Jorma Merikoski
Ari Virtanen
Pertti Koivisto

Johdatus diskreettiin matematiikkaan

Esipuhe

Monisteemme *Diskreetti matematiikka I* (kirjallisuusluettelossa [14]) ensimmäinen painos ilmestyi 1993. Tätä monistetta (samoin kuin sen aiempia Jorma Merikosken laatimia versioita) käytettiin alun perin matematiikan, tilastotieteen ja tietojenkäsittelyopin opiskelijoiden kurssilla Tampereen yliopistossa sekä peruskoulun luokanopettajaksi opiskelevien matematiikan erikoistumisopinnoissa Hämeenlinnan opettajankoulutuslaitoksella. Sittemmin monistetta alettiin käyttää muuallakin, mikä rohkaisi meitä uudistamaan sen oppikirjaksi.

Kirjan sisältöä voidaan käyttää valikoivasti esimerkiksi seuraavalla tavalla:

1. *Matematiikan ja sen lähitieteiden opiskelijat.* Periaatteessa koko sisältö, mutta käytännössä sitä ei ehdittäne käydä läpi yhdellä luentokurssilla. Tällöin tähdellä merkityt kohdat voidaan sivuuttaa. Ellei aika sittenkään riitä, luku 6 voidaan jättää koulutietojen varaan.

2. *Didaktisen matematiikan opiskelijat.* Pääkohdat luvuista 1–6 (paitsi 2.2). Kiinnitetään erityistä huomiota induktion osaamiseen, ekvivalenssirelaation, injektion, surjektion ja bijektion käsitteiden ymmärtämiseen sekä kombinatoriikan perustaitoihin.

3. *Kieliteknologian opiskelijat.* Kuten edellä, mutta joukko-opilliset väitteet tyydytään perustelemaan havainnollisesti Venn-diagrammeilla ja teoriaa kevennetään muuallakin. Lisäksi käsitellään luku 8. Ellei aika riitä, luku 6 voidaan jättää koulutietojen varaan.

4. *Lukiolaiset.* Matemaattisesti erityslahjakkaiden lukiolaisten yliopistotasoisella kurssilla menetellään kuten kohdassa 1. Tavanomaisella erikoiskurssilla sisällön valintaan on monta mahdollisuutta.

Osa harjoitustehtävistä on täydellisesti ratkaistu nettiosoitteessa

http://mtl.uta.fi/diskreetti/

ja osaan on siellä vastaukset tai lyhyet ratkaisuohjeet.

Monet kollegat, työtoverit ja opiskelijat ovat auttaneet meitä tämän kirjan ja sen aiempien monisteversioiden laatimisessa tekemällä sisältöä koskevia huomautuksia, osallistumalla tekniseen toimittamiseen, laatimalla nettiratkaisuja tai muulla tavalla. Heidän suuren lukumääränsä takia tyydymme kiittämään kaikkia yhteisesti mainitsematta muiden nimiä kuin Jarmo Niemelän, jota kiitämme kirjan erinomaisesta teknisestä toimitustyöstä. Lisäksi kiitämme Tampereen yliopistoa ja Suomen tietokirjailijat ry:tä saamastamme apurahasta.

Tampereella maaliskuussa 2004

Jorma Merikoski Ari Virtanen Pertti Koivisto

Sisällys

Luku 1

Logiikkaa

Kalle: Mutta filosofia, näetkös, se on tiede, joka opettaa meitä ajattelemaan. Esimerkiksi: kun sataa, niin kastuu; Cajus menee ulos sateeseen; siis Cajus kastuu.

Kaisa: Mutta jos Cajuksella on sateenvarjo?

Kalle: No, silloin kastuu sateenvarjo.

Kaisa: Voi Kalle kulta, kuinka turhaan sinä vaivaat päätäsi. Se on muka olevinaan filosofiaa, että Cajus kastuu eikä Cajus kastukaan. Ajatellahan osaa jokainen, kenellä vain on täysi järki.

(*Topelius* [27])

1.1 Lauselogiikkaa

1 Propositio eli suljettu lause

Matematiikassa on tärkeää, että määritelmät, lauseet ja päättelyt esitetään lyhyesti ja täsmällisesti, mutta samalla ymmärrettävästi ja riittävän yksityiskohtaisesti. Jos käytettäisiin pelkkää suomen kieltä tai muuta *luonnollista kieltä*, niin esityksestä tulisi pitkä ja kömpelö. Lyhempään ja selkeämpään esitykseen päästään ottamalla käyttöön lyhennysmerkintöjä eli symboleja matemaattisille käsitteille. Joskus on hyödyllistä ottaa käyttöön lyhennysmerkintöjä myös matemaattisille *päättelyille*. Silloin joudutaan pohtimaan, mitä erilaisissa päättelyissä varsinaisesti tapahtuu eli joudutaan ottamaan *tutkimuskohteeksi* päättelyt. Tällaisia asioita selvittelevä tieteenala on nimeltään *logiikka*. Se on historiallisesti luettu kuuluvaksi filosofiaan, mutta nykyisin logiikkaa tutkitaan filosofiassa, matematiikassa ja tietojenkäsittelytieteissä. *Matemaattinen logiikka* onkin nimensä mukaisesti matematiikan eräs osa-alue. Me olemme tässä kiinnostuneita logiikasta pelkästään työvälineenä ja perehdymme tämän alan alkeiskäsitteisiin ja menetelmiin vain sen verran kuin matematiikan opiskelun kannalta on tarpeellista.

Logiikan yksinkertaisin tutkimuskohde on *propositio* eli *suljettu lause*, josta käytämme myös hieman epätäsmällistä nimitystä 'lause'. (Tällöin sanalla 'lause' on eri merkitys kuin kieliopissa tai matematiikassa.) Tarkoitamme sillä ilmaisua, joka sisältää toden tai epätoden väitteen. Kysymys siitä, onko tietty ilmaisu propositio vai ei, saattaa olla ongelmallinen (teht. 1). Meidän ei kuitenkaan tarvitse huolehtia tällaisista pulmista, sillä määrittelemällä toden proposition *totuusarvoksi* 1 ja epätoden 0 saamme aikaan täysin formaalin systeemin. Voimme tällöin pitää propositioita olioina, joihin liittyy joko nolla tai ykkönen (jotka nekin ovat meille tässä pelkkiä symboleja, vailla merkitystä), eikä meidän tarvitse välittää siitä, mitä nämä oliot todellisuudessa ovat.

2 Loogiset konnektiivit

Propositiologiikassa eli *lauselogiikassa* tutkitaan annetuista lauseista *loogisten konnektiivien* avulla muodostettavien lauseiden ominaisuuksia. Määrittelemme *totuustaulukoilla* viisi loogista konnektiivia.

Negaatio $\neg$
"ei p"

p	$\neg p$
0	1
1	0

Konjunktio $\wedge$
"p ja q"

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Disjunktio $\vee$
"p tai q"

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Implikaatio $\Rightarrow$
"jos p, niin q"

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Ekvivalenssi $\Leftrightarrow$
"p, jos ja vain jos q"

p	q	$p \Leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Näistä totuustaulukoista näemme konnektiiveilla muodostetun *yhdistetyn lauseen* totuusarvon, kun alkuperäisten lauseiden p ja q totuusarvot tunnetaan.

Voimme lukea merkinnän '$p \Rightarrow q$' muillakin tavoilla, esimerkiksi "p:stä seuraa q", "p implikoi q:n", "p on riittävä ehto q:lle", "q on välttämätön ehto p:lle". Myös merkinnälle '$p \Leftrightarrow q$' on muita lukutapoja: "p silloin ja vain silloin, kun q", "p ja q ovat ekvivalentteja eli yhtäpitäviä", "p on välttämätön ja riittävä ehto q:lle".

Näillä konnektiiveilla on siis tietyt vastineet luonnollisessa kielessä, joka meillä on tavallinen suomen kieli:

$\neg$ "ei", "ei pidä paikkaansa, että…"

$\wedge$ "ja", "sekä … että…"

$\vee$ "tai", "joko … tai… (tai molemmat)"

$\Rightarrow$ "jos … niin…", "silloin kun … niin…"

$\Leftrightarrow$ "jos ja vain jos … niin…", "silloin ja vain silloin kun … niin…"

Tämä yhteys ei ole kuitenkaan näin suoraviivainen, sillä luonnollisessa kielessä näillä sanoilla ja sanonnoilla on monipuolisempi merkitys kuin logiikassa. Tarkastelemme asiaa lähemmin.

3 Vertailua luonnolliseen kieleen

Ja. Tavallisessa kielessä ja-sanalla voidaan ilmoittaa ajallisia ja muunkinlaisia järjestyksiä. Esimerkiksi lauseilla 'Kilpailijat A ja B tulivat maaliin' ja 'Caesar ja legioonalaiset tekivät sotaretken Galliaan' on eri sisältö kuin lauseilla 'Kilpailijat B ja A tulivat maaliin' ja 'Legioonalaiset ja Caesar tekivät sotaretken Galliaan'. Logiikassa on yhdentekevää, missä järjestyksessä ja-konnektiivilla yhdistettävät lauseet kirjoitetaan.

Tai. Tavallisessa suomen kielessä on oikeastaan kaksi erilaista tai-sanaa. Tarkastelemme lauseita 'Viran kelpoisuusehtona on filosofian maisterin tai diplomi-insinöörin tutkinto' ja 'Lounaan jälkiruoaksi voidaan valita kahvi tai jäätelö'. Viran hakija, joka on suorittanut *sekä* filosofian maisterin *että* diplomi-insinöörin tutkinnon, on edellisen lauseen tulkitsijan mielestä varmaankin pätevä mainittuun virkaan. Sen sijaan jälkimmäistä lausetta tarjoilija tuskin suostuu käsittämään niin, että asiakas saisi sekä kahvin että jäätelön. Looginen konnektiivi $\vee$ vastaa tai-sanaa "viranhakijan tulkinnalla". "Tarjoilijan tulkinta" eli *poissulkeva tai* lienee jokapäiväisessä kielenkäytössä yleisempi.

Jos ... niin. Lauselogiikan implikaatiolle ei voida antaa luonnollisen kielen syy-seuraus -tulkintaa. Tämän konnektiivin hyödyllisyys matemaattisena merkintänäkin näkyy vasta tautologioiden ja avointen lauseiden yhteydessä. Vanhan esimerkin mukaan lauseet '$2 + 2 = 5$' ja 'Kuu on juustoa' ovat kumpikin epätosia, joten implikaation totuustaulukon perusteella lause '$2 + 2 = 5 \Rightarrow$ Kuu on juustoa' eli 'Jos $2 + 2 = 5$, niin Kuu on juustoa' on tosi. Tämä kuulostaa täysin järjettömältä. Ammattitaitoinen selittelijä voisi kuitenkin yrittää todistella lauseen mielekkyyttä seuraavasti: Jos $2 + 2$ olisi 5, niin silloin maailma olisi niin sekaisin, että kaikki olisi mahdollista. Kuukin voisi olla juustoa tai mitä tahansa, mutta koska $2 + 2$ ei ole nyt eikä koskaan 5, niin Kuun pinnan laadusta ei tämän sinänsä toden implikaation perusteella voida sanoa mitään.

Tarkastelemme vielä lauseita 'Ulkona sataa' ja 'Minä en lähde kävelylle', joista muodostamme lauseen 'Ulkona sataa $\Rightarrow$ Minä en lähde kävelylle' eli 'Jos ulkona sataa, niin minä en lähde kävelylle'. Ainoa tapa osoittaa tämä lause epätodeksi on lähteä kävelylle sateeseen. Tällöin implikaation edellinen jäsen on tosi ja jälkimmäinen epätosi, joten tulemme juuri siihen totuusarvoyhdistelmään, joka tekee implikaation epätodeksi.

Jos ja vain jos ... niin. Tätäkään ei voida tulkita syy-seuraus -suhteena, kuten huomaamme esimerkiksi lauseesta 'Jos ja vain jos $2 + 2 = 5$, niin Kuu on juustoa', joka on tosi.

Luonnollisessa kielessä sanotaan usein "jos ... niin", vaikka tarkoitetaan "jos ja vain jos ... niin". Esimerkkeinä tutkimme lauseita 'Jos maksat 50 euroa, niin saat tämän kirjan' ja 'Jos opiskelet matematiikkaa ahkerasti, niin opit matematiikkaa'. Kuitenkin kirjakauppias tarkoittaa, että kirjan saa maksamalla 50 euroa *ja vain siten.* Ahkeraan opiskeluun hoputtaja taas haluaa sanoa, että matematiikkaa oppii opiskelemalla ahkerasti *eikä millään muulla tavalla.* Täten logiikan (mutta ei luonnollisen kielen) vaatimusten mukaista olisi sanoa ”Jos ja vain jos maksat 50 euroa, niin saat tämän kirjan” ja ”Jos ja vain jos opiskelet matematiikkaa ahkerasti, niin opit matematiikkaa”.

Matematiikassa on kuitenkin vakiintunut tapa, että *määritelmissä* sanotaan ”jos ... niin”, vaikka tarkoitetaan ”jos ja vain jos ... niin”. Esimerkiksi määritelmä ’Kolmiota sanotaan tasasivuiseksi, jos sen kaikki sivut ovat yhtä pitkät’ itse asiassa tarkoittaa: ”Kolmiota sanotaan tasasivuiseksi, jos ja vain jos sen kaikki sivut ovat yhtä pitkät”. *Matemaattisissa lauseissa* on sen sijaan tietenkin tärkeä erottaa, onko väite voimassa kumpaankin suuntaan vai pelkästään toiseen. Ilmaisu ’jos ja vain jos’ voidaan lyhentää muotoon ’joss’ (engl. ’iff’).

4 Useampi kuin yksi konnektiivi

Luonnollisen kielen yhdessä lauseessa saattaa esiintyä useita konnektiiveja. Tällöin asiayhteydestä on selvittävä, mitkä konnektiivit liittyvät mihinkin lausekokonaisuuteen, mutta joskus saattaa syntyä epäselviä tilanteita. Esimerkiksi lauseella ’Menen kapakkaan ja vietän hauskan illan tai luen tenttiin’ on kaksi mahdollista tulkintaa. Tulkinta, että lauseen esittäjä harkitsee, lukeeko hän kapakassa tenttiin vai viettääkö siellä hauskan illan, lienee käytännössä harvinainen. Lauselogiikassa käytetään sulkeita tällaisten epäselvyyksien välttämiseksi. Merkitään siis joko ’(Menen kapakkaan ja vietän hauskan illan) tai luen tenttiin’ tai ’Menen kapakkaan ja (vietän hauskan illan tai luen tenttiin)’ riippuen siitä, kumpaa tarkoitetaan. Vähentääksemme sulkeiden käyttöä sovimme, että loogisten konnektiivien suoritusjärjestys on

1. negaatiot,
2. konjunktiot ja disjunktiot,
3. implikaatiot ja ekvivalenssit,

ellei sulkumerkein toisin ilmoiteta.

Olemme logiikassa yleensä kiinnostuneita yhdistettyjen lauseiden totuusarvoista ”kaikissa mahdollisissa tilanteissa”. Jos meillä on esimerkiksi jokin lauseista p, q ja r muodostettu yhdistetty lause A, niin meillä ei ole useinkaan tietoa lauseiden p, q ja r totuusarvoista, vaan haluamme selvittää lauseen A totuusarvon kaikissa kahdeksassa mahdollisessa tapauksessa, jotka syntyvät, kun lauseet p, q ja r ovat toisistaan riippumatta joko tosia tai epätosia. Silloin on kätevää käyttää totuustaulukkoa, jossa kukin vaakarivi esittää yhtä mahdollista tapausta. Olemme jo konnektiivien määrittelyjen yhteydessä laatineet totuustaulukoita, joissa on käsitelty lauseiden p ja q neljä mahdollista totuusarvoyhdistelmää.

Esimerkki 1. Tutkimme totuustaulukon avulla lauseen $p \vee r \Rightarrow q \wedge r$ totuusarvoa.

p	q	r	$p \vee r$	$q \wedge r$	$p \vee r \Rightarrow q \wedge r$
0	0	0	0	0	1
0	0	1	1	0	0
0	1	0	0	0	1
0	1	1	1	1	1
1	0	0	1	0	0
1	0	1	1	0	0
1	1	0	1	0	0
1	1	1	1	1	1

Näemme toisesta vaakarivistä, että kun r on tosi sekä p ja q epätosia, niin $p \vee r \Rightarrow q \wedge r$ on epätosi. Muut totuusarvoyhdistelmät näemme muista vaakariveistä.

5 Konnektiivien palauttaminen toisiinsa

Kun teemme lauseita $\neg(\neg p \wedge \neg q)$, $\neg(p \wedge \neg q)$ ja $\neg(p \wedge \neg q) \wedge \neg(q \wedge \neg p)$ vastaavat totuustaulukot (tässä järjestyksessä), niin saamme samat totuustaulukot kuin mitä lauseilla $p \vee q$, $p \Rightarrow q$ ja $p \Leftrightarrow q$ (tässä järjestyksessä) on. Loogiset konnektiivit eivät ole siis toisistaan riippumattomia, vaan jos meillä on annettuna esimerkiksi vain negaatio ja konjunktio, niin voimme määritellä muut konnektiivit niiden avulla:

$$\begin{aligned} p \vee q &\stackrel{\text{def}}{=} \neg(\neg p \wedge \neg q), \\ p \Rightarrow q &\stackrel{\text{def}}{=} \neg(p \wedge \neg q), \\ p \Leftrightarrow q &\stackrel{\text{def}}{=} \neg(p \wedge \neg q) \wedge \neg(q \wedge \neg p). \end{aligned}$$

Tässä '$\ldots \stackrel{\text{def}}{=} \ldots$' tarkoittaa, että '... määritellään samaksi kuin...'. Tällaisiksi *peruskonnektiiveiksi*, joiden avulla muut konnektiivit määritellään, voimme ottaa myös esimerkiksi negaation ja disjunktion tai vaikkapa negaation ja implikaation. Kuitenkaan emme voi määritellä negaatiota käyttämällä pelkästään konjunktiota, disjunktiota, implikaatiota ja ekvivalenssia (s. 46, teht. 99).

Voimme palauttaa poissulkevan tai-konnektiivin $\underline{\vee}$ konjunktioon ja disjunktioon määrittelemällä

$$p \underline{\vee} q \stackrel{\text{def}}{=} (p \vee q) \wedge \neg(p \wedge q).$$

Voimme myös käyttää totuustaulukkoa (teht. 7). Muitakin loogisia konnektiiveja voidaan määritellä. Niistä *Shefferin*[1] *viiva* (teht. 8) ja *Peircen*[2] *nuoli* eli *Nicodin*[3] *funktio* (teht. 10) ovat mielenkiintoisia sikäli, että kaikki edellä määrittelemämme konnektiivit ovat palautettavissa kumpaankin niistä.

[1] *M. H. Sheffer (1901–1964), yhdysvaltalainen loogikko.*
[2] *Charles Peirce (1839–1914), yhdysvaltalainen filosofi.*
[3] *Jean Nicod (1893–1924), ranskalainen loogikko.*

Harjoitustehtäviä

1. Mitkä seuraavista ovat suljettuja lauseita? **a)** 'Paljonko kello on?', **b)** 'Hyvää huomenta', **c)** 'Kunpa tulisi kesä', **d)** '$x + 2 = 5$', **e)** 'Luvun π biljoonas desimaali on 7', **f)** 'Tämä lause on epätosi'.

2. Muodostettava lauseen **a)** $p \Rightarrow \neg p$, **b)** $p \wedge \neg p \Leftrightarrow p$ totuustaulukko.

3. Muodostettava lauseen **a)** $\neg p \wedge q$, **b)** $\neg(p \wedge q)$, **c)** $p \vee q \Rightarrow p \wedge q$ totuustaulukko.

4. Muodostettava lauseen **a)** $p \vee q \Rightarrow r$, **b)** $p \vee (q \Rightarrow r)$, **c)** $p \wedge q \Rightarrow \neg r$ totuustaulukko.

5. Esitettävä konjunktio, implikaatio ja ekvivalenssi negaation ja disjunktion avulla.

6. Esitettävä konjunktio, disjunktio ja ekvivalenssi negaation ja implikaation avulla.

7. Määriteltävä poissulkeva tai-konnektiivi totuustaulukolla.

8. Shefferin viiva | (eli NAND) määritellään seuraavasti.

p	q	$p \mid q$
0	0	1
0	1	1
1	0	1
1	1	0

Esitettävä $\neg p$, $p \wedge q$ ja $p \vee q$ Shefferin viivan avulla.

9. Esitettävä $p \Rightarrow q$ ja $p \Leftrightarrow q$ Shefferin viivan avulla.

10. Peircen nuoli eli Nicodin funktio $\downarrow$ (eli NOR) määritellään seuraavasti.

p	q	$p \downarrow q$
0	0	1
0	1	0
1	0	0
1	1	0

Esitettävä $\neg p$, $p \wedge q$ ja $p \vee q$ Peircen nuolen avulla.

11. Esitettävä $p \Rightarrow q$ ja $p \Leftrightarrow q$ Peircen nuolen avulla.

12. Esitettävä Peircen nuoli Shefferin viivan avulla ja Shefferin viiva Peircen nuolen avulla.

13. Kuinka monta kahdelle lauseelle määriteltyä loogista konnektiivia on olemassa?

14. Lauseista p_1, p_2, ..., p_n muodostetaan loogisilla konnektiiveilla uusi lause. Kuinka monta vaakariviä sen totuustaulukossa on?

15. Tässä ja seuraavissa tehtävissä oletetaan, että valehtelija valehtelee aina kaikessa. Kreetalainen Epimedes[4] sanoi: ”Kaikki kreetalaiset ovat valehtelijoita”. Valehteliko hän vai puhuiko hän totta? Onko tämä *Epimedes-paradoksi* itse asiassa ollenkaan paradoksi?

16. Kuvitellaan, että Epimedes sanoikin: ”Minä olen valehtelija”. **a)** Valehteliko hän vai puhuiko hän totta? Osoitettava, ettei tämäkään ole varsinaisesti paradoksi. **b)** Näytettävä, että se kuitenkin johtaa seuraavaan kummalliselta tuntuvaan päättelyyn: Jos minä sanon olevani valehtelija, niin en ole valehtelija (siis en valehtele aina kaikessa).

17. Eubulides[5] sanoi: ”Nyt minä valehtelen”. Osoitettava, että tämä on paradoksi.

18. Buridan[6] ”todisti” Jumalan olemassaolon tarkastelemalla seuraavia lauseita.

1. Jumala on olemassa.
2. Kumpikaan näistä lauseista ei ole tosi.

Osoitettava, että ainoa tapa välttää paradoksi on päätellä, että Jumala on olemassa.

19. Albert Saksilainen[7] tarkasteli seuraavia lauseita.

1. Lause 2 on epätosi.
2. Lause 1 on tosi.

a) Osoitettava, että tämä on paradoksi. **b)** Mitä yhteyttä tällä on Buridanin ”todistukseen”?

20. Kallelta ja Villeltä kysyttiin heidän nimiään. Kumpikin vastasi: ”Minun nimeni on Kalle, mutta minä valehtelen”. Valehtelivatko he vai puhuivatko he totta?

1.2 Tautologia ja päättely

1 Tautologia

Olkoot p, q, r, ... mielivaltaisia suljettuja lauseita (täsmällisempää olisi puhua lausemuuttujista). Tällöin voimme esimerkiksi totuustaulukolla tutkia, miten näistä lauseista loogisilla konnektiiveilla muodostettujen

[4] *Epimedes (tai Epimenides, n. 600 eKr), kreetalainen profeetta.*
[5] *Eubulides Miletolainen (n. 400 eKr), kreikkalainen filosofi.*
[6] *Jean Buridan (n. 1295 – n. 1358), ranskalainen filosofi.*
[7] *Albert Saksilainen (1316–1390), saksalainen filosofi, teologi ja matemaatikko.*

uusien lauseiden totuusarvot riippuvat alkuperäisten totuusarvoista. Jos uusi lause on aina tosi, olivatpa lauseiden p, q, $r, \ldots$ totuusarvot mitkä tahansa, sanomme, että kysymyksessä on *tautologia*. Siis tautologia on ”identtisesti tosi” lause, joten tieto tautologian totuudesta ei kerro ”todellisuudesta” mitään, koska tautologia on tosi ”kaikissa mahdollisissa maailmoissa”. Jos vaikkapa p tarkoittaa lausetta ’sataa’ ja q lausetta ’tuulee’, niin lause $p \wedge q$ ei ole tautologia (se on epätosi jos p tai q on epätosi) ja se kertookin olennaisen asian säästä: sataa ja tuulee. Sen sijaan lause $p \vee \neg p$ on tautologia (esim. 2a) eikä se kerrokaan säästä mitään: sataa tai ei sada.

Alkeellisin menetelmä tautologisuuden osoittamiseksi on käyttää totuustaulukkoa.

Esimerkki 2. Osoitettava, että lause

a) $p \vee \neg p$, **b)** $p \wedge (p \Rightarrow q) \Rightarrow q$

on tautologia.

Alla olevista totuustaulukoista näemme, että nämä lauseet ovat tosia, olivatpa alkuperäisten lauseiden totuusarvot mitä tahansa.

a)

p	$\neg p$	$p \vee \neg p$
0	1	1
1	0	1

b)

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$p \wedge (p \Rightarrow q) \Rightarrow q$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

Pääsemme vähemmällä kirjoittamisella merkitsemällä uusien lauseiden totuusarvot vastaavien konnektiivien alle. Tosin taulukkoon tulee tällöin enemmän pystyrivejä, sillä alkuperäisten lauseiden totuusarvot on syytä merkitä jokaisen niiden esiintymän kohdalle. Taulukon lukemisen helpottamiseksi lisäämme alimmaiseksi vaakarivin osoittamaan, missä järjestyksessä pystyrivit ovat syntyneet.

a)

p	$\vee$	$\neg$	p
0	1	1	0
1	1	0	1
1	3	2	1

b)

p	$\wedge$	$(p$	$\Rightarrow$	$q)$	$\Rightarrow$	q
0	0	0	1	0	1	0
0	0	0	1	1	1	1
1	0	1	0	0	1	0
1	1	1	1	1	1	1
1	2	1	3	1	4	1

2 Tärkeitä tautologioita

Seuraavat tautologiat voidaan osoittaa oikeiksi totuustaulukoilla, mutta ne voidaan ymmärtää myös ”terveellä järjellä” eli ”luonnollisella päättelyllä” pohtimalla tällaisten lauseiden merkitystä luonnollisessa kielessä.

Tautologia	**Nimi**
$p \Leftrightarrow p$	Identiteetin laki
$\neg(p \wedge \neg p)$	Poissuljetun ristiriidan laki
$p \vee \neg p$	Poissuljetun kolmannen laki
$\neg\neg p \Leftrightarrow p$	Kaksoisnegaation laki
$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	de Morganin[8] säännöt
$p \wedge p \Leftrightarrow p$ $p \vee p \Leftrightarrow p$	Idempotenssilait
$p \wedge q \Leftrightarrow q \wedge p$ $p \vee q \Leftrightarrow q \vee p$	Vaihdantalait
$p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$ $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$	Liitäntälait
$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$	Osittelulait
$(p \Rightarrow q) \Leftrightarrow \neg p \vee q$ $(p \Rightarrow q) \Leftrightarrow \neg(p \wedge \neg q)$	Implikaation määritelmä

Näissä tautologioissa esiintyvät lauseet p ja q voivat olla myös yhdistettyjä lauseita.

Esimerkki 3. **a)** Identiteetin lain perusteella lause $(p \wedge q) \Leftrightarrow (p \wedge q)$ on tautologia. **b)** Poissuljetun kolmannen lain perusteella lause $\neg(p \wedge q \Rightarrow r) \vee (p \wedge q \Rightarrow r)$ on tautologia.

3 Merkinnöistä $\Leftrightarrow$ ja $\Rightarrow$

Jos lause $p \Leftrightarrow q$ on tautologia, niin lauselogiikan kannalta lauseiden p ja q merkitys on sama, ja sanomme, että lauseet p ja q ovat *yhtäpitävät* eli *ekvivalentit*. Merkitsemme tällöin $p \equiv q$.

Logiikassa pitää erottaa toisistaan *objektikieli* (jota tutkitaan) ja *metakieli* (jolla tutkitaan). Kun siis tutkimme lauselogiikkaa suomen kielellä, niin objektikielenä on lauselogiikan kieli ja metakielenä on suomen kieli. Merkinnät '$p \Leftrightarrow q$' ja '$p \vee q \Leftrightarrow q \vee p$' ovat siis objektikielen ilmaisuja, kun taas lauseet '$p \Leftrightarrow q$ ei ole tautologia', 'lause $p \vee q \Leftrightarrow q \vee p$ on tautologia', '$p \vee q$ joss $q \vee p$' ja '$p \vee q \equiv q \vee p$' ovat metakielen ilmaisuja. Oikeastaan logiikassa on tapana käyttää objektikielen implikaatiolle ja ekvivalenssille merkintöjä $\rightarrow$ ja $\leftrightarrow$, jolloin merkinnät $\Rightarrow$ ja $\Leftrightarrow$ ovat metakielen käytössä. Tällöin voidaan merkitä $p \Rightarrow p$ ja $p \Leftrightarrow p$ tarkoittamaan, että lauselogiikan lauseet $p \rightarrow p$ ja $p \leftrightarrow p$ ovat tautologioita. Matematiikassa ei kuitenkaan

[8] *Augustus de Morgan (1806–1871), englantilainen matemaatikko.*

tarvitse muuten kuin logiikkaa tutkittaessa tehdä eroa objektikielen ja metakielen implikaatioiden ja ekvivalenssien välillä, joten tulemme toimeen yhdellä implikaatiomerkillä $\Rightarrow$ ja yhdellä ekvivalenssimerkillä $\Leftrightarrow$.

Liitäntälain mukaan lauseiden $p \wedge (q \wedge r)$ ja $(p \wedge q) \wedge r$ merkitys on sama, joten voimme jättää sulut pois ja käyttää merkintää $p \wedge q \wedge r$ kummallekin. Vastaavasti otamme käyttöön merkinnän $p \vee q \vee r$. Voimme yleistää nämä merkintäsopimukset koskemaan myös useamman kuin kolmen lauseen disjunktiota ja konjunktiota. *Metakielessä* (mutta ei objektikielessä, teht. 29) on kätevää käyttää myös implikaatio- ja ekvivalenssiketjuja. Tällöin esimerkiksi ketju $p \Leftrightarrow q \Leftrightarrow r$ eli 'p joss q joss r' tarkoittaa, että p, q, r ovat keskenään ekvivalentit, ja ketju $p \Rightarrow q \Rightarrow r$ tarkoittaa, että p:stä seuraa q ja q:sta seuraa r (ja täten myös, että p:stä seuraa r).

Yhdistetty lause ei lauselogiikan kannalta muutu merkitykseltään, jos jonkin siinä esiintyvän lauseen tilalle sijoitetaan loogisesti ekvivalentti lause. Täten voimme etsiä annetun lauseen kanssa yhtäpitäviä lauseita vaiheittain käyttämällä hyväksi tunnettuja tautologioita.

Esimerkki 4. ”Sievennettävä” lause $\neg(p \vee q \Rightarrow \neg p \wedge \neg q)$ esittämällä mahdollisimman yksinkertainen sen kanssa yhtäpitävä lause.

Soveltamalla implikaation määritelmää, kaksoisnegaatiota (kolmessa paikassa), de Morganin sääntöä ja idempotenssilakia saamme

$$\begin{aligned} \neg(p \vee q \Rightarrow \neg p \wedge \neg q) &\equiv \neg\neg\big((p \vee q) \wedge \neg(\neg p \wedge \neg q)\big) \\ &\equiv (p \vee q) \wedge (\neg\neg p \vee \neg\neg q) \\ &\equiv (p \vee q) \wedge (p \vee q) \equiv p \vee q. \end{aligned}$$

Tutkimamme lause on siis yhtäpitävä lauseen $p \vee q$ kanssa eli lause

$$\neg(p \vee q \Rightarrow \neg p \wedge \neg q) \Leftrightarrow p \vee q$$

on tautologia.

Lauselogiikan kannalta yhtäpitävissä lauseissa voi luonnollisessa kielessä olla vivahde-eroja. Vaikka esimerkiksi kaksinkertaisella kiellolla saadaan alkuperäisen lauseen kanssa loogisesti yhtäpitävä lause, tätä kieltoa käytetään usein eräänlaisena lieventäjänä. Jos esimerkiksi tietyn maan asiat ovat huonosti, niin vastuussa ollut poliittinen johtaja ei yleensä totea suoraan: ”Maan asiat ovat huonosti”, vaan jotenkin siihen tapaan, että ”Ei voida sanoa, että maan asiat ovat hyvin”. Vaikka näillä lauseilla on sama looginen sisältö, kuulija voi suhtautua niihin eri tavalla.

4 Päättely

Tarkastelemme perinteistä esimerkkiä

1. Kaikki ihmiset ovat kuolevaisia.
2. Sokrates on ihminen.
3. Siis Sokrates on kuolevainen.

Lauseet 1 ja 2 ovat *oletukset* eli *premissit*, ja lause 3 on *johtopäätös*. Päättely tuntuu *pätevältä*: koska kaikki ihmiset ovat kuolevaisia ja Sokrates on ihminen, niin varmasti silloin Sokrateskin on kuolevainen. Olennaista ei ole, ovatko kaikki ihmiset varmasti kuolevaisia tai kuka tai mikä Sokrates on. Olennaista on, että jos pidämme näitä oletuksia tosina, niin meidän tuntuu olevan pakko hyväksyä myös johtopäätös todeksi. Myös päättely

1. Kaikki antiikin kreikkalaiset tutkivat geometriaa.
2. Sokrates oli antiikin kreikkalainen.
3. Siis Sokrates tutki geometriaa.

tuntuu pätevältä, vaikka tiedämme, etteivät kaikki antiikin kreikkalaiset tutkineet geometriaa. Vaikka tämä *päättely* on oikea, emme tiedä, onko sen johtopäätös tosi vai epätosi. Emme näet tiedä, tutkiko Sokrates geometriaa vai ei.

Pätevä päättely *säilyttää totuuden*: jos premissit ovat tosia, niin myös johtopäätös on tosi. Voimme osoittaa päättelyn epäpäteväksi tarkastelemalla sellaista tilannetta, jossa premissit ovat tosia, mutta johtopäätös on epätosi. Jos keksimme tällaisen *vastaesimerkin*, niin päättely ei ole pätevä. Mutta jos johtopäätös on tosi aina, kun premissit toteutuvat, niin päättely on pätevä.

Todistusteoriassa tutkitaan johtopäätösten tekemistä premisseistä erilaisten päättelysääntöjen avulla. Tällöin päättelyt voidaan esittää täysin formaalisti, joten voimme tunnistaa pätevät päättelyt pelkästään niiden muodon perusteella. Yllä esittämämme päättelyt ovat logiikan kannalta samaa muotoa

$$\begin{array}{ll} \text{Premissit:} & \text{Jokainen } A \text{ on } B \\ & s \text{ on } A \\ \hline \text{Johtopäätös:} & s \text{ on } B \end{array}$$

Kaikessa inhimillisessä toiminnassa tehdään jatkuvasti päättelyjä vetoamatta mihinkään muodollisiin päättelysääntöihin. Tällöin symbolien tilalla tai niiden lisäksi käytetään luonnollista kieltä. Olemme jo aiemmin kutsuneet tällaista päättelyä *luonnolliseksi päättelyksi*. Sen vastakohta ei ole ”luonnoton” päättely vaan *formaali päättely*, joka äärimuodossaan voi olla (kirjaimellisestikin) pelkkää koneellista symbolien käsittelyä. (Puhuessamme luonnollisesta päättelystä emme tarkoita logiikassa olevia formaaleja luonnollisen päättelyn systeemejä. Nämä systeemit ovat saanet nimensä siitä, että niissä pyritään käyttämään sellaisia päättelysääntöjä, jotka vastaavat luonnollista päättelyä mahdollisimman hyvin.)

5 Päättelyn formalisoinnista

Kaikkea pätevää päättelyä ei voida formalisoida. Matematiikassakin käytetään tavallisesti luonnollista päättelyä. Logiikan periaatteetkin on viime kädessä perusteltava luonnollisella päättelyllä. Logiikan tutkiminen auttaa kuitenkin matemaattisten päättelyjen ymmärtämistä. Matemaattiset päättelyt ovat usein pitkiä ja monimutkaisia, ja aloittelijan saattaa olla vaikea varmistua tällaisen päättelyn pätevyydestä. Logiikassa tutkitaan päättelyä pelkistetyssä muodossa, jolloin päteviä päättelyjä on helpompi oppia tunnistamaan ja tekemään.

Voimme siis tehdä lauselogiikassa premisseistä p_1, p_2, …, p_n johtopäätöksen q, jos lause q ei voi olla epätosi premissien ollessa tosia. Implikaation ja konjunktion määritelmän perusteella tämä on yhtäpitävää sen kanssa, että lause $p_1 \wedge p_2 \wedge \cdots \wedge p_n \Rightarrow q$ on aina tosi. Saamme siis yksinkertaisen kriteerin pätevälle päättelylle.

> Premisseistä p_1, p_2, …, p_n voidaan tehdä johtopäätös q, jos (ja lauselogiikassa vain jos) $p_1 \wedge p_2 \wedge \cdots \wedge p_n \Rightarrow q$ on tautologia.

Esimerkiksi tautologiaa

$$p \wedge (p \Rightarrow q) \Rightarrow q$$

vastaa päättelysääntö *modus ponendo ponens* eli lyhyemmin *modus ponens*

$$\begin{array}{l} p \\ p \Rightarrow q \\ \hline q \end{array}$$

Matematiikassa käytetään usein tätä päättelyä, sillä tavanomainen päättelykaavio on tehdä premisseistä ’oletus pitää paikkansa’ ja ’jos oletus pitää paikkansa, niin väitös pitää paikkansa’ johtopäätös ’väitös pitää paikkansa’.

6 Lisää tärkeitä tautologioita

Jatkamme tautologiakokoelmaamme luettelemalla sellaisia tautologioita, jotka esiintyvät usein matemaattisissa todistuksissa ja joissa implikaatio on keskeisellä sijalla. Tautologioille antamamme nimet ovat itse asiassa niitä vastaavien päättelysääntöjen nimiä.

Tautologia	**Nimi**
$(p \Leftrightarrow q) \Leftrightarrow (p \Rightarrow q) \wedge (q \Rightarrow p)$	Ekvivalenssin ja implikaation yhteys
$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$	Kontrapositio
$p \wedge (p \Rightarrow q) \Rightarrow q$	Modus ponendo ponens
$(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p$	Modus tollendo tollens
$p \wedge (\neg q \Rightarrow \neg p) \Rightarrow q$	Reductio ad absurdum eli epäsuoran todistamisen sääntö
$(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$	Syllogismi

7 Lauselogiikan heikkoudesta päättelyissä

Lauselogiikkaa voidaan käyttää eräiden luonnollisella kielellä esitettyjen päättelyjen formalisoinnissa.

Esimerkki 5. Tarkastelemme Origeneen[9] päättelyä

1. Jos tiedän olevani *kuollut*, niin olen kuollut.
2. Jos *tiedän* olevani kuollut, niin en ole kuollut.
3. Siis en tiedä olevani kuollut.

Lauseet 1 ja 2 ovat siis premissejä ja 3 johtopäätös. Merkitsemällä $p =$ 'Tiedän olevani kuollut' ja $q =$ 'Olen kuollut' saamme tämän päättelyn muotoon

$$\begin{array}{l} p \Rightarrow q \\ \underline{p \Rightarrow \neg q} \\ \neg p \end{array}$$

Lause $(p \Rightarrow q) \wedge (p \Rightarrow \neg q) \Rightarrow \neg p$ on tautologia (teht. 32b), joten Origeneen päättely on loogisesti oikea. Tällä päättelyllä ei kuitenkaan voida sanoa mitään premissien eikä siis myöskään johtopäätöksen oikeellisuudesta.

Yritämme nyt formalisoida kohdan 4 alussa esitettyä päättelyä, jota merkitsemme (S):llä. Merkitsemällä $p =$ 'Kaikki ihmiset ovat kuolevaisia', $q =$ 'Sokrates on ihminen' ja $r =$ 'Sokrates on kuolevainen' saamme sen muotoon

$$\begin{array}{c} p \\ \underline{q} \\ r \end{array}$$

Lause $p \wedge q \Rightarrow r$ ei kuitenkaan ole tautologia. Tästä ei tietenkään seuraa, että (S) olisikin epäpätevä. Meidän on vain todettava, että emme pysty osoittamaan sen pätevyyttä lauselogiikan avulla. Lauselogiikka on kielenä niin alkeellinen, ettei näinkään yksinkertaista päättelyä voida siinä järkevästi formalisoida. Seuraavassa luvussa tutustumme *ensimmäisen kertaluvun predikaattilogiikkaan*, jonka avulla voimme tehdä niin. Emme kuitenkaan perehdy tähän kieleen niin perusteellisesti, että voisimme muodollisesti osoittaa (S):n päteväksi.

Harjoitustehtäviä

21. Todistettava tautologiaksi **a)** $p \wedge p \Leftrightarrow p \vee p$, **b)** $p \Rightarrow (\neg p \Rightarrow p)$. Miten nämä tautologiat voidaan perustella luonnollisella päättelyllä?

22. Valittava de Morganin säännöistä toinen ja todistettava se tautologiaksi. Miten tämä tautologia voidaan perustella luonnollisella päättelyllä?

23. Valittava osittelulaeista toinen ja todistettava se tautologiaksi. Miten tämä tautologia voidaan perustella luonnollisella päättelyllä?

[9] *Origenes (n. 185–254), kreikkalainen teologi.*

24. Olkoot p ja q tosia lauseita. Onko lause

$$\neg\big(\neg(p \Rightarrow \neg q) \vee \neg(q \Rightarrow \neg p)\big)$$

tosi vai epätosi? Käsiteltävä tehtävä **a)** totuustaulukon vastaavan vaakarivin perusteella, **b)** sieventämällä aluksi lause eli kirjoittamalla logiikan lakien avulla sen kanssa yhtäpitävä mahdollisimman yksinkertainen lause.

25. Määritellään loogiset vakiot $\top$ (verum) ja $\bot$ (falsum)

$\top$
1

$\bot$
0

Siis $\top$ on aina tosi ja $\bot$ epätosi. Todistettava tautologiaksi

a) $p \vee \top \Leftrightarrow \top$, **b)** $p \wedge \bot \Leftrightarrow \bot$, **c)** $p \wedge \top \Leftrightarrow p$, **d)** $p \vee \bot \Leftrightarrow p$.

Miten nämä tautologiat voidaan perustella luonnollisella päättelyllä?

26. Todistettava tautologiaksi

a) $p \vee \neg p \Leftrightarrow \top$, **b)** $p \wedge \neg p \Leftrightarrow \bot$,

c) $(p \Rightarrow \top) \Leftrightarrow \top$, **d)** $(\bot \Rightarrow p) \Leftrightarrow \top$.

Miten nämä tautologiat voidaan perustella luonnollisella päättelyllä?

27. Etsittävä tunnettuja tautologioita (myös tehtävissä 25 ja 26 esitettyjä sääntöjä) käyttämällä mahdollisimman yksinkertainen lauseen $p \Rightarrow (q \wedge p)$ kanssa yhtäpitävä lause, joka sisältää vain konnektiiveja $\neg$ ja $\wedge$. Tarkistettava tulos totuustaulukolla.

28. Negaatiota ei voida määritellä konjunktion, disjunktion, implikaation ja ekvivalenssin avulla (s. 46, teht. 99). Muuttuuko tilanne, jos sallitaan loogisten vakioiden $\top$ ja $\bot$ käyttö?

29. Voidaanko (objektikielessä) käyttää merkintää **a)** $p \Leftrightarrow q \Leftrightarrow r$ tarkoittamaan sekä lausetta $p \Leftrightarrow (q \Leftrightarrow r)$ että $(p \Leftrightarrow q) \Leftrightarrow r$, **b)** $p \Rightarrow q \Rightarrow r$ tarkoittamaan sekä lausetta $p \Rightarrow (q \Rightarrow r)$ että $(p \Rightarrow q) \Rightarrow r$?

30. Osoitettava tautologiaksi sieventämällä ekvivalenssin vasemmasta puolesta oikea puoli

a) $(p \wedge q \Rightarrow p) \Leftrightarrow \top$, **b)** $(q \Rightarrow p) \wedge (\neg p \Rightarrow q) \wedge (q \Rightarrow q) \Leftrightarrow p$.

31. Osoitettava tautologiaksi **a)** modus tollendo tollensia, **b)** syllogismia vastaava lause. Esitettävä esimerkki näiden päättelysääntöjen käytöstä.

32. **a)** Osoitettava tautologiaksi epäsuoran todistamisen sääntöä vastaava lause. Esitettävä esimerkki tämän päättelysäännön käytöstä. **b)** Osoitettava tautologiaksi lause $(p \Rightarrow q) \wedge (p \Rightarrow \neg q) \Rightarrow \neg p$ (esim. 5).

33. Formalisoitava seuraavat lauseet ja tutkittava, ovatko ne tautologioita.

a) Jos ja vain jos ulkona on kuutamo, niin teen töitä tai en tee.

b) Jos minä maatani rakastaisin,
polttaisin sen lipun
ja antaisin tuulen vapaasti
hulmuta ilmassa.

(Parkkinen [18], ks. myös Miettinen [16], teht. 5d).

34. Osoitettava seuraavat päättelysäännöt päteviksi.

a) $\dfrac{p}{p \vee q}$, **b)** $\dfrac{p \wedge q}{p}$, **c)** $\dfrac{\neg\neg p}{p}$, **d)** $\dfrac{p \Leftrightarrow q}{\neg p \Leftrightarrow \neg q}$.

35. Perusteltava alla olevan päättelyn pätevyys sekä lauselogiikan avulla että luonnollisella päättelyllä.

$$\begin{array}{l} p \vee q \\ p \Rightarrow r \\ q \Rightarrow r \\ \hline r \end{array}$$

36. Formalisoitava seuraava päättely ja tutkittava sen pätevyyttä.

1. Jos sataa, niin kalastamme, ja jos ei sada, niin uimme.
2. Kalastamme, jos emme ui.
3. Siis uimme, jos ja vain jos emme kalasta.

37. Formalisoitava seuraava päättely ja tutkittava sen pätevyyttä.

1. Jos menet naimisiin, niin kadut.
2. Jos et mene naimisiin, niin sitäkin kadut.
3. Jos siis menet naimisiin tai olet menemättä, niin joka tapauksessa kadut.

(Kierkegaard[10], ks. esim. Lehtinen [9], s. 96).

38. a) Tutkittava seuraavan kreikkalaisten sofistien päättelyn pätevyyttä.

1. Mitä et ole menettänyt, se sinulla on.
2. Et ole menettänyt sarvia.
3. Siis sinulla on sarvet.

b) Voidaanko tämä päättely formalisoida lauselogiikassa?

39. a) Aaro, Eero ja Iiro ovat taitavia loogikkoja (he myös tietävät toistensa taidot). Heidän kaikkien päähän pannaan hattu niin, etteivät he näe oman hattunsa väriä. Heille sanotaan: ”Hatut ovat punaisia tai vihreitä. Jos näet punaisen hatun, niin nosta kätesi.” Kaikkien hatut ovat punaisia, joten kaikki nostavat kätensä. Aarolta, Eerolta ja Iirolta kysytään

[10] *Søren Kierkegaard (1813–1855), tanskalainen filosofi.*

tässä järjestyksessä, minkä värinen hänen hattunsa on. Kuka tietää vastausvuorollaan hattunsa värin? **b)** Seurueessa on neljä loogikkoa, joille asetetaan sama tehtävä. Kaikkien hatut ovat punaisia. Jokaiselta kysytään vuoronperään, minkä värinen hänen hattunsa on. Mitä tapahtuu? **c)** Sama kysymys, kun seurueessa on n ($n > 4$) loogikkoa.

40. Pyhiinvaeltaja oli matkalla Mekkaan. Erääseen tienhaaraan tullessaan hän tiesi, että haarautuvista teistä toinen vei Mekkaan ja toinen ei, mutta ei tiennyt kumpi. Edelleen hän tiesi, että tienhaarassa on jompikumpi kahdesta oppaasta, joista toinen aina valehtelee ja toinen aina puhuu totta, mutta hän ei tiennyt kumpi. Opas suostui vastaamaan vain yhteen kysymykseen. Miten pyhiinvaeltaja sai selville oikean tien?

1.3 Predikaattilogiikkaa

1 Predikaatti eli avoin lause

Esimerkiksi '$2 + 2 = 5$' ja '$2 + 3 = 5$' ovat propositioita eli suljettuja lauseita, joista edellinen on epätosi ja jälkimmäinen tosi. Sen sijaan '$x + 2 = 5$' ei ole suljettu lause, sillä sen totuusarvo riippuu muuttujan x arvosta. Tällaisten väitteiden tutkiminen on kuitenkin logiikassa välttämätöntä. Olemmehan juuri huomanneet, että lauselogiikka on aivan liian alkeellinen menetelmä hiemankin monimutkaisempien päättelyjen formalisoimiseksi.

Predikaatilla eli *avoimella lauseella* tarkoitamme väitettä, jonka totuusarvo riippuu muuttujasta. Käytämme myös predikaatista epätäsmällistä nimitystä 'lause'. Se joukko, josta muuttuja valitaan, on predikaatin (tai, kuten myös sanotaan, predikaatin muuttujan) *määrittelyjoukko.*

Esimerkki 6. **a)** Predikaatin '$x + 2 = 5$' määrittelyjoukoksi voimme ottaa vaikkapa reaalilukujen joukon. Käytämme tälle predikaatille merkintää $p(x)$, jolloin esimerkiksi $p(1)$ ja $p(2)$ ovat epätosia, kun taas $p(3)$ on tosi. **b)** Predikaatin $q(x) =$ 'x on kala' määrittelyjoukoksi on luonnollista ottaa kaikkien eläinlajien joukko. Siis esimerkiksi q(hauki) ja q(lahna) ovat tosia, mutta q(lehmä) ja q(ihminen) ovat epätosia.

Predikaatti eli avoin lause $p(x)$ on siis ilmaisu, josta saadaan propositio eli suljettu lause aina, kun muuttujan x paikalle sijoitetaan predikaatin määrittelyjoukon alkio (täsmällisemmin: alkion nimi).

Edellä käsitellyt predikaatit ovat *yksipaikkaisia* eli ne sisältävät yhden muuttujan. Myös useampipaikkaisia predikaatteja voidaan tutkia.

Esimerkki 7. **a)** Predikaatin $p(x, y) =$ 'x on kirjoittanut kirjan nimeltä y' muuttujan x määrittelyjoukko voi olla vaikkapa kaikkien ihmisten joukko ja muuttujan y määrittelyjoukko kaikkien kirjojen joukko. **b)** Predikaatin $q(x, y) =$ '$x^2 + y^2 < 1$' kummankin muuttujan määrittelyjoukko voi olla reaalilukujen joukko. Vastaava suljettu lause on tosi, jos piste (x, y) on ympyrän $x^2 + y^2 = 1$ sisällä, ja epätosi muulloin.

Yksipaikkainen predikaatti ilmaisee tiettyä *ominaisuutta*: jos $p(x)$ on alkiolla x_0 tosi, niin voimme myös sanoa, että tällä alkiolla on ominaisuus p. Mitä yhteyttä logiikan predikaatilla on sitten kieliopin predikaatin kanssa? Karkea tapa jäsentää luonnollisella kielellä kirjoitettu lause on jakaa se kahteen osaan: mitä tehdään ja kuka tai mikä tekee. Esimerkiksi lauseessa 'Hauki on kala' ollaan kaloja, tekijänä hauki, ja lauseessa 'Kalle opiskelee logiikkaa' opiskellaan logiikkaa, tekijänä Kalle. Tekijää eli subjektia vastaa meillä logiikassa määrittelyjoukon alkio, ja sen, mitä lauseessa tehdään, ilmoittaa predikaatti. Tämä riittää logiikassa, mutta luonnollisessa kielessä lause jäsennetään tavallisesti sanojen tarkkuudella (subjekti-predikaatti-objekti, subjekti-predikaatti-predikatiivi jne).

Kaksi- tai useampipaikkaiset predikaatit ilmoittavat *suhteita* määrittelyjoukkojen alkioiden välillä: jos $p(x, y)$ on tosi tietyillä alkioilla x_0 ja y_0, niin voimme sanoa, että nämä alkiot ovat keskenään suhteessa p.

2 Kvanttorit

Tarvitsemme joukko-opista muutaman merkinnän. Jos x *kuuluu joukkoon* A eli x on joukon A *alkio*, niin merkitsemme $x \in A$. Jos $\neg\ x \in A$ eli x ei kuulu joukkoon A, niin merkitsemme $x \notin A$. *Tyhjässä joukossa* $\emptyset$ ei ole alkioita. Merkitsemme $\{x_1, x_2, \dots, x_n\}$ tarkoittamaan joukkoa, jonka alkiot ovat x_1, x_2, …, x_n. Edelleen merkitsemme, että

- $\mathbb{N}$ on luonnollisten lukujen 0, 1, 2, … joukko
- $\mathbb{Z}$ on kokonaislukujen joukko
- $\mathbb{Z}_+$ on positiivisten kokonaislukujen 1, 2, 3, … joukko
- $\mathbb{Z}_-$ on negatiivisten kokonaislukujen -1, -2, $-3, \dots$ joukko
- $\mathbb{Q}$ on rationaalilukujen joukko, $\mathbb{Q}_+$ positiivisten ja $\mathbb{Q}_-$ negatiivisten
- $\mathbb{R}$ on reaalilukujen joukko, $\mathbb{R}_+$ positiivisten ja $\mathbb{R}_-$ negatiivisten
- $\mathbb{C}$ on kompleksilukujen joukko.

Oletamme siis nämä joukot tunnetuiksi. Kysymys siitä, mitä nämä lukujoukot oikeastaan ovat, ei ole mitenkään yksinkertainen, ks. esim. Ebbinghaus ym. [2]. Luonnollisten lukujen määrittelyssä on kirjavuutta, sillä niillä tarkoitetaan usein positiivisia kokonaislukuja.

Olkoon $p(x)$ joukossa X määritelty predikaatti ja olkoon A jokin sellainen joukko joukon X alkioita, että $p(x)$ on tosi aina, kun $x \in A$. Siis joukon A *kaikilla* alkioilla on ominaisuus p. Tällöin sanomme, että lause

$$\forall x \in A \colon p(x)$$

on tosi. Muussa tapauksessa tämä lause on epätosi. Symboli $\forall$ on *universaalikvanttori* eli *kaikkikvanttori*. Lause luetaan: ”Joukon A kaikilla alkioilla on ominaisuus p” tai ”Ominaisuus $p(x)$ on voimassa aina, kun $x \in A$”. Matematiikassa on joskus mukava käyttää merkinnän $\forall x \in A \colon p(x)$ sijasta merkintää $p(x), \forall x \in A$, mutta silloin rikotaan predikaattilogiikan kielen sääntöjä.

Esimerkki 8. Lause
$$\forall x \in \mathbb{R}\colon x^2 \geq 0$$
tarkoittaa, että jokaisen reaaliluvun neliö on ei-negatiivinen, ja on siis tosi.

Esimerkki 9. Palaamme edellisessä luvussa olevaan päättelyyn

1. Kaikki ihmiset ovat kuolevaisia.
2. Sokrates on ihminen.
3. Siis Sokrates on kuolevainen.

Formalisoimme tämän päättelyn predikaattilogiikassa. Merkitsemällä $I(x)$ = 'x on ihminen', $K(x)$ = 'x on kuolevainen' ja s = 'Sokrates' saamme sen muotoon

$$\forall x\big(I(x) \Rightarrow K(x)\big) \wedge I(s) \Rightarrow K(s)$$

eli

$$\begin{array}{l} \forall x\big(I(x) \Rightarrow K(x)\big) \\ I(s) \\ \hline K(s) \end{array}$$

Logiikassa käytetään merkintää $\forall x\big(p(x)\big)$ tarkoittamaan, että mielivaltaisella oliolla on ominaisuus p. Matematiikassa yleensä "rajoitetaan kvantifiointia" ilmoittamalla se joukko, jonka alkioihin viitataan. Merkitsemällä kaikkien ihmisten joukkoa I:llä saamme päättelymme matemaattisen merkintäsysteemin mukaiseen muotoon

$$\begin{array}{l} \forall x \in I\colon K(x) \\ s \in I \\ \hline K(s) \end{array}$$

Jos joukossa A on *ainakin yksi* alkio, jolla on ominaisuus p, niin sanomme, että lause
$$\exists x \in A\colon p(x)$$
on tosi. Muulloin tämä lause on epätosi. Symboli $\exists$ on *eksistenssikvanttori* eli *olemassaolokvanttori*, ja tämä lause luetaan: "Joukossa A on (olemassa ainakin yksi) sellainen alkio, jolla on ominaisuus p" tai "Ominaisuus p on voimassa ainakin yhdellä joukon A alkiolla".

Vaikka lauseissa $\forall x \in A\colon p(x)$ ja $\exists x \in A\colon p(x)$ on näkyvissä muuttuja x, nämä lauseet eivät ole avoimia vaan suljettuja. Nimittäin muuttuja x ei ole nyt *vapaa* vaan *sidottu*: sen paikalle ei sijoiteta mitään tiettyä A:n alkiota.

Esimerkki 10. Lause

$$\exists x \in \mathbb{R}\colon x^2 - 5x + 6 = 0$$

on tosi, sillä löytyy vieläpä kaksi reaalilukua, joilla on ominaisuus $x^2 - 5x + 6 = 0$, nimittäin luvut 2 ja 3.

Loogisia konnektiiveja ja kvanttoreita kutsutaan yhteisesti *loogisiksi operaattoreiksi*.

3 Useampi kuin yksi kvanttori

Kvanttoreita voidaan käyttää myös monipaikkaisten predikaattien yhteydessä.

Esimerkki 11. Tarkastelemme lauseita

$$\forall x \in \mathbb{R} \colon \forall y \in \mathbb{R} \colon x + y = 0, \tag{1}$$

$$\exists x \in \mathbb{R} \colon \exists y \in \mathbb{R} \colon x + y = 0, \tag{2}$$

$$\forall x \in \mathbb{R} \colon \exists y \in \mathbb{R} \colon x + y = 0, \tag{3}$$

$$\exists y \in \mathbb{R} \colon \forall x \in \mathbb{R} \colon x + y = 0. \tag{4}$$

Lauseessa (1) väitetään, että $x+y=0$ aina, kun x ja y ovat reaalilukuja. Tämä lause on tietenkin epätosi. Lause (2) sanoo, että on olemassa sellaiset reaaliluvut x ja y, joilla on ominaisuus $x+y=0$, ja on siis tosi, sillä tällaisia parejahan on peräti ääretön määrä. Lause (3) tarkoittaa: ”Kaikilla reaaliluvuilla x on olemassa sellainen reaaliluku y, että $x + y = 0$”. Parempaa suomen kieltä ehkä olisi: ”Jokaista reaalilukua x kohti on olemassa. . . ” tai ”Aina kun x on mielivaltainen reaaliluku, on olemassa. . . ”. Tämä lause on tosi, sillä y:ksi kelpaa $-x$. Lause (4) kuuluu: ”On olemassa sellainen reaaliluku y, että kaikilla reaaliluvuilla x on voimassa $x+y=0$” eli ”Löytyy sellainen reaaliluku y, että $x + y = 0$, olipa x mikä tahansa reaaliluku”. Tämä lause on epätosi. Jos näet tällainen y olisi, niin täytyisi olla esimerkiksi $0 + y = 0$ ja $1 + y = 0$, mikä on mahdotonta.

Tarkastelemme vielä lauseita (3) ja (4). Voimme ajatella, että lause (4) saadaan lauseesta (3) siirtämällä olemassaolokvanttori kaikkikvanttorin oikealta puolelta vasemmalle. Tosi lause (3) muuttuu näin epätodeksi lauseeksi (4). Yleensäkin tällaisessa siirrossa saadaan alkuperäistä lausetta *ankarampi* lause. (Siis uusi lause on varmasti epätosi, jos vanha lause on epätosi, mutta saattaa olla epätosi silloinkin, kun vanha lause on tosi.) Tämä johtuu siitä, että lauseessa (3) y saa riippua x:stä, mutta lauseessa (4) saman y:n on kelvattava kaikille x:lle.

Esimerkki 12. Tarkastelemme predikaattia $n(x,y) =$ ’x on naimisissa y:n kanssa’, jossa muuttujan x määrittelyjoukko M on tietty joukko aviomiehiä ja muuttujan y määrittelyjoukko N on heidän vaimojensa joukko. Tällöin lause

$$\forall x \in M \colon \exists y \in N \colon n(x,y)$$

on tosi, sillä jokaiselle miehelle löytyy vaimo. Lause

$$\exists y \in N \colon \forall x \in M \colon n(x,y)$$

sen sijaan on epätosi (jos joukossa M ja siis myös N on alkioita enemmän kuin yksi), sillä ei voi löytyä naista, joka on naimisissa kaikkien miesten kanssa (Suomen avioliittolainsäädännön mukaan).

Käsittelemme vielä esimerkin tapauksesta, jossa tosi lause säilyy totena tällaisessa siirrossa.

Esimerkki 13. Lause

$$\forall x \in \mathbb{R}\colon \exists y \in \mathbb{R}\colon xy = 0$$

on tosi, sillä aina, kun x on annettu reaaliluku, löytyy sellainen y, että $xy = 0$, nimittäin $y = 0$. Mutta tämä y ei riipu x:stä, joten on olemassa sellainen y (nimittäin juuri tämä $y = 0$), että kaikilla x:llä on $xy = 0$. Täten myös lause

$$\exists y \in \mathbb{R}\colon \forall x \in \mathbb{R}\colon xy = 0$$

on tosi.

4 Loogisten konnektiivien käyttö

Lauselogiikan konnektiivien avulla voidaan yhdistää myös avoimia lauseita ja muodostaa siten uusia avoimia lauseita. Nekin voidaan sulkea kvanttoreilla.

Esimerkki 14. Avoimesta lauseesta

$$x + 1 > 0 \wedge 2x - 3 < 0$$

saamme olemassaolokvanttorilla suljetun lauseen

$$\exists x \in \mathbb{R}\colon x + 1 > 0 \wedge 2x - 3 < 0,$$

joka on tosi (miksi?).

Esimerkki 15. Tarkastelemme lausetta

$$\forall x \in \mathbb{R}\colon x > 0 \Rightarrow x + 1 > 0. \tag{1}$$

Tutkimme predikaatin $x > 0 \Rightarrow x + 1 > 0$ (täsmällisemmin: predikaatista sijoittamalla saadun suljetun lauseen) totuutta muuttujan x eri arvoilla. Saamme seuraavan taulukon.

	$x > 0$	$\Rightarrow$	$x + 1 > 0$
$x \leq -1$	0	1	0
$-1 < x \leq 0$	0	1	1
$x > 0$	1	1	1

Siis lause (1) on tosi. Näemme totuustaulukon viimeiseltä vaakariviltä, että kaikki ne reaaliluvut x, jotka toteuttavat ehdon $x > 0$, toteuttavat myös ehdon $x + 1 > 0$. Voimme täten ilman vaikeuksia tulkita tämän lauseen 'jos … niin' -ehdoksi eli lukea sen ”Jos $x > 0$, niin $x + 1 > 0$”.

Esimerkki 16. Lause

$$\forall x \in \mathbb{R}\colon x + 1 > 0 \Rightarrow x > 0$$

on epätosi. Nimittäin esimerkiksi arvolla $x = 0$ implikaation $x + 1 > 0 \Rightarrow x > 0$ edellinen jäsen on tosi ja jälkimmäinen epätosi.

Matematiikassa jätetään usein kaikkikvanttori kirjoittamatta lauseesta $\forall x \in X\colon p(x)$. Näin tehdään erityisesti silloin, kun $p(x)$ on implikaatiolla tai ekvivalenssilla saatu yhdistetty lause. Tällöin lausetta $p(x)$ ei tulkita avoimeksi lauseeksi, vaan siinä tulkitaan muuttujalla x olevan jokin kiinteä, mutta mielivaltainen arvo. Tällöin sanotaan usein: ”Olkoon x joukon X mielivaltainen alkio”, missä joukko X on muuttujan x määrittelyjoukko. Muussa tapauksessa määrittelyjoukon on selvittävä asiayhteydestä. Sovimme, että se on $\mathbb{R}$, ellei toisin mainita.

Esimerkki 17. Lauseesta

$$\neg\forall x \in \mathbb{R}\colon x+1>0 \Rightarrow x>0$$

ei voida jättää kaikkikvanttoria pois ilman, että sen merkitys muuttuu (miksei?). Tämä ei ole ristiriidassa yllä esitetyn kanssa, koska lause ei ala kaikkikvanttorilla. Ottamalla käyttöön merkinnän $\not\Rightarrow$ (lue: ”ei välttämättä seuraa”) voimme kirjoittaa tämän lauseen ilman kaikkikvanttoria muodossa

$$x+1>0 \not\Rightarrow x>0.$$

Näimme esimerkissä 15, että avointen lauseiden implikaatio on tulkittavissa ’jos … niin’ -ehdoksi. Tämä tulkinta saattaa kuitenkin tuntua oudolta implikaation edellisen jäsenen ollessa identtisesti epätosi. Esimerkiksi lause

$$x^2+x+1=0 \Rightarrow x=1$$

tuntuisi (määrittelyjoukossa $\mathbb{R}$) epätodelta, mutta tämä lause on tosi, sillä $x^2+x+1=0$ on aina epätosi. Identtisesti epätosi lause siis implikoi mitä tahansa lauseita. Ei kuitenkaan voida päätellä, että $x=1$ muka olisi yhtälön $x^2+x+1=0$ ratkaisu, sillä lause sanoo vain, että $x=1$ on *välttämätön* ehto ratkaisulle (siis muita ratkaisuja ei voi olla). Koska implikaatio toiseen suuntaan ei ole voimassa eli

$$x=1 \not\Rightarrow x^2+x+1=0,$$

niin tämä ehto ei kuitenkaan ole riittävä. Siis yhtälöllä $x^2+x+1=0$ ei ole (reaalisia) ratkaisuja.

Logiikassa sovitaan yleensä, että kvanttorin ”vaikutusalue” on sama kuin negaationkin eli kvanttoria välittömästi seuraava kaava. Matematiikassa tätä sääntöä ei aina noudateta, koska tuo vaikutusalue selviää tavallisesti asiayhteydestä. Yleensä sen tulkitaan ulottuvan ensimmäiseen sellaiseen konnektiiviin saakka, jota seuraa *suljettu* lause.

Esimerkki 18. **a)** Tulkitsemme merkinnän $\exists x \in \mathbb{R}\colon p(x) \wedge q(x)$ tarkoittavan lausetta $\exists x \in \mathbb{R}\colon \big(p(x) \wedge q(x)\big)$, vrt. esim. 14. **b)** Tulkitsemme merkinnän $\forall x \in \mathbb{R}\colon p(x) \Rightarrow q(x)$ tarkoittavan lausetta $\forall x \in \mathbb{R}\colon \big(p(x) \Rightarrow q(x)\big)$, vrt. esim. 15. **c)** Tulkitsemme merkinnän $\forall x \in \mathbb{R}\colon p(x) \Rightarrow p(0)$ tarkoittavan lausetta $\big(\forall x \in \mathbb{R}\colon p(x)\big) \Rightarrow p(0)$ eikä lausetta $\forall x \in \mathbb{R}\colon \big(p(x) \Rightarrow p(0)\big)$.

5 Luonnollinen päättely predikaattilogiikassa

Esimerkissä 15 lause $\forall x \in \mathbb{R}\colon p(x)$, missä $p(x) =$ '$x > 0 \Rightarrow x + 1 > 0$', on tosi, sillä avoin lause $p(x)$ on identtisesti tosi. Lauseen $p(x)$ identtinen totuus ei kuitenkaan ole perusteltavissa logiikan avulla vaan erisuuruuden $>$ ominaisuuksien perusteella. Voimme muodostaa sellaisiakin avoimia lauseita, joiden identtinen totuus seuraa suoraan lauselogiikasta. Jos nimittäin $p(x)$ on sellainen predikaatti, että lause $p(x)$ on tautologia, kun muuttujalla x ajatellaan olevan kiinteä (mutta mielivaltainen) arvo, niin lause $p(x)$ on identtisesti tosi ja lause $\forall x \in X: p(x)$ on täten tosi. Voimme joskus myös todeta suljetuista predikaattilogiikan lauseista konnektiiveilla muodostetun yhdistetyn lauseen totuuden pelkästään lauselogiikan avulla (teht. 56).

