui $R$ ja $S$ on ekvivalentsusseosed, siis $S \circ R$ on ekvivalentsusseos parajasti siis, kui $S \circ R = R \circ S$. Leia näide ekvivalentsusseostest $R$ ja $S$ (samal hulgal $A$), kus $S \circ R \neq R \circ S$.

# Kirjandus

***

[1] R. Hammack, *Book of proof*, Virginia Commonwealth University, 2013

[2] M. Kilp, *Algebra I*, Eesti Matemaatika Selts, Tartu, 2005

[3] V. Laan ja L. Tart, *Arvuteooria loengukonspekt*, TÜ, 2017

[4] P. Oja, *Hulgateooria*, TÜ Kirjastus, 2006.

[5] K. Rosen, *Discrete mathematics and its applications*, Boston, McGraw-Hill, 2012.