JOUKOT JA TODISTAMINEN

ANTTI KÄENMÄKI

”Toitteko minulle ihmisen, joka ei osaa laskea sormiaan?”

Kuolleiden kirja (kolmas vuosituhat eaa.)

27. joulukuuta 2024

Sisällys

Alkulause

Luentomoniste pyrkii kokoamaan esitetystä materiaalista kattavan ja ehkä myös hieman tarvittavaa laajemman kuvan, jolloin opiskelussa voidaan keskittyä yksittäisten aiheiden tarkempaan pohtimiseen. Monisteen marginaaleista löytyy linkit luentovideoihin, jotka pyrkivät käymään sisällön oleelliset asiat läpi ja rakentamaan monisteelle selkeän rungon. Ajatuksena on myös, että moniste voisi toimia muilla kursseilla taustamateriaalina, josta voi omaan tahtiin rauhassa kerrata esimerkiksi epäsuoran todistuksen vaiheet. Tavoitteena on ollut rakentaa kokonaisuus, joka antaa vahvan pohjan tuleville opinnoille. Monistetta kirjoittaessa on myös kiinnitetty erityistä huomiota matematiikan hyvään esittämiseen. Matematiikka on kieli ja sen oppimiseksi on ensiarvoisen tärkeää nähdä hyvin kirjoitettua matemaattista tekstiä.

Vaikka matemaattinen sisältö monisteessa on standardi, niin materiaalin valittu esitystapa noudattelee kirjoittajan omaa näkemystä – moniste onkin laajennettu versio kirjoittajan vuonna 2005 valmistuneesta luentomonisteesta *Johdatus matematiikkaan*. Päivitystyössä suurena apuna ovat olleet Richard Hammackin kirja *Book of Proof* vuodelta 2009 ja Kenneth H. Rosenin kirja *Discrete Mathematics and Its Applications* vuodelta 2012. Lisäksi hyödyksi ovat olleet Jorma Merikosken, Ari Virtasen ja Pertti Koiviston luentomoniste *Johdatus diskreettiin matematiikkaan* vuodelta 2004 sekä Veikko Rantalan ja Ari Virtasen luentomoniste *Logiikan peruskurssi* vuodelta 2003.

1. Mitä matematiikka on?

Luentovideo 1

Matematiikka tieteenä tutkii matematiikassa esiintyviä käsitteitä ja rakenteita sekä niiden suhteita täsmällisin päättelysäännöin ilman ensisijaista tavoitetta löytää sovelluksia matematiikan ulkopuolella. Käsitteet itsessään voivat olla peräisin todellisen maailman ongelmista ja saavutetut tulokset voivat myöhemmin osoittautua hyödyllisiksi käytännön sovelluksissa, mutta lähtökohtaisesti tällaiset yhteydet eivät ole ensisijainen motivaatio. Tavallisesti kiinnostus syntyy älyllisestä haasteesta ja perusteluiden esteettisestä kauneudesta.

Hämmästyttävän usein kuitenkin käy niin, että matemaattisen mielenkiinnon synnyttämiä tuloksia voidaan soveltaa. Esimerkiksi Apollonios[1] tutki antiikin aikana kartioleikkauksia ja myöhemmin huomattiin, että Newtonin[2] vuonna 1687 julkaisemassa kirjassa *Philosophiae Naturalis Principia Mathematica* esitetyn painovoimalain mukaan planeetat liikkuvat kartioleikkausten määräämillä radoilla. Toisena esimerkkinä voidaan mainita Eukleideen[3] n. vuonna 300 eaa. julkaisemassa teoksessa *Alkeet* esitetty tulos, lause 4.13, jonka mukaan mikä tahansa luonnollinen luku voidaan yksikäsitteisesti esittää alkulukujen tulona. Tiedonsiirrossa ja rahaliikenteessä käytettävän vuonna 1977 esitellyn RSA-salausalgoritmin turvallisuus perustuu olettamukseen, jonka mukaan erittäin suurten alkulukujen tulon alkulukuesityksen löytäminen on laskennallisesti työlästä.

Matematiikalla on laaja-alainen rooli jokapäiväisessä elämässä jo sitä kautta, että ymmärretään, kuinka erilaiset laitteet ja järjestelmät ympärillä toimivat. Matematiikkaa on kaikkialla, vaikka se ei aina ole perinteisessä mielessä näkyvillä. Nyky-yhteiskunnassa tarvitaan arjen matematiikkaa, mutta myös ongelmanratkaisukykyä ja ilmiöiden ymmärrystä, laaja-alaisempaa osaamista ajattelukyvyssä. Matematiikasta on tullut välttämätön edellytys kehitykselle. Jopa luonto noudattaa matematiikan lakeja. Einstein[4] onkin ihmetellyt kuinka voi olla niin, että havaintoihin liittymätön pelkästään ihmisen ajattelun tuotoksena syntynyt matematiikka voi kuvailla todellisuutta niin ihailtavan tarkasti. Fysiikka, kemia, biologia, tilastotiede,

[1] Apollonios Pergalainen (n. 240–190 eaa.)
[2] Isaac Newton (1643–1727)
[3] Eukleides Aleksandrialainen (n. 325–270 eaa.)
[4] Albert Einstein (1879–1955)

informaatiotiede, tekniikan ala, lääketiede, talouselämä, rahoitusala ja tähtitiede tarvitsevat kaikki matemaattisia menetelmiä ongelmien ratkaisemiseen. Ei varmasti ole yhtään liioiteltua sanoa, että matematiikka ja sen sovellukset ovat modernin maailman perusta.

Käytännössä matematiikan tekeminen ei ole pelkästään mekaanista laskemista tai valmiiden kaavojen soveltamista. Usein itse laskeminen onkin matematiikassa vain apuvälineen roolissa. Vaikka matemaatikot kenties itse haluavat ajatella, että matematiikka on sitä mitä matemaatikot tekevät, niin tiivistäen voidaan luonnehtia, että matematiikka on tietyistä alkuehdoista eli aksioomista johdettavien deduktiivisten päättelyketjujen eli todistusten muodostamia tosia lauseita, teoreemia. Deduktio on päättelyä yleisestä yksityiseen ja päättely on deduktiivinen, jos se säilyttää totuuden eli jos johtopäätös on oletusten looginen seuraus. Näin ollen matematiikassa, päin vastoin kuin muissa tieteissä, ei ole korjauksia, vain laajennuksia.

Eukleideen geometriaa ja lukuteoriaa käsittelevä kirja *Alkeet* on vanhin olemassa oleva matematiikan deduktiivinen esitys. Kirjaa pidetään onnistuneimpana ja vaikuttavimpana oppikirjana mitä on ikinä kirjoitettu. Sillä on ollut keskeinen merkitys tieteen kehitykselle aina 1900-luvun alkuun saakka. Kirjapainotaidon keksimisen ja vuoden 1482 ensipainoksen jälkeen siitä on arvioiden mukaan painettu ainakin tuhat painosta, häviten painosten määrässä ainoastaan Raamatulle. Kirjassa otettiin muutamia väitteitä, joita ei millään tapaa todistettu, päättelyn lähtökohdiksi. Näitä ilmeisiä tosiasioita eli aksioomia hyväksi käyttäen perusteltiin kirjan muut väitteet. Edellä mainitun alkulukuesityksen lisäksi tässä luentomonisteessa niistä käydään läpi alkulukujen lukumäärän äärettömyys lauseessa 5.10 ja luvun $\sqrt{2}$ irrationaalisuus lauseessa 5.17.

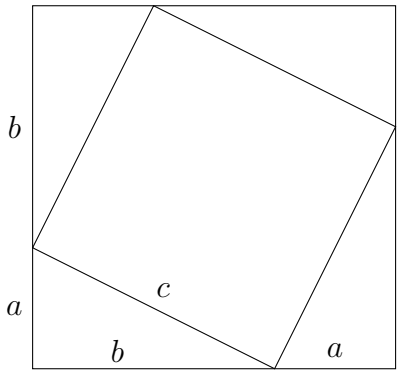
Tarkastellaan perustelemista esimerkinomaisesti Pythagoraan[5] lauseen avulla. Vaikka lause liitetään Pythagorakseen, niin se on historialtaan paljon vanhempi. Oletettavasti jokainen kehittynyt kulttuuri on historian saatossa keksinyt Pythagoraan lauseen. Neljä Babylonialaista savitaulua ajanjaksolta 1900-1600 eaa. osoittaa, että lause on jollain tapaa ymmärretty jo tänä aikana. Lause on myös mainittu

[5]Pythagoras (n. 570–495 eaa.)

intialaisessa *Baudhayana Sulba* sutrassa n. 800-400 eaa. ja kiinalaisessa tekstissä *Zhoubi Suanjing*, jonka vanhimmat säilyneet versiot ovat n. vuodelta 100 eaa.

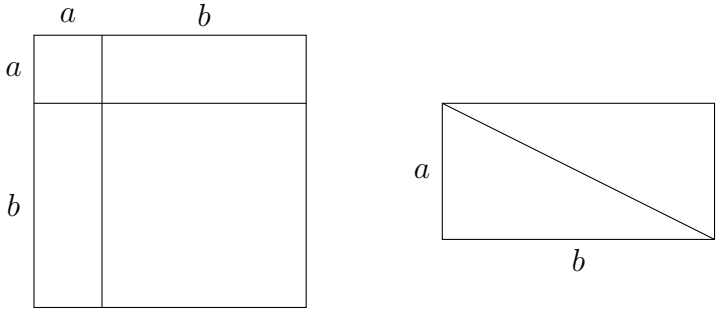
Lause 1.1 (Pythagoraan lause)**.** *Jos suorakulmaisen kolmion kateettien pituudet ovat a ja b ja hypotenuusan pituus on c, niin* $a^2 + b^2 = c^2$*.*

Todistus. Oheisessa kuvassa ison neliön pinta-ala on $(a+b)^2 = a^2 + 2ab + b^2$ ja



toisaalta se on myös neljän kolmion ja pienen neliön yhteenlaskettu pinta-ala eli $4\frac{ab}{2} + c^2 = 2ab + c^2$. Näin ollen $a^2 + 2ab + b^2 = 2ab + c^2$ eli $a^2 + b^2 = c^2$ kuten haluttiinkin. □

Perustelu näyttää aukottomalta. Onko tämä todistus Pythagoraan lauseelle? Lähemmin tarkastellen huomataan, että päättelyssä käytettiin esimerkiksi tietoa $(a+b)^2 = a^2 + 2ab + b^2$ ja suorakulmaisen kolmion pinta-alan kaavaa. On ilmeistä, että nämä eivät ole aksioomia, joten niiden on seurattava jostain. Oheiset kuviot



antavat näille geometriset perustelut. Seuraavaksi voisi kysyä miksi suorakulmion ala on sivujen pituuksien tulo ja miksi yhdenmuotoisilla kolmioilla on sama ala. Näin

jatkaen lopulta päästään tilanteeseen, jossa jokainen välivaihe on perusteltavissa aksioomilla. Tämä on formaali todistus Pythagoraan lauseelle. Näin pitkälle ei kuitenkaan käytännössä tarvitse mennä. Usein sanotaan, että todistus on päättelyketju, joka on perusteltu tarkasti. Tällä tarkoitetaan sitä, että jos päättelyssä voidaan viitata aikaisemmin osoitettuihin tai muuten tunnettuihin tuloksiin, niin tehdään näin. Edellä esitettyä päättelyketjua voidaan siten pitää todistuksena Pythagoraan lauseelle.

Vaikka matematiikan rakenteen synty voidaan jäljittää Eukleideen kirjaan *Alkeet*, niin matematiikan perusteellinen aksiomatisointi aloitettiin vasta 1900-luvun alussa. Esimerkiksi 1600-luvulla lopulla Leibniz[6] ja Newton[7] käyttivät differentiaali- ja integraalilaskentaa kehittäessään hyväkseen käsitettä infinitesimaali, joka tarkoittaa niin pientä suuretta, ettei sitä käytännössä tai edes periaatteessa voida mitata. Käsitteen määritelmä on epätyydyttävä, mutta sen avulla onnistuttiin silti saamaan aikaiseksi oikeita tuloksia.

Hilbert[8] julkaisi vuonna 1899 teoksen *Grundlagen der Geometrie*, jossa hän esitteli uudet geometrian aksioomat korvaamaan vanhat ja joiltain osin epämääräiset Eukleideen aksioomat. Tämä herätti tietysti kysymyksen voitaisiinko näin menetellä kaikilla matematiikan osa-alueilla. Seuraavana vuonna Hilbert esitti Pariisin matemaatikkojen kansainvälisessä kongressissa 23:n kysymyksen listan. Näistä neljä on edelleen täysin vailla vastausta. Listan toisena kysymyksenä oli aritmetiikan eli lukuteorian aksioomien ristiriidattomuuden osoittaminen. Russell[9] ja Whitehead[10] tarttuivat haasteeseen ja asettivat tavoitteekseen palauttaa aritmetiikka ja sitä kautta koko matematiikka symboliseen logiikkaan. He kirjoittivat kolmiosaista *Principia Mathematica* teossarjaa kymmenen vuotta ja osat lopulta julkaistiin vuosina 1910, 1912 ja 1913. Heidän työnsä oli niin perustavanlaatuista, että vasta toisen kirjan sivulla 86 he onnistuivat todistamaan, että $1 + 1 = 2$. Todistuksen jälkeen he kommentoivatkin humoristisesti, että yllä oleva lause on silloin tällöin hyödyllinen.

---

[6]Gottfried Wilhelm Leibniz (1646–1716)
[7]Isaac Newton (1643–1727)
[8]David Hilbert (1862–1943)
[9]Bertrand Arthur William Russell (1872–1970)
[10]Alfred North Whitehead (1861–1947)

Russel ja Whitehead eivät kuitenkaan pystyneet vastaamaan Hilbertin toiseen kysymykseen. He ainoastaan antoivat systemaattisen esityksen aritmetiikalle formaalina järjestelmänä. Kaksi vuosikymmentä myöhemmin vuonna 1931 Gödel[11] julkaisi kaikkien yllätykseksi artikkelin *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme*, jossa hän osoitti, että mikä tahansa aksioomajärjestelmä, joka määrittelee luonnolliset luvut ja niiden yhteen- ja kertolaskut, on välttämättä epätäydellinen eli että aritmetiikan aksioomien ristiriidattomuuden todistaminen vain aksioomia hyväksi käyttäen on mahdotonta. Tämä tarkoittaa sitä, että lukuteoriaa ei koskaan pystytä formalisoimaan niin, että kaikki sen todet väittämät olisivat johdettavissa aksioomista. Gödel siis romutti unelman siitä, että kaikki matematiikka olisi täydellisesti aksiomatisoitavissa.

On korostettava, että Gödel ei osoittanut aritmetiikkaa ristiriitaiseksi, vaan sen, että ristiriidattomuutta ei voida todistaa aritmetiikan sisällä. Käytännössä kaikki matemaattiset tulokset voidaan kuitenkin ristiriidattomasti kirjoittaa käyttäen hyväksi vain symbolista logiikkaa. Tämä tekee Einsteinin kysymyksestä, kuinka matematiikka voi kuvailla todellisuutta niin ihailtavan tarkasti, vielä mielenkiintoisemman. Voidaanko ajatella filosofi Platonin[12] hengessä, että matematiikka on erottamaton osa maailmankaikkeutta? Tällöin matematiikka on tieteen luonnollinen kieli yksinkertaisesti siitä syystä, että matematiikka on maailman synnynnäinen ominaisuus. Jos maailmankaikkeus yhtäkkiä lakkaisi olemasta, niin matemaattiset totuudet jatkaisivat silti olemassaoloaan. Matemaatikkojen tehtävänä on löytää uusia tuloksia ja ymmärrystä kuinka tulokset mallintavat todellista maailmaa. Vai pitääkö ajatella filosofi Kantin[13] hengessä, että matematiikka on luotu mallintamaan maailmaa? Ainoa syy miksi matematiikka kuvailee todellisuutta niin hyvin on se, että se on rakennettu tekemään juuri sitä. Jos maailmankaikkeus yhtäkkiä lakkaisi olemasta, niin matemaattiset totuudet katoaisivat samalla tapaa kuin shakki, jalkapallo tai mikä tahansa muu kokoelma keksittyjä sääntöjä. Matematiikka on ihmisen ajattelun tulos ja uusia tuloksia keksitään tarpeen mukaan.

[11] Kurt Friedrich Gödel (1906–1978)
[12] Platon (427–347 eaa.)
[13] Immanuel Kant (1724–1804)

Aritmetiikan aksiomatisointiin jäi jäljelle vielä yksi kysymys. Gödelin tuloksen perusteella matematiikassa on väitteitä, joita ei pystytä todistamaan. Siksi haluttiin tietää voidaanko ratkaista algoritmisesti, onko matemaattisella väitteellä todistusta vai ei. Tätä kutsuttiin päätösongelmaksi ja se on tarkennettu versio Hilbertin 23:n kysymyksen listan kymmenennestä kysymyksestä. Tähänkin kysymykseen vastaus osoittautui negatiiviseksi. Vuonna 1936 Turing[14] todisti artikkelissaan *On Computable Numbers, with an Application to the Entscheidungsproblem* Gödelin tulokseen perustaen, että ei ole olemassa yleistä menetelmää määrittää, mitkä ongelmat ovat ratkaistavissa ja mitkä ratkaisemattomia. Hän käytti todistuksessaan teoreettista mallia, ns. Turingin konetta, jolla hän määritteli tarkasti käsitteen algoritmi. Tulos löytyi soveltamalla universaalia konetta, eli "laitetta", joka pystyy simuloimaan mitä tahansa muuta Turingin konetta siihen ladattavien ohjeiden mukaan. Todistus muutti maailmaa pysyvästi – näitä laitteita kutsutaan nykyään tietokoneiksi.

Tämän luentomonisteen sisällöllisenä tavoitteena on selvittää matematiikan deduktiivinen rakenne sekä esitellä matematiikassa käytettäviä todistusmenetelmiä ja joukko-opin avulla rakennettuja käsitteitä. Lukijalta oletetaan lukion matematiikan sisällön hallintaa ja mielenkiintoa aiheeseen.

2. Lauselogiikkaa

Logiikka on oppia oikeasta ajattelusta. Se on kiinnostunut totuuden säilyttävistä päättelyistä, joissa johtopäätös on oletusten looginen seuraus. *Väitelause* on lause, joka on joko totta tai epätotta. Sen totuusarvoa merkitään vastaavasti symbolilla T tai E. Logiikkaa, joka tutkii väitelauseita ja niiden välisiä suhteita, sanotaan *lauselogiikaksi*. Vaikka lauselogiikka on peräisin Aristoteleen[15] ja Khyrippoksen[16] ajoilta, niin nykymuotoisen lauselogiikan kehittäjänä voidaan pitää Leibnitziä[17].

Luentovideo 2

2.1. **Loogiset konnektiivit.** *Loogisia konnektiiveja* ovat negaatio $\neg$, konjunktio $\wedge$, disjunktio $\vee$, implikaatio $\rightarrow$ ja ekvivalenssi $\leftrightarrow$. Yhdistelemällä väitelauseita

[14]Alan Mathison Turing (1912–1954)
[15]Aristoteles (384–322 eaa.)
[16]Khrysippos (279–207 eaa.)
[17]Gottfried Wilhelm Leibniz (1646–1716)

loogisilla konnektiiveilla saadaan uusia väitelauseita, ns. *molekyylilauseita*. Luetteloa, jossa esitetään kuinka molekyylilauseen totuusarvo riippuu siinä esiintyvien väitelauseiden totuusarvoista sanotaan *totuustaulukoksi*. Totuustaulukoiden avulla voidaan loogiset konnektiivit määritellä täsmällisesti. Nämä määritelmät ovat lauselogiikan aksioomia.

Yksinkertaisin loogisista konnektiiveista on *negaatio*, joka määritellään totuustaulukon avulla seuraavasti:

P	$\neg P$
T	E
E	T

Vasemmanpuoleisessa sarakkeessa on lueteltu väitelauseen P kaikki mahdolliset totuusarvot ja oikeanpuoleinen sarake kertoo kuinka $\neg P$ on määritelty kunkin totuusarvon tapauksessa. Jos väitelauseen P totuusarvo on tosi, niin sen negaation $\neg P$ totuusarvo on epätosi ja päinvastoin. Luonnollisessa kielessä negaatio $\neg P$ luetaan esimerkiksi "ei P", "ei ole niin, että P", "P ei päde", tai "P ei ole voimassa". Jos esimerkiksi $P =$ "aurinko paistaa", niin $\neg P =$ "aurinko ei paista".

Määritellään *konjunktio* totuustaulukon avulla seuraavasti:

P	Q	$P \wedge Q$
T	T	T
T	E	E
E	T	E
E	E	E

Taulukossa kaksi vasemmanpuoleisesta saraketta käy läpi väitelauseiden P ja Q kaikki mahdolliset totuusarvot ja oikeanpuoleinen sarake kertoo kuinka $P \wedge Q$ on määritelty kunkin totuusarvon tapauksessa. Konjunktio vastaa lähes täysin luonnollisen kielen ja-sanaa: luonnollisessa kielessä $P \wedge Q$ luetaankin P ja Q. Jos esimerkiksi $P =$ "aurinko paistaa" ja $Q =$ "tuulee", niin $(P \wedge Q) =$ "aurinko paistaa ja tuulee". Huomautetaan, että joissain tilanteissa luonnollisen kielen ja-sanaan liittyy järjestys kuten esimerkkilause "aakkosten kaksi ensimmäistä kirjainta ovat b ja a" havainnollisesti osoittaa. Konjunktiossa väitelauseiden järjestyksellä ei ole

väliä: $P \wedge Q$ ja $Q \wedge P$ ovat sama molekyylilause. Myöskään useamman konjunktion järjestyksellä ei ole väliä: $P \wedge (Q \wedge R)$ ja $(P \wedge Q) \wedge R$ ovat sama molekyylilause.

Määritellään *disjunktio* totuustaulukon avulla seuraavasti:

P	Q	$P \vee Q$
T	T	T
T	E	T
E	T	T
E	E	E

Disjunktio vastaa luonnollisen kielen sisällyttävää tai-sanaa: luonnollisessa kielessä $P \vee Q$ luetaankin P tai Q. Jos esimerkiksi $P =$ "pidän kesästä" ja $Q =$ "pidän jäätelöstä", niin molekyylilauseen $(P \vee Q) =$ "pidän kesästä tai jäätelöstä" ollessa tosi pidän vähintään toisesta, kesästä tai jäätelöstä. Ei siis ole poissuljettua, että pitäisin molemmista. Luonnollisen kielen tai-sanan kanssa pitää olla huolellinen. Asiayhteydestä riippuen se myös voi tarkoittaa poissulkevaa tai-sanaa kuten esimerkkilauseessa "jälkiruoaksi voi valita mustikkapiirakan tai uuniomenan", joka käytännössä tarkoittaa samaa kuin "jälkiruoaksi voi valita joko mustikkapiirakan tai uuniomenan". Korostetaan, että disjunktio ei vastaa poissulkevaa tai-sanaa, vaan molekyylilauseen $P \vee Q$ ollessa tosi molemmat väitelauseet P ja Q voivat olla tosia. Myöskään disjunktiossa väitelauseiden järjestyksellä ei ole väliä: $P \vee Q$ ja $Q \vee P$ ovat sama molekyylilause. Vastaavasti useamman disjunktion järjestys on vapaa: $P \vee (Q \vee R)$ ja $(P \vee Q) \vee R$ ovat sama molekyylilause.

Kahden väitelauseen välille määritellään *implikaatio* seuraavasti:

P	Q	$P \to Q$
T	T	T
T	E	E
E	T	T
E	E	T

Implikaatio ei täsmällisesti tarkoita syy-seuraussuhdetta, vaikka luonnollisessa kielessä $P \to Q$ luetaankin "jos P, niin Q", "P vain jos Q" tai "P:stä seuraa

Q". Molekyylilause $P \to Q$ on nimittäin määritelty todeksi aina kun väitelauseen P totuusarvo on epätosi. Jos esimerkiksi $P =$ "Maa on litteä", niin $P \to Q$ on tosi riippumatta väitelauseesta Q. Syy-seurausuhde toteutuu tilanteessa, jossa P ja $P \to Q$ ovat molemmat tosia. Jos esimerkiksi $P =$ "sataa" ja $Q =$ "on pilvistä", niin implikaatiossa $(P \to Q) =$ "jos sataa, niin on pilvistä" väitelause P on syy ja Q sen seuraus, ts. ei voi sataa jos ei ole pilvistä. Tällöin voidaan myös kirjoittaa, että "P on riittävä ehto Q:lle" tai "Q on välttämätön ehto P:lle". Se, että implikaatio $P \to Q$ määritellään todeksi kun P on epätosi saattaa aluksi vaikuttaa erikoiselta. Sitä voi yrittää hahmottaa esimerkiksi ehdokkaan vaalilupauksella "jos minut valitaan virkaan, niin lasken veroja". Jos ehdokas valitaan virkaan, niin äänestäjät odottavat hänen laskevan veroja. Jos taas ehdokasta ei valita, niin, vaikka äänestäjillä ei ole mitään odotuksia, hän voi silti muita keinoja hyväksi käyttäen laskea veroja. Vain siinä tapauksessa, että ehdokas on valittu ja hän ei laske veroja, hänen voidaan katsoa rikkoneen vaalilupauksensa.

Määritellään *ekvivalenssi* seuraavasti:

P	Q	$P \leftrightarrow Q$
T	T	T
T	E	E
E	T	E
E	E	T

Huomataan, että ekvivalenssilla tarkoitetaan implikaatiota molempiin suuntiin. Ekvivalenssi $P \leftrightarrow Q$ voidaankin luonnollisessa kielessä lukea "P on yhtäpitävää Q:n kanssa", "P jos ja vain jos Q" tai "P täsmälleen silloin, kun Q". Jos esimerkiksi $P =$ "sataa" ja $Q =$ "on pilvistä", niin ekvivalenssin $P \leftrightarrow Q$ ollessa tosi voi olla pilvistä vain, ja ainoastaan silloin, kun sataa. Pelkkä implikaatio $P \to Q$ ei sulje pois sitä mahdollisuutta, että voisi olla pilvistä ilman sadetta.

Luentovideo 3

2.2. **Tautologia.** *Tautologia* on molekyylilause, jonka totuusarvo on aina tosi, riippumatta siinä esiintyvien väitelauseiden totuusarvoista. Tautologian negaatiota sanotaan *ristiriidaksi*. Ristiriidan totuusarvo on siten aina epätosi, riippumatta siinä esiintyvien väitelauseiden totuusarvoista. Esimerkiksi totuustaulukot

P	$\neg P$	$P \vee \neg P$
T	E	T
E	T	T

P	$\neg P$	$\neg\neg P$	$\neg\neg P \leftrightarrow P$
T	E	T	T
E	T	E	T

osoittavat, että molekyylilauseet

$$P \vee \neg P \qquad \text{ja} \qquad \neg\neg P \leftrightarrow P \tag{2.1}$$

ovat tautologioita. Kyseisiä tautologioita kutsutaan *poissuljetun kolmannen laiksi* ja *kaksinkertaisen kiellon laiksi*. Jos esimerkiksi $P =$ "sataa", niin molekyylilause $(P \vee \neg P) =$ "sataa tai ei sada" on aina tosi. Lisäksi molekyylilauseella $\neg\neg P =$ "ei ole niin, että ei sada" on sama totuusarvo kuin väitelauseella P.