Predikaattilogiikan tosien lauseiden totuutta ei kuitenkaan yleensä voida perustella lauselogiikalla. Tällainen lause on esimerkiksi

$$\forall x \in \mathbb{R}\colon p(x) \Rightarrow p(0),$$

joten meidän on tyydyttävä käyttämään luonnollista päättelyä sen totuuden osoittamiseksi. Sama koskee kahta seuraavaa lausetta. (Joudumme käyttämään niissä sanaa 'lause' kahdessa eri merkityksessä.)

Lause 1 (Negaation siirto kvanttorin ohi). Olkoon $p(x)$ joukossa X määritelty predikaatti. Tällöin lauseet

$$\neg\forall x \in X: p(x) \Leftrightarrow \exists x \in X: \neg p(x) \tag{1}$$

ja

$$\neg\exists x \in X: p(x) \Leftrightarrow \forall x \in X: \neg p(x) \tag{2}$$

ovat tosia.

Todistamme kohdan (1) ja jätämme kohdan (2) harjoitustehtäväksi (teht. 55). Lause $\neg\forall x \in X: p(x)$ on tosi täsmälleen silloin, kun lause $\forall x \in X: p(x)$ on epätosi eli kun on olemassa ainakin yksi sellainen $x \in X$, että $p(x)$ on epätosi. Tämä on yhtäpitävää sen kanssa, että on olemassa ainakin yksi sellainen $x \in X$, että $\neg p(x)$ on tosi. Tämä taas tarkoittaa sitä, että lause $\exists x \in X: \neg p(x)$ on tosi. Olemme näin osoittaneet, että lause $\neg\forall x \in X: p(x)$ on tosi, jos ja vain jos lause $\exists x \in X: \neg p(x)$ on tosi.

Lause 2 (Kaikkikvanttorin siirto ekvivalenssiin). Olkoot $p(x)$ ja $q(x)$ joukossa X määriteltyjä predikaatteja. Tällöin päättely

$$\frac{\forall x \in X: p(x) \Leftrightarrow q(x)}{\forall x \in X: p(x) \Leftrightarrow \forall x \in X: q(x)}$$

on pätevä.

Todistus. Oletamme, että $\forall x \in X\colon p(x) \Leftrightarrow q(x)$. Kun siis $x \in X$ on mielivaltainen, niin $p(x)$, jos ja vain jos $q(x)$. Täten predikaatit $p(x)$ ja $q(x)$ ovat tosia samoilla x:n arvoilla. Siis $p(x)$ on tosi kaikilla $x \in X$ silloin ja vain silloin, kun myös $q(x)$ on tosi kaikilla $x \in X$. Toisin sanoen $\forall x \in X\colon p(x) \Leftrightarrow \forall x \in X\colon q(x)$.

Harjoitustehtäviä

Tehtävissä 41–47 on tutkittava, ovatko niissä esitetyt lauseet tosia vai epätosia.

41. **a)** $\forall x \in \mathbb{R}\colon x \geq -x$, **b)** $\forall x \in \mathbb{R}\colon x^2 = |x|^2$.

42. **a)** $\forall x \in \mathbb{Z}_+\colon (1+x)^2 > 1 + 2x$, **b)** $\forall x \in \mathbb{R}\colon (1+x)^2 > 1 + 2x$.

43. **a)** $\exists x \in \mathbb{R}\colon |x-1| < 0$, **b)** $\exists x \in \mathbb{Z}\colon 2x = 3x$.

44. **a)** $\forall x \in \mathbb{R}\colon x \in \mathbb{Z} \Rightarrow x + 2 \in \mathbb{Z}$, **b)** $\forall x \in \mathbb{R}\colon x \in \mathbb{Z} \Rightarrow \dfrac{x}{2} \in \mathbb{Z}$.

45. **a)** $\forall x \in \mathbb{R}_+\colon \forall y \in \mathbb{R}_+\colon y < x$, **b)** $\exists x \in \mathbb{R}_+\colon \exists y \in \mathbb{R}_+\colon y < x$.

46. **a)** $\forall x \in \mathbb{R}_+\colon \exists y \in \mathbb{R}_+\colon y < x$, **b)** $\exists y \in \mathbb{R}_+\colon \forall x \in \mathbb{R}_+\colon y < x$.

47. **a)** $\forall x \in \mathbb{N}\colon \exists y \in \mathbb{N}\colon y \leq x$, **b)** $\exists y \in \mathbb{N}\colon \forall x \in \mathbb{N}\colon y \leq x$.

48. Olkoon $p(x, y)$ predikaatti '$x + y = 2x - y$'. Ovatko seuraavat lauseet tosia vai epätosia?

a) $\forall x \in \mathbb{Z}\colon \exists y \in \mathbb{Z}\colon p(x, y)$, **b)** $\exists y \in \mathbb{Z}\colon \forall x \in \mathbb{Z}\colon p(x, y)$,

c) $\forall y \in \mathbb{Z}\colon \exists x \in \mathbb{Z}\colon p(x, y)$, **d)** $\exists x \in \mathbb{Z}\colon \forall y \in \mathbb{Z}\colon p(x, y)$.

49. Formalisoitava: **a)** Jokainen ei-kokonainen reaaliluku on kahden peräkkäisen kokonaisluvun välissä. **b)** Jokainen kokonaisluku on parillinen tai pariton.

50. Matemaattisessa analyysissa määritellään, että $\lim_{x \to x_0} f(x) = a$, jos jokaista positiivilukua ε kohti on olemassa sellainen positiiviluku δ_ε, että $|f(x) - a| < \varepsilon$ aina, kun $0 < |x - x_0| < \delta_\varepsilon$. Formalisoitava tämä määritelmä.

Tehtävissä 51–53 on tutkittava, ovatko niissä esitetyt lauseet tosia vai epätosia (joukossa $\mathbb{R}$).

51. **a)** $x = 3 \Rightarrow x^2 = 9$, **b)** $x^2 = 9 \Rightarrow x = 3$, **c)** $x < 3 \Rightarrow x^2 < 9$, **d)** $x^2 < 9 \Rightarrow x < 3$.

52. **a)** $x \neq 0 \Leftrightarrow |x| > 0$, **b)** $x > 0 \Leftrightarrow x = |x|$, **c)** $x^2 - 5x + 6 = 0 \Leftrightarrow x = 2 \wedge x = 3$, **d)** $x^2 - 5x + 6 = 0 \Leftrightarrow x = 2 \vee x = 3$.

53. **a)** $x^2 = -1 \Rightarrow x = 2$, **b)** $x^2 = -1 \Rightarrow x \neq 2$, **c)** $x^2 = -1 \Rightarrow x^2 \neq -1$.

54. Muodostettava lauseen **a)** $\forall x \in \mathbb{R}\colon x \geq 2 \vee x < 3$, **b)** $\exists x \in \mathbb{R}\colon 0 \leq x < 1$ negaatio siirtämällä negaatiokonnektiivi kvanttorin ohi. Mitkä ovat näin saatujen lauseiden totuusarvot?

55. Olkoon $p(x)$ joukossa X määritelty predikaatti. Osoitettava, että lause

$$\neg\exists x \in X : p(x) \Leftrightarrow \forall x \in X : \neg p(x)$$

on tosi.

56. Olkoon $p(x)$ joukossa $\mathbb{R}$ määritelty yksipaikkainen ja $q(x, y)$ kaksipaikkainen predikaatti. Osoitettava loogisesti todeksi

a) $\forall x \in \mathbb{R}\colon p(x) \Rightarrow \big(\exists x \in \mathbb{R}\colon \neg p(x) \Rightarrow \forall x \in \mathbb{R}\colon p(x)\big)$,

b) $\forall x \in \mathbb{R}\colon \exists y \in \mathbb{R}\colon \big(\neg q(x, y) \Rightarrow q(y, y)\big) \Leftrightarrow \big(\neg q(y, y) \Rightarrow q(x, y)\big)$.

57. Esitettävä sellaiset predikaatit $p(x)$ ja $q(x)$, että lauseet

$$\forall x \in \mathbb{R}\colon p(x) \Leftrightarrow q(x)$$

ja

$$\forall x \in \mathbb{R}\colon p(x) \Leftrightarrow \forall x \in \mathbb{R}\colon q(x)$$

eivät ole yhtäpitäviä. Vrt. lause 2.

58. Formalisoitava seuraava päättely ja tutkittava sen pätevyyttä.

1. 2 on transkendenttiluku.
2. Mikään transkendenttiluku ei ole algebrallinen luku.
3. Jokainen rationaaliluku on algebrallinen luku.
4. Jokainen kokonaisluku on rationaaliluku.
5. Siis 2 ei ole kokonaisluku.

59. Formalisoitava seuraava päättely ja tutkittava sen pätevyyttä.

1. 2 ei ole transkendenttiluku.
2. Jokainen luku, joka ei ole transkendenttiluku, on algebrallinen luku
3. Jotkin algebralliset luvut ovat rationaalilukuja.
4. Jotkin rationaaliluvut ovat kokonaislukuja.
5. Siis 2 on kokonaisluku.

60. Formalisoitava seuraava päättely (vrt. Miettinen [16], teht. 54) ja tutkittava sen pätevyyttä.

1. Jokainen faaraon tytär on nautiskelija.
2. Kukaan nainen ei ole nautiskelija.
3. Nefernefertite on faaraon tytär.
4. Siis harpyija huutaa merellä.

Luku 2

Induktio ja rekursio

Hölmöläinen haki halkoja metsästä. Hän heitti ensimmäisen halon rekeen sanoen hevoselle: "Ainakin tuon sinä jaksat vetää". Sitten hän heitti toisen halon sanoen: "Jos sinä jaksat tuon, niin jaksat tämänkin". Seuraavaksi hän heitti taas halon sanoen: "Jos sinä jaksat vetää nuo reessä olevat halot, niin jaksat tämänkin". Hän jatkoi samalla tavalla, kunnes reki oli aivan täynnä halkoja. Hölmöläinen oli ihmeissään, kun hevonen ei jaksanutkaan vetää rekeä.

(*Vanhan kansansadun mukaan*)

2.1 Induktioperiaate

1 Johdattelevia esimerkkejä

Tieteen teoriassa *induktiivinen* menetelmä tarkoittaa yleisten johtopäätösten tekemistä yksityistapauksista, jolloin siis edetään "yksityisestä yleiseen". *Deduktiivisessa* menetelmässä taas yksityistapauksia tutkitaan yleisten tulosten perusteella eli edetään "yleisestä yksityiseen". Induktiivinen menetelmä ei ole matematiikassa pätevä, sillä yksityiset esimerkit eivät riitä yleisen väitteen todistamiseksi. Kuitenkin on olemassa matemaattinen todistustekniikka nimeltä *induktioperiaate* eli (*matemaattinen*) *induktio*. Se ei ole varsinaisesti induktiivinen menetelmä, mutta sen perusidea kuulostaa yksityistapausten tutkimiselta, ja niin tätä nimeä on alettu käyttää.

Tarkastelemme aluksi ei-matemaattisia esimerkkejä induktioperiaatteen mukaisesta ajattelusta.

Esimerkki 19. Olkoon meillä ääretön jono ihmisiä. (Siis kuvittelemme, että tuollainen jono on olemassa.) Jonon ensimmäiselle kerrotaan tietty salaisuus. Toisaalta näistä ihmisistä tiedetään, että jokainen kuultuaan jonkin asian kertoo sen heti jonon seuraavalle. Tuntuu järkevältä päätellä, että tämä salaisuus tulee kaikkien jonossa olevien tietoon.

Esimerkki 20. Kuvitelkaamme, että meillä on ääretön jono palikkatorneja, joista jokainen kaatuessaan heti kaataa seuraavan. Jos jonon ensimmäinen torni kaadetaan, niin tuntuu järkevältä päätellä, että koko jono kaatuu.

Esimerkki 21. Tarkastelemme vielä "induktiotikkaita", jotka ulottuvat äärettömän korkealle ja joissa on äärettömän monta askelmaa. Tiedetään, että jos kiipeilijä astuu tietylle askelmalle, niin hän aina heti nousee sitä seuraavalle askelmalle. Jos kiipeilijä astuu ensimmäiselle askelmalle, niin tuntuu järkevältä ajatella, että hän käy kaikki askelmat läpi eli kiipeää äärettömän korkealle.

2 Induktio

Olkoon tehtävänä laskea n ensimmäisen parittoman positiivisen kokonaisluvun summa $1+3+\cdots+(2n-1)$. (Voisimme laskea sen helposti aritmeettisen sarjan summan kaavalla. Emme kuitenkaan toistaiseksi pidä tämän kaavan käyttöä luvallisena, sillä sen tarkka johtaminen vaatii nimenomaan induktiota, ks. kohta 4.) Tutkimme aluksi tilannetta pienillä n:n arvoilla.

$$\begin{aligned}
&1 = 1,\\
&1+3 = 4,\\
&1+3+5 = 9,\\
&1+3+5+7 = 16,\\
&1+3+5+7+9 = 25.
\end{aligned}$$

Ei tarvita paljoakaan mielikuvitusta huomaamaan, että oikealla puolella ovat lukujen 1, 2, 3, 4, 5 neliöt. ”Induktiivisella menetelmällä” meistä alkaa tuntua siltä, että yleisesti

$$1+3+\cdots+(2n-1) = n^2. \tag{1}$$

Tämä on vielä todistettava. Voisimme tutkia väitettä kokeellisesti esimerkiksi tietokoneella, mutta näin emme saisi pätevää todistusta, sillä emme voi käydä läpi kaikkia n:n arvoja. Meidän on siis meneteltävä muulla tavalla.

Tarkoittakoon p_n lausetta $1+3+\cdots+(2n-1) = n^2$. Huomasimme edellä, että $p_1, p_2, \ldots, p_5$ ovat tosia. Voisimme todistaa lauseen p_6 helposti suoraan laskemalla $1+3+5+7+9+11 = 36$, mutta voimme tehdä sen myös *laskematta koko summaa käyttämällä hyväksi lauseen p_5 totuutta.* Nimittäin

$$1+3+5+7+9+11 = (1+3+5+7+9)+11 \overset{p_5}{=} 25+11 = 36.$$

Vastaavasti p_5:n totuus seuraa p_4:n totuudesta jne, joten kaikki viime kädessä palautuu p_1:n totuuteen.

Samoin kuin p_5:n totuudesta seuraa p_6:n totuus, *minkä tahansa p_k:n totuudesta seuraa p_{k+1}:n totuus.* Jos näet p_k sattuisi olemaan tosi, niin silloin olisi $1+3+\cdots+(2k-1) = k^2$ ja edelleen

$$\begin{aligned}
1+3+\cdots+\bigl(2(k+1)-1\bigr) &= 1+3+\cdots+(2k+1)\\
&= \bigl(1+3+\cdots+(2k-1)\bigr)+(2k+1) \overset{p_k}{=} k^2+2k+1 = (k+1)^2.
\end{aligned}$$

Nyt p_1 on tosi, p_1:n totuudesta seuraa p_2:n totuus, p_2:n totuudesta seuraa p_3:n totuus jne. Yleisesti p_k:n totuudesta seuraa p_{k+1}:n totuus. Tästä päättelemme *matemaattisella induktiolla*, että p_n on tosi kaikilla $n \in \mathbb{Z}_+$. Väitös (1) on siis todistettu.

3 Induktioperiaatteen muotoilu. Esimerkkejä

Matemaattisen induktion pätevyys voidaan perustella luonnollisten lukujen eräiden ominaisuuksien avulla. Kun luonnolliset luvut määritellään *Peanon*[1] *aksioomilla* (ks. esim. Ebbinghaus ym. [2], Enderton [3], Jech [8]), niin induktioperiaate oletetaan aksioomaksi. Me tyydymme toteamaan, että se on intuitiivisesti helppo hyväksyä oikeaksi.

Esitämme nyt induktioperiaatteen yleisessä muodossa.

(Ensimmäinen) induktioperiaate. Olkoot p_0, $p_1, \ldots$ (tai p_m, $p_{m+1}, \ldots$, missä $m \in \mathbb{Z}$) lauseita. Olkoon tehtävänä todistaa, että lause p_n on tosi kaikilla $n \in \mathbb{N}$ (tai kaikilla $n \in \{m, m+1, \ldots\}$). Menetellään seuraavasti.

1 (Perusaskel). Osoitetaan, että p_0 on tosi (tai p_m on tosi).

2 (Induktioaskel). Osoitetaan, että p_k:n totuudesta aina seuraa p_{k+1}:n totuus. Toisin sanoen tehdään *induktio-oletus*, että p_n on tosi arvolla $n = k$, ja todistetaan *induktioväite*, että p_n on tällöin tosi arvolla $n = k+1$. (Vaihtoehtoinen induktioaskel on osoittaa, että p_{k-1}:n totuudesta aina seuraa p_k:n totuus.)

3 (Johtopäätös). Tämän jälkeen alkuperäinen väitös seuraa induktioperiaatteesta.

Voimme formalisoida induktioperiaatteen muotoon

$$\frac{\begin{array}{l} p_0 \\ \forall k \in \mathbb{N}\colon (p_k \Rightarrow p_{k+1}) \end{array}}{\forall n \in \mathbb{N}\colon p_n}$$

Esimerkki 22. Todistettava, että $1+2+\cdots+n = \frac{n(n+1)}{2}$ kaikilla $n \in \mathbb{Z}_+$.

Perusaskel. Kun $n = 1$, niin yhtälön vasemmalla puolella olevan summan ainoa termi on 1, joten tämä summa on 1. Oikea puoli on $\frac{1 \cdot 2}{2} = 1$. Siis yhtälö on voimassa, kun $n = 1$.

Induktioaskel. Induktio-oletus (IO) on, että yhtälö on voimassa, kun $n = k$, eli että

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

Induktioväite (IV) on, että tämä yhtälö on voimassa, kun $n = k + 1$, eli että

$$1 + 2 + \cdots + (k+1) = \frac{(k+1)\big((k+1)+1\big)}{2}. \tag{IV}$$

Induktioväitteen todistus. Induktioväitteen vasen puoli on yksinkertaisten laskujen ja induktio-oletuksen perusteella

[1] *Giuseppe Peano (1858–1932), italialainen matemaatikko.*

$$
\begin{aligned}
\mathrm{vp} &= 1+2+\cdots+(k+1) = (1+2+\cdots+k)+(k+1) \\
&\overset{\mathrm{IO}}{=} \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)+2(k+1)}{2} = \frac{(k+1)(k+2)}{2}.
\end{aligned}
$$

Oikea puoli

$$
\mathrm{op} = \frac{(k+1)\big((k+1)+1\big)}{2} = \frac{(k+1)(k+2)}{2}
$$

on sama, joten (IV) on todistettu.

Johtopäätös. Tehtävän yhtälö seuraa induktioperiaatteesta.

Yhtälömuotoinen induktioväite voidaan aina todistaa sieventämällä yhtälön molemmat puolet ja huomaamalla, että saadaan sama tulos. Tämä menetelmä on aloittelijalle helpoin, mutta tyylikkäämpää on muokata toisesta puolesta toinen.

Esimerkki 22, jatkoa. Voimme todistaa induktioväitteen myös seuraavalla muodollisesti hieman erilaisella tavalla.

$$
\begin{aligned}
\mathrm{vp} &= (1+2+\cdots+k)+(k+1) \\
&\overset{\mathrm{IO}}{=} \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)+2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2} = \frac{(k+1)\big((k+1)+1\big)}{2} = \mathrm{op}.
\end{aligned}
$$

Esimerkki 23. Olkoon $x \in \mathbb{R}$, $x > -1$. Todistettava *Bernoullin*[2] *epäyhtälö* $(1+x)^n \geq 1+nx$ kaikilla $n \in \mathbb{N}$.

Perusaskel. Kun $n = 0$, niin $\mathrm{vp} = (1+x)^0 = 1$ ja $\mathrm{op} = 1 + 0x = 1$, joten epäyhtälö on tällöin voimassa.

Induktioaskel. Induktio-oletus on

$$
\text{(IO)} \qquad (1+x)^k \geq 1+kx
$$

ja induktioväite on

$$
\text{(IV)} \qquad (1+x)^{k+1} \geq 1+(k+1)x.
$$

Induktioväitteen todistus. Koska $x > -1$, niin $1+x > 0$, joten

$$
\begin{aligned}
\mathrm{vp} &= (1+x)^{k+1} = (1+x)(1+x)^k \\
&\overset{\mathrm{IO}}{\geq} (1+x)(1+kx) = 1+(k+1)x+kx^2 \geq 1+(k+1)x = \mathrm{op}.
\end{aligned}
$$

Esimerkki 24. Todistettava: Aina kun $n \in \mathbb{N}$, niin n^2+n on parillinen.

Olisi helpointa kirjoittaa $n^2+n = n(n+1)$ ja todeta, että oikean puolen tekijöistä toinen on pariton ja toinen parillinen, joten niiden tulo on

[2] *Bernoullit, sveitsiläinen matemaatikkosuku 1600–1800-luvuilla. Bernoullin epäyhtälön on keksinyt Jakob Bernoulli (1654–1705).*

parillinen. Tarkkaan ottaen tämäkin yksinkertainen asia vaatisi induktiotodistuksen, sillä sen osoittamisessa, että kaikki kokonaisluvut ovat joko muotoa $2p$ tai $2p + 1$, on käytettävä induktiota.

Käsittelemme tehtävämme induktiolla. Merkitsemme $f(n) = n^2 + n$. Nyt $f(0) = 0$ on parillinen. Teemme induktio-oletuksen, että $f(k)$ on parillinen. Toisin sanoen on olemassa sellainen $p \in \mathbb{N}$, että $f(k) = 2p$. Tällöin

$$\begin{aligned} f(k+1) &= (k+1)^2 + (k+1) = k^2 + 2k + 1 + k + 1 \\ &= k^2 + k + 2(k+1) \overset{\text{IO}}{=} 2p + 2(k+1) = 2(p+k+1), \end{aligned}$$

joten $f(k+1)$ on parillinen. Siis induktioväite ja samalla tehtävämme väite on todistettu.

Esimerkki 25. Todistettava: Aina kun $n \in \mathbb{N}$, niin $n^3 - n$ on jaollinen 3:lla.

Olisi helpointa kirjoittaa $n^3 - n = n(n-1)(n+1)$ ja todeta, että oikean puolen tekijöistä yksi on jaollinen 3:lla, joten tulo on jaollinen 3:lla, mutta tarkkaan ottaen sekin vaatisi induktiotodistuksen, vrt. esim. 24.

Merkitsemme $f(n) = n^3 - n$. Nyt $f(0) = 0$ on jaollinen 3:lla. Teemme induktio-oletuksen: $f(k)$ on jaollinen 3:lla. Toisin sanoen on olemassa sellainen $p \in \mathbb{N}$, että $f(k) = 3p$. Tällöin

$$\begin{aligned} f(k+1) &= (k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1 \\ &= k^3 - k + 3(k^2 + k) \overset{\text{IO}}{=} 3p + 3(k^2 + k) = 3(p + k^2 + k), \end{aligned}$$

joten $f(k+1)$ on jaollinen 3:lla. Siis induktioväite on todistettu, ja tehtävämme on loppuun suoritettu.

4 Lukujonot ja sarjat

Kuvaus eli *funktio* jouko*lta* X joukk*oon* Y ($X, Y \neq \emptyset$, huomaa sijat) tarkoittaa havainnollisesti ”vastaavuutta”, joka liittää joukon X jokaiseen alkioon joukon Y tietyn alkion. Merkitsemme $f\colon X \to Y$ tarkoittamaan sitä, että f on tällainen kuvaus. Määrittelemme kuvauksen myöhemmin täsmällisesti (luku 5.1). *Lukujono* on kuvaus $f\colon \mathbb{Z}_+ \to \mathbb{R}$ (tai $\mathbb{N} \to \mathbb{R}$). Merkitsemme usein $f(n) = a_n$ ja puhumme lukujonosta $(a_1, a_2, \ldots)$ tai lukujonosta (a_n).

Tarkastelemme aluksi *aritmeettista jonoa* $(a_1, a_2, \ldots)$, missä kahden peräkkäisen *termin* erotus on vakio d. Siis $a_{n+1} - a_n = d$ kaikilla $n \in \mathbb{Z}_+$. Merkitsemällä $a_1 = a$ saamme tämän jonon yleiseksi termiksi

$$a_n = a + (n-1)d.$$

Todistamme tämän induktiolla. Arvolla $n = 1$ saamme toden yhtälön $a = a$. Voisimme esittää induktio-oletuksen muodossa ’väitös on tosi arvolla $n = k$’, kuten olemme aiemmin tehneet. Tottunut induktiotodistaja ei kuitenkaan viitsi ottaa käyttöön uutta kirjainta k, vaan hän esittää induktio-oletuksen muodossa 'väitös on tosi n:lle', jolloin induktioväite on 'väitös on tosi $(n+1)$:lle'. Teemme näin. Induktio-oletuksen perusteella $a_n = a + (n-1)d$, joten

$$a_{n+1} = a_n + d = a + (n-1)d + d = a + nd = a + \big((n+1) - 1\big)d.$$

Vastaavan *aritmeettisen sarjan osasumma* on

$$a_1 + a_2 + \cdots + a_n = n\frac{a_1 + a_n}{2}.$$

Todistamme tämän. Kun $n = 1$, saamme toden yhtälön $a_1 = a_1$. Teemme induktio-oletuksen: väitös on tosi n:lle. Käyttämällä tätä ja yleisen termin lauseketta saamme

$$\begin{aligned}
a_1 + a_2 + \cdots + a_{n+1} &= (a_1 + a_2 + \cdots + a_n) + a_{n+1} \\
&= n\frac{a_1 + a_n}{2} + a_{n+1} = n\frac{a + a + (n-1)d}{2} + a + nd \\
&= (n+1)a + \frac{n(n+1)}{2}d = (n+1)\Big(a + \frac{n}{2}d\Big) \\
&= (n+1)\frac{2a + nd}{2} = (n+1)\frac{a + (a + nd)}{2} = (n+1)\frac{a_1 + a_{n+1}}{2}.
\end{aligned}$$

Tutkimme seuraavaksi *geometrista jonoa* $(a_1, a_2, \ldots)$, missä $a_1 = a$ ja kahden peräkkäisen termin suhde on vakio q. Siis $a_{n+1}/a_n = q$ kaikilla $n \in \mathbb{Z}_+$. (Jos $a = 0$, niin sovimme, että kysymyksessä on jono $(0, 0, \ldots)$, ja jos $q = 0$, niin sovimme, että kysymyksessä on jono $(a, 0, 0, \ldots)$.) Tämän jonon yleinen termi on (teht. 72a)

$$a_n = aq^{n-1},$$

ja vastaavan *geometrisen sarjan* osasumma on ehdolla $q \neq 1$ (teht. 72b)

$$a_1 + a_2 + \cdots + a_n = a + aq + aq^2 + \cdots + aq^{n-1} = a\frac{1 - q^n}{1 - q}.$$

Jos ja vain jos $|q| < 1$, niin tällä summalla on (äärellinen) raja-arvo, kun $n \to \infty$. Tällöin sanomme, että geometrinen sarja $a + aq + aq^2 + \cdots$ *suppenee* ja että sen summa

$$a + aq + aq^2 + \cdots = \frac{a}{1 - q}.$$

Muussa tapauksessa tämä sarja *hajaantuu*.

Tarkastelemme lopuksi *harmonista jonoa* $\big(1, \frac{1}{2}, \frac{1}{3}, \ldots\big)$. Vastaavan *harmonisen sarjan* osasummalle

$$h_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

ei ole yksinkertaista lauseketta, mutta sille voidaan (teht. 73) todistaa epäyhtälö

$$h_{2^n} \geq 1 + \frac{n}{2}.$$

Kun $n \to \infty$, niin tämän epäyhtälön oikea puoli lähestyy ääretöntä. Tällöin myös vasen puoli lähestyy ääretöntä, joten harmoninen sarja $1 + \frac{1}{2} + \frac{1}{3} + \cdots$ hajaantuu. Hajaantuminen on kuitenkin erittäin hidasta.

Kuvitelkaamme, että meidän on tietokoneella tai ohjelmoitavalla laskimella tutkittava, suppeneeko vai hajaantuuko harmoninen sarja, ja että tässä tehtävässä käytetään liukulukuaritmetiikkaa (siis murtoluvut korvataan niiden desimaali- tai muilla vastaavilla likiarvoilla). Tällöin kone pitää lukuja $\frac{1}{n}$ nollina, kun n on tarpeeksi suuri, ja väittää, että tämä sarja suppenee. Kone väittää myös, että yllä oleva epäyhtälö on suurilla n:n arvoilla epätosi. Tietokoneen ja laskimen käyttö ilman riittävää kriittisyyttä ja matematiikan taitoa saattaa siis johtaa aivan vääriin tuloksiin.

Myös muiden sarjojen tutkimisessa induktioperiaate on kätevä erityisesti haluttaessa todistaa, että osasummalla on tietty yksinkertainen lauseke (teht. 62, 63, 74, 75). Tällaisen lausekkeen löytämisessä ei induktioperiaatteesta kuitenkaan ole apua, vaan lauseke on keksittävä kokeellisesti tai löydettävä jollakin muulla tavalla.

Harjoitustehtäviä

61. Todistettava (induktiolla, siis käyttämättä geometrisen sarjan summan kaavaa): $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ kaikilla $n \in \mathbb{N}$.

62. Todistettava: $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$ kaikilla $n \in \mathbb{Z}_+$.

63. Todistettava: $1^3 + 2^3 + \cdots + n^3 = \left(\frac{1}{2}n(n+1)\right)^2$ kaikilla $n \in \mathbb{Z}_+$.

64. Todistettava induktiolla, että luvut 1, 2, …, n voidaan järjestää jonoon $n!$ eri tavalla.

65. Todistettava: Jos $n \in \mathbb{Z}_+$ ja $n > 4$, niin $2^n > n^2$.

66. Todistettava: Jos $n \in \mathbb{Z}_+$ ja $n \geq 4$, niin $2^n < n!$.

67. Todistettava: Jos $n \in \mathbb{N}$, niin $n^3 + 2n$ on jaollinen 3:lla.

68. Todistettava: Jos $n \in \mathbb{N}$ on pariton, niin $n^2 - 1$ on jaollinen 8:lla.

69. Todistettava: Jos $n \in \mathbb{N}$, niin $n^3 - n$ on jaollinen 6:lla.

70. a) Miksi Bernoullin epäyhtälön (esim. 23) todistuksessa tarvitaan sitä, että $1+x > 0$? **b)** Kun $n \in \mathbb{Z}_+$, niin itse asiassa riittää, että $1+x \geq 0$ eli $x \geq -1$. Miksi? **c)** Jos $x = -1$, niin tapaus $n = 0$ on kuitenkin ongelmallinen. Miksi?

71. Todistettava induktiolla, että jokainen kokonaisluku on muotoa $2p$ tai $2p + 1$, missä p on kokonaisluku.

72. Todistettava (induktiolla) **a)** geometrisen jonon yleisen termin, **b)** geometrisen sarjan osasumman kaava. Käsiteltävä myös tapaus $q = 1$.

73. Todistettava harmonisen sarjan osasummalle epäyhtälö $h_{2^n} \geq 1 + \frac{n}{2}$.

74. Todistettava: $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1$ kaikilla $n \in \mathbb{Z}_+$.

75. Todistettava: $1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = \frac{1}{3}n(n+1)(n+2)$ kaikilla $n \in \mathbb{Z}_+$.

76. Koulussa aritmeettisen sarjan osasumman $s_n = a_1 + a_2 + \cdots + a_n$ ($a_2 - a_1 = a_3 - a_2 = \cdots = a_n - a_{n-1} = d$) kaava johdetaan tavallisesti kirjoittamalla

$$\begin{aligned} s_n &= a_1 + a_2 + \quad \cdots \quad + a_n \\ s_n &= a_n + a_{n-1} + \cdots + a_1 \end{aligned}$$

ja laskemalla nämä yhtälöt yhteen. Mikä on allekkain olevien termien summa? Miten jatketaan? Vaatiiko tämäkin todistus oikeastaan eräänlaisen induktiopäättelyn?

77. Koulussa geometrisen sarjan osasumman $s_n = a + aq + aq^2 + \cdots + aq^{n-1}$ ($q \neq 1$) kaava johdetaan tavallisesti kirjoittamalla

$$\begin{aligned} s_n &= a + aq + aq^2 + \cdots + aq^{n-1} \\ qs_n &= \qquad aq + aq^2 + \cdots + aq^{n-1} + aq^n. \end{aligned}$$

Miten jatketaan? Vaatiiko tämäkin todistus oikeastaan eräänlaisen induktiopäättelyn?

78. Mikä virhe on seuraavassa ”todistuksessa”? Osoitetaan induktiolla, että kaikki luonnolliset luvut ovat keskenään yhtäsuuria eli $0 = 1 = \cdots = n$ kaikilla $n \in \mathbb{N}$. Arvolla $n = 0$ tämä on selvästi voimassa. Tehdään induktio-oletus, että väitös on tosi arvolla $n = k$. Siis $0 = 1 = \cdots = k$. Tällöin myös $k + 1 = 0 + 0 = 0$, joten induktioväite $0 = 1 = \cdots = k + 1$ on todistettu.

79. Seuraavassa ”todistetaan”, että

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

kaikilla $n \in \mathbb{Z}_+$. Arvolla $n = 1$ väitös on tosi, sillä

$$\frac{1}{1 \cdot 2} = \frac{3}{2} - \frac{1}{1}.$$

Tehdään induktio-oletus, että väitös on tosi arvolla $n = k$. Tällöin

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

Siis induktioväite on todistettu. **a)** Miksi väitös on väärä? **b)** Mikä virhe on todistuksessa? **c)** Korjattava väitös ja todistettava se.

80. Vanha vitsi ”todistaa”, että kaikki naiset ovat vaaleatukkaisia, on seuraava. Esitetään tämä väitös muodossa ’Jos n naisen joukossa on ainakin yksi vaalea, niin tämän joukon kaikki naiset ovat vaaleita’ ja todistetaan se induktiolla. Väitös on selvästi tosi arvolla $n = 1$. Tehdään induktio-oletus, jonka mukaan väitös on tosi arvolla $n = k$. Olkoon $A = \{a_1, a_2, \ldots, a_{k+1}\}$ $k + 1$ naisen joukko, joka sisältää ainakin yhden vaalean. Tarvittaessa numerointia muuttamalla voidaan sopia, että a_1 on vaalea. Joukko $\{a_1, a_2, \ldots, a_k\}$ on k naisen joukko, joka sisältää ainakin yhden vaalean, joten induktio-oletuksen mukaan kaikki tämän joukon naiset ovat vaaleita. Mutta tällöin myös joukko $\{a_2, a_3, \ldots, a_{k+1}\}$ on k naisen joukko, joka sisältää ainakin yhden vaalean (itse asiassa $k-1$ vaaleaa, nimittäin a_2, a_3, $\ldots$, a_k), joten induktio-oletuksen mukaan tämänkin joukon kaikki naiset ovat vaaleita. Näin joukon A kaikki naiset on osoitettu vaaleiksi, joten induktioväite on todistettu ja todistuksemme on suoritettu loppuun. Missä vika?

∗2.2 Toinen induktioperiaate. Rekursio

1 Toinen induktioperiaate

Voidaan todistaa, että induktioaskeleen ’jos väitös on tosi arvolla $n = k$, niin se on tosi arvolla $n = k + 1$’ kanssa yhtäpitävä askel on ’jos väitös on tosi kaikilla arvoilla $n \le k$, niin se on tosi arvolla $n = k + 1$’. (Siis näistä askeleista toinen voidaan ottaa, jos ja vain jos toinenkin.) Intuitiivisesti tämä on selvä. Jos vaikkapa esimerkissä 19 jonon ihmisistä tiedetäänkin, että jokainen kuultuaan jonkin asian kertoo sen seuraavalle *yhdessä kaikkien jonossa edellä olevien kanssa*, niin tietenkin tulos on sama kuin tässä esimerkissä. Näin saamme *toisen induktioperiaatteen.*

Toinen induktioperiaate. Olkoot p_0, $p_1, \ldots$ (tai p_m, $p_{m+1}, \ldots$, missä $m \in \mathbb{Z}$) lauseita. Olkoon tehtävänä todistaa, että lause p_n on tosi kaikilla $n \in \mathbb{N}$ (tai kaikilla $n \in \{m, m+1, \ldots\}$). Menetellään seuraavasti.

1 (Perusaskel). Osoitetaan, että p_0 on tosi (tai p_m on tosi).

2 (Induktioaskel). Osoitetaan, että p_n:n totuudesta kaikilla $n \le k$ aina seuraa p_{k+1}:n totuus. Toisin sanoen tehdään *induktio-oletus*, että p_n on tosi arvoilla $n \le k$, ja todistetaan *induktioväite*, että p_n on tällöin tosi arvolla $n = k + 1$. (Vaihtoehtoinen induktioaskel on osoittaa, että p_n:n totuudesta kaikilla $n < k$ aina seuraa p_k:n totuus.)

3 (Johtopäätös). Tämän jälkeen alkuperäinen väitös seuraa induktioperiaatteesta.

Voimme formalisoida toisen induktioperiaatteen muotoon

$$\frac{\begin{array}{l} p_0 \\ \forall k \in \mathbb{N}\colon \big((\forall n \leq k\colon p_n) \Rightarrow p_{k+1}\big) \end{array}}{\forall n \in \mathbb{N}\colon p_n}$$

Toinen induktioperiaate on näennäisesti heikompi kuin ensimmäinen, sillä induktioaskeleessa oletetaan enemmän. Olemme kuitenkin jo todenneet, että nämä periaatteet ovat (joukossa $\mathbb{N}$) yhtäpitävät. Joudumme myöhemmin (s. 101) tilanteisiin, joissa näillä periaatteilla on eroa. Ensimmäinen induktioperiaate on (joukossa $\mathbb{N}$) usein mukavampi käyttää, mutta seuraavassa esimerkissä näin ei ole.

Esimerkki 26. Todistettava, että jokainen lukua 1 suurempi positiivinen kokonaisluku voidaan esittää alkulukujen tulona.

Tarkoittakoon p_n lausetta 'luku n voidaan esittää alkulukujen tulona'. Käytämme toista induktioperiaatetta.

Perusaskel. Lause p_2 on tosi, sillä 2 voidaan esittää tulona, jonka ainoa tekijä on tämä luku itse.

Induktioaskel. Teemme induktio-oletuksen: p_n on tosi aina, kun $2 \leq n < k$. Induktioväite on, että p_k on tosi eli että k voidaan esittää alkulukujen tulona. Jos k on alkuluku, niin asia on selvä. Jos taas k ei ole alkuluku, niin $k = ab$, missä $2 \leq a, b < k$. Induktio-oletuksen perusteella a ja b voidaan esittää alkulukujen tulona, joten tämä ominaisuus on myös tulolla ab.

2 Yleinen liitännäisyyslause

Olkoon $*$ epätyhjässä joukossa X määritelty *laskutoimitus* eli kuvaus $X \times X \to X$. Kun $x, y \in X$, käytämme "funktion arvolle" $*(x, y)$ merkintää $x * y$, joka siis on "tulos", kun alkioihin x ja y sovelletaan laskutoimitus $*$. Jos $*$ noudattaa liitäntälakia $x * (y * z) = (x * y) * z$, niin käytämme tälle lausekkeelle merkintää $x * y * z$, ja toteamme, että vastaavasti "sulut voidaan poistaa" silloinkin, kun alkioita on enemmän kuin kolme. Tarkkaan ottaen tämä *yleinen liitännäisyyslause* kuitenkin vaatii induktiotodistuksen. Sama huomautus koskee *yleistä vaihdannaisuuslausetta* (teht. 83).

Lause 3 (Yleinen liitännäisyyslause). Olkoon $*$ joukossa X ($\neq \emptyset$) määritelty liitännäinen laskutoimitus. Kun $x_1, x_2, \ldots, x_n \in X$, niin määritellään lauseke $x_1 * x_2 * \cdots * x_n$ tarkoittamaan sitä, että laskutoimitukset suoritetaan vasemmalta oikealle. Jos tähän lausekkeeseen lisätään sulkuja millä tahansa (mielekkäällä) tavalla, niin lausekkeen arvo ei muutu.

Todistus. Käytämme toista induktioperiaatetta. Arvolla $n = 3$ asia on selvä. Teemme induktio-oletuksen, että väitös on tosi aina, kun $3 \leq n < k$. Induktioväite on, että väitös on tosi kun $n = k$ eli että lausekkeen

$x_1 * x_2 * \cdots * x_k$ arvo ei muutu lisättäessä siihen sulkuja. Jos siis

$$\begin{aligned} x &= \big(\dots(x_1 * \dots(\dots(\dots)\dots) * x_i)\dots\big) \\ &\qquad * \big(\dots(x_{i+1} * \dots(\dots(\dots)\dots) * x_k)\dots\big), \\ y &= \big(\dots(x_1 * \dots(\dots(\dots)\dots) * x_j)\dots\big) \\ &\qquad * \big(\dots(x_{j+1} * \dots(\dots(\dots)\dots) * x_k)\dots\big), \end{aligned}$$

missä $1 \le i, j < k$, niin meidän on osoitettava, että $x = y$. Induktio-oletuksen perusteella voimme poistaa kaikki sisäsulut, joten

$$\begin{aligned} x &= (x_1 * x_2 * \cdots * x_i) * (x_{i+1} * x_{i+2} * \cdots * x_k), \\ y &= (x_1 * x_2 * \cdots * x_j) * (x_{j+1} * x_{j+2} * \cdots * x_k). \end{aligned}$$

Jos $i = j$, niin asia on selvä. Jos taas $i \ne j$, niin voimme yleisyyttä rajoittamatta sopia, että $i < j$. Merkitsemme $a = x_1 * x_2 * \cdots * x_i$, $b = x_{i+1} * x_{i+2} * \cdots * x_j$, $c = x_j * x_{j+1} * \cdots * x_k$. Induktio-oletuksen perusteella saamme lisäämällä sisäsulkuja sopivasti

$$x = a * (b * c), \qquad y = (a * b) * c,$$

joten liitäntälain mukaan $x = y$.

3 Rekursio

Induktioaskeleessa tiettyä n:n arvoa koskeva *väite* palautetaan arvoa $n-1$ koskevaan väitteeseen (ensimmäinen induktioperiaate) tai kaikkia n:ää pienempiä arvoja koskevaan väitteeseen (toinen induktioperiaate). Voimme myös palauttaa tiettyä n:n arvoa koskevan *määritelmän* pienempiä n:n arvoja koskeviin määritelmiin. Näin saamme menetelmän, jolla tiettyjä käsitteitä voidaan määritellä *rekursiivisesti.*

Kuvaus $f\colon \mathbb{N} \to \mathbb{R}$ esitetään tavallisesti ilmoittamalla, miten $f(n)$ riippuu n:stä. Joskus se kuitenkin kannattaa määritellä rekursiivisesti seuraavalla tavalla.

1 (Alkuarvot). Ilmoitetaan $f(0)$, $f(1)$, …, $f(k)$.

2 (Rekursiokaava). Kun $n \ge k$, niin esitetään, miten $f(n+1)$ riippuu luvuista $f(n)$, $f(n-1)$, …, $f(n-k)$.

Merkinnän $f(n)$ sijasta käytetään usein merkintää f_n tai y_n. Myös nimityksiä *rekursiivinen jono*, *rekursioyhtälö* ja *differenssiyhtälö* käytetään.

Esimerkki 27. Tarkastelemme rekursiivista lukujonoa

$$\begin{aligned} f_0 &= 1, \\ f_{n+1} &= 2f_n + 3 \end{aligned}$$

eli rekursioyhtälöä $f_{n+1} = 2f_n + 3$ *alkuehdolla* $f_0 = 1$. Tällöin $f_1 = 2 \cdot 1 + 3 = 5$, $f_2 = 2 \cdot 5 + 3 = 13$, $f_3 = 2 \cdot 13 + 3 = 29$ jne. Nyt herää kysymys, voidaanko tämä rekursioyhtälö *ratkaista* eli voidaanko f_n esittää pelkän n:n funktiona. Palaamme tähän tehtävässä 84.

Esimerkki 28. *Fibonaccin*[3] *luvut* määritellään yhtälöillä

$$f_0 = 0, \quad f_1 = 1,$$
$$f_n = f_{n-1} + f_{n-2}.$$

Siis jokainen Fibonaccin luku on kahden edellisen Fibonaccin luvun summa. Ensimmäiset tällaiset luvut ovat 0, 1, 1, 2, 3, 5, 8, 13, 21. Fibonaccin luvuille on yleinen lauseke (s. 153, teht. 370).

Esimerkki 29. Kertoman tavallinen määritelmä on $n! = 1 \cdot 2 \cdot \cdots \cdot n$ $(0! = 1)$. Voimme määritellä kertoman myös rekursiivisesti

$$0! = 1,$$
$$n! = n(n-1)!.$$

Nämä määritelmät ovat yhtäpitävät (teht. 88).

Esimerkki 30. Potenssin tavallinen määritelmä on $a^n = aa \cdots a$ (n kertaa). Voimme määritellä potenssin myös rekursiivisesti

$$a^1 = a,$$
$$a^n = aa^{n-1}.$$

Nämä määritelmät ovat yhtäpitävät (teht. 89).

Myös algoritmit ja ohjelmat voivat olla rekursiivisia, ks. esim. Rosen [21]. (Tosin useimmat rekursiivisesti määritellyt käsitteet voidaan tulkita funktioiksi.)

4 Rekursio lauselogiikassa

Voimme määritellä lauselogiikan kielen täsmällisesti käyttämällä rekursiota. (Määrittelimme tämän kielen hieman epätäsmällisesti luvussa 1.) Kutsumme lauselogiikan kielen ilmaisuja *propositiolauseiksi* (tai *hyvinmuodostetuiksi kaavoiksi*). Määritelmä on seuraava.

1. Lausemuuttujat $p, q, r, s, \ldots, p_0, p_1, p_2, \ldots$ ovat propositiolauseita.
2. Jos A on propositiolause, niin $\neg A$ on propositiolause.
3. Jos A ja B ovat propositiolauseita, niin $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$ ja $(A \Leftrightarrow B)$ ovat propositiolauseita.
4. Kaikki propositiolauseet saadaan yllä mainituilla tavoilla.

Rekursiivisesti määriteltyjä käsitteitä koskevien lauseiden todistamisessa voidaan soveltaa induktioperiaatteen kaltaista todistustekniikkaa. Tarkastelemme sitä lauselogiikassa.

[3] *Leonardo Fibonacci da Pisa (n. 1175–1250), italialainen matemaatikko.*

Induktio lauseen pituuden suhteen. Olkoon $\mathcal{O}$ tietty propositiolauseita koskeva ominaisuus. Olkoon tehtävänä todistaa, että tämä ominaisuus on kaikilla propositiolauseilla. Menetellään seuraavasti.

1 (Perusaskel). Osoitetaan, että kaikilla lausemuuttujilla on ominaisuus $\mathcal{O}$.

2 (Induktioaskel). Tehdään *induktio-oletus*, että propositiolauseilla A ja B on ominaisuus $\mathcal{O}$. Todistetaan *induktioväite*, että lauseilla $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \Rightarrow B)$ ja $(A \Leftrightarrow B)$ on ominaisuus $\mathcal{O}$.

3 (Johtopäätös). Tämän jälkeen alkuperäinen väitös seuraa induktioperiaatteesta.

Jos valitsemme konnektiivit $\neg$ ja $\wedge$ peruskonnektiiveiksi, joihin muut konnektiivit palautetaan (luku 1.1.5), niin propositiolauseiden määritelmän kohdassa 3 riittää mainita vain lause $(A \wedge B)$ ja induktiotodistuksissa riittää tarkastella muotoa $\neg A$ ja $(A \wedge B)$ olevia lauseita.

Esimerkki 31. Olkoot peruskonnektiivit $\neg$ ja $\wedge$. Määrittelemme vasemmanpuolisten ja oikeanpuolisten sulkujen lukumäärät vs ja os rekursiivisesti.

$$\begin{aligned} &\mathrm{vs}\, p_i = 0, && \mathrm{os}\, p_i = 0, \\ &\mathrm{vs}\, \neg A = \mathrm{vs}\, A, && \mathrm{os}\, \neg A = \mathrm{os}\, A, \\ &\mathrm{vs}(A \wedge B) = \mathrm{vs}\, A + \mathrm{vs}\, B + 1, \qquad && \mathrm{os}(A \wedge B) = \mathrm{os}\, A + \mathrm{os}\, B + 1. \end{aligned}$$

Todistamme, että jokaiselle propositiolauseelle A on $\mathrm{vs}\, A = \mathrm{os}\, A$.

Perusaskel. Kun A on lausemuuttuja, niin $\mathrm{vs}\, A = 0 = \mathrm{os}\, A$.

Induktioaskel. Teemme induktio-oletuksen, että $\mathrm{vs}\, A = \mathrm{os}\, A$ ja $\mathrm{vs}\, B = \mathrm{os}\, B$. Tällöin

$$\mathrm{vs}\, \neg A = \mathrm{vs}\, A \stackrel{\mathrm{IO}}{=} \mathrm{os}\, A = \mathrm{os}\, \neg A$$

ja

$$\mathrm{vs}(A \wedge B) = \mathrm{vs}\, A + \mathrm{vs}\, B + 1 \stackrel{\mathrm{IO}}{=} \mathrm{os}\, A + \mathrm{os}\, B + 1 = \mathrm{os}(A \wedge B).$$

Induktioväite on näin todistettu.

Johtopäätös. Induktioperiaatteen perusteella alkuperäinen väitös on voimassa kaikille lauseille.

5 Rakennepuu ja totuusjakauma

Tarkastelemme lopuksi lauselogiikan parin käsitteen rekursiivista määrittelyä.

Propositiolauseen A *rakennepuu* $\mathcal{T}A$ määritellään seuraavasti. Kun $A = p_i$, niin

$$\mathcal{T}A = p_i$$

Kun $A = \neg B$, niin

$$\mathcal{T}A = \begin{tikzcd} \neg B \arrow[d] \\ \mathcal{T}B \end{tikzcd}$$

Kun $A = (B \circ C)$, missä $\circ \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$, niin

$$\mathcal{T}A = \begin{tikzcd} & (B \circ C) \arrow[dl] \arrow[dr] & \\ \mathcal{T}B & & \mathcal{T}C \end{tikzcd}$$

Rakennepuun *korkeus* $\operatorname{hg} A$ määritellään niin, että $\operatorname{hg} p_i = 0$, $\operatorname{hg} \neg B = \operatorname{hg} B + 1$, $\operatorname{hg}(B \circ C) = \max\{\operatorname{hg} B, \operatorname{hg} C\} + 1$, missä $\circ \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$.

Esimerkki 32. Proposiotiolauseen $\neg p \wedge (q \Rightarrow \neg r)$ rakennepuu on

$$\begin{tikzcd} & \neg p \wedge (q \Rightarrow \neg r) \arrow[dl] \arrow[dr] & & \\ \neg p \arrow[d] & & q \Rightarrow \neg r \arrow[dl] \arrow[dr] & \\ p & q & & \neg r \arrow[d] \\ & & & r \end{tikzcd}$$

Sen korkeus on 3.

Olemme aiemmin tutkineet lauseiden totuusarvoja totuustaulukoilla. Teoreettisissa tarkasteluissa totuustaulukkoa hyödyllisempi on *totuusjakauma* eli *valuaatio*, joka on kuvaus $V\colon \{p_0, p_1, p_2, \ldots\} \to \{0, 1\}$. Propositiolauseen A *totuusarvo* $v(A) \in \{0, 1\}$ *totuusjakaumalla* V määritellään seuraavasti:

$$\begin{aligned} v(p_i) &= V(p_i), \\ v(\neg A) &= 1, \quad \text{joss} \quad v(A) = 0, \\ v(A \vee B) &= 0, \quad \text{joss} \quad v(A) = v(B) = 0, \\ v(A \wedge B) &= 1, \quad \text{joss} \quad v(A) = v(B) = 1, \\ v(A \Rightarrow B) &= 0, \quad \text{joss} \quad v(A) = 1 \text{ ja } v(B) = 0, \\ v(A \Leftrightarrow B) &= 1, \quad \text{joss} \quad v(A) = v(B). \end{aligned}$$

Kuvaukselle V ja sen laajennukselle v käytetään usein samaa merkintää ja kumpaakin kutsutaan valuaatioksi. Tämä hieman epätäsmällinen menettely on sikäli oikeutettu, että v määräytyy yksikäsitteisesti V:stä.

Esimerkki 33. Olkoon $V(p_0) = V(p_1) = 1$, $V(p_2) = V(p_3) = \cdots = 0$. Määritettävä $v\big((p_0 \vee p_2) \Rightarrow (p_1 \wedge p_2)\big)$. Vrt. esim. 1, totuustaulukon 7. rivi (s. 11).

Olkoon A tutkittava lause, jolloin A on $(B \Rightarrow C)$, missä B on $(p_0 \vee p_2)$ ja C on $(p_1 \wedge p_2)$. Koska $v(p_0) = V(p_0) = 1$, niin $v(B) = 1$. Koska $v(p_2) = V(p_2) = 0$, niin $v(C) = 0$. Koska $v(B) = 1$ ja $v(C) = 0$, niin $v(A) = 0$.

Harjoitustehtäviä

81. Kirjoitettava ja todistettava ensimmäinen de Morganin sääntö (s. 15) mielivaltaiselle (äärelliselle) määrälle lauseita.

82. Todistettava: Nollasta eroavien reaalilukujen tulo on positiivinen, jos ja vain jos negatiivisia tulontekijöitä on parillinen määrä.

83. Todistettava *yleinen vaihdannaisuuslause*: Olkoon $*$ joukossa X ($\neq \emptyset$) määritelty vaihdannainen ja liitännäinen laskutoimitus. Olkoon $x_1, x_2, \ldots, x_n \in X$ ja olkoot x_{i_1}, x_{i_2}, …, x_{i_n} nämä alkiot kirjoitettuna johonkin toiseen järjestykseen. Tällöin $x_1 * x_2 * \cdots * x_n = x_{i_1} * x_{i_2} * \cdots * x_{i_n}$.

84. Osoitettava, että rekursioyhtälön $f_{n+1} = 2f_n + 3$ ratkaisu alkuehdolla $f_0 = 1$ on $f_n = 4 \cdot 2^n - 3$.

85. Osoitettava, että yleisesti rekursioyhtälön $f_{n+1} = af_n + b$ ratkaisu, missä f_0 on annettu, on

$$f_n = a^n f_0 + \frac{1 - a^n}{1 - a} b,$$

kun $a \neq 1$, ja $f_n = f_0 + nb$, kun $a = 1$.

86. Ratkaistava rekursioyhtälö $f_{n+1} = -5f_n + 2$ alkuehdolla $f_0 = -1$ **a)** peräkkäisillä sijoituksilla, **b)** tehtävän 85 kaavan avulla.

87. Kuten tehtävä 86, mutta tarkastellaan rekursioyhtälöä $f_{n+1} = f_n - 2$ alkuehdolla $f_0 = 3$.

88. Todistettava, että kertoman rekursiivinen määritelmä (esim. 29) ja tavanomainen määritelmä ovat yhtäpitävät.

89. Todistettava, että potenssin rekursiivinen määritelmä (esim. 30) ja tavanomainen määritelmä ovat yhtäpitävät.

90. Onko **a)** $(\neg p)$, **b)** $\neg\neg\neg\neg\neg\neg q_3$, **c)** $p \Rightarrow \neg q$, **d)** $(p_0 \wedge p_1 \wedge p_2)$, **e)** $(p \wedge\wedge q)$, **f)** $(p \vee [q \vee r])$ sivulla 42 esitetyn määritelmän mukainen propositiolause?

91. **a)** Määriteltävä rekursiivisesti propositiolauseessa A esiintyvien konnektiivien lukumäärä $k(A)$. **b)** Todistettava, että $\operatorname{hg} A \leq k(A)$. **c)** Annettava esimerkki tapauksesta, jossa yhtäsuuruus ei ole voimassa.

92. Todistettava, että lauseessa, jossa ei esiinny negaatiota, on yhtä monta sulkuparia kuin konnektiivia.

93. Muodostettava propositiolauseen **a)** $\neg\big((p \Rightarrow q) \vee \neg r\big)$, **b)** $(A \wedge A)$, missä $A = (p \wedge B)$ ja $B = (q \wedge r)$ rakennepuu.

94. Todistettava, että propositiolauseen rakennepuu on yksikäsitteinen.

95. *Sumeassa logiikassa* lauseen totuusarvo voi olla mikä tahansa välin $[0, 1]$ reaaliluku. Olkoot peruskonnektiivit $\neg$, $\wedge$ ja $\vee$. *Sumea valuaatio* $[\circ]$ on sellainen kuvaus propositiolauseiden joukolta välille $[0, 1]$, joka toteuttaa ehdot

$$\begin{aligned}
&0 \leq [p] \leq 1, \text{ kun } p \text{ on lausemuuttuja,}\\
&[\neg A] = 1 - [A],\\
&[A \vee B] = \max([A], [B]),\\
&[A \wedge B] = \min([A], [B]).
\end{aligned}$$

Osoitettava (induktiolla lauseen pituuden suhteen), että sumea valuaatio on tavallisen valuaation yleistys siinä mielessä, että jos v ja $[\circ]$ toteuttavat ehdon $v(p) = [p]$ kaikilla lausemuuttujilla p, niin $v(A) = [A]$ kaikilla propositiolauseilla.

96. Jatkoa. Miten kannattaa määritellä **a)** $[A \Rightarrow B]$, **b)** $[A \Leftrightarrow B]$?

97. Totuustaulukossa tarkastellaan vain niiden lausemuuttujien totuusarvoja, jotka esiintyvät tutkittavassa lauseessa, kun taas valuaatiot antavat kaikkien lausemuuttujien totuusarvot. Oikeutettava totuustaulukkomenetelmä todistamalla (induktiolla lauseen pituuden suhteen): Jos v ja v' ovat sellaisia valuaatioita, että $v(p) = v'(p)$ aina, kun p on lauseessa A esiintyvä lausemuuttuja, niin $v(A) = v'(A)$.

98. Olkoon P pienin sellainen joukko propositiolauseita, joka toteuttaa ehdot (1) $p_0 \in P$, (2) jos $A, B \in P$, niin $(A \circ B) \in P$, kun $\circ \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$. Olkoon v jokin sellainen totuusjakauma, että $v(p_0) = 1$. Todistettava: Jos $A \in P$, niin $v(A) = 1$.

99. Osoitettava (edellisen tehtävän perusteella), että negaatiota ei voida määritellä konjunktion, disjunktion, implikaation ja ekvivalenssin avulla.

100. Osoitettava, että implikaatiota, disjunktiota ja konjunktiota ei voida määritellä negaation ja ekvivalenssin avulla.

Luku 3

Joukot ja niiden laskutoimitukset

Nyt kysymme: Onko Maryn nenä Venn-diagrammissa? Tietenkään ei, koska Mary itsekään ei ole siellä. Maryn nenä on siis esitettävä diagrammin ulkopuolella olevalla pisteellä. Kirjoittaja ei mene niin pitkälle, että asettaisi tämän kysymyksen. Vaikka Mary ilmeisesti istuu pulpetissaan eikä Venn-diagrammissa, hän tietyssä mielessä on myös tässä diagrammissa, sillä hänelle on annettu nimi "a" ja "a" on Venn-diagrammissa.

(*Freudentahl* [4])

3.1 Peruskäsitteitä

1 Joukko

Aluksi meidän pitäisi selvittää, mitä *joukolla* tarkoitetaan matematiikassa. Cantor[1] määritteli, että "joukolla ymmärretään mitä tahansa kokonaisuudeksi muodostettua kokoelmaa täysin määrättyjä erillisiä olioita, jotka ovat tajuntamme tai ajatuksemme kohteina". Tämä määritelmä ei kuitenkaan ole matemaattisesti tyydyttävä, sillä herää kysymys, mitä "kokoelmalla" sitten tarkoitetaan. *Intuitiivisessa* eli *naiivissa joukko-opissa* ei tällaisista asioista välitetä, vaan katsotaan, että käsitteet 'joukko', 'alkio', 'kuuluu joukkoon' ja 'ei kuulu joukkoon' ovat niin itsestään selvästi ihmisen välittömässä tajunnassa (intuitio), ettei niitä tarvitse määritellä. *Aksiomaattisessa joukko-opissa* taas pyritään aikaansaamaan peruskäsitteiden määrittelyä myöten tarkka looginen järjestelmä. Joukko-opin päämerkitys matematiikassa on olla työväline, joten matemaatikon ei välttämättä tarvitse olla syvällisesti perehtynyt joukko-oppiin, sillä intuitiivinen joukko-oppi riittää antamaan tarvittavat välineet. Tästä syystä matematiikan yliopisto-opiskelu yleensä aloitetaan tutustumalla intuitiiviseen joukko-oppiin. Niin teemme mekin. Aksiomaattista joukko-oppia (ks. esim. [3, 8]) ei matematiikan perusopetuksessa käsitellä emmekä mekään puutu siihen tässä.

Olemme aiemmin (s. 23) määritelleet merkinnät $x \in A$, $x \notin A$ ja eräät

[1] *Georg Cantor (1845–1919), saksalainen matemaatikko, joukko-opin perustaja.*

lukujoukot. Joukko voidaan *merkitä* luettelemalla sen alkiot tai ilmoittamalla sen määrittelevä ominaisuus taikka sen kaikkia alkioita luonnehtiva käsite. Merkintä

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

tarkoittaa joukkoa, jonka alkiot ovat x_1, x_2, ..., x_n, ja merkintä

$$\{\, x \in X \mid p(x) \,\}$$

tarkoittaa joukon X kaikkien niiden alkioiden joukkoa, joilla on ominaisuus p.

Joukkoja voidaan määritellä myös rekursiivisesti.

Esimerkki 34. Määrittelemme joukon S seuraavasti.

- $3 \in S$.
- Jos $x \in S$, niin $x + 3 \in S$.
- Joukossa S ei ole muita alkioita kuin edellä saadut.

Nyt S on kaikkien 3:lla jaollisten positiivisten kokonaislukujen joukko (teht. 105).

Kaksi joukkoa ovat *samat*, jos niissä on täsmälleen samat alkiot. (Sanaa 'yhtäsuuret' ei käytetä, sillä se sotkeutuu käsitteeseen 'yhtä paljon alkioita'.) Merkitsemme $A = B$ tarkoittamaan sitä, että joukot A ja B ovat samat; siis

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

Merkintä $A \neq B$ tarkoittaa, etteivät joukot A ja B ole samat.

Esimerkki 35. $\{0, 2, 4, \ldots\} = \{\, x \in \mathbb{N} \mid x/2 \in \mathbb{N} \,\} = \{$parilliset luonnolliset luvut$\}$.

Olkoon $a, b \in \mathbb{R}$, $a < b$. Määrittelemme *reaalilukuvälit*

$$\begin{aligned}
]a, b[&= \{\, x \in \mathbb{R} \mid a < x < b \,\}, \\
[a, b] &= \{\, x \in \mathbb{R} \mid a \leq x \leq b \,\}, \\
[a, b[&= \{\, x \in \mathbb{R} \mid a \leq x < b \,\}, \\
]a, b] &= \{\, x \in \mathbb{R} \mid a < x \leq b \,\}.
\end{aligned}$$

Väli $]a, b[$ on *avoin*, $[a, b]$ *suljettu* ja $[a, b[$ sekä $]a, b]$ *puoliavoimia*. Määrittelemme myös *äärettömät välit*

$$\begin{aligned}
]a, \infty[&= \{\, x \in \mathbb{R} \mid x > a \,\}, \\
[a, \infty[&= \{\, x \in \mathbb{R} \mid x \geq a \,\}, \\
]-\infty, b[&= \{\, x \in \mathbb{R} \mid x < b \,\}, \\
]-\infty, b] &= \{\, x \in \mathbb{R} \mid x \leq b \,\}.
\end{aligned}$$

Voimme myös merkitä, että $]-\infty, \infty[= \mathbb{R}$.

2 Osajoukko

Joukko A on joukon B *osajoukko*, jos joukon A jokainen alkio kuuluu joukkoon B. Tällöin sanomme, että A *sisältyy* B:hen ja että B *sisältää* A:n (alkio kuuluu, osajoukko sisältyy), ja merkitsemme

$$A \subseteq B \text{ (tai myös } B \supseteq A).$$

Siis

$$A \subseteq B \Leftrightarrow \forall x (x \in A \Rightarrow x \in B).$$

Merkitsemme $A \nsubseteq B$, ellei joukko A ole joukon B osajoukko. Jos $A \subseteq B$, mutta $A \neq B$, niin sanomme, että A on B:n *aito osajoukko*, ja merkitsemme $A \subset B$.

Esimerkki 36. **a)** $\{1,2,3\} \subset \mathbb{N}$, **b)** $]a,b[\subset [a,b]$, **c)** $[-1,1] \subset]-\infty,1]$.

Lause 4. Olkoot A, B ja C joukkoja. Tällöin on voimassa

(r) $A \subseteq A$ (refleksiivisyys).

(as) Jos $A \subseteq B$ ja $B \subseteq A$, niin $A = B$ (antisymmetrisyys).

(t) Jos $A \subseteq B$ ja $B \subseteq C$, niin $A \subseteq C$ (transitiivisuus).

Todistamme tämän lauseen.
(r) Mielivaltainen joukon A alkio on tietenkin joukon A alkio.
(as) *Oletus.* $A \subseteq B$ ja $B \subseteq A$. *Väitös.* $A = B$.
Todistus. Käytämme epäsuoraa todistusta. Teemme vastaoletuksen $A \neq B$. On siis olemassa ainakin yksi sellainen alkio x, jolle

$$x \in A,\ x \notin B \quad \text{tai} \quad x \notin A,\ x \in B.$$

Edellinen tapaus ei ole mahdollinen. Nimittäin koska $A \subseteq B$, niin jokainen joukon A alkio on aina myös joukon B alkio, joten ei voi olla sellaista alkiota x, että $x \in A$ ja $x \notin B$. Siitä, että $B \subseteq A$, seuraa vastaavasti, ettei jälkimmäinenkään tapaus ole mahdollinen. Vastaoletus on siis väärä, joten $A = B$.
(t) *Oletus.* $A \subseteq B$ ja $B \subseteq C$. *Väitös.* $A \subseteq C$.
Todistus. Olkoon $x \in A$. Koska $A \subseteq B$, niin $x \in B$. Edelleen, koska $B \subseteq C$, niin $x \in C$. Siis mielivaltainen joukon A alkio on myös joukon C alkio eli $A \subseteq C$.

Transitiivisuuden perusteella voimme kirjoittaa $A \subseteq B \subseteq C$ tarkoittamaan sitä, että $A \subseteq B$ ja $B \subseteq C$. Vastaavasti voimme käyttää merkintää $\subset$.

Esimerkki 37. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Tarkastelemme vielä lauseen 4 todistusta logiikan kannalta. Refleksiivisyys oli niin itsestään selvä, että sen todistaminen saattaa tästä syystä olla aloittelijalle jopa hankalaa. Yleensä tällaiset triviaalit todistukset sivuutetaan, mutta niitäkin on syytä harjoitella.

Transitiivisuuden todistaminen oli varsin suoraviivaista. Yleensä jos tehtävämme on todistaa, että jokin joukko A on toisen joukon C osajoukko, niin meidän on osoitettava, että mielivaltaiselle oliolle x on voimassa $x \in A \Rightarrow x \in C$. Todistaessamme implikaatiota $p \Rightarrow q$ meidän ei tarvitse välittää siitä tapauksesta, että p on epätosi, koska tämä implikaatio on silloin aina tosi. Olennaista on tutkia sitä tapausta, jolloin p on tosi. Todistaessamme implikaatiota $x \in A \Rightarrow x \in C$ oletamme siis, että $x \in A$, ja käyttämällä hyväksi tätä oletusta ja muita tunnettuja tosiasioita näytämme, että $x \in C$.

Antisymmetrisyyden todistimme epäsuorasti. Yleisesti, kun todistamme lauseen $p \Rightarrow q$ epäsuorasti, niin teemme oletuksen p lisäksi vastaoletuksen $\neg q$. Vastaoletus on siis *väitöksen* negaatio eikä oletuksen. Osoitamme, että vastaoletuksesta seuraa jokin mahdoton tulos eli ristiriita. Tällöin vastaoletuksen täytyy olla väärä, ja alkuperäinen väitös on siis oikea. Olemme (s. 18) esittäneet tautologian, joka oikeuttaa epäsuoran todistamisen.

Lause 5. Olkoot A ja B joukkoja. Tällöin seuraavat ehdot ovat yhtäpitäviä.

(1) $A = B$,

(2) $A \subseteq B$ ja $B \subseteq A$.

Kahden ominaisuuden yhtäpitävyys on usein parasta todistaa näyttämällä, että implikaatio on voimassa kumpaankin suuntaan. Todistamme lauseen 5 tällä tavalla.

(1) $\Rightarrow$ (2). Väitämme siis, että $A \subseteq A$. Tämä seuraa lauseesta 4(r).

(2) $\Rightarrow$ (1). Väitämme siis, että jos $A \subseteq B$ ja $B \subseteq A$, niin $A = B$. Tämä seuraa lauseesta 4(as).

Kahden joukon A ja B samuutta todistettaessa kannattaa usein osoittaa, että A on B:n osajoukko ja että B on A:n osajoukko. Itse asiassa tällöin sovelletaan implikaation ja ekvivalenssin yhteyttä. Joukkojen samuus tarkoittaa näet ekvivalenssia

$$x \in A \Leftrightarrow x \in B$$

mielivaltaiselle oliolle x. Lauselogiikan perusteella se on yhtäpitävä implikaatioiden

$$x \in A \Rightarrow x \in B$$

ja

$$x \in B \Rightarrow x \in A$$

kanssa, jotka vastaavat osajoukkona oloa.

3 Perusjoukko

Jokaista joukossa X määriteltyä predikaattia $p(x)$ vastaa X:n osajoukko $\{\, x \in X \mid p(x)\,\}$. Kääntäen jokaista X:n osajoukkoa A vastaa ainakin yksi predikaatti, nimittäin $p(x) =$ '$x \in A$'. Yksipaikkainen predikaatti ja joukko ovat kuitenkin eri käsitteitä, ja yhtä joukkoa voi vastata useampi predikaatti.

Esimerkki 38. Tarkastelemme reaalilukujen joukossa määriteltyjä predikaatteja $p(x) =$ '$x^3 - 3x^2 + 2x = 0$', $q(x) =$ '$x = 0 \vee x = 1 \vee x = 2$' ja $r(x) =$ '$x \in \mathbb{N} \wedge x < 3$'. Nämä ovat eri predikaatteja, mutta joukot $\{\, x \in \mathbb{R} \mid p(x)\,\}$, $\{\, x \in \mathbb{R} \mid q(x)\,\}$ ja $\{\, x \in \mathbb{R} \mid r(x)\,\}$ ovat samat.

Jos joukko muodostetaan predikaatin avulla, niin predikaatin määrittelyjoukko on tiedettävä.

Esimerkki 39. Merkintä $\{\, x \mid 1 \leq x \leq 3\,\}$ ei sellaisenaan tarkoita mitään, ellei predikaatin '$1 \leq x \leq 3$' määrittelyjoukkoa ole ilmoitettu. Jos tämä määrittelyjoukko on $\mathbb{N}$, niin $\{\, x \mid 1 \leq x \leq 3\,\} = \{1, 2, 3\}$. Jos taas se on $\mathbb{R}$, niin $\{\, x \mid 1 \leq x \leq 3\,\} = [1, 3]$.

Joukko-opilliset tarkastelut rajoitetaan tavallisesti koskemaan vain tietyn *perusjoukon* eli *avaruuden* X alkioita ja osajoukkoja. Tällöin sovitaan yleensä, että joukkomerkinnöissä esiintyvien predikaattien määrittelyjoukkona on perusjoukko X. Jos kuitenkaan predikaatin määrittelyjoukoksi ei voida ottaa koko perusjoukkoa, niin tämä määrittelyjoukko on syytä mainita.

Esimerkki 40. Olkoon perusjoukko $\mathbb{R}$. Jos halutaan merkitä niiden reaalilukujen joukko, joiden luonnollinen logaritmi > 1, niin ei voida kirjoittaa $\{\, x \in \mathbb{R} \mid \ln x > 1\,\}$, koska predikaatti '$\ln x > 1$' ei ole määritelty, kun $x \leq 0$. Tämän predikaatin määrittelyjoukko on $\mathbb{R}_+$, joten on kirjoitettava $\{\, x \in \mathbb{R}_+ \mid \ln x > 1\,\}$.

4 Russellin paradoksi

Perusjoukon X käyttöönotolla on muutakin merkitystä kuin epäselvyyksien välttäminen. Sen tärkein merkitys on välttää *Russellin*[2] *paradoksi*, joka syntyy, jos oletamme, että aina on olemassa joukko $\{\, x \mid p(x)\,\}$, kun $p(x)$ on yksipaikkainen predikaatti.

Russellin paradoksi on seuraava. Tarkastelemme kaikkien sellaisten joukkojen joukkoa M, jotka eivät kuulu itseensä; siis $M = \{\, x \mid x \notin x\,\}$. Saattaa vaikuttaa siltä, että mikään joukko ei voi olla itsensä alkio. Mutta esimerkiksi kaikkien joukkojen joukko (jos sellainen olisi olemassa) olisi joukko ja siten itsensä alkio. Samoin jos olisi olemassa joukko $\{\, x \mid x \text{ ei ole hevonen}\,\}$, niin se ei varmastikaan olisi hevonen ja täten sekin olisi itsensä alkio. (Kaikki kolme tässä mainittua joukkoa ovat sikäli epämääräisiä, että mitään perusjoukkoa ei ole mainittu niiden yhteydessä.)

[2] *Bertrand Russell (1872–1970), englantilainen loogikko ja filosofi.*

Kysymme, kuuluuko joukko M itseensä. Katsomme aluksi, mitä tapahtuisi, jos M kuuluisi itseensä. Tällöin M kuuluu niiden joukkojen joukkoon, jotka eivät kuulu itseensä. Mutta sehän tarkoittaa, ettei M kuulu itseensä, joten päädymme ristiriitaan. Miten sitten käy, jos M ei kuulu itseensä? Yhtä huonosti, sillä tällöin M ei kuulu niiden joukkojen joukkoon, jotka eivät kuulu itseensä eli M kuuluu itseensä. Siis M ei voi kuulua itseensä eikä olla kuulumatta, joten paradoksi on valmis.

Käyttämällä luonnollisen kielen sijasta loogista formalismia voimme muotoilla Russellin paradoksin lyhemmin. Joukon M määritelmän mukaan jokaiselle joukolle A pätee

$$A \in M \Leftrightarrow A \notin A.$$

Sijoittamalla tähän joukon A paikalle joukon M saamme paradoksin

$$M \in M \Leftrightarrow M \notin M.$$

Russellin paradoksia voidaan havainnollistaa seuraavasti. Kylässä on miespuolinen parturi, joka ajaa kylän kaikkien niiden miesten parran, jotka eivät itse aja partaansa, ja vain niiden. Ajaako hän oman partansa?

5 Tyhjä joukko, potenssijoukko ja komplementti

Myös joukko $\{\, x \in X \mid x \neq x \,\}$ saattaa vaikuttaa paradoksaaliselta. Se on kuitenkin meille entuudestaan (s. 23) tuttu *tyhjä joukko* $\emptyset$, jossa ei ole yhtään alkiota ja jonka olemassaolosta ei seuraa mitään ristiriitaista. Ristiriitaan päädyttäisiin vasta, jos olisi olemassa jokin sellainen x, että $x \in \emptyset$. Tyhjälle joukolle voidaan käyttää myös merkintää $\{\ \}$. Joukko $\{\emptyset\}$ ei ole tyhjä, sillä siinä on yksi alkio, nimittäin $\emptyset$.

Lause 6. Tyhjä joukko on jokaisen joukon osajoukko. Siis aina $\emptyset \subseteq A$.

Tämä lause seuraa siitä, että implikaatiossa $x \in \emptyset \Rightarrow x \in A$ edellinen jäsen $x \in \emptyset$ on aina epätosi, joten implikaatio on aina tosi.

Toinen ehkä havainnollisempi todistustapa on käyttää epäsuoraa todistusta. Haluamme siis osoittaa, että $\emptyset \subseteq A$, ja teemme vastaoletuksen, että $\emptyset \not\subseteq A$. Tällöin on olemassa sellainen x, että $x \in \emptyset$ ja $x \notin A$, joten tyhjässä joukossa olisi alkio x, mistä syntyy ristiriita. Vastaoletus on siis väärä, joten $\emptyset \subseteq A$.

Joukon A *potenssijoukko* $\mathcal{P}(A)$ on A:n kaikkien osajoukkojen joukko. Kun perusjoukko on X, niin kaikki tarkasteltavat joukot ovat X:n osajoukkoja ja siis $\mathcal{P}(X)$:n alkioita. Potenssijoukon määritelmän perusteella

$$A \subseteq B \Leftrightarrow A \in \mathcal{P}(B).$$

Aina $\emptyset \in \mathcal{P}(A)$ ja $A \in \mathcal{P}(A)$.

Esimerkki 41. Olkoon $A = \{0\}$ ja $B = \{0, 1, 2\}$. Tällöin

$$\begin{aligned} \mathcal{P}(A) &= \{\emptyset, \{0\}\}, \\ \mathcal{P}(\mathcal{P}(A)) &= \mathcal{P}(\{\emptyset, \{0\}\}) = \{\emptyset, \{\emptyset\}, \{\{0\}\}, \{\emptyset, \{0\}\}\}, \\ \mathcal{P}(B) &= \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}. \end{aligned}$$

Joukossa $\mathcal{P}(\mathcal{P}(B))$ on 256 alkiota, mikä näkyy seuraavasta lauseesta.

Lause 7. Jos joukossa on n alkiota, niin sillä on 2^n osajoukkoa.

Voisimme käyttää todistuksessa kombinatoriikan tuloperiaatetta (s. 135, lause 35), jonka tarkka osoittaminen vaatii kuitenkin induktiota. Näin induktiota oikeastaan tarvitaan myös kombinatoriikkaan perustuvassa todistuksessa. Todistamme nyt tämän lauseen suoraan induktiolla.

Kun $n = 0$, niin lause on selvästi voimassa (miksi?), joten tutkimme asiaa, kun $n \in \mathbb{Z}_+$. Yleisyyttä rajoittamatta voimme tarkastella joukkoa $\{1, 2, \ldots, n\}$. Arvolla $n = 1$ väitös on tosi, sillä joukolla $\{1\}$ on $2^1 = 2$ osajoukkoa, nimittäin $\emptyset$ ja $\{1\}$. Teemme induktio-oletuksen: Joukolla $\{1, 2, \ldots, n\}$ on 2^n osajoukkoa. Nämä osajoukot ovat myös joukon $\{1, 2, \ldots, n+1\}$ osajoukkoja. Tuomalla jokaiseen tällaiseen osajoukkoon uudeksi alkioksi $n+1$ saamme 2^n uutta osajoukkoa. Joukolla $\{1, 2, \ldots, n+1\}$ ei ole muita osajoukkoja, joten sen osajoukkojen lukumäärä on $2^n + 2^n = 2^{n+1}$.

Olkoon X perusjoukko ja $A \subseteq X$. Joukon A *komplementti* $\overline{A}$ on X:n niiden alkioiden joukko, jotka eivät kuulu A:han. Siis

$$\overline{A} = \{\, x \in X \mid \neg(x \in A) \,\} = \{\, x \in X \mid x \notin A \,\}.$$

Komplementti riippuu täten perusjoukosta.

Esimerkki 42. Jos perusjoukko on $\mathbb{Z}$, niin joukon $\mathbb{N}$ komplementti $\overline{\mathbb{N}} = \mathbb{Z}_-$, mutta jos perusjoukko onkin $\mathbb{N}$, niin $\overline{\mathbb{N}} = \emptyset$.

Olkoon $x \in X$. Tällöin $x \in \overline{A}$, jos ja vain jos $x \notin A$. Kun tarkastelemme vain perusjoukon X alkioita, niin lauseet $x \in X$ ja $x \notin \emptyset$ ovat identtisesti tosia, joten lauseet $x \notin X$ ja $x \in \emptyset$ ovat identtisesti epätosia. Täten $x \in X \Leftrightarrow x \notin \emptyset$ ja $x \notin X \Leftrightarrow x \in \emptyset$. Olemme siis todistaneet seuraavan lauseen kaksi ensimmäistä yhtälöä.

Lause 8. $\overline{\emptyset} = X,\ \overline{X} = \emptyset,\ \overline{\overline{A}} = A$ (kaikilla $A \subseteq X$).

Todistamme kolmannen yhtälön. Kaksoisnegaation lain (s. 15) ja komplementin määritelmän perusteella saamme

$$x \in A \Leftrightarrow \neg\neg(x \in A) \Leftrightarrow \neg(x \in \overline{A}) \Leftrightarrow x \in \overline{\overline{A}}.$$

Harjoitustehtäviä

101. Merkittävä

a) yhtälön $x^3 + x^2 - 2x - 2 = 0$ ratkaisujen joukko,

b) parillisten negatiivisten kokonaislukujen joukko,

c) luvulla 5 jaollisten kokonaislukujen joukko.

102. Merkittävä

a) niiden kokonaislukujen joukko, joiden ilmoittama vuosi on karkausvuosi,

b) niiden luonnollisten lukujen joukko, jotka ovat luonnollisten lukujen neliöitä,

c) niiden reaalilukujen joukko, jotka eivät toteuta mitään kokonaiskertoimista toisen asteen yhtälöä.

103. Merkittävä yksinkertaisimmassa muodossaan joukko

a) $\{\, x \in \mathbb{Z} \mid x^2 = 4 \,\}$, **b)** $\{\, x \in \mathbb{Z} \mid x^2 = 2 \,\}$, **c)** $\{\, x \in \mathbb{R} \mid x^2 = 2 \,\}$.

104. Merkittävä yksinkertaisimmassa muodossaan joukko

a) $\{\, x \in \mathbb{Z} \mid \exists y \in \mathbb{Z}\colon x + y = x \,\}$, **b)** $\{\, x \in \mathbb{Z} \mid \exists y \in \mathbb{Z}\colon x + y = y \,\}$,

c) $\{\, x \in \mathbb{Z} \mid \forall y \in \mathbb{Z}\colon x + y = y \,\}$.

105. Todistettava, että esimerkissä 34 määritelty joukko S on kaikkien 3:lla jaollisten positiivisten kokonaislukujen joukko.

106. Määriteltävä rekursiivisesti kaikkien 5:llä jaollisten kokonaislukujen joukko.

107. Lueteltava joukon **a)** $\{1, 2, 3\}$, **b)** $\big\{a, \{a\}\big\}$ osajoukot.

108. Olkoon $A = \{2, 3\}$. Minkä seuraavien joukkojen **a)** alkio, **b)** osajoukko A on?

$$B = \big\{\{2\}, \{3\}\big\}, \quad C = \big\{2, 3, \{2, 3\}\big\}, \quad D = \big\{2, \{2\}, 3, \{3\}\big\},$$
$$E = \big\{\{2\}, \{3\}, \{2, 3\}\big\}, \quad F = \big\{\{2, 3, \{2, 3\}\}\big\}.$$

109. Olkoot A, B, C sellaisia joukkoja, että $A \in B$ ja $B \in C$. Voiko olla $A \in C$?

110. Olkoot A, B ja C joukkoja. Todistettava oikeaksi tai vääräksi

a) $(A \notin B \wedge B \notin C) \Rightarrow A \notin C$, **b)** $(A \in B \wedge B \notin C) \Rightarrow A \notin C$,

c) $(A \subseteq B \wedge B \notin C) \Rightarrow A \notin C$.

111. Todistettava oikeaksi tai vääräksi

a) $x \in A \Rightarrow \{x\} \subseteq A$,

b) jos joukko A toteuttaa ehdon $x \in A \Rightarrow \{x\} \in A$, niin $A = \emptyset$.

112. Olkoot $A = \big\{\emptyset, \{\emptyset\}\big\}$ ja $B = \big\{\{\emptyset\}\big\}$. Ovatko seuraavat väitteet tosia vai epätosia?

a) $A \in \mathcal{P}(B)$, **b)** $A \subseteq \mathcal{P}(B)$, **c)** $A \subset \mathcal{P}(B)$,

d) $B \in \mathcal{P}(A)$, **e)** $B \subseteq \mathcal{P}(A)$, **f)** $B \subset \mathcal{P}(A)$.

113. Muodostettava **a)** $\mathcal{P}(\emptyset)$, **b)** $\mathcal{P}\big(\mathcal{P}(\emptyset)\big)$, **c)** $\mathcal{P}\Big(\mathcal{P}\big(\mathcal{P}(\emptyset)\big)\Big)$.

114. Muodostettava (luettelemalla alkiot) seuraavat joukot ja niiden komplementit perusjoukon $\mathbb{Z}$ suhteen.

a) $\{\, x \in \mathbb{Z} \mid x < 3 \lor x \geq 8 \,\}$, **b)** $\{\, x \in \mathbb{Z} \mid \exists y \in \mathbb{Z}\colon x + y = 0 \,\}$,

c) $\{\, x \in \mathbb{Z} \mid \forall y \in \mathbb{Z}\colon x + y = 0 \,\}$.

115. Esitettävä yksinkertaisimmassa muodossaan seuraavat joukot ja niiden komplementit perusjoukon $\mathbb{R}$ suhteen.

a) $\{\, x \in \mathbb{R} \mid x = 2x \,\}$, **b)** $\{\, x \in \mathbb{R} \mid x < 0 \land x = x^2 \,\}$,

c) $\{\, x \in \mathbb{R} \mid \neg(x > x + 1) \,\}$.

116. Muodostettava välin **a)** $]a, \infty[$, **b)** $[a, \infty[$, **c)** $]-\infty, b[$, **d)** $]-\infty, b]$ komplementti perusjoukon $\mathbb{R}$ suhteen.

117. Olkoot A ja B joukkoja. Todistettava, että $A = B$, jos ja vain jos $\mathcal{P}(A) = \mathcal{P}(B)$.

118. Olkoot A ja B joukkoja. Todistettava: $A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$.

119. Mitkä lauseen 4 kohdat pysyvät voimassa, jos osajoukkona olon $\subseteq$ sijasta tarkastellaan aitona osajoukkona oloa $\subset$?

120. Olkoon A perusjoukon X osajoukko. Onko $\mathcal{P}(\overline{A}) = \overline{\mathcal{P}(A)}$ yleisesti voimassa? (Jälkimmäisessä komplementissa perusjoukko on $\mathcal{P}(X)$.)

3.2 Joukkojen laskutoimituksia

1 Yhdiste, leikkaus ja erotus

Olkoon X perusjoukko ja $A, B \subseteq X$ eli $A, B \in \mathcal{P}(X)$. Määrittelemme

$$
\begin{aligned}
A \cup B &= \{\, x \in X \mid x \in A \lor x \in B \,\},\\
A \cap B &= \{\, x \in X \mid x \in A \land x \in B \,\},\\
A \setminus B &= \{\, x \in X \mid x \in A \land x \notin B \,\}.
\end{aligned}
$$

Joukko $A \cup B$ (lue: ”A yhdiste B”) on joukkojen A ja B *yhdiste* eli *unioni*. Se koostuu perusjoukon X niistä alkioista, jotka kuuluvat A:han tai B:hen (tai molempiin). Joukko $A \cap B$ (lue: ”A leikkaus B”) on näiden joukkojen *leikkaus* ja se koostuu niistä alkioista, jotka kuuluvat A:han ja B:hen. Joukko $A \setminus B$ (lue: ”A miinus B”) on joukkojen A ja B (*joukko-opillinen*) *erotus*. Sen muodostavat A:n ne alkiot, jotka eivät kuulu B:hen.

Leikkaus ja erotus voidaan esittää myös ilman perusjoukkoa X, sillä

$$A \cap B = \{\, x \in A \mid x \in B \,\} = \{\, x \in B \mid x \in A \,\}$$

ja

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

Joukon A komplementti $\overline{A}$ on siis perusjoukon X ja joukon A joukko-opillinen erotus

$$\overline{A} = X \setminus A.$$

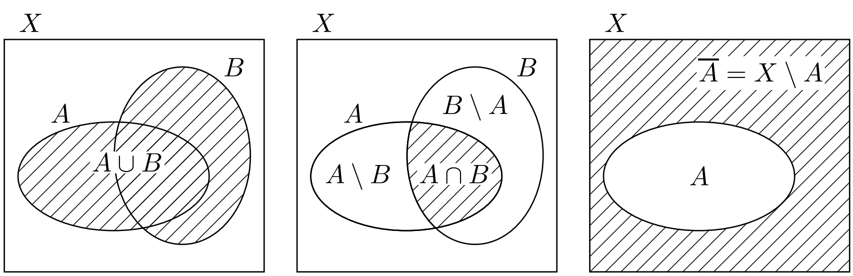
Merkintä $\overline{A}$ on yleensä mukavampi, mutta jos on epäselvää, minkä perusjoukon suhteen komplementti otetaan, niin kannattaa käyttää merkintää $X \setminus A$. Komplementti voidaan siis määritellä joukko-opillisen erotuksen avulla. Toisaalta joukko-opillinen erotus voidaan määritellä komplementin ja leikkauksen avulla

$$A \setminus B = A \cap \overline{B}.$$

Nimittäin

$$A \setminus B = \{\, x \in A \mid x \notin B \,\} = \{\, x \in A \mid x \in \overline{B} \,\} = A \cap \overline{B}.$$

Joukko-opin laskutoimituksia voidaan havainnollistaa *Venn*[3]*-diagrammeilla*, jolloin tarkasteltavat joukot esitetään tason pistejoukkoina.



2 Joukko-opin laskusääntöjen todistaminen

Joukko-opin laskutoimitukset $\cup$, $\cap$ ja $X\setminus$ vastaavat loogisia konnektiiveja $\vee$, $\wedge$ ja $\neg$. Yksi tapa todistaa joukko-opin laskusääntöjä on palauttaa ne vastaaviksi loogisia konnektiiveja koskeviksi väitteiksi ja sitten osoittaa nämä väitteet tautologioiksi. Pelkkä lauselogiikka ei kuitenkaan yleensä riitä, vaan on käytettävä myös predikaattilogiikkaa. Toinen tapa on käyttää luonnollista päättelyä. Kolmas tapa on käyttää aiemmin todistettuja joukko-opin laskusääntöjä.

[3] *John Venn (1834–1923), englantilainen loogikko.*

Joukko-opin laskusääntöjä voidaan havainnollisesti perustella Venn-diagrammeilla. Tällainen kuvion avulla tehtävä perustelu ei kuitenkaan täytä matemaattisia tarkkuusvaatimuksia. Tarkan todistuksen edellyttämät päättelyt tulevat kuviota piirrettäessä oikeastaan implisiittisesti tehdyiksi, mutta ne pitää kirjoittaa näkyviin, minkä jälkeen kuviota ei enää tarvitakaan muuhun kuin havainnollistamiseen. Täsmällisissä todistuksissa kuviota voidaan siis käyttää apuvälineenä, joka helpottaa varsinaisen todistuksen kirjoittamista ja lukemista, mutta valmiissa todistuksessa siihen ei saa enää nojautua.

Esimerkki 43. Tarkastelemme yhdisteen vaihdantalakia

$$A \cup B = B \cup A.$$

Yhdisteen määritelmän perusteella on selvää, että joukoilla $A \cup B$ ja $B \cup A$ on samat alkiot. Todistamme tämän täsmällisesti käyttämällä lauselogiikkaa. Olkoon $x \in X$. Tällöin

$$x \in A \cup B \overset{\mathrm{M}}{\Leftrightarrow} x \in A \vee x \in B \overset{\mathrm{T}}{\Leftrightarrow} x \in B \vee x \in A \overset{\mathrm{M}}{\Leftrightarrow} x \in B \cup A.$$

Ekvivalenssit $\overset{\mathrm{M}}{\Leftrightarrow}$ seuraavat yhdisteen määritelmästä. Ekvivalenssi $\overset{\mathrm{T}}{\Leftrightarrow}$ seuraa disjunktion vaihdantalaista eli tautologiasta

$$p \vee q \Leftrightarrow q \vee p.$$

Nyt siis $p =$ '$x \in A$', $q =$ '$x \in B$'.

Siis joukon X mielivaltaiselle alkiolle x pätee

$$x \in A \cup B \Leftrightarrow x \in B \cup A,$$

joten

$$\forall x \in X : x \in A \cup B \Leftrightarrow x \in B \cup A$$

eli $A \cup B = B \cup A$. Jouduimme tässä käyttämään predikaattilogiikan päättelysääntöä

$$\frac{p(x) \text{ on tautologia, kun } x \in X \text{ on mielivaltainen}}{\forall x \in X : p(x)}$$

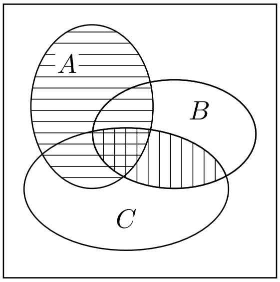
Tätä päättelysääntöä tarvitaan aina tällaisessa todistustavassa. Sen käyttöä ei yleensä kuitenkaan mainita, koska se vaikuttaa itsestään selvältä.

Esimerkki 44. Tarkastelemme osittelulakia

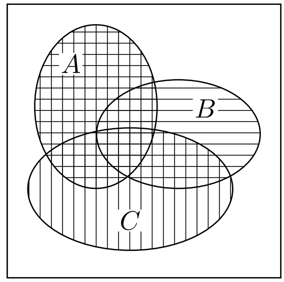
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

kolmella tavalla.

1. Venn-diagrammi. Kuviossa sekä joukkoa $A \cup (B \cap C)$ että joukkoa $(A \cup B) \cap (A \cup C)$ edustaa sama alue, joten osittelulaki näyttää olevan voimassa.



A vaakaviivoitettu
$B \cap C$ pystyviivoitettu
$A \cup (B \cap C)$ viivoitettu tai ruudutettu



$A \cup B$ vaakaviivoitettu
$A \cup C$ pystyviivoitettu
$(A \cup B) \cap (A \cup C)$ ruudutettu

2. Todistus lauselogiikan avulla. Kun $x \in X$, niin

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow x \in A \vee x \in B \cap C && \text{(yhdisteen määritelmä)} \\ &\Leftrightarrow x \in A \vee (x \in B \wedge x \in C) && \text{(leikkauksen määritelmä)} \\ &\Leftrightarrow (x \in A \vee x \in B) \\ &\qquad \wedge (x \in A \vee x \in C) && \text{(konnektiivien osittelulaki)} \\ &\Leftrightarrow x \in A \cup B \wedge x \in A \cup C && \text{(yhdisteen määritelmä)} \\ &\Leftrightarrow x \in (A \cup B) \cap (A \cup C) && \text{(leikkauksen määritelmä).} \end{aligned}$$

3. Todistus luonnollisella päättelyllä. Osoitamme, että

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C) \tag{1}$$

ja

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C), \tag{2}$$

minkä jälkeen väitös seuraa lauseesta 4(as) (s. 49).

Todistamme aluksi väitteen (1). Olkoon $x \in A \cup (B \cap C)$. Tällöin $x \in A$ tai $x \in B \cap C$. Jos $x \in A$, niin yhdisteen määritelmän perusteella $x \in A \cup B$ ja $x \in A \cup C$. Jos taas $x \in B \cap C$, niin myös tällöin $x \in A \cup B$ koska $x \in B$, ja $x \in A \cup C$ koska $x \in C$. Kummassakin tapauksessa siis $x \in A \cup B$ ja $x \in A \cup C$ eli $x \in (A \cup B) \cap (A \cup C)$. Joukon $A \cup (B \cap C)$ alkio on siis joukon $(A \cup B) \cap (A \cup C)$ alkio, joten (1) on tosi.

Todistamme sitten väitteen (2). Olkoon $x \in (A \cup B) \cap (A \cup C)$. Siis $x \in A \cup B$ ja $x \in A \cup C$. Jos $x \in A$, niin $x \in A \cup (B \cap C)$, jolloin asia on selvä. Voimme siis olettaa, että $x \notin A$. Koska $x \in A \cup B$, niin on oltava $x \in B$, ja koska $x \in A \cup C$, niin $x \in C$. Siis $x \in B \cap C$, joten nytkin $x \in A \cup (B \cap C)$. Näin (2) on todistettu.

Luonnollisessa päättelyssä on harkittava, kuinka paljon perusteluja kirjoittaa. Totesimme esimerkiksi, että yhdisteen määritelmän perusteella $x \in A \cup B$, koska $x \in A$. Emme katsoneet tarpeelliseksi perustella sitä enempää. Olisimme kuitenkin voineet todeta, että koska $x \in A$, niin $x \in A$ tai $x \in B$ ja täten $x \in A \cup B$.

3 Joukko-opin laskusääntöjä

Vastaavalla tavalla kuin edellä voimme todistaa muitakin laskusääntöjä joukoille. Esitämme tärkeimmät säännöt seuraavassa lauseessa.

Lause 9. Olkoon perusjoukkona X. Seuraavat laskusäännöt ovat voimassa.

Sääntö	**Nimi**
$A = A$	Identiteetin laki
$A \cap \overline{A} = \emptyset$ $A \cup \overline{A} = X$	Leikkaus ja yhdiste komplementin kanssa
$A \cap A = A$ $A \cup A = A$	Idempotenssilait
$A \cap \emptyset = \emptyset$ $A \cup \emptyset = A$	Leikkaus ja yhdiste tyhjän joukon kanssa
$A \cap X = A$ $A \cup X = X$	Leikkaus ja yhdiste perusjoukon kanssa
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	de Morganin säännöt
$A \cap B = B \cap A$ $A \cup B = B \cup A$	Vaihdantalait
$A \cap (B \cap C) = (A \cap B) \cap C$ $A \cup (B \cup C) = (A \cup B) \cup C$	Liitäntälait
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Osittelulait

Osa näiden todistuksista on harjoitustehtävinä (teht. 123–125).

Leikkaus ja yhdiste komplementin kanssa sekä de Morganin säännöt voidaan esittää myös muodossa

$$A \cap (X \setminus A) = \emptyset, \quad A \cup (X \setminus A) = X,$$
$$X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B), \quad X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B).$$

Lause 10. Olkoot A ja B perusjoukon X osajoukkoja. Tällöin

$$A \cap B \subseteq A \subseteq A \cup B.$$

Todistus on helppo.

Lause 11. Olkoot A ja B perusjoukon X osajoukkoja. Tällöin

$$A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}.$$

Todistus lauselogiikan avulla. Kun $x \in X$, niin kontraposition periaatteen (s. 18) mukaan lause $(x \in A \Rightarrow x \in B) \Leftrightarrow (x \notin B \Rightarrow x \notin A)$ on tautologia, joten

$$\forall x \in X\colon (x \in A \Rightarrow x \in B) \Leftrightarrow (x \notin B \Rightarrow x \notin A).$$

Nyt lauseen 2 (s. 28) mukaan

$$\forall x \in X\colon (x \in A \Rightarrow x \in B) \Leftrightarrow \forall x \in X\colon (x \notin B \Rightarrow x \notin A),$$

joten osajoukon määritelmän perusteella

$$A \subseteq B \Leftrightarrow \overline{B} \subseteq \overline{A}.$$

Jouduimme siis jälleen käyttämään predikaattilogiikkaa.

Todistus luonnollisella päättelyllä. Riittää osoittaa, että

$$A \subseteq B \Rightarrow \overline{B} \subseteq \overline{A}. \tag{1}$$

Nimittäin sijoittamalla A:n paikalle $\overline{A}$ ja B:n paikalle $\overline{B}$ saamme

$$\overline{A} \subseteq \overline{B} \Rightarrow \overline{\overline{B}} \subseteq \overline{\overline{A}},$$

ja edelleen, koska $\overline{\overline{A}} = A$ ja $\overline{\overline{B}} = B$ (lause 8), saamme implikaation (1) käänteiseen suuntaan

$$\overline{A} \subseteq \overline{B} \Rightarrow B \subseteq A.$$

Todistamme nyt (1):n. *Ol.* $A \subseteq B$. *Väit.* $\overline{B} \subseteq \overline{A}$. *Tod.* Olkoon $x \in \overline{B}$, jolloin $x \notin B$. Jos olisi $x \in A$, niin oletuksen perusteella saataisiin ristiriita $x \in B$. Siis $x \notin A$ eli $x \in \overline{A}$, joten $\overline{B} \subseteq \overline{A}$.

Esitämme vielä osajoukkona olon yhteyden joukko-opin laskutoimituksiin.

Lause 12. Olkoot A ja B perusjoukon X osajoukkoja. Seuraavat väitteet ovat yhtäpitäviä.

(1) $A \subseteq B$,

(2) $A \cap B = A$,

(3) $A \cup B = B$,

(4) $A \setminus B = \emptyset$.

Riittää todistaa jokin sopiva implikaatioketju, esimerkiksi (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1), toisin sanoen että (1) $\Rightarrow$ (2), (2) $\Rightarrow$ (3), (3) $\Rightarrow$ (4) ja (4) $\Rightarrow$ (1), ks. teht. 129. Todistamme implikaatiot (1) $\Rightarrow$ (2) ja (2) $\Rightarrow$ (3) luonnollisella päättelyllä ja jätämme loput harjoitustehtäväksi (teht. 130).

(1) $\Rightarrow$ (2). *Ol.* $A \subseteq B$. *Väit.* $A \cap B = A$. *Tod.* Jos $x \in A$, niin oletuksen mukaan $x \in B$, joten $x \in A \cap B$. Siis $A \subseteq A \cap B$. Toisaalta $A \cap B \subseteq A$ (lause 10), joten $A \cap B = A$ (s. 49, lause 4(as)).

(2) $\Rightarrow$ (3). *Ol.* $A \cap B = A$. *Väit.* $A \cup B = B$. *Tod.* Koska $B \subseteq A \cup B$ (lause 10), niin riittää (lause 4(as)) osoittaa, että $A \cup B \subseteq B$. Olkoon $x \in A \cup B$. Siis $x \in A$ tai $x \in B$. Jos $x \in B$, niin asia on selvä. Jos $x \in A$, niin koska $A \cap B = A$, silloinkin $x \in B$. Täten $A \cup B \subseteq B$.

Seuraavassa esimerkissä todistamme joukko-opillisen väitteen palauttamalla sen aiemmin todistettuihin laskusääntöihin.

Esimerkki 45. Osoitettava, että

$$(A \setminus B) \cap (B \setminus A) = \emptyset.$$

Voisimme käyttää lauselogiikkaa tai luonnollista päättelyä sen osoittamiseksi, että $x \in (A \setminus B) \cap (B \setminus A)$ on aina epätosi. Menettelemme kuitenkin toisin. Saamme

$$\begin{aligned}
(A \setminus B) \cap (B \setminus A) &= (A \cap \overline{B}) \cap (B \cap \overline{A}) && (D \setminus E = D \cap \overline{E}) \\
&= A \cap \big(\overline{B} \cap (B \cap \overline{A})\big) && \text{(liitäntälaki)} \\
&= A \cap \big((\overline{B} \cap B) \cap \overline{A}\big) && \text{(liitäntälaki)} \\
&= A \cap \big((B \cap \overline{B}) \cap \overline{A}\big) && \text{(vaihdantalaki)} \\
&= A \cap (\emptyset \cap \overline{A}) && \text{(leikkaus komplementin kanssa)} \\
&= A \cap (\overline{A} \cap \emptyset) && \text{(vaihdantalaki)} \\
&= A \cap \emptyset && \text{(leikkaus tyhjän joukon kanssa)} \\
&= \emptyset && \text{(leikkaus tyhjän joukon kanssa).}
\end{aligned}$$

Kun joukossa $\mathcal{P}(X)$ määritellään laskutoimitukset $\cup$, $\cap$ ja $X\setminus$, niin saatu *algebrallinen struktuuri* on *Boolen*[4] *algebra*. Se voidaan määritellä myös aksiomaattisesti valitsemalla joukko-opin laskusäännöistä sopivat aksioomiksi. Tällöin muut säännöt voidaan todistaa niiden avulla. Ks. esim. Sikorski [24].

4 Yhdisteen ja leikkauksen yleistykset

Olkoot A_1, $A_2, \ldots$ perusjoukon X osajoukkoja eli potenssijoukon $\mathcal{P}(X)$ alkioita. Liitäntälakien perusteella ei yhdisteessä $A_1 \cup A_2 \cup \cdots \cup A_n$ eikä leikkauksessa $A_1 \cap A_2 \cap \cdots \cap A_n$ tarvita sulkumerkkejä. Merkitsemme

$$\begin{aligned}
\bigcup_{k=1}^{n} A_k &= A_1 \cup A_2 \cup \cdots \cup A_n = \big\{\, x \in X \mid \exists k \in \{1, 2, \ldots, n\} \colon x \in A_k \,\big\}, \\
\bigcap_{k=1}^{n} A_k &= A_1 \cap A_2 \cap \cdots \cap A_n = \big\{\, x \in X \mid \forall k \in \{1, 2, \ldots, n\} \colon x \in A_k \,\big\}, \\
\bigcup_{k=1}^{\infty} A_k &= \{\, x \in X \mid \exists k \in \mathbb{Z}_+ \colon x \in A_k \,\}, \\
\bigcap_{k=1}^{\infty} A_k &= \{\, x \in X \mid \forall k \in \mathbb{Z}_+ \colon x \in A_k \,\}.
\end{aligned}$$

[4] *George Boole (1815–1864), englantilainen matemaatikko ja loogikko.*

Esimerkki 46. Olkoon $X = \mathbb{R}$, $A_k = [k-1, k]$, kun $k \in \mathbb{Z}_+$. Tällöin

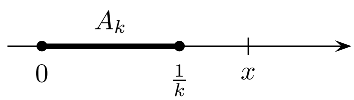
$$\bigcap_{k=1}^{3} A_k = [0,1] \cap [1,2] \cap [2,3] = \emptyset,$$
$$\bigcup_{k=1}^{n} A_k = [0,1] \cup [1,2] \cup \cdots \cup [n-1,n] = [0,n],$$
$$\bigcap_{k=1}^{\infty} A_k = \emptyset, \qquad \bigcup_{k=1}^{\infty} A_k = [0,\infty[\,.$$

Esimerkki 47. Olkoon $X = \mathbb{R}$, $A_k = [0, 1/k]$, kun $k \in \mathbb{Z}_+$. Osoitettava, että

$$\bigcup_{k=1}^{\infty} A_k = [0,1], \qquad \bigcap_{k=1}^{\infty} A_k = \{0\}.$$

Koska $A_1 \supseteq A_2 \supseteq \cdots$, niin x kuuluu johonkin näistä joukoista, jos ja vain jos $x \in A_1$. Siis $\bigcup_{k=1}^{\infty} A_k = A_1 = [0,1]$.

Jos $x = 0$, niin $x \in A_k$ kaikilla $k \in \mathbb{Z}_+$, joten $x \in \bigcap_{k=1}^{\infty} A_k$. Jos taas $x < 0$, niin esimerkiksi $x \notin A_1$, joten $x \notin \bigcap_{k=1}^{\infty} A_k$. Jos vihdoin $x > 0$, niin $x \notin A_k$, kun $k > \frac{1}{x}$, joten $x \notin \bigcap_{k=1}^{\infty} A_k$. Siis $\bigcap_{k=1}^{\infty} A_k = \{0\}$.



Joukkoa, jonka alkiot ovat joukkoja, kutsutaan usein *joukkoperheeksi* (engl. *family of sets*). Edellä tutkimiemme *indeksoitujen joukkoperheiden* indeksijoukko on äärellinen tai $\mathbb{Z}_+$. Voimme tarkastella sellaisiakin joukkoperheitä, joiden indeksijoukko on jokin muu. Olkoon $\{A_k\}_{k \in I}$ tällainen joukkoperhe, siis indeksijoukon I jokaiseen alkioon k liittyy tietty joukko A_k. Edellä määrittelemämme yhdisteet koostuvat niistä alkioista, jotka kuuluvat *ainakin yhteen* joukkoon A_k, ja leikkaukset niistä, jotka kuuluvat *kaikkiin* joukkoihin A_k. Täten voimme määritellä yleisesti

$$\bigcup_{k \in I} A_k = \{\, x \in X \mid \exists k \in I \colon x \in A_k \,\},$$
$$\bigcap_{k \in I} A_k = \{\, x \in X \mid \forall k \in I \colon x \in A_k \,\}.$$

Esimerkki 48. Jokainen joukko A $(\neq \emptyset)$ voidaan esittää alkioidensa muodostamien *yksiöiden* eli yksialkioisten joukkojen yhdisteenä (jolloin indeksijoukko $I = A$)

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

5 Luokkajako

Olkoon X perusjoukko ja $A, B \subseteq X$ eli $A, B \in \mathcal{P}(X)$. Joukot A ja B ovat *erillisiä*, jos niillä ei ole yhteisiä alkioita eli $A \cap B = \emptyset$. Olkoon I sellainen indeksijoukko, että $A_i \in \mathcal{P}(X)$ kaikilla $i \in I$. Joukot A_i $(i \in I)$ ovat *pareittain erillisiä*, jos A_i ja A_j ovat erillisiä aina, kun $i, j \in I$ ja $i \neq j$.

Joukkoperhe $\{A_k\}_{k \in I}$ on joukon X *ositus* eli *luokkajako*, jos sen joukot ovat epätyhjiä ja pareittain erillisiä sekä

$$X = \bigcup_{k \in I} A_k.$$

Esimerkki 49. Joukon $X = \{a, b, c, d, e, f\}$ eräs luokkajako on joukkoperhe

$$\big\{\{a, b, c\}, \{d, e\}, \{f\}\big\}.$$

Tällöin $I = \{1, 2, 3\}$, $A_1 = \{a, b, c\}$, $A_2 = \{d, e\}$, $A_3 = \{f\}$.

Esimerkki 50. Olkoon tietyssä koulussa n luokkaa. Olkoon A_1 1. luokan, A_2 2. luokan, $\ldots$, A_n n. luokan oppilaiden joukko. Tällöin koulun kaikkien oppilaiden joukon X eräs luokkajako on $\{A_1, A_2, \ldots, A_n\}$. Nimittäin nämä joukot ovat pareittain erillisiä (kukaan oppilas ei ole kahdella luokalla) ja $X = A_1 \cup A_2 \cup \cdots \cup A_n$ (jokainen oppilas on jollakin luokalla).

Esimerkki 51. Joukkoperhe $\{[0, 1], [1, 2], \ldots\}$ ei ole joukon $\mathbb{R}_{+0} = [0, \infty[$ luokkajako. Nimittäin esimerkiksi $[0, 1] \cap [1, 2] = \{1\}$, joten joukot eivät ole pareittain erillisiä. Sen sijaan joukkoperhe $\{[0, 1[\,, [1, 2[\,, \ldots\}$ on joukon $\mathbb{R}_{+0}$ luokkajako. Miksi?

Esimerkki 52. Joukkoperheet $\{X\}$ ja $\big\{\, \{x\} \mid x \in X \,\big\}$ ovat aina joukon $X \neq \emptyset$ luokkajakoja. Miksi?

Harjoitustehtäviä

121. Olkoon perusjoukko $X = \{1, 2, \ldots, 10\}$, $A = \{\, x \in X \mid x \text{ on parillinen} \,\}$, $B = \{\, x \in X \mid x \text{ on alkuluku} \,\}$. Muodostettava (luettelemalla alkiot) joukot A, B, $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, $\overline{A}$ ja $\overline{B}$.

122. Olkoon $A = \{1, 2, 3\}$ ja $B = \{1, n\}$, $n \in \mathbb{Z}_+$. Muodostettava joukot $A \cup B$, $A \cap B$, $A \setminus B$ ja $B \setminus A$. Mitä voidaan sanoa joukoista $\overline{A}$ ja $\overline{B}$?

123. Havainnollistettava Venn-diagrammilla liitäntälakia

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

Todistettava nämä säännöt (lauselogiikan avulla tai luonnollisella päättelyllä).

124. Kuten edellä, mutta tarkastellaan toista osittelulakia

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

125. Kuten edellä, mutta tarkastellaan de Morganin sääntöjä

a) $\overline{A \cup B} = \overline{A} \cap \overline{B}$, **b)** $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

126. Todistettava *absorptiolait*

a) $A \cup (A \cap B) = A$, **b)** $A \cap (A \cup B) = A$.

127. Onko yleisesti voimassa

a) $A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C)$,

b) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$?

128. Esitettävä yksinkertaisimmassa muodossaan joukko

a) $(A \setminus B) \cup (B \setminus A) \cup (A \cap B)$, **b)** $A \cup (B \setminus A)$, **c)** $A \cap (B \setminus A)$.

129. Todistettava: Jos implikaatioketju

$$p_1 \Rightarrow p_2 \Rightarrow p_3 \Rightarrow \cdots p_{n-1} \Rightarrow p_n \Rightarrow p_1$$

on voimassa, niin väitteet p_i, $i = 1, 2, \ldots, n$, ovat yhtäpitäviä eli kun $1 \leq i < j \leq n$, niin $p_i \Leftrightarrow p_j$.

130. Todistettava lause 12 loppuun osoittamalla, että (3) $\Rightarrow$ (4) ja (4) $\Rightarrow$ (1).

131. Olkoot A ja B perusjoukon X osajoukkoja. Seuraavassa "todistetaan", että aina $A \subseteq B$ tai $B \subseteq A$. Missä on virhe?

Olkoon $x \in X$. Lause

$$(x \in A \Rightarrow x \in B) \vee (x \in B \Rightarrow x \in A)$$

on tautologia, joten

$$\forall x \in X\colon \big((x \in A \Rightarrow x \in B) \vee (x \in B \Rightarrow x \in A)\big)$$

ja edelleen

$$\forall x \in X\colon (x \in A \Rightarrow x \in B) \vee \forall x \in X\colon (x \in B \Rightarrow x \in A).$$

Siis $A \subseteq B \vee B \subseteq A$.

132. Joukossa X määriteltyjen predikaattien $p(x)$ ja $q(x)$ *ratkaisujoukot* ovat $L_p = \{\, x \in X \mid p(x) \,\}$ ja $L_q = \{\, x \in X \mid q(x) \,\}$. Todistettava

a) $L_{p \vee q} = L_p \cup L_q$, **b)** $L_{p \wedge q} = L_p \cap L_q$, **c)** $L_{\neg p} = X \setminus L_p$,

d) jos ja vain jos $p(x) \Rightarrow q(x)$, niin $L_p \subseteq L_q$,

e) jos ja vain jos $p(x) \Leftrightarrow q(x)$, niin $L_p = L_q$.

133. Boolen algebrassa on voimassa *duaalisuusperiaate*. Jos jokin Boolen algebraa koskeva väite on tosi, niin samoin on sen *duaalinen väite*, joka saadaan alkuperäisestä väitteestä korvaamalla

- yhdiste $\cup$ leikkauksella $\cap$ ja leikkaus $\cap$ yhdisteellä $\cup$
- osajoukko $\subseteq$ osajoukolla $\supseteq$ ja osajoukko $\supseteq$ osajoukolla $\subseteq$
- joukko X tyhjällä joukolla $\emptyset$ ja joukko $\emptyset$ joukolla X, mutta komplementtia $X\setminus$ ei muuteta.

Jos erotukseen $A \setminus B$ halutaan soveltaa duaalisuusperiaatetta, niin se on kirjoitettava muotoon $A \cap (X \setminus B)$.

Annettava esimerkkejä keskenään duaalisista joukko-opin väitteistä.

134. Todistettava: Jos $A \subseteq C$ ja $B \subseteq D$, niin $A \cap B \subseteq C \cap D$. Mikä on duaalinen väite?

135. Onko yleisesti voimassa

a) $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$, **b)** $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$?

136. Olkoon $A_k =]0, 1/k[$. Muodostettava joukko

a) $\displaystyle\bigcup_{k=1}^{n} A_k$, **b)** $\displaystyle\bigcap_{k=1}^{n} A_k$, **c)** $\displaystyle\bigcup_{k=1}^{\infty} A_k$, **d)** $\displaystyle\bigcap_{k=1}^{\infty} A_k$.

137. Yleistettävä osittelulait mielivaltaiselle indeksijoukolle I osoittamalla, että

a) $\displaystyle A \cap \Big(\bigcup_{k\in I} B_k\Big) = \bigcup_{k\in I}(A \cap B_k)$, **b)** $\displaystyle A \cup \Big(\bigcap_{k\in I} B_k\Big) = \bigcap_{k\in I}(A \cup B_k)$.

138. Yleistettävä de Morganin säännöt mielivaltaiselle indeksijoukolle I osoittamalla, että

a) $\displaystyle\overline{\bigcap_{k\in I} A_k} = \bigcup_{k\in I} \overline{A_k}$, **b)** $\displaystyle\overline{\bigcup_{k\in I} A_k} = \bigcap_{k\in I} \overline{A_k}$.

139. Määritettävä joukon $\{1, 2, 3\}$ kaikki luokkajaot.

140. Olkoon X perusjoukko ja $A_1, A_2, A_3 \in \mathcal{P}(X)$. Osoitettava, että on olemassa sellaiset joukot $B_1, B_2, B_3 \in \mathcal{P}(X)$, että $B_1 \cap B_2 = B_2 \cap B_3 = B_3 \cap B_1 = \emptyset$, $A_1 = B_1$, $A_1 \cup A_2 = B_1 \cup B_2$ ja $A_1 \cup A_2 \cup A_3 = B_1 \cup B_2 \cup B_3$. Mikä luokkajako näin saadaan? Miten tätä voidaan yleistää?

Luku 4

Relaatiot

On ilmeistä, että koemme muotoa "a R b" olevan lauseen kuvaksi. Siinä merkki selvästikin on merkityksensä vertauskuva.

(*Wittgenstein* [31])

4.1 Tulojoukko ja relaatio

1 Järjestetty pari

Tutkittaessa joukkoja sellaisinaan ei niiden alkioiden järjestykseen kiinnitetä huomiota eikä saman alkion useampikertaisella esiintymisellä ole vaikutusta.

Esimerkki 53. **a)** $\{\text{Matti, Maija}\} = \{\text{Maija, Matti}\}$, **b)** $\{1, 2, 3\} = \{1, 3, 2\}$, **c)** $\{\text{Maija, Maija}\} = \{\text{Maija}\}$, **d)** $\{1, 1, 3\} = \{1, 3\}$.

Määrittelemme nyt käsitteitä, joissa tällaisiin asioihin kiinnitetään huomiota. Alkioiden x ja y muodostamalla *järjestetyllä parilla* tarkoitamme havainnollisesti sellaista jonoa, jossa x on ensimmäisenä ja y toisena, ja merkitsemme sitä (x, y). Kaksi järjestettyä paria ovat *samat*, jos niiden ensimmäiset alkiot keskenään ja toiset keskenään ovat samat

$$(x, y) = (u, v) \Leftrightarrow x = u \wedge y = v.$$

On tärkeää huomata järjestetyn parin ja ”järjestämättömän” kaksialkioisen joukon ero.

Esimerkki 54. **a)** Jos $x \neq y$, niin $\{x, y\} = \{y, x\}$, mutta $(x, y) \neq (y, x)$. **b)** $\{x, x\} = \{x\}$, mutta $(x, x) \neq (x)$, missä oikea puoli tarkoittaa jonoa, jonka ensimmäisellä ja ainoalla paikalla on x.

Mutta mitä tarkoittaa ”alkioiden järjestäminen jonoon”? Kaikkein vähimmällä pääsisimme menettelemällä kuten teimme joukko-opin ensimmäisille peruskäsitteille (s. 47) eli ajattelemalla, että järjestyksen käsite on ihmisen tajunnassa niin selvä ja primitiivinen, ettei sitä kannata yrittää tarkemmin määritellä. Tulemme kuitenkin pian (luku 4.5) huomaamaan, että yleinen *järjestetyn joukon* käsite on tarpeellista ja mahdollista määritellä matemaattisesti. Tämä määritelmä tarvitsee *relaation* ja edelleen järjestetyn parin käsitettä, joten asia saadaan kuntoon määrittelemällä järjestetty pari joukko-opin peruskäsitteiden avulla. Esitämme määritelmän, joka tuntuu keinotekoiselta, mutta joka toimii loogisesti. Määrittelemme, että $(x, y) = \big\{\{x\}, \{x, y\}\big\}$. Siis *järjestetty pari* (x, y) tarkoittaakin *joukkoa*, jonka *alkiot* ovat $\{x\}$ ja $\{x, y\}$!

Kun ajattelee järjestettyjen parien käyttöä vaikkapa niin, että (x, y) tarkoittaa tulosta, jossa korttipakasta on ensin otettu kortti x ja sitten kortti y, tämä määritelmä tuntuu tietenkin täysin mielettömältä. Jos otan pakasta kortit x ja y, niin saanko todellisuudessa kummallisen korttijoukon $\{\{x\}, \{x, y\}\}$? Vastaus tähän kysymykseen on tietenkin kielteinen jo siksi, ettei reaalimaailmassa yleensäkään esiinny matemaattisia käsitteitä konkreettisesti. Sovelluksissa käytettävän matemaattisen käsitteen määritelmän ei tarvitsekaan tuntua sovelluksen kannalta järkevältä, vaan riittää, että se toimii matemaattisesti, sillä sovelluksissa voidaan unohtaa tämän käsitteen varsinainen matemaattinen olemus. Matemaattisesti kiinnostavinta järjestetyn parin määritelmässä on, että sen antama samuuden käsite sopii yhteen samuuden määritelmän $(x, y) = (u, v) \Leftrightarrow x = u \wedge y = v$ kanssa. Näin on, sillä

$$\begin{aligned}
(x, y) = (u, v) &\Leftrightarrow \big\{\{x\}, \{x, y\}\big\} = \big\{\{u\}, \{u, v\}\big\} \\
&\Leftrightarrow \big(\{x\} = \{u\} \wedge \{x, y\} = \{u, v\}\big) \\
&\qquad \vee \big(\{x\} = \{u, v\} \wedge \{x, y\} = \{u\}\big) \\
&\Leftrightarrow (x = u \wedge y = v) \vee (x = u = v \wedge x = y = u) \\
&\Leftrightarrow (x = u \wedge y = v) \vee (x = u = v = y) \Leftrightarrow x = u \wedge y = v.
\end{aligned}$$

Matemaattisen käsitteen täsmällisen määritelmän ei siis välttämättä tarvitse vastata sitä mielikuvaa, joka meillä tästä käsitteestä on.

Myös järjestetyn *kolmikon* (x, y, z), *nelikön* (x, y, z, u) ja yleisesti n:kön käsitteet ovat intuitiivisesti selvät. Ne voidaan määritellä täsmällisesti esimerkiksi kuvauksina (luku 5.1) tai järjestettyinä joukkoina (luku 4.5). Kahden järjestetyn n:kön samuuden määritelmä voidaan tällöin esittää vastaavien alkioiden eli *koordinaattien* samuutena.

2 Tulojoukko

Joukkojen A ja B *tulojoukko* eli *karteesinen*[1] *tulo* on

$$A \times B = \{\, (x, y) \mid x \in A \wedge y \in B \,\}.$$

Siis $A \times B$ koostuu kaikista niistä järjestetyistä pareista (x, y), joilla $x \in A$ ja $y \in B$.

Esimerkki 55. Olkoon $A = \{1, 2, 3\}$ ja $B = \{4, 5\}$. Tällöin

$$\begin{aligned}
A \times B &= \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}, \\
B \times A &= \{(4, 1), (4, 2), (4, 3), (5, 1), (5, 2), (5, 3)\}.
\end{aligned}$$

Vastaavasti määrittelemme n joukon tulojoukon

$$A_1 \times \cdots \times A_n = \{\, (x_1, \ldots, x_n) \mid x_1 \in A_1 \wedge \cdots \wedge x_n \in A_n \,\}$$

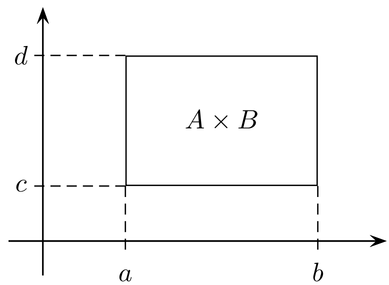
[1] *René Descartes (lat. Renatus Cartesius) (1596–1650), ranskalainen filosofi ja matemaatikko.*

ja merkitsemme

$$A^n = \overbrace{A \times A \times \cdots \times A}^{n \text{ kertaa}}.$$

Esimerkki 56. **a)** Joukko $\mathbb{R}^2$ on järjestettyjen reaalilukuparien joukko. Sen geometrinen vastine on taso. **b)** Joukko $\mathbb{R}^3$ on järjestettyjen reaalilukukolmikoiden joukko. Sen geometrinen vastine on kolmiulotteinen avaruus. **c)** Joukko $\mathbb{R}^n$ on järjestettyjen reaaliluku n:kköjen joukko. Sen vastine on n-ulotteinen avaruus. Vaikka meillä ei ole siitä geometrista mielikuvaa, voimme tutkia tätä avaruutta tulojoukkona.

Olkoon $A = [a, b]$ koordinaatiston x-akselilla ja $B = [c, d]$ y-akselilla. Joukon $A \times B$ geometrinen merkitys on kuvion suorakulmio.



3 Tulojoukon laskusääntöjä

Jos $A \neq B$ $(A, B \neq \emptyset)$, niin $A \times B \neq B \times A$ (esim. 55 ja teht. 145), joten tulojoukon muodostaminen ei noudata vaihdantalakia. Myöskään liitäntälaki ei ole voimassa. Nimittäin

$$\begin{aligned} A \times (B \times C) &= \{\, \big(x, (y, z)\big) \mid x \in A \wedge y \in B \wedge z \in C \,\}, \\ (A \times B) \times C &= \{\, \big((x, y), z\big) \mid x \in A \wedge y \in B \wedge z \in C \,\}, \\ A \times B \times C &= \{\, (x, y, z) \mid x \in A \wedge y \in B \wedge z \in C \,\}, \end{aligned}$$

mutta $\big(x, (y, z)\big)$, $\big((x, y), z\big)$ ja (x, y, z) eivät ole samat (teht. 146).

Lause 13. Tulojoukon muodostaminen noudattaa osittelulakia yhdisteen, leikkauksen ja erotuksen suhteen

(1) $(A_1 \cup A_2) \times B = (A_1 \times B) \cup (A_2 \times B)$,

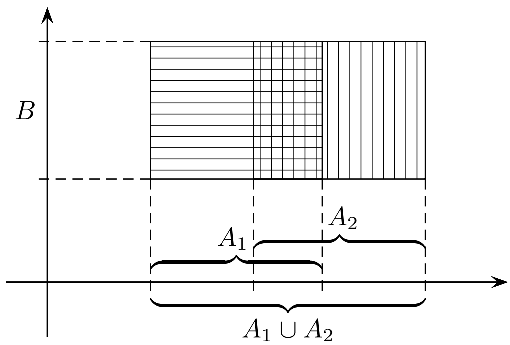
(2) $(A_1 \cap A_2) \times B = (A_1 \times B) \cap (A_2 \times B)$,

(3) $(A_1 \setminus A_2) \times B = (A_1 \times B) \setminus (A_2 \times B)$.

Vastaavat tulokset ovat voimassa joukolle $A \times (B_1 \cup B_2)$ jne. Todistamme näistä ominaisuuksista ensimmäisen ja jätämme muut harjoitustehtäviksi (teht. 147). Saamme

$$
\begin{aligned}
&(x,y) \in (A_1 \cup A_2) \times B \\
&\quad \Leftrightarrow x \in A_1 \cup A_2 \wedge y \in B && \text{(tulojoukon määritelmä)} \\
&\quad \Leftrightarrow (x \in A_1 \vee x \in A_2) \wedge y \in B && \text{(yhdisteen määritelmä)} \\
&\quad \Leftrightarrow (x \in A_1 \wedge y \in B) \vee (x \in A_2 \wedge y \in B) && \text{(konnektiivien osittelulaki)} \\
&\quad \Leftrightarrow (x,y) \in A_1 \times B \vee (x,y) \in A_2 \times B && \text{(tulojoukon määritelmä)} \\
&\quad \Leftrightarrow (x,y) \in (A_1 \times B) \cup (A_2 \times B) && \text{(yhdisteen määritelmä).}
\end{aligned}
$$

Kuvio havainnollistaa todistusta. Siinä $A_1 \times B$ on vaakaviivoitettu ja $A_2 \times B$ on pystyviivoitettu alue. Niiden yhdiste, viivoitettu tai ruudutettu alue, on todellakin $(A_1 \cup A_2) \times B$.



4 Relaation käsite

Jos $R \subseteq X \times Y$ $(X, Y \neq \emptyset)$, niin sanomme, että R on *relaatio* joukkojen X ja Y alkioiden välillä tai lyhemmin, että R on joukkojen X ja Y relaatio. Sanomme myös, että R on relaatio jouko*sta* X joukko*on* Y (huomaa sijat). Kutsumme joukkoa X relaation R *lähtöjoukoksi* ja joukkoa Y *maalijoukoksi.* Alkiot $x \in X$ ja $y \in Y$ ovat keskenään relaatiossa R eli $R(x, y)$ on voimassa, jos ja vain jos $(x, y) \in R$. Myös useampipaikkainen relaatio voidaan määritellä (ja myös yksipaikkainen). Yleisesti tarkoitamme joukkojen X_1, X_2, …, X_n $(\neq \emptyset)$ alkioiden välisellä relaatiolla osajoukkoa $R \subseteq X_1 \times X_2 \times \cdots \times X_n$, ja $R(x_1, x_2, \ldots, x_n)$ on voimassa, jos ja vain jos $(x_1, x_2, \ldots, x_n) \in R$. Joukkoa X_i voidaan tällöin kutsua relaation *i:nnen muuttujan määrittelyjoukoksi.*

Olkoon R relaatio joukosta X joukkoon Y, jolloin X on sen lähtöjoukko ja Y maalijoukko. Relaation R *määrittelyjoukko* M_R on joukon X niiden alkioiden joukko, jotka ovat relaatiossa joukon Y jonkin alkion kanssa eli

$$M_R = \{\, x \in X \mid \exists y \in Y \colon xRy \,\}.$$

Tämän relaation *arvojoukko* A_R on joukon Y niiden alkioiden joukko, jotka ovat relaatiossa joukon X jonkin alkion kanssa eli

$$A_R = \{\, y \in Y \mid \exists x \in X \colon xRy \,\}.$$

Lähtö-, maali-, määrittely- ja arvojoukosta voidaan puhua vain relaation ollessa kaksipaikkainen. Tällaisen relaation määrittelyjoukko on aivan eri käsite kuin edellä mainittu relaation muuttujan määrittelyjoukko.

Jos R on kaksipaikkainen relaatio, niin merkitsemme xRy tarkoittamaan sitä, että $R(x, y)$ on voimassa. Siis

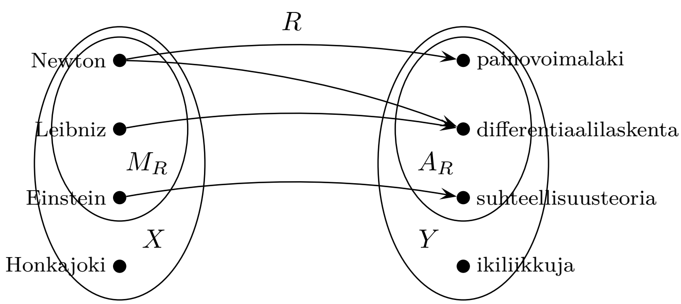
$$xRy \Leftrightarrow R(x, y) \Leftrightarrow (x, y) \in R.$$

Vastaavasti merkitsemme $x \not R y$ tarkoittamaan, että $R(x, y)$ ei ole voimassa.

Esimerkki 57. Kaikkein yksinkertaisimmat relaatiot joukkojen X ja Y alkioiden välillä ovat $\emptyset$ ja $X \times Y$. Jälkimmäisessä relaatiossa ovat keskenään kaikki alkiot x $(\in X)$ ja y $(\in Y)$, ja edellisessä eivät mitkään.

5 Relaatio nuolikuviona ja polkukuviona

Esimerkki 58. Olkoon $X = \{$Newton, Leibniz, Einstein, Honkajoki$\}$ ja $Y = \{$painovoimalaki, differentiaalilaskenta, suhteellisuusteoria, ikiliikkuja$\}$. Tarkastelemme joukkojen X ja Y alkioiden välistä relaatiota $R = \{$(Newton, painovoimalaki), (Newton, differentiaalilaskenta), (Leibniz, differentiaalilaskenta), (Einstein, suhteellisuusteoria)$\}$. Esitämme tämän relaation *nuolikuviolla*, jossa keskenään relaatiossa olevat alkiot yhdistetään nuolella.



Tällä relaatiolla on yksinkertainen *laki*

$$xRy \Leftrightarrow x \text{ on keksinyt } y\text{:n.}$$

Relaation R määrittelyjoukko $M_R = \{$Newton, Leibniz, Einstein$\}$ ja arvojoukko $A_R = \{$painovoimalaki, differentiaalilaskenta, suhteellisuusteoria$\}$.

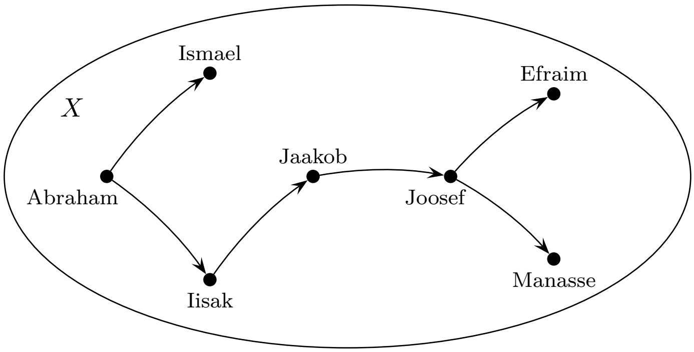
Jos relaation R lähtöjoukko ja maalijoukko ovat kumpikin X, niin sanomme, että R on *joukossa* X määritelty relaatio (tai *joukon* X relaatio).

Esimerkki 59. Joukon X *identtinen relaatio* on $I = \{\, (x, x) \mid x \in X \,\}$. Jokainen alkio on identtisessä relaatiossa itsensä kanssa eikä minkään muun kanssa.

Esimerkki 60. Tarkastelemme joukossa X = {Abraham, Ismael, Iisak, Jaakob, Joosef, Efraim, Manasse} määriteltyä relaatiota (siis joukon $X \times X$ osajoukkoa) R = {(Abraham, Ismael), (Abraham, Iisak), (Iisak, Jaakob), (Jaakob, Joosef), (Joosef, Efraim), (Joosef, Manasse)}, jonka laki on siis

$$xRy \Leftrightarrow x \text{ on } y\text{:n isä.}$$

Havainnollistamme tätä relaatiota *digraafilla* eli *polkukuviolla.*



6 Relaatio koordinaatistossa ja matriisina

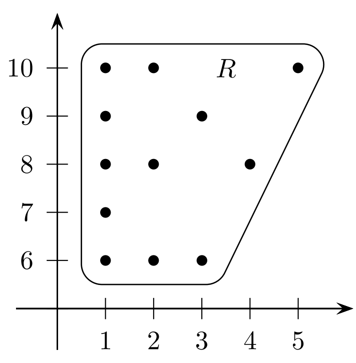
Esimerkki 61. Olkoon $X = \{1, 2, 3, 4, 5\}$, $Y = \{6, 7, 8, 9, 10\}$,

$$R = \{(1,6), (1,7), (1,8), (1,9), (1,10), (2,6), (2,8), (2,10), (3,6), (3,9), (4,8), (5,10)\},$$

joten

$$xRy \Leftrightarrow x \text{ on luvun } y \text{ tekijä.}$$

Esitämme tämän relaation *koordinaatistossa* ja *matriisina*, jonka i. vaakarivin ja k. pystyrivin alkio on 1, jos $x_i R y_k$, ja 0 muulloin. Tässä $x_1 = 1$, $x_2 = 2$, …, $x_5 = 5$, $y_1 = 6$, $y_2 = 7$, …, $y_5 = 10$.

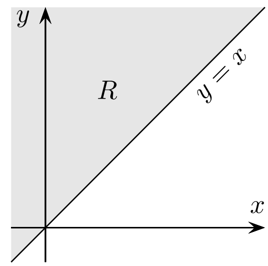


	6	7	8	9	10
1	1	1	1	1	1
2	1	0	1	0	1
3	1	0	0	1	0
4	0	0	1	0	0
5	0	0	0	0	1

Esimerkki 62. Joukossa $\mathbb{R}$ määriteltyä relaatiota

$$xRy \Leftrightarrow x \leq y$$

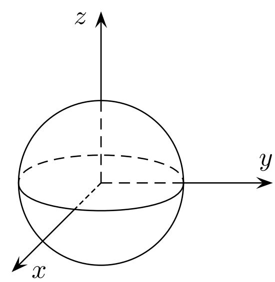
voimme havainnollistaa koordinaatistossa merkitsemällä xy-tasosta sen alueen, jonka pisteiden (x, y) koordinaatit ovat tässä relaatiossa eli toteuttavat ehdon $x \leq y$.