Huomataan, että jos $P \leftrightarrow Q$ on tautologia, niin ekvivalenssin määritelmän mukaan on vain kaksi vaihtoehtoa: P ja Q ovat molemmat joko tosia tai epätosia. Tällöin merkitään $P \Leftrightarrow Q$ ja sanotaan, että väitelauseet P ja Q ovat *loogisesti yhtäpitävät* (tai *ekvivalentit*). Merkinnällä $P \Leftrightarrow Q \Leftrightarrow R$ tarkoitetaan sitä, että $P \Leftrightarrow Q$ ja $Q \Leftrightarrow R$. Molekyylilauseessa esiintyvä väitelause voidaan siten korvata loogisesti yhtäpitävällä väitelauseella. Esimerkiksi kohdan (2.1) nojalla $\neg\neg P$ voidaan aina korvata väitelauseella P. Näin ollen muotoa $P \leftrightarrow Q$ olevat tautologiat antavat molekyylilauseille laskusääntöjä. Helposti esimerkiksi nähdään, että jos T on tautologia ja E ristiriita, niin $(P \vee T) \Leftrightarrow T$, $(P \vee P) \Leftrightarrow P \Leftrightarrow (P \vee E)$, $(P \wedge P) \Leftrightarrow P \Leftrightarrow (P \wedge T)$ ja $(P \wedge E) \Leftrightarrow E$.

Ekvivalenssin määritelmän yhteydessä todettiin, että ekvivalenssi tarkoittaa implikaatiota molempiin suuntiin. Täsmällisesti tällä tarkoitetaan molekyylilausetta

$$(P \leftrightarrow Q) \leftrightarrow ((P \to Q) \wedge (Q \to P)), \tag{2.2}$$

jonka totuustaulukko

P	Q	$P \to Q$	$Q \to P$	$(P \to Q) \wedge (Q \to P)$	$P \leftrightarrow Q$
T	T	T	T	T	T
T	E	E	T	E	E
E	T	T	E	E	E
E	E	T	T	T	T

osoittaa tautologiaksi. Ekvivalenssi $P \leftrightarrow Q$ on siis loogisesti yhtäpitävä implikaatioiden $P \to Q$ ja $Q \to P$ konjunktion kanssa. Selvitetään seuraavaksi konjunktion ja disjunktion välinen yhteys. Totuustaulukot

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P \vee \neg Q$
T	T	E	E	T	E	E
T	E	E	T	E	T	T
E	T	T	E	E	T	T
E	E	T	T	E	T	T

ja

P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$
T	T	E	E	T	E	E
T	E	E	T	T	E	E
E	T	T	E	T	E	E
E	E	T	T	E	T	T

osoittavat *De Morganin*[18] *lait*

$$\begin{aligned} \neg(P \wedge Q) &\quad \Leftrightarrow \quad \neg P \vee \neg Q, \\ \neg(P \vee Q) &\quad \Leftrightarrow \quad \neg P \wedge \neg Q. \end{aligned} \tag{2.3}$$

Jos esimerkiksi $P =$ "pidän kesästä" ja $Q =$ "pidän jäätelöstä", niin $\neg P \wedge \neg Q =$ "en pidä kesästä enkä jäätelöstä" on loogisesti yhtäpitävä molekyylilauseen $\neg(P \vee Q) =$ "ei ole niin, että pidän kesästä tai jäätelöstä" kanssa. De Morganin lakien eli kohdan (2.3) nojalla nähdään, että esimerkiksi molekyylilauseet $\neg(P \wedge \neg P)$ ja $\neg P \vee \neg\neg P$ ovat loogisesti yhtäpitävät. Koska kohdan (2.1) nojalla $\neg\neg P$ voidaan korvata väitelauseella P ja $\neg P \vee P$ on tautologia, niin myös *poissuljetun ristiriidan laki*

$$\neg(P \wedge \neg P) \tag{2.4}$$

on tautologia. Tästä kohdan (2.1) avulla nähdään, että $P \wedge \neg P$ on ristiriita.

Huomataan, että implikaatio voitaisiin vaihtoehtoisesti määritellä negaation ja disjunktion avulla, sillä totuustaulukon

[18] Augustus De Morgan (1806–1871)

P	Q	$\neg P$	$P \to Q$	$\neg P \vee Q$	$(P \to Q) \leftrightarrow (\neg P \vee Q)$
T	T	E	T	T	T
T	E	E	E	E	T
E	T	T	T	T	T
E	E	T	T	T	T

mukaan

$$P \to Q \quad \Leftrightarrow \quad \neg P \vee Q. \tag{2.5}$$

Koska tällöin $(\neg Q \to \neg P) \leftrightarrow (Q \vee \neg P)$, niin ollaan osoitettu *kontrapositio*

$$P \to Q \quad \Leftrightarrow \quad \neg Q \to \neg P. \tag{2.6}$$

Huomataan vielä, että De Morganin lakien eli kohdan (2.3) mukaan

$$\neg(P \to Q) \quad \Leftrightarrow \quad P \wedge \neg Q. \tag{2.7}$$

Jos esimerkiksi $P =$ "sataa" ja $Q =$ "on pilvistä", niin $(P \to Q) =$ "jos sataa, niin on pilvistä" on loogisesti yhtäpitävä molekyylilauseiden $(\neg P \vee Q) =$ "ei sada tai on pilvistä" ja $(\neg Q \to \neg P) =$ "jos ei ole pilvistä, niin ei sada" kanssa. Kohdista (2.5) ja (2.4) myös seuraa, että

$$P \quad \Leftrightarrow \quad \neg P \to (S \wedge \neg S). \tag{2.8}$$

Huomautetaan vielä, että terminologian kanssa on syytä olla tarkkana: implikaation $P \to Q$ negaatio on $\neg(P \to Q)$, kontrapositio on $\neg Q \to \neg P$ ja käänteinen suunta on $Q \to P$.

Totuustaulukoiden avulla nähdään *osittelulait*

$$\begin{aligned} P \wedge (Q \vee R) \quad &\Leftrightarrow \quad (P \wedge Q) \vee (P \wedge R), \\ P \vee (Q \wedge R) \quad &\Leftrightarrow \quad (P \vee Q) \wedge (P \vee R). \end{aligned} \tag{2.9}$$

Koska kohdan (2.5) ja De Morganin lakien eli kohdan (2.3) mukaan molekyylilauseet $(P \vee R) \to Q$ ja $(\neg P \wedge \neg R) \vee Q$ ovat loogisesti yhtäpitävät, niin osittelulakien eli kohdan (2.9) sekä kohdan (2.5) nojalla

$$(P \vee R) \to Q \quad \Leftrightarrow \quad (P \to Q) \wedge (R \to Q). \tag{2.10}$$

Näin ollen esimerkiksi ”jos sataa tai tuulee, niin on pilvistä” on loogisesti yhtäpitävä väitelauseiden ”jos sataa, niin on pilvistä” ja ”jos tuulee, niin on pilvistä” konjunktion kanssa.

Jos molekyylilause muodostetaan vain yhden väitelauseen avulla kuten esimerkiksi kohdassa (2.1), niin tautologiaksi toteaminen totuustaulukon avulla onnistuu kaksirivisellä taulukolla. Jos molekyylilause muodostetaan kahden väitelauseen avulla kuten esimerkiksi kohdissa (2.2), (2.3) ja (2.5), niin taulukointiin riittää $4 = 2^2$ riviä. Osittelulait eli kohdan (2.9) molekyylilauseet muodostuvat kolmesta väitelauseesta ja niiden tautologiaksi toteaminen onnistuu $8 = 2^3$ rivisellä taulukolla. Yleisesti, jos molekyylilauseessa esiintyy n väitelausetta, niin taulukointiin riittää 2^n riviä. Sanotaan, että luvun n kasvaessa rivien lukumäärä 2^n kasvaa *eksponentiaalisesti*. Jos esimerkiksi molekyylilause muodostuu sadasta väitelauseesta, niin totuustaulukossa on yhteensä $2^{100} \approx 1{,}2676506 \cdot 10^{30}$ riviä. Jos tietokone[19] pystyy tarkistamaan taulukosta 10^{18} rivin totuusarvon sekunnissa, niin koko totuustaulukon läpikäymiseen kuluisi noin $1{,}2676506 \cdot 10^{12}$ sekuntia eli reilu 40 170 vuotta. Voisiko tautologiaksi toteamisen tehdä jollakin nokkelammalla menetelmällä? Edellä esimerkiksi nähtiin, että useassa tapauksessa oli mahdollista käyttää tunnettuja loogisesti yhtäpitäviä lauseita ja sitä kautta välttää totuustaulukon käyttö kokonaan. Olisiko mahdollista, että tarvittavien operaatioiden lukumäärä olisi esimerkiksi vain $10n^k$ jollakin k, ts. luvun n kasvaessa operaatioiden lukumäärä kasvaisi *polynomisesti*. Jos $k = 10$, niin esimerkin tilanteessa tietokoneelta kuluisi tautologian selvittämiseksi korkeintaan 17 minuuttia. Kysymys on yksi kuuluisista Millenium-ongelmista ja sen ratkaisusta Clay-instituutti on luvannut miljoonan dollarin palkinnon.

Luentovideo 4

2.3. **Päätteleminen lauselogiikassa.** Muotoa

$$(P \wedge R) \to Q$$

olevaa molekyylilausetta kutsutaan *päättelylauseeksi*. Jos päättelylause on tautologia, niin implikaatiota merkitään $(P \wedge R) \Rightarrow Q$ ja sanotaan, että päättely on siinä *looginen*. Väitelausetta Q kutsutaan tällöin *johtopäätökseksi*. Huomautetaan, että $(P \wedge R \wedge S) \Leftrightarrow (P \wedge (R \wedge S))$ ja jos T on tautologia, niin $P \Leftrightarrow (P \wedge T)$.

[19] Euroopan nopeimman (v. 2022) supertietokoneen Lumin teoreettinen huipputeho on $0{,}55 \cdot 10^{18}$ liukulukulaskutoimitusta sekunnissa.

Näin ollen myös yleisemmät implikaatiot ovat päättelylauseita. Päättelylauseen totuustaulukko on seuraavanlainen:

P	R	Q	$P \wedge R$	$(P \wedge R) \to Q$
T	T	T	T	T
T	T	E	T	E
T	E	T	E	T
T	E	E	E	T
E	T	T	E	T
E	T	E	E	T
E	E	T	E	T
E	E	E	E	T

Huomataan, että jos P tai R on epätosi, niin myös $P \wedge R$ on epätosi ja siten päättelylause $(P \wedge R) \to Q$ pitää paikkansa riippumatta väitelauseen Q totuusarvosta. Tässä tilanteessa päättelyn loogisuus ei siis kerro mitään väitelauseen Q totuusarvosta. Oletetaan sitten, että molempien väitelauseiden P ja R totuusarvo on tosi. Tällöin molekyylilause $P \wedge R$ on tosi ja edellisessä totuustaulukossa vain kaksi ylimmäistä riviä ovat mahdollisia. Jos päättelylause $(P \wedge R) \to Q$ on tautologia, niin toiseksi ylin rivi ei tule kyseeseen ja väitelauseen Q totuusarvon täytyy olla tosi. Jos siis molemmat väitelauseet P ja R pitävät paikkansa, niin päättelyn loogisuus takaa johtopäätöksen Q totuuden.

Todetaan, että *syllogismissa*

$$(P \to Q) \wedge (Q \to R) \quad \Rightarrow \quad P \to R \tag{2.11}$$

päättely on looginen. Esimerkiksi "Jos sataa, niin on pilvistä. Jos on pilvistä, niin aurinko ei paista. Näin ollen, jos sataa, niin aurinko ei paista." on syllogismi ja päättely siinä on looginen. Huomataan, että kohtaan (2.5) vedoten syllogismi voidaan kirjoittaa yhtäpitävästi muodossa

$$(P \vee Q) \wedge (\neg P \vee R) \quad \Rightarrow \quad Q \vee R. \tag{2.12}$$

Näin ollen esimerkiksi päättely "Matematiikka on kivaa tai ei sada. Sataa tai logiikka on helppoa. Näin ollen matematiikka on kivaa tai logiikka on helppoa." on looginen.

Esimerkki 2.1. Tarkastellaan Origeneen[20] seuraavaa päättelyä: "Jos tiedän olevani *kuollut*, niin olen kuollut. Jos taas *tiedän* olevani kuollut, niin en ole kuollut. Näin ollen en tiedä olevani kuollut.". Ajatus tässä on se, että ensimmäinen lause toteaa kuolleen olevan kuollut. Toinen lause taas tekee havainnon, että jos on kykenevä tietämään asioita, niin ei voi olla kuollut. Merkitään $P =$ "tiedän olevani kuollut" ja $Q =$ "olen kuollut", jolloin päättely vastaa päättelylausetta

$$(P \to Q) \wedge (P \to \neg Q) \to \neg P.$$

Kohdan (2.6) mukaan molekyylilauseet $P \to \neg Q$ ja $Q \to \neg P$ ovat loogisesti yhtäpitävät ja kohdan (2.5) avulla nähdään, että näin ovat myös molekyylilauseet $\neg P$ ja $P \to \neg P$. Siten esitetty päättelylause on syllogismi ja kohdan (2.11) mukaan päättely on siinä looginen. Huomautetaan kuitenkin, että päättelyn loogisuus ei kerro mitään molekyylilauseiden $P \to Q$ ja $P \to \neg Q$ totuudesta eikä siten myöskään johtopäätöksen $\neg P$ totuudesta.

Totuustaulukon

P	Q	$P \to Q$	$P \wedge (P \to Q)$	$(P \wedge (P \to Q)) \to Q$
T	T	T	T	T
T	E	E	E	T
E	T	T	E	T
E	E	T	E	T

mukaan *suorassa todistuksessa*

$$P \wedge (P \to Q) \quad \Rightarrow \quad Q \tag{2.13}$$

päättely on looginen. Siten kohdan (2.6) mukaan myös *käänteisessä suorassa todistuksessa*

$$P \wedge (\neg Q \to \neg P) \quad \Rightarrow \quad Q \tag{2.14}$$

päättely on looginen. Huomataan vielä, että kohtien (2.8) ja (2.7) mukaan *epäsuorassa todistuksessa*

$$P \wedge ((P \wedge \neg Q) \to (S \wedge \neg S)) \quad \Rightarrow \quad Q \tag{2.15}$$

päättely on looginen.

[20]Origenes Adamantios (n. 185–254)

Jos tiedetään, että päättelyt

$$P \wedge R \quad \Rightarrow \quad T \qquad \text{ja} \qquad T \wedge S \quad \Rightarrow \quad Q$$

ovat loogisia, niin $(P \wedge R \wedge S) \rightarrow (T \wedge S)$ on tautologia ja siten kohdan (2.11) mukaan päättely

$$P \wedge R \wedge S \quad \Rightarrow \quad Q$$

on looginen. Tämä havainto antaa mahdollisuuden rakentaa loogisista päättelyistä *päättelyketjuja* sekä kääntäen, pilkkoa monimutkaisen oloisen päättelylauseen loogisuuden tarkastelu pienempiin palasiin. Usein päättelyketjuja havainnollistetaan kirjoittamalla $P \Rightarrow T \Rightarrow Q$, jolla tarkoitetaan sitä, että $(P \wedge R) \Rightarrow T$ ja $(T \wedge S) \Rightarrow Q$ joillakin väitelauseilla R ja S, jotka ovat esimerkiksi tunnettuja tosiasioita.

Esimerkki 2.2. Tarkastellaan seuraavaa päättelyä: ”Aurinko paistaa, mutta ei ole lämmin. Menemme kävelylle vain jos aurinko paistaa. Emme mene uimaan tai on lämmin. Jos emme mene kävelylle, niin menemme uimaan. Jos taas menemme kävelylle, niin ehdimme kotiin ajoissa. Näin ollen emme mene uimaan ja ehdimme kotiin ajoissa.”. Merkitään

$$P = \text{”aurinko paistaa”},$$
$$Q = \text{”on lämmin”},$$
$$R = \text{”menemme kävelylle”},$$
$$S = \text{”menemme uimaan”},$$
$$T = \text{”ehdimme kotiin ajoissa”},$$

jolloin päättely vastaa päättelylausetta

$$(P \wedge \neg Q \wedge (R \rightarrow P) \wedge (\neg S \vee Q) \wedge (\neg R \rightarrow S) \wedge (R \rightarrow T)) \rightarrow (\neg S \wedge T).$$

Osoitetaan päättelyketjun avulla, että päättely lauseessa on looginen. Koska kohdan (2.5) mukaan $\neg S \vee Q$ ja $S \rightarrow Q$ ovat loogisesti yhtäpitävät, niin käänteisen suoran todistuksen eli kohdan (2.14) mukaan päättely

$$(\neg Q \wedge (\neg S \vee Q)) \rightarrow \neg S \tag{2.16}$$

on looginen. Koska kohdan (2.6) mukaan $\neg R \to S$ ja $\neg S \to R$ ovat loogisesti yhtäpitävät, niin

$$((\neg R \to S) \wedge (R \to T)) \to (\neg S \to T) \tag{2.17}$$

on syllogismi ja kohdan (2.11) nojalla päättely on siinä looginen. Huomataan, että kohtien (2.16) ja (2.17) päättelyjä voidaan vielä jatkaa, sillä suoran todistuksen eli kohdan (2.13) mukaan päättely

$$(\neg S \wedge (\neg S \to T)) \to T \tag{2.18}$$

on looginen. Johtopäätös voidaan nyt lukea kohdista (2.16) ja (2.18). Nähdään, että päättely alkuperäisessä päättelylauseessa on looginen. Huomautetaan vielä, että koska päättelylause koostuu viidestä väitelauseesta, niin päättelyn loogisuuden toteaminen totuustaulukon avulla olisi vaatinut 32-rivisen taulukon.

3. Predikaattilogiikkaa

Avoimia väitelauseita käsittelevä *predikaattilogiikka* on lauselogiikkaa laajempi järjestelmä, jossa loogisten konnektiivien lisäksi esiintyvät kvanttorit. Avoimista väitelauseista saadaan kvanttoreiden avulla väitelauseita. Predikaattilogiikan kehittäjänä voidaan pitää Fregeä[21].

Luentovideo 5

3.1. **Kvanttorit.** Sanotaan, että $P(x)$ on alkioon x liittyvä *avoin väitelause*, jos kiinnittämällä alkion x arvo $P(x)$ on väitelause. Tällöin *kaikkikvanttori* (tai *universaalikvanttori*) $\forall$ määritellään asettamalla väitelause $\forall x : P(x)$ todeksi, kun $P(x)$ on tosi millä tahansa alkion x valinnalla. Toisin sanoen

$$\forall x : P(x) \quad \Leftrightarrow \quad \text{"}P(x) \text{ on tosi kaikilla } x\text{"}. \tag{3.1}$$

Luonnollisessa kielessä $\forall x : P(x)$ luetaankin "jokaisella x on $P(x)$" tai "$P(x)$ kaikilla x". Vastaavasti *olemassaolokvanttori* (tai *eksistenssikvanttori*) $\exists$ määritellään asettamalla väitelause $\exists x : P(x)$ todeksi, kun on olemassa alkio x siten, että $P(x)$ on tosi. Toisin sanoen

$$\exists x : P(x) \quad \Leftrightarrow \quad \text{"}P(x) \text{ on tosi jollakin } x\text{"}. \tag{3.2}$$

[21]Friedrich Ludwig Gottlob Frege (1848–1925)

Luonnollisessa kielessä $\exists x : P(x)$ luetaankin "on olemassa x siten, että $P(x)$" tai "$P(x)$ jollakin x". Jos esimerkiksi $N(x) =$ "x on nainen" ja $P(x) =$ "x:llä on pitkät hiukset", niin $(N(x) \to P(x)) =$ "naisella x on pitkät hiukset" ei ole väitelause, sillä ei tiedetä keneen lause kohdistuu. Se on avoin väitelause ja $(\forall x : N(x) \to P(x)) =$ "jokaisella naisella on pitkät hiukset" sekä $(\exists x : N(x) \to P(x)) =$ "on olemassa nainen, jolla on pitkät hiukset" ovat väitelauseita.

Matematiikassa esitetään usein muotoa $\forall x : P(x) \to Q(x)$ olevia väitelauseita luonnollisella kielellä. Jos esimerkiksi $P(n) =$ "$n \geqslant 3$ on alkuluku" ja $Q(n) =$ "n on pariton", niin väitelause $\forall n : P(n) \to Q(n)$ voidaan lukea monella eri tapaa: "jokainen lukua 2 suurempi alkuluku on pariton", "jos $n \geqslant 3$ on alkuluku, niin n on pariton", "lukuun ottamatta lukua 2, jokainen alkuluku on pariton" tai "mikä tahansa alkuluku, joka on lukua 2 suurempi, on myös pariton".

Huomataan, että jos väitelause $\forall x : P(x)$ on epätosi, niin kohdan (3.1) mukaan ei ole niin, että $P(x)$ on totta kaikilla alkion x valinnoilla. Toisin sanoen on olemassa alkio x siten, että $P(x)$ on epätosi, ja siten kohdan (3.2) mukaan väitelause $\exists x : \neg P(x)$ on tosi. Vastaavasti, jos väitelause $\exists x : P(x)$ on epätosi, niin samalla tavalla nähdään, että $\forall x : \neg P(x)$ on tosi. Ollaan siis perusteltu *negaation ja kvanttoreiden vaihtosäännöt*

$$\begin{aligned} \neg(\forall x : P(x)) \quad &\Leftrightarrow \quad \exists x : \neg P(x), \\ \neg(\exists x : P(x)) \quad &\Leftrightarrow \quad \forall x : \neg P(x). \end{aligned} \tag{3.3}$$

Jos esimerkiksi $O(x) =$ "x on kurssin opiskelija" ja $K(x) =$ "x on kiinnostunut matematiikasta", niin $(\forall x : O(x) \to K(x)) =$ "jokainen kurssin opiskelija on kiinnostunut matematiikasta" ja $(\exists x : O(x) \to K(x)) =$ "kurssilla on opiskelija, joka on kiinnostunut matematiikasta". Negaation ja kvanttoreiden vaihtosääntöjen sekä kohdan (2.7) mukaan $\neg(\forall x : O(x) \to K(x)) =$ "kurssilla on opiskelija, joka ei ole kiinnostunut matematiikasta" ja $\neg(\exists x : O(x) \to K(x)) =$ "kukaan kurssin opiskelijoista ei ole kiinnostunut matematiikasta".

Jos alkion x arvoiksi on vain äärellinen määrä vaihtoehtoja, niin negaation ja kvanttoreiden vaihtosäännöt seuraavat De Morganin laeista. Oletetaan, että alkion x mahdolliset arvot ovat $x_1, x_2, \ldots, x_n$. Tällöin kohtien (3.1) ja (3.2) avulla nähdään,

että

$$\begin{aligned} \forall x : P(x) \quad &\Leftrightarrow \quad P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n), \\ \exists x : P(x) \quad &\Leftrightarrow \quad P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n). \end{aligned} \tag{3.4}$$

Näin ollen De Morganin lakien eli kohdan (2.3) mukaan

$$\begin{aligned} \neg(\forall x : P(x)) \quad &\Leftrightarrow \quad \neg P(x_1) \vee \neg P(x_2) \vee \cdots \vee \neg P(x_n), \\ \neg(\exists x : P(x)) \quad &\Leftrightarrow \quad \neg P(x_1) \wedge \neg P(x_2) \wedge \cdots \wedge \neg P(x_n). \end{aligned}$$

Jos esimerkiksi $P(x) =$ "viikonpäivänä x sataa", niin $\forall x : P(x)$ voidaan lukea "koko viikon sataa" tai kohdan (3.4) mukaan "maanantaina sataa, tiistaina sataa, ..., lauantaina sataa ja sunnuntaina sataa".

Tarkastellaan vielä kaikkikvanttorin ja konjunktion sekä olemassaolokvanttorin ja disjunktion suhdetta yleisessä tilanteessa. Väitelause $\forall x : P(x) \wedge Q(x)$ on tosi kohdan (3.1) mukaan silloin, kun $P(x)$ ja $Q(x)$ ovat tosia millä tahansa alkion x valinnalla. Tämä on selvästi yhtäpitävä sen kanssa, että $P(x)$ on tosi millä tahansa alkion x valinnalla ja $Q(x)$ on tosi millä tahansa alkion x valinnalla, ts. $(\forall x : P(x)) \wedge (\forall x : Q(x))$ on tosi. Näin ollen

$$\forall x : P(x) \wedge Q(x) \quad \Leftrightarrow \quad (\forall x : P(x)) \wedge (\forall x : Q(x)) \tag{3.5}$$

Negaation ja kvanttoreiden vaihtosääntöjen eli kohdan (3.3) ja De Morganin lakien eli kohdan (2.3) mukaan tämän avulla todetaan, että

$$\exists x : P(x) \vee Q(x) \quad \Leftrightarrow \quad (\exists x : P(x)) \vee (\exists x : Q(x)). \tag{3.6}$$

Todetaan lopuksi, että

$$\begin{aligned} (\forall x : P(x)) \vee (\forall x : Q(x)) \quad &\Rightarrow \quad \forall x : P(x) \vee Q(x), \\ \exists x : P(x) \wedge Q(x) \quad &\Rightarrow \quad (\exists x : P(x)) \wedge (\exists x : Q(x)). \end{aligned}$$

Lisäksi

$$(\forall x : P(x)) \rightarrow (\forall x : Q(x)) \quad \Rightarrow \quad \forall x : P(x) \rightarrow Q(x).$$

Jos esimerkiksi $P(x) =$ "x on prinsessa" ja $Q(x) =$ "x on kuninkaallinen", niin $(\forall x : P(x)) \vee (\forall x : Q(x))$ luetaan "jokainen on prinsessa tai jokainen on kuninkaallinen" ja $\forall x : P(x) \vee Q(x)$ luetaan "jokainen on prinsessa tai kuninkaallinen". Tässä

jälkimmäinen väitelause on tosi myös silloin, kun puolet kansasta on prinsessoja ja toinen puoli kuninkaallisia. Huomataan myös, että $\exists x : P(x) \wedge Q(x)$ luetaan "joku kuninkaallinen on prinsessa" ja $(\exists x : P(x)) \wedge (\exists x : Q(x))$ luetaan "joku on prinsessa ja joku on kuninkaallinen". Tässä jälkimmäinen väitelause on tosi myös silloin, kun kyseessä on kaksi eri henkilöä. Lisäksi $(\forall x : P(x)) \to (\forall x : Q(x))$ luetaan "jos jokainen on prinsessa, niin kaikki ovat kuninkaallisia" ja $\forall x : P(x) \to Q(x)$ luetaan "prinsessat ovat kuninkaallisia".

Luentovideo 6

3.2. **Päätteleminen predikaattilogiikassa.** Predikaattilogiikassa tehtävät päättelyt palautetaan kaikkikvanttorin ja olemassaolokvanttorin määritelmien (3.1) ja (3.2) kautta lauselogiikan päättelyiksi.

Esimerkki 3.1. Tarkastellaan seuraavaa päättelyä: "Kurssin jokainen osallistuja pitää matematiikasta. Kaikki ihmiset eivät pidä matematiikasta. Siispä on olemassa ihminen, joka ei osallistu kurssille.". Merkitään $K(x) =$ "x on kurssin osallistuja" ja $M(x) =$ "x pitää matematiikasta", jolloin päättely vastaa päättelylausetta

$$((\forall x : K(x) \to M(x)) \wedge \neg(\forall x : M(x))) \to (\exists x : \neg K(x)). \tag{3.7}$$

Osoitetaan, että päättely on lauseessa looginen. Tätä varten voidaan olettaa, että väitelauseet $(\forall x : K(x) \to M(x))$ ja $\neg(\forall x : M(x))$ ovat tosia. Koska negaation ja kvanttoreiden vaihtosääntöjen eli kohdan (3.3) mukaan $\neg(\forall x : M(x))$ ja $\exists x : \neg M(x)$ ovat loogisesti yhtäpitävät, niin kohdan (3.2) mukaan on olemassa x_0 siten, että $\neg M(x_0)$ pitää paikkansa. Kohdan (3.1) mukaan $K(x) \to M(x)$ on totta kaikilla x, joten erityisesti $K(x_0) \to M(x_0)$ on totta. Koska kohdan (2.6) mukaan $K(x_0) \to M(x_0)$ ja $\neg M(x_0) \to \neg K(x_0)$ ovat loogisesti yhtäpitävät ja kohdan (2.14) mukaan

$$((\neg M(x_0) \to \neg K(x_0)) \wedge \neg M(x_0)) \to \neg K(x_0)$$

on käänteinen suora todistus ja siten tautologia, niin $\neg K(x_0)$ on johtopäätöksenä tosi. Siten kohdan (3.2) mukaan $\exists x : \neg K(x)$ on tosi ja päättelylause (3.7) on tautologia.