Esimerkki 63. Kolmipaikkaisen relaation

$$R(x, y, z) \Leftrightarrow x^2 + y^2 + z^2 = 1,$$

jonka kaikkien muuttujien määrittelyjoukko on $\mathbb{R}$, geometrinen merkitys xyz-koordinaatistossa on origokeskisen yksikköpallon pinta.



Harjoitustehtäviä

141. Mikä on järjestetyn parin täsmällisen määritelmän mukaan $A \times A$, kun $A = \{a\}$?

142. Osoitettava, ettei järjestettyä kolmikkoa voida määritellä asettamalla $(x, y, z) = \big\{\{x\}, \{x, y\}, \{x, y, z\}\big\}$. Ohje: Vertaa toisiinsa järjestettyjä kolmikoita $(1, 1, 2)$ ja $(1, 2, 1)$.

143. Järjestetty kolmikko määritellään usein asettamalla $(x, y, z) = \big((x, y), z\big)$. **a)** Esitettävä tämä määritelmä käyttämällä joukkoja. **b)** Todettava määritelmän se huono puoli, että nyt kuitenkin $(x, y, z) \neq \big(x, (y, z)\big)$, joten on melko mielivaltaista valita järjestetyistä pareista $\big((x, y), z\big)$ ja $\big(x, (y, z)\big)$ pelkästään jompikumpi tarkoittamaan järjestettyä kolmikkoa (x, y, z).

144. Muodostettava $A \times B$, kun **a)** $A = \{1, 2\}$, $B = \{a, b\}$, **b)** $A = \big\{1, \{2\}\big\}$, $B = \big\{\{a\}, b\big\}$.

145. Todistettava: Jos $A \neq B$ ja $A, B \neq \emptyset$, niin $A \times B \neq B \times A$.

146. Olkoot x, y ja z tiettyjä alkioita. Osoitettava, että $\big(x, (y, z)\big) = \big((x, y), z\big)$ ei ole yleisesti voimassa. Ks. myös teht. 143.

147. Todistettava lauseessa 13 esitetyt tulojoukon ominaisuudet (2) ja (3).

148. Todistettava: $A \times B = \emptyset \Leftrightarrow A = \emptyset \vee B = \emptyset$.

149. Osoitettava, ettei $A \cup (B \times C) = (A \cup B) \times (A \cup C)$ ole yleisesti voimassa. Voiko se itse asiassa olla koskaan voimassa?

150. Todistettava: $A \subseteq B \wedge C \subseteq D \Rightarrow A \times C \subseteq B \times D$.

151. Olkoon X perusjoukko ja $A, B, C, D \in \mathcal{P}(X)$. Todistettava oikeaksi tai vääräksi

a) $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$,

b) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$,

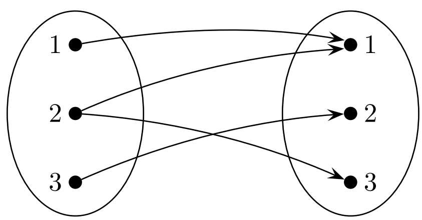
c) $(\overline{A \times B}) = \overline{A} \times \overline{B}$. (vasemmalla puolella perusjoukko on $X \times X$).

152. Olkoon $X = \{1, 2, 3, 4\}$. Muodostettava (luettelemalla alkiot) joukon X relaatio

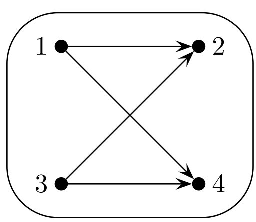
a) $xRy \Leftrightarrow x = y + 1$, **b)** $xRy \Leftrightarrow x \geq 2y$.

153. **a)** Esitettävä joukkojen $X = \{1, 2, 3, 4\}$ ja $Y = \{a, b, c, d\}$ relaatio $R = \{(1, a), (1, b), (3, b), (3, c), (4, c)\}$ i) nuolikuviona, ii) matriisina. **b)** Mikä on tämän relaation i) lähtöjoukko, ii) maalijoukko, iii) määrittelyjoukko, iv) arvojoukko?

154. **a)** Esitettävä polkukuviona seuraavan nuolikuvion relaatio.



b) Esitettävä nuolikuviona seuraavan polkukuvion relaatio.



155. Esitettävä esimerkin **a)** 60 relaatio matriisina, **b)** 61 relaatio nuolikuviona, **c)** 62 relaatio polkukuviona, kun $X = \{1, 2, 3\}$.

156. Esitettävä koordinaatistossa joukon $\mathbb{R}$ relaatio

a) $xRy \Leftrightarrow y \geq x^2$, **b)** $xRy \Leftrightarrow y < -x^2 + 1 \wedge y > x + 1$.

157. Esitettävä koordinaatistossa joukon $\mathbb{R}$ kolmipaikkainen relaatio

a) $R(x, y, z) \Leftrightarrow x + y + z = 1$,

b) $R(x, y, z) \Leftrightarrow x \geq 0 \wedge y \geq 0 \wedge z \geq 0 \wedge x + y + z \leq 1$.

158. Olkoon $X = \{1, 2, 3\}$. Muodostettava joukkojen X ja $\mathcal{P}(X)$ relaatio

$$xRy \Leftrightarrow x \in y.$$

159. Olkoon M tietty miesjoukko ja N tietty naisjoukko. Mikä on joukosta M joukkoon N määritellyn relaation

$$xRy \Leftrightarrow x \text{ on } y\text{:n aviomies}$$

a) lähtö-, **b)** maali-, **c)** määrittely-, **d)** arvojoukko?

160. Kuinka monta relaatiota joukosta X joukkoon Y on olemassa, kun **a)** $X = \{1, 2\}$, $Y = \{1, 2, 3\}$, **b)** $X = \{1, 2, \ldots, m\}$, $Y = \{1, 2, \ldots, n\}$?

4.2 Käänteisrelaatio ja yhdistetty relaatio

1 Käänteisrelaatio

Olkoon R relaatio joukosta X joukkoon Y. Sen *käänteisrelaatio* R^{-1} on joukosta Y joukkoon X määritelty relaatio, jonka laki on

$$yR^{-1}x \Leftrightarrow xRy.$$

Siis

$$R^{-1} = \{\, (y, x) \in Y \times X \mid (x, y) \in R \,\}.$$

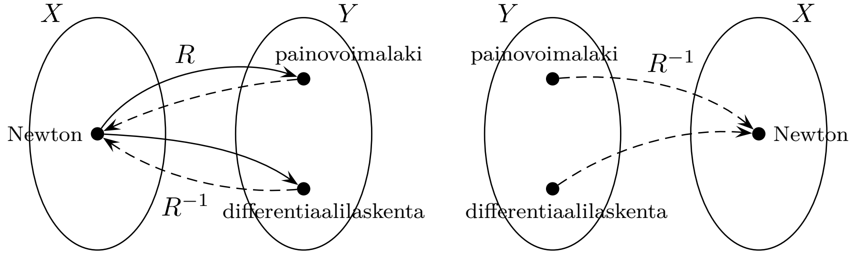
Esimerkki 64. Esimerkin 58 relaation R käänteisrelaatio $R^{-1} = \{$(painovoimalaki, Newton), (differentiaalilaskenta, Newton), (differentiaalilaskenta, Leibniz), (suhteellisuusteoria, Einstein)$\}$. Relaation R^{-1} laki on

$$yR^{-1}x \Leftrightarrow x \text{ on keksinyt } y\text{:n},$$

mutta se on parasta esittää kirjoittamalla ensin y ja sitten x

$$yR^{-1}x \Leftrightarrow y \text{ on } x\text{:n keksimä.}$$

Käänteisrelaation R^{-1} nuolikuvio on muuten sama kuin relaation R, paitsi nuolten kulkusuunnat vaihtuvat. Jos lähtöjoukko halutaan vasemmalle puolelle, niin nuolikuvio on piirrettävä uudestaan vaihtamalla joukkojen paikkaa.



Esimerkki 65. Esimerkin 60 relaation R käänteisrelaation R^{-1} laki on

$$yR^{-1}x \Leftrightarrow x \text{ on } y\text{:n isä}$$

eli

$$yR^{-1}x \Leftrightarrow y \text{ on } x\text{:n poika.}$$

Kirjoittamalla x:n paikalle y:n ja y:n paikalle x:n saamme sen muotoon

$$xR^{-1}y \Leftrightarrow x \text{ on } y\text{:n poika.}$$

Esimerkki 66. Olkoon M tietty miesjoukko ja N tietty naisjoukko. Joukosta M joukkoon N olevan relaation

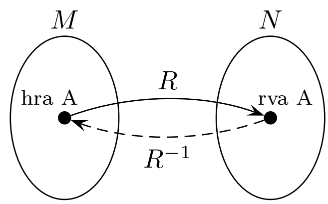
$$xRy \Leftrightarrow x \text{ on } y\text{:n mies}$$

käänteisrelaatio R^{-1} on joukosta N joukkoon M, ja sen laki on

$$yR^{-1}x \Leftrightarrow x \text{ on } y\text{:n mies}$$

eli

$$yR^{-1}x \Leftrightarrow y \text{ on } x\text{:n vaimo.}$$



2 Yhdistetty relaatio

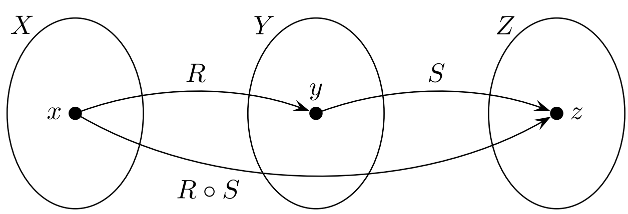
Olkoon R relaatio joukosta X joukkoon Y ja olkoon S relaatio joukosta Y joukkoon Z. Siis R:n maalijoukko on sama kuin S:n lähtöjoukko. Näiden relaatioiden *yhdistetty relaatio* $R \circ S$ on joukosta X joukkoon Z määritelty relaatio, jonka laki on

$$x(R \circ S)z \Leftrightarrow \exists y \in Y : xRy \wedge ySz.$$

Toisin sanoen

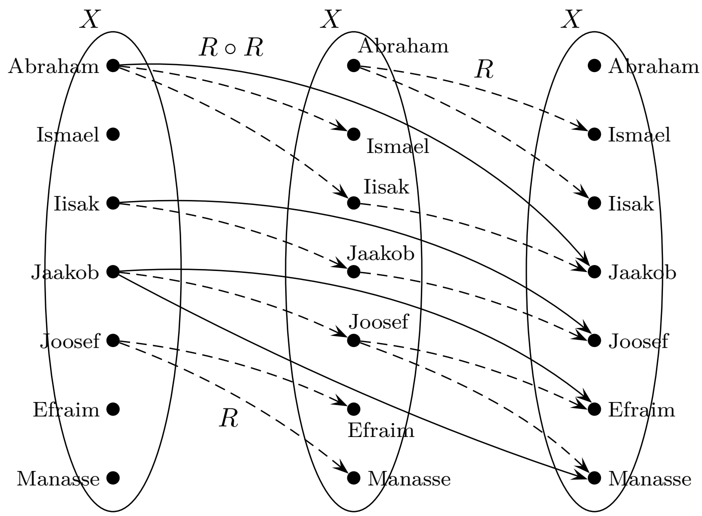
$$R \circ S = \{\, (x, z) \in X \times Z \mid \exists y \in Y : (x, y) \in R \wedge (y, z) \in S \,\}.$$

Alkiot $x \in X$ ja $z \in Z$ ovat siis keskenään relaatiossa $R \circ S$, jos ja vain jos nuolikuviossa päästään x:stä nuolia pitkin z:aan.

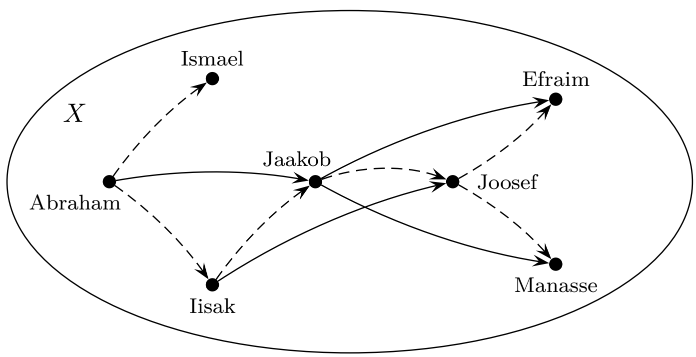


Esimerkki 67. Esimerkkien 60 ja 65 relaation R yhdistetty relaatio itsensä kanssa on $R^2 = R \circ R = \{$(Abraham, Jaakob), (Iisak, Joosef), (Jaakob, Efraim), (Jaakob, Manasse)$\}$. Nyt $X = Y = Z$ ja merkitsemme $R^2 = R \circ R$. Tämän relaation laki on

$$xR^2y \Leftrightarrow x \text{ on } y\text{:n isoisä.}$$



Alkio x on relaatiossa R^2 alkion y kanssa, jos ja vain jos relaation R polkukuviossa x:stä päästään y:hyn kahden nuolen pituisella reitillä.



Esimerkki 68. Olkoot X ja Y tiettyjä naisjoukkoja sekä Z tietty miesjoukko. Määrittelemme joukosta X joukkoon Y relaation

$$x\ddot{A}y \Leftrightarrow x \text{ on } y\text{:n äiti,}$$

jolloin myös

$$x\ddot{A}y \Leftrightarrow y \text{ on } x\text{:n tytär.}$$

Määrittelemme joukosta Y joukkoon Z relaation

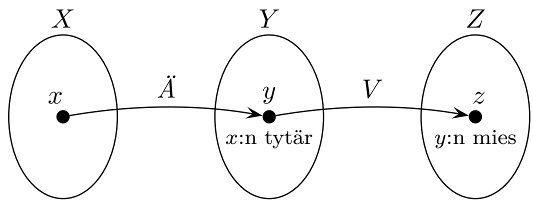
$$yVz \Leftrightarrow y \text{ on } z\text{:n vaimo,}$$

jolloin myös

$$yVz \Leftrightarrow z \text{ on } y\text{:n mies.}$$

Nyt

$$x(\ddot{A} \circ V)z \Leftrightarrow \exists y \in Y : x\ddot{A}y \land yVz \Leftrightarrow x \text{ on } z\text{:n anoppi.}$$

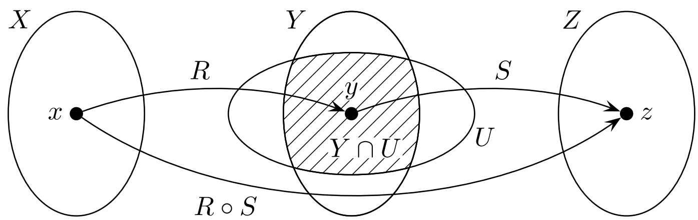


Yleistämme nyt relaatioiden yhdistämisen määritelmän luopumalla R:n maalijoukon ja S:n lähtöjoukon samuudesta. Olkoon R relaatio joukosta X joukkoon Y ja olkoon S relaatio joukosta U joukkoon Z. Menettelemme kuten edellä, mutta meidän on vaadittava, että $y \in Y \cap U$. Saamme

$$x(R \circ S)z \Leftrightarrow \exists y \in Y \cap U \colon xRy \wedge ySz$$

eli

$$R \circ S = \{\, (x, z) \in X \times Z \mid \exists y \in Y \cap U \colon (x, y) \in R \wedge (y, z) \in S \,\}.$$



3 Relaatioiden laskusääntöjä

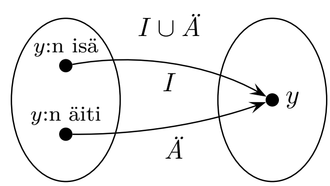
Relaatioille voidaan suorittaa joukko-opin laskutoimituksia.

Esimerkki 69. Tietyssä ihmisjoukossa X määritellään

$$xIy \Leftrightarrow x \text{ on } y\text{:n isä}$$

ja

$$x\ddot{A}y \Leftrightarrow x \text{ on } y\text{:n äiti.}$$



Tällöin

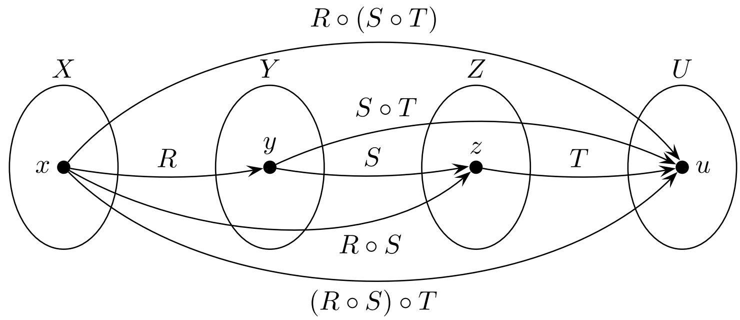
$$x(I \cup \ddot{A})y \Leftrightarrow xIy \vee x\ddot{A}y \Leftrightarrow x \text{ on } y\text{:n vanhempi.}$$

Relaatioiden yhdistäminen $\circ$ ei noudata vaihdantalakia (teht. 166), mutta noudattaa liitäntälakia.

Lause 14. Olkoon R relaatio joukosta X joukkoon Y, S relaatio joukosta Y joukkoon Z ja T relaatio joukosta Z joukkoon U. Tällöin $R \circ (S \circ T) = (R \circ S) \circ T$.

Todistus.

$$
\begin{aligned}
& x\big(R \circ (S \circ T)\big)u \\
\Leftrightarrow\ & \exists y \in Y : xRy \wedge y(S \circ T)u && \text{(yhdistetyn relaation määritelmä)} \\
\Leftrightarrow\ & \exists y \in Y : xRy \wedge (\exists z \in Z : ySz \wedge zTu) && \text{(yhdistetyn relaation määritelmä)} \\
\Leftrightarrow\ & \exists y \in Y : \exists z \in Z : xRy \wedge (ySz \wedge zTu) && \text{($\exists z \in Z$ siirr. xRy:n vas. puolelle)} \\
\Leftrightarrow\ & \exists z \in Z : \exists y \in Y : (xRy \wedge ySz) \wedge zTu && \text{($\exists$:n järj. vaihto, liitäntälaki)} \\
\Leftrightarrow\ & \exists z \in Z : x(R \circ S)z \wedge zTu && \text{(yhdistetyn relaation määritelmä)} \\
\Leftrightarrow\ & x\big((R \circ S) \circ T\big)u && \text{(yhdistetyn relaation määritelmä).}
\end{aligned}
$$



Liitäntälain perusteella voimme jättää sulut pois ja siis kirjoittaa $R \circ S \circ T$. Vastaavasti voimme menetellä, kun yhdistettäviä relaatioita on useampia.

Jos R on joukossa X määritelty relaatio, niin merkitsemme $R^n = R \circ \cdots \circ R$ (n kpl). Ilmeisesti xR^ny, jos ja vain jos relaation R polkukuviossa alkiosta x päästään alkioon y reitillä, jossa on n nuolta. Lisäksi on luonnollista määritellä $R^0 = I$ (joukon X identtinen relaatio) ja $R^{-n} = (R^{-1})^n$.

Relaation potenssimerkintä on valitettavasti ristiriidassa tulojoukon potenssimerkinnän $A^n = A \times \cdots \times A$ (n kpl) kanssa. Jos siitä aiheutuu väärinkäsityksen vaara, niin relaation potenssia voidaan merkitä vaikkapa $R^{(n)}$.

Lause 15. Olkoot R ja S joukossa X määriteltyjä relaatioita. Tällöin

(1) $(R^{-1})^{-1} = R$,

(2) $R \subseteq S \Rightarrow R^{-1} \subseteq S^{-1}$,

(3) $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$,

(4) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$,

(5) $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

Todistamme kohdan (2) ja jätämme muut harjoitustehtäviksi (teht. 167–168). Oletamme, että $R \subseteq S$, ja osoitamme, että jokainen relaation R^{-1}

alkio (siis järjestetty pari) kuuluu myös relaatioon S^{-1}. Olkoot $x, y \in X$ sellaisia, että $(x, y) \in R^{-1}$. Tällöin käänteisrelaation määritelmän perusteella $(y, x) \in R$. Koska $R \subseteq S$, niin $(y, x) \in S$, joten käänteisrelaation määritelmän mukaan $(x, y) \in S^{-1}$. Siis jokainen joukon R^{-1} alkio on myös joukon S^{-1} alkio, joten $R^{-1} \subseteq S^{-1}$.

*4 Relaatiot ja Boolen matriisit

Lukijalta edellytetään matriisialgebran perustiedot, ks. esim. [15].

Määrittelemme disjunktion totuustaulukon (s. 8) perusteella lukujen 0 ja 1 *Boolen yhteenlaskun*

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1 \oplus 0 = 1 \oplus 1 = 1$$

ja konjunktion totuustaulukon perusteella niiden *Boolen kertolaskun*

$$0 \otimes 0 = 0 \otimes 1 = 1 \otimes 0 = 0, \quad 1 \otimes 1 = 1.$$

Lauselogiikan säännöistä (s. 15) seuraa, että Boolen yhteenlasku ja kertolasku noudattavat tavanomaisia laskusääntöjä.

Olkoon R relaatio äärellisestä joukosta X äärelliseen joukkoon Y. Olkoon X:n alkioiden lukumäärä m ja Y:n n. Relaation R matriisi M_R on $m \times n$ -matriisi, jonka alkiot ovat nollia tai ykkösiä. Kutsumme tällaista matriisia *Boolen matriisiksi.*

Olkoot $A = (a_{ik})$ ja $B = (b_{ik})$ Boolen $m \times n$ -matriiseja. Määrittelemme niiden Boolen yhteenlaskun kuten matriisien tavallisen yhteenlaskun, mutta käytämme Boolen summaa. Siis $A \oplus B$ on sellainen $m \times n$ -matriisi $C = (c_{ik})$, että

$$c_{ik} = a_{ik} \oplus b_{ik}$$

kaikilla $i \in \{1, 2, \ldots, m\}$, $k \in \{1, 2, \ldots, n\}$.

Vastaavasti määrittelemme näiden matriisien *alkioittaisen* Boolen kertolaskun. Siis $A \otimes B$ on sellainen $m \times n$ -matriisi $C = (c_{ik})$, että

$$c_{ik} = a_{ik} \otimes b_{ik}.$$

(Matriisien tavanomaista *alkioittaista* kertolaskua ei käsitellä matriisialgebran alkeiskurssilla.)

Olkoon nyt $A = (a_{ik})$ Boolen $m \times n$ -matriisi ja $B = (b_{ik})$ Boolen $n \times s$ -matriisi. Määrittelemme niiden Boolen kertolaskun $\odot$ kuten matriisien tavanomaisen kertolaskun, mutta käytämme Boolen summaa ja tuloa. Siis $A \odot B$ on sellainen $m \times s$ -matriisi $C = (c_{ik})$, että

$$c_{ik} = (a_{i1} \otimes b_{1k}) \oplus (a_{i2} \otimes b_{2k}) \oplus \cdots \oplus (a_{in} \otimes b_{nk})$$

kaikilla $i \in \{1, 2, \ldots, m\}$, $k \in \{1, 2, \ldots, s\}$.

Esimerkki 70. Olkoon

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

Tällöin

$$A \oplus B = \begin{pmatrix} 1 \oplus 0 & 1 \oplus 1 & 0 \oplus 0 \\ 0 \oplus 0 & 1 \oplus 0 & 0 \oplus 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix},$$

$$A \otimes B = \begin{pmatrix} 1 \otimes 0 & 1 \otimes 1 & 0 \otimes 0 \\ 0 \otimes 0 & 1 \otimes 0 & 0 \otimes 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\begin{aligned} A \odot C &= \begin{pmatrix} (1 \otimes 1) \oplus (1 \otimes 0) \oplus (0 \otimes 0) & (1 \otimes 1) \oplus (1 \otimes 1) \oplus (0 \otimes 1) \\ (0 \otimes 1) \oplus (1 \otimes 0) \oplus (0 \otimes 0) & (0 \otimes 1) \oplus (1 \otimes 1) \oplus (0 \otimes 1) \end{pmatrix} \\ &= \begin{pmatrix} 1 \oplus 0 \oplus 0 & 1 \oplus 1 \oplus 0 \\ 0 \oplus 0 \oplus 0 & 0 \oplus 1 \oplus 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Relaatioiden laskutoimitukset ja niiden matriisien Boolen laskutoimitukset vastaavat toisiaan.

Lause 16. Olkoot R ja S relaatioita joukosta X joukkoon Y sekä olkoon T relaatio joukosta Y joukkoon Z. Jos X, Y ja Z ovat äärelliset, niin

(1) $M_{R \cup S} = M_R \oplus M_S$,

(2) $M_{R \cap S} = M_R \otimes M_S$,

(3) $M_{R \circ T} = M_R \odot M_T$.

Jätämme todistuksen harjoitustehtäväksi (teht. 176ab, 177).

Käänteisrelaation matriisi ei ole alkuperäisen relaation matriisin käänteismatriisi (kuten nimen perusteella voisi luulla), vaan transpoosi.

Lause 17. Olkoon R äärellisten joukkojen välinen relaatio. Tällöin

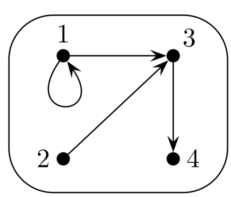
$$M_{R^{-1}} = M_R^{\mathsf{T}}.$$

Todistus. Teht. 176c.

Harjoitustehtäviä

161. Joukossa $X = \{a, b, c, d\}$ määritellään relaatiot $R = \{(a, a), (a, b), (b, d)\}$ ja $S = \{(a, d), (b, c), (b, d), (c, b)\}$. Mitä on **a)** $R \circ S$, **b)** R^{-1}, **c)** S^2?

162. Olkoon R viereisen polkukuvion relaatio. Piirrettävä relaation **a)** R^{-1}, **b)** R^2, **c)** $R \circ R^{-1}$ polkukuvio.



163. Tietyssä ihmisjoukossa määritellään relaatio $xIy \Leftrightarrow x$ on y:n isä. Vastaavasti määritellään relaatiot $Ä =$ 'äiti' ja $V =$ 'vaimo'. Mikä on relaation **a)** $I^{-1} \cup Ä^{-1}$, **b)** $P = V^{-1} \cup V$, **c)** $V \circ (I \cup Ä)$, **d)** $P \circ V$ laki?

164. Jatkoa. Määritellään myös relaatiot $B =$ 'veli' ja $S =$ 'sisar'. Muodostettava relaatio **a)** 'serkku', **b)** 'eno', **c)** 'lanko'.

165. Olkoot R ja S relaatioita joukossa X. Todistettava oikeaksi tai vääräksi: **a)** Jos $R^{-1} = S^{-1}$, niin $R = S$. **b)** Jos $R^2 = S^2$, niin $R = S$.

166. Osoitettava, ettei relaatioiden yhdistäminen noudata vaihdantalakia.

167. Olkoon R relaatio joukosta X joukkoon Y ja olkoon S relaatio joukosta Y joukkoon Z. Todistettava

a) $(R^{-1})^{-1} = R$, **b)** $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

168. Olkoot R ja S relaatioita joukosta X joukkoon Y. Todistettava

a) $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$, **b)** $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$.

169. Noudattaako relaation potenssi $R^n = R \circ \cdots \circ R$ (n kpl), $R^0 = I$, $R^{-n} = (R^{-1})^n$ tavallisen potenssin laskusääntöjä?

170. Olkoot R ja S relaatioita joukossa X. Todistettava: Jos $R \subseteq S$, niin $R^n \subseteq S^n$ kaikilla $n \in \mathbb{Z}$.

171. Olkoon X äärellinen joukko ja n sen alkioiden lukumäärä sekä olkoon R relaatio joukossa X. Todistettava: On olemassa sellaiset $p, q \in \mathbb{N}$, että $p, q \leq 2^{n^2}$, $p \neq q$ ja $R^p = R^q$. Ohje: Tutki joukon $X \times X$ osajoukkojen lukumäärää ja palauta mieleesi relaation määritelmä.

172. Olkoon $X = \{1, 2, \ldots, n\}$, $n \geq 3$. Esitettävä sellainen relaatio R joukossa X, että R, R^2, R^3, ..., R^{n+1} ovat kaikki eri relaatioita.

173. Olkoot R_1 relaatio joukosta X joukkoon Y, R_2 ja R_3 relaatioita joukosta Y joukkoon Z sekä R_4 relaatio joukosta Z joukkoon U. Todistettava toinen väitteistä

a) $R_1 \circ (R_2 \cup R_3) = (R_1 \circ R_2) \cup (R_1 \circ R_3)$,

b) $(R_2 \cup R_3) \circ R_4 = (R_2 \circ R_4) \cup (R_3 \circ R_4)$.

174. Jatkoa. Todistettava toinen väitteistä

a) $R_1 \circ (R_2 \cap R_3) \subseteq (R_1 \circ R_2) \cap (R_1 \circ R_3)$,

b) $(R_2 \cap R_3) \circ R_4 \subseteq (R_2 \circ R_4) \cap (R_3 \circ R_4)$.

Näytettävä esimerkillä, että osajoukot voivat olla aitoja.

175. Joukossa $X = \{1, 2\}$ määritellään relaatiot $R = \{(1,1), (1,2), (2,1)\}$ ja $S = \{(1,2), (2,2)\}$. **a)** Muodostettava relaatiot $R \cup S$, $R \cap S$ ja $R \circ S$. **b)** Laskettava matriisit $M_R \oplus M_S$, $M_R \otimes M_S$ ja $M_R \odot M_S$ sekä todettava, että saadaan a-kohdan relaatioiden matriisit.

176. Olkoot R ja S relaatioita äärellisestä joukosta X äärelliseen joukkoon Y. Todistettava

a) $M_{R\cup S} = M_R \oplus M_S$, **b)** $M_{R\cap S} = M_R \otimes M_S$, **c)** $M_{R^{-1}} = M_R^{\mathsf{T}}$.

177. Olkoon R relaatio äärellisestä joukosta X äärelliseen joukkoon Y ja S relaatio joukosta Y äärelliseen joukkoon Z. Todistettava, että $M_{R\circ S} = M_R \odot M_S$.

178. Olkoon R relaatio äärellisestä joukosta X äärelliseen joukkoon Y. Miten saadaan $M_{\overline{R}}$, kun M_R tunnetaan?

179. Olkoon R relaatio äärellisessä joukossa X. Kun M_R tunnetaan, niin miten saadaan M_{R^n} tapauksessa **a)** $n \in \mathbb{Z}_+$, **b)** $n = 0$, **c)** $n \in \mathbb{Z}_-$?

180. Olkoot R ja S relaatioita äärellisestä joukosta X äärelliseen joukkoon Y. Mikä matriisien M_R ja M_S välinen ehto on yhtäpitävä sen kanssa, että $R \subseteq S$?

4.3 Relaation ominaisuuksia. ∗Sulkeumat

1 Relaation ominaisuuksia

Joukossa X määritelty relaatio R on

(r) *refleksiivinen*, jos xRx kaikilla $x \in X$,

(ir) *irrefleksiivinen*, jos $x\not{R}x$ kaikilla $x \in X$,

(s) *symmetrinen*, jos $xRy \Rightarrow yRx$,

(as) *antisymmetrinen*, jos $xRy \wedge yRx \Rightarrow x = y$,

(t) *transitiivinen*, jos $xRy \wedge yRz \Rightarrow xRz$,

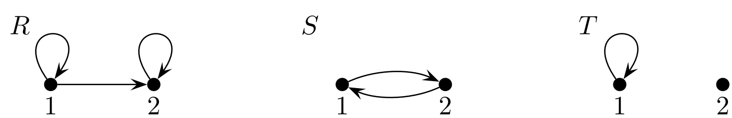
(v) *vertailullinen*, jos $xRy \vee yRx$ kaikilla $x, y \in X$.

Tarkastelemme näitä ominaisuuksia lähemmin.

(r) Jokainen alkio on relaatiossa itsensä kanssa, jolloin polkukuviossa jokaisesta alkiosta menee nuoli itseensä.

(ir) Mikään alkio ei ole relaatiossa itsensä kanssa. Polkukuviossa mistään alkiosta ei mene nuolta itseensä.

Esimerkki 71. Olkoon $X = \{1, 2\}$. Relaatio $R = \{(1, 1), (1, 2), (2, 2)\}$ on refleksiivinen. Relaatio $S = \{(1, 2), (2, 1)\}$ on irrefleksiivinen. Relaatio $T = \{(1, 1)\}$ ei ole refleksiivinen eikä irrefleksiivinen.



(s) Jos relaatio on voimassa ”toiseen suuntaan”, niin se on voimassa ”toiseenkin suuntaan”. Jos polkukuviossa on nuoli jostakin pisteestä toiseen, niin nuoli on myös vastakkaiseen suuntaan.

(as) Eri alkiot eivät voi olla relaatiossa ”kumpaankin suuntaan”. Jos polkukuviossa on nuoli jostakin pisteestä toiseen, niin nuolta ei ole vastakkaiseen suuntaan.

Esimerkki 71, jatkoa. Relaatio R on antisymmetrinen, mutta ei ole symmetrinen. Relaatio S on symmetrinen, mutta ei ole antisymmetrinen. Relaatio T on symmetrinen ja antisymmetrinen. Nimittäin implikaatio

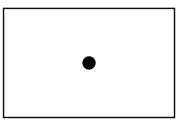
$$xTy \Rightarrow yTx$$

on tosi, koska oletuksesta xTy seuraa, että $x = y = 1$, jolloin myös yTx. Samoin implikaatio

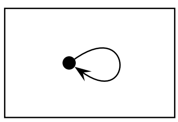
$$xTy \wedge yTx \Rightarrow x = y$$

on tosi, koska oletuksesta taas seuraa, että $x = y$.

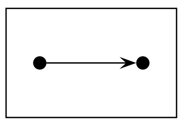
Polkukuviosta on helppo nähdä, milloin (r), (ir), (s) tai (as) *ei ole* voimassa.



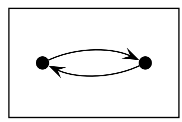
Kaataa (r):n



Kaataa (ir):n



Kaataa (s):n



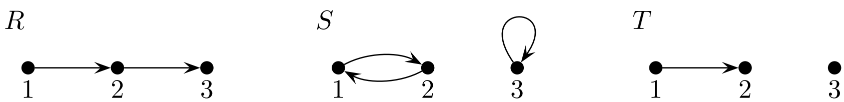
Kaataa (as):n

(t) Jos nuoli menee polkukuviossa x:stä y:hyn ja y:stä z:aan, niin se menee myös x:stä z:aan. Jos siis jostakin pisteestä päästään toiseen kahden nuolen pituisella reitillä, niin sinne päästään myös yhden nuolen reitillä.

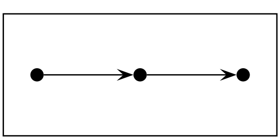
Esimerkki 72. Olkoon $X = \{1, 2, 3\}$. Relaatio $R = \{(1, 2), (2, 3)\}$ ei ole transitiivinen ($(1, 2) \in R$ ja $(2, 3) \in R$, mutta $(1, 3) \notin R$). Relaatio $S = \{(1, 2), (2, 1), (3, 3)\}$ ei ole transitiivinen ($(1, 2) \in S$ ja $(2, 1) \in S$, mutta $(1, 1) \notin S$). Relaatio $T = \{(1, 2)\}$ on transitiivinen. Nimittäin implikaation

$$xTy \wedge yTz \Rightarrow xTz$$

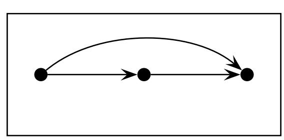
edellinen jäsen on aina epätosi, joten implikaatio on tosi.



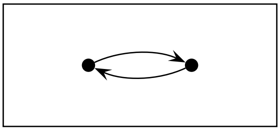
Polkukuviosta on helppo nähdä, milloin (t) *ei ole* voimassa.



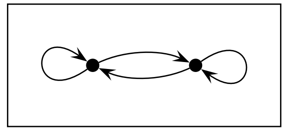
Kaataa (t):n



Vaadittava lisäys



Kaataa (t):n



Vaadittava lisäys

(v) Jätämme vertailullisuuden havainnollistamisen harjoitustehtäväksi (teht. 185).

Esimerkki 73. Olkoon $R = \{(1,1), (1,3), (2,2), (2,3), (3,1), (3,3), (4,3), (4,4)\}$ joukossa $X = \{1,2,3,4\}$ määritelty relaatio. Se on refleksiivinen, mutta ei irrefleksiivinen, ei symmetrinen ($(4,3) \in R$, mutta $(3,4) \notin R$), ei antisymmetrinen ($(1,3), (3,1) \in R$), ei transitiivinen ($(2,3), (3,1) \in R$, mutta $(2,1) \notin R$) eikä vertailullinen ($(1,2) \notin R$, $(2,1) \notin R$).

Esimerkki 74. Joukossa $\mathbb{Z}_+$ määritelty relaatio

$$xRy \Leftrightarrow x \text{ on luvun } y \text{ tekijä}$$

on refleksiivinen (luku on aina itsensä tekijä), antisymmetrinen (jos x on y:n tekijä ja y on x:n tekijä, niin $x = y$) ja transitiivinen (jos x on y:n tekijä ja y on z:n tekijä, niin x on z:n tekijä). Sen sijaan R ei ole irrefleksiivinen (koska se on refleksiivinen), ei symmetrinen (esim. 3 on luvun 9 tekijä, mutta 9 ei ole luvun 3 tekijä) eikä vertailullinen (esim. luvuista 5 ja 7 kumpikaan ei ole toisensa tekijä).

Esimerkki 75. Tyhjä relaatio $\emptyset$ on irrefleksiivinen, symmetrinen, antisymmetrinen ja transitiivinen, mutta ei refleksiivinen eikä vertailullinen. (Relaation määritelmän mukaan perusjoukko $X \neq \emptyset$.)

Esimerkki 76. ”Täysi” relaatio $X \times X$ on refleksiivinen, symmetrinen, transitiivinen ja vertailullinen, mutta ei irrefleksiivinen. Se on antisymmetrinen, jos joukossa X on vain yksi alkio, mutta ei muulloin.

2 Ominaisuuksia koskevia lauseita

Lause 18. Joukossa X määritelty relaatio R on

(1) refleksiivinen, jos ja vain jos $I \subseteq R$,

(2) irrefleksiivinen, jos ja vain jos $R \cap I = \emptyset$,

(3) symmetrinen, jos ja vain jos $R^{-1} = R$,

(4) antisymmetrinen, jos ja vain jos $R \cap R^{-1} \subseteq I$,

(5) transitiivinen, jos ja vain jos $R \circ R \subseteq R$,

(6) vertailullinen, jos ja vain jos $R \cup R^{-1} = X \times X$.

Todistamme kohdan (4) ja jätämme muut harjoitustehtäviksi (teht. 187–189).

Vain jos. *Ol.* R on antisymmetrinen. *Väit.* $R \cap R^{-1} \subseteq I$. *Tod.* Olkoon $(x, y) \in R \cap R^{-1}$. Siis $(x, y) \in R$ ja $(x, y) \in R^{-1}$, jolloin käänteisrelaation määritelmän perusteella $(y, x) \in R$. Antisymmetrisyyden perusteella tästä seuraa $x = y$, joten $(x, y) \in I$. Siis $R \cap R^{-1} \subseteq I$.

Jos. *Ol.* $R \cap R^{-1} \subseteq I$. *Väit.* R on antisymmetrinen. *Tod.* Olkoon $(x, y) \in R$ ja $(y, x) \in R$. Käänteisrelaation määritelmän perusteella $(x, y) \in R^{-1}$. Siis $(x, y) \in R \cap R^{-1}$, joten oletuksen mukaan $(x, y) \in I$ eli $x = y$. Siis R on antisymmetrinen.

Lause 19. Olkoon R joukossa X määritelty relaatio. Tällöin

(1) $R \cup I$ on refleksiivinen,

(2) $R \cup R^{-1}$ on symmetrinen,

(3) $\bigcup_{k=1}^{\infty} R^k$ on transitiivinen.

Todistus. Kohta (1) on edellisen lauseen kohdan (1) seuraus, sillä $I \subseteq R \cup I$. Kohta (2) seuraa edellisen lauseen kohdasta (3), sillä lauseiden 15(3) ja 15(1) (s. 79) perusteella

$$(R \cup R^{-1})^{-1} = R^{-1} \cup (R^{-1})^{-1} = R^{-1} \cup R = R \cup R^{-1}.$$

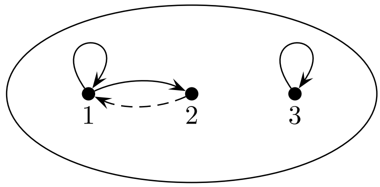
Kohdan (3) todistamiseksi oletamme, että $(x, y) \in \bigcup_{k=1}^{\infty} R^k$ ja $(y, z) \in \bigcup_{k=1}^{\infty} R^k$. Tällöin $(x, y) \in R^m$ ja $(y, z) \in R^n$ joillakin $m, n \in \mathbb{Z}_+$. Yhdistetyn relaation määritelmän perusteella $(x, z) \in R^m \circ R^n$. Koska $R^m \circ R^n = R^{m+n}$ (s. 82, teht. 169), niin $(x, z) \in \bigcup_{k=1}^{\infty} R^k$. Siis $\bigcup_{k=1}^{\infty} R^k$ on transitiivinen.

∗3 Sulkeumat

Jos relaatiolla R ei ole haluttua ominaisuutta, voimme joissakin tapauksissa täydentää (uusia alkioita lisäämällä) siitä relaation R', jolla on tämä ominaisuus. Voimme aina täydentää R:n refleksiiviseksi, symmetriseksi, transitiiviseksi tai vertailulliseksi. Sen sijaan emme saa relaatiosta irrefleksiivistä tai antisymmetristä täydentämällä, vaan päinvastoin poistamalla alkioita.

Esimerkki 77. Täydennettävä joukossa $X = \{1, 2, 3\}$ määritelty relaatio $R = \{(1, 1), (1, 2), (3, 3)\}$ symmetriseksi.

Meidän on välttämättä lisättävä R:ään alkio $(2, 1)$, jolloin saamme symmetrisen relaation $R' = \{(1, 1), (1, 2), (2, 1), (3, 3)\}$. Voimme lisätä muitakin alkioita, esimerkiksi alkion $(2, 2)$. Jos lisäämme esimerkiksi alkion $(2, 3)$, niin meidän on lisättävä myös $(3, 2)$.



Tähän tehtävään on siis useita ratkaisuja, mutta jos kysytään ”pienintä” R:n sisältävää symmetristä relaatiota, niin ratkaisu on yksikäsitteinen, nimittäin R'.

Olkoon R relaatio joukossa X. Jos R' on sellainen relaatio joukossa X, että

(1) R' on refleksiivinen (symmetrinen, transitiivinen),

(2) $R \subseteq R'$,

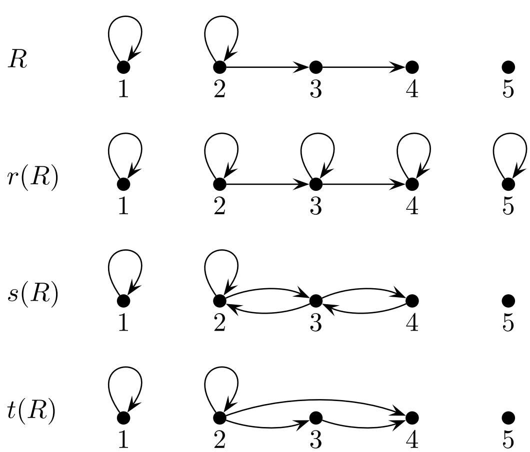
(3) $R' \subseteq S$ aina, kun S on refleksiivinen (symmetrinen, transitiivinen) ja $R \subseteq S$,

niin relaatio R' on relaation R *refleksiivinen* (*symmetrinen*, *transitiivinen*) *sulkeuma*. Käytämme refleksiiviselle sulkeumalle merkintää $r(R)$, symmetriselle $s(R)$ ja transitiiviselle $t(R)$.

Huomaamme helposti (teht. 192), että R on refleksiivinen (symmetrinen, transitiivinen) täsmälleen silloin, kun $r(R) = R$ ($s(R) = R$, $t(R) = R$). Huomaamme myös helposti (teht. 193), ettei näitä sulkeumia voi olla enempää kuin yksi.

Esimerkki 78. Olkoon $X = \{1, 2, 3, 4, 5\}$ ja $R = \{(1, 1), (2, 2), (2, 3), (3, 4)\}$. Tällöin

$$\begin{aligned} r(R) &= \{(1,1),(2,2),(2,3),(3,3),(3,4),(4,4),(5,5)\}, \\ s(R) &= \{(1,1),(2,2),(2,3),(3,2),(3,4),(4,3)\}, \\ t(R) &= \{(1,1),(2,2),(2,3),(2,4),(3,4)\}. \end{aligned}$$



Esimerkki 79. Olkoon $X = \mathbb{Z}$ ja $R = \{\,(x, y) \mid x < y\,\}$. Tällöin

$$r(R) = \{\,(x, y) \mid x \leq y\,\}, \quad s(R) = \{\,(x, y) \mid x \neq y\,\}, \quad t(R) = R.$$

Olkoon R joukossa X määritelty relaatio. Seuraavat lauseet osoittavat, että $r(R)$, $s(R)$ ja $t(R)$ ovat aina olemassa.

Lause 20. $r(R) = R \cup I$.

Todistus. Osoitamme, että $R \cup I$ toteuttaa $r(R)$:n määritelmän ehdot (1)–(3). (1) Lauseen 19(1) perusteella $R \cup I$ on refleksiivinen. (2) Selvästi $R \subseteq R \cup I$. (3) Olkoon S sellainen refleksiivinen relaatio, että $R \subseteq S$. Lauseen 18(1) mukaan $I \subseteq S$, joten myös $R \cup I \subseteq S$.

Lause 21. $s(R) = R \cup R^{-1}$.

Todistus. (1) Lauseen 19(2) perusteella $R \cup R^{-1}$ on symmetrinen. (2) Selvästi $R \subseteq R \cup R^{-1}$. (3) Olkoon S sellainen symmetrinen relaatio, että $R \subseteq S$. Lauseen 15(2) (s. 79) mukaan $R^{-1} \subseteq S^{-1}$, joten, koska $S^{-1} = S$ (lause 18(3)), on $R^{-1} \subseteq S$. Siis myös $R \cup R^{-1} \subseteq S$.

Lause 22. $t(R) = \displaystyle\bigcup_{k=1}^{\infty} R^k$.

Todistus. (1) Lauseen 19(3) perusteella $\bigcup_{k=1}^{\infty} R^k$ on transitiivinen. (2) Selvästi $R \subseteq \bigcup_{k=1}^{\infty} R^k$. (3) Olkoon S sellainen transitiivinen relaatio, että $R \subseteq S$. Olkoon $k \in \mathbb{Z}_+$, jolloin $R^k \subseteq S^k$ (teht. 170). Koska lisäksi $S^k \subseteq S$ (teht. 189), niin $R^k \subseteq S$, joten myös $\bigcup_{k=1}^{\infty} R^k \subseteq S$.

Jos X on äärellinen, niin transitiivisen sulkeuman muodostamiseksi riittää tutkia äärellistä määrää R:n potensseja.

Lause 23. Jos R on relaatio n-alkioisessa joukossa, niin $t(R) = \bigcup_{k=1}^{n} R^k$.

Todistus. Teht. 199.

Esimerkki 80. Olkoon $X = \{a, b, c, d\}$ ja $R = \{(a, a), (b, c), (c, d)\}$. Tällöin

$$\begin{aligned} r(R) &= R \cup I = R \cup \{(a, a), (b, b), (c, c), (d, d)\} \\ &= \{(a, a), (b, b), (b, c), (c, c), (c, d), (d, d)\}, \end{aligned}$$

$$
\begin{aligned}
s(R) &= R \cup R^{-1} = R \cup \{(a,a),(c,b),(d,c)\} \\
&= \{(a,a),(b,c),(c,b),(c,d),(d,c)\}, \\
t(R) &= R \cup R^2 \cup R^3 \cup R^4 = R \cup \{(a,a),(b,d)\} \cup \{(a,a)\} \cup \{(a,a)\} \\
&= \{(a,a),(b,c),(b,d),(c,d)\}.
\end{aligned}
$$

Esimerkki 81. Olkoon $X = \mathbb{R}$ ja $R = \{\,(x,y) \mid y = x+1\,\}$. Tällöin

$$
\begin{aligned}
r(R) &= R \cup I = R \cup \{\,(x,y) \mid y = x\,\} = \{\,(x,y) \mid y = x+1 \vee y = x\,\}, \\
s(R) &= R \cup R^{-1} = R \cup \{\,(x,y) \mid y = x-1\,\} \\
&= \{\,(x,y) \mid y = x+1 \vee y = x-1\,\}, \\
t(R) &= \bigcup_{k=1}^{\infty} R^k = \bigcup_{k=1}^{\infty} \{\,(x,y) \mid y = x+k\,\} \\
&= \{\,(x,y) \mid \exists k \in \mathbb{Z}_+ : y = x+k\,\}.
\end{aligned}
$$

Harjoitustehtäviä

181. Onko joukossa $\mathbb{Z}$ määritelty relaatio R refleksiivinen, irrefleksiivinen, symmetrinen, antisymmetrinen, transitiivinen tai vertailullinen, kun relaation R laki on **a)** $x = y$, **b)** $x \neq y$, **c)** $x < y$, **d)** $x \leq y$?

182. Kuten edellä, mutta laki on **a)** $xy \geq 1$, **b)** $x = y+1 \vee x = y-1$, **c)** $x = y^2$, **d)** $x \geq y^2$.

183. Muodostettava (mikäli mahdollista) joukon $X = \{a,b,c,d\}$ sellainen relaatio, joka on

a) ei-refleksiivinen, symmetrinen ja transitiivinen,

b) refleksiivinen, ei-symmetrinen ja transitiivinen,

c) refleksiivinen, symmetrinen ja ei-transitiivinen.

184. Muodostettava (mikäli mahdollista) joukon $X = \{1,2,3\}$ sellainen relaatio, joka on

a) symmetrinen ja antisymmetrinen,

b) symmetrinen ja ei-antisymmetrinen,

c) ei-symmetrinen ja antisymmetrinen,

d) ei-symmetrinen ja ei-antisymmetrinen.

185. **a)** Havainnollistettava vertailullista relaatiota. **b)** Osoitettava, että vertailullinen relaatio on refleksiivinen. **c)** Millainen polkukuvion ominaisuus kaataa vertailullisuuden?

186. Joukossa X määritelty relaatio on *asymmetrinen*, jos $xRy \Rightarrow y \not R x$. Mitkä tehtävien 181 ja 182 relaatioista ovat asymmetrisiä?

187. Todistettava, että joukossa X määritelty relaatio R on

a) refleksiivinen, jos ja vain jos $I \subseteq R$,

b) irrefleksiivinen, jos ja vain jos $R \cap I = \emptyset$.

188. Jatkoa. Todistettava, että R on

a) symmetrinen, jos ja vain jos $R^{-1} = R$,

b) vertailullinen, jos ja vain jos $R \cup R^{-1} = X \times X$.

189. Jatkoa. Osoitettava, että seuraavat ehdot ovat yhtäpitäviä.

(1) R on transitiivinen,

(2) $R \circ R \subseteq R$,

(3) $R^n \subseteq R$ kaikilla $n \in \mathbb{Z}_+$.

190. Olkoon R relaatio joukossa X. **a)** Todistettava: Jos R on refleksiivinen ja transitiivinen, niin $R^2 = R$. **b)** Onko käänteinen väite tosi?

191. Olkoon $R = \{(0,1),(1,1),(1,2),(2,0),(2,2),(3,0)\}$ joukossa $X = \{0,1,2,3\}$ määritelty relaatio. Määritettävä $r(R)$, $s(R)$ ja $t(R)$.

192. Olkoon R relaatio joukossa X. Todistettava: Jos ja vain jos R on refleksiivinen (symmetrinen, transitiivinen), niin $r(R) = R$ ($s(R) = R$, $t(R) = R$).

193. Osoitettava, että tietyn relaation refleksiivisen (symmetrisen, transitiivisen) sulkeuman ehtoja ei voi toteuttaa useampi kuin yksi relaatio.

194. Miksi ei voida määritellä relaation vertailullista sulkeumaa?

195. Olkoon R relaatio joukossa X. Todistettava, että $r(R)$ ($s(R)$, $t(R)$) on kaikkien niiden joukossa X määriteltyjen refleksiivisten (symmetristen, transitiivisten) relaatioiden leikkaus, jotka sisältävät relaation R.

196. Onko yleisesti

a) $r(R \cup S) = r(R) \cup r(S)$, **b)** $s(R \cup S) = s(R) \cup s(S)$,

c) $t(R \cup S) = t(R) \cup t(S)$?

Ellei, niin onko toisen puolen joukko toisen osajoukko?

197. Olkoon $X = \{a,b,c,d\}$, $R = \{(a,a),(b,c),(c,d)\}$. Muodostettava **a)** $rs(R) = r\big(s(R)\big)$, **b)** $rt(R)$, **c)** $st(R)$, **d)** $ts(R)$.

198. Todistettava, että yleisesti

a) $rs(R) = sr(R)$, **b)** $rt(R) = tr(R)$, **c)** $st(R) \subseteq ts(R)$.

Näytettävä, että c-kohdassa osajoukko voi olla aito.

199. Todistettava: Jos R on relaatio n-alkioisessa joukossa X, niin $t(R) = \bigcup_{k=1}^{n} R^k$. Ohje: Osoita, että jos joukon X kahden alkion välissä on polku (eli peräkkäisten nuolten reitti), niin niiden välissä on sellainen polku, jonka pituus (eli nuolten lukumäärä) on korkeintaan $n-1$.

200. Esitettävä (mikäli mahdollista) jokin joukossa $\{1, 2, 3, 4, 5\}$ määritelty relaatio R, jolle $t(R) \neq R \cup R^2 \cup R^3 \cup R^4$.

4.4 Ekvivalenssirelaatio

1 Ekvivalenssirelaation määritelmä

Matematiikassa ja muuallakin joudutaan usein tekemisiin sellaisten relaatioiden kanssa, joiden lakina on tietyn ominaisuuden samuus. Alkiot voidaan tällöin jakaa "luokkiin" niin, että kaikki ne alkiot, joilla on sama ominaisuus, kuuluvat samaan luokkaan. Tällaiset tarkastelut saadaan täsmällisiksi käyttämällä *ekvivalenssirelaation* käsitettä. Joukossa X määritelty relaatio on ekvivalenssirelaatio tai lyhemmin *ekvivalenssi* (jota ei saa sekoittaa loogiseen ekvivalenssiin), jos se on refleksiivinen, symmetrinen ja transitiivinen. Ekvivalenssirelaatiota merkitään tavallisesti symbolilla $\sim$ (lue: "mato"). Keskenään ekvivalenssirelaatiossa olevat alkiot ovat *ekvivalentteja.*

Esimerkki 82. Kaikkein yksinkertaisin ekvivalenssirelaatio on alkioiden samuus

$$x \sim y \Leftrightarrow x = y.$$

Alkioiden eroavuus

$$x \sim y \Leftrightarrow x \neq y$$

ei sen sijaan ole ekvivalenssi, sillä se ei ole refleksiivinen eikä transitiivinen.

Esimerkki 83. Löydämme alkeisgeometriasta monia ekvivalenssirelaatioita, esimerkiksi

$$x \sim y \Leftrightarrow x \text{ ja } y \text{ ovat yhdensuuntaiset,} \tag{1}$$

jolloin $X = \{\text{tason tai avaruuden suorat}\}$,

$$x \sim y \Leftrightarrow x \text{ ja } y \text{ ovat yhtenevät,} \tag{2}$$

ja

$$x \sim y \Leftrightarrow x \text{ ja } y \text{ ovat yhdenmuotoiset,} \tag{3}$$

jolloin $X = \{\text{tason tai avaruuden kolmiot (tai tietyt kuviot)}\}$. Se *sama ominaisuus*, joka on keskenään ekvivalenteilla alkioilla, on kohdassa (1) suunta, kohdassa (2) muoto ja koko sekä kohdassa (3) muoto.

Olkoon $\sim$ ekvivalenssi joukossa X ja $a \in X$. Joukko

$$a/\!\sim\, = \{\, x \in X \mid x \sim a \,\}$$

on alkion a määräämä *ekvivalenssiluokka*. Se on siis kaikkien niiden alkioiden joukko, jotka ovat a:n kanssa ekvivalentteja. Käytämme kaikkien ekvivalenssiluokkien joukolle merkintää $X/\!\sim$. Siis $X/\!\sim\, = \{\, a/\!\sim \mid a \in X \,\}$.

Ekvivalenssirelaation symmetrisyydestä seuraa, että myös

$$a/\!\sim\, = \{\, x \in X \mid a \sim x \,\}.$$

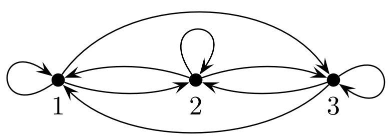
Refleksiivisyydestä seuraa, että $a \sim a$ ja siis $a \in a/\!\sim$, joten minkään alkion määräämä ekvivalenssiluokka ei ole tyhjä. Ekvivalenssiluokalle $a/\!\sim$ voidaan käyttää mukavampaa merkintää $[a]$, jos asiayhteys on sellainen, ettei relaatiota $\sim$ tarvitse korostaa.

Esimerkki 84. Joukossa $X = \{1, 2, \dots, 5\}$ määritelty relaatio $\sim\, = \{(1,1),$ $(2,2), (3,3), (4,4), (5,5), (1,2), (2,1), (1,3), (3,1), (2,3), (3,2), (4,5), (5,4)\}$ on ekvivalenssi. Alkion 1 määräämä ekvivalenssiluokka

$$1/\!\sim\, = \{\, x \in X \mid x \sim 1 \,\} = \{1, 2, 3\}.$$

Vastaavasti

$$2/\!\sim\, = 3/\!\sim\, = \{1, 2, 3\}, \quad 4/\!\sim\, = 5/\!\sim\, = \{4, 5\}.$$



Ekvivalenssiluokat ovat $\{1, 2, 3\}$ ja $\{4, 5\}$, joten $X/\!\sim\, = \big\{\{1, 2, 3\}, \{4, 5\}\big\}$. Polkukuviossa ekvivalenssiluokat erottuvat erillisiksi ”saarekkeiksi”, ja kussakin saarekkeessa nuoli kulkee jokaisesta pisteestä jokaiseen.

2 Ekvivalenssiluokkien ominaisuuksia

Edellisen esimerkin perusteella vaikuttaa siltä, että ekvivalenssiluokat muodostuvat keskenään ekvivalenteista alkioista siten, että kukin alkio kuuluu täsmälleen yhteen ekvivalenssiluokkaan. Tutkimme asiaa tarkemmin.

Lause 24. Olkoon $\sim$ ekvivalenssirelaatio joukossa X ja $a, b \in X$. Tällöin $a/\!\sim\, = b/\!\sim$, jos ja vain jos $a \sim b$.

Todistus. Vain jos. *Ol.* $a/\!\sim\, = b/\!\sim$. *Väit.* $a \sim b$. *Tod.* Koska $a \in a/\!\sim$, niin oletuksen perusteella myös $a \in b/\!\sim$, joten $a \sim b$.

Jos. *Ol.* $a \sim b$. *Väit.* $a/\!\sim\, = b/\!\sim$. *Tod.* Osoitamme ensiksi, että $a/\!\sim\, \subseteq b/\!\sim$. Olkoon $x \in a/\!\sim$ eli $x \sim a$. Oletuksen mukaan $a \sim b$, joten transitiivisuuden perusteella $x \sim b$. Siis $x \in b/\!\sim$, joten $a/\!\sim\, \subseteq b/\!\sim$. Osoitamme toiseksi, että $b/\sim \subseteq a/\sim$. Olkoon $x \in b/\sim$ eli $x \sim b$. Oletuksen ja symmetrisyyden perusteella $b \sim a$, joten transitiivisuudesta seuraa $x \sim a$. Siis $x \in a/\sim$, joten $b/\sim \subseteq a/\sim$.

Lause 25. Jos $\sim$ on ekvivalenssirelaatio joukossa X, niin joukon X jokainen alkio kuuluu täsmälleen yhteen ekvivalenssiluokkaan.

Todistus. Jokainen $x \in X$ kuuluu *ainakin* yhteen ekvivalenssiluokkaan, nimittäin ekvivalenssiluokkaan $x/\sim$. Oletamme nyt, että x kuuluu kahteen ekvivalenssiluokkaan $a/\sim$ ja $b/\sim$. Siis $x \sim a$ ja $x \sim b$. Symmetrisyyden perusteella $a \sim x$ ja edelleen transitiivisuuden perusteella $a \sim b$. Täten lauseen 24 mukaan $a/\sim = b/\sim$, joten x kuuluu *korkeintaan* yhteen ekvivalenssiluokkaan. Olemme näin osoittaneet, että x kuuluu *täsmälleen* yhteen ekvivalenssiluokkaan.

Lauseen 25 mukaan ekvivalenssiluokat muodostavat joukon X luokkajaon. Siis X on ekvivalenssiluokkien yhdiste ja eri ekvivalenssiluokat ovat erillisiä. Lisäksi mikään ekvivalenssiluokka ei ole tyhjä. Lauseesta 24 seuraa, että kaksi alkiota kuuluu samaan ekvivalenssiluokkaan täsmälleen silloin, kun ne ovat ekvivalentteja.

Esimerkki 85. (Vrt. s. 63, esim. 50.) Olkoon X erään koulun oppilaiden joukko. Relaatio

$$x \sim y \Leftrightarrow x \text{ ja } y \text{ ovat samalla luokalla}$$

on ekvivalenssi. Kaikki keskenään samalla luokalla olevat muodostavat aina yhden ekvivalenssiluokan, joten ekvivalenssiluokat ovat juuri nämä koululuokat. Jos taas määritellään ekvivalenssirelaatio

$$x \sim y \Leftrightarrow x \text{ ja } y \text{ ovat samaa sukupuolta,}$$

niin ekvivalenssiluokkia on kaksi: toisen muodostavat koulun pojat ja toisen tytöt.

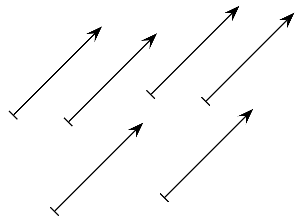
Ekvivalenssiluokan alkiota käytetään usein luokkansa *edustajana* ja luokka voidaan tietyssä mielessä *samastaa* edustajaansa. (Näin tehdään matematiikan ulkopuolellakin: sanotaan esimerkiksi, että Suomi liittyi EU:hun, käy kauppaa, voitti tietyt urheilukilpailut jne, vaikka tosiasiassa nämä asiat tapahtuvat tiettyjen Suomen edustajien toimesta. Tällaiset toimet eivät tosin ole "hyvin määriteltyjä", ks. kohta 3.)

3 Ekvivalenssiluokilla laskeminen

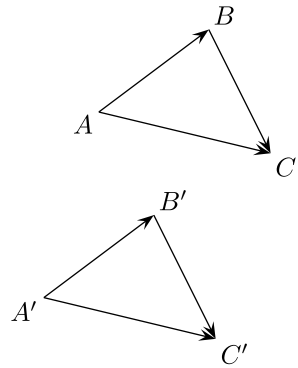
Esimerkki 86. Tarkoitamme *suuntajanalla* janaa, jolla on määrätty suunta (toinen kahdesta mahdollisesta; "nollasuuntajanan" suunta on määrittelemätön). Määrittelemme tason tai avaruuden suuntajanojen joukossa ekvivalenssirelaation

$$x \sim y \Leftrightarrow x\text{:llä ja } y\text{:llä on sama pituus ja sama suunta.}$$

Kutsumme vastaavia ekvivalenssiluokkia (geometrisiksi) *vektoreiksi*. Siis vektori on kaikkien keskenään yhtä pitkien ja samansuuntaisten suuntajanojen joukko. Vektoreita tutkittaessa ei kuitenkaan tavallisesti tarvitse käsitellä tätä joukkoa kokonaisuudessaan, vaan riittää tarkastella erästä sen edustajaa, siis yhtä suuntajanaa.



Kahden vektorin $\boldsymbol{a}$ ja $\boldsymbol{b}$ summa määritellään seuraavasti. Valitaan jokin suuntajana $\overrightarrow{AB} \in \boldsymbol{a}$ ja sitten suuntajana $\overrightarrow{BC} \in \boldsymbol{b}$. Summa $\boldsymbol{a} + \boldsymbol{b}$ on se vektori, johon kuuluu suuntajana $\overrightarrow{AC}$. Meidän on vielä osoitettava, että näin määritelty summa *ei riipu yhteenlaskettavien edustajina olevien suuntajanojen valinnasta*, sillä muuten määritelmässä ei olisi mitään järkeä. Jos siis myös $\overrightarrow{A'B'} \in \boldsymbol{a}$ ja $\overrightarrow{B'C'} \in \boldsymbol{b}$, niin meidän on näytettävä, että $\overrightarrow{A'C'}$ kuuluu samaan vektoriin kuin $\overrightarrow{AC}$ eli näillä suuntajanoilla on sama pituus ja sama suunta. Yksinkertainen geometrinen tarkastelu (suorita) osoittaa, että näin on.



Muutkin vektorien laskutoimitukset määritellään edustajien avulla ja ne on osoitettava riippumattomiksi edustajien valinnasta.

Jos joukossa X on määritelty laskutoimitus, niin joukossa $X/{\sim}$ voidaan määritellä vastaava laskutoimitus ekvivalenssiluokkien edustajien avulla. Tällöin on huolehdittava siitä, ettei määritelmä riipu edustajien valinnasta eli että laskutoimitus joukossa $X/{\sim}$ on *hyvin määritelty* (engl. *well-defined*). Tästä meillä oli edellä esimerkki, ja käsittelemme vielä toisen.

Esimerkki 87. Osoitettava, että joukossa $\mathbb{Z}$ määritelty relaatio

$$x \sim y \Leftrightarrow x - y \text{ on jaollinen luvulla } 5$$

on ekvivalenssi. Muodostettava ekvivalenssiluokat ja määriteltävä niiden yhteen- ja kertolasku edustajien vastaavien laskutoimitusten avulla.

(r) Aina $x \sim x$, sillä $x - x = 0$ on jaollinen 5:llä. Siis $\sim$ on refleksiivinen.

(s) Jos $x \sim y$, niin $x - y$ on jaollinen 5:llä, jolloin myös vastaluku $y - x$ on jaollinen 5:llä eli $y \sim x$. Siis $\sim$ on symmetrinen.

(t) Olkoon $x \sim y$ ja $y \sim z$, joten $x - y$ ja $y - z$ ovat jaollisia 5:llä eli on olemassa sellaiset $p, q \in \mathbb{Z}$, että $x - y = 5p$, $y - z = 5q$. Laskemalla nämä yhtälöt yhteen saamme $x - z = 5(p + q)$, joten $x - z$ on jaollinen 5:llä eli $x \sim z$. Siis $\sim$ on transitiivinen.

Ekvivalenssiluokat ovat

$$\begin{aligned}
0/{\sim} &= \{\, x \in \mathbb{Z} \mid x - 0 \text{ on jaollinen 5:llä} \,\} = \{0, \pm 5, \pm 10, \ldots\},\\
1/{\sim} &= \{\, x \in \mathbb{Z} \mid x - 1 \text{ on jaollinen 5:llä} \,\} = \{1, 6, 11, \ldots, -4, -9, \ldots\},
\end{aligned}$$

$$\begin{aligned}2/{\sim} &= \{2,7,12,\ldots,-3,-8,\ldots\},\\ 3/{\sim} &= \{3,8,13,\ldots,-2,-7,\ldots\},\\ 4/{\sim} &= \{4,9,14,\ldots,-1,-6,\ldots\}.\end{aligned}$$

Muita ekvivalenssiluokkia ei ole, sillä $5/{\sim} = 0/{\sim}$, $6/{\sim} = 1/{\sim}$ jne. Yleisesti

$$x/{\sim} = \{\, x+5k \mid k \in \mathbb{Z} \,\}.$$

Kutsumme näitä ekvivalenssiluokkia *jäännösluokiksi modulo* 5 ja merkitsemme $\mathbb{Z}/{\sim} = \mathbb{Z}_5$. Voimme myös merkitä $0_5 = 0/{\sim}$, $1_5 = 1/{\sim}$ jne. Vastaavat tarkastelut voidaan suorittaa (teht. 208) yleisesti relaatiolle

$$x \sim y \Leftrightarrow x - y \text{ on jaollinen luvulla } n,$$

missä $n \in \mathbb{Z}_+$ on annettu. (Miksi ei kannata tutkia $n \in \mathbb{Z}_-$? Miksi tapaus $n = 1$ ei ole kiinnostava?) Kutsumme tätä ekvivalenssirelaatiota *kongruenssiksi modulo n* ja käytämme ekvivalenssiluokkien eli *kongruenssiluokkien* joukolle merkintää $\mathbb{Z}_n$.

Määrittelemme joukossa $\mathbb{Z}_5$ yhteen- ja kertolaskun. Kysymme siis, mitä on esimerkiksi luokkien 3_5 ja 4_5 summa ja tulo. Otamme edustajat $3 \in 3_5$ ja $4 \in 4_5$, joiden summa on 7 ja tulo 12. Koska $7 \in 2_5$ ja $12 \in 2_5$ (miksi?), määrittelemme $3_5 + 4_5 = 2_5$ ja $3_5 \cdot 4_5 = 2_5$. Menettelemällä vastaavasti muillekin summille ja tuloille saamme seuraavat yhteen- ja kertolaskutaulut, joissa alaindeksi 5 on jätetty kirjoittamatta.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Osoitamme, että nämä laskutoimitukset

$$x/{\sim} + y/{\sim} = (x+y)/{\sim}, \quad x/{\sim} \cdot y/{\sim} = (xy)/{\sim}$$

ovat hyvin määriteltyjä eli eivät riipu luokkien edustajista x ja y. Olkoon $x' \in x/{\sim}$ ja $y' \in y/{\sim}$, jolloin $x' \sim x$ ja $y' \sim y$ eli $x' - x$ ja $y' - y$ ovat 5:llä jaollisia, joten on olemassa sellaiset $p, q \in \mathbb{Z}$, että $x' - x = 5p$, $y' - y = 5q$. Meidän on näytettävä, että $(x'+y')/{\sim} = (x+y)/{\sim}$ ja $(x'y')/{\sim} = (xy)/{\sim}$. Näin on, sillä $x' + y' - (x+y) = x' - x + y' - y = 5p + 5q = 5(p+q)$ ja $x'y' - xy = (x+5p)(y+5q) - xy = 5(qx + py + 5pq)$.

Summa ja tulo voidaan määritellä yleisesti joukossa $\mathbb{Z}_n$. Ne voidaan osoittaa hyvin määritellyiksi (teht. 213).

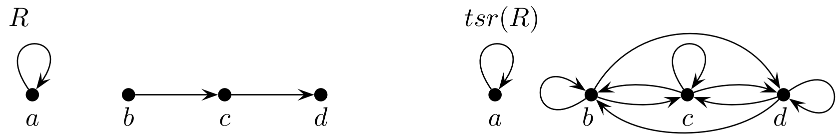
∗4 Yhteydet sulkeumiin ja luokkajakoihin

Olkoon R relaatio tietyssä joukossa. Kutsumme täydentämällä saatua relaatiota $tsr(R)$ relaation R *määräämäksi* ekvivalenssiksi. Se on pienin R:n sisältävä ekvivalenssi (teht. 218).

Esimerkki 88. Jos $X = \{a, b, c, d\}$ ja $R = \{(a, a), (b, c), (c, d)\}$, niin

$$tsr(R) = \{(a, a), (b, b), (b, c), (b, d), (c, b), (c, c), (c, d), (d, b), (d, c), (d, d)\}.$$

Ekvivalenssiluokat ovat $\{a\}$ ja $\{b, c, d\}$, joten $X/R = \big\{\{a\}, \{b, c, d\}\big\}$.



Olemme todenneet, että jokainen ekvivalenssirelaatio määrittelee luokkajaon, nimittäin jaon ekvivalenssiluokkiin. Osoitamme nyt käänteisesti, että jokainen luokkajako määrittelee ekvivalenssirelaation. Tarkastelemme joukon $X(\neq \emptyset)$ luokkajakoa $\mathcal{A} = \{A_k\}_{k \in I}$, jolloin

$$X = \bigcup_{k \in I} A_k, \text{ missä } A_i \cap A_k = \emptyset \text{ aina, kun } i \neq k.$$

Määrittelemme joukossa X relaation

$$x \sim y \Leftrightarrow x \text{ ja } y \text{ kuuluvat samaan joukkoon } A_k,$$

joka on helppo osoittaa ekvivalenssiksi. Nyt $X/\!\sim\, = \mathcal{A}$.

Harjoitustehtäviä

201. Onko nyt elävien ihmisten joukossa määritelty relaatio **a)** 'vähintään yhtä vanha kuin', **b)** 'sukulainen', **c)** 'samaa sukupuolta' **d)** 'saman maan kansalainen', **e)** 'työtoveri', **f)** 'ystävä' aina ekvivalenssi?

202. Onko Suomen kaupunkien joukossa määritelty relaatio $\sim$ ekvivalenssi, kun $x \sim y$ tarkoittaa, että x:stä pääsee y:hyn **a)** maitse, **b)** junalla, **c)** alle kahdessa tunnissa? Myönteisessä tapauksessa määritettävä ekvivalenssiluokat.

203. Kuinka monta ekvivalenssiluokkaa on tavallisessa korttipakassa määritellyllä ekvivalenssirelaatiolla **a)** $x \sim y \Leftrightarrow x$:llä ja y:llä on sama maa, **b)** $x \sim y \Leftrightarrow x$:llä ja y:llä on sama arvo?

204. Esitettävä luettelemalla alkiot joukon $X = \{1, 2, 3, 4\}$ se ekvivalenssirelaatio R, jolle $X/R = \big\{\{1, 2\}, \{3, 4\}\big\}$.

205. Joukossa X määritellään ekvivalenssirelaatio **a)** $x \sim y \Leftrightarrow x = y$, **b)** $x \sim y$ kaikilla $x, y \in X$. Muodostettava $X/\!\sim$.

206. **a)** Osoitettava, että joukossa $X = \{1, 2, 3, 4\}$ määritelty relaatio

$$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1), (2, 3), (3, 2)\}$$

ei ole ekvivalenssi. **b)** Täydennettävä R ekvivalenssiksi lisäämällä siihen mahdollisimman vähän alkioita.

207. Onko joukossa $\mathbb{R}$ määritelty relaatio

a) $x \sim y \Leftrightarrow x + y \in \mathbb{Z}$,

b) $x \sim y \Leftrightarrow x - y \in \mathbb{Z}$

ekvivalenssi? Myönteisessä tapauksessa määritettävä ekvivalenssiluokat.

208. Olkoon $n \in \mathbb{Z}_+$. Näytettävä, että joukossa $\mathbb{Z}$ määritelty kongruenssi modulo n

$$x \sim y \Leftrightarrow x - y \text{ on jaollinen luvulla } n$$

on ekvivalenssi, ja määritettävä ekvivalenssiluokat.

209. Seuraavassa ”todistetaan”, että ekvivalenssirelaation ominaisuudet eivät ole riippumattomia, vaan symmetrisyydestä ja transitiivisuudesta seuraa refleksiivisyys. Olkoon $x \in X$ mielivaltainen ja $y \in X$ sellainen, että $x \sim y$. Nyt $y \sim x$ (s), joten edelleen $x \sim x$ (t). Missä vika?

210. Millainen on (äärellisessä joukossa määritellyn) ekvivalenssirelaation matriisi?

211. Olkoon R relaatio joukossa X. Osoitettava seuraavat ehdot yhtäpitäviksi.

(1) R on ekvivalenssi,

(2) $R^n \subseteq R$ kaikilla $n \in \mathbb{Z}$,

(3) R on refleksiivinen ja *euklidinen* eli $xRy \wedge xRz \Rightarrow yRz$.

212. **a)** Määriteltävä (geometrisen) vektorin kertominen skalaarilla. **b)** Osoitettava, että se on hyvin määritelty.

213. Todistettava, että joukon $\mathbb{Z}_n$ alkioiden yhteen- ja kertolasku ovat hyvin määriteltyjä.

214. Muodostettava joukon $\mathbb{Z}_6$ yhteen- ja kertolaskutaulu. Mikä ero on yhtälön $a \cdot x = b$ ratkeavuudella joukossa $\mathbb{Z}_5$ ja joukossa $\mathbb{Z}_6$?

215. Olkoot R ja S ekvivalensseja. Onko **a)** $R \cap S$, **b)** R^{-1}, **c)** $R \circ S$ tällöin aina ekvivalenssi?

216. Osoitettava, että jos R ja S ovat ekvivalensseja, niin $R \cup S$ ei yleensä ole ekvivalenssi, mutta $t(R \cup S)$ on.

217. Olkoon R relaatio joukossa X. Osoitettava, että $rst(R) = srt(R) = str(R)$ ja $rts(R) = tsr(R) = tsr(R)$, mutta ei välttämättä $rst(R) = rts(R)$.

218. Olkoon R relaatio joukossa X. Todistettava, että $tsr(R)$ on **a)** ekvivalenssi, **b)** pienin ekvivalenssi, joka sisältää R:n, **c)** kaikkien R:n sisältävien ekvivalenssien leikkaus.

219. Olkoot $\{ A_i \mid i \in I \}$ ja $\{ B_j \mid j \in J \}$ joukon X luokkajakoja. Onko **a)** $\{ A_i \cup B_j \mid i \in I,\ j \in J \}$, **b)** $\{ A_i \cap B_j \mid i \in I,\ j \in J \}$, **c)** $\{ A_i \cap B_j \mid i \in I,\ j \in J,\ A_i \cap B_j \neq \emptyset \}$ aina joukon X luokkajako? Myönteisessä tapauksessa muodostettava tätä luokkajakoa vastaava ekvivalenssi.

220. Tietyn koulun oppilaiden joukossa määritellään ekvivalenssirelaatio $R =$ 'samalla luokalla' ja $S =$ 'samaa sukupuolta'. Mikä luokkajako vastaa ekvivalenssirelaatiota **a)** $R \cap S$, **b)** $t(R \cup S)$?

4.5 Järjestysrelaatio

1 Järjestysrelaation määritelmä

Ekvivalenssirelaatio on siis käsitteen 'liittyy tietty sama ominaisuus' abstraktio. Toinen matematiikassa ja muuallakin keskeinen relaatioon johtava käsite syntyy vertailtaessa järjestystä. Ryhdymme nyt abstrahoimaan käsitteitä 'pienempi kuin' ja 'vähemmän kuin'. Tutkimme näitä käsitteitä muodossa 'pienempi tai yhtäsuuri kuin' ja 'vähemmän tai yhtä paljon kuin'. Sanomme, että joukossa X määritelty relaatio on *järjestysrelaatio* eli lyhemmin *järjestys*, jos se on refleksiivinen, antisymmetrinen, transitiivinen ja vertailullinen. Järjestysrelaatiota merkitään tavallisesti symbolilla $\preceq$ (lue: "edeltää").

Refleksiivisyys tarkoittaa, että kukin alkio edeltää itseään. Antisymmetrisyys tarkoittaa, etteivät kaksi eri alkiota voi molemmat edeltää toisiaan. Transitiivisuus merkitsee, että edeltävyys on "periytyvää": jos alkio edeltää jotakin toista alkiota, niin se edeltää myös kaikkia niitä alkioita, joita tämä toinen alkio edeltää. Vertailullisuus taas merkitsee, että kahdesta alkiosta aina toinen edeltää toista.

Relaatio, joka on refleksiivinen, antisymmetrinen ja transitiivinen, muttei välttämättä vertailullinen, on *osittainen järjestys* eli *osittainjärjestys.* Itse järjestysrelaatiota voimme sanoa myös *täydelliseksi järjestykseksi* tai *lineaariseksi järjestykseksi.* Jos $\preceq$ on järjestys, niin relaatiota

$$x \prec y \Leftrightarrow x \preceq y \wedge x \neq y$$

(lue: "edeltää aidosti") kutsutaan usein "aidoksi järjestykseksi", mikä on hieman kummallista "aito"-sanan käyttöä, koska nyt "aito järjestys" ei olisikaan järjestys. Kutsumme tätä relaatiota paremman puutteessa *tiukaksi järjestykseksi.* Edelleen merkitsemme $y \succeq x \Leftrightarrow x \preceq y$. Vastaavasti määrittelemme merkinnän $\succ$.

Joukko X, jossa on määritelty järjestysrelaatio, on *järjestetty joukko.* Täsmällisempää on sanoa, että järjestetyllä joukolla tarkoitetaan joukon X ja järjestysrelaation $\preceq$ muodostamaa järjestettyä paria $(X, \preceq)$. Vastaavasti määrittelemme *osittain järjestetyn joukon.* Joukko (jonka alkioiden lukumäärä > 1) voidaan järjestää monella eri tavalla.

Esimerkki 89. Yksinkertaisin tapa järjestää joukko $\mathbb{R}$ on asettaa

$$x \preceq y \Leftrightarrow x \leq y.$$

Yhtä hyvin voisimme määritellä

$$x \preceq y \Leftrightarrow x \geq y.$$

Relaatio

$$x \preceq y \Leftrightarrow |x| \leq |y|$$

ei sen sijaan ole järjestys, sillä antisymmetrisyys ei ole voimassa esimerkiksi alkioille $x = 5$, $y = -5$. Tällaista relaatiota, joka on refleksiivinen ja transitiivinen, muttei välttämättä antisymmetrinen, kutsutaan *kvasijärjestykseksi.*

Esimerkki 90. Joukon X osajoukkojen joukossa $\mathcal{P}(X)$ määritelty relaatio

$$A \preceq B \Leftrightarrow A \subseteq B$$

on osittainen järjestys (s. 49, lause 4), mutta ei täydellinen (jos joukossa X on enemmän kuin yksi alkio). Jos näet $x, y \in X$, $x \neq y$, niin joukot $A = \{x\}$, $B = \{y\}$ eivät edellä toisiaan kumpaankaan suuntaan, joten $\preceq$ ei ole vertailullinen.

2 Hasse-diagrammi

Esimerkki 91. (Ks. kuviot seuraavalla sivulla.) Tarkastelemme joukkoa $X = \{a, b, c\}$. Yksinkertaisin tapa järjestää X osittain on määritellä $R = \{(a, a), (b, b), (c, c)\}$. Myös esimerkiksi relaatiot $S = \{(a, a), (b, b), (c, c), (a, b)\}$ ja $T = \{(a, a), (b, b), (c, c), (a, b), (a, c)\}$ ovat osittaisia järjestyksiä. Niitä havainnollistaa polkukuviota paremmin *Hasse*[2]*-diagrammi*, jossa keskenään relaatiossa olevat eri alkiot yhdistetään viivalla niin, että alempi edeltää ylempää. Kuvio voidaan piirtää myös vasemmalta oikealle. Näin on syytä menetellä erityisesti täydellisen järjestyksen tapauksessa. Esimerkiksi $U = \{(a, a), (b, b), (c, c), (a, b), (a, c), (b, c)\}$ on täydellinen järjestys (osoita), mikä näkyy Hasse-diagrammissa niin, että alkiot ovat ”peräkkäin”. Tämä voidaan havainnollistaa myös ilman Hasse-diagrammia yksinkertaisesti kirjoittamalla alkiot peräkkäin. Joukkomerkinnässä käytetään tällöin kaarisulkeita aaltosulkeiden sijasta korostamassa sitä, että kysymyksessä on järjestetty joukko.

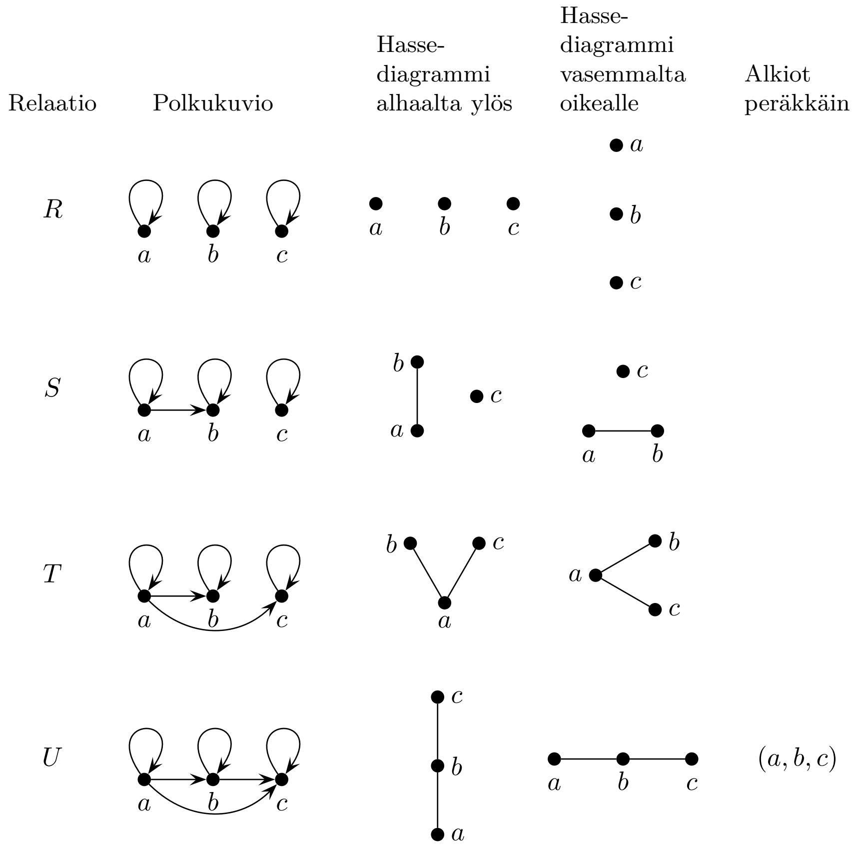
Esimerkki 92. Luonnollinen yritys järjestää joukko $\mathbb{R}^2$ olisi asettaa

$$(x_1, y_1) \preceq (x_2, y_2) \Leftrightarrow x_1 \leq x_2 \wedge y_1 \leq y_2.$$

Tämä on kuitenkin vain osittainen järjestys, sillä esimerkiksi alkiot $(0, 1)$ ja $(1, 0)$ eivät edellä toisiaan kumpaankaan suuntaan, joten $\preceq$ ei ole vertailullinen. Täydellinen järjestys saadaan vertaamalla aluksi vaikkapa ensimmäisiä alkioita ja niiden ollessa samat toisia

$$(x_1, y_1) \preceq (x_2, y_2) \Leftrightarrow x_1 < x_2 \vee (x_1 = x_2 \wedge y_1 \leq y_2).$$

[2] *Helmut Hasse (1898–1979), saksalainen matemaatikko.*



Voimme järjestää joukon $\mathbb{R}^3$ vastaavalla tavalla (teht. 228a) ja yleisesti joukon $\mathbb{R}^n$. Saatua järjestysrelaatiota kutsutaan *sanakirjajärjestykseksi*, sillä sanat järjestetään aakkosjärjestykseen samalla periaatteella. Nämä tarkastelut voidaan helposti yleistää koskemaan yleisen tulojoukon $X \times Y$ ja edelleen joukon $X_1 \times \cdots \times X_n$ järjestämistä (teht. 228c).

∗3 Hyvinjärjestys

Sanomme, että järjestetty joukko $(X, \preceq)$ on *hyvinjärjestetty*, jos sen jokaisessa epätyhjässä osajoukossa on *pienin alkio*, joka edeltää kaikkia muita. (Vastaavasti *suurin alkio* määritellään alkiona, jota kaikki muut edeltävät.) Siis

$$(X, \preceq) \text{ on hyvinjärjestetty}$$
$$\Leftrightarrow \big(A \subseteq X \land A \neq \emptyset \Rightarrow \exists a \in A\colon (x \in A \Rightarrow a \preceq x)\big).$$

Esimerkki 93. Määrittelemme joukossa $\mathbb{Z}$ järjestysrelaatiot

$$xRy \Leftrightarrow x \leq y,$$
$$xSy \Leftrightarrow x = 0 \lor (x < 0 \land y > 0) \lor (xy > 0 \land |x| \geq |y|),$$

$$xTy \Leftrightarrow x = 0 \vee (x < 0 \wedge y > 0) \vee (xy > 0 \wedge |x| \leq |y|),$$
$$xUy \Leftrightarrow |x| < |y| \vee (|x| = |y| \wedge x < 0) \vee x = y.$$

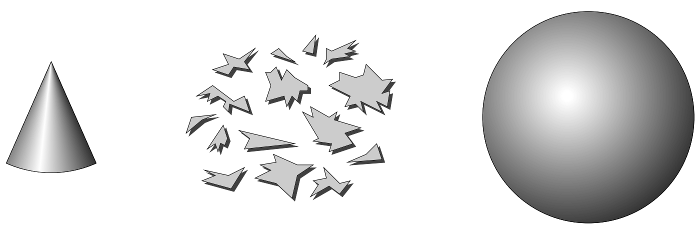
Asettamalla joukon $\mathbb{Z}$ alkiot järjestyksen mukaiseen jonoon saamme

$$(\mathbb{Z}, R) = (\ldots, -2, -1, 0, 1, 2, \ldots), \quad (\mathbb{Z}, S) = (0, \ldots, -2, -1, \ldots, 2, 1),$$
$$(\mathbb{Z}, T) = (0, -1, -2, \ldots, 1, 2, \ldots), \quad (\mathbb{Z}, U) = (0, -1, 1, -2, 2, \ldots).$$

Joukko $(\mathbb{Z}, R)$ ei ole hyvinjärjestetty, koska esimerkiksi siinä itsessään ei ole pienintä alkiota. Myöskään $(\mathbb{Z}, S)$ ei ole hyvinjärjestetty. Joukossa $\mathbb{Z}$ tosin on nyt pienin alkio 0, mutta esimerkiksi joukossa $\mathbb{Z}_-$ tällaista alkiota ei ole. (Lukua -2 edeltävät kolme pistettä tarkoittavat etenemistä oikealta vasemmalle.) Sen sijaan $(\mathbb{Z}, T)$ ja $(\mathbb{Z}, U)$ ovat hyvinjärjestettyjä.

Hyvinjärjestysperiaatteen eli *Zermelon*[3] *väittämän* mukaan jokainen joukko voidaan hyvinjärjestää. On kuitenkin vaikea kuvitella millainen olisi hyvinjärjestys esimerkiksi joukossa $\mathbb{R}$. Hyvinjärjestysperiaate vain ilmoittaa hyvinjärjestyksen olemassaolon, mutta ei anna menetelmää sen konstruoimiseksi.

Hyvinjärjestysperiaate ja sen kanssa yhtäpitävä *valinta-aksiooma* (ks. luku 5.5) vievät syvälle matematiikan perimmäisiin kysymyksiin, sillä on voimassa kiusallinen *Banachin*[4]*–Tarskin*[5] *paradoksi*. Sen mukaan kaksi mielivaltaista kolmiulotteisen avaruuden kappaletta voidaan jakaa äärelliseen määrään osia, jotka ovat pareittain yhtenevät! Siis esimerkiksi pieni kartio voidaan pilkkoa äärelliseen määrään osia niin, että kun nämä osat kootaan toisella tavalla, niin saadaan suuri pallo!



Valitettavasti tämä täysin järjettömän tuntuinen väite on matemaattinen tosiasia, jos valinta-aksiooma hyväksytään. Jos taas valinta-aksiooma hylätään, niin matematiikkaa ei pystytä kovinkaan paljoa rakentamaan. Onneksi tästä paradoksista ei kuitenkaan seuraa, että kaikilla kappaleilla olisi sama tilavuus. Nimittäin ne osat, joihin kappaleet jaetaan, ovat niin eriskummallisia (*ei-mitallisia*) joukkoja, että niiden tilavuutta ei voida määritellä. Siksi tämä pilkkominen ja uudelleen kokoaminen ei ole fysikaalisesti mahdollista.

Olemme huomanneet, että ensimmäistä ja toista induktioperiaatetta voidaan soveltaa missä tahansa kokonaislukujoukossa $M = \{m, m+1,$

[3] *Ernst Zermelo (1871–1953), saksalainen matemaatikko.*
[4] *Stefan Banach (1892–1945), puolalainen matemaatikko.*
[5] *Alfred Tarski (1902–1983), puolalais-yhdysvaltalainen loogikko.*

$m+2, \ldots\}$. On luonnollista kysyä, voidaanko niitä soveltaa mielivaltaisessa järjestetyssä joukossa X. Ensimmäisen induktioperiaatteen osalta vastaus on kielteinen. Koska joukon X alkiolla ei välttämättä ole "välitöntä seuraajaa" (kuten kokonaisluvun k välitön seuraaja on $k+1$), niin ensimmäistä induktioperiaatetta ei voida edes esittää joukossa X. Sen sijaan toinen voidaan. Tällöin induktioaskel on, että totuudesta kaikilla tietyn alkion edeltäjillä seuraa totuus tällä alkiolla. Voidaan todistaa, että toinen induktioperiaate on pätevä, jos (ja vain jos) X on hyvinjärjestetty (teht. 239).

Toinen induktioperiaate (yleisessä hyvinjärjestetyssä joukossa). Olkoon $(X, \preceq)$ hyvinjärjestetty joukko. Oletetaan, että jokaista $x \in X$ vastaa lause p_x. Olkoon tehtävänä todistaa, että p_x on tosi kaikilla $x \in X$. Menetellään seuraavasti.

1 (Perusaskel). Osoitetaan, että p_a on tosi, missä a on joukon X pienin alkio.

2 (Induktioaskel). Osoitetaan, että p_y:n totuudesta kaikilla $y \prec x$ aina seuraa p_x:n totuus. Toisin sanoen tehdään *induktio-oletus*, että p_y on tosi kaikilla $y \prec x$, ja todistetaan *induktioväite*, että p_x on tällöin tosi.

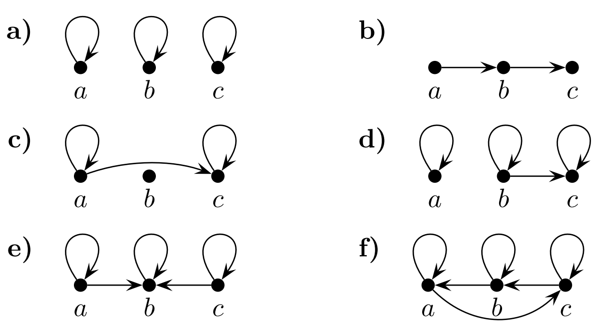
3 (Johtopäätös). Tämän jälkeen alkuperäinen väitös seuraa induktioperiaatteesta.

Voimme formalisoida tämän lyhyesti muotoon

$$\begin{array}{l} p_a \quad (a \text{ on joukon } X \text{ pienin alkio}) \\ \forall x \in X : \big((\forall y \prec x : p_y) \Rightarrow p_x\big) \\ \hline \forall x \in X : p_x \end{array}$$

Harjoitustehtäviä

221. Ovatko seuraavien polkukuvioiden määrittelemät relaatiot osittaisia tai täydellisiä järjestyksiä joukossa $X = \{a, b, c\}$?



222. Oletetaan seuraavat relaatiot määritellyiksi sopivissa perusjoukoissa. Millaisia "järjestyksiä" ne ovat (kvasi-, tiukka osittainen, osittainen, tiukka täydellinen, täydellinen tai ei mikään näistä)? **a)** 'nuorempi', **b)** 'vähintään yhtä vanha', **c)** 'edeltävä opintosuoritus', **d)** 'tietyn henkilön mielestä vähintään yhtä hyvä elokuva', **e)** 'jälkeläinen', **f)** 'vähintään yhtä kaukana Tampereelta'.

223. a) Osoitettava, että joukossa $X = \{1, 2, 3, 4\}$ määritelty relaatio $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (1, 3), (1, 4), (3, 4)\}$ on osittainen muttei täydellinen järjestys. **b)** Voidaanko sitä täydentää (lisäämällä alkioita) niin, että saadaan täydellinen järjestys?

224. Joukossa $X = \{1, 2, 3, 4\}$ määritellään $1 \prec 2$, $1 \prec 3$, $2 \prec 3$, $3 \prec 4$, $4 \prec 1$. **a)** Osoitettava, ettei $\prec$ ole tiukka järjestys. **b)** Voidaanko sitä täydentää niin, että saadaan tiukka järjestys?

225. Osoitettava, että joukossa $\mathbb{Z}_+$ määritelty relaatio

$$x \preceq y \Leftrightarrow y \text{ on jaollinen luvulla } x$$

on osittainen järjestys, muttei täydellinen.

226. Onko joukossa $\mathbb{R}^2$ määritelty relaatio

$$(x_1, y_1) \preceq (x_2, y_2) \Leftrightarrow x_1 \leq x_2 \vee y_1 \leq y_2$$

järjestys?

227. Voiko **a)** osittainen, **b)** täydellinen järjestys olla ekvivalenssi?

228. Järjestettävä **a)** $\mathbb{R}^3$, **b)** $\mathbb{R} \cup \mathbb{R}^2 \cup \mathbb{R}^3$, **c)** $X_1 \times \cdots \times X_n$, missä X_1, $\ldots$, X_n ovat järjestettyjä joukkoja.

229. Millainen on (äärellisessä joukossa määritellyn) järjestysrelaation matriisi?

230. Todistettava: Joukossa X määritelty relaatio R on osittainen järjestys, jos ja vain jos se on transitiivinen ja $R \cap R^{-1} = I$.

231. Olkoon $\prec$ tiukka järjestys joukossa X. Osoitettava, että jokaisella $x, y \in X$ täsmälleen yksi ehdoista

$$x \prec y, \quad x \succ y, \quad x = y$$

on voimassa.

232. Todistettava: **a)** Jos R' on joukon X tiukka järjestys, niin $R = R' \cup I$ on tämän joukon järjestys. **b)** Jos R on joukon X järjestys, niin $R = R' \cup I$, missä R' on tiukka järjestys.

233. Olkoon X tietty joukko olioita, joita henkilö A vertailee keskenään ja olkoot Q, P, E joukon X sellaisia relaatioita, joiden intuitiiviset merkitykset ovat

$$\begin{aligned} &xQy \Leftrightarrow A\text{:n mielestä } x \text{ on vähintään yhtä hyvä kuin } y,\\ &xPy \Leftrightarrow A\text{:n mielestä } x \text{ on parempi kuin } y,\\ &xEy \Leftrightarrow A\text{:n mielestä } x \text{ ja } y \text{ ovat yhtä hyviä.} \end{aligned}$$

Relaatio Q on *heikko* ja P on *vahva preferenssi* sekä E on *indifferenssi.*

Mitä ominaisuuksia (refleksiivisyys, transitiivisuus yms.) relaatioilta Q, P ja E pitää vaatia, jotta A:ta voitaisiin pitää rationaalisena?

234. Olkoon Q transitiivinen ja vertailullinen relaatio joukossa X. Määritellään

$$xEy \Leftrightarrow xQy \wedge yQx, \quad xPy \Leftrightarrow \neg yQx.$$

Todistettava

a) Relaatio E on ekvivalenssi.

b) Relaatio P on transitiivinen ja asymmetrinen (teht. 186).

c) Aina, kun $x, y \in X$, niin täsmälleen yksi ehdoista xEy, xPy, yPx on voimassa.

d) Jos xEy, niin $xQz \Leftrightarrow yQz$.

235. Jatkoa. Ekvivalenssiluokkien $[x] = x/E$ joukossa X/E määritellään

$$[x] \preceq [y] \Leftrightarrow xQy.$$

Osoitettava, että relaatio $\preceq$ on **a)** hyvin määritelty eli ei riipu ekvivalenssiluokkien edustajista, **b)** järjestys.

236. Olkoot R ja S järjestyksiä joukossa X. Onko **a)** $R \cup S$, **b)** $R \cap S$, **c)** R^{-1}, **d)** $R \circ S$ järjestys?

237. Olkoon Σ äärellinen järjestetty joukko kirjaimia ja olkoon Σ^+ niistä muodostettujen äärellisten jonojen joukko. **a)** Määritellään joukossa Σ^+ sanakirjajärjestys, joka toimii samalla periaatteella kuin sanojen asettaminen aakkosjärjestykseen. Osoitettava, ettei sanakirjajärjestys ole hyvinjärjestys joukossa Σ^+. Ohje: Olkoon $a, b \in \Sigma$ ja $a \prec b$. Tutki joukkoa $\{b, ab, aab, \ldots\}$. **b)** Määritellään joukossa Σ^+ *standardijärjestys* niin, että eripituiset sanat järjestetään kirjainten lukumäärän mukaan ja samanpituiset sanakirjajärjestykseen. Osoitettava, että standardijärjestys on hyvinjärjestys.

238. Olkoon $(X, \preceq)$ järjestetty joukko. Alkio $y \in X$ on alkion $x \in X$ *välitön edeltäjä* ja alkio x on alkion y *välitön seuraaja*, jos $y \prec x$ eikä ole sellaista $z \in X$, että $y \prec z \prec x$. **a)** Osoitettava, että hyvinjärjestetyssä joukossa jokaisella alkiolla paitsi (mahdollisella) suurimmalla on välitön seuraaja. Ohje: Tutki alkion kaikkien seuraajien joukkoa. **b)** Mainittava jokin ei-hyvinjärjestetty joukko, jonka millään alkiolla ei ole välitöntä seuraajaa. **c)** Onko hyvinjärjestetyn joukon kaikilla muilla alkioilla paitsi pienimmällä välitön edeltäjä?

239. Todistettava: Joukko on hyvinjärjestetty, jos ja vain jos siinä on voimassa toinen induktioperiaate. Ohjeita: ”Vain jos”. Tee vastaoletus, että lauseet p_x $(x \in X)$ toteuttavat perus- ja induktioaskeleen, mutta että joukko $S = \{\, x \in X \mid p_x \text{ on epätosi} \,\}$ on epätyhjä. Olkoon s sen pienin alkio. Miten saat ristiriidan? ”Jos”. Tee vastaoletus, että on olemassa sellainen joukko $S \subseteq X$, $S \neq \emptyset$, jossa ei ole pienintä alkiota. Osoita, että lause $p_x =$ '$y \in S \Rightarrow y \succeq x$' on tosi kaikilla $x \in X$. Miten tästä syntyy ristiriita?

240. Olkoon $a \in \mathbb{Z}$, $b \in \mathbb{Z}_+$. **a)** Todistettava *jakoyhtälö*: On olemassa sellaiset $q, r \in \mathbb{Z}$, että $0 \leq r < b$ ja $a = qb + r$. Ohje: Tutki joukkoa $\{\, a - sb \mid s \in \mathbb{Z} \,\} \cap \mathbb{N}$. Käytä hyväksi sitä, että $\mathbb{N}$ on hyvinjärjestetty. **b)** Osoitettava, että q ja r ovat yksikäsitteiset.

Luku 5

Kuvaukset

Pykälien … tarkoituksena on esittää joukon ja funktion käsitteet, joita ilman emme *voi tehdä* mitään *matematiikassa – ja toisaalta, joita käyttämällä voimme tehdä* kaiken.

(*Godement* [5])

5.1 Kuvauksen määritelmä ja muita peruskäsitteitä

1 Kuvaus relaationa

Kuvaus eli funktio f jouko*lta* X joukk*oon* Y ($X, Y \neq \emptyset$, huomaa sijat) tarkoittaa havainnollisesti ”vastaavuutta”, joka liittää joukon X jokaiseen alkioon joukon Y tietyn alkion. Määritelläksemme ”vastaavuuden” täsmällisesti tarkastelemme relaatiota f joukosta X joukkoon Y. Tämä relaatio on *kuvaus* eli *funktio* joukolta X joukkoon Y, jos ensiksikin sen lähtöjoukko ja määrittelyjoukko ovat samat

$$M_f = X \tag{1}$$

eli

$$\forall x \in X : \exists y \in Y : (x, y) \in f, \tag{1}$$

ja toiseksi, jos mikään $x \in X$ ei ole relaatiossa useamman kuin yhden alkion $y \in Y$ kanssa

$$(x, y_1) \in f \wedge (x, y_2) \in f \Rightarrow y_1 = y_2. \tag{2}$$

Ehdon (1) mukaan jokaista $x \in X$ vastaa *ainakin* yksi sellainen $y \in Y$, että $(x, y) \in f$. Ehdon (2) mukaan jokaista x:ää vastaa *korkeintaan* yksi tällainen y. (Kuitenkin eri x:iä voi vastata sama y, ja voi olla, että jokin y ei vastaa mitään x:ää.) Yhdessä nämä ehdot sanovat, että jokaista x:ää vastaa *täsmälleen* yksi y. Ottamalla käyttöön kvanttorin $\exists!$ tarkoittamaan ilmaisua ’on olemassa yksikäsitteinen’ voimme esittää ehdot (1) ja (2) yhtenä ehtona

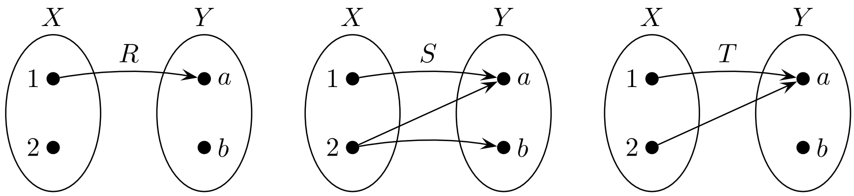
$$\forall x \in X : \exists!\ y \in Y : (x, y) \in f. \tag{1, 2}$$

Esimerkki 94. Onko joukosta $X = \{1, 2\}$ joukkoon $Y = \{a, b\}$ määritelty relaatio **a)** $R = \{(1, a)\}$, **b)** $S = \{(1, a), (2, a), (2, b)\}$, **c)** $T = \{(1, a), (2, a)\}$ kuvaus joukolta X joukkoon Y?

a) Ei ole, koska X:n alkiota 2 ei vastaa mikään Y:n alkio.

b) Ei ole, koska X:n alkiota 2 vastaa kaksi Y:n alkiota.

c) On, vaikka kahta X:n alkiota vastaa Y:n alkio a ja mikään X:n alkio ei vastaa Y:n alkiota b.



2 Kuva ja alkukuva

Merkitsemme $y = f(x)$ tarkoittamaan sitä, että $(x, y) \in f$. Siis

$$y = f(x) \Leftrightarrow (x, y) \in f.$$

Sanomme, että y on *funktion f arvo muuttujan eli argumentin arvolla x.* Sanomme myös, että y on x:n *kuva* ja x on y:n *alkukuva.* Jokaisella $x \in X$ on siis täsmälleen yksi kuva. Alkiolla $y \in Y$ voi sen sijaan olla alkukuvia yksi, useampia tai ei yhtään.

Jos f on kuvaus joukolta X joukkoon Y, niin merkitsemme

$$f\colon X \to Y \quad \text{tai} \quad X \xrightarrow{f} Y.$$

Joukko X on kuvauksen f (kuten relaation f) *määrittelyjoukko* ja Y *maalijoukko. Joukon $A \subseteq X$ kuva* $f(A)$ on A:n alkioiden kuvien joukko. Siis

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

Joukon $B \subseteq Y$ alkukuva $f^{-1}(B)$ on X:n niiden alkioiden joukko, joiden kuva kuuluu B:hen, eli B:n alkioiden alkukuvien joukko. Siis

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

Kuvauksen f (kuten relaation f) *arvojoukko* on määrittelyjoukon X alkioiden kuvien joukko eli määrittelyjoukon X kuva

$$f(X) = \{\, y \in Y \mid \exists x \in X : y = f(x) \,\} = \{\, f(x) \mid x \in X \,\}.$$

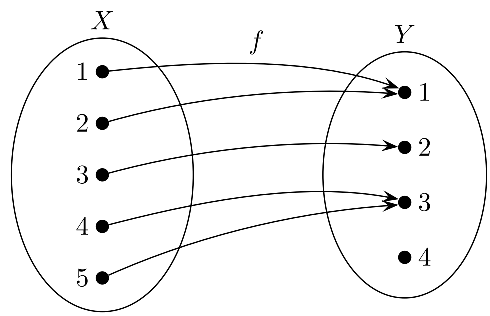
Siis aina $f(X) \subseteq Y$. Nämä joukot voivat olla samoja, mutta eivät välttämättä. Kuvauksen f määrittelyjoukkoa voidaan merkitä myös M_f:llä ja arvojoukkoa A_f:llä.

Esimerkki 95. Olkoon $X = \{1, 2, 3, 4, 5\}$, $Y = \{1, 2, 3, 4\}$ ja $f = \{(1, 1), (2, 1), (3, 2), (4, 3), (5, 3)\}$, joten meillä on kuvaus $f\colon X \to Y$. Voimme merkitä myös

$$f(1) = 1, \quad f(2) = 1, \quad f(3) = 2, \quad f(4) = 3, \quad f(5) = 3.$$

Havainnollistamme tätä kuvausta nuolikuviolla ja tutkimme eräitä kuvia ja alkukuvia. Esimerkiksi

$$f(\{1,2\}) = \{1\}, \quad f(\{1,2,3\}) = \{1,2\}, \quad f(X) = \{1,2,3\} \neq Y,$$
$$f^{-1}(\{1\}) = \{1,2\}, \quad f^{-1}(\{4\}) = \emptyset, \quad f^{-1}(\{3\}) = \{4,5\} = f^{-1}(\{3,4\}).$$



3 Lisähuomioita

Esimerkki 96. Yksinkertaisimmat kuvaukset eli funktiot ovat *identtinen kuvaus* $f\colon X \to X\colon f(x) = x$ ja *vakiokuvaus* $f\colon X \to Y\colon f(x) = y_0$, missä $y_0 \in Y$ on kiinteä.

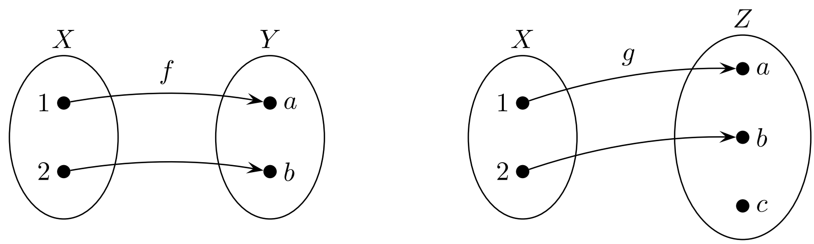
Esimerkki 97. Funktion f (kuten relaation f) *sääntö* voidaan joskus esittää analyyttisena lausekkeena, esimerkiksi $f\colon \mathbb{R} \to \mathbb{R}\colon f(x) = 2x + 3$. Niin ei kuitenkaan tarvitse välttämättä olla, jolloin saattaa olla muunlainen *algoritmi* funktion säännölle, kuten esimerkiksi *kattofunktiolla* $\lceil x \rceil =$ pienin kokonaisluku, joka $\geq x$ ja *Dirichlet'n*[1] *funktiolla* $f\colon \mathbb{R} \to \mathbb{R}\colon f(x) = 1$, kun $x \in \mathbb{Q}$, $f(x) = 0$, kun $x \in \mathbb{R} \setminus \mathbb{Q}$.

Kaikilla funktioilla ei ole algoritmilla ilmaistavaa sääntöä. Tämä johtuu siitä, että (tietyn kieliset äärelliset) algoritmit muodostavat *numeroituvan joukon* (luku 5.4), mutta esimerkiksi kaikkien funktioiden $\mathbb{R} \to \mathbb{R}$ joukko on *ylinumeroituva*. Tästäkin syystä funktion relaatiomääritelmä on hyödyllinen, sillä kysymys siitä mitä ”vastaavuus” yleisesti tarkoittaa, olisi vaikea selvittää muulla tavalla.

Kuvaukset $f\colon X \to Y$ ja $g\colon U \to V$ ovat *samat*, jos $X = U$, $Y = V$ sekä f ja g ovat tulojoukkojen osajoukkoina samat. Siksi olisi täsmällisempää määritellä kuvaus $f\colon X \to Y$ *järjestettynä kolmikkona* (X, Y, f).

Esimerkki 98. Olkoon $X = \{1,2\}$, $Y = \{a,b\}$, $Z = \{a,b,c\}$. Kuvaukset $f\colon X \to Y\colon f(1) = a,\ f(2) = b$ ja $g\colon X \to Z\colon g(1) = a,\ g(2) = b$ eivät ole samat, vaikka tulojoukkojen osajoukkoina $f = g = \{(1,a),(2,b)\}$. Nimittäin näillä kuvauksilla on eri maalijoukot.

[1] *Lejeune Dirichlet (1805–1859), ranskalainen matemaatikko.*

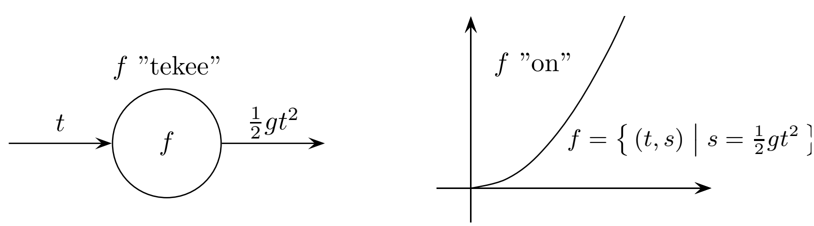


Esimerkki 99. Kuvaukset $f\colon \mathbb{R} \to \mathbb{R}\colon f(x) = 2x + 3$, $g\colon \mathbb{Z} \to \mathbb{R}\colon g(x) = 2x+3$ ja $h\colon \mathbb{Z} \to \mathbb{Z}\colon h(x) = 2x+3$ ovat kaikki eri kuvauksia, vaikka niillä on yhteinen sääntö.

Olemme aiemmin (s. 62) määritelleet *indeksoidun joukkoperheen*, joka koostuu annetun joukon X tietyistä osajoukoista niin, että indeksijoukon I jokaiseen alkioon k "liitetään" tietty joukko $A_k \subseteq X$. Tämä "liittäminen" voidaan täsmällisesti määritellä kuvauksena, joten kysymyksessä on itse asiassa kuvaus $f\colon I \to \mathcal{P}(X)$, missä $f(k) = A_k$.

Edelleen meillä on ollut aiemmin (s. 68) puhe *järjestetyn jonon* $(x_1, x_2, \ldots, x_n)$ käsitteestä. Se voidaan täsmällisesti määritellä (paitsi järjestettynä joukkona myös) kuvauksena $\{1, 2, \ldots, n\} \to X$. Vastaavasti määrittelemme *äärettömän* jonon $(x_1, x_2, \ldots)$ kuvauksena $\mathbb{Z}_+ \to X$. Tämä tapa suhtautua jonoihin tekee mahdolliseksi tulojoukon määrittelemisen silloinkin, kun joukkoja on ääretön määrä (teht. 253).

Kuvauksen relaatiomääritelmää on arvosteltu. Nimittäin sovelluksissa funktiolle on luonteenomaista tietty *dynaamisuus*. Kun esimerkiksi sanotaan, että ympyrän kehän pituus on säteen funktio, vapaasti putoavan kappaleen putoamismatka on ajan funktio tai puhelinnumero on puhelimen omistajan funktio, niin kaikissa tapauksissa funktio "tekee" tiettyä (ilmoittaa pituuden, putoamismatkan, puhelinnumeron). Relaatiomääritelmän mukainen funktio ei kuitenkaan "tee" mitään, vaan pelkästään "on". Siis funktio määritellään tällöin ikään kuin kuvaajan kautta eikä sellaisena "koneena", joka ilmoittaa $f(x)$:n, kun x on annettu.



Kuvauksen eli funktion määritelmällä ei ole kuitenkaan varsinaisesti merkitystä funktioita tutkittaessa, eikä relaatiomääritelmä estä ajattelemasta funktioita dynaamisesti. Kun relaatiomääritelmällä on saatu se etu, että asia voidaan esittää täsmällisesti, tämä määritelmä on tehnyt tehtävänsä ja voidaan periaatteessa sen jälkeen unohtaa.

4 Kuvan ja alkukuvan ominaisuuksia

Lopuksi tutkimme, miten kuva ja alkukuva käyttäytyvät joukko-opillisissa laskutoimituksissa.

Lause 26. Jos $f\colon X \to Y$ on kuvaus, $A, A_1, A_2 \subseteq X$ ja $B, B_1, B_2 \subseteq Y$, niin

(1) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$,

(2) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$,

(3) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$,

(4) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$,

(5) $A \subseteq f^{-1}\big(f(A)\big)$,

(6) $f\big(f^{-1}(B)\big) \subseteq B$.

Ominaisuuksissa (2), (5) ja (6) osajoukko voi olla aito (teht. 252).

Todistamme ominaisuudet (2) ja (3) ja jätämme muut harjoitustehtäviksi (teht. 247 ja 248).

(2) $y \in f(A_1 \cap A_2)$

$$
\begin{aligned}
&\Leftrightarrow \exists x \in A_1 \cap A_2 \colon y = f(x) && \text{(kuvan määritelmä)}\\
&\Rightarrow \exists x \in A_1 \colon y = f(x)\\
&\qquad \wedge \exists x \in A_2 \colon y = f(x) && \text{(leikkauksen määritelmä)}\\
&\Leftrightarrow y \in f(A_1) \wedge y \in f(A_2) && \text{(kuvan määritelmä)}\\
&\Leftrightarrow y \in f(A_1) \cap f(A_2) && \text{(leikkauksen määritelmä).}
\end{aligned}
$$

(3) $x \in f^{-1}(B_1 \cup B_2)$

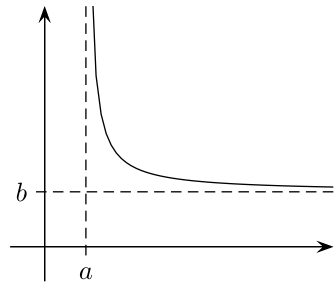
$$
\begin{aligned}
&\Leftrightarrow f(x) \in B_1 \cup B_2 && \text{(alkukuvan määritelmä)}\\
&\Leftrightarrow f(x) \in B_1 \vee f(x) \in B_2 && \text{(yhdisteen määritelmä)}\\
&\Leftrightarrow x \in f^{-1}(B_1) \vee x \in f^{-1}(B_2) && \text{(alkukuvan määritelmä)}\\
&\Leftrightarrow x \in f^{-1}(B_1) \cup f^{-1}(B_2) && \text{(yhdisteen määritelmä).}
\end{aligned}
$$

Ominaisuuden (2) todistuksen kolmannella rivillä olevan implikaation suuntaa ei voida kääntää, sillä lauseessa $\exists x \in A_1 \colon \ldots$ olevan x:n ei tarvitse olla sama kuin lauseessa $\exists x \in A_2 \colon \ldots$

Harjoitustehtäviä

241. Onko relaatio R kuvaus joukolta $X = \{1, 2, 3\}$ joukkoon $Y = \{4, 5, 6\}$, kun R on **a)** $\{(1, 4), (2, 5)\}$, **b)** $\{(1, 4), (1, 5), (2, 5), (3, 6)\}$, **c)** $\{(1, 4), (2, 4), (3, 4)\}$, **d)** $\{(1, 5), (2, 6), (3, 7)\}$?

242. **a)** Osoitettava, että alla koordinaatistossa esitetty relaatio f

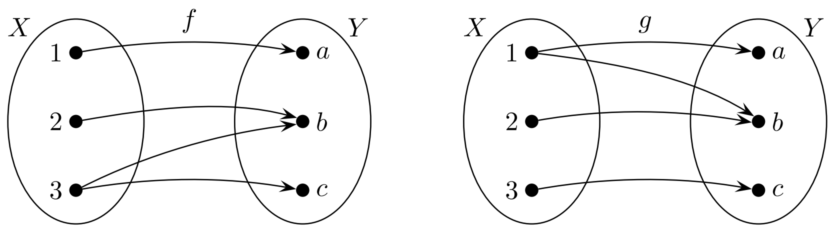


ei ole kuvaus $\mathbb{R} \to \mathbb{R}$. **b)** Muodostettava mahdollisimman laaja sellainen joukko $X \subseteq \mathbb{R}$, että f on kuvaus $X \to \mathbb{R}$. **c)** Mikä on tällöin f:n arvojoukko?

243. Olkoon X kaikkien maapallolla elävien ihmisten joukko ja Y kaikkien maapallolla elävien tai eläneiden ihmisten joukko. Onko f kuvaus $X \to Y$, kun $f(x)$ on x:n **a)** isä, **b)** äiti, **c)** vanhempi, **d)** lapsi, **e)** esikoinen?

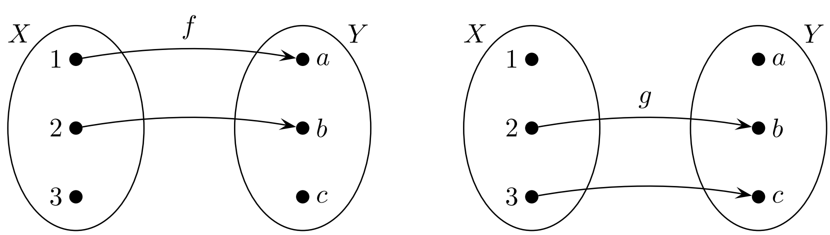
244. Olkoon $f\colon \mathbb{R} \to \mathbb{R}\colon f(x) = x^2$. Määritettävä **a)** $f([1,2])$, **b)** $f([-2,3])$, **c)** $f^{-1}(\{1\})$, **d)** $f^{-1}([0,4])$, **e)** $f^{-1}([-4,-1])$, **f)** $f^{-1}([-4,4])$, **g)** funktion f arvojoukko.

245. Olkoon $X = \{1,2,3\}$, $Y = \{a,b,c\}$. **a)** Osoitettava, että nuolikuvioiden esittämät relaatiot f ja g



eivät ole kuvauksia $X \to Y$. **b)** Saadaanko näistä relaatioista tällainen kuvaus jollakin joukko-opin laskutoimituksella?

246. Kuten edellä, mutta tarkastellaan seuraavien nuolikuvioiden relaatioita.



247. Todistettava lauseen 26 ominaisuudet (1) ja (5).

248. Todistettava lauseen 26 ominaisuudet (4) ja (6).

249. Olkoon $X = \{1, 2\}$. Muodostettava kaikki kuvaukset $f\colon X \to X$.

250. Olkoot X ja Y äärellisiä joukkoja sekä olkoon f kuvaus $X \to Y$. Millainen on relaation f matriisi?

251. Olkoot $p(x)$ ja $q(x)$ joukossa X määriteltyjä avoimia lauseita. Lauseen 26 ominaisuuksien (1)–(4) todistukset antavat aiheen kysyä, ovatko seuraavat lauseet tosia vai epätosia.

a) $\forall x \in X : p(x) \vee q(x) \Leftrightarrow \forall x \in X : p(x) \vee \forall x \in X : q(x)$,

b) $\forall x \in X : p(x) \wedge q(x) \Leftrightarrow \forall x \in X : p(x) \wedge \forall x \in X : q(x)$,

c) $\exists x \in X : p(x) \vee q(x) \Leftrightarrow \exists x \in X : p(x) \vee \exists x \in X : q(x)$,

d) $\exists x \in X : p(x) \wedge q(x) \Leftrightarrow \exists x \in X : p(x) \wedge \exists x \in X : q(x)$.

Selvitettävä tämä kysymys.

252. Kuvaus $f\colon \mathbb{Z} \to \mathbb{Z}$ määritellään

$$f(x) = \text{suurin 5:llä jaollinen kokonaisluku, joka} \leq x.$$

Mainittava jotkin sellaiset joukot $A, A_1, A_2, B \subseteq \mathbb{Z}$, että

a) $f(A_1 \cap A_2) \neq f(A_1) \cap f(A_2)$,

b) $f^{-1}\big(f(A)\big) \neq A$,

c) $f\big(f^{-1}(B)\big) \neq B$.

253. Miten määritellään joukkojen **a)** $A_1, A_2, \ldots$, **b)** A_k $(k \in I)$ tulojoukko?

254. Ovatko lauseen 26 ominaisuudet (1)–(4) voimassa, jos laskutoimitukset sovelletaan kahden joukon sijasta äärettömän monelle joukolle?

255. Olkoon $f\colon X \to Y$ kuvaus ja $A_1, A_2 \subseteq X$, $B_1, B_2 \subseteq Y$. Onko tällöin yleisesti voimassa

a) $f(A_1 \setminus A_2) = f(A_1) \setminus f(A_2)$,

b) $f^{-1}(B_1 \setminus B_2) = f^{-1}(B_1) \setminus f^{-1}(B_2)$?

256. Olkoot $f\colon X \to U$ ja $g\colon Y \to V$ kuvauksia. Osoitettava, että $h\colon X \times Y \to U \times V : h\big((x, y)\big) = \big(f(x), g(y)\big)$ on kuvaus.

257. Jatkoa. Olkoon $A \subseteq X$, $B \subseteq Y$, $C \subseteq U$, $D \subseteq V$. Onko

a) $h(A \times B) = f(A) \times g(B)$,

b) $h^{-1}(C \times D) = f^{-1}(C) \times g^{-1}(D)$

yleisesti voimassa?

258. Olkoot f_1 ja f_2 kuvauksia $X \to Y$. Osoitettava, että relaatiot $f_1 \cup f_2$ ja $f_1 \cap f_2$ eivät yleensä ole kuvauksia $X \to Y$. Voivatko nämä relaatiot itse asiassa olla koskaan kuvauksia?

259. Tarkastellaan kuvausta $f\colon X \to Y$, kun $X = \bigl\{1, 2, \{1, 2\}\bigr\}$, $Y = \{1, 2\}$, $f(1) = f(2) = 1$, $f(\{1, 2\}) = 2$. Kuvan määritelmän mukaan $f(\{1, 2\}) = \{f(1), f(2)\} = \{1\}$, mutta toisaalta kuvauksen f lain mukaan $f(\{1, 2\}) = 2$. Missä vika?

260. Olkoon $f\colon X \to Y$ kuvaus. Todistettava oikeaksi tai vääräksi

a) $f\bigl(f^{-1}(f(A))\bigr) = f(A)$ kaikilla $A \subseteq X$,

b) $f^{-1}\bigl(f(f^{-1}(B))\bigr) = f^{-1}(B)$ kaikilla $B \subseteq Y$.

5.2 Bijektio

1 Injektio, surjektio ja bijektio

Sanomme, että kuvaus $f\colon X \to Y$ on *injektio*, jos

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

eli

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Siis kuvaus on injektio, jos eri alkiot kuvautuvat eri alkioille eli maalijoukon jokainen alkio on määrittelyjoukon *korkeintaan* yhden alkion kuva.

Edelleen sanomme, että f on *surjektio*, jos $Y = f(X)$ eli

$$\forall y \in Y : \exists x \in X : y = f(x).$$

Siis kuvaus on surjektio, jos sen maalijoukko on sama kuin arvojoukko eli maalijoukon jokainen alkio on määrittelyjoukon *ainakin* yhden alkion kuva.

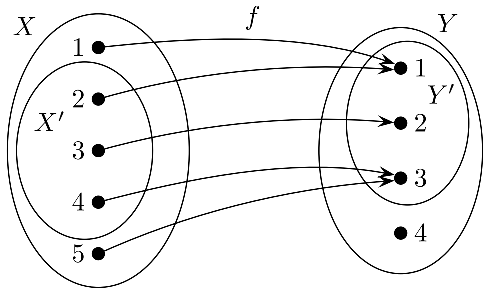
Kuvaus f on *bijektio*, jos se on sekä injektio että surjektio. Tällöin maalijoukon jokainen alkio on määrittelyjoukon *täsmälleen* yhden alkion kuva. Siis bijektiolle $f\colon X \to Y$ on

$$\forall y \in Y : \exists! x \in X : y = f(x).$$

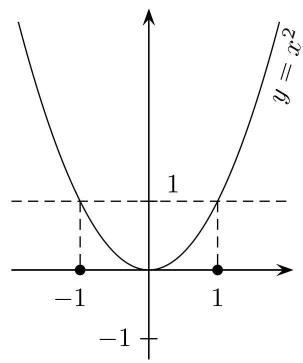
Esimerkki 100. Olkoon $X = \{1, 2, 3, 4, 5\}$, $Y = \{1, 2, 3, 4\}$. Kuvaus $f\colon X \to Y\colon f(1) = f(2) = 1$, $f(3) = 2$, $f(4) = f(5) = 3$ ei ole injektio, sillä $f(1) = f(2)$ (ja $f(4) = f(5)$). Myöskään f ei ole surjektio, sillä mikään alkio ei kuvaudu alkiolle 4.

Jos kuvaus ei ole bijektio, niin saamme bijektion pienentämällä määrittely- ja maalijoukkoa sopivasti.

Esimerkki 100, jatkoa. Voimme valita vaikkapa $X' = \{2, 3, 4\}$, $Y' = \{1, 2, 3\}$, jolloin kuvaus $f'\colon X' \to Y'\colon f'(x) = f(x)$ on bijektio.



Esimerkki 101. Funktio $f\colon \mathbb{R} \to \mathbb{R}\colon f(x) = x^2$ ei ole injektio, koska esimerkiksi $f(-1) = f(1)$ (ja yleensäkin vastalukujen kuvat ovat samat). Tämä funktio ei ole myöskään surjektio, koska se ei saa esimerkiksi arvoa -1 (eikä yleensäkään mitään negatiivista arvoa). Kuvion perusteella näyttää siltä, että poistamalla maalijoukosta negatiiviset luvut saamme surjektion. Näyttää myös siltä, että poistamalla määrittelyjoukosta (vaikkapa) negatiiviset luvut saamme injektion. Siis näyttää siltä, että kun merkitsemme $\mathbb{R}_{+0} = \mathbb{R}_+ \cup \{0\}$, niin funktio $f\colon \mathbb{R}_{+0} \to \mathbb{R}_{+0}\colon f(x) = x^2$ on bijektio. Kuvio ei kuitenkaan riitä analyyttisen väitteen perusteluksi, vaan meidän on tutkittava asiaa tarkemmin (teht. 271).



$*2$ Reaalifunktion osoittaminen bijektioksi

Nyt käsiteltävät asiat eivät oikeastaan ole diskreettiä matematiikkaa vaan analyysia, mutta on johdonmukaista tarkastella niitä tässä.

Olkoon I reaalilukuväli (joka voi olla äärellinen tai ääretön, avoin, puoliavoin tai suljettu). Välillä I määritelty reaalifunktio f on *aidosti kasvava*, jos

$$x_1 < x_2 \Rightarrow f(x_1) < f(x_2),$$

ja *aidosti vähenevä*, jos

$$x_1 < x_2 \Rightarrow f(x_1) > f(x_2).$$

Funktio f on *aidosti monotoninen*, jos se on aidosti kasvava tai aidosti vähenevä.

Lause 27. Välillä I määritelty jatkuva reaalifunktio on injektio, jos ja vain jos se on aidosti monotoninen.

Todistus. Jos. *Ol.* f on aidosti monotoninen. *Väit.* f on injektio. *Tod.* Olkoon $x_1, x_2 \in I$, $x_1 \neq x_2$. Yleisyyttä rajoittamatta voimme sopia, että $x_1 < x_2$. Tällöin $f(x_1) < f(x_2)$, jos f on aidosti kasvava, ja $f(x_1) > f(x_2)$, jos f on aidosti vähenevä. Joka tapauksessa $f(x_1) \neq f(x_2)$, joten f on injektio.

Vain jos. *Ol.* f on injektio. *Väit.* f on aidosti monotoninen. *Tod.* Teemme vastaoletuksen, että f ei ole aidosti monotoninen. Tällöin on olemassa sellaiset $x_1, x_2, x_3 \in I$, että $x_1 < x_2 < x_3$ ja joko $f(x_1) \leq f(x_2) \geq f(x_3)$ tai $f(x_1) \geq f(x_2) \leq f(x_3)$. Yksikin yhtäsuuruus kaataa injektiivisyyden, joten joko $f(x_1) < f(x_2) > f(x_3)$ tai $f(x_1) > f(x_2) < f(x_3)$.

Oletamme aluksi, että $f(x_1) < f(x_2) > f(x_3)$. Olkoon m suurempi luvuista $(f(x_1) + f(x_2))/2$ ja $(f(x_2) + f(x_3))/2$. Jatkuvana funktiona f saa välillä $]x_1, x_2[$ (ainakin) kaikki välille $]f(x_1), f(x_2)[$ kuuluvat arvot ja välillä $]x_2, x_3[$ välin $]f(x_3), f(x_2)[$ arvot. Koska m kuuluu näihin kumpaankin väliin ja koska $]x_1, x_2[\cap]x_2, x_3[= \emptyset$, niin f saa arvon m (ainakin) kahdella x:n arvolla, joten se ei ole injektio.

Jos $f(x_1) > f(x_2) < f(x_3)$, niin menettelemme muuten kuten edellä, paitsi tarkastelemme välejä $]f(x_2), f(x_1)[$ ja $]f(x_2), f(x_3)[$.

Siis kummassakin tapauksessa vastaoletus johtaa ristiriitaan oletuksen kanssa, joten se on väärä ja f on aidosti monotoninen.

Jos-suunnassa ei tarvita f:n jatkuvuutta. Sen sijaan vain jos -suunta ei ole yleisesti voimassa, mikäli jatkuvuudesta luovutaan (teht. 272).

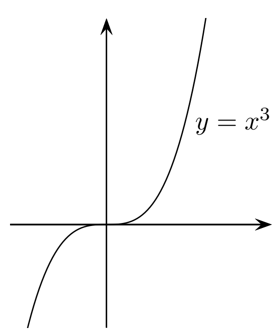
Lause 28. Jatkuva funktio $f\colon I \to \mathbb{R}$, missä I on väli, on surjektio, jos ja vain jos se saa mielivaltaisen suuria ja mielivaltaisen pieniä arvoja.

Todistus. Jos. *Ol.* f saavuttaa mielivaltaisen suuria ja pieniä arvoja. *Väit.* f on surjektio. *Tod.* Olkoon $y \in \mathbb{R}$. Oletuksen mukaan f saavuttaa jonkin y:tä suuremman arvon, olkoon se M, ja jonkin y:tä pienemmän arvon, olkoon se m. Jatkuvana funktiona f saa kaikki välin $[m, M]$ arvot, joten, koska y on tällä välillä, niin f saa myös arvon y. Siis f on surjektio.

Vain jos. *Ol.* f on surjektio. *Väit.* f saa mielivaltaisen suuria ja mielivaltaisen pieniä arvoja. *Tod.* Koska f saa *kaikki* reaaliarvot, niin väitös on triviaalisti tosi.

Vain jos -suunnassa ei tarvita f:n jatkuvuutta. Sen sijaan jos-suunta ei ole yleisesti voimassa, mikäli jatkuvuudesta luovutaan (teht. 273).

Esimerkki 102. Osoitettava, että kuvaus $f\colon \mathbb{R} \to \mathbb{R}\colon f(x) = x^3$ on bijektio.



Kuvaajan perusteella sekä injektiivisyys (x:n eri arvoja vastaavat y:n eri arvot) että surjektiivisuus (jokaista y:n arvoa vastaa tietty x:n arvo) näyttävät selviltä. Emme kuitenkaan tyydy kuvioon, vaan todistamme väitteen analyyttisesti. Menettelemme alkeellisesti käyttämällä injektion ja surjektion määritelmiä (emmekä lauseita 27 ja 28). Olkoon $x_1 \neq x_2$. Koska

$$x_1^3 - x_2^3 = (x_1 - x_2)(x_1^2 + x_1 x_2 + x_2^2)$$

ja kummatkin tulontekijät ovat $\neq 0$ (teht. 274), niin $x_1^3 \neq x_2^3$. Siis f on injektio. Olkoon nyt $y \in \mathbb{R}$ mielivaltainen. Yhtälöllä $y = x^3$ on aina ratkaisu, nimittäin $x = \sqrt[3]{y}$. (Oletamme tämän tunnetuksi. Ellemme tee niin, käytämme lausetta 28.) Siis f on surjektio ja edelleen bijektio.

Esimerkki 103. Osoitettava, että kuvaus $f\colon \mathbb{R} \to \mathbb{R}\colon f(x) = x^5 + x^3$ on bijektio.

Injektiivisyyden osoittamiseksi voisimme menetellä kuten edellä, mutta joutuisimme tekemisiin melko hankalien lausekkeiden kanssa. Surjektiivisuuden näyttämiseksi ei edellä esitetty menetelmä toimi, sillä emme voi ratkaista algebrallisesti yhtälöä $y = x^5 + x^3$, kun $y \in \mathbb{R}$ on mielivaltainen. Selviydymme kuitenkin helposti käyttämällä lauseita 27 ja 28. Koska

$$f'(x) = 5x^4 + 3x^2 \geq 0$$

ja yhtäsuuruus on voimassa vain yhdessä pisteessä $x = 0$, niin f on aidosti kasvava ja lauseen 27 mukaan injektio. Surjektiivisuus seuraa lauseen 28 mukaan siitä, että f on jatkuva, $\lim_{x\to\infty} f(x) = \infty$ ja $\lim_{x\to-\infty} f(x) = -\infty$.