Esimerkki 3.2. Tarkastellaan *Liisan seikkailut ihmemaassa* -kirjan kirjoittajan Lewis Carrollin[22] päättelyä: "Kolibrit ovat värikkäitä. Ei ole olemassa hunajalla eläviä

[22]Charles Lutwidge Dodgson (1832–1898)

suuria lintuja. Linnut, jotka eivät elä hunajalla ovat värittömiä. Näin ollen kolibrit ovat pieniä." Merkitään $K(x) =$ "x on kolibri", $V(x) =$ "x on värikäs", $S(x) =$ "x on suuri lintu", $H(x) =$ "x elää hunajalla", jolloin päättely vastaa päättelylausetta

$$(\forall x : K(x) \to V(x)) \wedge \neg(\exists x : H(x) \wedge S(x)) \wedge (\forall x : \neg H(x) \to \neg V(x)) \\ \to (\forall x : K(x) \to \neg S(x)). \tag{3.8}$$

Osoitetaan, että päättely on lauseessa looginen. Tätä varten voidaan olettaa, että väitelauseet $\forall x : K(x) \to V(x))$, $\neg(\exists x : H(x) \wedge S(x))$ ja $(\forall x : \neg H(x) \to \neg V(x)$ ovat tosia. Huomataan, että negaation ja kvanttoreiden vaihtosääntöjen eli kohdan (3.3) sekä kohdan (2.7) mukaan $\neg(\exists x : H(x) \wedge S(x))$ ja $\forall x : H(x) \to \neg S(x)$ ovat loogisesti yhtäpitävät. Näin ollen kohtien (3.5) ja (3.1) mukaan

$$(K(x) \to V(x)) \wedge (H(x) \to \neg S(x)) \wedge (\neg H(x) \to \neg V(x)) \tag{3.9}$$

on tosi kaikilla x. Koska kohdan (2.6) mukaan $\neg H(x) \to \neg V(x)$ ja $V(x) \to H(x)$ ovat loogisesti yhtäpitävät, niin

$$((K(x) \to V(x)) \wedge (\neg H(x) \to \neg V(x))) \to (K(x) \to H(x)) \tag{3.10}$$

on syllogismi ja kohdan (2.11) mukaan päättely on siinä looginen. Koska myös

$$((K(x) \to H(x)) \wedge (\neg H(x) \to \neg S(x))) \to (K(x) \to \neg S(x)) \tag{3.11}$$

on syllogismi, niin kohdan (3.9) ja kohtien (3.10) ja (3.11) muodostaman päättelyketjun nojalla $K(x) \to \neg S(x)$ on tosi kaikilla x. Siten kohdan (3.1) mukaan $\forall x : K(x) \to \neg S(x)$ on tosi ja päättely on lauseessa looginen.

Huomautetaan, että vaikka edellisten esimerkkien perustelut päättelyiden loogisuudelle ovat täsmälliset, niin luettavuuden ja ymmärrettävyyden kannalta arkikieliset perustelut olisivat varmasti selkeämmät.

Luentovideo 7

3.3. **Sisäkkäiset kvanttorit.** Avoin väitelause voi liittyä useampaan alkioon. Jos esimerkiksi $P(x, y)$ on alkioihin x ja y liittyvä avoin väitelause, niin alkiot x ja y kiinnittämällä $P(x, y)$ on väitelause. Kiinnittämällä vain alkio y nähdään, että $P(x, y)$ on alkioon x liittyvä avoin väitelause. Myös $\forall y : P(x, y)$ ja $\exists y : P(x, y)$ ovat alkioon x liittyviä avoimia väitelauseita. Näin ollen esimerkiksi kahdella sisäkkäisellä kvanttorilla muodostettu $\forall x : (\exists y : P(x, y))$, jota merkitään lyhyemmin

$\forall x\,\exists y : P(x,y)$, on väitelause. Huomataan, että kohtien (3.1) ja (3.2) mukaan

$$\forall x\,\forall y : P(x,y) \quad \Leftrightarrow \quad \forall y\,\forall x : P(x,y),$$
$$\exists x\,\exists y : P(x,y) \quad \Leftrightarrow \quad \exists y\,\exists x : P(x,y).$$

Näistä ensimmäisen yhtäpitävä väitelause voidaan lukea "jokaisella x ja y on $P(x,y)$" tai "$P(x,y)$ kaikilla x ja y". Jälkimmäisen taas voidaan lukea "on olemassa x ja y siten, että $P(x,y)$" tai "$P(x,y)$ joillakin x ja y". Todetaan myös, että

$$\exists x\,\forall y : P(x,y) \quad \Rightarrow \quad \forall y\,\exists x : P(x,y).$$

Tässä implikaation vasen puoli voidaan lukea "on olemassa x siten, että $P(x,y)$ kaikilla y" ja oikea puoli "jokaiselle y on olemassa x siten, että $P(x,y)$". Jos esimerkiksi $P(x,y) =$ "x on hevosen y kengittäjä", niin $\exists x\,\forall y : P(x,y)$ luetaan "on olemassa kaikkien hevosten kengittäjä" ja $\forall y\,\exists x : P(x,y)$ luetaan "jokaiselle hevoselle on kengittäjä". Jälkimmäinen väitelause on tosi myös silloin, kun useampi kengittäjä hoitaa hevosten kengityksen.

Esimerkki 3.3. Olkoot $T(x) =$ "opiskelijalla x on tietokone" ja $K(x,y) =$ "opiskelijat x ja y ovat kavereita". Tällöin molekyylilause

$$\forall x : (T(x) \vee (\exists y : K(x,y) \wedge T(y)))$$

luetaan "jokaisella opiskelijalla on tietokone tai kaveri, jolla on tietokone". Molekyylilause

$$\exists x\,\forall y\,\forall z : (K(x,y) \wedge K(x,z) \wedge "y \neq z") \rightarrow \neg K(y,z)$$

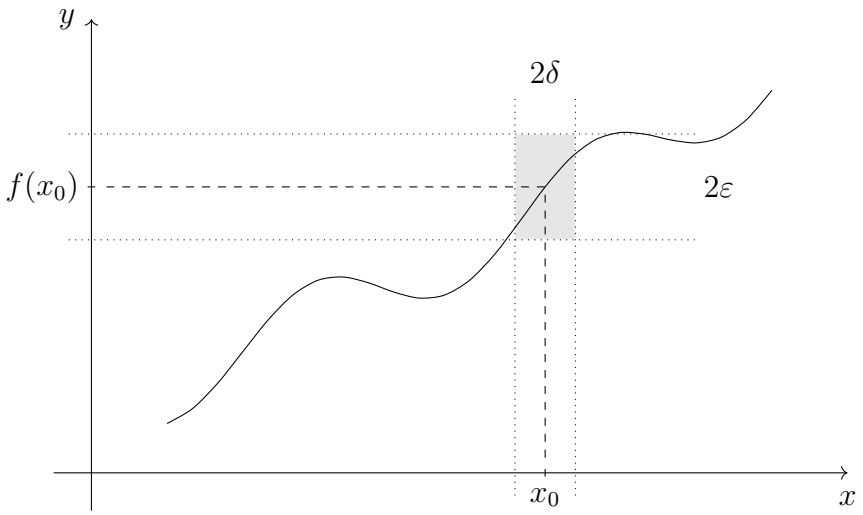
taas luetaan "on olemassa opiskelija, jonka kaverit eivät ole keskenään kavereita".

Esimerkki 3.4. Reaalifunktion f kuvaajaa voidaan hahmotella xy-koordinaatistossa. Kuvaus määritellään täsmällisesti kappaleessa 7.1. Intuitiivisesti ajatellaan, että funktio on jatkuva, jos sen kuvaaja "voidaan piirtää kynää paperista nostamatta". Jatkuvuuden täsmällisen määritelmän mukaan f on *jatkuva pisteessä* x_0, jos molekyylilauseen

$$\forall \varepsilon > 0\,\exists \delta > 0\,\forall x : |x - x_0| < \delta \rightarrow |f(x) - f(x_0)| < \varepsilon$$

totuusarvo on tosi. Huomautetaan, että valittua notaatiota täsmällisesti seuraten avoimet väitelauseet yllä pitäisi olla sitaateissa, esimerkiksi "$|x - x_0| < \delta$". Sitaatit

kuitenkin yleensä jätetään pois. Sanotaan, että f on *jatkuva*, jos se on jatkuva jokaisessa määrittelyvälinsä pisteessä. Oheinen kuva havainnollistaa määritelmän



vaatimusta. Kuvan funktio näyttäisi olevan jatkuva pisteessä x_0: vaikka kuvan vaakasuora katkoviivoin esitetty "putki" valittaisiin kuinka kapeaksi tahansa, niin pystysuora "putki" voidaan valita siten, että sen rajaama funktion kuvaaja sisältyy tummennettuun suorakaiteeseen.

Negaation ja kvanttoreiden vaihtosääntöjen eli kohdan (3.3) mukaan

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

Koska saman vaihtosäännön mukaan $\neg(\exists x : P(x,y))$ ja $\forall x : \neg P(x,y)$ ovat loogisesti yhtäpitävät, niin nähdään, että

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

Vastaavilla päättelyillä nähdään, että

$$\begin{aligned}
\neg(\forall y\, \forall x : P(x,y)) \quad &\Leftrightarrow \quad \exists y\, \exists x : \neg P(x,y), \\
\neg(\exists y\, \forall x : P(x,y)) \quad &\Leftrightarrow \quad \forall y\, \exists x : \neg P(x,y), \\
\neg(\exists y\, \exists x : P(x,y)) \quad &\Leftrightarrow \quad \forall y\, \forall x : \neg P(x,y).
\end{aligned}$$

Ollaan siis yleistetty negaation ja kvanttoreiden vaihtosäännöt: sisäkkäisiä kvanttoreita sisältävän väitelauseen negaatio saadaan vaihtamalla olemassaolokvanttorit kaikkikvanttoreiksi ja päinvastoin sekä ottamalla avoimesta väitelauseesta negaatio.

Esimerkki 3.5. Selvitetään esimerkin 3.3 lauseen ”jokaisella opiskelijalla on tietokone tai kaveri, jolla on tietokone” negaatio. Merkitään $T(x) =$ ”opiskelijalla x on tietokone” ja $K(x, y) =$ ”opiskelijat x ja y ovat kavereita”, jolloin esimerkin 3.3 mukaan lauseen negaatio on molekyylilause

$$\neg(\forall x : T(x) \vee (\exists y : K(x, y) \wedge T(y))).$$

Tämä on negaation ja kvanttoreiden vaihtosääntöjen eli kohdan (3.3), De Morganin lakien eli kohdan (2.3) ja kohdan (2.7) mukaan loogisesti yhtäpitävä molekyylilauseen

$$\exists x : \neg T(x) \wedge (\forall y : K(x, y) \to \neg T(y))$$

kanssa. Lauseen negaatio voidaan siis lukea ”jollakin opiskelijalla ei, eikä myöskään hänen kavereillaan, ole tietokonetta”.

Selvitetään sitten esimerkin 3.3 toisen lauseen ”on olemassa opiskelija, jonka kaverit eivät ole keskenään kavereita” negaatio. Esimerkin 3.3 mukaan se on molekyylilause

$$\neg(\exists x\, \forall y\, \forall z : (K(x, y) \wedge K(x, z) \wedge \text{”}y \neq z\text{”}) \to \neg K(y, z)).$$

Tämä taas on negaation ja kvanttoreiden vaihtosääntöjen, De Morganin lakien ja kohdan (2.7) mukaan loogisesti yhtäpitävä molekyylilauseen

$$\forall x\, \exists y\, \exists z : K(x, y) \wedge K(x, z) \wedge \text{”}y \neq z\text{”} \wedge K(y, z)$$

kanssa. Lauseen negaatio voidaan siis lukea ”jokaisella opiskelijalla on kavereita, jotka ovat keskenään kavereita”.

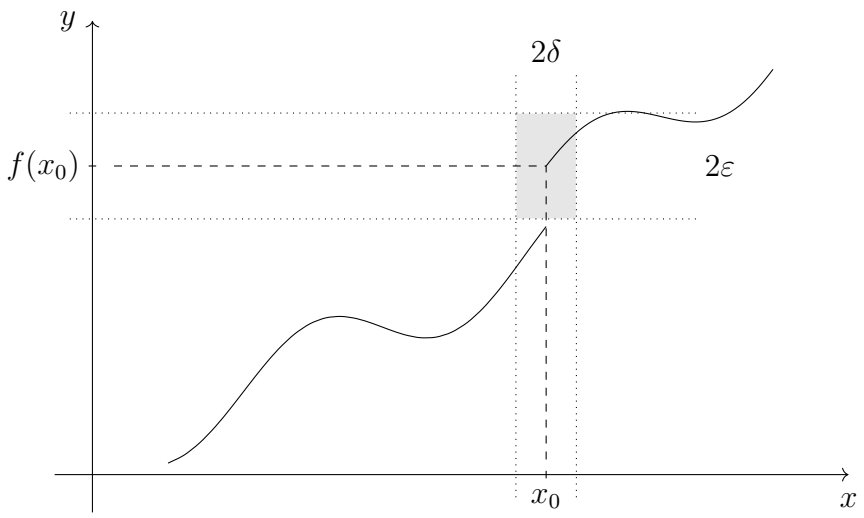
Esimerkki 3.6. Reaalifunktio f ei ole jatkuva pisteessä x_0, jos molekyylilauseen

$$\forall \varepsilon > 0\, \exists \delta > 0\, \forall x : |x - x_0| < \delta \to |f(x) - f(x_0)| < \varepsilon$$

totuusarvo on epätosi. Negaation ja kvanttoreiden vaihtosäännön eli kohdan (3.3) sekä kohdan (2.7) mukaan tämä on yhtäpitävää sen kanssa, että molekyylilause

$$\exists \varepsilon > 0 \, \forall \delta > 0 \, \exists x : |x - x_0| < \delta \wedge |f(x) - f(x_0)| \geqslant \varepsilon$$

on tosi. Oheinen kuva havainnollistaa epäjatkuvuutta. Kuvan funktio ei ole jatkuva



pisteessä x_0, sillä vaakasuora "putki" voidaan valita siten, että valittiin pystysuora "putki" kuinka tahansa, niin sen rajaama funktion kuvaaja ei kokonaisuudessaa sisälly tummennettuun suorakaiteeseen.

4. Todistamisesta

Määritelmä antaa käsitteelle täsmällisen merkityksen. Matemaattisessa tekstissä määritelty käsite on tapana korostaa kursiivilla. Vaikka lauselogiikan kannalta määritelmän tarkoitus on tehdä kahdesta väitelauseesta yhtäpitävät, niin määritelmät on tapana antaa ehdollisina:

Määritelmä. Lukua kaksi suurempi luonnollinen luku on *alkuluku*, jos sitä ei voida esittää kahden sitä aidosti pienemmän luonnollisen luvun tulona.

Tämä käytäntö ei ole ristiriitainen, jos tulkitaan, että määriteltyä käsitettä ei ole olemassa ilman määrittelevää ominaisuutta.

Matematiikassa *lause* (tai *teoreema*) on ei-ilmeinen toteamus, joka on osoitettu todeksi aksioomia ja aikaisempia lauseita hyväksi käyttäen. *Todistus* on päättelyketju, jolla lauseen totuusarvo voidaan päättelysääntöjen avulla todentaa. Lause on siten deduktiivisesti johdettavissa aksioomista, ts. lause on aksioomien looginen johtopäätös. Lauseita, joita ei pidetä niin merkittävinä, kutsutaan usein *propositioiksi* ja lauseita, joiden rooli on lähinnä toimia tärkeämpien lauseiden todistuksen apuna, kutsutaan *lemmoiksi*. Lauseita, jotka saadaan helposti esimerkiksi yhdistämällä kaksi aikaisempaa lausetta, voidaan kutsua myös *seurauksiksi* (tai *korollaareiksi*).

Lause voi vain todeta ominaisuuden, kuten seuraava lause tekee:

Lause. *Alkulukuja on äärettömän monta.*

Tämä esimerkkilause on lause 5.10. Usein lauseet ovat kuitenkin ehdollisia toteamuksia $P \to Q$ kahden väitelauseen P ja Q välillä. Tässä väitelausetta P sanotaan *oletukseksi* ja väitelausetta Q *väitteeksi*. Seuraava esimerkkilause on lause 5.15.

Lause. *Jos $n \geqslant 3$ on alkuluku, niin n on pariton.*

Jos $P(n) =$ "$n \geqslant 3$ on alkuluku" ja $Q(n) =$ "n on pariton", niin edellinen lause voidaan yhtäpitävästi kirjoittaa muodossa $\forall n : P(n) \to Q(n)$. Kiinnittämällä n saadaan ehdollinen toteamus oletuksen $P(n)$ ja väitteen $Q(n)$ välille. Lauseen todistamiseksi on siis pystyttävä loogisesti päättelemään, että väite on oletuksen johtopäätös eli $P(n) \Rightarrow Q(n)$ millä tahansa luvun n valinnalla. Tapoja tähän voi olla useita. Lauseen väite on siten välttämätön seuraus oletuksista: väite on heti voimassa kunhan vain lauseen oletukset pätevät, ilman mitään lisäoletuksia.

Vaikka lauseet voidaan kirjoittaa symbolisesti käyttäen hyväksi vain predikaattilogiikkaa ja joukko-oppia, johon tutustutaan luvussa 6, niin usein luettavuuden ja ymmärrettävyyden kannalta ne on tapana esittää luonnollista kieltä hyväksi käyttäen. Sama pätee todistuksiin, joiden tarkoitus on loogisesti järjestetyillä arkikielisillä perusteluilla vakuuttaa lukija lauseen totuudesta. Tavoitteena on pyrkiä niin selkeään esitykseen, että lukija voisi halutessaan laajentaa todistuksen formaaliksi symboliseksi loogiseksi päättelyksi – kappaleessa 3.2 esitettyyn tarkkuuteen ei ole tarkoituksenmukaista mennä. Arkikielisten perusteluiden oikeellisuus

on tyypillisesti helpompi tarkistaa kuin symbolisten ja usein todistukset pyritään kirjoittamaan niin, että ne myös jollain tapaa selittävät miksi lause on totta.

Uusien lauseiden löytäminen ja niille todistusten keksiminen on matematiikan tutkimuksen ydin. Määritelmät, lauseet ja todistukset ovat myös olemassa olevan matematiikan ja sen esittämisen keskiössä. Lauseiden tehtävä on toimia hyödyllisinä "mustina laatikoina" ottaen sisään oletukset ja antaen ulos väitteen. Esimerkiksi Pythagoraan lauseelle voidaan antaa mikä tahansa suorakulmainen kolmio ja se kertoo kuinka tämän kolmion kateettien ja hypotenuusan pituudet suhtautuvat toisiinsa. Todistukset kirjoitetaan aina tiettyä kohdeyleisöä varten – aloitteleva matemaatikko tarvinnee enemmän yksityiskohtia kuin pidemmälle edennyt matemaatikko, joka jo tuntee useimmat tavallisimmat todistusmenetelmät.

Lauseisiin ja niiden todistuksiin liitetään usein esteettisiä määritteitä. Niitä voidaan luonnehtia triviaaleiksi, vaikeiksi, syvällisiksi tai kauniiksi. Joskus todistuksen löytäminen on kiinni uuden näkökulman keksimisestä. Esimerkiksi Pythagoraan lauseen todistus on suoraviivainen heti sen jälkeen kun hoksaa tehdä pinta-alatarkasteluja. Seuraavan lauseen väite on helppo ymmärtää, mutta sen todistus on syvällinen.

Lause (Fermat'n suuri lause)**.** *Jos $n \geqslant 3$ on luonnollinen luku, niin ei ole olemassa luonnollisia lukuja a, b ja c siten, että $a^n + b^n = c^n$.*

Fermat[23] esitti väitteen kirjansa marginaalissa vuonna 1637. Se pysyi todistamatta yli 350 vuotta, kunnes Wiles[24] onnistui seitsemän vuoden työnteon jälkeen löytämään sille todistuksen vuonna 1995. Toteamuksia, joiden jostain syystä uskotaan pitävän paikkansa kutsutaan *konjektuureiksi*. Seuraava Goldbachin[25] vuonna 1742 esittämä konjektuuri on yksi lukuteorian vanhimmista ja tunnetuimmista avoimista ongelmista:

Konjektuuri (Goldbachin konjektuuri)**.** *Jos luonnollinen luku $n \geqslant 4$ on parillinen, niin on olemassa alkuluvut p ja q siten, että $p + q = n$.*

[23]Pierre de Fermat (1601–1665)
[24]Andrew Wiles (1953–)
[25]Christian Goldbach (1690–1764)

Lauseen 5.15 mukaan lukua kaksi lukuun ottamatta kaikki alkuluvut ovat parittomia ja lauseen 4.2 kohdan (2) nojalla kahden parittoman kokonaisluvun summa on parillinen. Näin ollen oletus parillisuudesta on välttämätön. Konjektuurille ei ole vielä löydetty todistusta. Laskennallisesti on tarkistettu, että se pitää paikkansa kaikilla luonnollisilla luvuilla $n \leqslant 4 \cdot 10^{18}$. Helfgott[26] esitteli vuonna 2013 todistuksen Goldbachin heikolle konjektuurille, joka väittää, että parittomille luonnollisille luvuille $n \geqslant 7$ on olemassa alkuluvut p, q ja r siten, että $p + q + r = n$. Jos Goldbachin konjektuuri olisi totta, niin heikko konjektuuri seuraisi siitä triviaalisti: jos $n - 3$ on kahden alkuluvun summa, niin n on kolmen alkuluvun summa.

Luentovideo 8

4.1. **Suora todistus.** Suora todistus on

$$P \wedge (P \to Q) \quad \Rightarrow \quad Q.$$

Päättelylause todettiin kohdassa (2.13) tautologiaksi, joten päättely on suorassa todistuksessa looginen. Suorassa todistuksessa siis oletetaan, että P on voimassa, ja sen jälkeen yritetään oletuksen avulla loogisesti päätellä, että väite Q on oletuksen P johtopäätös. Jos tässä onnistutaan, niin myös väite Q pitää paikkansa. Pääpiirteissään lauseen $P \to Q$ todistaminen suoralla todistuksella näyttää aina seuraavalta:

Lause. *Jos P, niin Q.*

Todistus. Oletetaan, että P pitää paikkansa.

$$\vdots$$

Näin ollen myös Q on voimassa. □

Kolmen pisteen tilalle yllä kirjataan päättelyketju, jossa määritelmiä ja tunnettuja lauseita hyväksi käyttäen saadaan oletuksesta P loogisesti pääteltyä väite Q. Tapana on, että todistuksen loppumista merkitään symbolilla □. Vanhemmista teksteistä saattaa myös löytää samaan tarkoitukseen käytetyn lyhenteen QED (ts. quod erat demonstrandum) tai MOT (ts. mikä oli todistettava). Todistus, joka esitettiin Pythagoraan lauseelle luvussa 1 on suora todistus. Käydään seuraavaksi

[26]Harald Andrés Helfgott (1977–)

läpi lisää esimerkkejä suorista todistuksista. Kerrataan sitä varten kuitenkin ensin tuttujen käsitteiden määritelmiä sekä käsitteisiin liittyviä ominaisuuksia.

Luonnolliset luvut ovat $1, 2, 3, \ldots$. Oletuksena siis on, että 1 on luonnollinen luku ja että jokaisella luonnollisella luvulla on seuraaja, joka myös on luonnollinen luku mutta ei ole 1 eikä minkään muun luonnollisen luvun seuraaja. Lisäksi pidetään tunnettuna, että luonnollisten lukujen yhteen- ja kertolaskut ovat edelleen luonnollisia lukuja ja että millä tahansa kokoelmalla luonnollisia lukuja on olemassa pienin alkio luonnollisten lukujen järjestyksen mielessä.

Lukumääräluvut ovat $0, 1, 2, 3, \ldots$ ja *kokonaisluvut* ovat $\ldots, -2, -1, 0, 1, 2, \ldots$. Lukumääräluvut siis saadaan luonnollisista luvuista lisäämällä niihin luku 0 ja kokonaisluvut lisäämällä lukumäärälukuihin jokaisen luonnollisen luvun vastaluku. Kahden kokonaisluvun erotus, joka siis määritellään vastaluvun avulla summana, on siten aina kokonaisluku. *Rationaaliluvut* ovat muotoa $\frac{m}{n}$, missä m on kokonaisluku ja n on luonnollinen luku. Nollasta eroavilla rationaaliluvuilla on siis olemassa rationaalinen käänteisluku. Rationaalilukujen jakolaskussa jaettava kerrotaan jakajan käänteisluvulla ja tulos on aina rationaaliluku. *Reaaliluvut* ajatellaan yksinkertaisuuden vuoksi lukusuoran pisteiksi. Reaalilukuja, jotka eivät ole rationaalisia kutsutaan *irrationaaliluvuiksi*.

Tarkastellaan esimerkinomaisesti kokonaislukujen parillisuutta ja parittomuutta. Painotetaan vielä, että tavoitteena on esitellä todistustekniikoita ja matemaattisen teorian kehittämistä – ei niinkään tuloksia, joista varsinkin ensimmäiset ovat triviaaleja. Sanotaan, että kokonaisluku n on *parillinen*, jos on olemassa kokonaisluku k siten, että $n = 2k$. Vastaavasti sanotaan, että n on *pariton*, jos $n = 2k + 1$ jollakin kokonaisluvulla k. Tavoitteena on siis ymmärtää mitä nämä määritelmät tarkkaan ottaen tarkoittavat ja minkälaisia ominaisuuksia parillisilla ja parittomilla luvuilla on. Mikä on esimerkiksi n:n ensimmäisen parittoman luonnollisen luvun summa? Onko n^2 pariton aina kun n on pariton? Huomataan, että todistukseksi ei riitä laskea neliöitä mistään äärellisestä määrästä parittomia lukuja:

n	1	3	5	7	9	11	13	$\cdots$	21	$\cdots$	101	$\cdots$
n^2	1	9	25	49	81	121	169	$\cdots$	441	$\cdots$	10201	$\cdots$

Tämän tyyppisiä päättelyitä tehdään kuitenkin paljon muissa tieteissä. Esimerkiksi jos tuhannesta suomalaisesta on tiettyä mieltä 600, niin tästä usein vedetään johtopäätös, että jollakin virhemarginaalilla 60 % suomalaisista on tätä mieltä.

Lause 4.1. *(1) Jos kokonaisluku n on parillinen, niin $-n$ on parillinen.*
(2) Jos kokonaisluku n on pariton, niin $-n$ on pariton.

Todistus. Osoitetaan kohta (2) ja jätetään kohta (1) harjoitustehtäväksi. Jos $P(n) =$ "n on pariton" ja $Q(n) =$ "$-n$ on pariton", niin lause voidaan yhtäpitävästi kirjoittaa muodossa $\forall n : P(n) \to Q(n)$. Kiinnittämällä n päästään tekemään suora todistus. Olkoon siis n siten, että $P(n)$ pitää paikkansa, ts. n on pariton kokonaisluku. Tällöin määritelmän mukaan on olemassa kokonaisluku k siten, että $n = 2k+1$. Koska $-n$ voidaan nyt kirjoittaa muodossa $-n = -(2k+1) = -2k-1 = 2(-k-1)+1 = 2l+1$, missä $l = -k-1$ on kokonaisluku, niin määritelmän nojalla myös $-n$ on pariton, ts. $Q(n)$ on voimassa. □

Lause 4.2. *(1) Kahden parillisen kokonaisluvun summa on parillinen.*
(2) Kahden parittoman kokonaisluvun summa on parillinen.
(3) Parillisen ja parittoman kokonaisluvun summa on pariton.