Jos $f\colon X \to Y$ on surjektio, niin sanomme, että f on kuvaus jouko*lta* X jouko*lle* Y. Yleisessä tapauksessa f on kuvaus joukolta X joukk*oon* Y. Jos $R \subseteq X \times Y$, niin R on relaatio jouko*sta* X joukk*oon* Y.

Harjoitustehtäviä

261. Onko $f\colon \mathbb{R} \to \mathbb{R}$ injektio, surjektio tai bijektio, kun $f(x)$ on

a) x^5, **b)** x^6, **c)** $x^3 - x^2$, **d)** $x^3 - 3x^2 + 3x$?

262. Sama kysymys, kun $f(x)$ on

a) $\sin x$, **b)** $x + \sin x$, **c)** e^x, **d)** $\ln x$.

263. Määritettävä jotkin sellaiset mahdollisimman laajat joukot $X, Y \subseteq \mathbb{R}$, että $f\colon X \to Y$ on bijektio, kun $f(x)$ on **a)** $\sin x$, **b)** $\tan x$.

264. Olkoon $p\mathbb{N} = \{\, pn \mid n \in \mathbb{N} \,\}$. Osoitettava, että kuvaus **a)** $f\colon 3\mathbb{N} \to 5\mathbb{N}\colon f(n) = (5/3)n$, **b)** $f\colon 3\mathbb{N}\setminus\{0, 3\} \to 5\mathbb{N}\colon f(n) = 5(n-6)/3$ on bijektio.

265. Jatkoa. Miksi alkiot 0 ja 3 täytyy b-kohdassa poistaa f:n määrittelyjoukosta?

266. Muodostettava kaikki **a)** injektiot $\{1, 2\} \to \{a, b, c\}$, **b)** surjektiot $\{1, 2, 3\} \to \{a, b\}$, **c)** bijektiot $\{1, 2, 3\} \to \{a, b, c\}$.

267. Olkoon $f\colon X \to X$ kuvaus, missä X on äärellinen joukko. Osoitettava, että seuraavat ehdot ovat yhtäpitäviä: (1) f on injektio, (2) f on surjektio, (3) f on bijektio.

268. Olkoon $f\colon X \to Y$ kuvaus. Osoitettava, että kuvaus $g\colon X \to f(X)\colon g(x) = f(x)$ on surjektio.

269. Olkoot funktiot f ja g bijektioita $\mathbb{R} \to \mathbb{R}$. **a)** Osoitettava, että funktio $h\colon \mathbb{R} \to \mathbb{R}\colon h(x) = f(x) + g(x)$ ei välttämättä ole bijektio. **b)** Millä funktioita f ja g koskevalla lisäoletuksella se on bijektio?

270. Olkoot X ja Y äärellisiä joukkoja sekä olkoon f **a)** injektio, **b)** surjektio, **c)** bijektio $X \to Y$. Millainen on relaation f matriisi?

271. Todistettava, että funktio $f\colon \mathbb{R}_{+0} \to \mathbb{R}_{+0}\colon f(x) = x^2$ on bijektio.

272. Mainittava jokin injektio $\mathbb{R} \to \mathbb{R}$, joka ei ole aidosti monotoninen.

273. Mainittava jokin funktio $f\colon \mathbb{R} \to \mathbb{R}$, jolle $\lim_{x\to\infty} f(x) = \infty$ ja $\lim_{x\to-\infty} f(x) = -\infty$, mutta joka ei ole surjektio.

274. Olkoon $x_1, x_2 \in \mathbb{R}$. Todistettava: Jos $x_1 \neq x_2$, niin $x_1^2 + x_1x_2 + x_2^2 > 0$.

275. **a)** Osoitettava, että tehtävässä 252 (s. 113) määritelty kuvaus $f\colon \mathbb{Z} \to \mathbb{Z}$:

$$f(x) = \text{suurin 5:llä jaollinen kokonaisluku, joka} \leq x$$

ei ole injektio eikä surjektio. **b)** Määritettävä jotkin sellaiset mahdollisimman laajat joukot $X, Y \subseteq \mathbb{R}$, että kuvaus $g\colon X \to Y\colon g(x) = f(x)$ on bijektio.

276. Todistettava: Kuvaus $f\colon X \to Y$ on injektio, jos ja vain jos kaikilla $A_1, A_2 \subseteq X$ on

$$f(A_1 \cap A_2) = f(A_1) \cap f(A_2).$$

277. Todistettava: Kuvaus $f\colon X \to Y$ on injektio, jos ja vain jos kaikilla $A \subseteq X$ on

$$f^{-1}\big(f(A)\big) = A.$$

278. Todistettava: Kuvaus $f\colon X \to Y$ on surjektio, jos ja vain jos kaikilla $B \subseteq Y$ on

$$f\big(f^{-1}(B)\big) = B.$$

279. Olkoot X ja Y joukkoja sekä $X \subseteq Y$. *Luonnollinen injektio* eli joukon X *upotuskuvaus* joukkoon Y on kuvaus $i\colon X \to Y\colon i(x) = x$. Osoitettava, että i on injektio.

280. Olkoon joukossa X määritelty luokkajako $\{A_k\}_{k\in I} = Y$. Kun $x \in X$, tarkoittakoon A_{k_x} sitä Y:n joukkoa, joka sisältää x:n. *Luonnollinen surjektio* on kuvaus $\pi\colon X \to Y\colon \pi(x) = A_{k_x}$. Osoitettava, että π on **a)** todellakin kuvaus, **b)** surjektio.

5.3 Käänteiskuvaus ja yhdistetty kuvaus

1 Käänteiskuvaus

Olkoon $f\colon X \to Y$ kuvaus, jolloin

$$f = \{\, (x,y) \in X \times Y \mid y = f(x) \,\}.$$

Relaatiolla f on aina käänteisrelaatio

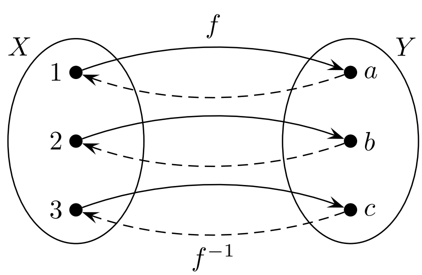
$$f^{-1} = \{\, (y,x) \in Y \times X \mid y = f(x) \,\},$$

mutta se ei välttämättä ole kuvaus, vaikka f on kuvaus. Jos f on bijektio, niin jokaista $y \in Y$ vastaa täsmälleen yksi sellainen $x \in X$, että $y = f(x)$. Siis tällöin f^{-1} on kuvaus, vieläpä bijektio. Kutsumme sitä f:n *käänteiskuvaukseksi*. Bijektion $f\colon X \to Y$ käänteiskuvaus on siis $f^{-1}\colon Y \to X$ ja

$$y = f(x) \Leftrightarrow x = f^{-1}(y).$$

Merkintöjen samanlaisuudesta huolimatta käänteiskuvausta ei saa sekoittaa alkukuvaan. Jos $f\colon X \to Y$ on *mielivaltainen kuvaus* ja $B \subseteq Y$, niin $f^{-1}(B)$ on X:n tietty osajoukko. Kuvaus f^{-1} ei kuitenkaan välttämättä ole olemassa (mutta käänteisrelaatio f^{-1} on). Jos taas f on *bijektio*, niin kuvaus f^{-1} on olemassa ja $f^{-1}(B)$ merkityksessä ”joukon B alkukuva kuvauksessa f” on sama kuin $f^{-1}(B)$ merkityksessä ”joukon B kuva kuvauksessa f^{-1}”.

Esimerkki 104. Olkoon $X = \{1,2,3\}$, $Y = \{a,b,c\}$ ja $f\colon X \to Y$ kuvaus, jonka sääntö on $f(1) = a$, $f(2) = b$, $f(3) = c$. Kuvaus f on bijektio, ja käänteiskuvauksen $f^{-1}\colon Y \to X$ sääntö on $f^{-1}(a) = 1$, $f^{-1}(b) = 2$, $f^{-1}(c) = 3$.



Analyysissa määritellään eräitä funktioita tiettyjen funktioiden käänteisfunktioina.

Esimerkki 105. Funktio $f\colon \mathbb{R}_{+0} \to \mathbb{R}_{+0}\colon f(x) = x^n$, missä $\mathbb{R}_{+0} = \mathbb{R}_+ \cup \{0\}$ ja $n \in \mathbb{Z}_+$, on bijektio. Sen käänteisfunktio on $f^{-1}\colon \mathbb{R}_{+0} \to \mathbb{R}_{+0}\colon f^{-1}(y) = \sqrt[n]{y}$. Toisin sanoen, kun $x \geq 0$, niin

$$y = x^n \Leftrightarrow x = \sqrt[n]{y}.$$

Käänteiskuvauksenkin muuttujaa voidaan haluttaessa merkitä x:llä. Voidaan siis myös kirjoittaa $f^{-1}(x) = \sqrt[n]{x}$.

Esimerkki 106. Funktio $f\colon \mathbb{R} \to \mathbb{R}_+ \colon f(x) = \mathrm{e}^x$ on bijektio, jonka käänteisfunktio on $f^{-1}\colon \mathbb{R}_+ \to \mathbb{R}\colon f^{-1}(y) = \ln y$. Toisin sanoen

$$y = \mathrm{e}^x \Leftrightarrow x = \ln y.$$

Esimerkki 107. Funktiot

$$\begin{aligned} &s\colon [-\pi/2, \pi/2] \to [-1,1]\colon s(x) = \sin x,\\ &c\colon [0,\pi] \to [-1,1]\colon c(x) = \cos x,\\ &t\colon\ ]-\pi/2, \pi/2[\to \mathbb{R}\colon t(x) = \tan x \end{aligned}$$

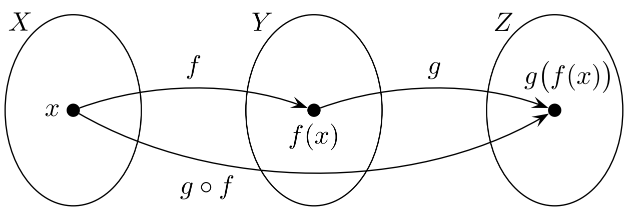
ovat bijektioita. Niiden käänteisfunktiot ovat *syklometriset funktiot* eli *arkusfunktiot* $s^{-1} = \arcsin$, $c^{-1} = \arccos$, $t^{-1} = \arctan$.

2 Yhdistetty kuvaus

Kuvausten $f\colon X \to Y$ ja $g\colon Y \to Z$ *yhdistetty kuvaus* eli *kuvaustulo* on kuvaus $g \circ f\colon X \to Z$, jonka sääntö on

$$(g \circ f)(x) = g\bigl(f(x)\bigr).$$

Siis $(g \circ f)(x)$ saadaan niin, että alkioon x sovelletaan *ensin* kuvaus f ja tulokseen $f(x)$ *sitten* kuvaus g.



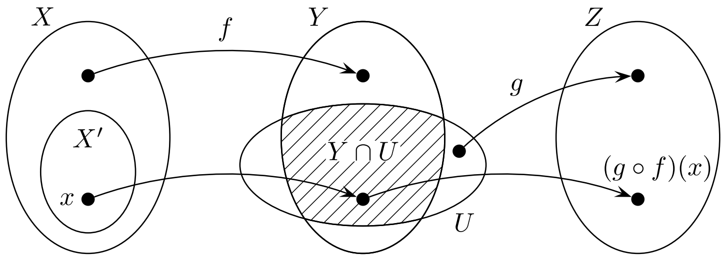
Kuvausten yhdistämisen merkintä on ristiriidassa relaatioiden yhdistämismerkinnän (s. 76) kanssa, koska relaatioiden f ja g yhdistettyä relaatiota merkitään $f \circ g$. Ristiriidan syynä on merkinnän $f(x)$ "takaperoisuus": vaikka meillä on *ensin* alkio x, johon *sitten* sovelletaan kuvaus f, niin kirjoittamisjärjestys on päinvastainen: ensin f, sitten x. Se, että $y = f(x)$, tarkoittaa relaatiossa oloa $x\ f\ y$, jolloin jälkimmäisessä merkinnässä järjestys on "oikea". Näin olisi parempi käyttää merkinnän $y = f(x)$ sijasta merkintää $y = (x)f$, jolloin voisimme merkitä $(x)(f \circ g) = ((x)f)g$ ja käyttää f:n ja g:n kuvaustulolle yhdistetyn relaation merkintää $f \circ g$. Tämä sopisi yhteen suoritusjärjestyksen "ensin f, sitten g" kanssa. Merkintä $f(x)$, jonka otti käyttöön Euler[2], johtuu pelkästään historiallisista syistä.

Eräät kirjoittajat käyttävätkin merkintää $(x)f$, mutta enemmistö on pysynyt vanhassa merkinnässä $f(x)$, joten vanhoillisuus näyttää menneen johdonmukaisuuden edelle. Me liitymme tähän enemmistöön, joten meidän on valitettavasti käytettävä kuvausten f ja g yhdistetylle kuvaukselle

[2] *Leonhard Euler (1707–1783), sveitsiläinen matemaatikko.*

merkintää $g \circ f$, vaikka käytämme relaatioiden f ja g yhdistetylle relaatiolle merkintää $f \circ g$.

Jotta kuvaukset f ja g voitaisiin yhdistää, niin f:n maalijoukon täytyy määritelmän mukaan olla sama kuin g:n määrittelyjoukko. Koska maalijoukot eivät useinkaan ole mielenkiintoisia ja niitä voidaan tarvittaessa muuttaa upotuskuvauksella (teht. 295), on syytä sallia kuvausten yhdistäminen silloinkin kun f:n maalijoukko ei ole g:n määrittelyjoukko, mutta näillä joukoilla on yhteisiä alkioita (vrt. relaatioiden yhdistäminen s. 78). Tarkastelemme siis kuvauksia $f\colon X \to Y$ ja $g\colon U \to Z$, missä $Y \cap U \neq \emptyset$. Merkitsemme $X' = \{\, x \in X \mid f(x) \in U \,\}$ ja määrittelemme yhdistetyn kuvauksen $g \circ f\colon X' \to Z$ niin, että $(g \circ f)(x) = g\bigl(f(x)\bigr)$.



Seuraavissa esimerkeissä meitä kiinnostavat vain funktioiden lait, joten jätämme määrittely- ja maalijoukkojen miettimisen harjoitustehtäväksi (teht. 289).

Esimerkki 108. Olkoon $f(x) = \sin x$, $g(x) = x^2$. Tällöin $(g \circ f)(x) = g(\sin x) = (\sin x)^2$ ja $(f \circ g)(x) = f(x^2) = \sin x^2$. Edelleen $(f \circ f)(x) = \sin \sin x$ ja $(g \circ g)(x) = (x^2)^2 = x^4$.

Vastaavasti määrittelemme useamman kuin kahden kuvauksen yhdistämisen. Kuvausten

$$\begin{aligned} &f_1\colon X_0 \to X_1,\\ &f_2\colon X_1 \to X_2,\\ &\ \vdots\\ &f_n\colon X_{n-1} \to X_n \end{aligned}$$

yhdistetty kuvaus eli kuvaustulo on kuvaus $f_n \circ \cdots \circ f_1\colon X_0 \to X_n$, jonka sääntö on

$$(f_n \circ \cdots \circ f_1)(x) = f_n\bigl(f_{n-1}(\ldots(f_2(f_1(x)))\ldots)\bigr).$$

Esimerkki 109. Olkoon $f(x) = \sqrt{x}$, $g(x) = \mathrm{e}^x + x$, $h(x) = 1/(x+2)$. Tällöin

$$\begin{aligned} (h \circ g \circ f)(x) &= h\bigl(g(f(x))\bigr)\\ &= h\bigl(g(\sqrt{x}\,)\bigr) = h\bigl(\mathrm{e}^{\sqrt{x}} + \sqrt{x}\,\bigr) = \frac{1}{\mathrm{e}^{\sqrt{x}} + \sqrt{x} + 2}. \end{aligned}$$

Esimerkin 108 perusteella kuvaustulo ei noudata vaihdantalakia. Sen sijaan se noudattaa liitäntälakia, sillä lauseen 14 (s. 78) mukaan relaatioiden yhdistäminen noudattaa tätä lakia. Todistamme sen vielä erikseen kuvauksille. Koska

$$\big(h \circ (g \circ f)\big)(x) = h\big((g \circ f)(x)\big) = h\big(g(f(x))\big) = (h \circ g \circ f)(x)$$

ja

$$\big((h \circ g) \circ f\big)(x) = (h \circ g)\big(f(x)\big) = h\big(g(f(x))\big) = (h \circ g \circ f)(x),$$

niin

$$h \circ (g \circ f) = (h \circ g) \circ f = h \circ g \circ f.$$

Harjoitustehtäviä

281. Osoitettava, että funktio $f\colon \mathbb{R} \to \mathbb{R}$ on bijektio, ja määritettävä sen käänteisfunktio, kun $f(x)$ on **a)** $2x$, **b)** $3x + 4$, **c)** $ax + b$ $(a \neq 0)$.

282. Muodostettava tehtävässä 264b (s. 117) määritellyn bijektion $f\colon 3\mathbb{N} \setminus \{0, 3\} \to 5\mathbb{N}\colon f(n) = 5(n-6)/3$ käänteiskuvaus.

283. Olkoon $X = [-2, \infty[$ ja $Y = [1, \infty[$. Osoitettava, että funktio

$$f\colon X \to Y\colon f(x) = x^2 + 4x + 5$$

on bijektio, ja määritettävä sen käänteisfunktio.

284. Piirrettävä samaan koordinaatistoon edellisen tehtävän funktioiden f ja f^{-1} kuvaajat. Mikä yleinen ominaisuus on funktion ja käänteisfunktion kuvaajilla toisiinsa nähden?

285. Mainittava jokin bijektio $f\colon \mathbb{R} \to \mathbb{R}$, jolle $f^{-1} = f$.

286. Olkoon $f\colon X \to Y$ bijektio. Osoitettava, että $(f^{-1})^{-1} = f$.

287. Piirrettävä trigonometristen ja syklometristen funktioiden kuvaajat.

288. Määritettävä $f \circ g$ ja $g \circ f$, kun funktioiden $f\colon \mathbb{R} \to \mathbb{R}$ ja $g\colon \mathbb{R} \to \mathbb{R}$ lait ovat **a)** $f(x) = 2x$, $g(x) = 3x$, **b)** $f(x) = x^2$, $g(x) = x^3$, **c)** $f(x) = mx$, $g(x) = nx$, **d)** $f(x) = x^m$, $g(x) = x^n$.

289. Muodostettava jotkin järkevät määrittely- ja maalijoukot esimerkkien 108 ja 109 funktioille.

290. Olkoon $f(x) = 1/(1+x)$, $g(x) = 1/(1-x)$. Muodostettava funktion $f \circ g - g \circ f$ sääntö. (Siis mitä on $(f \circ g)(x) - (g \circ f)(x)$?) Tutkittava määrittelyjoukkoja.

291. Olkoon X $(\neq \emptyset)$ joukko. Olkoon F kaikkien kuvausten $X \to X$ ja B kaikkien bijektioiden $X \to X$ joukko ja i identtinen kuvaus $X \to X$.

Todistettava: **a)** Kaikilla $f \in F$ on

$$f \circ i = i \circ f = f.$$

b) Kaikilla $f, g \in B$ on

(1) $f^{-1} \circ f = f \circ f^{-1} = i$, (2) $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

292. Ovatko edellisen tehtävän tulokset voimassa, jos kuvausten sijasta tarkastellaan yleisiä relaatioita?

293. Olkoot f ja g bijektioita $X \to X$. Osoitettava, että on olemassa bijektiot u ja $v \colon X \to X$, joille $f \circ u = g$ ja $v \circ f = g$.

294. Tarkastellaan kuvausta $f \colon \mathbb{R}^2 \to \mathbb{R}^2 \colon f(x, y) = (x+y, x-y)$. **a)** Onko f bijektio? **b)** Muodostettava $f \circ f$. **c)** Onko $f \circ f$ bijektio?

295. Olkoon $f \colon X \to Y$ kuvaus ja $\emptyset \neq Y \subseteq Z$. Todistettava: On olemassa sellainen kuvaus $g \colon Y \to Z$, että kuvauksen $h = g \circ f \colon X \to Z$ sääntö on $h(x) = f(x)$.

296. Olkoot $f \colon X \to Y$ ja $g \colon Y \to Z$ bijektioita. Osoitettava, että $g \circ f$ on bijektio. Onko näin myös joillakin lievemmillä oletuksilla?

297. Olkoot $f \colon X \to Y$ ja $g \colon Y \to X$ kuvauksia. Todistettava: Jos $g \circ f = i$ (joukon X identtinen kuvaus), niin f on injektio ja g surjektio.

298. Todistettava: Jos tehtävän 297 oletuksilla myös $f \circ g = i$ (i tarkoittaa nyt joukon Y identtistä kuvausta), niin f ja g ovat bijektioita ja $g = f^{-1}$.

299. Olkoot X ja Y joukkoja sekä $f \colon X \to Y$ kuvaus. Osoitettava, että f voidaan esittää muodossa

$$f = i \circ g \circ \pi,$$

missä i on eräs luonnollinen injektio (teht. 279), π eräs luonnollinen surjektio (teht. 280) ja g eräs bijektio. Ohje: Tutki ekvivalenssirelaation $x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2)$ ekvivalenssiluokkia ja määrittele π niin, että alkio kuvautuu ekvivalenssiluokalleen.

300. Olkoon $X = \{1, 2, 3, 4, 5\}$, $Y = \{1, 2, 3, 4\}$, $f \colon X \to Y \colon f(1) = f(2) = 1$, $f(3) = 2$, $f(4) = f(5) = 3$. Muodostettava tehtävässä 299 mainitut kuvaukset i, g, π.

5.4 Mahtavuudet. Numeroituvat joukot

1 Mahtavuudet

Jos meidän on perusteltava, että joukossa $A = \{a, b, c\}$ on yhtä monta alkiota kuin joukossa $B = \{d, e, f\}$, niin laskemme tietenkin alkiot ja huomaamme, että kummassakin niitä on kolme. Voimme perustella tämän myös laskematta alkioiden lukumäärää, sillä lukumäärien *vertailu* on alkeellisempi toimitus kuin lukumäärien *laskeminen*. Tällöin asetamme joukkojen A ja B alkiot ”vastaamaan toisiaan” eli muodostamme bijektion $g\colon A \to B$ esimerkiksi niin, että $g(a) = d$, $g(b) = e$, $g(c) = f$.

Yleisesti sanomme, että joukot A ja B ovat keskenään *yhtä mahtavia* eli niihin liittyy *sama kardinaaliluku*, jos on olemassa bijektio joukolta A joukolle B. Merkitsemme tällöin $A \sim B$. On vielä sovittava erikseen (miksi?), että $\emptyset \sim \emptyset$. Käytämme siis samaa merkintää kuin ekvivalenssirelaatiolle, joten on odotettavissa, että *mahtavuuksien yhtäsuuruus* on ekvivalenssi.

Lause 29. Olkoon X perusjoukko. Mahtavuuksien yhtäsuuruus on ekvivalenssirelaatio joukossa $\mathcal{P}(X)$.

Todistus. Refleksiivisyys. Olkoon $A \subseteq X$. Jos $A \neq \emptyset$, niin identtinen kuvaus $i\colon A \to A$ on bijektio, joten $A \sim A$. Jos taas $A = \emptyset$, niin tekemämme sopimuksen mukaan $A \sim A$.

Symmetrisyys. Olkoon $A, B \subseteq X$ ja $A \sim B$. Jos $A = \emptyset$, niin täytyy olla myös $B = \emptyset$, joten $B \sim A$. Jos taas $A \neq \emptyset$, niin on olemassa bijektio $f\colon A \to B$. Tällöin myös käänteiskuvaus $f^{-1}\colon B \to A$ on bijektio, joten $B \sim A$.

Transitiivisuus. Olkoon $A, B, C \subseteq X$. Jos $A \sim B$ ja $B \sim C$ sekä $A, B, C \neq \emptyset$, niin on olemassa bijektiot $f\colon A \to B$ ja $g\colon B \to C$, jolloin yhdistetty kuvaus $g \circ f\colon A \to C$ on bijektio (teht. 296), ja täten $A \sim C$. Jos taas A, B tai C on tyhjä, niin täytyy olla $A = B = C = \emptyset$, joten silloinkin $A \sim C$.

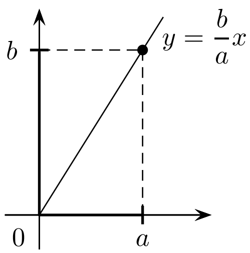
Sanomme, että joukko A on *äärellinen*, jos $A = \emptyset$ tai $A \sim \{1, 2, \ldots, n\}$ jollakin $n \in \mathbb{Z}_+$. Muussa tapauksessa A on *ääretön*.

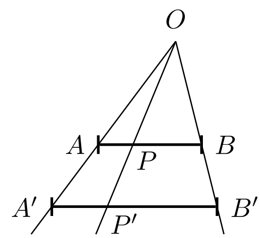
Esimerkki 110. Luonnollisten lukujen joukko $\mathbb{N}$ ja parillisten luonnollisten lukujen joukko $2\mathbb{N} = \{0, 2, 4, 6, \ldots\}$ ovat keskenään yhtä mahtavia. Kuvaus $f\colon \mathbb{N} \to 2\mathbb{N}\colon f(n) = 2n$ on nimittäin bijektio. Huomaamme vastaavuuden myös kirjoittamalla näiden joukkojen alkiot vastaamaan toisiaan.

$$\begin{aligned} \mathbb{N}\colon&\ 0,\ 1,\ 2,\ 3, \ldots,\ \ n, \ldots \\ 2\mathbb{N}\colon&\ 0,\ 2,\ 4,\ 6, \ldots,\ 2n, \ldots \end{aligned}$$

Luonnollisia lukuja on siis tavallaan ”yhtä monta” kuin parillisia luonnollisia lukuja. Äärettömyyteen liittyvät ongelmat, joista tämä on yksi, askarruttivat jo antiikin kreikkalaisia, joiden mielestä kokonaisuus oli aina osiansa ”suurempi”. Me selviydymme tästä toteamalla, että selitys on joukon $\mathbb{N}$ äärettömyydessä: vain äärellisille joukoille mahtavuuksien yhtäsuuruus vastaa täysin meidän intuitiivista ”yhtä monen” käsitettämme. Jokainen ääretön joukko on yhtä mahtava jonkin aidon osajoukkonsa kanssa.

Esimerkki 111. Kaikki janat ovat keskenään yhtä mahtavia pistejoukkoja. Toisin sanoen kaikki suljetut reaalilukuvälit ovat keskenään yhtä mahtavia. Todistukseksi riittää tutkia (miksi?) välejä $[0, a]$ ja $[0, b]$. Kuvaus $f\colon [0, a] \to [0, b]\colon f(x) = bx/a$ on bijektio, joten $[0, a] \sim [0, b]$. Ks. vasemmanpuoleinen kuvio. Voimme perustella tämän väitteen myös geometrisesti. Oikeanpuoleisen kuvion konstruktio määrittelee janojen AB ja $A'B'$ välisen bijektion $f(P) = P'$.





Määrittelemme vielä, että joukon A mahtavuus on *pienempi tai yhtäsuuri* kuin joukon B mahtavuus, jos A on yhtä mahtava B:n jonkin osajoukon kanssa. Sanomme myös, että B:n mahtavuus on silloin *suurempi tai yhtäsuuri* kuin A:n, ja merkitsemme $A \precsim B$ tai $B \succsim A$. On helppo huomata, että $A \precsim B$, jos ja vain jos $A = \emptyset$ tai on olemassa injektio A:lta B:hen, mikä on edelleen yhtäpitävää sen kanssa, että $A = \emptyset$ tai on olemassa surjektio B:ltä A:lle. Ks. teht. 309.

Lause 30. Olkoon X perusjoukko. Mahtavuuksien pienempi tai yhtäsuuri -relaatio määriteltynä tehtävän 235 (s. 104) mukaisesti on järjestysrelaatio ekvivalenssiluokkien joukossa $\mathcal{P}(X)/{\sim}$, missä $\sim$ tarkoittaa mahtavuuksien yhtäsuuruusrelaatiota. Toisin sanoen

(r) $A \precsim A$ kaikilla $A \in \mathcal{P}(X)$,

(as) $A \precsim B \wedge B \precsim A \Rightarrow A \sim B$,

(t) $A \precsim B \wedge B \precsim C \Rightarrow A \precsim C$,

(v) $A \precsim B \vee B \precsim A$ kaikilla $A, B \in \mathcal{P}(X)$.

Todistus. Refleksiivisyys. Olkoon $A \subseteq X$. Koska $A \sim A$ ja $A \subseteq A$, niin $A \precsim A$.

Transitiivisuus. Olkoon $A, B, C \subseteq X$. Jos $A \precsim B$ ja $B \precsim C$ sekä $A \neq \emptyset$, niin on olemassa injektiot $f\colon A \to B$ ja $g\colon B \to C$. Tällöin yhdistetty kuvaus $g \circ f\colon A \to C$ on injektio, joten $A \precsim C$. Jos taas $A = \emptyset$, niin $A \subseteq C$, joten silloinkin $A \precsim C$.

Antisymmetrisyyden ja vertailullisuuden todistukset ovat vaikeahkoja ja sivuutamme ne. Ks. esim. Enderton [3], Jech [8]. Lausetta, jonka mukaan antisymmetrisyys on voimassa, kutsutaan *Schröderin*[3]*–Bernsteinin*[4] *lauseeksi*.

Jos $A \precsim B$, mutta ei ole $A \sim B$, niin A:n mahtavuus on *pienempi* kuin B:n eli B:n mahtavuus on *suurempi* kuin A:n, jolloin merkitsemme $A \prec B$ tai $B \succ A$.

Esimerkki 112. Olkoon $A_n = \{1, 2, \ldots, n\}$, $n = 1, 2, 3, \ldots$ Tällöin $A_k \prec A_m$, jos ja vain jos $k < m$, ja jokainen joukko A_n on äärellinen, joten

$$\emptyset \prec A_1 \prec A_2 \prec A_3 \prec \cdots \prec \mathbb{N}.$$

2 Numeroituvat joukot

Joukko, joka on äärellinen tai yhtä mahtava luonnollisten lukujen joukon kanssa, on *numeroituva*. Numeroituvan joukon alkiot voidaan luetella.

Lause 31. Kokonaislukujen joukko on numeroituva.

Todistus. Kirjoitamme joukkojen $\mathbb{N}$ ja $\mathbb{Z}$ alkiot vastaamaan toisiaan.

$$\begin{array}{lccccl} \mathbb{N}: & 0, & 1, & 2, & 3, & 4, \ldots \\ \mathbb{Z}: & 0, & 1, & -1, & 2, & -2, \ldots \end{array}$$

Tämän vastaavuuden määrittelee bijektio $f\colon \mathbb{N} \to \mathbb{Z}$:

$$f(n) = \begin{cases} (n+1)/2, & \text{kun } n \text{ on pariton,} \\ -n/2, & \text{kun } n \text{ on parillinen.} \end{cases}$$

Rationaalilukujen joukko on lukusuoralla ”tiheässä”, joten sen numeroituvuus tuntuu uskomattomalta. Niin kuitenkin on.

Lause 32. Rationaalilukujen joukko on numeroituva.

Todistus. Riittää tarkastella joukkoa $\mathbb{Q}_+$, sillä sen numeroituvuudesta seuraa $\mathbb{Q}$:n numeroituvuus. Jos näet $\mathbb{Q}_+ = \{q_1, q_2, q_3, \ldots\}$ niin $\mathbb{Q} = \mathbb{Q}_- \cup \{0\} \cup \mathbb{Q}_+ = \{0, q_1, -q_1, q_2, -q_2, \ldots\}$.

[3] *Ernst Schröder (1841–1902), saksalainen matemaatikko ja loogikko.*
[4] *Felix Bernstein (1878–1956), saksalainen matemaatikko.*

Tapa 1. Muodostamme seuraavan taulukon, jossa jokaisella $\mathbb{Q}_+$:n alkiolla on oma paikkansa (itse asiassa äärettömän monta paikkaa).

$$
\begin{array}{cccccccccccc}
1 & \to & 2 & & 3 & \to & 4 & & 5 & \to & 6 & \dots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \\
1/2 & & 2/2 & & 3/2 & & 4/2 & & 5/2 & & 6/2 & \dots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & & & \\
1/3 & & 2/3 & & 3/3 & & 4/3 & & 5/3 & & 6/3 & \dots \\
 & \swarrow & & \nearrow & & \swarrow & & & & & & \\
1/4 & & 2/4 & & 3/4 & & 4/4 & & 5/4 & & 6/4 & \dots \\
\downarrow & \nearrow & & \swarrow & & & & & & & & \\
1/5 & & 2/5 & & 3/5 & & 4/5 & & 5/5 & & 6/5 & \dots \\
 & \swarrow & & & & & & & & & & \\
1/6 & & 2/6 & & 3/6 & & 4/6 & & 5/6 & & 6/6 & \dots \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & \ddots
\end{array}
$$

Järjestämme taulukon luvut jonoon nuolten osoittamalla tavalla. Jos kohdattu luku on jo jonossa, niin sivuutamme sen. Saamme jonon

$$1,\ 2,\ \frac{1}{2},\ \frac{1}{3},\ 3,\ 4,\ \frac{3}{2},\ \frac{2}{3},\ \frac{1}{4},\ \frac{1}{5},\ 5,\ 6,\ \frac{5}{2},\ \frac{4}{3},\ \frac{3}{4},\ \frac{2}{5},\ \frac{1}{6},\dots,$$

jossa jokainen $\mathbb{Q}_+$:n alkio esiintyy täsmälleen kerran. Siis $\mathbb{Q}_+ \sim \mathbb{N}$.

Tapa 2. Voimme edetä myös seuraavien nuolten mukaan.

$$
\begin{array}{cccccccccccc}
1 & & 2 & & 3 & & 4 & & 5 & & 6 & \dots \\
 & \nearrow & & \nearrow & & \nearrow & & \nearrow & & \nearrow & & \\
1/2 & & 2/2 & & 3/2 & & 4/2 & & 5/2 & & 6/2 & \dots \\
 & \nearrow & & \nearrow & & \nearrow & & \nearrow & & & & \\
1/3 & & 2/3 & & 3/3 & & 4/3 & & 5/3 & & 6/3 & \dots \\
 & \nearrow & & \nearrow & & \nearrow & & & & & & \\
1/4 & & 2/4 & & 3/4 & & 4/4 & & 5/4 & & 6/4 & \dots \\
 & \nearrow & & \nearrow & & & & & & & & \\
1/5 & & 2/5 & & 3/5 & & 4/5 & & 5/5 & & 6/5 & \dots \\
 & \nearrow & & & & & & & & & & \\
1/6 & & 2/6 & & 3/6 & & 4/6 & & 5/6 & & 6/6 & \dots \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & \ddots
\end{array}
$$

Tällöin saamme jonon

$$1,\ \frac{1}{2},\ 2,\ \frac{1}{3},\ 3,\ \frac{1}{4},\ \frac{2}{3},\ \frac{3}{2},\ 4,\ \frac{1}{5},\ 5,\ \frac{1}{6},\ \frac{2}{5},\ \frac{3}{4},\ \frac{4}{3},\ \frac{5}{2},\ 6,\dots$$

Tapa 3. Kuvaus $f\colon \mathbb{Q}_+ \to \mathbb{N}\colon f(\frac{m}{n}) = 2^m 3^n$, missä $\mathrm{syt}(m,n) = 1$, on injektio (teht. 308), joten $\mathbb{Q}_+ \precsim \mathbb{N}$. Myös kuvaus $g\colon \mathbb{N} \to \mathbb{Q}_+\colon g(x) = x+1$ on injektio, joten $\mathbb{N} \precsim \mathbb{Q}_+$. Relaation $\precsim$ antisymmetrisyydestä seuraa nyt, että $\mathbb{Q}_+ \sim \mathbb{N}$.

3 Ylinumeroituvat joukot

Joukon $\mathbb{Q}$ numeroituvuus saattaa houkutella otaksumaan, että kaikki joukot ovat numeroituvia. Näin ei kuitenkaan ole, vaan on olemassa *ylinumeroituvia* joukkoja, joiden mahtavuus on suurempi kuin joukon $\mathbb{N}$ mahtavuus.

Lause 33. Reaalilukujen joukko on ylinumeroituva.

Todistus. Riittää tarkastella väliä $I =]0,1]$, sillä $]0,1[\preceq \mathbb{R}$. Itse asiassa $]0,1] \sim \mathbb{R}$ (teht. 303, 305). Jokainen $x \in]0,1]$ voidaan esittää desimaalikehitelmänä

$$x = 0{,}a_1a_2\ldots,$$

missä oikea puoli tarkoittaa lukua, jonka desimaalinumerot ovat $a_1, a_2, \ldots$ Esimerkiksi $1/3 = 0{,}333\ldots$, $1 = 0{,}999\ldots$, $1/2 = 0{,}5000\ldots = 0{,}4999\ldots$ Desimaalikehitelmä ei siis ole yksikäsitteinen "päättyville desimaaliluvuille". Sovimme, että tällöin käytetään peräkkäisiin yhdeksikköihin päättyvää esitystä; siis $1/2 = 0{,}4999\ldots$, $1/4 = 0{,}24999\ldots$

Teemme vastaoletuksen: I on numeroituva, jolloin sen alkiot voidaan järjestää jonoon $x_1, x_2, \ldots$, siis $I = \{x_1, x_2, \ldots\}$. Etsimme sellaisen luvun $x \in I$, joka ei ole tässä jonossa. Muodostamme lukujen $x_1, x_2, \ldots$ desimaalikehitelmät

$$\begin{aligned} x_1 &= 0{,}x_{11}x_{12}x_{13}\ldots, \\ x_2 &= 0{,}x_{21}x_{22}x_{23}\ldots, \\ x_3 &= 0{,}x_{31}x_{32}x_{33}\ldots, \\ &\vdots \end{aligned}$$

ja määrittelemme luvun $y \in I$ niin, että sen desimaalikehitelmän $0{,}y_1y_2\ldots$ numerot ovat

$$y_k = \begin{cases} 7, & \text{kun } x_{kk} \neq 7, \\ 8, & \text{kun } x_{kk} = 7. \end{cases}$$

Lukujen y ja x_1 ensimmäiset desimaalit siis eroavat toisistaan, joten $y \neq x_1$. Toisten desimaalien eroamisen perusteella $y \neq x_2$, kolmansien $y \neq x_3$ jne. Täten y ei voi olla joukon $I = \{x_1, x_2, \ldots\}$ mikään luku, ja näin olemme ristiriidassa sen kanssa, että $y \in I$. (Tätä ristiriitaa voitaisiin yrittää kiertää sanomalla, että jokin x_k on kyllä y, vaikka näillä on eri desimaalikehitelmät. Mutta y:n desimaalikehitelmä ei sisällä yhdeksikköjä eikä nollia, joten se on yksikäsitteinen.) Luvun y voimme konstruoida muillakin tavoilla (miten?).

Käyttämämme *Cantorin diagonaalimenetelmä* on hyödyllinen monissa ylinumeroituvuustodistuksissa.

Kontinuumihypoteesin mukaan ei ole olemassa sellaista joukkoa, jonka mahtavuus on suurempi kuin joukon $\mathbb{N}$ mutta pienempi kuin joukon $\mathbb{R}$. Voidaan todistaa (ks. esim. Enderton [3], Jech [8]), että kontinuumihypoteesi on riippumaton joukko-opin aksioomista. Edelleen voidaan todistaa (ks. esim. Enderton [3], Jech [8], Lipschutz [11]), että joukon $\mathcal{P}(X)$ mahtavuus on aina suurempi kuin joukon X. Täten äärettömiä mahtavuuksia on äärettömän monta.

∗5.5 Valinta-aksiooma

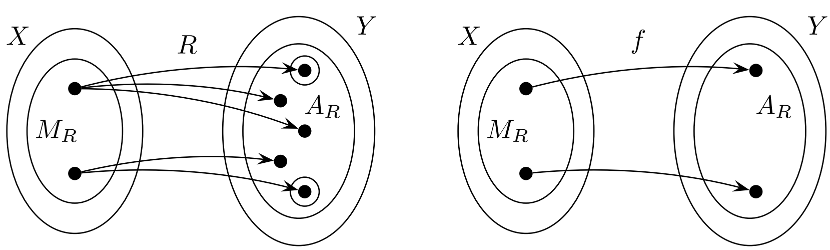
Palaamme nyt *valinta-aksioomaan*, josta meillä on jo (s. 101) ollut alustavasti puhe. Tämä aksiooma esitetään tavallisesti seuraavassa muodossa.

Valinta-aksiooma (tavanomainen muotoilu). Olkoon $\{A_k\}_{k\in I}$ indeksoitu perhe epätyhjiä joukkoja. Tällöin on olemassa sellainen ”valintafunktio” $\varphi\colon \{A_k\}_{k\in I} \to \bigcup_{k\in I} A_k$, että $\varphi(A_k) \in A_k$ kaikilla $k \in I$.

Havainnollisesti tämä tarkoittaa, että jokaisesta A_k-joukosta voidaan ”valita” yksi alkio $\varphi(A_k)$, ja näistä alkioista voidaan muodostaa ”uusi” joukko $\{\varphi(A_k)\}_{k\in I}$. Tuntuu itsestään selvältä, että näin täytyy olla. Toisin sanoen valinta-aksiooma täten muotoiltuna vaikuttaa uskottavalta. Toisaalta olemme (s. 101) todenneet, että tämä aksiooma on yhtäpitävä hyvinjärjestysperiaatteen kanssa. Kuitenkin tuntuu kummalliselta, että esimerkiksi joukko $\mathbb{R}$ voidaan hyvinjärjestää, joten valinta-aksiooma muotoiltuna hyvinjärjestysperiaatteena ei vaikutakaan enää yhtä uskottavalta.

Intuition varaan ei siis tässä kannata rakentaa mitään. Valinta-aksioomaa ei voida todistaa aksiomaattisessa joukko-opissa oikeaksi eikä vääräksi, joten se täytyy ottaa uudeksi aksioomaksi.

Tarkastelemme vielä valinta-aksiooman erästä toista muotoilua. Olkoon R epätyhjä relaatio joukosta X joukkoon Y. Tämä relaatio ei ole välttämättä kuvaus $M_R \to Y$ (missä M_R on R:n määrittelyjoukko), sillä joitakin M_R:n alkioita x voi vastata useampi kuin yksi Y:n alkio. Tuntuu itsestään selvältä, että voimme tällöin ”valita” näistä monesta alkiosta yhden ja asettaa sen vastaamaan x:ää, ja näin menettelemällä saamme kuvauksen $f\colon M_R \to Y$. Tämäkin ”itsestäänselvyys” on yhtäpitävä valinta-aksiooman kanssa.



Valinta-aksiooma (relaatiomuotoilu). Olkoon R epätyhjä relaatio joukosta X joukkoon Y. Tällöin on olemassa relaatio $f \subseteq R$, joka on kuvaus $M_R \to Y$.

Lause 34. Valinta-aksiooman tavanomainen muotoilu (tm) ja relaatiomuotoilu (rm) sekä hyvinjärjestysperiaate (hp) ovat yhtäpitäviä.

Tyydymme todistamaan vain helpot osat (hp) $\Rightarrow$ (tm) ja (tm) $\Rightarrow$ (rm). Muiden osien todistukset ja valinta-aksiooman muita muotoja, ks. esim. [3, 8].

(hp) $\Rightarrow$ (tm). Olkoon $\{A_k\}_{k\in I}$ indeksoitu perhe epätyhjiä joukkoja. Määrittelemme kaikissa näissä joukoissa hyvinjärjestyksen, jolloin funktio $\varphi(A_k) = A_k$:n pienin alkio kelpaa valintafunktioksi. (Siis ”valitsemme” kustakin joukosta pienimmän alkion ja muodostamme niistä ”uuden” joukon.)

(tm) $\Rightarrow$ (rm). Olkoon R epätyhjä relaatio joukosta X joukkoon Y. Kun $x \in M_R$, niin olkoon $S_x = \{\, y \in Y \mid xRy \,\}$. Sovellamme (tm):ää joukkoperheeseen $\{S_x\}_{x\in M_R}$; olkoon φ näin saatu valintafunktio. (Siis ”valitsemme” yhden alkion kustakin sellaisesta joukosta Y:n alkioita, jotka ovat relaatiossa R X:n saman alkion kanssa, ja muodostamme niistä ”uuden” joukon.) Nyt $f(x) = \varphi(S_x)$ on vaadittu kuvaus.

Kaikissa valinnoissa ei tarvita valinta-aksioomaa. Sitä tarvitaan, kun tehdään äärettömän monta valintaa, mutta ei ole käytettävissä täsmällisiä sääntöjä niiden tekemiseksi.

Esimerkki 113. Olkoon R epätyhjä relaatio joukosta X joukkoon Y ja olkoon $x \in M_R$. Tällöin voidaan ilman valinta-aksioomaa valita sellainen y_x, että xRy_x. Jos M_R on ääretön, niin valinta-aksioomaa sen sijaan tarvitaan joukon $U = \{\, y_x \mid x \in M_R \,\}$ muodostamiseksi. Toisin sanoen valinta-aksioomaa tarvitaan, kun kaikille $x \in M_R$ halutaan ”valita” relaatiossa R oleva y_x ja muodostaa niistä ”uusi” joukko U.

Tarkastelemme lopuksi kahta ei-matemaattista esimerkkiä valinta-aksiooman mukaisesta ajattelusta. Esimerkin 114 on esittänyt Russell.

Esimerkki 114. Olkoon meillä äärettömän monta kenkäparia. Voimme muodostaa kaikkien vasemman jalan kenkien joukon ilman valinta-aksioomaa. Meidän täytyy kylläkin tehdä äärettömän monta valintaa, mutta meillä on niihin täsmällinen sääntö. Jos taas meillä on äärettömän monta sukkaparia, ja tehtävänä on muodostaa joukko, jossa on yksi sukka kustakin parista, niin tarvitaan valinta-aksioomaa. Nimittäin nyt meillä ei ole täsmällistä valintasääntöä.

Esimerkki 115. Olkoon meillä äärettömän monta ihmisjoukkoa, joissa jokaisessa on ainakin kaksi ihmistä. Valinta-aksioomaa tarvitaan sellaisen joukon muodostamiseksi, jossa on yksi ihminen jokaisesta näistä joukoista. Sen sijaan tätä aksioomaa ei tarvita sellaisen joukon muodostamiseksi, jonka jäseniä ovat näiden joukkojen nuorimmat (tai vastaavasti vanhimmat, köyhimmät, rikkaimmat, tyhmimmät, viisaimmat tms.) ihmiset. Tällöin oletetaan, että kunkin joukon nuorin (tai vastaavasti muun aseman omaava) voidaan täsmällisesti määritellä.

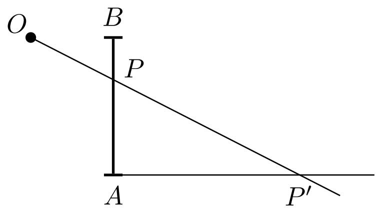
Harjoitustehtäviä

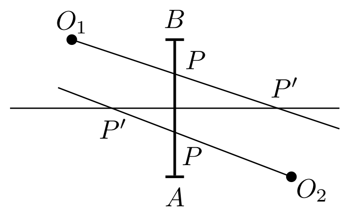
301. Todistettava, että 5:llä jaollisten ja 7:llä jaollisten positiivisten kokonaislukujen joukot ovat keskenään yhtä mahtavia.

302. Edellisen tehtävän yleistys. Olkoon $h, k \in \mathbb{Z}_+$ ja $h\mathbb{Z}_+$ h:lla jaollisten sekä $k\mathbb{Z}_+$ k:lla jaollisten positiivisten kokonaislukujen joukko. Osoitettava, että $h\mathbb{Z}_+ \sim k\mathbb{Z}_+$.

303. Olkoon $a < b$. Todistettava: **a)** $]a, b[\sim \mathbb{R}_+$, **b)** $]a, b[\sim \mathbb{R}$, **c)** $\mathbb{R}_+ \sim \mathbb{R}$.

304. Perusteltava seuraavien kuvioiden avulla geometrisesti, että **a)** janan ja puolisuoran sisäpisteiden, **b)** janan sisäpisteiden ja suoran pisteiden joukot ovat yhtä mahtavia.





305. Osoitettava, että kaikki avoimet, suljetut ja puoliavoimet välit ovat yhtä mahtavia.

306. Osoitettava, että tason kaikkien origokeskisten ympyröiden joukko on yhtä mahtava kuin joukko $\mathbb{R}_+$.

307. Osoitettava, että tason kaikkien ympyröiden joukko ja ylöspäin aukeavien paraabelien joukko ovat yhtä mahtavia.

308. Todistettava, että kuvaus $f(m/n) = 2^m 3^n$, missä $\mathrm{syt}(m, n) = 1$, on injektio $\mathbb{Q}_+ \to \mathbb{N}$.

309. Olkoot A ja B epätyhjiä joukkoja. Todistettava yhtäpitäviksi

(1) On olemassa sellainen $B' \subseteq B$, että $A \sim B'$.

(2) On olemassa injektio $A \to B$.

(3) On olemassa surjektio $B \to A$.

Tarvitaanko todistuksessa valinta-aksioomaa?

310. Olkoot A_1, $A_2, \ldots$ numeroituvia joukkoja. Osoitettava, että **a)** $\bigcup_{k=1}^{n} A_k$, **b)** $\bigcup_{k=1}^{\infty} A_k$ on numeroituva. Ohje b-kohtaan: Menettele kuten $\mathbb{Q}_+$:n numeroituvuustodistuksessa. Tarvitaanko valinta-aksioomaa i) a-kohdan, ii) b-kohdan, iii) $\mathbb{Q}_+$:n ylinumeroituvuuden todistamisessa?

311. Onko **a)** kahden, **b)** n numeroituvan joukon tulojoukko numeroituva?

312. Olkoot A_1, $A_2, \ldots$ numeroituvia joukkoja. Onko joukko $A_1 \times A_2 \times \cdots = \{ (x_1, x_2, \ldots) \mid x_k \in A_k,\ \forall k \in \mathbb{Z}_+ \}$ numeroituva?

313. Todistettava, että jokaisella äärettömällä joukolla on numeroituva ääretön osajoukko. Tarvitaanko todistuksessa valinta-aksioomaa?

314. Osoitettava, että irrationaalilukujen joukko on ylinumeroituva.

315. Mikä on kaikkien mahdollisten sanojen joukon mahtavuus, kun sanalla tarkoitetaan **a)** äärellistä, **b)** myös ääretöntä äärellisestä aakkostosta muodostettua jonoa?

316. Vilenkinin kirjassa [28] on lainaus Stanislaw Lemin teoksesta "The Interstellar Milkman, Ion the Quiet", jossa numeroituvien ja ylinumeroituvien joukkojen ominaisuuksia valaistaan hauskalla tavalla Hilbertin[5] esittämän esimerkin mukaisesti. Tässä kirjassa tapahtuu mm. seuraavaa.

Hotelli Kosmos sijaitsee jossakin tähtisumun ACD-1587 tienoilla. Tässä hotellissa on (numeroituvasti) ääretön määrä huoneita. Ion the Quiet saapuu fotoniraketillaan Kosmoksen pihalle aikoen yöpyä hotellissa. Valitettavasti hotelli oli täynnä, sillä parhaillaan oli meneillään universaali eläintieteilijäkongressi. Sen osanottajat, joita oli (numeroituvasti) ääretön määrä, olivat varanneet koko hotellin. Onneksi paikalle osui hotellin neuvokas johtaja, joka järjesti asian: Ion pääsee huoneeseen numero 1, huoneessa 1 ollut eläintieteilijä siirretään huoneeseen 2, huoneessa 2 ollut huoneeseen 3 jne.

Seuraavana aamuna hotelliin pyrki uusia vieraita, nimittäin universaalin filatelistikongressin osanottajat, joita oli (numeroituvasti) ääretön määrä. Hetken mietittyään hotellin johtaja keksi keinon, millä nämäkin vieraat saatiin sijoitetuksi täpötäyteen hotelli Kosmokseen. Mikä tämä keino oli?

317. Jatkoa edelliseen tehtävään. Illalla vaikeudet jatkuivat. Jokaisessa galaksissa, joita on kaikkiaan (numeroituvasti) ääretön määrä, on nimittäin Kosmoksen kaltainen hotelli, jotka kaikki olivat täynnä. Jostakin syystä kaikki muut hotellit paitsi Kosmos päätettiin sulkea, ja niiden asukkaat kuljetettiin Kosmokseen. Johtaja oli epätoivoissaan: hänen oli saatava (numeroituvasti) äärettömän monen hotellin vieraat, joita kutakin hotellia kohti oli (numeroituvasti) ääretön määrä, mahtumaan jo entuudestaan täyteen hotelli Kosmokseen. Johtaja, kokki ja kirjanpitäjä esittivät ratkaisunsa, jotka kaikki osoittautuivat vääriksi. Lopulta muuan filatelisti, erään galaksin matemaattisen akatemian esimies, ratkaisi ongelman. Mikä tämä ratkaisu oli?

318. Jatkoa edelliseen tehtävään. Hotelliyhtymän johtokunta määräsi, että Kosmoksessa on laadittava luettelo kaikista mahdollisista tavoista, joil-

[5] *David Hilbert (1862–1943), saksalainen matemaatikko.*

la sinne voidaan sijoittaa vieraita. Täyttä huonetta tarkoittaa numero 1 ja tyhjää 0. Esimerkiksi

$$10101010\ldots$$

tarkoittaa sitä, että paritonnumeroiset huoneet ovat varattuja ja parillisnumeroiset vapaita,

$$11111111\ldots$$

tarkoittaa sitä, että koko hotelli on täynnä, ja

$$00000000\ldots$$

sitä, että hotelli on tyhjä.

Muutaman päivän ahkeran työn jälkeen hotellin johtaja tuli Ion the Quietin luo mukanaan äärettömän pitkä lista. Ion väitti, ettei listassa voi olla kaikkia mahdollisia tapoja vieraiden sijoittamiseksi. Miten hän perusteli väitteensä?

319. Osoitettava, että kaikkien äärettömien bittijonojen joukko on ylinumeroituva. Mikä uusi todistus näin saadaan joukon $\mathbb{R}$ ylinumeroituvuudelle?

320. Osoitettava, että $\mathcal{P}(\mathbb{N})$ on ylinumeroituva. Ohje: Mikä vastaavuus on joukon $\mathbb{N}$ osajoukkojen ja äärettömien bittijonojen välillä?

Luku 6

Kombinatoriikkaa

Ja lukumäärämies – sen nimen sai hän –
kumartaa, alistuvan murheisena
pois tassutellen Aniaran yöhön.

(*Martinson* [12])

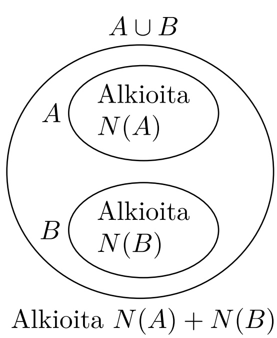
6.1 Summa- ja tuloperiaate. Seula- ja laatikkoperiaate

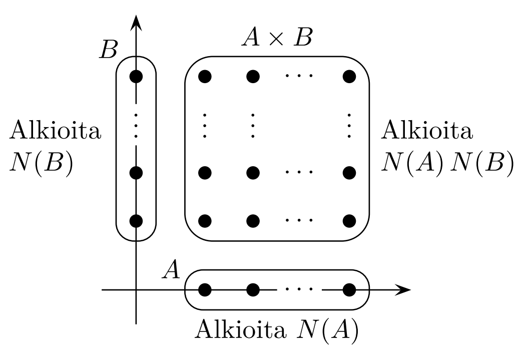
1 Summa- ja tuloperiaate

Kombinatoriikassa tutkitaan menetelmiä erilaisten äärellisten joukkojen alkioiden lukumäärien laskemiseksi. Merkitköön $N(A)$ äärellisen joukon A alkioiden lukumäärää. Vaikka seuraava lause on aivan alkeellinen, se on koko kombinatoriikan perusta.

Lause 35. Olkoot A ja B äärellisiä joukkoja. Tällöin

$$N(A \cup B) = N(A) + N(B), \text{ jos } A \cap B = \emptyset \quad \text{(summaperiaate)},$$
$$N(A \times B) = N(A)\,N(B) \quad \text{(tuloperiaate)}.$$





Tämä lause on voimassa silloinkin, kun joukkoja on enemmän kuin kaksi (teht. 321). Jos $B \subseteq A$, niin summaperiaatteesta seuraa (teht. 322) ”erotusperiaate”

$$N(A \setminus B) = N(A) - N(B).$$

Esimerkki 116. Kuinka monta sellaista bittijonoa on olemassa, joiden **a)** pituus on 4, **b)** pituus on n, **c)** pituus on 4, ensimmäinen bitti on 0 ja viimeinen bitti on 1, **d)** pituus on n ja ainakin ne bitit, joiden järjestysnumero on parillinen, ovat 1?

a) Olkoon $A = \{0, 1\}$. Tarkasteltava jono on joukon $A \times A \times A \times A$ alkio. Tuloperiaatteen mukaan tämän joukon alkioiden lukumäärä on $2 \cdot 2 \cdot 2 \cdot 2 = 16$.

b) Vastaavasti saamme tulokseksi 2^n.

c) Tutkittava joukko on $\{0\} \times A \times A \times \{1\}$. Sen alkioiden lukumäärä on tuloperiaatteen mukaan $1 \cdot 2 \cdot 2 \cdot 1 = 4$.

d) Jos n on parillinen, niin saamme vastaavasti $2 \cdot 1 \cdot 2 \cdot 1 \cdots 2 \cdot 1 = 2^{n/2}$. Jos taas n on pariton, niin kysytty lukumäärä on $2 \cdot 1 \cdot 2 \cdot 1 \cdots 1 \cdot 2 = 2^{(n+1)/2}$.

Esimerkki 117. Eräässä BASIC-ohjelmointikielen versiossa muuttujan nimen saa muodostaa englantilaisten aakkosten 26 kirjaimesta A, B, ..., Z ja numeroista 0, 1, ..., 9 niin, että nimessä on yksi tai kaksi tällaista merkkiä ja ensimmäinen merkki on kirjain. Lisäksi kielessä on viisi kahden merkin pituista varattua sanaa. Isoja ja pieniä kirjaimia ei eroteta toisistaan. Kuinka monta muuttujan nimeä on tässä kielessä?

Olkoon A yhden merkin pituisten ja B kahden merkin pituisten sallittujen nimien joukko, jolloin kaikkien sallittujen nimien joukko $C = A \cup B$. Selvästi $N(A) = 26$. Tuloperiaatteen mukaan ja poistamalla varatut sanat saamme $N(B) = 26(26 + 10) - 5 = 931$. Koska $A \cap B = \emptyset$, niin summaperiaatteen mukaan $N(C) = N(A) + N(B) = 26 + 931 = 957$.

Esimerkki 118. Erään tietokoneen jokaisella käyttäjällä on salasana, jonka pituus voi olla 6, 7 tai 8 merkkiä. Nämä merkit ovat (esimerkin 117 mukaisia) kirjaimia ja numeroita, joista ainakin yksi on numero. Kuinka monta salasanaa on olemassa?

Olkoon A_k k:n pituisten salasanojen, B_k k:n pituisten merkkijonojen ja C_k k:n pituisten kirjainjonojen joukko, missä $k \in \{6, 7, 8\}$. Koska $A_6 = B_6 \setminus C_6$, saamme tulo- ja erotusperiaatteen mukaan $N(A_6) = N(B_6) - N(C_6) = 36^6 - 26^6 = 1867866564$. Vastaavasti $N(A_7) = N(B_7) - N(C_7) = 70332353920$ ja $N(A_8) = N(B_8) - N(C_8) = 2612282842880$, joten salasanojen lukumäärä on $N(A_6) + N(A_7) + N(A_8) = 2684483063360$. Salasanoja riittäisi siis noin 500 jokaiselle maapallon asukkaalle!

Esimerkki 119. Johdettava tuloperiaatteella lauseke n-alkioisen joukon osajoukkojen lukumäärälle. Vrt. lause 7 (s. 53).

Olkoon $A = \{1, 2, \ldots, n\}$. Jokainen n-alkioinen bittijono määrää joukon A erään osajoukon, nimittäin sen, jonka alkioina ovat ykkösbittien järjestysluvut. Esimerkiksi bittijonoa $1100\ldots00$ vastaa osajoukko $\{1, 2\}$ (jos $n \geq 2$), jonoa $00\ldots0$ tyhjä joukko ja jonoa $11\ldots1$ A itse. Täten osajoukkojen lukumäärä on bittijonojen lukumäärä 2^n

Esimerkki 120. Kuinka monta kuvausta $\{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$ on olemassa?

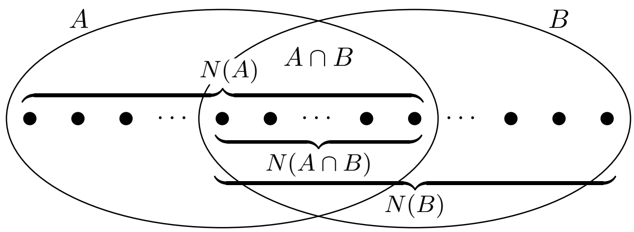
Olkoon f tällainen kuvaus. Koska $f(1)$ voidaan valita n eri tavalla (luvuista $1, 2, \ldots, n$) ja samoin $f(2)$, $f(3)$, ..., $f(m)$, niin kuvausten lukumäärä on tuloperiaatteen mukaan n^m.

2 Seula- ja laatikkoperiaate

Olkoot A ja B äärellisiä joukkoja. Joukot A ja $B \setminus (A \cap B)$ ovat erillisiä, joten summa- ja erotusperiaatteen mukaan

$$\begin{aligned} N(A \cup B) &= N\bigl(A \cup (B \setminus (A \cap B))\bigr) = N(A) + N\bigl(B \setminus (A \cap B)\bigr) \\ &= N(A) + N(B) - N(A \cap B). \end{aligned}$$

Voimme havainnollistaa tätä seuraavalla ajattelulla: Jos laskemme lukumäärän $N(A \cup B)$ muodostamalla summan $N(A) + N(B)$, niin joukon $A \cap B$ alkiot tulevat mukaan kahteen kertaan, joten niiden lukumäärä $N(A \cap B)$ on vähennettävä summasta.



Olemme todistaneet seuraavan lauseen alkuosan.

Lause 36 (Seulaperiaate). Olkoot A ja B äärellisiä joukkoja. Tällöin

$$\begin{aligned} N(A \cup B) &= N(A) + N(B) - N(A \cap B), \\ N(A \cup B \cup C) &= N(A) + N(B) + N(C) - N(A \cap B) \\ &\qquad - N(B \cap C) - N(A \cap C) + N(A \cap B \cap C). \end{aligned}$$

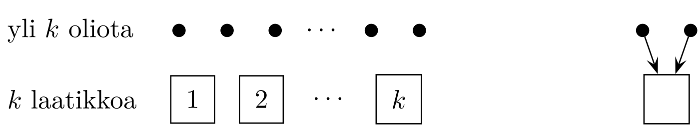
Loppuosa seuraa siitä, että

$$N(A \cup B \cup C) = N\bigl(A \cup (B \cup C)\bigr) = N(A) + N(B \cup C) - N\bigl((A \cap (B \cup C)\bigr)$$

ja

$$\begin{aligned} N\bigl(A \cap (B \cup C)\bigr) &= N\bigl((A \cap B) \cup (A \cap C)\bigr) \\ &= N(A \cap B) + N(A \cap C) - N\bigl((A \cap B) \cap (A \cap C)\bigr) \\ &= N(A \cap B) + N(A \cap C) - N(A \cap B \cap C). \end{aligned}$$

Jos enemmän kuin k oliota on sijoitettava k laatikkoon, niin kaikille ei riitä omaa laatikkoa. Tämä alkeellinen huomio on yllättävän tehokas eräissä kombinatoriikan tehtävissä.



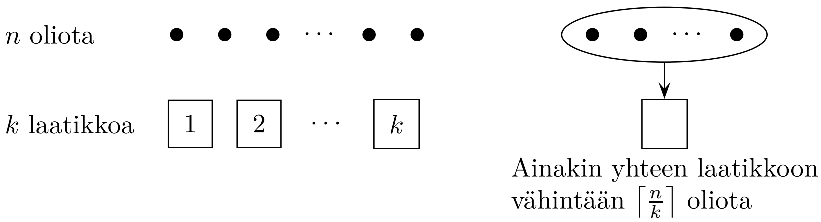
Ainakin yhteen laatikkoon ainakin kaksi oliota

Lause 37 (Laatikkoperiaate). Jos vähintään $k+1$ oliota on sijoitettava k laatikkoon, niin ainakin yhteen laatikkoon tulee vähintään kaksi oliota.

Palautamme mieleen (s. 109, esim. 97), että *kattofunktio* $\lceil x \rceil$ tarkoittaa pienintä kokonaislukua, joka on $\geq x$.

Lause 38 (Yleistetty laatikkoperiaate). Jos n oliota on sijoitettava k laatikkoon, niin ainakin yhteen laatikkoon tulee vähintään $\lceil n/k \rceil$ oliota.

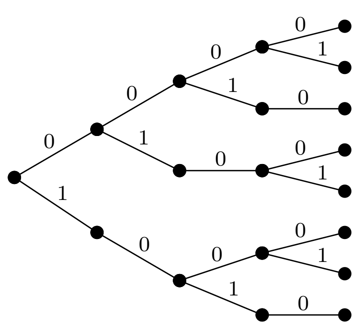
Todistus. Teht. 332.



Esimerkki 121. Kuinka monta sellaista neljän bitin jonoa on, jotka eivät sisällä kahta peräkkäistä ykköstä?

Tapa 1. Merkitköön x mielivaltaista bittiä. Olkoon A muotoa $11xx$ olevien jonojen joukko. Merkitsemme lyhyesti $A = \{11xx\}$. Vastaavasti olkoon $B = \{x11x\}$, $C = \{xx11\}$. Nyt $A \cap B = \{111x\}$, $B \cap C = \{x111\}$, $A \cap C = A \cap B \cap C = \{1111\}$. Tuloperiaatteen mukaan $N(A) = N(B) = N(C) = 4$, $N(A \cap B) = N(B \cap C) = 2$, $N(A \cap C) = N(A \cap B \cap C) = 1$, ja edelleen seulaperiaatteen mukaan $N(A \cup B \cup C) = 4 + 4 + 4 - 2 - 2 - 1 + 1 = 8$. Siis on kahdeksan sellaista neljän bitin jonoa, jotka sisältävät ainakin kaksi peräkkäistä ykköstä. Koska neljän bitin jonoja on kaikkiaan 16 (esim. 116a), niin sellaisia jonoja, jotka eivät sisällä kahta peräkkäistä ykköstä, on $16 - 8 = 8$.

Tapa 2. Käymällä läpi alla olevan *puumallin* kaikki mahdolliset reitit ”juuresta” ”lehtiin” huomaamme, että sellaisten reittien lukumäärä, joissa ei ole kahta peräkkäistä ykköstä, on 8.



Esimerkki 122. Merkitsemme $[n] = \{1, 2, \ldots, n\}$. Kuinka monta surjektiota $[5] \to [3]$ on olemassa?

Kun $i \in \{1, 2, 3\}$, niin merkitsemme $A_i = \{\, f\colon [5] \to [3] \mid i \notin f([5]) \,\}$. Esimerkiksi A_1 on niiden f:ien joukko, jotka eivät saa arvoa 1, ja $A_1 \cap A_2$ on niiden f:ien joukko, jotka eivät saa arvoa 1 eikä 2. Tällöin $A_1 \cup A_2 \cup A_3 = \{\, f\colon [5] \to [3] \mid f \text{ ei surjektio} \,\}$. Seulaperiaatteen mukaan

$$\begin{aligned} N(A_1 \cup A_2 \cup A_3) &= N(A_1) + N(A_2) + N(A_3) \\ &\qquad - N(A_1 \cap A_2) - N(A_1 \cap A_3) - N(A_2 \cap A_3) \\ &\qquad + N(A_1 \cap A_2 \cap A_3) \\ &= 3 \cdot 2^5 - 3 \cdot 1^5 + 1 \cdot 0^5 = 93. \end{aligned}$$

Kuvauksia $f\colon [5] \to [3]$ on $3^5 = 243$ (esim. 120), joten surjektioita on $243 - 93 = 150$.

Esimerkki 123. Eräällä matematiikan kurssilla on 76 opiskelijaa. Vähintään kuinka monella opiskelijalla on sama horoskooppimerkki?

Koska horoskooppimerkkejä on 12, saamme yleistetyn laatikkoperiaatteen mukaan tulokseksi $\lceil 76/12 \rceil = 7$.

Esimerkki 124. Kuntoilija K päättää käydä kesäkuussa lenkillä joka päivä ja lenkkeillä kaikkiaan 45 kertaa. Osoitettava, että tällöin on olemassa tiettyjen peräkkäisten päivien muodostama ajanjakso, jolloin hän lenkkeilee täsmälleen 14 kertaa.

Olkoon a_k kaikkien niiden lenkkien lukumäärä, jotka K on tehnyt kesäkuun k. päivänä tai ennen sitä. Tällöin $1 \le a_1 < a_2 < \cdots < a_{30} = 45$, joten $15 \le a_1 + 14 < a_2 + 14 < \cdots < a_{30} + 14 = 59$. Kaikki luvut a_k ja $a_k + 14$ ovat siis positiivisia kokonaislukuja ja ≤ 59. Koska näitä lukuja on 60 kappaletta, niin laatikkoperiaatteen mukaan ainakin kaksi niistä ovat samoja. Koska luvut a_k ovat keskenään erisuuret ja samoin luvut $a_k + 14$, niin toisen samoista luvuista täytyy olla edellistä tyyppiä ja toisen jälkimmäistä. Siis on olemassa sellaiset i ja j, että $a_i = a_j + 14$. Täten $a_i - a_j = 14$ eli K tekee 14 lenkkiä kesäkuun $(j+1)$. ja i. päivien välisenä aikana (nämä päivät mukaan luettuina).

Esimerkki 125. Eräissä juhlissa kuusi ihmistä istuutuu satunnaisesti saman pöydän ääreen. Osoitettava, että heidän joukossaan on kolmen hengen ryhmä, jonka jäsenet joko ovat kaikki kätelleet toinen toisiaan tai joista yksikään ei ole kätellyt ryhmän kahta muuta jäsentä.

Olkoon A tietty juhlija. Tarkastelemme kahta laatikkoa: $\{A\text{:ta kätelleet}\}$ ja $\{A\text{:ta kättelemättömät}\}$. Yleistetyn laatikkoperiaatteen mukaisesti on olemassa $\lceil \frac{5}{2} \rceil = 3$ henkilöä, jotka joko ovat kaikki kätelleet A:ta tai joista kukaan ei ole kätellyt häntä. Olkoot B, C ja D nämä henkilöt.

Tapaus 1. B, C ja D ovat kätelleet A:ta. Jos kukaan heistä ei ole kätellyt toisiaan, niin asia on selvä. Jos taas kaksi heistä, vaikkapa B ja C, ovat kätelleet toisiaan, niin A, B ja C ovat kätelleet toisiaan.

Tapaus 2. B, C ja D eivät ole kätelleet A:ta. Jos he kaikki ovat kätelleet toisiaan, niin asia on selvä. Jos taas kaksi heistä, vaikkapa B ja C, eivät ole kätelleet toisiaan, niin A, B ja C muodostavat ryhmän, jossa kukaan ei ole kätellyt toistaan.

Harjoitustehtäviä

321. Yleistettävä summa- ja tuloperiaate useammalle kuin kahdelle joukolle ja todistettava ne induktiolla.

322. Todistettava erotusperiaate summaperiaatteen avulla.

323. Kuinka monta suomalaista auton rekisteritunnusta on olemassa?

324. Suunnilleen kuinka monta erilaista 1900-luvulla syntyneen suomalaisen henkilötunnusta on olemassa? (Henkilötunnuksen viimeinen merkki on tarkistusmerkki, joka määräytyy edellisten merkkien perusteella.)

325. Kuinka monessa n bitin jonossa on **a)** kolme ensimmäistä bittiä ykkösiä ja muut nollia, **b)** kolme peräkkäistä ykköstä ja muut nollia?

326. **a)** Kuinka monessa n bitin jonossa kolmesta ensimmäisestä bitistä ainakin kaksi on ykkösiä ja kolmesta viimeisestä bitistä korkeintaan yksi on ykkönen? **b)** Kuten edellä, mutta sanan 'ja' tilalla on 'tai'.

327. *Palindromi* on oikealta vasemmalle sama kuin vasemmalta oikealle. **a)** Millä todennäköisyydellä satunnaisesti valittu n bitin jono on palindromi? **b)** Mikä on tämän todennäköisyyden raja-arvo, kun $n \to \infty$?

328. Millä todennäköisyydellä n henkilön joukossa on ainakin kaksi, joilla on sama syntymäpäivä (mutta ei välttämättä sama syntymävuosi)? Oletetaan, ettei kukaan ole syntynyt karkausvuonna ja että kaikki syntymäpäivät ovat yhtä todennäköisiä.

329. Muuan kirjastonhoitaja ajatteli laatia koneellisesti "yleiskirjaston", joka käsittäisi kaikki ne 500-sivuiset kirjat, jotka saataisiin käyttämällä 50 merkkiä (kirjaimet, numerot, välimerkit, sanan loppumista ilmoittava merkki) kaikilla mahdollisilla tavoilla, kun yhdelle sivulle mahtuu 2000 merkkiä. Suurin osa näistä kirjoista olisi täysin järjettömiä sisällöltään, mutta joukossa olisivat myös mm. kaikki romaanit ja tieteelliset teokset, jotka on jo kirjoitettu, ja myös kaikki ne, jotka koskaan tullaan kirjoittamaan. **a)** Kuinka monta kirjaa kirjastossa olisi? **b)** Jos yhden kirjan paksuus on 3 cm, niin kuinka korkea kirjapino niistä saataisiin? **c)** Jos kirjastonhoitaja liikkuisi valon nopeudella ylöspäin, niin kuinka kauan kestäisi hänen matkansa pinon juurelta huipulle?

330. Erään yhtiön myyntimiehen on käytävä 15 kaupungissa. Matkakustannukset kaikista kaupungeista kaikkiin muihin tiedetään. Yhtiön atk-suunnittelija päättää etsiä edullisimman matkareitin. Selvitettyään koeohjelmalla, että yhden reitin kustannusten laskeminen vie tietokoneelta 0,01 s aikaa, hän on varma siitä, että edullisin reitti löytyy helposti käymällä kaikki vaihtoehdot läpi. Oletko samaa mieltä?

331. Yleistettävä (ilman todistusta) seulaperiaate n joukolle.

332. Todistettava yleistetty laatikkoperiaate.

333. Eräästä matematiikan, tietojenkäsittelyopin ja tilastotieteen opiskelijoiden joukosta 100 opiskeli matematiikkaa, 200 tietojenkäsittelyoppia ja 50 tilastotiedettä. Näistä opiskelijoista 40 opiskeli sekä tietojenkäsittelyoppia että tilastotiedettä, 80 sekä matematiikkaa että tietojenkäsittelyoppia ja 30 sekä matematiikkaa että tilastotiedettä. Kaikkia kolmea ainetta opiskeli 20. Kuinka monta opiskelijaa tässä joukossa oli kaikkiaan?

334. Kuusinumeroinen puhelinnumero alkaa 4:llä ja muut numerot ovat määräytyneet sattumanvaraisesti. Millä todennäköisyydellä näin saadussa luvussa esiintyy ainakin kerran peräkkäin numerot 1 ja 3 tässä järjestyksessä?

335. Luvuista $1, 2, \dots, 8$ valitaan viisi lukua. Osoitettava, että niiden joukossa on ainakin yksi sellainen lukupari, jonka summa on 9.

336. Miten esimerkki 124 muuttuu, jos K teki saman suunnitelman vuoden 1996 helmikuuksi?

337. Kilpailujen 51 osallistujaa saa kukin numeron väliltä 1000–1099. Osoitettava, että ainakin kaksi kilpailijaa saa peräkkäiset numerot.

338. Onko Suomessa ainakin kaksi henkilöä, joilla on tällä hetkellä pankkitilillään (tai tileillään) täsmälleen sama (nollasta eroava) määrä rahaa?

339. Osoitettava, ettei esimerkin 125 väite pidä paikkaansa, jos seurueessa on vain viisi jäsentä.

340. Osoitettava, että jokaisessa seurueessa on ainakin kaksi henkilöä, jotka ovat kätelleet yhtä monta seurueen jäsentä.

6.2 Permutaatiot ja kombinaatiot

1 Permutaatiot

Joukon *permutaatio* on sen bijektio itselleen.

Esimerkki 126. Joukon $A = \{1, 2, 3\}$ eräs permutaatio on kuvaus $f\colon A \to A$: $f(1) = 3$, $f(2) = 2$, $f(3) = 1$. Voimme määritellä tämän kuvauksen myös yksinkertaisesti muodostamalla joukon A alkioiden kuvien jonon eli kirjoittamalla $(3, 2, 1)$.

Voimme siis havainnollisesti sanoa, että äärellisen joukon permutaatio saadaan järjestämällä tämä joukko eli kirjoittamalla sen alkiot jossakin järjestyksessä.

Esimerkki 126, jatkoa. Joukon $\{1,2,3\}$ permutaatiot ovat $(1,2,3)$, $(2,3,1)$, $(3,1,2)$, $(1,3,2)$, $(3,2,1)$ ja $(2,1,3)$.

Tarkastelemme äärellistä joukkoa A, jonka alkioiden lukumäärä $N(A) = n$. Joukon A k-*permutaatio* $(0 < k \leq n)$ on sen k-alkioisen osajoukon permutaatio. Täten joukon A n-permutaatio on sen ”tavallinen” permutaatio. Lisäksi sovimme, että 0-permutaatio on ”tyhjä permutaatio”.

Esimerkki 127. Joukon $\{1,2,3\}$ 2-permutaatiot ovat $(1,2)$, $(2,1)$, $(1,3)$, $(3,1)$, $(2,3)$ ja $(3,2)$.

Lause 39. Olkoon A äärellinen joukko. Jos $N(A) = n$ ja $0 \leq k \leq n$, niin joukon A k-permutaatioiden lukumäärä on

$$n(n-1)\cdots\big(n-(k-1)\big) = \frac{n!}{(n-k)!}.$$

Todistus. Jos $k = 0$, niin asia on selvä. (Vasemmanpuolisen ”tyhjän tulon” arvoksi määritellään 1.) Olkoon nyt $k > 0$. Tulkitsemme k-permutaation k-alkioiseksi jonoksi. Sen ensimmäinen alkio voidaan valita n eri tavalla (mikä tahansa A:n alkio), toinen alkio $n-1$ eri tavalla (mikä tahansa muu alkio paitsi ensimmäinen), kolmas alkio $n-2$ eri tavalla (mikä tahansa muu paitsi ensimmäinen ja toinen) jne. Vihdoin k. alkio voidaan valita $n-(k-1)$ eri tavalla. Väitös seuraa nyt tuloperiaatteesta.

Asettamalla $k = n$ saamme n-alkioisen joukon permutaatioiden lukumääräksi $n!$.

Esimerkki 128. Korttipakasta otetaan viisi korttia. Millä todennäköisyydellä ne kaikki ovat patoja?

Otamme alkeistapauksiksi permutaatiot. Kiinnitämme siis huomiota korttien järjestykseen. Alkeistapausten lukumäärä on 52 kortin joukon 5-permutaatioiden lukumäärä $52 \cdot 51 \cdot 50 \cdot 49 \cdot 48$. Suotuisien alkeistapausten lukumäärä on 13 patakortin joukon 5-permutaatioiden lukumäärä $13 \cdot 12 \cdot 11 \cdot 10 \cdot 9$. Kysytty todennäköisyys on täten

$$\frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9}{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48} \approx 0{,}000495.$$

2 Kombinaatiot

Tarkastelemme edelleen joukkoa A, jolle $N(A) = n$. Joukon A k-*kombinaatio* $(0 \leq k \leq n)$ on sen k-alkioinen osajoukko. Siis 0-kombinaatio on tyhjä joukko ja n-kombinaatio on A itse.

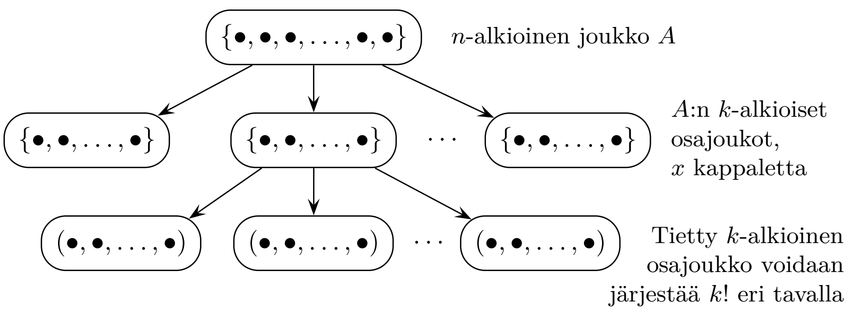
Esimerkki 129. Joukon $\{1,2,3\}$ 2-kombinaatiot ovat $\{1,2\}$, $\{1,3\}$ ja $\{2,3\}$.

Kombinaatioiden lukumäärän laskemista varten määrittelemme *binomikertoimen*

$$\binom{n}{k} = \frac{n(n-1)\cdots\big(n-(k-1)\big)}{k!} = \frac{n!}{k!(n-k)!}.$$

Lause 40. Olkoon A äärellinen joukko. Jos $N(A) = n$ ja $0 \le k \le n$, niin joukon A k-kombinaatioiden lukumäärä on $\binom{n}{k}$.

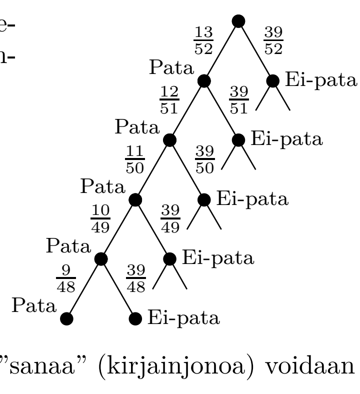
Todistus. Tapaus $k = 0$ on selvä, joten oletamme, että $k > 0$. Olkoon joukon A k-kombinaatioiden lukumäärä x. Joukon A k-alkioinen osajoukko voidaan siis valita x eri tavalla. Tietty k-alkioinen osajoukko voidaan lauseen 39 mukaan järjestää $k!$ eri tavalla, joten tuloperiaatteen mukaan k-permutaatioiden lukumäärä on $k!x$. Toisaalta se on lauseen 39 mukaan $n(n-1)\cdots\big(n-(k-1)\big)$. Yhtälöstä $k!x = n(n-1)\cdots\big(n-(k-1)\big)$ seuraa väitös.



Esimerkki 128, jatkoa. Käsittelemme tehtävän uudestaan ottamalla alkeistapauksiksi kombinaatiot. Emme siis kiinnitä huomiota korttien järjestykseen. Kaikkien alkeistapausten lukumäärä on 52 kortin joukon 5-kombinaatioiden lukumäärä $\binom{52}{5}$. Suotuisien alkeistapausten lukumäärä on 13 patakortin joukon 5-kombinaatioiden lukumäärä $\binom{13}{5}$. Kysytty todennäköisyys on täten $\binom{13}{5}/\binom{52}{5} \approx 0{,}000495$.

Kolmas tapa on käyttää puumallia. Etenemällä kuvion "patahaaraa" pitkin saamme todennäköisyydeksi

$$\frac{13}{52}\frac{12}{51}\frac{11}{50}\frac{10}{49}\frac{9}{48} \approx 0{,}000495.$$



Esimerkki 130. Kuinka monta erilaista "sanaa" (kirjainjonoa) voidaan muodostaa sanasta MIMMI?

Tällaisia sanoja on yhtä paljon kuin tapoja valita paikat I-kirjaimille eli valita järjestysnumeroista $\{1, 2, 3, 4, 5\}$ kaksi. Niiden lukumäärä on 5-alkioisen joukon 2-kombinaatioiden lukumäärä $\binom{5}{2} = 10$.

3 Multinomikertoimet

Binomikerroin $\binom{n}{k}$ ilmoittaa, kuinka monella tavalla n-alkioinen joukko voidaan jakaa kahteen osajoukkoon niin, että toiseen tulee k alkiota ja toiseen $n - k$. Yleisemmin kysymme, kuinka monella tavalla n-alkioinen joukko voidaan jakaa m osajoukkoon niin, että osien alkioiden lukumäärät ovat k_1, k_2, ..., k_m $(k_1 + k_2 + \cdots + k_m = n)$. Vastataksemme tähän määrittelemme *multinomikertoimen*

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1!\, k_2! \cdots k_m!}.$$

Lause 41. Olkoon A äärellinen joukko. Jos $N(A) = n$, $0 \leq k_1, k_2, \ldots, k_m \leq n$ ja $k_1 + k_2 + \cdots + k_m = n$, niin A voidaan esittää $\binom{n}{k_1, k_2, \ldots, k_m}$ eri tavalla yhdisteenä $A_1 \cup A_2 \cup \cdots \cup A_m$, missä joukkojen A_1, A_2, ..., A_m alkioiden lukumäärät ovat k_1, k_2, ..., k_m.

Todistus. Olkoot A_1, A_2, ..., A_m tällaiset joukot. Joukon A_1 alkiot voidaan valita $\binom{n}{k_1}$ eri tavalla, minkä jälkeen joukon A_2 alkiot voidaan valita $\binom{n-k_1}{k_2}$ eri tavalla. Jatkamalla vastaavasti ja soveltamalla tuloperiaatetta saamme valintojen lukumääräksi

$$\binom{n}{k_1}\binom{n-k_1}{k_2} \cdots \binom{n - k_1 - k_2 - \cdots - k_{m-1}}{k_m},$$

josta sieventämällä (teht. 349) seuraa väitös.

Esimerkki 131. Korttipelissä jaetaan 52 korttia tasan neljälle pelaajalle. Kuinka monella eri tavalla kortit voivat jakautua?

Kortit voivat jakautua $\binom{52}{13, 13, 13, 13} \approx 5{,}4 \cdot 10^{28}$ eri tavalla.

Esimerkki 132. Kuinka monta erilaista "sanaa" voidaan muodostaa sanasta MIMMIMAMMA?

Tapa 1. Emme käytä multinomikertoimia. M-kirjainten järjestysnumerot voidaan valita $\binom{10}{6}$ eri tavalla. Jäljelle jääneistä numeroista A-kirjainten numerot voidaan valita $\binom{4}{2}$ eri tavalla. Loput kaksi numeroa tulevat I-kirjaimille. Kysytty lukumäärä on nyt tuloperiaatteen mukaan

$$\binom{10}{6}\binom{4}{2} = \frac{10!}{6! \cdot 4!} \frac{4!}{2! \cdot 2!} = \frac{10!}{6! \cdot 2! \cdot 2!} = 1260.$$

Tapa 2. Käytämme multinomikertoimia. Jaamme kirjainten järjestysnumeroiden joukon $\{1, \ldots, 10\}$ kolmeen osajoukkoon niin, että ensimmäisessä (M-kirjainten paikat) on 6 alkiota, toisessa (A-kirjainten paikat) 2 alkiota ja kolmannessa (I-kirjainten paikat) 2 alkiota. Tällaisten jakojen lukumäärä on

$$\binom{10}{6,2,2} = \frac{10!}{6! \cdot 2! \cdot 2!} = 1260.$$

4 Monijoukot

Olemme aiemmin (s. 67, esim. 53) todenneet, että joukon alkion useampikertaisella esiintymisellä ei ole vaikutusta. Joskus kuitenkin sen kannattaa antaa vaikuttaa. Esimerkin 130 aihepiiriin liittyvissä tarkasteluissa saattaa olla kätevää sopia, että sanan MIMMI kirjainten joukko on $\{\mathrm{M}, \mathrm{I}, \mathrm{M}, \mathrm{M}, \mathrm{I}\} = \{\mathrm{M}, \mathrm{M}, \mathrm{M}, \mathrm{I}, \mathrm{I}\}$. Tavallisessa joukko-opissa emme kuitenkaan voi tehdä näin, vaan meidän on kirjoitettava esimerkiksi $\{\mathrm{M}_1, \mathrm{I}_1, \mathrm{M}_2, \mathrm{M}_3, \mathrm{I}_2\} = \{\mathrm{M}_1, \mathrm{M}_2, \mathrm{M}_3, \mathrm{I}_1, \mathrm{I}_2\}$. Siksi tarvitsemme toisenlaista joukko-oppia, jonka tutkimuskohde on englanniksi *multiset* (ja suomeksi paremman puutteessa *monijoukko*). Monijoukossa alkion useampikertaisella esiintymisellä on merkitys.

Esimerkki 133. Olkoon $A = \{1, 1, 2\}$, $B = \{1, 2, 2\}$. Jos A ja B ovat joukkoja, niin $A = B$, mutta jos ne ovat monijoukkoja, niin $A \neq B$. Käytämme monijoukoille merkinnän $\{\ldots\}$ sijasta merkintää $\{\!\!\{\ldots\}\!\!\}$. Siis $\{\!\!\{1, 1, 2\}\!\!\} \neq \{\!\!\{1, 2, 2\}\!\!\}$.

Esimerkki 134. Eräässä ”hedelmäpelissä” pelaaja saa omenoista, appelsiineista ja päärynöistä neljän hedelmän joukon. Kuinka monta tällaista joukkoa on olemassa?

Voisimme luetella kaikki alkioiden $o =$ omena, $a =$ appelsiini ja $p =$ päärynä muodostamat nelialkioiset monijoukot ja huomata että niitä on 15. Haluamme kuitenkin ratkaista tehtävän tyylikkäämmin. Ajattelemme pelaajan saamat hedelmät järjestetyksi niin, että ensin ovat omenat, sitten appelsiinit ja lopuksi päärynät. Esimerkiksi $**/*/*$ tarkoittaa monijoukkoa $\{\!\!\{o, o, a, p\}\!\!\}$, kun taas $/****/$ tarkoittaa monijoukkoa $\{\!\!\{a, a, a, a\}\!\!\}$. Ongelma on, kuinka monella tavalla voimme ryhmitellä neljä hedelmää $*$ kahdella ”erottimella” /. Voimme ajatella, että hedelmille ja erottimille on kaikkiaan 6 ”paikkaa”, jolloin erottimien paikat voidaan valita $\binom{6}{2} = 15$ eri tavalla. Tämä on siis vastaus. (Saman tuloksen saisimme tutkimalla hedelmien paikkoja. Miten?)

Esimerkki 135. Kuinka monella eri tavalla n-alkioisesta joukosta voidaan valita k-alkioinen monijoukko?

Käytämme esimerkin 134 menetelmää. Selvitämme, kuinka monella tavalla k alkiota $*$ voidaan ryhmitellä, kun käytössä on $n-1$ erotinta /. Jos esimerkiksi $n = 5$ ja $k = 4$, niin ryhmittely $*/**//*/$ tarkoittaa monijoukkoa $\{\!\!\{1, 2, 2, 4\}\!\!\}$ ja ryhmittely $////****$ monijoukkoa $\{\!\!\{5, 5, 5, 5\}\!\!\}$. Alkioille ja erottimille on kaikkiaan $k + n - 1$ paikkaa, joten erottimien paikat voidaan valita $\binom{k+n-1}{n-1}$ eri tavalla. Tämä on kysytty lukumäärä.

Monijoukko voidaan määritellä täsmällisesti järjestettynä parina (A, f), missä A on ”tavallinen” joukko ja f on kuvaus $A \to \mathbb{N}$.

Esimerkki 134, jatkoa. Tässä $A = \{o, a, p\}$. Monijoukolle $(A, f) = \{\!\{o, o, a, p\}\!\}$ on $f(o) = 2$, $f(a) = f(p) = 1$ ja monijoukolle $(A, g) = \{\!\{a, a, a, a\}\!\}$ on $g(o) = 0$, $g(a) = 4$, $g(p) = 0$.

Harjoitustehtäviä

341. Eräässä yhdistyksessä on 25 jäsentä. Kuinka monella tavalla sille voidaan valita **a)** nelihenkinen johtokunta, **b)** puheenjohtaja, varapuheenjohtaja, sihteeri ja rahastonhoitaja?

342. Šakkiturnaukseen osallistuu 12 pelaajaa. Jokainen pelaa jokaista vastaan kerran mustilla ja kerran valkeilla. Kuinka monta peliä on turnauksessa?

343. Pyöreä illallispöytä on katettu $2n$ henkilölle. Illallisille osallistuvat pariskunnat A_1, A_2, $\ldots$, A_n. Istumajärjestys arvotaan. Millä todennäköisyydellä **a)** hra A_1 pääsee istumaan vaimonsa viereen, **b)** ketkään herroista eivät pääse istumaan vierekkäin?

344. Kuinka monta erilaista bittijonoa voidaan muodostaa käyttämällä kuutta nollaa ja kahdeksaa ykköstä?

345. Kuinka monta erilaista ”sanaa” voidaan muodostaa sanan MIMMI kirjaimista, jos näitä kirjaimia voidaan myös jättää käyttämättä?

346. Kuinka monta erilaista ”sanaa” voidaan muodostaa sanan ABRACADABRA (kaikista) kirjaimista?

347. Korttipakasta jaetaan kuudelle pelaajalle kullekin viisi korttia. Kuinka monella tavalla kortit voivat jakautua?

348. Olkoon $n, k \in \mathbb{N}$, $k \leq n$. Osoitettava, että $\binom{n}{k} = \binom{n}{n-k}$, **a)** suoraan laskemalla, **b)** kombinatorisella perustelulla tutkimalla kahdella eri tavalla sitä, että n henkilön yhdistys valitsee k henkilön johtokunnan.

349. Sievennettävä lauseen 41 todistuksessa oleva lauseke ja todettava, että tulokseksi saadaan $\binom{n}{k_1, k_2, \ldots, k_m}$.

350. Kuinka monta ei-negatiivista kokonaislukuratkaisua on yhtälöllä $x + y + z = 11$?

351. Kuinka monta sellaista (vakio)veikkausriviä on olemassa, jossa on 6 ykköstä, 3 ristiä ja 4 kakkosta?

352. Olkoon $n, k \in \mathbb{N}$, $1 \leq k \leq n$. **a)** Osoitettava, että $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$. **b)** Tulkittava tämä yhtälö *Pascalin*[1] *kolmion* muodostamissääntönä.

353. Olkoon $n \in \mathbb{Z}_+$, $a, b \in \mathbb{R}$. Todistettava

[1] *Blaise Pascal (1623–1662), ranskalainen matemaatikko ja filosofi.*

a) *binomikaava* $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$,

b) binomikaavan yleistys

$$(a_1+a_2+\cdots+a_m)^n = \sum_{\substack{k_1+k_2+\cdots+k_m=n \\ 0\le k_1,k_2,\ldots,k_m\le n}} \binom{n}{k_1,k_2,\ldots,k_m} a_1^{k_1} a_2^{k_2}\cdots a_m^{k_m}.$$

Ohjeita: **a)** Käytä induktiota tai kombinatorista päättelyä (jolloin ajattelet $(a+b)^n$:n kehitetyksi polynomiksi ja selvität, miten saadaan termin $a^{n-k}b^k$ kerroin). **b)** Käytä kombinatorista päättelyä.

354. Todistettava: **a)** $\sum_{k=0}^{n} \binom{n}{k} = 2^n$, **b)** $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$.

355. Olkoon $m, n, r \in \mathbb{N}$, $r \le m, n$. Todistettava: $\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}$.

356. Olkoon $m, n \in \mathbb{Z}_+$. Kuinka monta injektiota $[m] \to [n]$ on olemassa ($[k] = \{1, 2, \ldots, k\}$)?

357. Olkoon $m, n \in \mathbb{Z}_+$ ja olkoon $\mathrm{sur}(m, n)$ surjektioiden $[m] \to [n]$ lukumäärä. Osoitettava, että (vrt. esim. 122, s. 139)

$$\mathrm{sur}(m,n) = \sum_{k=0}^{n} \binom{n}{k} (-1)^k (n-k)^m.$$

358. **a)** Olkoon $m \in \mathbb{Z}_+$. Todistettava: Joukon $[m]$ ekvivalenssirelaatioiden lukumäärä on

$$\sum_{n=1}^{m} \frac{\mathrm{sur}(m,n)}{n!}.$$

b) Kuinka monta ekvivalenssirelaatiota on joukossa [5]?

359. Seurueessa on n henkilöä, joiden kesken arvotaan k palkintoa ($1 \le k \le n$). Kuinka monella tavalla palkinnot voivat jakautua, jos sama henkilö **a)** ei voi, **b)** voi saada useampia palkintoja ja jos palkinnot ovat i) samanlaisia, ii) kaikki erilaisia?

360. Miten monijoukkojen laskutoimitukset voidaan määritellä vai voidaanko mitenkään? Jos voidaan, niin pysyvätkö tavallisen joukko-opin laskusäännöt voimassa?

**Luku 7*

Rekursioyhtälöistä

As I was going to St. Ives,
I met a man with seven wives.
Each wife had seven sacks,
Each sack had seven cats,
Each cat had seven kits.
Kits, cats, sacks and wives –
How many were going to St. Ives?

(*Englantilainen laulu*)

7.1 Lineaarinen homogeeninen vakiokertoiminen rekursioyhtälö

1 Ratkaisun olemassaolo. Karakteristinen yhtälö

Olemme aiemmin (s. 45, teht. 85) käsitelleet *ensimmäisen kertaluvun lineaarisia vakiokertoimisia rekursioyhtälöitä.* Tarkastelemme nyt *toisen* kertaluvun tällaista *homogeenista* yhtälöä

$$(H) \qquad y_{n+2} + ay_{n+1} + by_n = 0,$$

missä a ja b ovat annettuja reaalilukuja.

Lause 42. Kun y_0 ja y_1 on annettu, niin rekursioyhtälöllä (H) on yksikäsitteinen ratkaisu, joka toteuttaa nämä alkuehdot.

Tämä lause seuraa siitä, että lukujonoja voidaan määritellä rekursiivisesti (vrt. luku 2.2.3). Siis y_0 ja y_1 määräävät y_2:n $(= -ay_1 - by_0)$, y_1 ja y_2 y_3:n jne.

Etsimme aluksi sellaisia lukuja $r \neq 0$, että funktio $y_n = r^n$ toteuttaa (H):n. (Jos $r = 0$, niin (H) on aina toteutettu.) On mukavaa käyttää (H):n vasemmalle puolelle lyhennysmerkintää

$$L(y_n) = y_{n+2} + ay_{n+1} + by_n.$$

Koska

$$L(r^n) = r^{n+2} + ar^{n+1} + br^n = (r^2 + ar + b)r^n$$

ja $r \neq 0$, niin täytyy olla

$$(K) \qquad r^2 + ar + b = 0.$$

Kutsumme tätä tavallista toisen asteen yhtälöä rekursioyhtälön (H) *karakteristiseksi yhtälöksi.* Saamme siis kysytyt r:n arvot ratkaisemalla karakteristisen yhtälön (K). Olkoot r_1 ja r_2 sen ratkaisut.

Tapaus 1. Ratkaisut r_1 ja r_2 ovat reaaliset ja erisuuret. Jokainen funktio

$$y_n = c_1 r_1^n + c_2 r_2^n,$$

missä c_1 ja c_2 ovat mielivaltaisia vakioita, on (H):n ratkaisu, sillä

$$\begin{aligned} L(c_1 r_1^n + c_2 r_2^n) &= L(c_1 r_1^n) + L(c_2 r_2^n) \\ &= c_1 L(r_1^n) + c_2 L(r_2^n) = c_1 0 + c_2 0 = 0. \end{aligned}$$

Tapaus 2. Ratkaisut r_1 ja r_2 ovat reaaliset ja yhtäsuuret. Merkitsemme $r = r_1 = r_2$. Siis $y_n = r^n$ toteuttaa (H):n. Osoitamme, että myös $y_n = nr^n$ toteuttaa sen. Koska r on (K):n kaksinkertainen ratkaisu, niin $r^2 + ar + b = 0$ ja derivaatta $2r + a = 0$, joten

$$\begin{aligned} L(nr^n) &= (n+2)r^{n+2} + a(n+1)r^{n+1} + bnr^n \\ &= (r^2 + ar + b)nr^n + (2r + a)r^{n+1} = 0 + 0 = 0. \end{aligned}$$

Edelleen jokainen funktio

$$y_n = c_1 r^n + c_2 n r^n$$

on (H):n ratkaisu. Voimme osoittaa sen kuten tapauksessa 1 tai tehtävän 361 perusteella.

Tapaus 3. Ratkaisut r_1 ja r_2 eivät ole reaalisia. Olkoon $r_1 = \alpha + \mathrm{i}\beta$, missä $\alpha, \beta \in \mathbb{R}$, $\beta \neq 0$. Tällöin $r_2 = \alpha - \mathrm{i}\beta$. Pääsemme reaalialueelle käyttämällä luvun r_1 *napakoordinaattiesitystä* (teht. 362)

$$r_1 = R(\cos\theta + \mathrm{i}\sin\theta),$$

missä

$$R = \sqrt{\alpha^2 + \beta^2}, \quad \tan\theta = \frac{\beta}{\alpha}.$$

(Jos $\alpha = 0$, niin $\theta = \frac{\pi}{2}$.) Tällöin

$$r_2 = R(\cos\theta - \mathrm{i}\sin\theta).$$

Olkoot d_1 ja d_2 mielivaltaisia kompleksilukuja. Tällöin $d_1 r_1^n + d_2 r_2^n$ on (H):n ratkaisu. Moivren kaavan (teht. 363) perusteella

$$\begin{aligned} d_1 r_1^n + d_2 r_2^n &= d_1(R\cos\theta + \mathrm{i}R\sin\theta)^n + d_2(R\cos\theta - \mathrm{i}R\sin\theta)^n \\ &= d_1 R^n(\cos n\theta + \mathrm{i}\sin n\theta) + d_2 R^n(\cos n\theta - \mathrm{i}\sin n\theta) \\ &= R^n\big((d_1 + d_2)\cos n\theta + \mathrm{i}(d_1 - d_2)\sin n\theta\big) \\ &= R^n(c_1\cos n\theta + c_2\sin n\theta), \end{aligned}$$

missä

$$c_1 = d_1 + d_2, \quad c_2 = \mathrm{i}(d_1 - d_2).$$

Ajattelemalla kompleksiluvut d_1 ja d_2 valituiksi niin, että c_1 ja c_2 ovat reaalisia, huomaamme, että jokainen funktio

$$y_n = R^n(c_1\cos n\theta + c_2\sin n\theta),$$

missä c_1 ja c_2 ovat mielivaltaisia reaalivakioita, on (H):n ratkaisu (teht. 364).

2 Yleinen ratkaisu

Seuraava lause ilmoittaa rekursioyhtälön (H) *yleisen ratkaisun.*

Lause 43. Olkoot r_1 ja r_2 rekursioyhtälön

$$(H) \qquad y_{n+2} + ay_{n+1} + by_n = 0$$

karakteristisen yhtälön

$$(K) \qquad r^2 + ar + b = 0$$

ratkaisut. Tällöin jokainen funktio

$$\begin{aligned}
&y_n = c_1 r_1^n + c_2 r_2^n, && \text{jos } r_1 \neq r_2,\\
&y_n = c_1 r^n + c_2 n r^n, && \text{jos } r_1 = r_2 = r,\\
&y_n = R^n(c_1 \cos n\theta + c_2 \sin n\theta), && \text{jos } r_1 = \alpha + \mathrm{i}\beta,\ r_2 = \alpha - \mathrm{i}\beta,\ \beta \neq 0\\
& && \Big(R = \sqrt{\alpha^2 + \beta^2};\ \text{jos } \alpha \neq 0, \text{ niin}\\
& && \tan\theta = \tfrac{\beta}{\alpha}, \text{ jos } \alpha = 0, \text{ niin } \theta = \tfrac{\pi}{2}\Big),
\end{aligned}$$

missä c_1 ja c_2 ovat mielivaltaisia vakioita, on rekursioyhtälön (H) ratkaisu. Käänteisesti, jokainen (H):n ratkaisu on tätä muotoa.

Todistus. Alkuosan todistimme edellä. Todistamme loppuosan olettaen, että r_1 ja r_2 ovat reaaliset ja erisuuret, ja jätämme muut tapaukset harjoitustehtäväksi (teht. 373).

Olkoon (y_n) rekursioyhtälön (H) ratkaisu. Väitämme, että on olemassa $c_1, c_2 \in \mathbb{R}$, joille $y_n = c_1 r_1^n + c_2 r_2^n$ kaikilla $n \in \mathbb{N}$. Sijoittamalla $n = 0$ ja $n = 1$ saamme yhtälöparin

$$\begin{aligned}
y_0 &= c_1 + c_2\\
y_1 &= r_1 c_1 + r_2 c_2,
\end{aligned}$$

josta

$$c_1 = \frac{y_1 - r_2 y_0}{r_1 - r_2}, \qquad c_2 = \frac{y_1 - r_1 y_0}{r_2 - r_1}.$$

Koska myös $z_n = c_1 r_1^n + c_2 r_2^n$ toteuttaa (H):n alkuehdoilla $z_0 = y_0$, $z_1 = y_1$, niin lauseen 42 mukaan $(y_n) = (z_n)$, mistä väitös seuraa.

Esimerkki 136. Ratkaistava rekursioyhtälö

a) $y_{n+2} - 2y_{n+1} - 3y_n = 0$, **b)** $y_{n+2} - 4y_{n+1} + 4y_n = 0$,

c) $y_{n+2} + 9y_n = 0$.

a) Karakteristisen yhtälön $r^2 - 2r - 3 = 0$ ratkaisut ovat $r_1 = -1$, $r_2 = 3$, joten rekursioyhtälön yleinen ratkaisu on $y_n = c_1(-1)^n + c_2 3^n$.

b) Karakteristisen yhtälön $r^2 - 4r + 4 = 0$ ratkaisu on $r_1 = r_2 = 2$, joten kysytty ratkaisu on $y_n = c_1 2^n + c_2 n 2^n$.

c) Karakteristisen yhtälön $r^2 + 9 = 0$ ratkaisut ovat $r_1 = 3\mathrm{i}$, $r_2 = -3\mathrm{i}$. Siis $\alpha = 0$, $\beta = 3$, $R = 3$, $\theta = \frac{\pi}{2}$, joten

$$y_n = 3^n \Big(c_1 \cos \frac{n\pi}{2} + c_2 \sin \frac{n\pi}{2} \Big).$$

Rekursioyhtälöllä (H) on siis aina äärettömän monta ratkaisua (lause 43), mutta yksi ja vain yksi tietyt alkuehdot toteuttava ratkaisu (lause 42).

Esimerkki 137. Määritettävä edellisen esimerkin c-kohdan rekursioyhtälön se ratkaisu, joka toteuttaa alkuehdot $y_0 = 0$, $y_1 = 1$.

Tapa 1. Määritämme yleisen ratkaisun vakiot niin, että alkuehdot ovat toteutetut. Saamme yhtälöryhmän $c_1 = 0$, $3c_2 = 1$, joten $c_1 = 0$, $c_2 = \frac{1}{3}$. Kysytty ratkaisu on siis $y_n = 3^{n-1} \sin \frac{n\pi}{2}$.

Tapa 2. Emme määritä yleistä ratkaisua, vaan lähdemme liikkeelle alkuehdoista. Saamme $y_0 = 0$, $y_1 = 1$, $y_2 = -9y_0 = 0$, $y_3 = -9y_1 = -9$, $y_4 = -9y_2 = 0$, $y_5 = -9y_3 = 81$.

Induktiolla on nyt helppo osoittaa (teht. 371), että

$$\begin{aligned} &y_n = 0, && \text{kun } n \text{ on parillinen,} \\ &y_n = (-1)^{(n-1)/2} 3^{n-1}, && \text{kun } n \text{ on pariton.} \end{aligned}$$

Tavoilla 1 ja 2 saadut ratkaisut ovat eri muodossa, mutta ne on helppo (teht. 371) nähdä samoiksi.

Harjoitustehtäviä

361. Olkoot $y_n = u_n$ ja $y_n = v_n$ rekursioyhtälön

$$y_{n+2} + ay_{n+1} + by_n = 0$$

ratkaisuja ja olkoot c_1 ja c_2 reaalilukuja. Osoitettava, että myös $y_n = c_1 u_n + c_2 v_n$ on tämän rekursioyhtälön ratkaisu.

362. Johdettava kompleksiluvulle $z = x + \mathrm{i}y \neq 0$ napakoordinaattiesitys

$$z = |z| \, (\cos\theta + \mathrm{i} \sin\theta),$$

missä luvun z *itseisarvo* $|z|$ ja *vaihekulma* θ määritellään niin, että

$$|z| = \sqrt{x^2 + y^2}, \qquad \tan\theta = \frac{y}{x}$$

(jos $x = 0$, niin $\theta = \pm\pi/2$) ja θ on valittu oikeasta neljänneksestä (mitä se tarkoittaa?).

363. Todistettava: **a)** Kahden kompleksiluvun tulon i) itseisarvo on näiden lukujen itseisarvojen tulo, ii) vaihekulma on näiden lukujen vaihekulmien summa (toisistaan 2π:n monikerroilla eroavat vaihekulmat katsotaan samoiksi). **b)** *Moivren*[1] *kaava*

$$\big(|z| \, (\cos\theta + \mathrm{i} \sin\theta)\big)^n = |z|^n \, (\cos n\theta + \mathrm{i} \sin n\theta).$$

[1] *Abraham de Moivre (1667–1754), ranskalainen matemaatikko.*

364. Olkoon $c_1, c_2 \in \mathbb{R}$. Osoitettava, että on olemassa sellaiset $d_1, d_2 \in \mathbb{C}$, että $c_1 = d_1 + d_2$, $c_2 = \mathrm{i}(d_1 - d_2)$.

365. Ratkaistava rekursioyhtälö

a) $y_{n+2} - 3y_{n+1} - 10y_n = 0$, **b)** $8y_{n+2} - 6y_{n+1} + y_n = 0$.

366. Ratkaistava rekursioyhtälö

a) $y_{n+2} - 2y_{n+1} + y_n = 0$, **b)** $9y_{n+2} - 6y_{n+1} + y_n = 0$.

367. Ratkaistava rekursioyhtälö

a) $y_{n+2} - 2y_{n+1} + 2y_n = 0$, **b)** $3y_{n+2} - 6y_{n+1} + 4y_n = 0$.

368. Määritettävä tehtävien 365, 366 ja 367 a-kohtien rekursioyhtälöiden ratkaisut alkuehdoilla $y_0 = 0$, $y_1 = 1$.

369. Millä a:n (reaali)arvoilla rekursioyhtälön $y_{n+2} - ay_{n+1} - 2a^2y_n = 0$ jokaiselle ratkaisulle on voimassa $\lim\limits_{n\to\infty} y_n = 0$?

370. Johdettava Fibonaccin luvuille lausekkeet ratkaisemalla rekursioyhtälö $y_n = y_{n-1} + y_{n-2}$ alkuehdoilla $y_0 = 0$, $y_1 = 1$.

371. Suoritettava esimerkissä 137 oleva induktiotodistus ja osoitettava, että tapojen 1 ja 2 antamat tulokset ovat samat.

372. Ratkaistava *kolmannen* kertaluvun lineaarinen homogeeninen vakiokertoiminen rekursioyhtälö

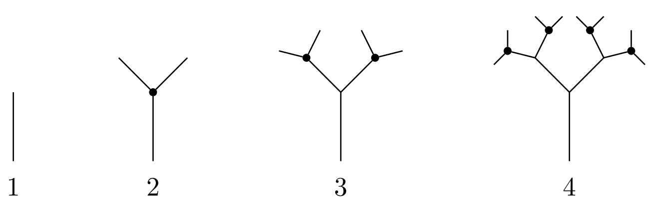
a) $y_{n+3} - 6y_{n+2} + 11y_{n+1} - 6y_n = 0$,

b) $y_{n+3} - 3y_{n+2} + 3y_{n+1} - y_n = 0$.

373. Todistettava lauseen 43 loppuosan kaksi jäljellä olevaa tapausta.

374. Todistettava: Jos rekursioyhtälön $y_{n+2} + ay_{n+1} + by_n = 0$ yleinen ratkaisu on $y_n = R^n(c_1 \cos n\theta + c_2 \sin n\theta)$, niin se voidaan esittää myös muodossa $y_n = AR^n \cos(n\theta + \delta)$, missä A ja δ ovat mielivaltaisia vakioita.

375. Puu kasvaa niin, että joka vuosi sen jokainen latvaoksa haarautuu kahdeksi uudeksi latvaoksaksi. Olkoon y_n latvaoksien lukumäärä n. vuotena ($y_1 = 1$). **a)** Kirjoitettava y_n:lle rekursioyhtälö. **b)** Ratkaistava yhtälö. **c)** Kuinka monta latvaoksaa puussa on 10. vuotena?



376. Rahaa heitetään n kertaa. Olkoon p_n todennäköisyys sille, ettei saada kahta peräkkäistä kruunua. **a)** Määriteltävä lukujono (p_n) rekursiivisesti ja johdettava p_n:lle lauseke. **b)** Millä todennäköisyydellä 12 heitossa ei saada kahta peräkkäistä kruunua? **c)** Mikä yhteys on jonon (p_n) ja Fibonaccin jonon (teht. 370) välillä?

377. Osoitettava, että n:s Fibonaccin luku f_n (teht. 370) saadaan laskemalla $\frac{1}{\sqrt{5}}\big((1+\sqrt{5})/2\big)^n$ ja pyöristämällä tulos lähimpään kokonaislukuun.

378. Todistettava Fibonaccin luvuille rekursioyhtälö $f_n^2 = (-1)^{n+1} + f_{n-1}f_{n+1}$, missä $n \geq 2$.

379. Käsiteltävä kysymys toisen kertaluvun lineaarisen homogeenisen vakiokertoimisen *differentiaaliyhtälön*

$$y'' + ay' + by = 0$$

ratkaisemisesta. Ohje: Etsi sellaisia lukuja r, että (muuttujan x) funktio $y = \mathrm{e}^{rx}$ on tämän differentiaaliyhtälön ratkaisu. Näin saat *karakteristisen yhtälön* r:lle. Sen ei-reaalisten ratkaisujen tapauksessa käytä *Eulerin kaavaa*

$$\mathrm{e}^{\mathrm{i}\theta} = \cos\theta + \mathrm{i}\sin\theta.$$

380. Ratkaistava differentiaaliyhtälö

a) $y'' - 5y' + 6y = 0$, **b)** $y'' + 4y' + 4y = 0$, **c)** $y'' - 2y' + 5y = 0$.

7.2 Lineaarinen vakiokertoiminen rekursioyhtälö

1 Yhteys homogeeniseen yhtälöön

Tarkastelemme nyt toisen kertaluvun lineaarista vakiokertoimista rekursioyhtälöä

$$(R) \qquad y_{n+2} + ay_{n+1} + by_n = d_n,$$

missä a ja b ovat vakioita ja d_n on lukujono eli joukossa $\mathbb{N}$ määritelty funktio. Käytämme vasemmalle puolelle jälleen merkintää $L(y_n)$. Vastaava homogeeninen yhtälö eli lyhemmin *homogeeniyhtälö* on $L(y_n) = 0$ eli

$$(H) \qquad y_{n+2} + ay_{n+1} + by_n = 0.$$

Sanomme rekursioyhtälön *yksityisratkaisuksi* sen yhtä ratkaisua. Siis yksityisratkaisu saadaan yleisestä ratkaisusta antamalla siinä oleville vakioille tietyt arvot.

Lause 44. Rekursioyhtälön (R) yleinen ratkaisu on sen yksityisratkaisun ja vastaavan homogeeniyhtälön (H) yleisen ratkaisun summa.

Tarkemmin sanottuna tämä lause tarkoittaa seuraavaa. Olkoon v_n rekursioyhtälön (R) jokin yksityisratkaisu, olkoon $u_n(c_1, c_2)$ vastaavan homogeeniyhtälön (H) yleinen ratkaisu, ja olkoon w_n (R):n mielivaltainen yksityisratkaisu. Tällöin w_n on muotoa $v_n + u_n(c_1, c_2)$, missä c_1:llä ja c_2:lla on tietyt arvot. Käänteisesti jokainen muotoa $v_n + u_n(c_1, c_2)$ oleva funktio on (R):n ratkaisu.

Todistamme ensin alkuosan. Koska $L(w_n) = d_n$ ja $L(v_n) = d_n$, niin $L(w_n - v_n) = L(w_n) - L(v_n) = d_n - d_n = 0$, joten $w_n - v_n$ toteuttaa (H):n ja on siis muotoa $u_n(c_1, c_2)$. Täten $w_n = v_n + u_n(c_1, c_2)$.

Loppuosa seuraa siitä, että

$$L\big(v_n + u_n(c_1, c_2)\big) = L(v_n) + L\big(u_n(c_1, c_2)\big) = d_n + 0 = d_n.$$

Lause 45. Kun y_0 ja y_1 on annettu, niin rekursioyhtälöllä

$$(R) \qquad y_{n+2} + ay_{n+1} + by_n = d_n$$

on yksikäsitteinen ratkaisu, joka toteuttaa nämä alkuehdot.

Todistus. Samanlainen kuin lauseen 42 todistus.

2 Esimerkkejä

Koska osaamme ratkaista (H):n, niin ainoa uusi tehtävä (R):n ratkaisemisessa on yhden yksityisratkaisun etsiminen. Se onnistuu kokeilemalla sellaisia funktioita, jotka ovat jotenkin samaa tyyppiä kuin d_n.

Esimerkki 138. $y_{n+2} - 2y_{n+1} - 3y_n = 2^n$.

Olemme ratkaisseet homogeeniyhtälön $y_{n+2} - 2y_{n+1} - 3y_n = 0$ esimerkissä 136a saaden tulokseksi $y_n = c_1(-1)^n + c_2 3^n$. Yritämme yksityisratkaisuksi funktiota $y_n = A2^n$ valitsemalla A:n sopivasti. Koska

$$L(A2^n) = A2^{n+2} - 2A2^{n+1} - 3A2^n = -3A2^n,$$

niin täytyy olla $A = -\frac{1}{3}$, joten yksityisratkaisu on $y_n = -(\frac{1}{3})2^n$. Lisäämällä tähän homogeeniyhtälön yleisen ratkaisun saamme $y_n = -(\frac{1}{3})2^n + c_1(-1)^n + c_2 3^n$.

Esimerkki 139. $y_{n+2} - 2y_{n+1} - 3y_n = 3^n$.

Homogeeniyhtälö on sama kuin edellä. Muotoa $y_n = A3^n$ olevan yksityisratkaisun etsiminen ei onnistu. Tämä funktio toteuttaa näet homogeeniyhtälön, joten vasemmaksi puoleksi tulee kaikilla A:n arvoilla 0 eikä siis millään 3^n. Sen sijaan yritys $y_n = nA3^n$ onnistuu. Saamme

$$L(nA3^n) = (n+2)A3^{n+2} - 2(n+1)A3^{n+1} - 3nA3^n = 12A3^n,$$

joten $A = \frac{1}{12}$, yksityisratkaisu on $y_n = \frac{1}{12}n3^n$ ja yleinen ratkaisu on $y_n = \frac{1}{12}n3^n + c_1(-1)^n + c_2 3^n$.

Esimerkki 140. $y_{n+2} - 4y_{n+1} + 4y_n = n$.

Olemme ratkaisseet homogeeniyhtälön esimerkissä 136b saaden tulokseksi $y_n = c_1 2^n + c_2 n 2^n$. Muotoa $y_n = An$ olevaa yksityisratkaisua ei kannata yrittää, sillä sen sijoittaminen vasemmalle puolelle antaa myös vakiotermin. Siksi yritämme funktiota $y_n = An + B$. Koska

$$\begin{aligned} L(An+B) &= A(n+2) + B - 4\bigl(A(n+1)+B\bigr) + 4(An+B) \\ &= An - 2A + B, \end{aligned}$$

niin $A = 1$, $-2A + B = 0$ eli $A = 1$, $B = 2$. Siis yksityisratkaisu on $y_n = n + 2$ ja yleinen ratkaisu on $y_n = n + 2 + c_1 2^n + c_2 n 2^n$.

Esimerkki 141. $y_{n+2} + 9y_n = \cos \frac{n\pi}{4}$.

Olemme ratkaisseet homogeeniyhtälön esimerkissä 136c saaden tulokseksi $y_n = 3^n\bigl(c_1 \cos \frac{n\pi}{2} + c_2 \sin \frac{n\pi}{2}\bigr)$. Muotoa $y_n = A\cos \frac{n\pi}{4}$ olevaa yksityisratkaisua ei kannata yrittää, sillä se antaa myös sinejä. Siksi yritämme funktiota $y_n = A\cos \frac{n\pi}{4} + B \sin \frac{n\pi}{4}$. Saamme

$$\begin{aligned} &L\Bigl(A\cos\frac{n\pi}{4} + B\sin\frac{n\pi}{4}\Bigr) \\ &\quad = A\cos\frac{(n+2)\pi}{4} + B\sin\frac{(n+2)\pi}{4} + 9\Bigl(A\cos\frac{n\pi}{4} + B\sin\frac{n\pi}{4}\Bigr) \\ &\quad = A\Bigl(\cos\frac{n\pi}{4}\cos\frac{\pi}{2} - \sin\frac{n\pi}{4}\sin\frac{\pi}{2}\Bigr) \\ &\qquad\quad + B\Bigl(\sin\frac{n\pi}{4}\cos\frac{\pi}{2} + \cos\frac{n\pi}{4}\sin\frac{\pi}{2}\Bigr) + 9\Bigl(A\cos\frac{n\pi}{4} + B\sin\frac{n\pi}{4}\Bigr) \\ &\quad = -A\sin\frac{n\pi}{4} + B\cos\frac{n\pi}{4} + 9A\cos\frac{n\pi}{4} + 9B\sin\frac{n\pi}{4} \\ &\quad = (9A+B)\cos\frac{n\pi}{4} + (-A+9B)\sin\frac{n\pi}{4}, \end{aligned}$$

joten $9A + B = 1$, $-A + 9B = 0$ eli $A = \frac{9}{82}$, $B = \frac{1}{82}$. Tehtävämme ratkaisu on siis $y_n = \frac{9}{82}\cos\frac{n\pi}{4} + \frac{1}{82}\sin\frac{n\pi}{4} + 3^n\bigl(c_1\cos\frac{n\pi}{2} + c_2\sin\frac{n\pi}{2}\bigr)$.

Luvuissa 7.1 ja 7.2 esitetyillä menetelmillä voidaan ratkaista muidenkin kertalukujen lineaarisia vakiokertoimisia rekursioyhtälöitä.

Harjoitustehtäviä

381. Ratkaistava rekursioyhtälö

a) $y_{n+2} - 3y_{n+1} + 2y_n = 3^n$, **b)** $y_{n+2} - 3y_{n+1} + 2y_n = 2^n$.

382. Ratkaistava rekursioyhtälö

a) $y_{n+2} - 3y_{n+1} + 2y_n = 1$, **b)** $4y_{n+2} - 4y_{n+1} + y_n = 2$.

383. Ratkaistava tehtävien 381a ja 382a rekursioyhtälöt alkuehdoilla $y_0 = 0$, $y_1 = 1$.

384. Ratkaistava rekursioyhtälö

a) $y_{n+2} - y_{n+1} + 2y_n = n^2$, **b)** $y_{n+2} - 2y_{n+1} + y_n = 5 + 3n$.

385. Ratkaistava rekursioyhtälö

a) $y_{n+2} + y_n = \sin \dfrac{n\pi}{2}$, **b)** $8y_{n+2} - 6y_{n+1} + y_n = 5 \sin \dfrac{n\pi}{2}$.

386. Ratkaistava tehtävien 384a ja 385a rekursioyhtälöt alkuehdoilla $y_0 = y_1 = 2$.

387. Ratkaistava rekursioyhtälö $y_{n+2} - 4y_{n+1} + 4y_n = 2^n$.

388. Ratkaistava rekursioyhtälö **a)** $y_{n+1} - 5y_n = n^2$, **b)** $y_{n+1} - 5y_n = 5^n$.

389. Määritettävä rekursioyhtälön $y_{n+1} + ay_n = b$ yleinen ratkaisu ja se yksityisratkaisu, joka saadaan, kun y_0 on annettu. Vrt. teht. 85.

390. Ratkaistava rekursioyhtälö $y_{n+3} - 6y_{n+2} + 11y_{n+1} - 6y_n = n$.

391. Ratkaistava rekursioyhtälö $y_{n+1} - 2y_n = y_n y_{n+1}$ palauttamalla se sopivalla sijoituksella lineaariseksi.

392. Millä a:n arvoilla rekursioyhtälöllä $y_{n+2} + y_{n+1} - ay_n = 1$ on vakioratkaisu?

393. Olkoon Y_t erään maan kansantulo vuonna t. *Samuelsonin*[2] *mallin* mukaan

$$Y_t = \alpha(1 + \beta)Y_{t-1} - \alpha\beta Y_{t-2} + 1,$$

missä α ja β ovat positiivisia vakioita. Tutkittava kansantulon kehitystä, kun **a)** $\alpha = 0{,}5$, $\beta = 1$, **b)** $\alpha = 0{,}8$, $\beta = 2$.

394. Eläinpopulaation kasvua kuvataan rekursioyhtälöllä $p_{n+1} = q(1 - rp_n)p_n$, missä p_n on populaation koko n. vuotena, $q > 1$ on kasvukerroin ja $r \geq 0$ on hidastumiskerroin. Eräässä mallissa $q = 2{,}7$ ja $r = 0{,}001$. Tutkittava populaation kehitystä 10 vuoden aikana ja esitettävä se graafisesti, kun alkupopulaatio p_0 on **a)** 100, **b)** 25, **c)** 800.

395. Pelaajat A ja B heittävät vuorotellen rahaa. Pelin voittaa se, joka saa ensimmäisenä kruunun. Edellisen pelin voittaja saa aloittaa seuraavan pelin. Ensimmäisen pelin aloittaa A. Olkoon p_n todennäköisyys sille, että hän voittaa n:nnen pelin. **a)** Laskettava p_1. **b)** Muodostettava p_n:lle rekursioyhtälö. **c)** Ratkaistava tämä rekursioyhtälö. **d)** Millä todennäköisyydellä A voittaa i) viidennen, ii) kymmenennen pelin?

396. K. R. Gabriel ja J. Neumann [*Quart. J. R. Met. Soc.* **88** (1962), 90–95] ovat tutkineet, voidaanko siitä, sataako Tel Avivissa tänään vai ei, ennustaa sitä, sataako siellä huomenna vai ei. Vuosien 1923–1950 aineiston perusteella he päättelivät, että marraskuussa sadepäivää seuraa sadepäivä todennäköisyydellä 0,60 ja poutapäivää seuraa poutapäivä todennäköisyydellä 0,87. Oletetaan, että Tel Avivissa on sateinen marraskuun päivä. Millä todennäköisyydellä siellä on sadetta **a)** ylihuomenna,

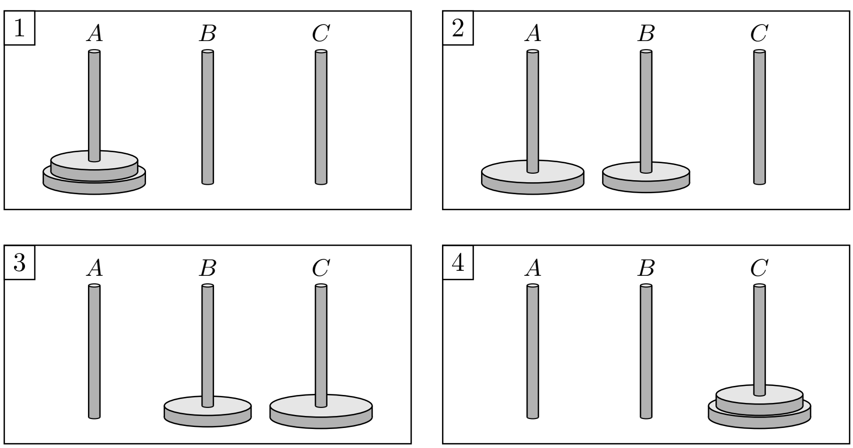
[2] *Paul Samuelson (1915–), yhdysvaltalainen taloustieteilijä.*

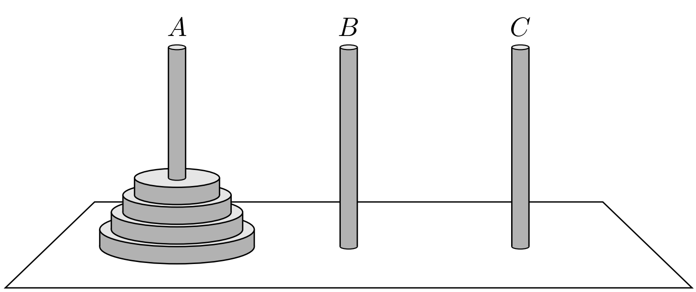
b) viikon kuluttua, **c)** koko viikon, **d)** vuoden kuluttua? Ohje: Olkoon p_n todennäköisyys sille, että n päivän kuluttua sataa. Muodosta ensimmäisen kertaluvun rekursioyhtälö p_n:lle ja ratkaise se.

397 (Uhkapelurin vararikko-ongelma). Peluri voittaa yhdessä pelissä yhden euron todennäköisyydellä p ja häviää yhden euron todennäköisyydellä $q = 1 - p$. Hänen alkupääomansa on k euroa ja tavoitteensa on n euroa ($n > k$). Jos pelurin rahat loppuvat, niin hänen on lopetettava pelaaminen. Millä todennäköisyydellä peluri saavuttaa tavoitteensa?

398. Seuraavassa ”todistetaan” lause 45 vääräksi. Tarkastellaan rekursioyhtälöä $y_{n+2} + y_n = 2$ alkuehdoilla $y_0 = 1$ ja $y_2 = 1$. Jokainen funktio $y_n = c \sin \frac{n\pi}{2} + 1$, missä c on mielivaltainen vakio, on sen ratkaisu, joten ratkaisu ei olekaan yksikäsitteinen. Missä vika?

399 (Hanoin tornit). Kolme keppiä A, B ja C on pystytetty maahan. Kepissä A on n rengasta päällekkäin suuruusjärjestyksessä alhaalta ylöspäin. Tehtävänä on saada kaikki renkaat keppiin C siirtämällä yhtä kerrallaan niin, että missään vaiheessa niitä ei ole pienemmän renkaan päällä ja että jokainen rengas on aina jossakin kepeistä A, B ja C. Alla olevissa kuvissa on tehtävän ratkaisu tapauksessa $n = 2$ sekä alkutilanne tapauksessa $n = 4$.





a) Ratkaistava tehtävä tapauksessa $n = 4$.

b) Miten voidaan edellisen perusteella käsitellä tapaus $n = 5$?

c) Jos tehtävä on ratkaistu tapauksessa $n = k$, niin miten se silloin voidaan ratkaista tapauksessa $n = k + 1$?

d) Osoitettava, että n renkaan tapauksessa tämä tehtävä voidaan suorittaa $2^n - 1$ siirrolla.

400. Lineaarisia vakiokertoimisia *differentiaaliyhtälöitä* ratkaistaan samalla periaatteella kuin rekursioyhtälöitä (ks. teht. 379). Ratkaistava differentiaaliyhtälö

a) $y'' + 2y' + y = x$, **b)** $y'' + 9y = \cos x$, **c)** $y'' - y' + 2y = \mathrm{e}^{-x}$.

∗Luku 8

Automaatit ja muodolliset kielet

Kuvan alla oli kolme pientä hyönteistä: BOY (*poika*). *Hän oli juuri keksinyt, että nuo kolme kirjainta toistuivat kirjan sivulla monta kertaa samassa järjestyksessä. . . . Näin Tarzan edistyi kovin hitaasti, sillä hän oli tietämättään ottanut itselleen erittäin vaikean ja vaivalloisen urakan . . . oppia lukemaan tietämättä yhtään mitään kirjaimista tai kirjakielestä tai edes aavistamatta sellaisen olevan olemassa.*

(*Burroughs* [1])

8.1 Säännölliset lausekkeet ja säännölliset kielet

1 Johdanto

Luonnolliset kielet, kuten esimerkiksi suomi ja englanti, ovat syntyneet kaiken inhimillisen kommunikaation tarpeisiin. Sen sijaan *muodolliset kielet* ovat tarkoitetut tiettyyn täysin rajattuun kommunikaatioon. Luonnollisten kielten kehitys on vienyt tuhansia vuosia, kun taas muodolliset kielet on tavallisesti laadittu lyhyehkössä ajassa. Luonnolliset kielet ovat kehittyneet melko vapaasti, kunnes niistä tuli ”sivistyskieliä”, jolloin niiden kehitystä alettiin ohjailla. Sen sijaan muodollisia kieliä ovat tehneet täysin määrätyt henkilöt aivan haluamallaan tavalla.

Kielen *syntaksi* eli *kielioppi* selvittää, mitkä ilmaisut kuuluvat tähän kieleen eli ovat ”kieliopillisesti” oikeita. Kielen *semantiikka* eli *merkitysoppi* selvittää, mitä nämä ilmaisut tarkoittavat. Luonnollisen kielen syntaksi on erittäin monimutkainen ja semantiikka vieläkin monimutkaisempi, kun taas muodolliset kielet pyritään laatimaan niin, että niiden syntaksi ja semantiikka olisivat mahdollisimman yksinkertaiset.

Luonnollista kieltä puhutaan ja kirjoitetaan asettamalla sanoja peräkkäin, joten tällaisen kielen perusyksikkö on sana. Voitaisiin ajatella, että perusyksikön pitäisi olla kirjain tai äänne, koska sanat saadaan asettamalla niitä peräkkäin. Näin ei kuitenkaan ole, koska yksittäisellä kirjaimella tai äänteellä ei ole omaa itsenäistä merkitystä.

Olkoon Σ epätyhjä äärellinen joukko. Kutsumme sitä *aakkostoksi* ja sen alkioita *aakkosiksi*, *kirjaimiksi* tai *merkeiksi*. Merkitsemme Σ^*:llä kaikkien niiden äärellisten jonojen joukkoa, jotka saadaan kirjoittamalla aakkosia peräkkäin. Kutsumme joukon Σ^* osajoukkoa L *muodolliseksi kieleksi.* Siihen voi kuulua myös *tyhjä jono* ε, jossa ei ole yhtään aakkosta. (Tyhjä jono ei kylläkään ole järjestetty jono s. 110 määritelmän mielessä, koska emme pidä "tyhjää kuvausta" kuvauksena.) Kutsumme joukon L alkioita kielen L *sanoiksi. Tyhjässä kielessä* $\emptyset$ ei ole yhtään sanaa, ei edes tyhjää sanaa. Kieli $\{\varepsilon\}$ on epätyhjä, vaikka siihen kuuluu vain tyhjä sana ε. Samastamme yksikirjaimiset jonot ja kirjaimet. Siis kirjaimet ovat yksikirjaimisia sanoja.

Jos joukon Σ alkiot ovat luonnollisen kielen sanoja, saattaa tuntua oudolta kutsua niitä aakkosiksi. Tällöin voimme kutsua niitä *sanoiksi* ja joukon L alkioita kielen L *lauseiksi.*

Kieli L on *äärellinen* tai *ääretön* sen mukaan, onko siinä äärellinen vai ääretön määrä sanoja. Jos L on äärellinen ja sen sanojen lukumäärä on pienehkö, sen syntaksi voidaan esittää luettelemalla sen kaikki sanat.

Esimerkki 142. Veikattaessa vakioveikkauksen yhtä kohdetta (mahdollisesti järjestelmällä) käytetään yksinkertaista muodollista kieltä L, jonka aakkosto $\Sigma = \{1, \times, 2\}$. Kielen L syntaksin saamme luettelemalla tämän kielen kaikki sanat eli muodostamalla joukon $L = \{1, \times, 2, 1\times, 12, \times 2, 1\times 2\}$. Tämän kielen semantiikka on seuraava:

Merkintä	Tulkinta
1	'kotijoukkue voittaa'
$\times$	'tulee tasapeli'
2	'vierasjoukkue voittaa'
$1\times$	'kotijoukkue voittaa tai tulee tasapeli'
12	'kotijoukkue tai vierasjoukkue voittaa'
$\times 2$	'vierasjoukkue voittaa tai tulee tasapeli'
1×2	'ottelu voi päättyä miten tahansa'

Esimerkki 143. Armeijan nk. sulkeisten komentokieli L on täsmällisesti määritelty, joten voimme pitää sitä muodollisena kielenä. Sen aakkosto $\Sigma = \{$asento, lepo, käännös, vasempaan, oikeaan, $\ldots\}$ (mutta äärellinen). Esimerkiksi 'asento' ja 'käännös vasempaan päin' kuuluvat kieleen L, mutta 'käännös vasempaan' ei kuulu. Tämän kielen semantiikassa jokaisella sanalla on täysin määrätty merkitys. Esimerkiksi 'lepo' ei tarkoita tavallista lepäämistä.