Todistus. Osoitetaan kohta (3) ja jätetään kohdat (1) ja (2) harjoitustehtäviksi. Jos $P(m,n) =$ "m on parillinen ja n on pariton" ja $Q(m,n) =$ "$m+n$ on pariton", niin lause voidaan yhtäpitävästi kirjoittaa muodossa $\forall m,n : P(m,n) \to Q(m,n)$. Kiinnittämällä m ja n päästään tekemään suora todistus. Olkoot siis m ja n siten, että $P(m,n)$ pitää paikkansa, ts. m on parillinen kokonaisluku ja n on pariton kokonaisluku. Tällöin määritelmän mukaan on olemassa kokonaisluvut k ja l siten, että $m = 2k$ ja $n = 2l+1$. Koska summa $m+n$ voidaan nyt kirjoittaa muodossa $m+n = 2k+(2l+1) = 2(k+l)+1$, missä $k+l$ on kokonaisluku, niin määritelmien nojalla $m+n$ on pariton, ts. $Q(m,n)$ on voimassa. □

Seuraus 4.3. *(1) Kahden parillisen kokonaisluvun erotus on parillinen.*
(2) Kahden parittoman kokonaisluvun erotus on parillinen.
(3) Parillisen ja parittoman kokonaisluvun erotus on pariton.

Todistus. Koska $m-n = m+(-n)$ kaikilla kokonaisluvuilla m ja n, niin lauseen väitteet seuraavat suoraan soveltamalla lausetta 4.1 lauseessa 4.2. □

Lause 4.4. *(1) Kahden parillisen kokonaisluvun tulo on parillinen.*
(2) Kahden parittoman kokonaisluvun tulo on pariton.
(3) Parillisen ja parittoman kokonaisluvun tulo on parillinen.

Todistus. Osoitetaan kohta (3) ja jätetään kohdat (1) ja (2) harjoitustehtäväksi. Jos $P(m,n) =$ "m on parillinen ja n on pariton" ja $Q(m,n) =$ "mn on parillinen", niin lause voidaan yhtäpitävästi kirjoittaa muodossa $\forall m,n : P(m,n) \to Q(m,n)$. Kiinnittämällä m ja n päästään tekemään suora todistus. Olkoot siis m ja n siten, että $P(m,n)$ pitää paikkansa, ts. m on parillinen kokonaisluku ja n on pariton kokonaisluku. Tällöin määritelmän mukaan on olemassa kokonaisluvut k ja l siten, että $m = 2k$ ja $n = 2l+1$. Koska tulo mn voidaan nyt kirjoittaa muodossa $mn = 2k(2l+1) = 4kl + 2k = 2(2kl+k)$, missä $2kl+k$ on kokonaisluku, niin määritelmän nojalla mn on parillinen, ts. $Q(m,n)$ on voimassa. □

Seuraava lause antaa positiivisen vastauksen edellä esitettyyn kysymykseen onko n^2 pariton aina kun n on pariton.

Seuraus 4.5. *(1) Parillisen kokonaisluvun neliö on parillinen.*
(2) Parittoman kokonaisluvun neliö on pariton.

Todistus. Lauseen väitteet seuraavat suoraan lauseen 4.4 kohdista (1) ja (2). □

Luentovideo 9

4.2. **Induktiotodistus.** Luonnollisiin lukuihin liittyviä, muotoa $\forall n : Q(n)$ olevia lauseita voidaan todistaa *induktiotodistuksella*:

$$Q(1) \wedge (\forall k : Q(k) \to Q(k+1)) \quad \Rightarrow \quad \forall n : Q(n).$$

Todistuksessa on kolme vaihetta: Ensin *alkuaskeleessa* osoitetaan, että väitelause $Q(1)$ on tosi. Tämän jälkeen tehdään *induktio-oletus* eli kiinnitetään luonnollinen luku k ja oletetaan, että $Q(k)$ pitää paikkansa. Jos induktio-oletuksen avulla onnistutaan loogisesti päättelemään *induktioväite* $Q(k+1)$, niin induktioperiaatteen mukaan $Q(n)$ on voimassa jokaisella luonnollisella luvulla n. Askelta induktio-oletuksesta induktioväitteeseen kutsutaan *induktioaskeleeksi*. Pääpiirteissään lauseen $\forall n : Q(n)$ todistaminen induktiotodistuksella näyttää aina seuraavalta:

Lause. *Jos n on luonnollinen luku, niin $Q(n)$.*

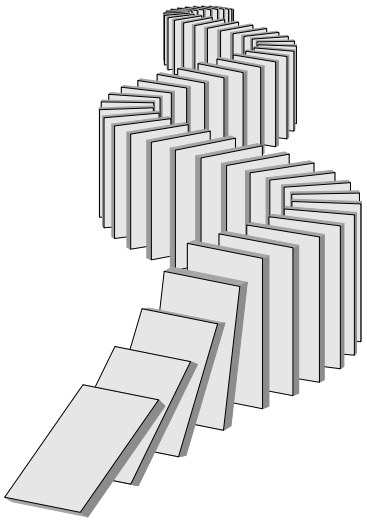
Todistus. Todetaan, että $Q(1)$ on tosi. Kiinnitetään luonnollinen luku k ja oletetaan, että $Q(k)$ pitää paikkansa.

$$\vdots$$

Näin ollen myös $Q(k+1)$ on voimassa. Siispä $Q(n)$ pätee kaikilla n. □

Kolmen pisteen tilalle yllä kirjataan päättelyketju, jossa induktio-oletusta $Q(k)$, tunnettuja lauseita ja loogista päättelyä hyväksi käyttäen saadaan osoitettua induktioväite $Q(k+1)$.

Ajatus induktioperiaatteessa on seuraava: Koska $Q(1)$ pitää paikkansa, niin induktioaskel takaa sen, että myös $Q(2)$ on voimassa. Koska nyt $Q(2)$ pitää paikkansa, niin induktioaskeleeseen toistamiseen vedoten nähdään, että myös $Q(3)$ on voimassa. Näin jatkamalla saadaan induktioperiaatteen mukaan kaikki luonnolliset luvut käytyä läpi. Induktiotodistusta voidaan havainnollistaa helposti dominonappuloiden avulla: Asetetaan äärettömän monta dominonappulaa[27] pystyyn vieri viereen.



Kaatamalla ensimmäinen saadaan ketjureaktiona kaadettua kaikki muutkin.

Induktioperiaate, ts. se, että päättely on induktiotodistuksessa looginen, on itse asiassa seuraus luonnollisten lukujen ominaisuudesta, jonka mukaan millä tahansa kokoelmalla luonnollisia lukuja on olemassa pienin alkio. Tarkastellaan kokoelmaa luonnollisia lukuja n, joille $Q(n)$ ei päde. Jos n_0 on tähän kokoelmaan liittyvä

[27]Oheinen kuva on muokattu Marc Wibrow'n alkuperäisestä (©2014, CC BY 2.5).

pienin alkio, niin täytyy olla $n_0 \geqslant 2$ sillä $Q(1)$ osoitettiin alkuaskeleessa todeksi. Näin ollen $n_0 - 1$ on edelleen luonnollinen luku ja koska n_0 on pienin alkio, jolle $Q(n)$ ei päde, niin väitteen $Q(n_0 - 1)$ täytyy päteä. Mutta koska induktioaskeleen mukaan tästä seuraa se, että väite $Q(n_0)$ pitää paikkansa, niin tällaista luonnollista lukua n_0 ei ole olemassa eikä siten myöskään luonnollisia lukuja n, joille $Q(n)$ ei päde. Siispä väitteen $Q(n)$ täytyy päteä kaikilla luonnollisilla luvuilla n.

Induktioperiaate mahdollistaa käsitteiden määrittelemisen *rekursiivisesti*. Oletetaan, että käsitteelle $K(1)$ on annettu arvo ja jos $k \in \mathbb{N}$, niin määritellään käsitteelle $K(k+1)$ arvo käsitteen $K(k)$ arvon avulla. Käsite $K(n)$ tulee näin määriteltyä induktioperiaatteen nojalla yksikäsitteisesti kaikille $n \in \mathbb{N}$. Esimerkiksi luonnollisen luvun n *kertoma* $n!$ määritellään asettamalla $1! = 1$ ja rekursiivisesti $(k+1)! = k! \cdot (k+1)$ kaikille $k \in \mathbb{N}$. Tällöin esimerkiksi $2! = 1! \cdot 2 = 1 \cdot 2$, $3! = 2! \cdot 3 = 1 \cdot 2 \cdot 3$ ja $10! = 1 \cdot 2 \cdot 3 \cdots 9 \cdot 10$.

Sanotaan, että *aritmeettinen sarja* on äärellisen monen aritmeettisesti kasvavan luvun summa. Lukujono kasvaa *aritmeettisesti*, jos kahden peräkkäisen luvun erotus on vakio.

Lause 4.6 (Aritmeettisen sarjan summakaava)**.** *Jos n on luonnollinen luku, niin*

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

Todistus. Merkitään

$$Q(n) = \text{ ”}1 + 2 + 3 + \cdots + n = \tfrac{1}{2}n(n+1)\text{”}$$

ja osoitetaan induktiotodistuksella, että $Q(n)$ pätee kaikilla luonnollisilla luvuilla n. Koska väitelauseen $Q(1) = \text{ ”}1 = \frac{1}{2} \cdot 1 \cdot (1+1)\text{”}$ totuusarvo on tosi, niin alkuaskel on voimassa. Tehdään induktio-oletus eli kiinnitetään luonnollinen luku k ja oletetaan, että $Q(k)$ on voimassa. Tällöin siis pätee

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}.$$

Induktioväitteenä on osoittaa, että väitelause

$$Q(k+1) = \text{ ”}1 + 2 + 3 + \cdots + k + (k+1) = \tfrac{1}{2}(k+1)(k+2)\text{”}$$

on totuusarvoltaan tosi. Soveltamalla induktio-oletusta induktioväitteessä $Q(k+1)$ esiintyvän yhtälön vasempaan puoleen nähdään, että

$$\begin{aligned} 1+2+3+\cdots+k+(k+1) &= \frac{k(k+1)}{2}+(k+1) \\ &= \frac{k(k+1)+2(k+1)}{2} = \frac{(k+1)(k+2)}{2}. \end{aligned}$$

Näin ollen $Q(k+1)$ on voimassa. Induktioperiaatteen mukaan $Q(n)$ on siis voimassa kaikilla luonnollisilla luvuilla n. □

Esimerkki 4.7. Tarinan mukaan ala-asteen opettaja antoi huonosti käyttäytyneelle Gaussille[28] tehtäväksi laskea luvut $1, \ldots, 100$ yhteen. Opettajan hämmästykseksi nuori Gauss sai oikean vastauksen selville hetkessä. Aritmeettisen sarjan summakaavaan eli lauseeseen 4.6 nojaten tiedetään, että vastaus on

$$1+2+3+\cdots+100 = \frac{100 \cdot 101}{2} = 5\,050.$$

Gaussin menetelmä oli oletettavasti huomata, että listaamalla luvut numerojärjestykseen sekä laskemalla alkupäästä lukien n:s ja loppupäästä lukien n:s luku yhteen antaa aina vastaukseksi 101. Esimerkiksi $1+100 = 101$, $2+99 = 101$ ja $10+91 = 101$. Listassa tällaisia lukupareja on 50 kappaletta, joten lukujen summaksi saadaan $(1+100)+(2+99)+(3+98)+\cdots+(50+51) = 50 \cdot 101 = 5\,050$.

Jotta listan kaikista luvuista saadaan muodostettua parit em. tavalla, niin lukuja pitää olla parillinen määrä. Jos tehtävänä olisi esimerkiksi ollut laskea luvut $1, \ldots, 99$ yhteen, niin tällöin 50 on listan keskimmäinen luku eikä sille ole paria. Muista luvuista voidaan kuitenkin muodostaa 49 paria, joiden luvut yhteen laskemalla saadaan 100. Näin ollen $1+2+3+\cdots+99 = 50+(1+99)+(2+98)+(3+97)+\cdots+(49+51) = 50+49 \cdot 100 = 4\,950$.

Seuraava lause antaa vastauksen aikaisemmin esitettyyn kysymykseen mikä on n:n ensimmäisen parittoman luonnollisen luvun summa.

Lause 4.8. *Jos n on luonnollinen luku, niin*

$$1+3+5+\cdots+(2n-1) = n^2.$$

[28]Johann Carl Friedrich Gauss (1777–1855)

Todistus. Merkitään

$$Q(n) = \text{"}1 + 3 + 5 + \cdots + (2n-1) = n^2\text{"}$$

ja osoitetaan induktiotodistuksella, että $Q(n)$ pätee kaikilla luonnollisilla luvuilla n. Koska väitelauseen $Q(1) = \text{"}1 = 1^2\text{"}$ totuusarvo on tosi, niin alkuaskel on voimassa. Tehdään induktio-oletus eli kiinnitetään luonnollinen luku k ja oletetaan, että $Q(k)$ on voimassa. Tällöin siis pätee

$$1 + 3 + 5 + \cdots + (2k-1) = k^2.$$

Induktioväitteenä on osoittaa, että väitelause

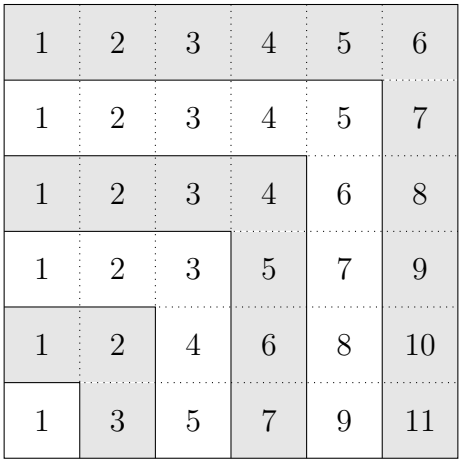
$$Q(k+1) = \text{"}1 + 3 + 5 + \cdots + (2k-1) + (2k+1) = (k+1)^2\text{"}$$

on totuusarvoltaan tosi. Soveltamalla induktio-oletusta induktioväitteessä $Q(k+1)$ esiintyvän yhtälön vasempaan puoleen nähdään, että

$$1 + 3 + 5 + \cdots + (2k-1) + (2k+1) = k^2 + (2k+1) = (k+1)^2.$$

Näin ollen $Q(k+1)$ on voimassa. Induktioperiaatteen mukaan $Q(n)$ on siis voimassa kaikilla luonnollisilla luvuilla n. □

Esimerkki 4.9. Lauseen 4.8 väitettä voidaan havainnollistaa geometrisesti kuten oheisessa kuvassa. Esimerkiksi vasemman alakulman 3×3-ruudukon pinta-ala on



$3^2 = 9$ yksikköä ja se on 5 yksikköä suurempi kuin 2×2-ruudukon pinta-ala $2^2 = 4$.

Todistetaan lause 4.8 esimerkin vuoksi vielä suoralla todistuksella käyttäen hyväksi aritmeettisen sarjan summakaavaa eli lausetta 4.6. Olkoon n luonnollinen luku. Tällöin lauseen 4.6 nojalla nähdään suoraan, että

$$\begin{aligned} 1+3+5+\cdots+(2n-1) &= (2\cdot 1-1)+(2\cdot 2-1)+\cdots+(2n-1) \\ &= (2\cdot 1+2\cdot 2+2\cdot 3+\cdots+2n)-n \\ &= 2(1+2+3+\cdots+n)-n \\ &= 2\frac{n(n+1)}{2}-n = n^2. \end{aligned}$$

Sanotaan, että *geometrinen sarja* on äärellisen monen geometrisesti kasvavan luvun summa. Lukujono kasvaa *geometrisesti*, jos kahden peräkkäisen luvun osamäärä on vakio.

Lause 4.10 (Geometrisen sarjan summakaava)**.** *Jos n on luonnollinen luku ja $\lambda \neq 1$ on reaaliluku, niin*

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

Todistus. Merkitään

$$Q(n) = \text{ ”}1+\lambda+\lambda^2+\cdots+\lambda^{n-1} = (1-\lambda^n)/(1-\lambda)\text{”}$$

ja osoitetaan induktiotodistuksella, että $Q(n)$ pätee kaikilla luonnollisilla luvuilla n. Koska väitelauseen $Q(1) = \text{”}1 = (1-\lambda)/(1-\lambda)\text{”}$ totuusarvo on tosi, niin alkuaskel on voimassa. Tehdään induktio-oletus eli kiinnitetään luonnollinen luku k ja oletetaan, että $Q(k)$ pitää paikkansa. Tällöin siis pätee

$$1+\lambda+\lambda^2+\cdots+\lambda^{k-1} = \frac{1-\lambda^k}{1-\lambda}.$$

Induktioväitteenä on osoittaa, että väitelause

$$Q(k+1) = \text{ ”}1+\lambda+\lambda^2+\cdots+\lambda^{k-1}+\lambda^k = (1-\lambda^{k+1})/(1-\lambda)\text{”}$$

on totuusarvoltaan tosi. Soveltamalla induktio-oletusta induktioväitteessä $Q(k+1)$ esiintyvän yhtälön vasempaan puoleen nähdään, että

$$\begin{aligned} 1+\lambda+\lambda^2+\cdots+\lambda^{k-1}+\lambda^k &= \frac{1-\lambda^k}{1-\lambda}+\lambda^k \\ &= \frac{1-\lambda^k+\lambda^k(1-\lambda)}{1-\lambda} = \frac{1-\lambda^{k+1}}{1-\lambda}. \end{aligned}$$

Näin ollen $Q(k+1)$ on voimassa. Induktioperiaatteen mukaan $Q(n)$ on siis voimassa kaikilla luonnollisilla luvuilla n. □

Esimerkki 4.11. Todistetaan lause 4.10 esimerkin vuoksi vielä suoralla todistuksella: Olkoon n luonnollinen luku ja $\lambda \neq 1$. Koska

$$\begin{aligned} &(1-\lambda)(1+\lambda+\lambda^2+\cdots+\lambda^{n-1}) \\ &\quad = (1+\lambda+\lambda^2+\cdots+\lambda^{n-1}) - \lambda(1+\lambda+\cdots+\lambda^{n-2}+\lambda^{n-1}) \\ &\quad = (1+\lambda+\lambda^2+\cdots+\lambda^{n-1}) - (\lambda+\lambda^2+\cdots+\lambda^{n-1}+\lambda^n) \\ &\quad = 1-\lambda^n, \end{aligned}$$

niin väite seuraa jakamalla luvulla $1-\lambda$.

Esimerkki 4.12. Tarinan mukaan intialainen hallitsija kysyi shakkipelin keksijältä mitä hän halusi pelin kehittämisestä palkkiokseen. Keksijä pyysi ainoastaan niin monta vehnän jyvää kuin saadaan koko shakkilaudalta, kun jyviä asetetaan sen ensimmäiselle ruudulle yksi, toiselle ruudulle kaksi, kolmannelle neljä, neljännelle kahdeksan ja näin jatkamalla jokaiselle ruudulle kaksi kertaa niin monta kuin edelliselle ruudulle. Hallitsija hämmästyi keksijän vaatimatonta pyyntöä ja suostui siihen. Kannattiko pyyntöön suostua?

Shakkilauta on 8×8 ruudukko, joten ruutuja laudalla on yhteensä 64 kappaletta. Näin ollen geometrisen sarjan summakaavan eli lauseen 4.10 mukaan vehnän jyviä tarvittiin

$$1+2+2^2+2^3+\cdots+2^{63} = \frac{1-2^{64}}{1-2} = 2^{64}-1$$

kappaletta. Koska $2^{64} \approx 18{,}4 \cdot 10^{18}$, niin jyvien kokonaislukumäärä on yli 18 triljoonaa. Vehnän jyvän massa on tyypillisesti noin 65 milligrammaa. Palkkio vastaa noin $18{,}4 \cdot 10^{18} \cdot 65$ mg $= 1196 \cdot 10^{18}$ mg $= 1196 \cdot 10^9$ tn eli noin 1196 miljardia tonnia vehnää. Vertailun vuoksi voidaan todeta, että koko maailman vuotuinen

vehnäsato 2010-luvulla oli keskimäärin noin 725 miljoonaa tonnia. Palkkio vastaa siis noin 1650-kertaisesti koko maailman vuotuista vehnäsatoa.

Useamman samankaltaisen termin yhteenlaskua merkitään lyhyemmin merkin $\sum$ avulla. Jos esimerkiksi m ja n ovat kokonaislukuja siten, että $m < n$, ja $a_m, a_{m+1}, \ldots, a_n$ ovat reaalilukuja, niin

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + \cdots + a_n.$$

Geometrisen sarjan summakaava eli lause 4.10 voidaan tällöin, annetulle luonnolliselle luvulle n ja reaaliluvulle $\lambda \neq 1$, esittää muodossa

$$\sum_{i=0}^{n-1} \lambda^i = \frac{1-\lambda^n}{1-\lambda}.$$

Äärettömiä summia voidaan esittää vastaavasti. Jos $\lambda = \frac{1}{2}$, niin näyttäisi, että $\sum_{i=0}^{n} 2^{-i} = 2(1-2^{-n})$ on sitä lähempänä lukua 2 mitä suuremmaksi n valitaan. Vaikuttaisi siis siltä, että $\sum_{i=0}^{\infty} 2^{-i} = 2$. Huomataan kuitenkin, että ääretön summa ei välttämättä ole olemassa, sillä esimerkiksi luvun n kasvaessa summa $\sum_{i=1}^{n}(-1)^{n+1}$ saa vuoron perään arvoja 1 ja 0 sekä lauseen 4.8 mukaan summa $\sum_{i=1}^{n} 2i-1 = n^2$ kasvaa rajatta.

Olkoon $p \geqslant 2$ luonnollinen luku. Jos ei ole olemassa luonnollisia lukuja m ja n siten, että $2 \leqslant m, n \leqslant p-1$ ja $mn = p$, niin sanotaan, että p on *alkuluku*. Huomataan, että pienin alkuluku on 2. Luonnollisella luvulla n on *alkulukuesitys*, jos se voidaan esittää alkulukujen tulona, ts. on olemassa luonnollinen luku k ja alkuluvut $p_1, \ldots, p_k$ siten, että $n = p_1 \cdots p_k$. Lukuja $p_1, \ldots, p_k$ kutsutaan luvun n *alkulukutekijöiksi*. Jokaisella alkuluvulla on triviaalisti alkulukuesitys.

Lause 4.13 (Aritmetiikan peruslause)**.** *Jos n on luonnollinen luku siten, että $n \geqslant 2$, niin luvulla n on alkulukuesitys.*

Todistus. Merkitään

$$Q(n) = \text{ "luonnollisilla luvuilla } 2, \ldots, n+1 \text{ on alkulukuesitys"}$$

ja osoitetaan induktiotodistuksella, että $Q(n)$ pätee kaikilla luonnollisilla luvuilla n. Koska 2 on alkuluku, niin väitelauseen $Q(1)$ = "luonnollisella luvulla 2 on

alkulukuesitys" totuusarvo on tosi ja alkuaskel on voimassa. Tehdään induktio-oletus eli kiinnitetään luonnollinen luku k ja oletetaan, että $Q(k)$ pitää paikkansa. Tällöin siis luonnollisilla luvuilla $2, \ldots, k+1$ on alkulukuesitys. Induktioväitteenä on osoittaa, että väitelause

$$Q(k+1) = \text{ "luonnollisilla luvuilla } 2, \ldots, k+1, k+2 \text{ on alkulukuesitys"}$$

on totuusarvoltaan tosi. Koska induktio-oletuksen mukaan luvuilla $2, \ldots, k+1$ on alkulukuesitys, niin induktioväitteen todistamiseksi riittää osoittaa, että luvulla $k+2$ on alkulukuesitys. Jos $k+2$ on alkuluku, niin näin on triviaalisti. Voidaan siis olettaa, että $k+2$ ei ole alkuluku. Alkuluvun määritelmän mukaan on siis olemassa luonnolliset luvut m ja l siten, että $2 \leqslant m, l \leqslant k+1$ ja $ml = k+2$. Koska induktio-oletuksen nojalla luvuilla m ja l on alkulukuesitykset, niin $k+2 = ml$ on näiden esitysten tulona alkulukujen tulo. Näin ollen $Q(k+1)$ on voimassa ja induktioperiaatteen mukaan $Q(n)$ on voimassa kaikilla luonnollisilla luvuilla n. $\square$

Aritmetiikan peruslause pätee vielä vahvemmassa muodossa. Voidaan nimittäin osoittaa, että luonnollisen luvun alkulukuesitys on yksikäsitteinen. Sivuutetaan tämän todistaminen, mutta todetaan, että väite on mielenkiintoinen: kuinka saadaan tuloja auki laskematta osoitettua, että esimerkiksi alkulukujen tulot $25\,013 \cdot 2\,000\,003$ ja $50\,021 \cdot 1\,000\,099$ ovat eri luku? Alkulukuesityksen yksikäsitteisyys on myös syy miksi lukua 1 ei hyväksytä alkuluvuksi: jos se olisi alkuluku, niin $1 \cdot 2$ ja $1 \cdot 1 \cdot 2$ olisivat molemmat luvun 2 alkulukuesityksiä.

5. Lisää todistamisesta

Luentovideo 10

Kohdan (2.10) nojalla

$$(P \vee R) \to Q \quad \Leftrightarrow \quad (P \to Q) \wedge (R \to Q).$$

Näin ollen ehdollinen toteamus $(P \vee R) \to Q$ on loogisesti yhtäpitävä lauseen $(P \to Q) \wedge (R \to Q)$ kanssa ja siten muotoa $(P \vee R) \to Q$ oleva lause todistetaan osoittamalla ehdolliset toteamukset $P \to Q$ ja $R \to Q$ todeksi. Vaikka lauseen oletus ei olisi muotoa $P \vee R$, niin todistamisen kannalta saattaa olla välttämätöntä jakaa tarkastelu kahteen tai useampaan tapaukseen. Tarkastellaan tällaista tilannetta yksinkertaisen esimerkin avulla. Positiivisen ja negatiivisen luvun tulon

on negatiivinen sekä kahden negatiivisen luvun tulo on positiivinen. Näin ollen seuraavan lauseen todistuksessa on syytä tarkastella positiiviset ja negatiiviset reaaliluvut erikseen.

Lause 5.1. *Jos x on reaaliluku, niin $x^2 \geqslant 0$.*

Todistus. Jos $P(x) =$ "$x \geqslant 0$", niin lause voidaan yhtäpitävästi kirjoittaa muodossa $\forall x : P(x) \vee \neg P(x) \to P(x^2)$. Kiinnittämällä x nähdään, että osoitettavana on kaksi ehdollista toteamusta, $P(x) \to P(x^2)$ ja $\neg P(x) \to P(x^2)$.

Olkoon siis x reaaliluku siten, että $P(x)$ pitää paikkansa, ts. $x \geqslant 0$. Tällöin selvästi $x^2 \geqslant 0$ eli $P(x^2)$ on voimassa. Oletetaan sitten, että x toteuttaa väitelauseen $\neg P(x)$, ts. $x < 0$. Koska $x^2 = (-x)(-x)$ on kahden positiivisen luvun tulo, niin $x^2 \geqslant 0$ eli $P(x^2)$ on jälleen voimassa. Molemmat ehdolliset toteamukset ovat siis voimassa ja siten itse lausekin on voimassa. □

Kohdan (2.2) nojalla

$$P \leftrightarrow Q \quad \Leftrightarrow \quad (P \to Q) \wedge (Q \to P).$$

Näin ollen ehdollinen toteamus $P \leftrightarrow Q$ on loogisesti yhtäpitävä lauseen $(P \to Q) \wedge (Q \to P)$ kanssa ja siten muotoa $P \leftrightarrow Q$ oleva lause todistetaan osoittamalla ehdolliset toteamukset $P \to Q$ ja $Q \to P$ todeksi. Tarkastellaan tällaista tilannetta esimerkin avulla. Seurauksen 4.5 kohdan (2) nojalla tiedetään, että jos kokonaisluku n on pariton, niin myös n^2 on pariton. Esimerkkejä auki laskien näyttäisi, että jos n^2 on pariton, niin myös n on pariton. Vaikuttaa siis siltä, että ehdot olisivat yhtäpitävät. Esitetään tämä konjektuurina:

Konjektuuri 5.2. *(1) Kokonaisluku on parillinen täsmälleen silloin, kun sen neliö on parillinen.*

(2) Kokonaisluku on pariton täsmälleen silloin, kun sen neliö on pariton.