Esimerkki 144. Lauselogiikan kieli L on muodollinen kieli. Sen aakkosto $\Sigma = \{p, q, \ldots, p_0, p_1, p_2, \ldots, \neg, \vee, \wedge, \Rightarrow, \Leftrightarrow, (,)\}$ Voimme pitää tätä aakkostoa äärellisenä, sillä vaikka lausemuuttujia p_0, p_1, $p_2, \ldots$ onkin ääretön määrä, ne voidaan esittää käyttämällä vain kahta merkkiä esimerkiksi seuraavasti: $p_0 = p'$, $p_1 = p''$, $p_2 = p'''$, ... Määrittelimme aiemmin (s. 42) tämän kielen syntaksin niin, että L on kaikkien propositiolauseiden eli hyvinmuodostettujen kaavojen joukko. Semantiikan saamme totuusarvoilla, jotka voimme määritellä täsmällisesti totuusjakauman eli valuaation käsitteen kautta (s. 44).

Esimerkki 145. Tietokoneiden ohjelmointikielet ovat muodollisia kieliä.

2 Kielten laskutoimituksia

Tästä eteenpäin tarkoitamme kielellä muodollista kieltä, ellei tosin mainita.

Koska muodolliset kielet ovat joukkoja, niin voimme määritellä niille tavanomaiset joukko-opin laskutoimitukset, joista kiinnostavin on yhdiste. Kielet eivät kuitenkaan ole mitä tahansa joukkoja, vaan sellaisia, joiden alkiot ovat merkkijonoja. Siksi määrittelemme niille pari uutta laskutoimitusta.

Sanojen α ja β *ketju* eli *konkatenaatio* $\alpha \cdot \beta$ saadaan kirjoittamalla peräkkäin nämä sanat. Vastaavasti määrittelemme useamman kuin kahden sanan ketjun. Selvästi on voimassa liitäntälaki $\alpha{\cdot}(\beta{\cdot}\gamma) = (\alpha{\cdot}\beta){\cdot}\gamma = \alpha{\cdot}\beta{\cdot}\gamma$.

Kielten L ja K ketjun eli konkatenaation $L \cdot K$ sanat ovat L:n sanan ja K:n sanan ketjuja. Siis

$$L \cdot K = \{\, \alpha \cdot \beta \mid \alpha \in L,\ \beta \in K \,\}.$$

Voimme käyttää merkintöjen $\alpha \cdot \beta$ ja $L \cdot K$ sijasta lyhempiä merkintöjä $\alpha\beta$ ja LK. Vastaavasti määrittelemme useamman kuin kahden kielen ketjun. Selvästi on voimassa liitäntälaki $L \cdot (K \cdot H) = (L \cdot K) \cdot H = L \cdot K \cdot H$.

Seuraavaksi määrittelemme sanan α *potenssin*

$$\begin{aligned} \alpha^n &= \alpha \cdots \alpha \quad (n \text{ kappaletta}), \\ \alpha^1 &= \alpha, \\ \alpha^0 &= \varepsilon. \end{aligned}$$

Vastaavasti määrittelemme kielen L potenssin

$$\begin{aligned} L^n &= L \cdots L \quad (n \text{ kappaletta}), \\ L^1 &= L, \\ L^0 &= \{\varepsilon\}. \end{aligned}$$

Lopuksi määrittelemme, että kielen L *Kleenen*[1] *sulkeuma* on L:n kaikkien potenssien yhdiste

$$L^* = L^0 \cup L^1 \cup L^2 \cup \cdots$$

Esimerkki 146. Kun $a \in \Sigma$, niin

$$\{a\}^* = \{\, a^n \mid n \in \mathbb{N} \,\} = \{\varepsilon, a, aa, aaa, \ldots\}.$$

Esimerkki 147. $\emptyset^* = \{\varepsilon\}$.

Esimerkki 148. Kielille $L = \{a, b\}$ ja $K = \{x, y\}$ on

$$\begin{aligned} L \cdot K &= \{ax, ay, bx, by\}, \\ L^2 &= \{a^2, ab, ba, b^2\}, \\ L^* &= \{\varepsilon, a, b, a^2, ab, ba, b^2, a^3, a^2b, aba, ab^2, ba^2, bab, b^2a, b^3, a^4, \ldots\}. \end{aligned}$$

[1] *Stephen C. Kleene (1909–1994), yhdysvaltalainen loogikko.*

3 Säännöllinen lauseke

Olkoon L kieli, jonka aakkosto on Σ, eli olkoon L joukon Σ^* osajoukko. Voimme joskus (mutta emme aina, ks. teht. 420) määritellä L:n käyttämällä luonnollista kieltä tai tavanomaisia joukkomerkintöjä.

Esimerkki 149. Olkoon Σ suomen kielen aakkosto. Määrittelemme erään kielen L kolmella muodollisesti erilaisella tavalla. **a)** Käytämme luonnollista kieltä. Kieli L on kaikkien niiden sanojen joukko, jotka alkavat a:lla ja päättyvät $ö$:hön. **b)** Kirjoitamme äärettömänä luettelona

$$L = \{aö, a^2ö, abö, \ldots, aö^2, a^3ö, a^2bö, \ldots, aö^3, a^4ö, \ldots\},$$

mutta L:n muodostamissääntö ei näy siitä kovin hyvin. **c)** Parempi merkintä on

$$L = \{\, a\xi ö \mid \xi \in \Sigma^* \,\}.$$

Kun muodollisia kieliä tutkitaan, ne pyritään määrittelemään lyhyesti ja täsmällisesti. Luonnollinen kieli ei sovi hyvin tähän tarkoitukseen. Joukkomerkintä kylläkin sopii eräiden kielten määrittelyyn, mutta tiettyjä kieliä voidaan määritellä parhaiten *säännöllisillä lausekkeilla*. Nämä lausekkeet muodostavat eräänlaisen *metakielen* eli sellaisen muodollisen kielen, jolla määritellään muodollisia kieliä. Olkoon Σ aakkosto. Säännöllisten lausekkeiden kielen L aakkosto on $\Sigma \cup \{\emptyset, \varepsilon, (,), \cup, \cdot, ^*\}$ ja syntaksi on seuraava.

1. $\emptyset$ on säännöllinen lauseke.
2. ε on säännöllinen lauseke.
3. Jos $a \in \Sigma$, niin a on säännöllinen lauseke.
4. Jos ξ ja η ovat säännöllisiä lausekkeita, niin $(\xi \cup \eta)$ ja $(\xi \cdot \eta)$ ovat säännöllisiä lausekkeita.
5. Jos x on säännöllinen lauseke, niin x^* on säännöllinen lauseke.
6. Muita säännöllisiä lausekkeita ei ole.

Määrittelemme nyt kielen L semantiikan. Käytämme säännöllisestä lausekkeesta lyhennystä s.l.

1. S.l. $\emptyset$ tarkoittaa tyhjää joukkoa $\emptyset$.
2. S.l. ε tarkoittaa tyhjän sanan muodostamaa joukkoa $\{\varepsilon\}$.
3. Jos $a \in \Sigma$, niin s.l. a tarkoittaa joukkoa $\{a\}$.
4. Jos s.l. ξ tarkoittaa joukkoa X ja s.l. η joukkoa Y, niin s.l. $(\xi \cup \eta)$ tarkoittaa joukkoa $X \cup Y$ ja s.l. $(\xi \cdot \eta)$ joukkoa $X \cdot Y$ eli lyhemmin joukkoa XY.
5. Jos s.l. ξ tarkoittaa joukkoa X, niin s.l. ξ^* tarkoittaa joukkoa X^*.

Seuraavissa esimerkeissä Σ on suomen kielen aakkosten joukko.

Esimerkki 150. **a)** S.l. $(a \cup (b \cup c))$ tarkoittaa joukkoa $\{a\} \cup (\{b\} \cup \{c\}) = \{a, b, c\}$. **b)** S.l. $\big((t \cup (h \cup l)) \cdot (u \cdot (p \cdot u))\big)$ tarkoittaa joukkoa $\{\mathit{tupu}, \mathit{hupu}, \mathit{lupu}\}$. **c)** S.l. $(\emptyset \cup a)$ tarkoittaa joukkoa $\{a\}$, mutta $(\varepsilon \cup a)$ tarkoittaa joukkoa $\{\varepsilon, a\}$. **d)** S.l. $(\emptyset \cdot a)$ tarkoittaa joukkoa $\emptyset$, mutta $(\varepsilon \cdot a)$ tarkoittaa joukkoa $\{a\}$. **e)** S.l. $(a \cup (b \cup (c \cup (\ldots (\ddot{a} \cup \ddot{o})))) \ldots)$ (kirjoitettuna kokonaisuudessaan) tarkoittaa joukkoa Σ.

Esimerkki 151. **a)** S.l. $(a \cdot b)^*$ tarkoittaa joukkoa $\{\varepsilon, ab, (ab)^2, (ab)^3, \ldots\}$. **b)** S.l. $\big(a \cdot (\xi^* \cdot \ddot{o})\big)$, missä ξ on esimerkin 150e s.l., tarkoittaa niiden sanojen joukkoa, jotka alkavat a:lla ja päättyvät $\ddot{o}$:hön, vrt. esim. 149. **c)** S.l. $\big(\xi \cdot ((a \cup \ddot{o}) \cdot \xi^*)\big)$, missä ξ on kuten edellä, tarkoittaa niiden sanojen joukkoa, joissa on ainakin kaksi kirjainta ja järjestyksessä toinen kirjain on a tai $\ddot{o}$.

Olkoot ξ, η ja ζ säännöllisiä lausekkeita, jotka tarkoittavat joukkoja X, Y ja Z. Tällöin säännölliset lausekkeet $\big(\xi \cup (\eta \cup \zeta)\big)$ ja $\big((\xi \cup \eta) \cup \zeta\big)$ tarkoittavat samaa joukkoa. Nimittäin edellisen merkitys on $X \cup (Y \cup Z)$ ja jälkimmäisen $(X \cup Y) \cup Z$, ja yhdisteen liitäntälain perusteella nämä joukot ovat samat. Siksi voimme jättää kaikki sulut pois ja kirjoittaa $\xi \cup \eta \cup \zeta$. Vastaavasti huomaamme, että säännölliset lausekkeet $\big(\xi \cdot (\eta \cdot \zeta)\big)$ ja $\big((\xi \cdot \eta) \cdot \zeta\big)$ tarkoittavat samaa joukkoa $X \cdot Y \cdot Z$, joten voimme nytkin kirjoittaa ilman sulkuja $\xi \cdot \eta \cdot \zeta$. Voimme menetellä samoin silloinkin, kun säännöllisiä lausekkeita on enemmän kuin kolme.

Esimerkki 152. S.l. $(a \cup b \cup c) \cdot d^* \cdot e \cdot f$ tarkoittaa niiden sanojen joukkoa, joiden kirjaimista ensimmäinen on a, b tai c, viimeistä edellinen on e, viimeinen on f, ja kaikki muut, mikäli niitä on, ovat d:itä.

4 Säännöllinen kieli

Kutsumme *säännölliseksi kieleksi* (lyhennettynä s.k.) sellaista kieltä, joka voidaan määritellä säännöllisellä lausekkeella. Kaikki edellisissä esimerkeissä tarkastelemamme kielet ovat säännöllisiä. Myös ei-säännöllisiä kieliä on olemassa (teht. 419 ja esim. 156).

Säännöllisyys säilyy yhdisteessä, ketjussa ja Kleenen sulkeumassa.

Lause 46. Olkoon Σ aakkosto. Tällöin

1. $\emptyset$ on s.k.
2. $\{\varepsilon\}$ on s.k.
3. Jos $a \in \Sigma$, niin $\{a\}$ on s.k.
4. Jos L ja K ovat säännöllisiä kieliä, niin $L \cup K$ ja $L \cdot K$ ovat säännöllisiä kieliä.
5. Jos L on s.k., niin L^* on s.k.
6. Muita säännöllisiä kieliä ei ole.

Todistamme lauseen alkuosan ja jätämme loppuosan harjoitustehtäviksi (teht. 412–413).

1. Tyhjä kieli $\emptyset$ on s.k., koska sen määrittelee s.l. $\emptyset$.

2. Kieli $\{\varepsilon\}$ on s.k., koska sen määrittelee s.l. ε.

3. Kun $a \in \Sigma$, niin $\{a\}$ on s.k., koska sen määrittelee s.l. a.

4 (yhdiste). Jos s.l. ξ määrittelee kielen L ja s.l. η kielen K, niin s.l. $(\xi \cup \eta)$ määrittelee kielen $L \cup K$.

Ominaisuus 4 on voimassa useammallekin kuin kahdelle kielelle (teht. 414). Myös komplementti $\overline{L}$ ja leikkaus $L \cap K$ ovat säännöllisiä (teht. 435–436).

Harjoitustehtäviä

401. Muodostettava kielen L määrittelevä s.l., kun L koostuu niistä bittijonoista, **a)** joiden pituus on kaksi bittiä, **b)** jotka alkavat ja päättyvät ykkösellä, **c)** joissa on täsmälleen kaksi ykköstä, **d)** joissa ei ole peräkkäisiä ykkösiä.

402. Kuvailtava luonnollisella kielellä tai joukkona se kieli, jonka määrittelee s.l. **a)** $(0 \cup 1) \cdot 0 \cdot 1$, **b)** $\emptyset \cup \varepsilon \cup 0 \cup 1$, **c)** $1^2 \cdot (0 \cup 1)^*$, **d)** $(0 \cup 1)^* \cdot (0 \cup 1)^3$.

403. Olkoon $\Sigma = \{a, b, c\}$. Muodostettava kielen L määrittelevä s.l., kun L koostuu niistä sanoista, joissa a-kirjaimia on **a)** ainakin kaksi, **b)** korkeintaan kaksi, **c)** parillinen määrä, **d)** pariton määrä.

404. Olkoon $\Sigma = \{a, b, c\}$. Kuvailtava luonnollisella kielellä tai joukkona se kieli, jonka määrittelee s.l. **a)** $(a \cup b) \cdot c^2$, **b)** $(a \cup b \cup c)^* \cdot a \cdot (a \cup b \cup c)^*$, **c)** $(a \cup b \cup c)^* \cdot a \cdot (a \cup b \cup c)$, **d)** $a \cdot a^* \cdot b \cdot b^*$.

405. Tarkoittakoon $\xi \equiv \eta$ sitä, että säännöllisillä lausekkeilla ξ ja η on sama merkitys eli ne vastaavat samaa joukkoa. Olemme todenneet, että liitäntälait $\xi \cup (\eta \cup \zeta) \equiv (\xi \cup \eta) \cup \zeta$ ja $\xi \cdot (\eta \cdot \zeta) \equiv (\xi \cdot \eta) \cdot \zeta$ ovat yleisesti voimassa. Ovatko voimassa **a)** vaihdantalait $\xi \cup \eta \equiv \eta \cup \xi$ ja $\xi \cdot \eta \equiv \eta \cdot \xi$, **b)** osittelulait $\xi \cdot (\eta \cup \zeta) \equiv (\xi \cdot \eta) \cup (\xi \cdot \zeta)$ ja $(\xi \cup \eta) \cdot \zeta \equiv (\xi \cdot \zeta) \cup (\eta \cdot \zeta)$?

406. Mitä sääntöjä kielten välinen ketju noudattaa edellisen tehtävän perusteella ja mitä se ei noudata?

407. Määriteltävä rekursiivisesti **a)** sanan, **b)** kielen potenssi.

408. Olkoon L kieli ja $m, n \in \mathbb{N}$. Onko yleisesti voimassa **a)** samankantaisten potenssien ketjusääntö $L^m \cdot L^n = L^{m+n}$, **b)** potenssin potenssin sääntö $(L^m)^n = L^{mn}$?

409. Olkoot L ja K kieliä ja olkoon $n \in \mathbb{N}$. Onko ketjun potenssin sääntö $(L \cdot K)^n = L^n \cdot K^n$ yleisesti voimassa?

410. Onko säännöllisille lausekkeille yleisesti voimassa **a)** $(\xi^*)^* \equiv \xi^*$, **b)** $(\xi \cup \eta)^* \equiv \xi^* \cup \eta^*$, **c)** $(\xi \cdot \eta)^* \equiv \xi^* \cdot \eta^*$?

411. Mitä sääntöjä kielen Kleenen sulkeuma noudattaa edellisen tehtävän perusteella ja mitä se ei noudata?

412. Todistettava, että **a)** kahden säännöllisen kielen ketju, **b)** säännöllisen kielen Kleenen sulkeuma on säännöllinen.

413. Todistettava, ettei ole olemassa muita säännöllisiä kieliä kuin lauseessa 46 mainitut.

414. Todistettava, että säännöllisten kielten äärellinen **a)** yhdiste, **b)** ketju, **c)** potenssi on säännöllinen.

415. Olkoon Σ aakkosto. Sanan $\alpha \in \Sigma^*$ *pituus* $l(\alpha)$ tarkoittaa sen kirjainten lukumäärää. **a)** Määriteltävä tämä käsite rekursiivisesti. **b)** Todistettava: Sanoille α ja β on $l(\alpha \cdot \beta) = l(\alpha) + l(\beta)$. **c)** Yleistettävä tämä n:lle sanalle ja osoitettava sen perusteella, että $l(\alpha^n) = nl(\alpha)$.

416. Olkoon Σ aakkosto. Sanan $\alpha \in \Sigma^*$ *toisinpäinen sana* α' saadaan kirjoittamalla α:n kirjaimet päinvastaisessa järjestyksessä. **a)** Määriteltävä tämä käsite rekursiivisesti. **b)** Todistettava: Sanoille α ja β on $(\alpha \cdot \beta)' = \beta' \cdot \alpha'$.

417. Kielen L *toisinpäinen kieli* L' on sen toisinpäisten sanojen joukko. Siis $L' = \{\, \alpha' \mid \alpha \in L \,\}$. Olkoot L ja K kieliä. Todistettava oikeaksi tai vääräksi: **a)** $(L \cup K)' = L' \cup K'$, **b)** $(L \cdot K)' = L' \cdot K'$.

418. Todistettava, että säännöllisen kielen toisinpäinen kieli on säännöllinen.

419. Osoitettava, että (tietyssä aakkostossa) **a)** i) säännöllisten lausekkeiden, ii) säännöllisten kielten joukko on numeroituva, mutta **b)** kaikkien kielten joukko on ylinumeroituva. **c)** Pääteltävä tästä, että on olemassa ei-säännöllisiä kieliä.

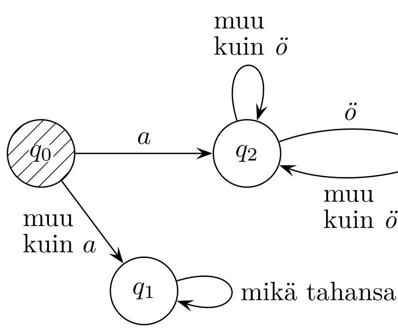
420. Osoitettava, että (tietyssä aakkostossa) **a)** kaikki säännölliset kielet voidaan periaatteessa määritellä luonnollisella kielellä, mutta **b)** kaikkia kieliä ei voida.

8.2 Automaatit

1 Automaatin käsite

Jos tietyllä ohjelmointikielellä L laaditussa tietokoneohjelmassa on syntaktinen virhe eli kieleen L kuulumaton sana, niin kone antaa virheilmoituksen. Tietokone siis ”tunnistaa” kielen L ”hyväksymällä” sen sanat ja ”hylkäämällä” muut. Alamme nyt tutkia kysymystä, voidaanko muodollisia kieliä yleensäkin tunnistaa abstrakteilla ”koneilla”.

Esimerkki 153. Tarkastelimme esimerkissä 149 sitä kieltä L, jonka sanat ovat a-alkuisia ja $ö$-loppuisia suomen kielen kirjaimista muodostettuja sanoja. Teemme abstraktin ”koneen” M, joka hyväksyy kielen L kaikki sanat ja vain ne. Aluksi M on ”alkutilassa q_0”, jossa se lukee sanan ensimmäisen kirjaimen. Jos kirjain ei ole a, niin M hylkää sanan siirtymällä ”hylkäystilaan q_1”. Jos taas se on a, niin M siirtyy ”uuteen tilaan q_2”, jossa se lukee seuraavan kirjaimen. Jos tämä kirjain on $ö$, niin M siirtyy ”lopputilaan q_3”. Jos sana päättyy tähän, niin M hyväksyy sen. Muussa tapauksessa M lukee seuraavan kirjaimen ja pysyy tilassa q_3 tai siirtyy tilaan q_2 sen mukaan, onko luettu kirjain $ö$ vai jokin muu. Näin jatketaan, kunnes sanan kaikki kirjaimet on luettu. Jos ja vain jos M on silloin tilassa q_3, niin se hyväksyy sanan. Voimme esittää tämän kaiken *tiladiagrammilla*, jossa alkutila on viivoitettu ja lopputila on ympyröity kahdesti.



Yleisesti kutsumme *äärelliseksi automaatiksi* yhdelmää $M = (Q, \Sigma, \delta, q_0, F)$. Tässä *tilojen joukko* Q ja (*syöte*)*aakkosto* Σ ovat epätyhjiä äärellisiä joukkoja, *siirtymäfunktio* δ on kuvaus $Q \times \Sigma \to Q$, *alkutila* q_0 on tilajoukon Q alkio, ja *lopputilojen joukko* F on tämän joukon osajoukko. Jos $q \in Q$ ja $s \in \Sigma$, niin $\delta(q, s)$ ilmoittaa, mihin tilaan M siirtyy luettuaan tilassa q merkin s.

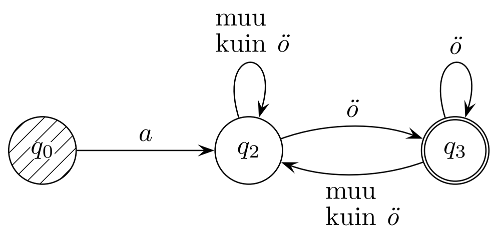
Emme käsittele muita automaatteja kuin äärellisiä. Siksi puhumme lyhyesti automaatista, kun tarkoitamme äärellistä automaattia.

Automaatti M *hyväksyy* eli *tunnistaa* sanan $\sigma \in \Sigma^*$, jos se on σ:n lukemisen jälkeen jossakin lopputilassa. Automaatin M hyväksymät sanat muodostavat sen määrittelemän eli hyväksymän eli tunnistaman *kielen*.

Esimerkki 153, jatkoa. ”Kone” M on automaatti $M = (Q, \Sigma, \delta, q_0, F)$, missä $Q = \{q_0, q_1, q_2, q_3\}$, $\Sigma = \{a, b, \ldots, ö\}$, $F = \{q_3\}$, ja

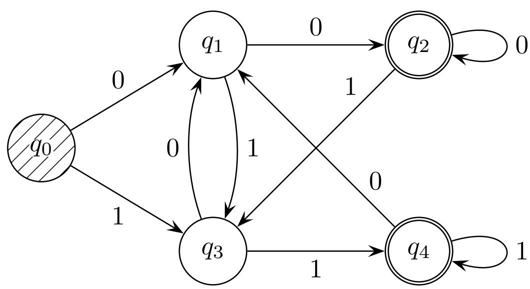
$$\begin{aligned}
&\delta(q_0, a) = q_2, && \delta(q_0, \xi) = q_1, \text{ kun } \xi \neq a,\\
&\delta(q_1, \xi) = q_1 \text{ kaikilla } \xi \in \Sigma, &&\\
&\delta(q_2, \ddot{o}) = q_3, && \delta(q_2, \xi) = q_2, \text{ kun } \xi \neq \ddot{o},\\
&\delta(q_3, \ddot{o}) = q_3, && \delta(q_3, \xi) = q_2, \text{ kun } \xi \neq \ddot{o}.
\end{aligned}$$

Jos M joutuu tilaan q_1, niin se pysyy siinä eikä missään tapauksessa tule hyväksymään käsittelemäänsä sanaa. Meidän ei välttämättä tarvitse piirtää tuollaista ”roskatilaa” näkyviin. Sovimme, että ne merkit, joita vastaavia nuolia ei ole tiladiagrammissa, johtavat ”roskatilaan” eli aiheuttavat hylkäämisen.



Lopputiloja voi olla enemmänkin kuin yksi. On myös mahdollista, ettei niitä ole yhtään, mutta sellaiset automaatit eivät ole kiinnostavia.

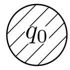
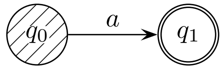
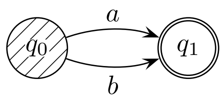
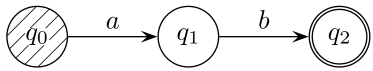
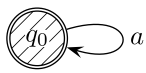
Esimerkki 154. Kuvion automaatin tunnistama kieli koostuu niistä bittijonoista, jotka päättyvät (ainakin) kahteen peräkkäiseen nollaan tai (ainakin) kahteen peräkkäiseen ykköseen.



2 Automaattien ja säännöllisten kielten yhteys

Säännöllisen kielen määritelmän mukaan säännölliset lausekkeet ja säännölliset kielet vastaavat toisiaan. Tarkastelemme nyt näiden ja automaattien vastaavuutta.

Olkoon $a, b \in \Sigma$. Käymme läpi yksinkertaisimmat säännölliset lausekkeet sekä niitä vastaavat automaatit ja kielet.

s.l.	automaatti	kieli
$\emptyset$		$\emptyset$
ε		$\{\varepsilon\}$
a		$\{a\}$
$a \cup b$		$\{a, b\}$
$a \cdot b$		$\{ab\}$
a^*		$\{\varepsilon, a, a^2, a^3, \ldots\}$

Koska jokainen automaatti voidaan muodostaa yllä olevista ”rakennuspalikoista”, niin olemme havainnollisesti perustelleet seuraavan lauseen. (Täsmällinen todistus, ks. esim. [17, 19, 21].) Muistamme, että tarkoitamme automaatilla äärellistä automaattia.

Lause 47. Kieli on säännöllinen, jos ja vain jos se voidaan tunnistaa automaatilla.

Olkoot M ja N automaatteja sekä olkoot L ja K niiden tunnistamat kielet. Lauseen 46 mukaan kielet $L \cup K$, $L \cdot K$ ja L^* ovat säännöllisiä, joten kysymme, mitkä automaatit tunnistavat nämä kielet.

Sovimme, että automaatti voi vaihtaa tilaa myös lukematta mitään merkkiä eli lukemalla ”tyhjän merkin” ε (jota emme kuitenkaan pidä aakkosena). Sanomme, että tällöin tapahtuu *ε-siirto*.

Yleisemmin määrittelemme *epädeterministisen automaatin*, joka voi olla (ε-siirron jälkeen) samanaikaisesti useammassa kuin yhdessä tilassa tai ei yhdessäkään tilassa. Automaatti, jossa on ε-siirto, on epädeterministinen, koska se on samanaikaisesti sekä ε-siirtoa edeltävässä että sitä seuraavassa tilassa.

Voidaan todistaa (ks. esim. [17, 19, 21]), että jokaista epädeterminististä automaattia vastaa sen kanssa *yhtäpitävä* deterministinen automaatti (joka siis on aina yhdessä tilassa). Automaattien yhtäpitävyys tarkoittaa, että ne tunnistavat saman kielen.

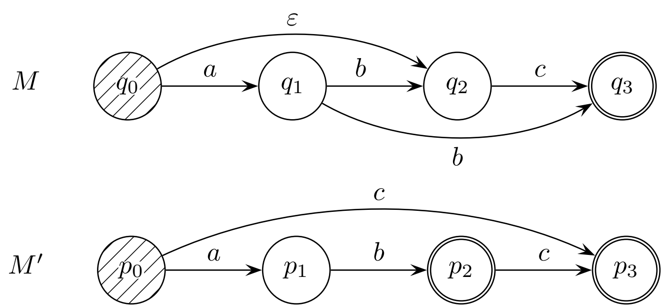
Epädeterministisen automaatin täsmällinen määritelmä on muuten sama kuin deterministisen (s. 168), paitsi että δ on kuvaus $Q \times (\Sigma \cup \{\varepsilon\}) \to \mathcal{P}(Q)$, joten δ liittää jokaiseen tila-syöteपariin yhden tai useamman tilan tai ei yhtään tilaa. Triviaalisti $q \in \delta(q, \varepsilon)$ kaikilla $q \in Q$, mutta emme merkitse niitä.

Esimerkki 155. Kuvion epädeterministinen automaatti M on samanaikaisesti tiloissa q_0 ja q_2. Se voi olla myös samanaikaisesti tiloissa q_2 ja q_3 (luettuaan q_1:ssä b:n), mutta ei samanaikaisesti näissä kolmessa tilassa. Tämä automaatti tunnistaa kielen $L = \{ab, abc, c\}$. Täsmällisesti $M = (Q, \Sigma, \delta, q_0, F)$, missä $Q = \{q_0, q_1, q_2, q_3\}$, $\Sigma = \{a, b, c\}$, $F = \{q_3\}$, ja

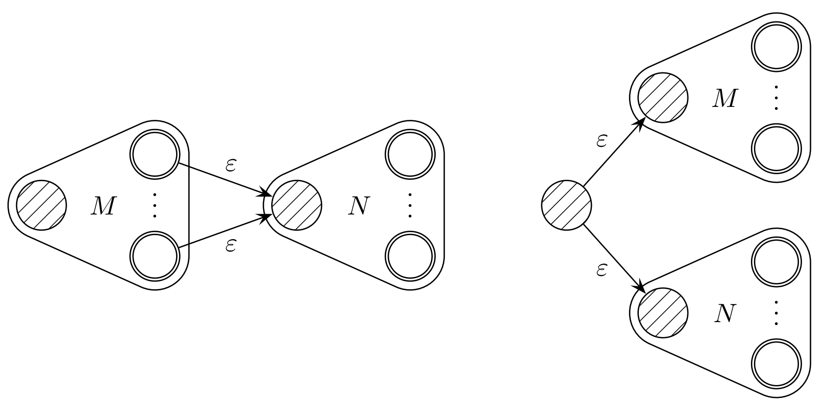
$$\begin{aligned} \delta(q_0, a) &= \{q_1\}, & \delta(q_0, \varepsilon) &= \{q_0, q_2\}, \\ \delta(q_1, b) &= \{q_2, q_3\}, & \delta(q_2, c) &= \{q_3\}. \end{aligned}$$

Kuviossa on myös yhtäpitävä deterministinen automaatti $M' = (P, \Sigma, \delta', p_0, F')$, missä $P = \{p_0, p_1, p_2, p_3\}$, $\Sigma = \{a, b, c\}$, $F' = \{p_2, p_3\}$, ja

$$\delta'(p_0, a) = p_1, \qquad \delta'(p_1, b) = p_2, \qquad \delta'(p_0, c) = \delta'(p_2, c) = p_3.$$

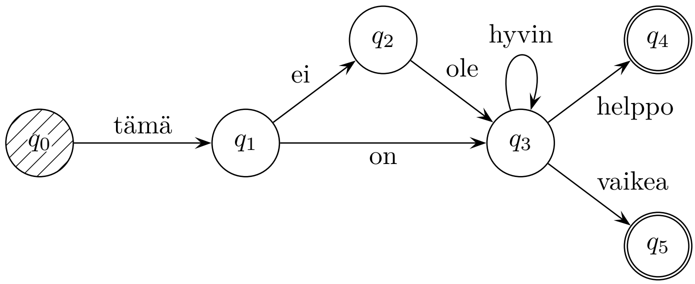


Voimme nyt vastata kysymykseemme. Saamme kielen $L \cdot K$ tunnistavan automaatin ”kytkemällä M ja N sarjaan” eli siirtymällä M:n lopputiloista N:n alkutilaan ε-siirroilla. Saamme kielen $L \cup K$ tunnistavan automaatin ”kytkemällä M ja N rinnan” eli määrittelemällä uuden alkutilan, josta siirrytään M:n ja N:n alkutiloihin ε-siirroilla. Kielen L^* tunnistavan automaatin muodostamisen jätämme harjoitustehtäväksi (teht. 434).



Harjoitustehtäviä

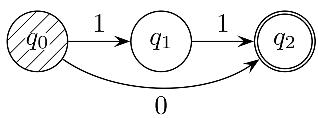
421. Minkä kielen kuvion automaatti tunnistaa?



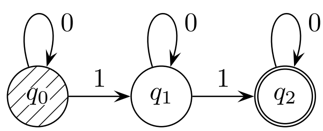
422. Tavara, jonka hinta on 3 euroa, saadaan automaatista, joka toimii 1 ja 2 euron kolikoilla. Jos automaatti on saanut ainakin 3 euroa, niin se antaa tavaran, mutta ei palauta mahdollisia ylimääräisiä kolikoita. Muodostettava tätä automaattia vastaava abstrakti automaatti, jonka aakkosto $\Sigma = \{1, 2\}$ ja joka on lopputilassa, kun luettujen aakkosten summa on ainakin 3.

423. Mikä s.l. vastaa kuvion automaattia?

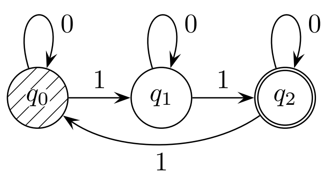
a)



b)



c)



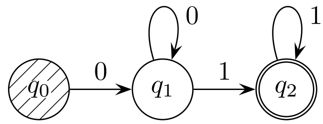
424. Olkoon $\Sigma = \{a, b, c\}$. Muodostettava kielen L tunnistava automaatti, kun L **a)** on $\{a^3, a^2b, a^2c\}$, **b)** koostuu niistä sanoista, joissa on kaksi a:ta ja muut b:itä, **c)** koostuu niistä sanoista, joissa on kaksi peräkkäistä a:ta ja muut b:itä.

425. Olkoon $\Sigma = \{0, 1\}$. Muodostettava automaatti, jonka tunnistaman kielen määrittelee s.l. **a)** 10^*1, **b)** $(10^*1)^*$, **c)** $(10^*1)^*1$.

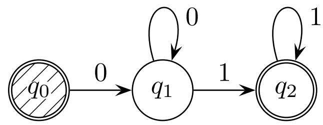
426. Olkoon $\Sigma = \{0, 1\}$. Muodostettava automaatti, jonka tunnistaman kielen määrittelee s.l. **a)** $(10^*1)^*(0 \cup 1)$, **b)** $(10^*1)^*(0 \cup 1)^*$, **c)** $(10^*1)^*(0^* \cup 1^*)$.

427. Minkä kielen kuvion automaatti tunnistaa?

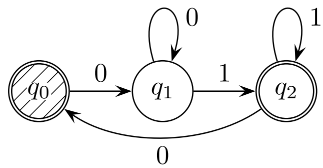
a)



b)

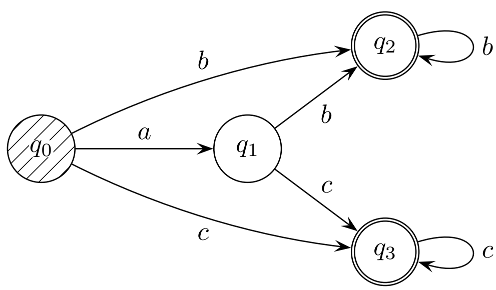


c)



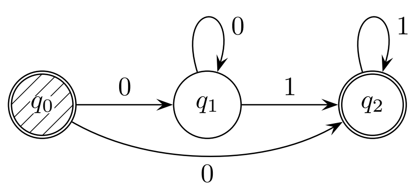
428. Olkoon Σ suomen kielen aakkosten joukko. Muodostettava automaatti, jonka tunnistama kieli L on sanan *yö* kaikkien yksikön sijamuotojen joukko. Toisin sanoen $L = \{$*yö*, *yön*, *yötä*, *yönä*, *yöksi*, *yössä*, *yöstä*, *yöhön*, *yöllä*, *yöltä*, *yölle*, *yöttä*, *öineen*, *öin*$\}$.

429. Olkoon $\Sigma = \{a, b, c\}$. Kuviossa on jätetty merkitsemättä ne nuolet, joita pitkin edetessä automaatti ei missään tapauksessa hyväksy luettavaa sanaa. Täydennettävä kuvio (lisäämällä ”roskatila”) niin, että jokaista tila-aakkosparia vastaa nuoli.

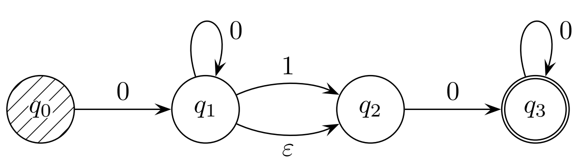


430. Muodostettava kuvion epädeterministisen automaatin kanssa yhtäpitävä deterministinen automaatti.

a)



b)



431. **a)** Esitettävä tiladiagrammina automaatti $M = (Q, \Sigma, \delta, q_0, F)$, missä $Q = \{q_0, q_1, q_2, q_3, q_4, q_5\}$, $\Sigma = \{0, 1\}$, $F = \{q_4, q_5\}$, ja

$$\delta(q_0, 0) = \delta(q_2, 0) = \delta(q_3, 0) = \delta(q_4, 0) = \delta(q_5, 0) = q_0,$$
$$\delta(q_1, 0) = q_2, \quad \delta(q_0, 1) = \delta(q_2, 1) = q_1, \quad \delta(q_1, 1) = q_3,$$
$$\delta(q_3, 1) = q_4, \quad \delta(q_4, 1) = q_5, \quad \delta(q_5, 1) = q_4.$$

b) Muodostettava sellainen automaatin M kanssa yhtäpitävä automaatti, jossa on mahdollisimman vähän tiloja.

432. Olkoon $\Sigma = \{a, b, c\}$. Olkoon L niistä sanoista koostuva kieli, joissa on täsmälleen yksi a, ja olkoon K niistä sanoista koostuva kieli, joissa on täsmälleen yksi b. Muodostettava **a)** kielen L tunnistava automaatti M, **b)** kielen K tunnistava automaatti N, **c)** kielen $L \cup K$ tunnistava automaatti "kytkemällä M ja N rinnan", **d)** kielen $L \cdot K$ tunnistava automaatti "kytkemällä M ja N sarjaan".

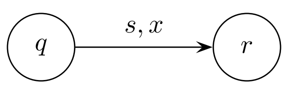
433. Jatkoa. Muodostettava c- ja d-kohtien automaattien kanssa yhtäpitävät deterministiset automaatit.

434. Olkoon M säännöllisen kielen L tunnistava automaatti. **a)** Miten voidaan muodostaa kielen L^* tunnistava automaatti? **b)** Tarkasteltava esimerkkinä tehtävän 432 automaattia M.

435. Olkoon M säännöllisen kielen L tunnistava automaatti. **a)** Miten voidaan muodostaa komplementtikielen $\overline{L}$ tunnistava automaatti? **b)** Tarkasteltava esimerkkinä tehtävän 432 automaattia M. **c)** Todettava a-kohdan perusteella, että säännöllisen kielen komplementti on säännöllinen.

436. Olkoot L ja K säännöllisiä kieliä sekä olkoot M ja N vastaavat automaatit. **a)** Miten voidaan muodostaa kielen $L \cap K$ tunnistava automaatti? **b)** Käsiteltävä esimerkkinä tehtävän 432 automaatteja M ja N. **c)** Todettava a-kohdan perusteella, että kahden säännöllisen kielen leikkaus on säännöllinen, ja yleistettävä tämä tulos kaikille äärellisille leikkauksille.

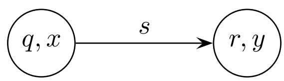
437. *Mealyn kone* on yhdelmä $M = (Q, \Sigma, \Theta, \delta, \lambda, q_0)$, missä *tilojen joukko* Q, *syöteaakkosten joukko* Σ ja *tulosteaakkosten joukko* Θ ovat epätyhjiä äärellisiä joukkoja, *siirtymäfunktio* δ on kuvaus $Q \times \Sigma \to Q$, *tulostusfunktio* λ on kuvaus $Q \times \Sigma \to \Theta \cup \{\varepsilon\}$, ja *alkutila* q_0 on tilajoukon Q alkio. Siis jokaista merkkiä lukiessaan M tulostaa tietyn merkin, joka riippuu M:n tilasta ja luetusta merkistä. Se, että M tilassa q lukiessaan merkin s tulostaa merkin x ja siirtyy tilaan r, esitetään tiladiagrammissa kuvion osoittamalla tavalla.



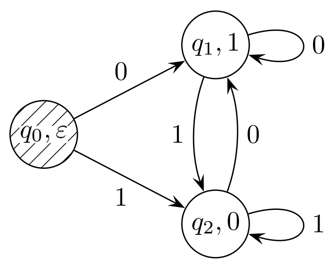
Tavara, jonka hinta on 3 euroa, saadaan automaatista, joka toimii 1 ja 2 euron kolikoilla. Muodostettava tätä automaattia vastaava abstrakti Mealyn kone M, kun $\Sigma = \{1, 2, p\}$ ja $\Theta = \{1, t\}$, missä p tarkoittaa napin painamista ja t tavaraa. Jos M lukee p:n, tapahtuu seuraavaa. Jos M on saanut alle 3 euroa, se ei tulosta mitään (eli tulostaa ε:n). Jos se on saanut 3 euroa, se tulostaa t:n ja palaa alkutilaan. Jos se on saanut yli 3 euroa, se tulostaa t:n ja vaihtorahat sekä palaa alkutilaan.

438. Muodostettava Mealyn kone, joka lukee kaksi ei-negatiivista binäärilukua ja tulostaa niiden summan binäärilukuna. Yhteenlaskettavat ilmoitetaan yhtämoninumeroisina kummastakin vuorotellen numero kerrallaan oikealta vasemmalle. Jos toisessa yhteenlaskettavassa on vähemmän numeroita, niin sen alkuun lisätään nollia. Jos esimerkiksi on laskettava yhteen luvut 101 ja 11, niin jälkimmäinen luku esitetään muodossa 011 ja numerot annetaan järjestyksessä 1 1 0 1 1 0.

439. *Mooren kone* on yhdelmä $M = (Q, \Sigma, \Theta, \delta, \lambda, q_0)$, missä *tilojen joukko* Q, *syöteaakkosten joukko* Σ ja *tulosteaakkosten joukko* Θ ovat epätyhjiä äärellisiä joukkoja, *siirtymäfunktio* δ on kuvaus $Q \times \Sigma \to Q$, *tulostusfunktio* λ on kuvaus $Q \to \Theta \cup \{\varepsilon\}$, ja *alkutila* q_0 on tilajoukon Q alkio. Siis jokaista merkkiä lukiessaan M tulostaa tietyn merkin, joka riippuu M:n tilasta (mutta ei luetusta merkistä). Se, että M tilassa q tulostaa merkin x ja lukiessaan merkin s siirtyy tilaan r, jossa se tulostaa y:n, esitetään tiladiagrammissa kuvion osoittamalla tavalla.



Vertailtava keskenään alla vasemmalla olevan Mealyn koneen ja oikealla olevan Mooren koneen toimintaa.



440. Olkoon $\Sigma = \Theta = \{0, 1\}$. Muodostettava **a)** Mealyn, **b)** Mooren kone, joka tulostaa numeron 0, jos siihen asti luettujen ykkösten lukumäärä on parillinen, ja numeron 1, jos se on pariton.

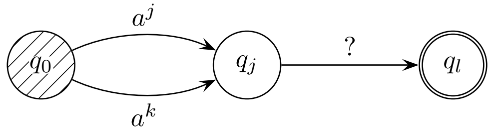
8.3 Muodolliset kieliopit

1 Johdanto

Olemme huomanneet (lause 47), että säännöllisiä kieliä voidaan määritellä paitsi säännöllisillä lausekkeilla myös automaateilla. Jos kaikki kielet olisivat säännöllisiä, voisimme tyytyä tähän. Kuitenkin olemme myös jo huomanneet (teht. 419), etteivät kaikki kielet ole säännöllisiä. Tarkastelemme seuraavaksi esimerkkiä sellaisesta kielestä.

Esimerkki 156. Olkoon $\Sigma = \{a, b\}$. Osoitettava, että kieli $L = \{ a^n b^n \mid n \in \mathbb{Z}_+ \} = \{ab, a^2b^2, a^3b^3, \ldots\}$ ei ole säännöllinen.

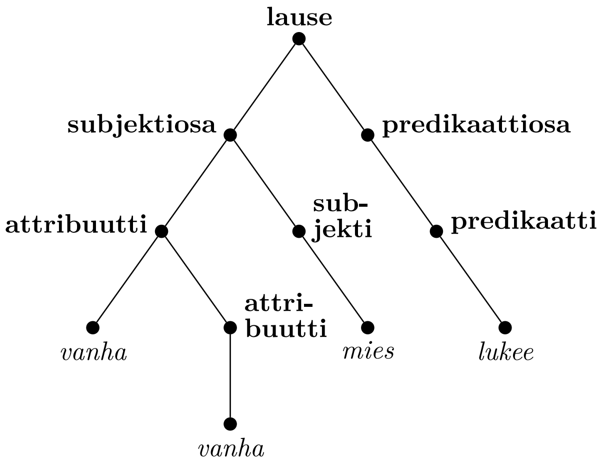
Teemme vastaoletuksen, että L on säännöllinen. Tällöin se voidaan tunnistaa eräällä automaatilla M. Olkoon q_i se tila, jossa M on luettuaan sanan a^ib^i alkuosan a^i ($i \in \mathbb{Z}_+$). Koska tiloja on vain äärellinen määrä, on oltava sellaiset indeksit j ja k, että $j \neq k$, mutta $q_j = q_k$. Täten M pääsee alkutilasta tilaan q_j sekä j:n pituisella että k:n pituisella a-jonolla. Koska M ei q_j:ssä ollessaan ”muista”, mitä kautta se on sinne tullut, niin se ei voi hyväksyä sanaa $a^ib^i \in L$, jos se hylkää sanan $a^ib^k \notin L$. Siis vastaoletus on väärä, joten L ei ole säännöllinen.



Esimerkki 157. Olkoon $\Sigma = \{$*vanha*, *nuori*, *mies*, *nainen*, *lukee*, *kirjaa*, *lehteä*$\}$. Kieli $L = \{$*vanha*, *nuori*$\}^*\{$*mies*, *nainen*$\}\{$*lukee*$\}\{\varepsilon$, *kirjaa*, *lehteä*$\}$, jonka sanoja (tai pikemminkin lauseita) ovat esimerkiksi *nuori nainen lukee kirjaa* ja *vanha nuori vanha mies lukee lehteä*, on säännöllinen, mutta määrittelemme sen uudella tavalla.

1. **lause** on **subjektiosa predikaattiosa** (Tämä tarkoittaa, että lause saadaan kirjoittamalla ensin subjektiosa ja sitten predikaattiosa.)
2. **subjektiosa** on **attribuutti subjekti**
3. **subjektiosa** on **subjekti**
4. **predikaattiosa** on **predikaatti objekti**
5. **predikaattiosa** on **predikaatti**
6. **attribuutti** on *vanha* **attribuutti**
7. **attribuutti** on *nuori* **attribuutti**
8. **attribuutti** on *vanha*
9. **attribuutti** on *nuori*
10. **subjekti** on *mies*
11. **subjekti** on *nainen*
12. **predikaatti** on *lukee*
13. **objekti** on *kirjaa*
14. **objekti** on *lehteä.*

Näiden *sääntöjen* perusteella voimme *johtaa* kielen L kaikki lauseet. Kuvion *johtamispuulla* saamme lauseen *vanha vanha mies lukee.* Säännöt 6 ja 7 ovat rekursiivisia. Niiden mukaan **attribuutti** saadaan kirjoittamalla **attribuutin** eteen *vanha* tai *nuori.* Soveltamalla niitä toistuvasti ja käyttämällä lopuksi sääntöjä 8 ja 9 saamme minkä tahansa (äärellisen) jonon sanoista *vanha* ja *nuori*.



2 Muodollisen kieliopin käsite

Muodollinen kielioppi on yhdelmä $G = (\Sigma, V, R, S)$. Siinä *päätemerkkien* eli *terminaalisymbolien joukko* Σ ja *välikemerkkien* eli *nonterminaalisymbolien joukko* V ovat erillisiä äärellisiä joukkoja. *Sääntöjoukko* R on joukon $(W^* \cdot V \cdot W^*) \times W^*$ äärellinen osajoukko, missä *merkkijoukko* eli *symbolijoukko* $W = \Sigma \cup V$. *Säännöt* ovat joukon R alkioita eli järjestettyjä pareja (α, β), missä $\alpha \in W^* \cdot V \cdot W^*$ (eli sisältää ainakin yhden välikemerkin) ja $\beta \in W^*$. Jos $(\alpha, \beta) \in R$ eli (α, β) on sääntö, niin merkitsemme $\alpha \to \beta$. *Alkumerkki* eli *alkusymboli* S on tietty välikemerkki. Puhuessamme kieliopista tarkoitamme seuraavassa muodollista kielioppia.

Kieliopin G määrittelemä eli *tuottama kieli* L koostuu niistä sanoista, jotka voidaan *johtaa* lähtemällä alkumerkistä S ja soveltamalla sääntöjoukon R sääntöjä, kunnes saadaan jono, jossa on pelkkiä päätemerkkejä. Kieliopin G päätemerkit vastaavat kielen L aakkosia. Sovimme, että myös tyhjä merkki ε on päätemerkki, vaikka emme pidä sitä joukon Σ alkiona.

Esimerkki 156, jatkoa. Jos kielen L sanan alkuun lisätään a ja loppuun b, niin saadaan L:n sana. Aloittamalla sanasta ab ja toistamalla tätä saamme L:n kaikki sanat ja vain ne. Toisin sanoen **sana** saadaan muodostamalla a **sana** b, mutta **sana** on myös ab. Alkumerkki S eli **sana** on ainoa välikemerkki, joten $V = \{S\}$. Päätemerkit ovat a ja b, joten $\Sigma = \{a, b\}$. Koska **sana** on a **sana** b, niin $S \to aSb$. Koska myös **sana** on ab, niin $S \to ab$. Siis $R = \{S \to aSb, S \to ab\}$. Jos kirjoitamme säännöt allekkain, emme käytä joukkosulkeita, vaan merkitsemme

$$
\begin{aligned}
S &\to aSb \\
S &\to ab.
\end{aligned}
$$

Esimerkki 157, jatkoa. Päätemerkkien joukko $\Sigma = \{vanha, nuori, mies, nainen, lukee, kirjaa, lehteä\}$. Välikemerkkien joukko $V = \{S, SO, PO, AT, SU, PR, OB\}$, missä alkumerkki S tarkoittaa **sanaa**, merkki SO **subjektiosaa** jne. Sääntöjoukko R on

$$\begin{aligned}
&S \to SO\ PO\\
&SO \to AT\ SU\\
&SO \to SU\\
&PO \to PR\ OB\\
&PO \to PR\\
&AT \to vanha\ AT\\
&AT \to nuori\ AT\\
&AT \to vanha\\
&AT \to nuori\\
&SU \to mies\\
&SU \to nainen\\
&PR \to lukee\\
&OB \to kirjaa\\
&OB \to lehteä.
\end{aligned}$$

3 Chomskyn kielityypit

Kieliopin G sääntöjoukko R voidaan valita vapaasti, mutta jos halutaan esimerkiksi, että G:n tuottama kieli L on säännöllinen, niin R:lle täytyy asettaa ehtoja. Yleisesti voidaan kysyä, mitä ehtoja R:n pitäisi toteuttaa, jotta L:llä olisi haluttuja ominaisuuksia. Voidaan kysyä myös toisinpäin: Jos G toteuttaa tietyt ehdot, mitä ominaisuuksia silloin on L:llä? Nämä kysymykset johtavat *Chomskyn*[2] *kielityyppeihin*.

Merkitsemme päätemerkkejä pienillä latinalaisilla kirjaimilla, välikemerkkejä isoilla latinalaisilla kirjaimilla ja merkkijonoja pienillä kreikkalaisilla kirjaimilla. Tällainen jono voi sisältää sekä pääte- että välikemerkkejä tai vain toisia niistä. Se voi myös olla tyhjä jono ε.

Tyypin 0 kieliopin säännöille $\alpha \to \beta$ ei aseteta ehtoja. Kuitenkin α:ssa täytyy R:n määritelmän mukaan olla ainakin yksi välikemerkki. Siis erityisesti α ei saa olla ε.

Tyypin 1 kieliopin säännöt ovat muotoa $\alpha A\beta \to \alpha\gamma\beta$ $(\gamma \neq \varepsilon)$ tai $A \to \varepsilon$. Sanomme, että tällainen kielioppi, kuten myös sen määrittelemä kieli, on *kontekstiriippuva* (engl. *context sensitive*). Nimittäin se, mitä A:lle tapahtuu tuollaista sääntöä sovellettaessa, riippuu A:n "kontekstista" eli "ympäristöstä" α ja β (ellei $\alpha = \beta = \varepsilon$).

Tyypin 2 kieliopin säännöt ovat muotoa $A \to \gamma$. Tällainen kielioppi, kuten myös sen määrittelemä kieli, on *kontekstiriippumaton* (engl. *context*

[2] *Noam Chomsky (1928–), yhdysvaltalainen kielitieteilijä.*

free). Nimittäin se, mitä A:lle tapahtuu, ei riipu A:n ”ympäristöstä”.

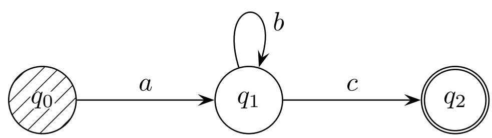
Tyypin 3 kieliopin säännöt ovat muotoa $A \to aB$ tai $A \to a$. (Koska pidämme ε:ia päätemerkkinä, niin erityisesti sääntö $A \to \varepsilon$ on sallittu.) Tällainen kielioppi on *säännöllinen*, mikä nimitys johtuu lauseesta 48.

Esimerkki 158. Jos R sisältää mm. säännöt (1) $A \to aA$ ja (2) $aAb \to aBb$, niin jokaisessa saadussa merkkijonossa A voidaan korvata aA:lla, mutta myös aAb voidaan korvata aBb:llä. Jos esimerkiksi on saatu merkkijono aAb, niin siihen voidaan soveltaa vaikkapa ensiksi sääntöä (1), jolloin saadaan $aaAb$, ja samaa sääntöä toisen kerran, jolloin saadaan $aaaAb$, ja sitten sääntöä (2), jolloin saadaan $aaaBb$. Soveltamalla heti sääntöä (2) tulos on aBb.

Lause 48. Kieli on säännöllinen, jos ja vain jos sen tuottaa tyypin 3 kielioppi.

Todistus (ks. esim. [17, 21, 19]) perustuu siihen, että kieliopin välikemerkit vastaavat kielen tunnistavan automaatin tiloja.

Esimerkki 159. Olkoon $\Sigma = \{a, b, c\}$. Kielen $L = \{ac, abc, ab^2c, ab^3c, \ldots\} = \{\, ab^nc \mid n \in \mathbb{N} \,\}$ määrittelee s.l. ab^*c. Tämän kielen tunnistaa automaatti M, jonka tiladiagrammi on



Muodostamme L:n tuottavan kieliopin G. Sen välikemerkit vastaavat M:n tiloja, joten käytämme samoja merkintöjä. Siis $G = (\Sigma, V, R, q_0)$, missä päätemerkkien joukko $\Sigma = \{a, b, c\}$, välikemerkkien joukko $V = \{q_0, q_1, q_2\}$, alkumerkki on q_0, ja sääntöjoukko R on

$$q_0 \to aq_1$$
$$q_1 \to bq_1$$
$$q_1 \to cq_2$$
$$q_2 \to \varepsilon.$$

Saamme yksinkertaisemman *yhtäpitävän* (eli saman kielen L määrittelevän) kieliopin jättämällä M:n lopputilaa q_2 vastaavan välikemerkin q_2 pois. Tällöin $V = \{q_0, q_1\}$ ja R on

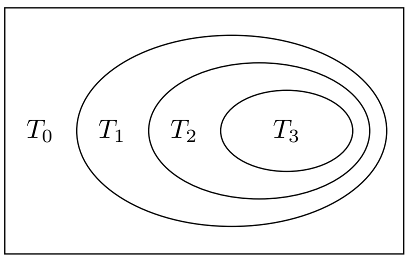
$$q_0 \to aq_1$$
$$q_1 \to bq_1$$
$$q_1 \to c.$$

Esimerkki 156, jatkoa. Kielioppi $G = (\Sigma, V, S, R)$, missä $\Sigma = \{a, b\}$, $V = \{S\}$ ja R on

$$S \to aSb$$
$$S \to ab,$$

on tyypin 2 kielioppi eli kontekstiriippumaton kielioppi, joten sen tuottama kieli $L = \{\, a^n b^n \mid n \in \mathbb{Z}_+ \,\}$ on tyypin 2 kieli eli kontekstiriippumaton kieli. (Määrittelemme, että kieli on tyyppiä t, jos sen tuottaa tyypin t kielioppi.)

Chomskyn kielityypittely on hierarkkinen sikäli, että korkeamman tyypin kielten joukko on alemman tyypin kielten joukon aito osajoukko (teht. 451). On kylläkin hieman omituista sanoa, että tyypin 2 kieli on sekä kontekstiriippumaton että kontekstiriippuva, mutta tällainen terminologia on vakiintunut.



Lauseista 47 ja 48 seuraa, että kieli on tyyppiä 3, jos ja vain jos se voidaan tunnistaa (äärellisellä) automaatilla. Myös muilla kielillä on yhteyksiä automaatteihin, jotka eivät silloin voi olla äärellisiä. Kieli on tyyppiä 2, jos ja vain jos se voidaan tunnistaa *pinoautomaatilla* (engl. *pushdown automaton*). Kieli on tyyppiä 0, jos ja vain jos se voidaan tunnistaa *Turingin*[3] *koneella.* Tyypin 1 kielet voidaan tunnistaa sellaisella Turingin koneella, joka pysähtyy kaikilla syötteillä. Nämä käsitteet ja asiat eivät kuulu meidän alkeisesityksemme piiriin, joten tyydymme viittaamaan kirjallisuuteen (esim. [17, 19, 21]).

Harjoitustehtäviä

441. Muodostettava kielioppi, joka tuottaa **a)** tyhjän kielen, **b)** sen kielen, jossa on vain tyhjä sana, **c)** sen kielen, jossa on vain sana a.

442. Olkoon $a, b \in \Sigma$. Muodostettava kielioppi, joka tuottaa saman kielen kuin s.l. **a)** $a \cup b$, **b)** $a \cdot b$, **c)** a^*.

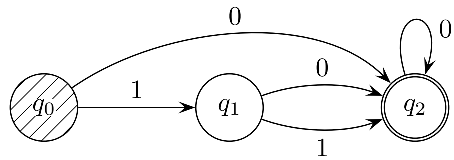
443. Olkoon $\Sigma = \{a, b\}$. Muodostettava kielioppi, joka tuottaa kielen **a)** $\{\, a^n b^n \mid n \in \mathbb{N} \,\}$ (vrt. esim. 156), **b)** $\{\, a^m b^n \mid m, n \in \mathbb{N} \,\}$.

[3] *Alan Turing (1912–1954), englantilainen matemaatikko, tietojenkäsittelytieteen pioneeri.*

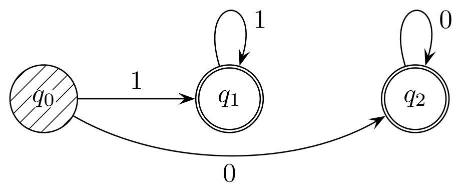
444. Olkoon $\Sigma = \{a, b, c\}$. Muodostettava kielioppi, joka tuottaa kielen **a)** $\{\, a^n b^n c \mid n \in \mathbb{N} \,\}$, **b)** $\{\, c a^n b^n \mid n \in \mathbb{N} \,\}$.

445. Olkoon $\Sigma = \{0, 1\}$. Muodostettava kielioppi, joka tuottaa saman kielen kuin kuvion automaatti.

a)



b)



446. Muodostettava kieli, jonka tuottaa kielioppi $G = (\Sigma, V, S, R)$, kun $\Sigma = \{a, b\}$, $V = \{S, A, B\}$ ja R on **a)** $\{S \to AB, A \to ab, B \to bb\}$, **b)** $\{S \to AB, S \to aA, A \to a, B \to ba\}$.

447. Muodostettava kieli, jonka tuottaa kielioppi $G = (\Sigma, V, S, R)$, kun $\Sigma = \{a, b\}$, $V = \{S, A, B\}$ ja R on **a)** $\{S \to A, S \to B, A \to aA, A \to a, B \to bB, B \to b\}$, **b)** $\{S \to AB, A \to aAb, B \to bBa, A \to \varepsilon, B \to \varepsilon\}$.

448. Muodostettava kieli, jonka tuottaa kielioppi $G = (\Sigma, V, S, R)$, kun $\Sigma = \{a, b\}$ ja **a)** $V = \{S\}$, $R = \{S \to aS, S \to aSb, S \to \varepsilon\}$, **b)** $V = \{S, A\}$, $R = \{S \to aA, A \to aAb, A \to \varepsilon\}$.

449. Muodostettava esimerkin 157 kielen sanan (tai paremmin lauseen) **a)** *nuori nainen lukee kirjaa*, **b)** *vanha nuori vanha mies lukee lehteä* johtamispuu.

450. Muutettava esimerkin 157 kieliopin sääntöjä niin, ettei tämä kielioppi tuota sellaisia lauseita, joissa lukija on samanaikaisesti vanha ja nuori.

451. Muodostettava **a)** tyypin 0 kielioppi, joka ei ole tyyppiä 1, **b)** tyypin 1 kielioppi, joka ei ole tyyppiä 2, **c)** tyypin 2 kielioppi, joka ei ole tyyppiä 3.

452. Ovatko edellisen tehtävän kielioppien tuottamat kielet myös korkeampaa tyyppiä kuin nämä kieliopit?

453. Osoitettava, että kielioppi $G = (\Sigma, V, S, R)$, missä $\Sigma = \{a, b, c\}$, $V = \{S, B, C\}$, ja $R = \{S \to aSBC, S \to aBC, aB \to ab, CB \to BC, bB \to bb, bC \to bc, cC \to cc\}$, tuottaa kielen $L = \{\, a^n b^n c^n \mid n \in \mathbb{Z}_+ \,\}$. Voidaan todistaa, että G, joka on tyyppiä 1, ei ole yhtäpitävä minkään tyyppiä 2 olevan kieliopin kanssa. Täten L on tyypin 1 kieli, joka ei ole tyyppiä 2.

454. Olkoot G ja H kielioppeja sekä olkoot L ja K niiden tuottamat kielet. **a)** Miten voidaan muodostaa kielioppi, joka tuottaa kielen $L \cup K$? **b)** Jos L ja K ovat tiettyä samaa tyyppiä, niin onko myös $L \cup K$ sitä tyyppiä?

455. Kuten edellä, mutta yhdisteen $L \cup K$ sijasta tarkastellaan ketjua $L \cdot K$.

456. Olkoon G kielioppi ja L sen tuottama kieli. **a)** Miten voidaan muodostaa kielioppi, joka tuottaa toisinpäisen kielen L'? **b)** Ovatko L ja L' samaa tyyppiä?

457. Sana α on *palindromi*, jos se on sama kuin sen toisinpäinen sana α'. **a)** Muodostettava kielioppi, jonka tuottama kieli on niiden bittijonojen joukko, jotka i) ovat, ii) eivät ole palindromeja. **b)** Mitä tyyppiä nämä kielet ovat?

458. Todistettava oikeaksi tai vääräksi: Kaikki äärelliset kielet ovat tyyppiä 3.

459. Olkoon $\Sigma = \{a, b\}$. Minkä tyypin kielen muodostavat ne sanat, joissa on yhtä monta a:ta kuin b:tä?

460. Mitä tyyppiä ovat luonnolliset kielet vai ovatko mitään?

Kirjallisuusluettelo

Tärkeimmät käyttämämme lähdekirjat ovat Lin & Lin [10], Halmos [7], Sigler [23] ja Rosen [21]. Joukko-oppia käsittelee laajemmin Lipschutz [11] ja aivan perusteellisesti Enderton [3] sekä Jech [8]. Lukukäsitettä tarkastelee syvällisesti Ebbinghaus ym. [2]. Suomenkielisiä kirjoja logiikasta ovat Miettinen [16], Rantala & Virtanen [20], Salminen & Väänänen [22] ja näitä vaativampi Väänänen [29]. Kieliteknologian opiskelijalle sopiva lyhyt johdatus automaatteihin ja muodollisiin kieliin on Wintner [30]. Perusteellinen esitys kielitieteen matemaattisista menetelmistä on Partee ym. [19]. Paljon muutakin hyvää kirjallisuutta on tietenkin olemassa.

[1] E. R. Burroughs, *Tarzan, apinain kuningas.* WSOY, 1973.

[2] H. D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, R. Remmert, *Numbers.* Springer, 1995.

[3] H. B. Enderton, *Elements of Set Theory.* Acad. Pr., 1977.

[4] H. Freudentahl, *Mathematics as an Educational Task.* Reidel, 1973.

[5] R. Godement, *Cours d'Algébre.* Hermann, 1963.

[6] R. P. Grimaldi, *Discrete and Combinatorial Mathematics: an applied introduction.* 2nd ed. Addison-Wesley, 1989.

[7] P. R. Halmos, *Naive Set Theory.* Van Nostrand, 1960.

[8] T. Jech, *Set Theory.* Acad. Pr., 1978.

[9] T. Lehtinen, *Søren Kierkegaard, intohimon, ahdistuksen ja huumorin filosofi.* Kirjapaja, 1994.

[10] S-Y. Lin, Y-F. Lin, *Set Theory: An Intuitive Approach.* Houghton Mifflin, 1974.

[11] S. Lipschutz, *Schaum's Outline of Theory and Problems of Set Theory and Related Topics.* New York, 1964.

[12] H. Martinson, *Aniara.* 2. p. WSOY, 1963.

[13] J. Merikoski, Joukko-opin ja algebran alkeiskurssi. Tampereen yliopisto, matemaattisten tieteiden laitos, 1989.

[14] J. Merikoski, A. Virtanen, P. Koivisto, Diskreetti matematiikka I. Tampereen yliopisto, matematiikan, tilastotieteen ja filosofian laitos, moniste B 42. 11. p. 2001.

[15] J. Merikoski, K. Väänänen, T. Laurinolli, T. Sankilampi, *Matematiikan taito 15: Lineaarialgebra.* WSOY, 1998.

[16] S. K. Miettinen, *Logiikan peruskurssi.* 2. uud. p. Gaudeamus, 1993.

[17] P. Orponen, Laskennan teoria. Helsingin yliopisto, tietojenkäsittelytieteen laitos, 1993.

[18] P. Parkkinen, *Jos minä maatani rakastaisin.* Weilin+Göös, 1967.

[19] B. H. Partee, A. ter Meulen, R. E. Wall, *Mathematical Methods in Linquistics.* Kluwer, 1993.

[20] V. Rantala, A. Virtanen, Logiikkaa: Teoriaa ja sovelluksia. Tampereen yliopisto, matematiikan, tilastotieteen ja filosofian laitos, moniste B 43. 2. p. 1999.

[21] K. H. Rosen, *Discrete Mathematics and Its Applications.* 2nd ed. McGraw-Hill, 1991.

[22] H. Salminen, J. Väänänen, *Johdatus logiikkaan.* Gaudeamus, 1992.

[23] L. E. Sigler, *Exercises in Set Theory.* Springer, 1976.

[24] R. Sikorski, *Boolean Algebras.* 3rd ed. Springer, 1969.

[25] D. F. Stanat, D. F. McAllister, *Discrete Mathematics in Computer Science.* Prentice Hall, 1977.

[26] P. Suppes, *Introduction to Logic.* 10th ed. D. Van Nostrand, 1967.

[27] S. Topelius, *Lukemisia lapsille IV.* WSOY, 1946.

[28] N. Ya. Vilenkin, *Stories about Sets.* Acad. Pr., 1968.

[29] J. Väänänen, *Matemaattinen logiikka.* Gaudeamus, 1987.

[30] S. Wintner, Formal Language Theory for Natural Language Processing. Department of Computer Science, University of Haifa, 2001.

[31] L. Wittgenstein, *Tractatus logico-philosophicus eli Loogis-filosofinen tutkielma.* WSOY, 1971.

Hakemisto