Konjektuurissa esitellään kokonaisluvun parillisuudelle ja parittomuudelle yhtäpitävät ehdot. Konjektuurin todistamiseksi pitää siis osoittaa implikaatiot molempiin suuntiin. Seurauksen 4.5 mukaan toinen implikaatio jo tunnetaan, mutta kuinka toisen suunnan ehdollinen toteamus todistetaan? Jos kokonaisluvun n neliö n^2 on pariton, niin halutaan päätellä, että myös n on pariton. Suorassa todistuksessa

lähdettäisiin liikkeelle oletuksesta: Koska n^2 on pariton ja lauseen 5.1 mukaan positiivinen, niin on olemassa lukumääräluku k siten, että $n^2 = 2k + 1$. Nähdään siis, että $n = \sqrt{2k+1}$. Kuinka tästä voidaan päätellä, että $n = 2l + 1$ jollakin kokonaisluvulla l? Pitääkö konjektuuri edes paikkansa? Tämä selviää seurauksessa 5.14.

Joskus yhtäpitäviä ehtoja on useampi. Ne on tapana esittää kootusti kuten seuraavassa esimerkkilauseessa:

Lause 5.3. *Jos n on kokonaisluku, niin seuraavat ehdot ovat keskenään yhtäpitävät:*

(1) n on pariton,
(2) $n + 1$ on parillinen,
(3) $\frac{1}{2}(n + 1)$ on kokonaisluku.

Todistus. Jätetään lauseessa esiintyvien väitelauseiden täsmällinen selvittäminen harjoitustehtäväksi. Osoitetaan ensin, että kohdasta (1) seuraa kohta (2). Oletetaan siis, että n on pariton. Tällöin on olemassa kokonaisluku k siten, että $n = 2k + 1$. Näin ollen $n + 1 = (2k + 1) + 1 = 2(k + 1)$ on parillinen. Osoitetaan sitten, että kohdasta (2) seuraa kohta (3). Koska $n + 1$ on parillinen, niin on olemassa kokonaisluku l siten, että $n + 1 = 2l$. Näin ollen $\frac{1}{2}(n + 1) = \frac{1}{2} \cdot 2l = l$ on kokonaisluku. Osoitetaan lopuksi, että kohdasta (3) seuraa kohta (1). Koska $\frac{1}{2}(n+1)$ on kokonaisluku, niin merkitsemällä $m = \frac{1}{2}(n + 1)$ nähdään, että $n + 1 = 2m$ eli $n = 2m - 1 = 2(m - 1) + 1$. Näin ollen n on pariton. □

Edellinen lause todistettiin osoittamalla lauseessa esitetyille kohdille implikaatioketju (1) ⇒ (2) ⇒ (3) ⇒ (1). Tämä riittää osoittamaan kaikki ehdot keskenään yhtäpitäviksi: esimerkiksi (1) ⇔ (3), sillä (1) ⇒ (2) ⇒ (3) ja (3) ⇒ (1).

Vaikka muotoa $\forall x : P(x) \to Q(x)$ olevissa lauseissa muutaman esimerkkitilanteen varmistaminen ei riitä todistukseksi, niin usein lauseet ja niiden todistusten ideat löytyvät tekemällä äärellinen määrä havaintoja. Tarkastellaan esimerkkitilannetta, jossa jostain syystä halutaan tarkemmin ymmärtää muotoa $1+(-1)^n(2n-1)$ olevia lukuja. Käydään läpi kymmenen ensimmäistä luonnollista lukua n:

n	1	2	3	4	5	6	7	8	9	10
$1 + (-1)^n(2n - 1)$	0	4	−4	8	−8	12	−12	16	−16	20

Laskettujen havaintojen valossa näyttäisi, että luku $1 + (-1)^n(2n - 1)$ on luvun 4 *monikerta*, ts. se on muotoa $4k$, missä k on jokin kokonaisluku. Voisiko tämä päteä yleisesti? Havainnot eivät tietenkään vielä todista väitettä, mutta kuten konjektuurin 5.2 tapauksessa, ne antavat motivaation tarkastella esitettyä väitettä. Voidaan myös kysyä toisin päin: onko jokainen luvun 4 monikerta esitettävissä muodossa $1 + (-1)^n(2n - 1)$, missä n on jokin luonnollinen luku? Seuraava lause antaa molempiin kysymyksiin positiivisen vastauksen.

Lause 5.4. *Kokonaisluku k on luvun 4 monikerta täsmälleen silloin, kun on olemassa luonnollinen luku n siten, että $k = 1 + (-1)^n(2n - 1)$.*

Todistus. On siis osoitettava seuraavat kaksi lausetta:

(1) Jokaiselle luonnolliselle luvulle n on olemassa kokonaisluku k siten, että $1 + (-1)^n(2n - 1) = 4k$.
(2) Jokaiselle kokonaisluvulle k on olemassa luonnollinen luku n siten, että $1 + (-1)^n(2n - 1) = 4k$.

Jätetään lauseissa esiintyvien väitelauseiden täsmällinen selvittäminen harjoitustehtäväksi. Osoitetaan ensin kohta (1). Olkoon siis n luonnollinen luku. Lauseen 5.11 mukaan n on joko parillinen tai pariton. Oletetaan ensin, että n on parillinen. Tällöin on olemassa kokonaisluku k siten, että $n = 2k$. Lisäksi $(-1)^n = 1$. Näin ollen $1+(-1)^n(2n-1) = 1+(2(2k)-1) = 4k$ on luvun 4 monikerta. Oletetaan sitten, että n on pariton, jolloin $(-1)^n = -1$ ja on olemassa kokonaisluku k siten, että $n = 2k+1$. Näin ollen tässäkin tapauksessa $1 + (-1)^n(2n - 1) = 1 - (2(2k + 1) - 1) = 4(-k)$ on luvun 4 monikerta.

Osoitetaan sitten kohta (2). Olkoon k kokonaisluku, jolloin on kolme vaihtoehtoa: $k = 0$, k on luonnollinen luku tai k on negatiivinen kokonaisluku. Jos $k = 0$, niin valitsemalla $n = 1$ nähdään, että $(-1)^n = -1$ ja $1 + (-1)^n(2n - 1) = 1 - (2 - 1) = 0 = 4\cdot 0$. Jos taas k on luonnollinen luku, niin valitsemalla $n = 2k$ nähdään, että n on parillinen luonnollinen luku, $(-1)^n = 1$ ja $1 + (-1)^n(2n - 1) = 1 + (2(2k) - 1) = 4k$. Lopuksi, jos k on negatiivinen kokonaisluku, niin valitsemalla $n = 1 - 2k$ nähdään, että $n = 2(-k)+1$ on pariton luonnollinen luku, $(-1)^n = -1$ ja $1+(-1)^n(2n-1) = 1 - (2(1 - 2k) - 1) = 4k$. □

Usein annetut määritelmät johtavat kysymykseen käsitteiden olemassaolosta. Esimerkiksi reaaliluvut määritellään lukusuoran pisteiksi ja irrationaaliluvut ovat reaalilukuja, jotka eivät ole rationaalisia. Onko irrationaalilukuja olemassa? Mitä jos kaikki reaaliluvut olisivatkin rationaalilukuja? Lauseessa 5.17 tullaan näkemään, että näin ei ole. Osoittamalla, että $\sqrt{2}$ ei ole rationaaliluku, lause näyttää, että irrationaalilukuja on olemassa. Olemassaolon takaava lause on muotoa $\exists x : Q(x)$. Sen todistamiseksi pitää siis osoittaa, että on olemassa x_0, jolle $Q(x_0)$ on voimassa.

Lause 5.5. *On olemassa luonnollinen luku n, joka voidaan esittää kahdella tavalla kahden luonnollisen luvun kuution summana.*

Todistus. Jos $Q(n) =$ "n voidaan esittää kahdella tavalla kahden luonnollisen luvun kuution summana", niin lause voidaan yhtäpitävästi kirjoittaa muodossa $\exists n : Q(n)$. Koska $1^3 + 12^3 = 1729 = 9^3 + 10^3$, niin valitsemalla $n_0 = 1729$ nähdään, että $Q(n_0)$ on voimassa. Siten kohdan (3.2) mukaan $\exists n : Q(n)$ on tosi. □

Tarinan mukaan Hardy[29] vieraili Ramanujanin[30] luona sairaalassa. Hardy mainitsi tulleensa taksilla numero 1729 ja sanoi sen olevan varsin tylsä luku. Ramanujan vastasi heti, että ei se ole tylsä luku – se on pienin kokonaisluku, joka on esitettävissä kahden positiivisen kuution summana kahdella eri tavalla.

Edellisessä lauseessa olemassaolo voitiin perustella konkreettisella valinnalla. Usein tämä ei ole mahdollista kuten seuraavan lauseen todistus havainnollistaa.

Lause 5.6. *On olemassa irrationaaliluvut x ja y siten, että x^y on rationaalinen.*

Todistus. Jos $Q(x, y) =$ "x ja y ovat irrationaalilukuja ja x^y on rationaaliluku", niin lause voidaan yhtäpitävästi kirjoittaa muodossa $\exists x, y : Q(x, y)$. Olkoot $x = \sqrt{2}^{\sqrt{2}}$ ja $y = \sqrt{2}$. Lauseen 5.17 mukaan y on irrationaaliluku. Jos x on irrationaaliluku, niin

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$$

on rationaaliluku. Jos taas x on rationaaliluku, niin $y^y = \sqrt{2}^{\sqrt{2}}$ on rationaaliluku. Näin ollen joko $Q(x, y)$ tai $Q(y, y)$ on voimassa ja siten kohdan (3.2) mukaan $\exists x, y : Q(x, y)$ on tosi. □

[29] Godfrey Harold Hardy (1877–1947)
[30] Srinivasa Ramanujan (1887–1920)

Edellisen lauseen todistuksessa oletettiin tunnetuksi lauseen 5.17 havainto, että $\sqrt{2}$ on irrationaaliluku. Huomautetaan, että matematiikan deduktiivisen rakenteen vuoksi tällainen "eteenpäin viittaaminen" ei ole suositeltavaa. Riskinä on se, että jos lauseen 5.17 todistus tarvitsisi lausetta 5.6, niin syntyisi *kehäpäätelmä*. Onneksi tässä tapauksessa näin ei ole, kuten lukija voi helposti tarkistaa.

Jos on olemassa täsmälleen yksi x_0, jolle $Q(x_0)$ on voimassa, niin sanotaan, että on olemassa *yksikäsitteinen* x, jolle $Q(x)$ pätee. Esimerkiksi aritmetiikan peruslauseen eli lauseen 4.13 yhteydessä todettiin, vaikkakaan ei todistettu, että luonnollisen luvun alkulukuesitys on yksikäsitteinen. Olemassaolon yksikäsitteisyyttä usein merkitään symbolisesti lisäämällä olemassaolokvanttorin perään huutomerkki, $\exists! x : Q(x)$. Alkion x_0 yksikäsitteisyyden todistamiseksi pitää siis osoittaa, että $Q(x_0)$ on tosi ja kaikilla $x \neq x_0$ väitelause $Q(x)$ on epätosi, ts. $\forall x \neq x_0 : \neg Q(x)$ pätee.

Tarkastellaan konjektuuria $\forall x : P(x) \to Q(x)$. Sillä on kaksi vaihtoehtoa, se on joko tosi tai epätosi. Lauseen todeksi osoittamiseksi on jo esitelty erilaisia menetelmiä ja tullaan esittelemään vielä muutama lisää. Mutta kuinka konjektuuri voidaan todistaa vääräksi? Halutaan siis osoittaa, että molekyylilause $\neg\forall x : P(x) \to Q(x)$ on tosi. Muistaen, että kohdan (2.7) nojalla $\neg(P \to Q) \leftrightarrow (P \wedge \neg Q)$, negaation ja kvanttoreiden vaihtosäännön eli kohdan (3.3) mukaan tämä on loogisesti yhtäpitävää sen kanssa, että $\exists x : P(x) \wedge \neg Q(x)$ on tosi. Näin ollen konjektuuri voidaan osoittaa vääräksi näyttämällä, että on olemassa alkio x, jolle $P(x) \wedge \neg Q(x)$ pitää paikkansa. Tällaista alkiota kutsutaan *vastaesimerkiksi*.

Konjektuuri 5.7. *Jos n on luonnollinen luku, niin $n^2 - n + 41$ on alkuluku.*

Jos $Q(n) =$ "$n^2 - n + 41$ on alkuluku", niin konjektuuri voidaan yhtäpitävästi kirjoittaa muodossa $\forall n : Q(n)$. Ahkeran laskemisen[31] jälkeen nähdään, että $Q(n)$ pätee 40:lle ensimmäiselle luonnolliselle lukuvulle n:

n	1	2	3	4	5	6	$\cdots$	10	$\cdots$	20	$\cdots$	40
$n^2 - n + 41$	41	43	47	53	61	71	$\cdots$	131	$\cdots$	421	$\cdots$	1601

[31] Yksinkertaisimmillaan voi laittaa tietokoneen tarkistamaan, että $(n^2 - n + 41)/k$ ei ole kokonaisluku millään luonnollisilla luvuilla $k \leqslant \sqrt{n^2 - n + 41}$ ja $n \leqslant 40$.

Laskettujen esimerkkien valossa näyttäisi siltä, että $n^2 - n + 41$ on alkuluku kaikilla luonnollisilla luvuilla n. Voisiko näin olla? Negaation ja kvanttoreiden vaihtosäännön eli kohdan (3.3) mukaan konjektuuri nähdään vääräksi osoittamalla $\exists n : \neg Q(n)$ todeksi. Toisin sanoen, konjektuurin vääräksi osoittamiseen riittää löytää yksi luonnollinen luku n, jolle $Q(n)$ ei ole totta. Vastaesimerkiksi kelpaa esimerkiksi $n = 41$, sillä tällä valinnalla $n^2 - n + 41 = 41 \cdot 41 = 1681$ ei ole alkuluku. Konjektuuri 5.7 ei siten pidä paikkaansa.

Esitellään seuraavaksi lisää tapoja todistaa muotoa $P \to Q$ olevia lauseita.

Luentovideo 11

5.1. **Käänteinen suora todistus.** Kohdan (2.6) nojalla

$$P \to Q \quad \Leftrightarrow \quad \neg Q \to \neg P.$$

Näin ollen ehdollinen toteamus $P \to Q$ on loogisesti yhtäpitävä lauseen $\neg Q \to \neg P$ kanssa. Käänteinen suora todistus on

$$P \wedge (\neg Q \to \neg P) \quad \Rightarrow \quad Q.$$

Päättelylause todettiin kohdassa (2.14) tautologiaksi, joten päättely on käänteisessä suorassa todistuksessa looginen. Käänteisessä suorassa todistuksessa siis oletetaan, että sekä oletus P että väitteen negaatio $\neg Q$ eli *antiteesi* ovat voimassa, ja sen jälkeen yritetään antiteesin $\neg Q$ avulla loogisesti päätellä, että oletuksen negaatio $\neg P$ on antiteesin $\neg Q$ johtopäätös. Jos tässä onnistutaan, niin ollaan ristiriitaisesti saatu P ja $\neg P$ yhtäaikaa voimaan. Näin ollen antiteesi $\neg Q$ ei voi olla totta ja väite Q pitää paikkansa. Pääpiirteissään lauseen $P \to Q$ todistaminen käänteisellä suoralla todistuksella näyttää aina seuraavalta:

Lause. *Jos P, niin Q.*

Todistus. Oletetaan, että P ja $\neg Q$ pitävät paikkansa.

$$\vdots$$

Siispä $\neg P$ on tosi, mikä on ristiriita. Näin ollen Q on voimassa. □

Kolmen pisteen tilalle yllä kirjataan päättelyketju, jossa määritelmiä ja tunnettuja lauseita hyväksi käyttäen saadaan antiteesista $\neg Q$ loogisesti pääteltyä oletuksen

negaatio $\neg P$. Tarkastellaan käänteistä suoraa todistusta seuraavan esimerkkilauseen avulla:

Lause 5.8. *Jos reaaliluvuille x ja y pätee $y^3 - x^3 \leqslant xy^2 - yx^2$, niin tällöin $y \leqslant x$.*

Todistus. Jos $P(x, y) =$ "$y^3 - x^3 \leqslant xy^2 - yx^2$" ja $Q(x, y) =$ "$y \leqslant x$", niin lause voidaan yhtäpitävästi kirjoittaa muodossa $\forall x, y : P(x, y) \to Q(x, y)$. Kiinnittämällä x ja y päästään tekemään käänteinen suora todistus. Olkoot siis reaaliluvut x ja y siten, että oletus $P(x, y)$ ja antiteesi $\neg Q(x, y)$ pitävät paikkansa. Koska tällöin $y > x$, niin $y - x > 0$. Kertomalla tätä epäyhtälöä puolittain positiivisella luvulla $x^2 + y^2$ nähdään, että

$$yx^2 + y^3 - x^3 - xy^2 = (y - x)(x^2 - y^2) > 0.$$

Näin ollen $y^3 - x^3 > xy^2 - yx^2$, ts. $\neg P(x, y)$ pätee. Tämä on ristiriita oletuksen $P(x, y)$ kanssa ja siten $Q(x, y)$ on voimassa, ts. $y \leqslant x$. □

5.2. **Epäsuora todistus.** Kohdan (2.8) nojalla

$$R \quad \Leftrightarrow \quad \neg R \to (S \wedge \neg S).$$

Jos väitelauseen R paikalle kirjoitetaan lause $P \to Q$, niin muistaen, että kohdan (2.7) mukaan $\neg(P \to Q) \Leftrightarrow (P \wedge \neg Q)$, yllä oleva voidaan kirjoittaa muodossa

$$P \to Q \quad \Leftrightarrow \quad (P \wedge \neg Q) \to (S \wedge \neg S).$$

Näin ollen ehdollinen toteamus $P \to Q$ on loogisesti yhtäpitävä lauseen $(P \wedge \neg Q) \to (S \wedge \neg S)$ kanssa. Epäsuora todistus on

$$P \wedge ((P \wedge \neg Q) \to (S \wedge \neg S)) \quad \Rightarrow \quad Q.$$

Päättelylause todettiin kohdassa (2.15) tautologiaksi, joten päättely on epäsuorassa todistuksessa looginen. Epäsuorassa todistuksessa siis oletetaan, että sekä oletus P että antiteesi $\neg Q$ ovat voimassa ja sen jälkeen yritetään näiden avulla loogisesti päätellä jokin ristiriita $S \wedge \neg S$. Jos tässä onnistutaan, niin antiteesi $\neg Q$ ei voi olla totta ja väite Q pitää paikkansa. Käänteisessä suorassa todistuksessa tavoitteena on löytää ristiriita oletuksen kanssa, mutta epäsuorassa todistuksessa ristiriidaksi

kelpaa mikä vaan. Pääpiirteissään lauseen $P \to Q$ todistaminen käänteisellä suoralla todistuksella näyttää aina seuraavalta:

Lause. *Jos P, niin Q.*

Todistus. Oletetaan, että P ja $\neg Q$ pitävät paikkansa.

$$\vdots$$

Siispä löydettiin väitelause S siten, että S ja $\neg S$ ovat yhtäaikaa totta. Tämä on ristiriita, joten väite Q on voimassa. □

Kolmen pisteen tilalle yllä kirjataan päättelyketju, jossa määritelmiä ja tunnettuja lauseita hyväksi käyttäen saadaan oletuksesta P ja antiteesista $\neg Q$ loogisesti pääteltyä jokin ristiriita $S \wedge \neg S$. Huomataan, että käänteinen suora todistus on epäsuoran todistuksen erikoistapaus: siinä ristiriitana on $P \wedge \neg P$. Tarkastellaan epäsuoraa todistusta seuraavan esimerkkilauseen avulla:

Lause 5.9. *Ei ole olemassa reaalilukua $x > 0$, jolle $x + \frac{1}{x} < 2$.*

Todistus. Jos $P(x) =$ "$x > 0$" ja $Q(x) =$ "$x + \frac{1}{x} \geqslant 2$", niin lause voidaan yhtäpitävästi kirjoittaa muodossa $\forall x : P(x) \to Q(x)$. Kiinnittämällä x päästään tekemään epäsuora todistus. Olkoon siis reaaliluku x siten, että oletus $P(x)$ ja antiteesi $\neg Q(x)$ pitävät paikkansa, ts. $x > 0$ ja $x + \frac{1}{x} < 2$. Kertomalla epäyhtälö $x + \frac{1}{x} < 2$ puolittain luvulla $x > 0$ nähdään, että

$$x^2 + 1 < 2x.$$

Tästä seuraa suoraan, että

$$(x-1)^2 = x^2 - 2x + 1 < 0.$$

Näin ollen väitelause $S(x) =$ "$(x-1)^2 < 0$" on tosi. Lauseen 5.1 mukaan $(x-1)^2 \geqslant 0$, joten myös väitelause $\neg S(x) =$ "$(x-1)^2 \geqslant 0$" on tosi. Tämä on ristiriita, joten antiteesi $\neg Q(x)$ ei voi olla totta ja väite $Q(x)$ pitää paikkansa, ts. $x + \frac{1}{x} \geqslant 2$. □

Luentovideo 12

5.3. **Alkuluvuista ja irrationaaliluvuista.** Aritmetiikan peruslauseeseen eli lauseeseen 4.13 nojautuen voidaan epäsuoralla todistuksella osoittaa, että alkulukuja on äärettömän monta. Edellisissä kappaleissa todistuksiin kirjattiin lauseissa

esiintyvät väitelauseet. Tästä eteenpäin niiden täsmällinen selvittäminen jätetään lukijalle.

Lause 5.10. *Alkulukuja on äärettömän monta.*

Todistus. Osoitetaan väite epäsuoralla todistuksella. Tehdään siis antiteesi ja oletetaan, että alkulukuja on äärellinen määrä. Muistetaan, että pienin alkuluku on 2. Merkitään alkulukujen lukumäärää luonnollisella luvulla k ja olkoot alkuluvut $p_1, \ldots, p_k$. Määritellään

$$p = p_1 \cdots p_k + 1$$

ja huomataan, että p ei ole alkuluku: koska selvästi $p > p_i$ kaikilla i, niin p ei ole yksikään alkuluvuista $p_1, \ldots, p_k$. Näin ollen aritmetiikan peruslauseen eli lauseen 4.13 mukaan se voidaan esittää kahden tai useamman alkuluvun tulona. Siten luku p jaettuna em. tulossa esiintyvällä alkuluvulla on erityisesti luonnollinen luku. Mutta suoralla jakolaskulla nähdään, että

$$\frac{p}{p_i} = p_1 \cdots p_{i-1} p_{i+1} \cdots p_k + \frac{1}{p_i}$$

ei ole luonnollinen luku millään i. Tämä ristiriita osoittaa, että antiteesi ei voi olla oikein. Siispä alkulukuja on äärettömän monta. □

Huomautetaan, että ristiriita edellisen lauseen todistuksessa löydettiin hyvin erikoisella tavalla. Jatketaan seuraavaksi kokonaislukujen parillisuuden ja parittomuuden tarkastelua. Muistetaan, että kokonaisluku n on parillinen (tai vastaavasti pariton), jos on olemassa kokonaisluku k siten, että $n = 2k$ (tai vastaavasti $n = 2k + 1$). On varmasti yleisesti tunnettua, että jokainen kokonaisluku on joko parillinen tai pariton. Mutta kuinka tämä tieto seuraa määritelmistä? Parillisuus ja parittomuus määritellään antamalla molemmille käsitteille määrittelevä ominaisuus. Määritelmistä ei suoraan näy kuinka käsitteet suhtautuvat toisiinsa. Seuraava lause selvittää tämän täsmällisesti:

Lause 5.11. *Jokainen kokonaisluku on joko parillinen tai pariton.*

Todistus. Lauseessa on todistettavana kaksi väitettä. On ensinnäkin näytettävä, että jokainen kokonaisluku on välttämättä parillinen tai pariton. Lisäksi pitää osoittaa, että mikään kokonaisluku ei voi olla parillinen ja pariton yhtäaikaa.

Osoitetaan ensin, että jokainen kokonaisluku on parillinen tai pariton. Huomataan, että 0 on parillinen. Riittää osoittaa väite luonnollisille luvuille, sillä tällöin väite seuraa negatiivisille kokonaisluvuille lauseesta 4.1. Tehdään epäsuora todistus ja oletetaan vastoin väitettä, että on olemassa luonnollisia lukuja, jotka eivät ole parillisia eikä parittomia. Olkoon n näistä luvuista pienin. Tällöin $n-1$ on parillinen tai pariton. Jos $n-1$ on parillinen, niin on olemassa kokonaisluku k siten, että $n-1=2k$. Näin ollen $n=2k+1$ eli n on pariton. Jos taas $n-1$ on pariton, niin $n-1=2k+1$ jollakin kokonaisluvulla k ja siten $n=2k+2=2(k+1)$ eli n on parillinen. Oli $n-1$ kumpi tahansa, parillinen tai pariton, niin ollaan päädytty ristiriitaan sen kanssa, että n ei ole kumpaakaan. Näin ollen luonnollisia lukuja, jotka eivät ole parillisia eikä parittomia, ei ole olemassa.

Osoitetaan sitten, että mikään kokonaisluku ei voi olla parillinen ja pariton yhtäaikaa. Osoitetaan väite epäsuoralla todistuksella. Tehdään antiteesi ja oletetaan, että on olemassa kokonaisluku n, joka on parillinen ja pariton. On siis olemassa kokonaisluvut k ja l siten, että $n=2k+1$ ja $n=2l$. Tällöin

$$0=n-n=2l-(2k+1)=2(l-k)-1$$

eli $l-k=\frac{1}{2}$. Tämä on kuitenkin mahdotonta, sillä kahden kokonaisluvun erotus on aina kokonaisluku. Näin ollen ei ole olemassa kokonaislukuja, jotka olisivat yhtäaikaa parillisia ja parittomia. □

Lause 5.12. *(1) Jos kahden kokonaisluvun summa tai erotus on parillinen, niin luvut ovat joko molemmat parillisia tai molemmat parittomia.*

(2) Jos kahden kokonaisluvun summa tai erotus on pariton, niin luvuista toinen on parillinen ja toinen pariton.

Todistus. Osoitetaan kohta (1) käänteisellä suoralla todistuksella. Tehdään antiteesi ja lauseeseen 5.11 vedoten oletetaan, että luvuista toinen on parillinen ja toinen pariton. Tällöin lauseen 4.2 kohdan (3) ja seurauksen 4.3 kohdan (3) nojalla niiden summa ja erotus ovat parittomia, mikä on ristiriidassa oletuksen kanssa. Siten antiteesi ei voi olla voimassa ja väite pätee.

Osoitetaan sitten kohta (2) käänteisellä suoralla todistuksella. Tehdään antiteesi ja lauseeseen 5.11 vedoten oletetaan, että luvut ovat joko molemmat parillisia tai

molemmat parittomia. Tällöin lauseen 4.2 kohtien (1) ja (2) sekä seurauksen 4.3 kohtien (1) ja (2) nojalla niiden summa ja erotus ovat parillisia, mikä on ristiriidassa oletuksen kanssa. Siten antiteesi ei voi olla voimassa ja väite pätee. □

Lause 5.13. *(1) Jos kahden kokonaisluvun tulo on parillinen, niin joko molemmat luvut ovat parillisia tai sitten luvuista toinen on parillinen ja toinen pariton.*
(2) Jos kahden kokonaisluvun tulo on pariton, niin molemmat luvut ovat parittomia.

Todistus. Osoitetaan kohta (1) käänteisellä suoralla todistuksella. Tehdään antiteesi ja lauseeseen 5.11 vedoten oletetaan, että molemmat luvut ovat parittomia. Tällöin lauseen 4.4 kohdan (2) nojalla niiden tulo on pariton, mikä on ristiriidassa oletuksen kanssa. Siten antiteesi ei voi olla voimassa ja väite pätee.

Osoitetaan sitten kohta (2) käänteisellä suoralla todistuksella. Tehdään antiteesi ja lauseeseen 5.11 vedoten oletetaan, että joko molemmat luvut ovat parillisia tai sitten luvuista toinen on parillinen ja toinen pariton. Tällöin lauseen 4.4 kohtien (1) ja (3) nojalla niiden tulo on parillinen, mikä on ristiriidassa oletuksen kanssa. Siten antiteesi ei voi olla voimassa ja väite pätee. □

Seuraava lause osoittaa, että konjektuuri 5.2 pitää paikkansa.

Seuraus 5.14. *(1) Kokonaisluku on parillinen täsmälleen silloin, kun sen neliö on parillinen.*
(2) Kokonaisluku on pariton täsmälleen silloin, kun sen neliö on pariton.

Todistus. Lauseen väitteet seuraavat suoraan seurauksen 4.5 ja lauseen 5.13 kohdista (1) ja (2). □

Lause 5.15. *Lukuun ottamatta lukua* 2*, jokainen alkuluku on pariton.*

Todistus. Osoitetaan väite käänteisellä suoralla todistuksella. Tehdään antiteesi ja lauseeseen 5.11 vedoten oletetaan, että on olemassa lukua 2 suurempi parillinen alkuluku; olkoon se p. Koska p on parillinen, niin on olemassa luonnollinen luku k siten, että $p = 2k$. Jos $k = 1$, niin $2 = p \geqslant 3$, mikä on mahdotonta. Jos taas $k > p - 1$ eli $k \geqslant p$, niin $p = 2k \geqslant 2p$ eli $1 \geqslant 2$, mikä myös on mahdotonta. Siten

$p = 2k$ jollakin luonnollisella luvulla k, jolle $2 \leqslant k \leqslant p - 1$, eli p ei ole alkuluku. Tämä on ristiriita oletuksen kanssa. Siten antiteesi ei päde ja lukua 2 suurempia parillisia alkulukuja ei ole olemassa. □

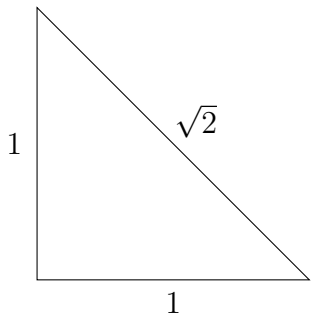
Lause 5.16. *Jos x on nollasta eroava rationaaliluku, niin on olemassa kokonaisluku m ja luonnollinen luku n siten, että ainakin toinen luvuista on pariton ja $x = \frac{m}{n}$.*

Todistus. Olkoon $x \neq 0$ rationaaliluku. Tarkastellaan luonnollisia lukuja l, joille on olemassa nollasta eroava kokonaisluku k siten, että $x = \frac{k}{l}$. Koska x on rationaalinen, niin tällaisia lukuja l on olemassa. Olkoon n näistä luvuista pienin ja olkoon m nollasta eroava kokonaisluku siten, että $x = \frac{m}{n}$. Osoitetaan, että toinen luvuista m tai n on pariton. Tehdään antiteesi ja oletetaan, että m ja n ovat molemmat parillisia. Tällöin on olemassa nollasta eroava kokonaisluku p ja luonnollinen luku q siten, että $m = 2p$ ja $n = 2q$. Näin ollen

$$x = \frac{m}{n} = \frac{p}{q}.$$

Koska $q < n$, niin tämä on ristiriita luvun n minimaalisuuden kanssa. □

Osoitetaan seuraavaksi, että on olemassa ainakin yksi irrationaaliluku. Koska



Pythagoraan lauseen eli lauseen 1.1 mukaan on olemassa $\sqrt{2}$-pituinen jana, niin luku $\sqrt{2}$ löytyy lukusuoralta eli se on reaaliluku.

Lause 5.17. *Reaaliluku $\sqrt{2}$ on irrationaalinen.*

Todistus. Osoitetaan väite epäsuoralla päättelyllä. Muodostetaan antiteesi eli oletetaan vastoin väitettä, että $\sqrt{2}$ on rationaalinen. Koska selvästi $\sqrt{2} \neq 0$, niin lauseen

5.16 mukaan on olemassa kokonaisluku m ja luonnollinen luku n siten, että ainakin toinen luvuista on pariton ja $\sqrt{2} = \frac{m}{n}$. Näin ollen $2 = \sqrt{2}^2 = \left(\frac{m}{n}\right)^2 = \frac{m^2}{n^2}$ eli

$$2n^2 = m^2$$

ja m^2 on parillinen. Siten seurauksen 5.14 kohdan (1) mukaan myös m on parillinen. On siis olemassa kokonaisluku k siten, että $m = 2k$. Näin ollen

$$m^2 = (2k)^2 = 4k^2.$$

Yhdistämällä edelliset yhtälön nähdään, että $n^2 = 2k^2$. Näin ollen luku n^2 on parillinen ja seurauksen 5.14 kohdan (1) mukaan myös n on parillinen. Tämä on ristiriita, sillä toisen luvuista n ja m piti olla pariton. □

6. Joukko-oppia

Joukko-oppi on predikaattilogiikkaa laajempi järjestelmä ja se tutkii alkioiden muodostamia kokoelmia eli joukkoja. Joukko-oppia voidaan pitää modernin matematiikan perustana, esimerkiksi reaaliluvut ja kuvauksen käsite voidaan täsmällisesti määritellä sen avulla. Se tarjoaa myös tehokkaat välineet matematiikan tekemiseen ja esittämiseen. Joukko-opin kehittäjänä voidaan pitää Cantoria[32].

6.1. **Joukko ja alkio.** Sovitaan, että *joukko* koostuu kokoelmasta alkioita. Vaaditaan myös, että joukko ei voi olla itsensä alkio. Alkio x joko kuuluu joukkoon A, jolloin merkitään $x \in A$, tai sitten x ei kuulu joukkoon A, jolloin merkitään $x \notin A$. Käytetään myös terminologiaa, että x sisältyy tai ei sisälly joukkoon A. Edellä esitelty sopimus on tarkkaan ottaen kehäpäätelmä, sillä matematiikassa joukko ja kokoelma tarkoittavat samaa asiaa, ja se johtaa helposti ongelmiin. Tarkastellaan esimerkiksi kaikkien mahdollisten joukkojen muodostamaa kokoelmaa. Sopimuksen mukaan tämä kokoelma on joukko, eikä se siten voi sisältyä itseensä. Näin ollen on olemassa joukko, joka ei sisälly kaikkien joukkojen muodostamaan kokoelmaan. Tätä ristiriitaa kutsutaan *Cantorin paradoksiksi*. Cantorin määritelmä joukolle on

Luentovideo 13

[32]Georg Ferdinand Ludwig Philipp Cantor (1845–1918)

alussa esitelty sopimus ja tähän liityvää joukko-oppia kutsutaan *naiiviksi joukko-opiksi*. Siinä ajatellaan, että käsitteet joukko ja alkio ovat itsestään selviä. Joukkoja, jonka alkiot ovat joukkoja kutsutaan *kokoelmiksi* tai *perheiksi*.

Joukko voidaan määritellä luettelemalla sen kaikki alkiot. Merkintä

$$\{x_1, x_2, \ldots, x_n\}$$

tarkoittaa joukkoa, jonka alkiot ovat $x_1, x_2, \ldots, x_n$. *Tyhjä joukko* $\emptyset$ on joukko, jolla ei ole yhtään alkiota. Huomataan, että joukko $\{\emptyset\}$ ei ole tyhjä, sillä se sisältää tyhjän joukon $\emptyset$. Luonnollisten lukujen, lukumäärälukujen ja kokonaislukujen muodostamat joukot ovat

$$\begin{aligned}\mathbb{N} &= \{1, 2, 3, \ldots\},\\ \mathbb{N}_0 &= \{0, 1, 2, 3, \ldots\},\\ \mathbb{Z} &= \{\ldots, -2, -1, 0, 1, 2, \ldots\}.\end{aligned}$$

Esimerkki 6.1. (1) Kotimaisten kielten tutkimuskeskuksen vuosina 1995–2004 kirjoittaman Ison suomen kieliopin mukaan joukko $\{\mathrm{a}, \mathrm{e}, \mathrm{i}, \mathrm{o}, \mathrm{u}, \mathrm{y}, \ä, \ö\}$ sisältää kaikki suomen kielen vokaalit ja joukko $\{\mathrm{d}, \mathrm{h}, \mathrm{j}, \mathrm{k}, \mathrm{l}, \mathrm{m}, \mathrm{n}, \mathrm{ng}, \mathrm{p}, \mathrm{r}, \mathrm{s}, \mathrm{t}, \mathrm{v}\}$ kaikki konsonantit. Vierassanoja kirjoitettaessa voidaan suomessa tarvita lisäksi ainakin joukon $\{\mathrm{b}, \mathrm{c}, \mathrm{f}, \mathrm{g}, \mathrm{q}, \š, \mathrm{w}, \mathrm{x}, \mathrm{z}\}$ konsonantteja sekä joukon $\{\å, \ü\}$ vokaaleja.

(2) Binäärijärjestelmässä luvut esitetään käyttäen hyväksi joukon $\{0, 1\}$ alkioita eli bittejä. Tällaisen järjestelmän toteuttaminen elektronisilla piireillä on suoraviivaista. Heksadesimaalijärjestelmässä lukujen esittämiseen on käytössä joukon $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F}\}$ alkiot. Molempia järjestelmiä käytetään yleisesti tietotekniikassa, sillä yksi heksadesimaalijärjestelmän merkki vastaa suoraan binäärijärjestelmän neljää peräkkäistä bittiä. Näin esimerkiksi 8-bittisen binääriluvun eli tavun arvo voidaan ilmaista kahden merkin pituisella heksadesimaaliluvulla. Heksadesimaaliluvut siis suoraviivaisesti antavat binääriluvuille helpommin luettavan esityksen.

Joukko voidaan määritellä myös ilmoittamalla sen määrittelevä ominaisuus. Jos $P(x)$ on alkioon x liittyvä avoin väitelause, niin naiivissa joukko-opissa se määrittelee joukon A väitelauseen $\forall x : x \in A \leftrightarrow P(x)$ totuuden kautta. Tällöin

merkitään

$$A = \{x : P(x)\},$$

joka luonnollisessa kielessä luetaan "joukko A koostuu kaikista niistä pisteistä x, jotka toteuttavat ehdon $P(x)$". Toisin sanoen,

$$x \in \{x' : P(x')\} \quad \Leftrightarrow \quad \text{"}P(x) \text{ on tosi"}. \tag{6.1}$$

Usein halutaan, että joukon A alkiot ovat jonkun tilanteeseen sopivan *perusjoukon* X alkioita. Tällöin merkitään $A = \{x \in X : P(x)\}$. Merkitään reaalilukujen muodostamaa joukkoa symbolilla $\mathbb{R}$, jolloin rationaalilukujen joukko on

$$\begin{aligned}\mathbb{Q} &= \{x : \text{on olemassa } m \in \mathbb{Z} \text{ ja } n \in \mathbb{N} \text{ siten, että } x = \tfrac{m}{n}\} \\ &= \{x \in \mathbb{R} : x = \tfrac{m}{n} \text{ joillakin } m \in \mathbb{Z} \text{ ja } n \in \mathbb{N}\}.\end{aligned}$$

Huomautetaan, että joukon esitystapa ei välttämättä ole yksikäsitteinen: esimerkiksi $\{1, 2\} = \{2, 1\} = \{n \in \mathbb{N} : n < 3\} = \{x \in \mathbb{R} : x^2 = 3x - 2\}$. Jos $a, b \in \mathbb{R}$ siten, että $a < b$, niin määritellään *reaalilukuvälit* asettamalla

$$\begin{aligned}[a, b] &= \{x \in \mathbb{R} : a \leqslant x \leqslant b\}, \\ (a, b] &= \{x \in \mathbb{R} : a < x \leqslant b\}, \\ [a, b) &= \{x \in \mathbb{R} : a \leqslant x < b\}, \\ (a, b) &= \{x \in \mathbb{R} : a < x < b\}.\end{aligned} \tag{6.2}$$

Sanotaan, että väli $[a, b]$ on *suljettu*, väli (a, b) on *avoin* sekä välit $[a, b)$ ja $(a, b]$ ovat *puoliavoimia*. Avointa väliä voidaan myös merkitä $]a, b[$ sekä puoliavoimia $[a, b[$ ja $]a, b]$. Määritellään myös *äärettömät välit* asettamalla

$$\begin{aligned}[a, \infty) &= \{x \in \mathbb{R} : x \geqslant a\}, \\ (a, \infty) &= \{x \in \mathbb{R} : x > a\}, \\ (-\infty, b] &= \{x \in \mathbb{R} : x \leqslant b\}, \\ (-\infty, b) &= \{x \in \mathbb{R} : x < b\}.\end{aligned}$$

Voidaan myös merkitä $(-\infty, \infty) = \mathbb{R}$.

Esimerkki 6.2. (1) Jos $n \in \mathbb{N}$, niin luonnollisten lukujen k, joille $k \leqslant n$, muodostama joukko on

$$[n] = \{k \in \mathbb{N} : k \leqslant n\} = \{k \in \mathbb{Z} : k \in [1, n]\} = \{1, 2, \ldots, n-1, n\}.$$

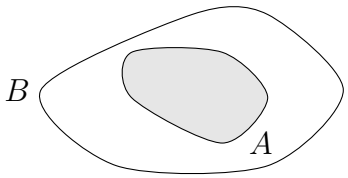
(2) Parillisten kokonaislukujen joukko on

$$\begin{aligned} E &= \{n \in \mathbb{Z} : n = 2k \text{ jollakin } k \in \mathbb{Z}\} \\ &= \{2k \in \mathbb{Z} : k \in \mathbb{Z}\} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\} \end{aligned}$$

ja parittomien

$$\begin{aligned} O &= \{n \in \mathbb{Z} : n = 2k+1 \text{ jollakin } k \in \mathbb{Z}\} \\ &= \{2k+1 \in \mathbb{Z} : k \in \mathbb{Z}\} = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}. \end{aligned}$$

Sanotaan, että joukko A on joukon B *osajoukko*, jos jokainen joukon A alkio kuuluu joukkoon B. Tällöin merkitään $A \subset B$, missä $\subset$ on *inkluusio*, ja sanotaan



myös, että "A sisältyy joukkoon B" tai "B sisältää joukon A". Toisin sanoen,

$$A \subset B \quad \Leftrightarrow \quad (\forall x : x \in A \to x \in B). \tag{6.3}$$

Esimerkiksi $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Harjoitellaan seuraavan lauseen avulla joukkojen inkluusion todistamista.

Lause 6.3. *Jos $a, b \in \mathbb{R}$ siten, että $a < b$, niin $(a, b) \subset [a, b]$.*

Todistus. Olkoot $a, b \in \mathbb{R}$ siten, että $a < b$. Kohdan (6.3) mukaan $(a, b) \subset [a, b]$ ja $\forall x : x \in (a, b) \to x \in [a, b]$ ovat loogisesti yhtäpitävät. On siis osoitettava, että jokaiselle $x \in (a, b)$ on voimassa $x \in [a, b]$. Olkoon siis $x \in (a, b)$. Muistetaan, että avoimen välin määritelmän (6.2) mukaan $(a, b) = \{x \in \mathbb{R} : a < x < b\}$. Näin ollen kohdan (6.1) nojalla pätee $a < x < b$. Koska tällöin triviaalisti pätee myös $a \leqslant x \leqslant b$, niin suljetun välin määritelmän (6.2) ja kohdan (6.1) mukaan $x \in [a, b]$, mikä pitikin osoittaa. □

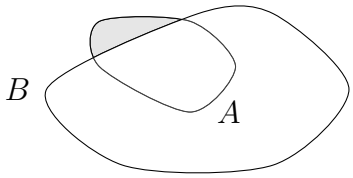
Todistuksessa käytetty menetelmä pätee yleisesti. Jos $P(x)$ ja $Q(x)$ ovat alkioon x liittyviä avoimia väitelauseita sekä $A = \{x : P(x)\}$ ja $B = \{x : Q(x)\}$ niitä vastaavat joukot, niin inkluusion $A \subset B$ todistamiseksi pitää osoittaa, että jokainen x, joka toteuttaa ehdon $P(x)$, toteuttaa myös ehdon $Q(x)$. Toisin sanoen, kohtien (6.3) ja (6.1) mukaan

$$\{x : P(x)\} \subset \{x : Q(x)\} \quad \Leftrightarrow \quad \forall x : P(x) \to Q(x). \tag{6.4}$$

Jos A tai B on määritelty alkiot luettelemalla, niin inkluusion todistaminen on vielä suoraviivaisempaa. Huomataan, että jokainen joukko sisältyy itseensä, ts. $A \subset A$ aina kun A on joukko, ja että tyhjä joukko sisältyy mihin tahansa joukkoon, ts. $\emptyset \subset A$ aina kun A on joukko. Lisäksi, kun A, B ja C ovat joukkoja siten, että $A \subset B \subset C$, niin kohtien (6.3) ja (2.11) mukaan $A \subset C$. Jos A ei ole joukon B osajoukko, niin merkitään $A \not\subset B$. Kohdan (6.3), negaation ja kvanttoreiden vaihtosääntöjen eli kohdan (3.3) sekä kohdan (2.7) mukaan

$$A \not\subset B \quad \Leftrightarrow \quad \exists x : x \in A \wedge x \notin B. \tag{6.5}$$

Jos siis on olemassa joukon A alkio, joka ei kuulu joukkoon B, niin A ei ole joukon



B osajoukko. Esimerkiksi $[a, b] \not\subset (a, b)$ millään $a < b$, sillä $a, b \in [a, b]$ ja $a, b \notin (a, b)$ kaikilla $a, b \in \mathbb{R}$. Lauseessa 5.17 todettiin, että $\mathbb{R} \not\subset \mathbb{Q}$. Lisäksi on helppo nähdä, että $\mathbb{Q} \not\subset \mathbb{Z} \not\subset \mathbb{N}_0 \not\subset \mathbb{N}$.

Jos joukot A ja B ovat toistensa osajoukot, niin sanotaan, että ne ovat *samat* ja merkitään $A = B$. Toisin sanoen,

$$A = B \quad \Leftrightarrow \quad A \subset B \wedge B \subset A. \tag{6.6}$$

Joukot siis osoitetaan samoiksi todistamalla inkluusiot molempiin suuntiin. Vaikka inkluusio on osittainen järjestys, joka määritellään kappaleessa 7.2, niin ei ole tapana sanoa, että A ja B ovat yhtäsuuret. Termi yhtäsuuruus kun saatetaan helposti käsittää niin, että joukoilla A ja B on yhtä paljon alkioita. Se, että joukot

ovat samat on vahvempi vaatimus. Kohtien (6.6), (6.3), (3.5) ja (2.2) mukaan

$$A = B \quad \Leftrightarrow \quad \forall x : x \in A \leftrightarrow x \in B, \tag{6.7}$$

joten joukot ovat samat vain, ja ainoastaan silloin, kun niillä on täsmälleen samat alkiot. Jos joukot A ja B eivät ole samat, niin merkitään $A \neq B$. Kohdan (6.6), De Morganin lakien eli kohdan (2.3) sekä kohtien (6.5) ja (3.6) mukaan

$$A \neq B \quad \Leftrightarrow \quad \exists x : (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A). \tag{6.8}$$

Näin ollen jos löytyy joukon A alkio, joka ei kuulu joukkoon B tai toisin päin, niin joukot A ja B eivät ole samat. Jos $A \neq \emptyset$, niin sanotaan, että A on *epätyhjä*. Tällöin joukossa A on olemassa alkio $x \in A$. Tämä myös nähdään kohdan (6.8) avulla.

Cantorin paradoksin ristiriidasta päästään eroon olettamalla, että kaikkien joukkojen muodostamaa joukkoa ei ole olemassa. *Russellin*[33] *paradoksi* kuitenkin osoittaa, että naiivi joukko-oppi ei silti ole pelastettavissa. Kuten edellä todettiin, naiivissa joukko-opissa avoin väitelause $P(x)$ määrittää joukon $\{x : P(x)\}$. Russelin paradoksissa asetetaan $P(x) =$ "x ei kuulu joukkoon x". Tällöin $R = \{x : P(x)\}$ on joukko ja siten joko $R \in R$ tai $R \notin R$. Vaikka naiivissa joukko-opissa vaaditaan, että joukko ei voi olla itsensä alkio, niin näytetään silti, että molemmat vaihtoehdot johtavat ristiriitaan. Jos $R \in R$, niin kohdan (6.1) mukaan $P(R)$ on tosi eli täytyy päteä $R \notin R$, mikä on ristiriita. Jos taas $R \notin R$, niin vastaavasti kohdan (6.1) mukaan $P(R)$ on epätosi eli $R \in R$ pätee ja taas päädyttiin ristiriitaan. Joukon R olemassaolo aiheuttaa siis naiivissa joukko-opissa ristiriidan.

Esimerkki 6.4 (Parturiparadoksi). Russellin paradoksin idean voi esittää havainnollisesti seuraavalla esimerkillä. Kylässä on miesparturi, joka ajaa parran täsmälleen niiltä kylän miehiltä, jotka eivät itse aja omaa partaansa. Jos parturi ajaa oman partansa, niin parturin täytyy tällöin olla yksi niistä miehistä, jotka eivät itse aja omaa partaansa. Jos taas parturi ei aja omaa partaansa, niin parturi on yksi niistä miehistä, jotka eivät itse aja omaa partaansa, ja siten parturin kuuluu ajaa oma partansa.

[33]Bertrand Arthur William Russell (1872–1970)

Russellin paradoksi oli alkusysäys aksiomaattisen joukko-opin kehittämiselle. Tavoitteena oli löytää aksioomajärjestelmä, jonka tuottama joukko-oppi noudattaa naiivin joukko-opin intuitiota, mutta välttää sen ristiriidat. Sen lopulta kehittivät Zermelo[34] ja Fraenkel[35] käyttäen hyväksi vain predikaattilogiikka ja alkiorelaatiota $\in$. Käsite relaatio määritellään luvussa 7. Aksiomaattista joukko-oppia voidaankin pitää modernin matematiikan perustana. Järjestelmässä on yhdeksän aksioomaa ja yksi niistä on erotteluaksiooma. Se sallii joukkojen muodostamisen avoimilla väitelauseilla vain annetuilla perusjoukoilla ja aksiomaattinen joukko-oppi välttää näin Russellin paradoksin. Toinen mainitsemisen arvoinen aksiooma on valinta-aksiooma. Se olettaa, että mistä tahansa kokoelmasta epätyhjiä joukkoja voi muodostaa joukon valitsemalla alkion jokaisesta kokoelman joukosta. Valinta-aksiooma on aksioomana erikoinen, sillä Gödel[36] onnistui todistamaan vuonna 1940, että se ei ole ristiriidassa joukko-opin muiden aksioomien kanssa. Myöhemmin vuonna 1963 Cohen[37] osoitti, että sitä ei myöskään voi todistaa oikeaksi lähtemällä muusta joukko-opista. Gödelin vuonna 1931 osoittaman epätäydellisyyslauseen mukaan matematiikassa on väitteitä, joita ei pystytä todistamaan. Cohenin tulos siis näyttää, että valinta-aksiooma on esimerkki tällaisesta väitteestä. Valinta-aksiooma on yhteydessä hyvän järjestyksen periaatteeseen, jonka mukaan mikä tahansa joukko voidaan järjestää niin, että sen jokaisella osajoukolla on pienin alkio. Järjestyksen käsite määritellään kappaleessa 7.2. Esimerkiksi luonnollisilla luvuilla on tämä ominaisuus. Valinta-aksiooma vaikuttaa päivänselvältä ominaisuudelta, mutta reaaliluvuilla pienimmän alkion olemassaolo jonkun järjestyksen suhteen vaikuttaa kummalliselta. Bona[38] onkin lausunut, että valinta-aksiooma on ilmiselvästi totta ja hyvän järjestyksen periaate on ilmiselvästi väärin. Vitsi tässä on siinä, että valinta-aksiooma ja hyvän järjestyksen periaate ovat loogisesti yhtäpitävät.

Aksiomaattista joukko-oppia ei tarkastella tämän enempää. Riittää tietää, että joukko-oppia varten on olemassa aksioomajärjestelmä, jolla onnistutaan välttämään naiivin joukko-opin paradoksit. Huomautetaan myös, että joukko-opin merkitys

[34]Ernst Friedrich Ferdinand Zermelo (1871–1953)
[35]Abraham Halevi Fraenkel (1891–1965)
[36]Kurt Friedrich Gödel (1906–1978)
[37]Paul Joseph Cohen (1934–2007)
[38]Jerry Lloyd Bona (1945–)

matematiikassa on pääsääntöisesti olla työväline. Näin ollen matemaatikon ei välttämättä tarvitse olla syvällisesti perehtynyt aksiomaattiseen joukko-oppiin – naiivi joukko-oppi riittää antamaan tarvittavat välineet.

Luentovideo 14

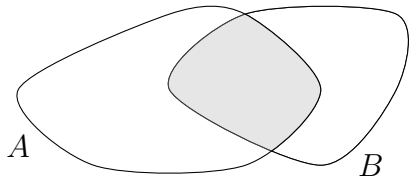
6.2. **Joukko-opin operaatiot.** Joukon A *komplementti* on joukko

$$A^c = \{x : x \notin A\}. \tag{6.9}$$

Kohdan (6.1) mukaan $x \in A^c$ täsmälleen silloin, kun $x \notin A$. Loogisista konnektiiveista komplementti vastaa negaatiota. Joukon komplementtiin sisältyvät kaikki ne alkiot, jotka eivät kuulu itse joukkoon. Joukkojen A ja B *leikkaus* on joukko

$$A \cap B = \{x : x \in A \text{ ja } x \in B\}. \tag{6.10}$$

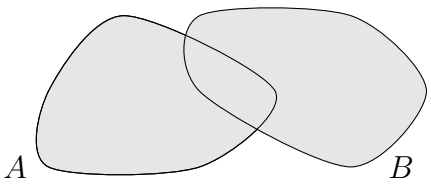
Kohdan (6.1) mukaan $x \in A \cap B$ täsmälleen silloin, kun $x \in A$ ja $x \in B$. Leikkaus siis vastaa konjunktiota. Oheisessa joukkojen A ja B leikkausta havainnollistavassa



kuvassa avoimen väitelauseen $x \in A \wedge x \in B$ totuusarvo on tosi kaikilla tummennetun alueen alkioilla x. Esimerkiksi $A \cap A = A$, $A \cap A^c = \emptyset$ ja $A \cap \emptyset = \emptyset$ millä tahansa joukolla A. Huomataan myös, että $A \cap B = \{x \in A : x \in B\} = \{x \in B : x \in A\}$. Joukkojen A ja B *yhdiste* on joukko

$$A \cup B = \{x : x \in A \text{ tai } x \in B\}. \tag{6.11}$$

Kohdan (6.1) mukaan $x \in A \cup B$ täsmälleen silloin, kun $x \in A$ tai $x \in B$. Näin ollen yhdiste vastaa disjunktiota. Oheisessa joukkojen A ja B yhdistettä

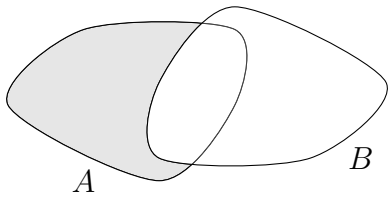


havainnollistavassa kuvassa avoimen väitelauseen $x \in A \vee x \in B$ totuusarvo on

tosi kaikilla tummennetun alueen alkioilla x. Esimerkiksi $A \cup A = A$ ja $A \cup \emptyset = A$ millä tahansa joukolla A. Joukkojen A ja B *erotus* on joukko

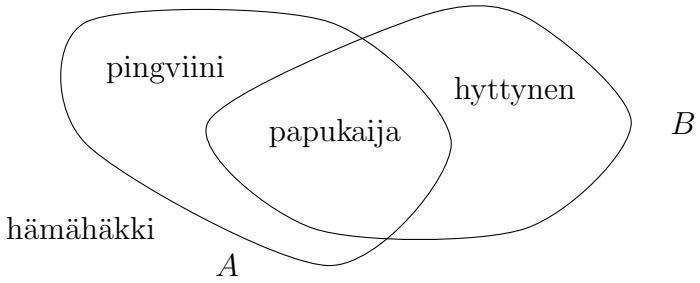
$$A \setminus B = \{x : x \in A \text{ ja } x \notin B\}.$$

Kohdan (6.1) mukaan $x \in A \setminus B$ täsmälleen silloin, kun $x \in A$ ja $x \notin B$. Näin ollen



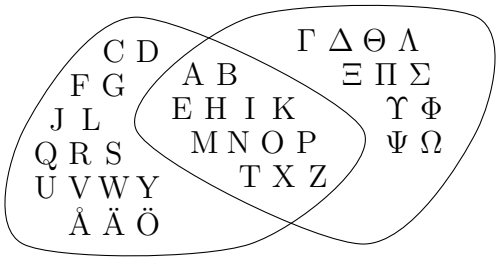
leikkauksen ja komplementin määritelmiin eli kohtiin (6.10) ja (6.9) nojautuen nähdään, että $A \setminus B = A \cap B^c$. Usein joukon A komplementilla A^c tarkoitetaan joukkoa $X \setminus A$ jonkun perusjoukon X suhteen. Tällöin $A \cup A^c = A \cup (X \setminus A) = X$. Esimerkiksi rationaalilukujen komplementilla $\mathbb{Q}^c$ yleensä viitataan irrationaalilukujen joukkoon $\mathbb{R} \setminus \mathbb{Q}$, jolloin $\mathbb{Q} \cup \mathbb{Q}^c = \mathbb{R}$.

Esimerkki 6.5. (1) Olkoon A kaikkien kaksijalkaisten ja B kaikkien lentävien olioiden muodostama joukko. Tällöin esimerkiksi pingviini kaksijalkaisena oliona, joka ei



osaa lentää, sisältyy joukkoon $A \setminus B$, ts. se sisältyy joukkoon A, mutta ei joukkoon B. Hyttynen taas kuusijalkaisena lentävänä oliona kuuluu joukkoon $B \setminus A$ ja papukaija kaksijalkaisena lentävänä oliona sisältyy joukkoon $A \cap B$. Kaikki edellä mainitut oliot kuuluvat joukkoon $A \cup B$ kun taas hämähäkki on sen komplementissa.

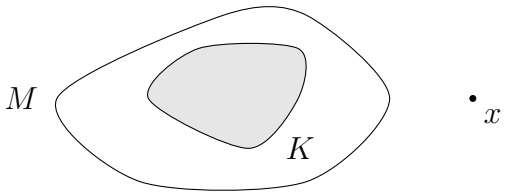
(2) Suomen kielen suuraakkosten joukko on {A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, Å, Ä, Ö} ja kreikan kielen suuraakkosten joukko on {A, B, Γ, Δ, E, Z, H, Θ, I, K, Λ, M, N, Ξ, O, Π, P, Σ, T, Υ, Φ, X, Ψ, Ω}. Oheinen kuva havainnollistaa näiden joukkojen leikkausta ja erotuksia.



Esimerkki 6.6. Tarkastellaan esimerkin 3.1 päättelyä joukko-opin avulla. Olkoon $K = \{x : x \text{ on kurssin osallistuja}\}$ ja $M = \{x : x \text{ pitää matematiikasta}\}$. Tällöin päättelylause (3.7) voidaan joukko-opin merkinnöin kirjoittaa seuraavasti:

$$(K \subset M) \wedge (M^c \neq \emptyset) \quad \Rightarrow \quad K^c \neq \emptyset.$$

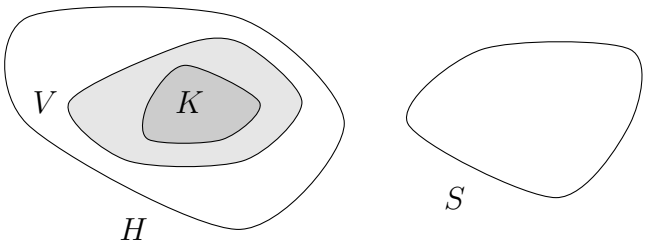
Koska $M^c \neq \emptyset$, niin on olemassa $x \notin M$. Näin ollen päättelyn loogisuutta voidaan helposti havainnollistaa oheisella kuvalla:



Tarkastellaan myös esimerkin 3.2 päättelyä joukko-opin avulla. Olkoon $K = \{x : x \text{ on kolibri}\}$, $V = \{x : x \text{ on värikäs}\}$, $S = \{x : x \text{ on suuri lintu}\}$ ja $H = \{x : x \text{ elää hunajalla}\}$. Tällöin päättelylause (3.8) voidaan joukko-opin merkinnöin kirjoittaa seuraavasti:

$$(K \subset V) \wedge (H \cap S = \emptyset) \wedge (H^c \subset V^c) \quad \Rightarrow \quad K \subset S^c.$$

Päättelyn loogisuutta voidaan nyt helposti havainnollistaa oheisella kuvalla:



Jos komplementointi, leikkaaminen ja yhdistäminen ajatellaan laskutoimituksiksi, niin seuraavat lauseet esittelevät niille laskusääntöjä. Ne ovat analogiset negaation, konjunktion ja disjunktion vastaavien laskusääntöjen kanssa, jotka esiteltiin kappaleessa 2.2 loogisina yhtäpitävyyksinä. Itse asiassa joukko-opin laskusäännöt seuraavat näistä tautologioista. Sanotaan, että annetun perusjoukon osajoukot varustettuna näillä laskutoimituksilla muodostavat *algebran*. Kuten loogisten konnektiivien kanssa, *vaihdantalait*

$$\begin{aligned} A \cap B &= B \cap A, \\ A \cup B &= B \cup A \end{aligned} \tag{6.12}$$

sekä *liitäntälait*

$$\begin{aligned} (A \cap B) \cap C &= A \cap (B \cap C), \\ (A \cup B) \cup C &= A \cup (B \cup C) \end{aligned} \tag{6.13}$$

ovat määritelmien triviaaleja seurauksia ja niiden todistukset jätetään harjoitustehtäviksi. Seuraava lause antaa *De Morganin lait* joukoille. Lauselogiikan De Morganin lait esiteltiin kohdassa (2.3).

Lause 6.7 (De Morganin lait)**.** *Jos A ja B ovat joukkoja, niin*

$$\begin{aligned} (A \cap B)^c &= A^c \cup B^c, \\ (A \cup B)^c &= A^c \cap B^c. \end{aligned}$$

Todistus. Osoitetaan, että $(A \cap B)^c = A^c \cup B^c$ pitää paikkansa ja jätetään toinen väite harjoitustehtäväksi. Kohdan (6.7) mukaan pitää siis osoittaa, että $\forall x : x \in (A \cap B)^c \leftrightarrow x \in A^c \cup B^c$ on tosi. Kiinnitetään x ja huomataan, että komplementin määritelmän eli kohdan (6.9) mukaan $x \in (A \cap B)^c$ täsmälleen silloin, kun $x \notin A \cap B$. Näin ollen $x \in (A \cap B)^c$ on väitelauseen $x \in A \cap B$ negaatio. Koska leikkauksen määritelmän eli kohdan (6.10) mukaan $x \in A \cap B$ täsmälleen silloin, kun $x \in A \wedge x \in B$, niin lauselogiikan De Morganin lakien eli kohdan (2.3) mukaan

$$\neg(x \in (A \cap B)) \quad \Leftrightarrow \quad \neg(x \in A) \vee \neg(x \in B).$$

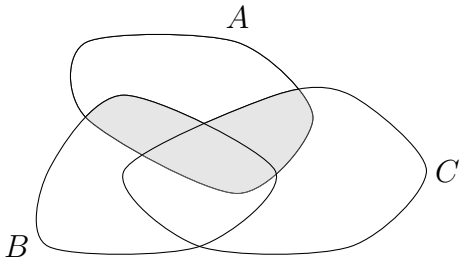
Koska $\neg(x \in A) \vee \neg(x \in B)$ komplementin määritelmän mukaan täsmälleen silloin, kun $x \in A^c \vee x \in B^c$, ja edelleen yhdisteen määritelmän eli kohdan (6.11) mukaan täsmälleen silloin, kun $x \in A^c \cup B^c$, niin väite pätee. □

Seuraava lause taas antaa *osittelulait* joukoille. Lauselogiikan osittelulait esiteltiin kohdassa (2.9).

Lause 6.8 (Osittelulait)**.** *Jos A, B ja C ovat joukkoja, niin*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Todistus. Osoitetaan, että $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ pitää paikkansa ja jätetään toinen väite harjoitustehtäväksi. Oheinen kuva havainnollistaa väitteen



joukkoa. Kohdan (6.6) mukaan on siis todistettava, että

(1) $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$,
(2) $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$.

Osoitetaan ensin kohta (1). Muistaen kohta (6.3) kiinnitetään $x \in A \cap (B \cup C)$, jolloin leikkauksen määritelmän eli kohdan (6.10) mukaan $x \in A$ ja $x \in B \cup C$. Koska $x \in B \cup C$, niin yhdisteen määritelmän eli kohdan (6.11) mukaan $x \in B$ tai $x \in C$. Jos $x \in B$, niin edellisen nojalla $x \in A \cap B$. Jos taas $x \in C$, niin vastaavasti $x \in A \cap C$. Näin ollen, koska $x \in A$ ja $x \in B \cup C$, niin $x \in (A \cap B) \cup (A \cap C)$. Siispä kohta (1) pätee.

Osoitetaan sitten kohta (2). Olkoon $x \in (A \cap B) \cup (A \cap C)$, jolloin $x \in A \cap B$ tai $x \in A \cap C$. Jos $x \in A \cap B$, niin $x \in A$ ja $x \in B$. Näin ollen $x \in A$ ja $x \in B \cup C$ eli $x \in A \cap (B \cup C)$. Jos taas $x \in A \cap C$, niin $x \in A$ ja $x \in C$. Siten tässäkin tapauksessa $x \in A$ ja $x \in B \cup C$ eli $x \in A \cap (B \cup C)$. Siispä kohta (2) pätee. □

Huomataan, että De Morganin lait joukoille eli lause 6.7 todistettiin kohdan (6.7) avulla listaamalla loogisesti yhtäpitäviä ehtoja sille, että alkio sisältyy joukkoon. Todistus siis palautuu suoraan lauselogiikan De Morganin lakeihin eli kohtaan (2.3). Joukkojen osittelulakien eli lauseen 6.8 todistus oltaisiin voitu tehdä vastaavasti. Usein kuitenkin samoiksi on todistettavana joukot, jotka on muodostettu avoimista väitelauseista. Näin ollen, lähes poikkeuksetta, joukot kannattaa todistaa samoiksi kuten lauseen 6.8 todistuksessa eli kohtaan (6.6) vedoten osoittamalla inkluusiot molempiin suuntiin.

6.3. **Useamman joukon leikkaus ja yhdiste.** Liitäntälakien eli kohdan (6.13) ja vaihdantalakien eli kohdan (6.12) mukaan kolmea joukkoa leikatessa tai yhdistettäessä operaatioiden järjestyksellä ei ole väliä. Näin ollen voidaan määritellä useamman joukon leikkaus ja yhdiste. Jos $n \in \mathbb{N}$, niin joukkojen $A_1, A_2, \ldots, A_n$ *leikkaus* on

Luentovideo 15

$$\bigcap_{i=1}^{n} A_i = \{x : x \in A_i \text{ kaikilla } i \in \{1, \ldots, n\}\}$$

ja *yhdiste* on

$$\bigcup_{i=1}^{n} A_i = \{x : x \in A_i \text{ jollakin } i \in \{1, \ldots, n\}\}.$$

Tällöin kohtien (6.1), (3.1) ja (3.4) sekä leikkauksen ja yhdisteen määritelmien eli kohtien (6.10) ja (6.11) mukaan pätee

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n,$$

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n.$$

Äärettömän joukon $A_1, A_2, A_3, \ldots$ *leikkaus* on

$$\bigcap_{i=1}^{\infty} A_i = \{x : x \in A_i \text{ kaikilla } i \in \mathbb{N}\}$$

ja *yhdiste* on

$$\bigcup_{i=1}^{\infty} A_i = \{x : x \in A_i \text{ jollakin } i \in \mathbb{N}\}.$$

Korostetaan, että esimerkiksi $\bigcap_{i=1}^{\infty} A_i$ on vain merkintä joukolle $\{x : P(x)\}$, missä $P(x) =$ "$x \in A_i$ kaikilla $i \in \mathbb{N}$". Siten kohdan (6.1) mukaan $x \in \bigcap_{i=1}^{\infty} A_i$ täsmälleen silloin, kun $P(x)$ on voimassa. Sanotaan, että laajentamalla joukko-opin laskutoimitukset äärettömän joukon leikkauksella ja yhdisteellä annetun perusjoukon osajoukot muodostavat *σ-algebran*.

Edellä määriteltiin leikkaus ja yhdiste kokoelmien $\{A_i\}_{i=1}^n$ ja $\{A_i\}_{i\in\mathbb{N}}$ joukoille. Näissä kokoelmissa *indeksijoukko* on $\{1, 2, \ldots, n\}$ tai $\mathbb{N}$. Leikkaus ja yhdiste voidaan määritellä myös kokoelmalle, jossa indeksijoukko on mikä tahansa joukko. Olkoon I indeksijoukko ja $\{A_i\}_{i\in I}$ kokoelma joukkoja. Tässä siis oletetaan, että indeksijoukon I jokaiseen alkioon i liittyy jokin joukko A_i. Tällöin kokoelman $\{A_i\}_{i\in I}$ joukkojen *leikkaus* on

$$\bigcap_{i\in I} A_i = \{x : x \in A_i \text{ kaikilla } i \in I\} \tag{6.14}$$

ja *yhdiste* on

$$\bigcup_{i\in I} A_i = \{x : x \in A_i \text{ jollakin } i \in I\}. \tag{6.15}$$

Esimerkiksi jokainen epätyhjä joukko A voidaan esittää alkioittensa muodostamien joukkojen yhdisteenä:

$$A = \bigcup_{x\in A} \{x\}.$$

Indeksijoukkona tässä on siis joukko itse. Sanotaan, että kokoelma $\{A_i\}_{i\in I}$ on joukon A *ositus*, jos kokoelman joukot ovat *keskenään pistevieraat* eli

$$A_i \cap A_j = \emptyset \tag{6.16}$$

kaikilla $i, j \in I$, joilla $i \neq j$, ja kokoelma *peittää* joukon A eli

$$A = \bigcup_{i\in I} A_i. \tag{6.17}$$

Esimerkiksi kokoelma $\{\{x\}\}_{x\in A}$ osittaa joukon A, oli A mikä tahansa epätyhjä joukko. Huomataan myös, että parillisten ja parittomien kokonaislukujen eli esimerkin 6.2 kohdan (2) joukkojen E ja O muodostama kokoelma $\{E, O\}$ on lauseen 5.11 mukaan kokonaislukujoukon $\mathbb{Z}$ ositus.

Seuraava lause osoittaa, että De Morganin lait eli lause 6.7 yleistyy mille tahansa kokoelmalle joukkoja. Lauseen 6.7 väite saadaan valitsemalla $I = \{1, 2\}$.

Lause 6.9 (De Morganin lait)**.** *Jos I on indeksijoukko ja $\{A_i\}_{i\in I}$ kokoelma joukkoja, niin*

$$\left(\bigcap_{i\in I} A_i\right)^c = \bigcup_{i\in I} A_i^c \qquad ja \qquad \left(\bigcup_{i\in I} A_i\right)^c = \bigcap_{i\in I} A_i^c.$$

Todistus. Osoitetaan, että vasemman puoleinen väite pitää paikkansa ja jätetään oikean puoleinen väite harjoitustehtäväksi. Olkoon siis $x \in (\bigcap_{i\in I} A_i)^c$, jolloin $x \notin \bigcap_{i\in I} A_i$. Leikkauksen määritelmän eli kohdan (6.14) mukaan ei siis ole totta, että $x \in A_i$ kaikilla $i \in I$. Näin ollen negaation ja kvanttoreiden vaihtosääntöjen eli kohdan (3.3) mukaan on olemassa $i \in I$ siten, että $x \in A_i^c$. Yhdisteen määritelmän eli kohdan (6.15) mukaan tällöin $x \in \bigcup_{i\in I} A_i^c$. Siispä $(\bigcap_{i\in I} A_i)^c \subset \bigcup_{i\in I} A_i^c$.

Olkoon sitten $x \in \bigcup_{i\in I} A_i^c$, jolloin on olemassa $i \in I$ siten, että $x \in A_i^c$. Negaation ja kvanttoreiden vaihtosäännön mukaan ei siis ole totta, että $x \in A_i$ kaikilla $i \in I$. Näin ollen $x \notin \bigcap_{i\in I} A_i$ eli $x \in (\bigcap_{i\in I} A_i)^c$. Siispä $\bigcup_{i\in I} A_i^c \subset (\bigcap_{i\in I} A_i)^c$. □

Seuraava lause yleistää osittelulait eli lauseen 6.8 mille tahansa kokoelmalle joukkoja. Lauseen 6.8 väite saadaan valitsemalla $I = \{1, 2\}$.

Lause 6.10 (Osittelulait)**.** *Jos A on joukko, I on indeksijoukko ja $\{A_i\}_{i\in I}$ on kokoelma joukkoja, niin*

$$A \cap \left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} A \cap A_i \qquad ja \qquad A \cup \left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I} A \cup A_i.$$

Todistus. Osoitetaan, että vasemman puoleinen väite pitää paikkansa ja jätetään oikean puoleinen väite harjoitustehtäväksi. Olkoon siis $x \in A \cap (\bigcup_{i\in I} A_i)$, jolloin $x \in A$ ja $x \in \bigcup_{i\in I} A_i$. Yhdisteen määritelmän eli kohdan (6.15) mukaan on siis olemassa $i \in I$ siten, että $x \in A_i$. Koska lisäksi $x \in A$, niin $x \in A \cap A_i$. Näin ollen $x \in \bigcup_{i\in I} A \cap A_i$. Siispä $A \cap (\bigcup_{i\in I} A_i) \subset \bigcup_{i\in I} A \cap A_i$.

Olkoon sitten $x \in \bigcup_{i\in I} A \cap A_i$, jolloin on olemassa $i \in I$ siten, että $x \in A \cap A_i$ eli $x \in A$ ja $x \in A_i$. Näin ollen $x \in A$ ja $x \in \bigcup_{i\in I} A_i$ eli $x \in A \cap (\bigcup_{i\in I} A_i)$. Siispä $\bigcup_{i\in I} A \cap A_i \subset A \cap (\bigcup_{i\in I} A_i)$. □

7. Relaatio

Luentovideo 16

Alkioiden x ja y muodostama *järjestetty pari* (x, y) on Kuratowskin[39] määritelmän mukaan joukko $\{\{x\}, \{x, y\}\}$. Tällaisille pareille pätee $(x, y) = (z, w)$ täsmälleen silloin, kun $x = z$ ja $y = w$. Huomautetaan, että järjestettyä paria ei voida määritellä kahden alkion jonoksi, sillä jono on kuvaus ja kuvaus tullaan kappaleessa 7.1 määrittelemään järjestetyn parin avulla määriteltävän relaation avulla. Joukkojen A ja B *karteesinen tulo* on joukko

$$A \times B = \{(x, y) : x \in A \text{ ja } y \in B\}. \tag{7.1}$$

Esimerkiksi *taso*, jota myös usein kutsutaan xy-koordinaatistoksi, on

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\}.$$

Määritellään rekursiivisesti $\mathbb{R}^{n+1} = \mathbb{R}^n \times \mathbb{R}$ kaikille $n \in \mathbb{N}$. Tällöin esimerkiksi *avaruus* on

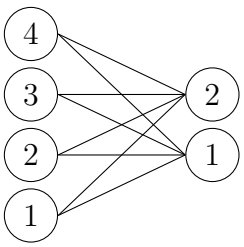
$$\mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\}.$$

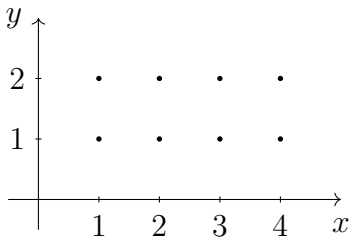
Sanotaan, että *relaatio* joukolta A joukolle B on karteesisen tulon $A \times B$ osajoukko. Jos $R \subset A \times B$ ja $(x, y) \in R$, niin sanotaan, että alkio $x \in A$ on *relaatiossa* R alkion $y \in B$ kanssa. Relaatio siis kertoo kuinka kahden joukon alkiot suhtautuvat toisiinsa.

Esimerkki 7.1. Olkoot $A = \{1, 2, 3, 4\}$, $B = \{1, 2\}$, $C = [1, 4]$ ja $D = [1, 2]$. Tällöin joukkoa

$$A \times B = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2), (4, 1), (4, 2)\}$$

voidaan havainnollistaa listaamalla joukon A ja joukon B alkiot omiin sarakkeisiinsa



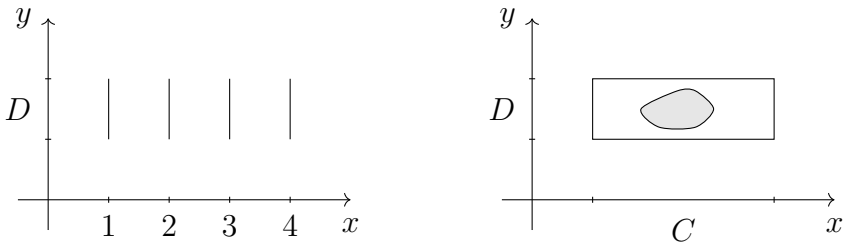


[39] Kazimierz Kuratowski (1896–1980)

ja yhdistämällä alkioparit viivoilla. Sitä voidaan myös havainnollistaa tason $\mathbb{R}^2$ osajoukkona. Joukkoja

$$A \times D = (\{1\} \times [1,2]) \cup (\{2\} \times [1,2]) \cup (\{3\} \times [1,2]) \cup (\{4\} \times [1,2]),$$
$$C \times D = [1,4] \times [1,2].$$

voidaan samaan tapaan havainnollistaa tason $\mathbb{R}^2$ osajoukkoina. Oikean puoleisessa

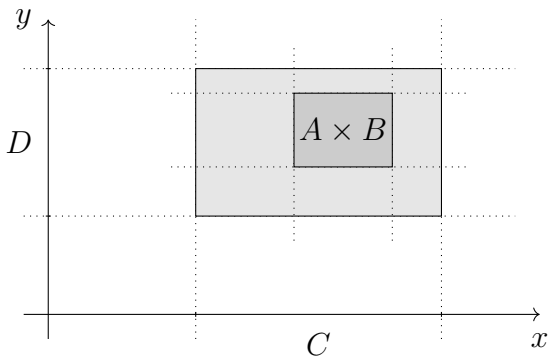


kuvassa on myös hahmoteltu erästä relaatiota joukolta C joukolle D.

Lause 7.2. *Jos A, B, C ja D ovat joukkoja siten, että A ja B ovat epätyhjiä, niin $A \subset C$ ja $B \subset D$ täsmälleen silloin, kun*

$$A \times B \subset C \times D.$$

Todistus. Jos A, B, C ja D ovat suljettuja reaalilukuvälejä, niin oheinen kuva



havainnollistaa lauseen väitettä. Osoitetaan, että ehdoista $A \subset C$ ja $B \subset D$ seuraa $A \times B \subset C \times D$, ja jätetään toinen suunta harjoitustehtäväksi. Muistaen kohta (6.3) kiinnitetään $\mathbf{x} \in A \times B$, jolloin karteesisen tulon määritelmän eli kohdan (7.1) mukaan on olemassa $x \in A$ ja $y \in B$ siten, että $\mathbf{x} = (x, y)$. Koska oletuksen mukaan

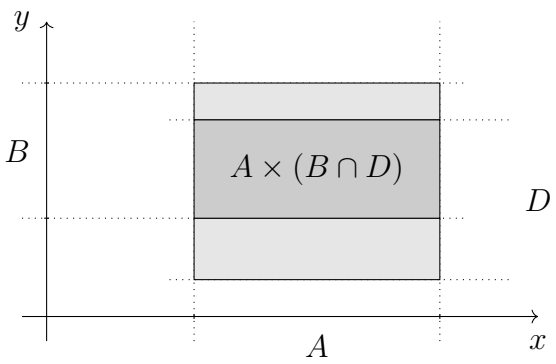
$A \subset C$ ja $B \subset D$, niin pätee myös $x \in C$ ja $y \in D$. Näin ollen karteesisen tulon määritelmän mukaan $(x, y) \in C \times D$ eli $\mathbf{x} \in C \times D$. Siispä väite pätee. □

Seuraavat kaksi lausetta tarkastelevat kuinka joukkojen leikkaaminen ja yhdistäminen toimivat karteesisessa tulossa.

Lause 7.3. *Jos A, B ja D ovat joukkoja, niin*

$$A \times (B \cap D) = (A \times B) \cap (A \times D),$$
$$A \times (B \cup D) = (A \times B) \cup (A \times D).$$

Todistus. Osoitetaan, että $A \times (B \cap D) = (A \times B) \cap (A \times D)$ pitää paikkansa ja jätetään toinen väite harjoitustehtäväksi. Jos A, B ja D ovat suljettuja



reaalilukuvälejä, niin väitettä voidaan havainnollistaa oheisella kuvalla. Olkoon $(x, y) \in A \times (B \cap D)$, jolloin karteesisen tulon määritelmän eli kohdan (7.1) mukaan $x \in A$ ja $y \in B \cap D$. Koska $y \in B$ ja $y \in D$, niin $(x, y) \in A \times B$ ja $(x, y) \in A \times D$ eli $(x, y) \in (A \times B) \cap (A \times D)$. Näin ollen $A \times (B \cap D) \subset (A \times B) \cap (A \times D)$.

Jos taas $(x, y) \in (A \times B) \cap (A \times D)$, niin $(x, y) \in A \times B$ ja $(x, y) \in A \times D$ ja siten $x \in A$, $y \in B$ ja $y \in D$. Näin ollen $(x, y) \in A \times (B \cap D)$. Siispä $(A \times B) \cap (A \times D) \subset A \times (B \cap D)$. □

Seuraava lause kertoo kuinka leikkaaminen ja yhdistäminen toimivat karteesisessa tulossa yleisemmässä tilanteessa. Valitsemalla siinä $C = A$ ollaan lauseen 7.3 tilanteessa.

Lause 7.4. *Jos A, B, C ja D ovat joukkoja, niin*

$$(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D),$$
$$(A \times B) \cup (C \times D) \subset (A \cup C) \times (B \cup D).$$

Todistus. Todistus jätetään harjoitustehtäväksi. □

7.1. **Kuvaus.** Relaation $R \subset A \times B$ *käänteisrelaatio* on joukko

Luentovideo 17

$$R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\} \subset B \times A. \tag{7.2}$$

Huomataan, että käänteisrelaatio on relaatio joukolta B joukolle A ja että käänteisrelaation käänteisrelaatio on relaatio itse. Jos $C \subset A$, niin sanotaan, että joukon C *kuvajoukko* relaatiossa $R \subset A \times B$ on

$$R(C) = \{y \in B : (x, y) \in R \text{ jollakin } x \in C\} \subset B. \tag{7.3}$$

Sanotaan, että relaatio $R \subset A \times B$ on *kaikkialla määritelty*, jos joukon B kuvajoukko käänteisrelaatiossa on joukko A, ts. $R^{-1}(B) = A$. Relaatio R on *yksiarvoinen*, jos joukossa $\{y \in B : (x, y) \in R\}$ on korkeintaan yksi alkio kaikilla $x \in A$ eli jokainen joukon A alkio on relaatiossa korkeintaan yhden joukon B alkion kanssa, ts. jokaisella $x \in A$ ja $y, z \in B$ ehdoista $(x, y) \in R$ ja $(x, z) \in R$ seuraa $y = z$.

Lause 7.5. *Jos A ja B ovat joukkoja, niin relaatio $R \subset A \times B$ on kaikkialla määritelty täsmälleen silloin, kun jokaiselle $x \in A$ on olemassa $y \in B$ siten, että $(x, y) \in R$.*

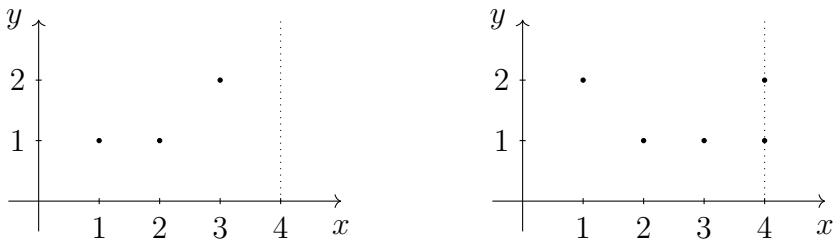
Todistus. Oletetaan ensin, että R on kaikkialla määritelty. Tällöin määritelmän mukaan $A \subset R^{-1}(B)$. Näin ollen käänteisrelaation määritelmän eli kohdan (7.2) ja kuvajoukon määritelmän eli kohdan (7.3) mukaan jokaiselle $x \in A$ on olemassa $y \in B$ siten, että $(y, x) \in R^{-1}$ eli $(x, y) \in R$.

Oletetaan sitten, että jokaiselle $x \in A$ on olemassa $y \in B$ siten, että $(x, y) \in R$ eli $(y, x) \in R^{-1}$. Tällöin määritelmien mukaan $A \subset R^{-1}(B)$. Koska triviaalisti $R^{-1}(B) \subset A$, niin R on kaikkialla määritelty. □

Sanotaan, että relaatio $f \subset A \times B$ on *kuvaus* (tai *funktio*), jos se on kaikkialla määritelty ja yksiarvoinen. Lauseen 7.5 ja yksiarvoisuuden määritelmän mukaan

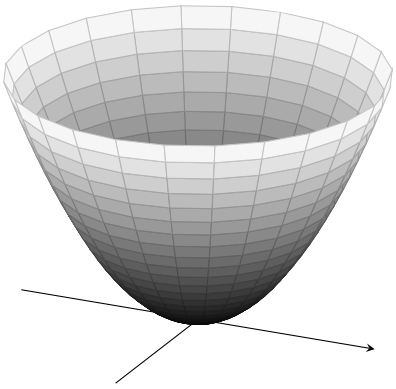
f on kuvaus täsmälleen silloin, kun jokaiselle $x \in A$ on olemassa yksikäsitteinen $y \in B$ siten, että $(x, y) \in f$. Tällöin käytetään merkintää $f(x) = y$ ja sanotaan, että y on alkion x *kuvapiste* kuvauksessa f. Kuvaus voidaan siis määritellä ilmoittamalla kuinka kuvapiste määräytyy kullekin lähtöjoukon alkiolle. Kuvausta f joukolta A joukolle B merkitään $f\colon A \to B$ ja sanotaan, että A on kuvauksen *lähtöjoukko* ja B *maalijoukko*.

Esimerkki 7.6. (1) Olkoot $A = \{1, 2, 3, 4\}$ ja $B = \{1, 2\}$. Tällöin relaatio $\{(1, 1), (2, 1), (3, 2)\} \subset A \times B$ on yksiarvoinen, mutta ei ole kaikkialla määritelty, sillä alkio



$4 \in A$ ei ole relaatiossa minkään joukon B alkion kanssa. Relaatio $\{(1, 2), (2, 1), (3, 1), (4, 1), (4, 2)\} \subset A \times B$ on kaikkialla määritelty, mutta ei ole yksiarvoinen, sillä alkio $4 \in A$ on relaatiossa alkioiden $1 \in B$ ja $2 \in B$ kanssa. Näin ollen kumpikaan relaatioista ei ole kuvaus joukolta A joukolle B.

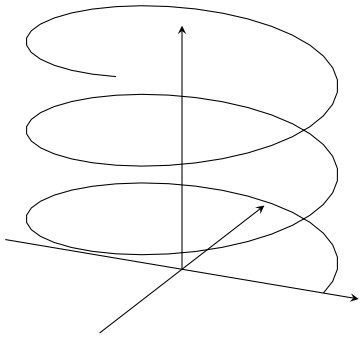
(2) Tarkastellaan relaatiota $f = \{(x, y, x^2 + y^2) : (x, y) \in \mathbb{R}^2\} \subset \mathbb{R}^2 \times \mathbb{R}$ ja perustellaan, että se on kuvaus $f\colon \mathbb{R}^2 \to \mathbb{R}$. Relaatio f on lauseen 7.5 mukaan selvästi



kaikkialla määritelty, sillä jokainen lähtöjoukon alkio $(x, y) \in \mathbb{R}^2$ on relaatiossa jonkun maalijoukon $\mathbb{R}$ alkion, nimittäin reaaliluvun $x^2 + y^2$ kanssa. Koska määritelmän

mukaan reaaliluku $x^2 + y^2$ on myös ainoa maalijoukon alkio, jonka kanssa (x, y) voi olla relaatiossa, niin f on yksiarvoinen. Siispä f on kuvaus $f\colon \mathbb{R}^2 \to \mathbb{R}$. Kuvausta f on havainnollistettu oheisessa kuvassa. Siinä lähtöjoukkona toimiva taso $\mathbb{R}^2$ on "vaakasuorassa" ja maalijoukko $\mathbb{R}$ on "pystyssä" eli lähtöjoukkoon nähden kohtisuorassa. Kuvaus f siis liittää jokaiseen lähtöjoukon $\mathbb{R}^2$ eli "vaakasuoran" tason pisteeseen yksikäsitteisen reaaliluvun, joka kuvasta katsoen määräytyy kuljetun matkan pituutena kulkiessa lähtöpisteestä "pystysuoraan" ylöspäin kuvaajalle.

(3) Tarkastellaan relaatiota $g = \{(t, \cos(t), \sin(t)) : t \in \mathbb{R}\} \subset \mathbb{R} \times \mathbb{R}^2$ ja perustellaan, että se on kuvaus $g\colon \mathbb{R} \to \mathbb{R}^2$. Koska jokainen lähtöjoukon alkio $t \in \mathbb{R}$ on



relaatiossa jonkun maalijoukon alkion, nimittäin tason pisteen $(\cos(t), \sin(t))$ kanssa, niin g on lauseen 7.5 nojalla kaikkialla määritelty. Koska määritelmän mukaan tason piste $(\cos(t), \sin(t))$ on myös ainoa maalijoukon alkio, jonka kanssa t voi olla relaatiossa, niin g on yksiarvoinen. Näin ollen g on kuvaus $g\colon \mathbb{R} \to \mathbb{R}^2$. Oheinen kuva havainnollistaa kuvausta g. Siinä lähtöjoukko $\mathbb{R}$ on "pystyssä" ja maalijoukko $\mathbb{R}^2$ on "vaakasuorassa" eli lähtöjoukkoon nähden kohtisuorassa. Kuvaus g siis liittää jokaiseen lähtöjoukon $\mathbb{R}$ eli "pystysuoran" reaalilukuakselin pisteeseen yksikäsitteisen tason pisteen, joka kuvasta katsoen määräytyy kulkemalla lähtöpisteestä "vaakasuoraan" kuvaajalle ja "pudottautumalla" alas maalijoukolle eli "vaakasuoralle" tasolle $\mathbb{R}^2$.

Kuvaus $f\colon A \to B$ voidaan siis esittää muodossa

$$f = \{(x, f(x)) \in A \times B : x \in A\} \subset A \times B. \tag{7.4}$$

Jos kuvaus $f\colon A \to B$ ajatellaan "sääntönä", joka liittää jokaiseen joukon A alkioon täsmälleen yhden joukon B alkion, niin kohdan (7.4) joukkoa kutsutaan

usein kuvauksen f *kuvaajaksi* – siitä huolimatta, että se on määritelmänsä mukaan kuvaus itse. Kuvajoukon määritelmän eli kohdan (7.3) mukaan joukon $C \subset A$ *kuvajoukko* kuvauksessa $f\colon A \to B$ on joukko

$$f(C) = \{f(x) \in B : x \in C\} \subset B. \tag{7.5}$$

Joukon $D \subset B$ *alkukuva* kuvauksessa f on joukon D kuvajoukko käänteisrelaatiossa f^{-1} eli

$$f^{-1}(D) = \{x \in A : f(x) \in D\} \subset A. \tag{7.6}$$

Koska kuvaus on kaikkialla määritelty, niin huomataan, että maalijoukon alkukuva on lähtöjoukko, ts. $f^{-1}(B) = A$.

Tarkastellaan seuraavaksi mitä joukkojen leikkauksen ja yhdisteen kuvajoukosta voidaan sanoa.

Lause 7.7. *Jos $f\colon A \to B$ on kuvaus ja $C, D \subset A$ ovat joukkoja, niin*

$$f(C \cap D) \subset f(C) \cap f(D),$$
$$f(C \cup D) = f(C) \cup f(D).$$

Todistus. Osoitetaan, että $f(C \cup D) = f(C) \cup f(D)$ pitää paikkansa ja jätetään toinen väite harjoitustehtäväksi. Olkoon siis $y \in f(C \cup D)$, jolloin kuvajoukon määritelmän eli kohdan (7.5) mukaan on olemassa $x \in C \cup D$ siten, että $f(x) = y$. Koska $x \in C$ tai $x \in D$, niin $f(x) \in f(C)$ tai $f(x) \in f(D)$ eli $f(x) \in f(C) \cup f(D)$. Siispä $f(C \cup D) \subset f(C) \cup f(D)$.

Jos taas $y \in f(C) \cup f(D)$, niin $y \in f(C)$ tai $y \in f(D)$. On siis olemassa $x \in C$ ja $x' \in D$ siten, että $y = f(x)$ tai $y = f(x')$. Koska $x, x' \in C \cup D$, niin $y \in f(C \cup D)$. Siispä $f(C) \cup f(D) \subset f(C \cup D)$. □

Seuraavan lauseen mukaan joukkojen leikkaaminen ja yhdistäminen voidaan tehdä ennen alkukuvan ottamista tai sen jälkeen.

Lause 7.8. *Jos $f\colon A \to B$ on kuvaus ja $C, D \subset B$ ovat joukkoja, niin*

$$f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D),$$
$$f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D).$$

Todistus. Osoitetaan, että $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$ pitää paikkansa ja jätetään toinen väite harjoitustehtäväksi. Olkoon siis $x \in f^{-1}(C \cap D)$, jolloin alkukuvan määritelmän eli kohdan (7.6) mukaan $f(x) \in C \cap D$. Koska $f(x) \in C$ ja $f(x) \in D$, niin $x \in f^{-1}(C)$ ja $x \in f^{-1}(D)$ eli $x \in f^{-1}(C) \cap f^{-1}(D)$. Siispä $f^{-1}(C \cap D) \subset f^{-1}(C) \cap f^{-1}(D)$.

Jos taas $x \in f^{-1}(C) \cap f^{-1}(D)$, niin $x \in f^{-1}(C)$ ja $x \in f^{-1}(D)$. Näin ollen $f(x) \in C$ ja $f(x) \in D$ eli $f(x) \in C \cap D$ ja siten $x \in f^{-1}(C \cap D)$. Siispä $f^{-1}(C) \cap f^{-1}(D) \subset f^{-1}(C \cap D)$. □

Selvitetään vielä mitä useamman joukon leikkauksen ja yhdisteen kuvajoukosta voidaan sanoa.

Lause 7.9. *Jos $f\colon A \to B$ on kuvaus, I on indeksijoukko ja $\{A_i\}_{i\in I}$ kokoelma joukon A osajoukkoja, niin*

$$f\left(\bigcap_{i\in I} A_i\right) \subset \bigcap_{i\in I} f(A_i) \qquad \textit{ja} \qquad f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i).$$

Todistus. Osoitetaan jälkimmäinen väite ja jätetään ensimmäinen väite harjoitustehtäväksi. Olkoon siis $y \in f(\bigcup_{i\in I} A_i)$, jolloin on olemassa $x \in \bigcup_{i\in I} A_i$ siten, että $f(x) = y$. Koska $x \in \bigcup_{i\in I} A_i$, niin on olemassa $i_0 \in I$ siten, että $x \in A_{i_0}$. Näin ollen $y = f(x) \in f(A_{i_0})$ ja $y \in \bigcup_{i\in I} f(A_i)$. Siispä $f(\bigcup_{i\in I} A_i) \subset \bigcup_{i\in I} f(A_i)$.

Jos taas $y \in \bigcup_{i\in I} f(A_i)$, niin on olemassa $i_0 \in I$ siten, että $y \in f(A_{i_0})$. On siis olemassa $x \in A_{i_0}$ siten, että $f(x) = y$. Koska $x \in \bigcup_{i\in I} A_i$, niin $y = f(x) \in f(\bigcup_{i\in I} A_i)$. Siispä $\bigcup_{i\in I} f(A_i) \subset f(\bigcup_{i\in I} A_i)$. □

Myös useamman joukon tapauksessa joukkojen leikkaaminen ja yhdistäminen voidaan tehdä ennen alkukuvan ottamista tai sen jälkeen.

Lause 7.10. *Jos $f\colon A \to B$ on kuvaus, I on indeksijoukko ja $\{B_i\}_{i\in I}$ kokoelma joukon B osajoukkoja, niin*

$$f^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} f^{-1}(B_i) \qquad \textit{ja} \qquad f^{-1}\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} f^{-1}(B_i).$$

Todistus. Osoitetaan ensimmäinen väite ja jätetään jälkimmäinen väite harjoitustehtäväksi. Olkoon siis $x \in f^{-1}(\bigcap_{i\in I} B_i)$, jolloin $f(x) \in \bigcap_{i\in I} B_i$. Koska $f(x) \in B_i$

kaikilla $i \in I$, niin $x \in f^{-1}(B_i)$ kaikilla $i \in I$ eli $x \in \bigcap_{i\in I} f^{-1}(B_i)$. Siispä $f^{-1}(\bigcap_{i\in I} B_i) \subset \bigcap_{i\in I} f^{-1}(B_i)$.

Jos taas $x \in \bigcap_{i\in I} f^{-1}(B_i)$, niin $x \in f^{-1}(B_i)$ kaikilla $i \in I$. Näin ollen $f(x) \in B_i$ kaikilla $i \in I$ eli $f(x) \in \bigcap_{i\in I} B_i$ ja siten $x \in f^{-1}(\bigcap_{i\in I} B_i)$. Siispä $\bigcap_{i\in I} f^{-1}(B_i) \subset f^{-1}(\bigcap_{i\in I} B_i)$. □

Luentovideo 18

7.2. **Ekvivalenssi ja järjestys.** Relaatiota joukolta A joukolle A kutsutaan lyhyemmin relaatioksi joukolla A. Jos R ja S ovat relaatioita joukolla A, niin niiden *yhdistetty relaatio* on $S \circ R = \{(x, z) : (x, y) \in R \text{ ja } (y, z) \in S \text{ jollakin } y \in A\} \subset A \times A$. *Yksikkörelaatio* joukolla A on $I = \{(x, x) : x \in A\}$. Relaatio R joukolla A on

(1) *refleksiivinen*, jos $I \subset R$,
(2) *antirefleksiivinen*, jos $I \cap R = \emptyset$,
(3) *symmetrinen*, jos $R = R^{-1}$,
(4) *antisymmetrinen*, jos $R \cap R^{-1} \subset I$,
(5) *transitiivinen*, jos $R \circ R \subset R$,
(6) *täysi*, jos $R \cup R^{-1} = A \times A$.

Sanotaan, että relaatio on *ekvivalenssi*, jos se on refleksiivinen, symmetrinen ja transitiivinen. Ekvivalensseja merkitään usein symbolilla $\sim$ tai vastaavilla. Jos $\sim \subset A \times A$ on ekvivalenssi joukolla A ja $(x, y) \in \sim$, niin voidaan myös merkitä $x \sim y$. Jos taas $(x, y) \notin \sim$, niin voidaan vastaavasti merkitä $x \not\sim y$.

Relaatio on *osittainen järjestys*, jos se on refleksiivinen, antisymmetrinen ja transitiivinen. Täyttä osittaista järjestystä sanotaan *järjestykseksi*. Järjestyksiä merkitään usein symbolilla $\preccurlyeq$ tai vastaavilla. Jos $\preccurlyeq \subset A \times A$ on osittainen järjestys joukolla A, niin voidaan taas merkitä $x \preccurlyeq y$, jos $(x, y) \in \preccurlyeq$, ja $x \not\preccurlyeq y$, jos $(x, y) \notin \preccurlyeq$. Käytetään vastaavaa merkintää myös muiden joukon A relaatioiden kanssa.

Lause 7.11. *Relaatio R joukolla A on*

(1) refleksiivinen täsmälleen silloin, kun jokaiselle $x \in A$ pätee xRx,
(2) antirefleksiivinen täsmälleen silloin, kun jokaiselle $x \in A$ pätee $x \not R x$,
(3) symmetrinen täsmälleen silloin, kun jokaiselle $x, y \in A$ ehdosta xRy seuraa yRx,

(4) antisymmetrinen täsmälleen silloin, kun jokaiselle $x, y \in A$ ehdoista xRy ja yRx seuraa $x = y$,

(5) transitiivinen täsmälleen silloin, kun jokaiselle $x, y, x \in A$ ehdoista xRy ja yRz seuraa xRz,

(6) täysi täsmälleen silloin, kun jokaiselle $x, y \in A$ pätee xRy tai yRx.

Todistus. Kohta (1) pitää paikkansa, sillä kohdan (6.3) mukaan $I \subset R$ ja $\forall x, y : (x, y) \in I \to (x, y) \in R$ ovat yhtäpitävät ja näistä jälkimmäinen on selvästi yhtäpitävä ehdon $\forall x : x \in A \to (x, x) \in R$ kanssa. Kohta (2) taas pitää negaation ja kvanttoreiden vaihtosäännön eli kohdan (3.3) mukaan paikkansa, sillä $I \cap R \neq \emptyset$, $\exists x, y : (x, y) \in I \wedge (x, y) \in R$ ja $\exists x : (x, x) \in R$ ovat yhtäpitävät. Osoitetaan sitten kohta (3). Kohdan (6.7) mukaan $R = R^{-1}$ on yhtäpitävä ehdon $\forall x, y : (x, y) \in R \leftrightarrow (x, y) \in R^{-1}$ kanssa. Koska $\forall x, y : (x, y) \in R \to (y, x) \in R^{-1}$ nähdään vain alkioiden x ja y roolit vaihtamalla yhtäpitäväksi ehdon $\forall x, y : (x, y) \in R^{-1} \to (y, x) \in R$ kanssa, niin kohta (3) pätee.

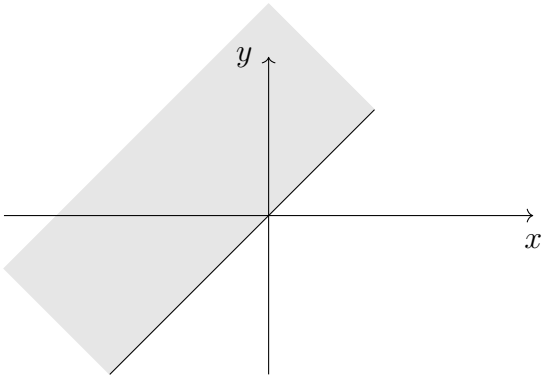
Kohta (4) pitää paikkansa, sillä kohdan (6.3) mukaan $R \cap R^{-1} \subset I$ on yhtäpitävä ehdon $\forall x, y : (x, y) \in R \cap R^{-1} \to (x, y) \in I$ ja edelleen kohdan (7.2) nojalla ehdon $\forall x, y : (x, y) \in R \wedge (y, x) \in R \to x = y$ kanssa. Kohta (5) taas pitää paikkansa, sillä kohdan (6.3) ja relaation $R \circ R$ mukaan ehdot $R \circ R \subset R$, $\forall x, z : (x, z) \in R \circ R \to (x, z) \in R$ ja $\forall x, y, z : (x, y) \in R \wedge (y, z) \in R \to (x, z) \in R$ ovat yhtäpitävät. Osoitetaan lopuksi kohta (6). Kohtien (6.3) ja (7.2) mukaan ehdot $A \times A \subset R \cup R^{-1}$, $\forall x, y : (x, y) \in R \cup R^{-1}$ ja $\forall x, y : (x, y) \in R \vee (y, x) \in R$ ovat yhtäpitävät. Koska mikä tahansa relaatio joukolla A on joukon $A \times A$ osajoukko, niin kohta (6) pätee. □

Jos $\preccurlyeq$ on järjestys joukolla A, niin sen avulla voidaan määritellä *aito järjestys* $\prec$ asettamalla $x \prec y$, jos $x \preccurlyeq y$ ja $x \neq y$. Tällöin jokaiselle $x, y \in A$ pätee joko $x \prec y$, $x = y$ tai $y \prec x$. Vakiintunut terminologia on relaatioiden kannalta tässä kohdin hieman epälooginen, sillä aito järjestys ei ole refleksiivinen eikä antisymmetrinen eikä siten järjestys.

Esimerkki 7.12. (1) Kohdassa (6.3) määritelty inkluusio $\subset$ on osittainen järjestys annetun perusjoukon X osajoukkojen muodostamalla kokoelmalla. Tarkistetaan vaaditut ehdot lauseen 7.11 avulla: Inkluusio on refleksiivinen, sillä $A \subset A$ kaikilla

joukoilla A. Se on antisymmetrinen, sillä kohdan (6.6) mukaan ehdoista $A \subset B$ ja $B \subset A$ seuraa $A = B$. Inkluusio on transitiivinen, sillä kohtien (6.3) ja (2.11) mukaan ehdoista $A \subset B$ ja $B \subset C$ seuraa $A \subset C$. Se ei kuitenkaan ole järjestys, sillä esimerkiksi $\{x\} \not\subset \{y\}$ ja $\{x\} \not\subset \{y\}$ aina kun $x, y \in X$ siten, että $x \neq y$.

(2) Tavallinen pienempi tai yhtäsuuri kuin -merkki $\leqslant$ on relaatio $\{(x, y) \in \mathbb{R}^2 : x \leqslant y\}$, jota voidaan tason $\mathbb{R}^2$ osajoukkona havainnollistaa oheisella kuvalla.



Lauseen 7.11 avulla on helppo nähdä, että se on järjestys joukolla $\mathbb{R}$: Koska $x \leqslant x$ kaikilla $x \in \mathbb{R}$, niin $\leqslant$ on refleksiivinen. Koska ehdoista $x \leqslant y$ ja $y \leqslant x$ seuraa $x = y$, niin $\leqslant$ on antisymmetrinen. Koska ehdoista $x \leqslant y$ ja $y \leqslant z$ seuraa $x \leqslant z$, niin $\leqslant$ on transitiivinen. Koska $x \leqslant y$ tai $y \leqslant x$ kaikilla $x, y \in \mathbb{R}$, niin $\leqslant$ on täysi.

(3) Määritellään relaatio $\sim$ joukolla $\mathbb{Z}$ asettamalla $m \sim n$, jos on olemassa $k \in \mathbb{Z}$ siten, että $m - n = 5k$. Relaatio $\sim$ on tällöin lauseen 7.11 mukaan ekvivalenssi: Olkoon $n \in \mathbb{Z}$, jolloin $n-n = 0$ ja $n \sim n$ eli $\sim$ on refleksiivinen. Olkoon sitten $m \sim n$. Tällöin on olemassa $k \in \mathbb{Z}$ siten, että $m-n = 5k$. Koska $n-m = 5(-k)$, niin myös $n \sim m$ ja $\sim$ on symmetrinen. Olkoon lopuksi $m \sim n$ ja $n \sim p$. Tällöin on olemassa $k, l \in \mathbb{Z}$ siten, että $m-n = 5k$ ja $n-p = 5l$. Koska $m-p = m-n+n-p = 5(k+l)$, niin myös $m \sim p$ ja $\sim$ on transitiivinen.

Jos $\sim$ on ekvivalenssi joukolla A, niin alkion $x \in A$ määräämää kuvajoukkoa

$$[x] = \sim(\{x\}) = \{y \in A : x \sim y\} \subset A$$

kutsutaan *ekvivalenssiluokaksi*. Ekvivalenssiluokkien muodostama kokoelma

$$A/_\sim = \{[x] : x \in A\}$$

on joukon A *tekijäjoukko* ekvivalenssin $\sim$ suhteen. Seuraava lause osoittaa, että tekijäjoukko on ositus eli se toteuttaa ehdot (6.16) ja (6.17).

Lause 7.13. *Jos $\sim$ on ekvivalenssi joukolla A, niin kokoelma $A/_\sim$ on joukon A ositus. Kääntäen, jos kokoelma $\{A_i\}_{i\in I}$ on joukon A ositus, niin $\{(x,y) : x,y \in A_i$ jollakin $i \in I\}$ on ekvivalenssi joukolla A.*

Todistus. Osoitetaan ensimmäinen väite ja jätetään jälkimmäinen väite harjoitustehtäväksi. Oletetaan siis, että $\sim$ on ekvivalenssi joukolla A. Olkoon $x, y \in A$. Jos $[x] \cap [y] \neq \emptyset$, niin on olemassa $z \in [x] \cap [y]$. Tällöin $z \in [x]$ ja $z \in [y]$ eli $x \sim z$ ja $y \sim z$. Koska $\sim$ on symmetrinen ja $y \sim z$, niin lauseen 7.11 kohdan (3) nojalla $z \sim y$. Koska $\sim$ on transitiivinen, $x \sim z$ ja $z \sim y$, niin lauseen 7.11 kohdan (5) nojalla $x \sim y$. Jos siis $w \in [x]$, niin symmetrisyyden ja transitiivisuuden nojalla $w \in [y]$. Jos taas $w \in [y]$, niin vastaavasti nähdään, että $w \in [x]$. Siispä $[x] = [y]$. Ollaan siis osoitettu, että jokaiselle $x, y \in A$ pätee joko $[x] \cap [y] = \emptyset$ tai $[x] = [y]$. Näin ollen (6.16) on voimassa.

Koska $[x] \subset A$ kaikilla $x \in A$, niin $\bigcup_{x\in A}[x] \subset A$. Toisaalta, koska $x \in [x]$ ja siten $\{x\} \subset [x]$ kaikilla $x \in A$, niin kohdan (6.3) mukaan $A = \bigcup_{x\in A}\{x\} \subset \bigcup_{x\in A}[x]$. Siispä

$$A = \bigcup_{x\in A}[x]$$

ja myös (6.17) on voimassa. □

Esimerkki 7.14. Tarkastellaan esimerkin 7.12 kohdan (3) ekvivalenssia $\sim$. Luvun $n \in \mathbb{Z}$ määräämä ekvivalenssiluokka on joukko $[n] = \{n - 5k : k \in \mathbb{Z}\}$. Koska jokainen $n \in \mathbb{Z}$ on ekvivalentti jonkun joukon $\{0, 1, 2, 3, 4\}$ luvun kanssa, niin $\mathbb{Z}/_\sim = \{[0], [1], [2], [3], [4]\}$. Lauseen 7.13 mukaan tämä kokoelma osittaa kokonaisluvut.

Henkilöhakemisto

Hakemisto