Mika Hirvensalo

Insinöörimatematiikka: Diskreetti Matematiikka 2024

Sisällys

Huomioita sisällöstä: Insinöörimatematiikan opintokokonaisuuden tarkoitus on esittää perustiedot valikoiduista matematiikan työkaluista, joita sovelletaan teknillisillä aloilla.

Diskreettiä matematiikkaa tarvitaan erityisesti digitaalisen informaation ja siihen liittyvien ongelmien mallintamisessa. Näin ollen ei ole yllättävää, että diskreetin matematiikan merkitys on kasvanut erittäin voimakkaasti 1900-luvun puolivälin jälkeen.

Luku 1
Relaatiot ja funktiot

Ennen perehtymistä tämän luvun aihepiiriin on syytä kerrata kurssilta Insinöörimatematikka 1 joukko-opin peruskäsitteet ja merkinnät, kuten joukkoon kuulumisrelaatio $\in$, sisältyminen $\subseteq$ ja joukkojen esitystavat.

Johdatuksena funktiokäsitteeseen voidaan tarkastella seuraavia esimerkkejä. Polynomilausekkeet, kuten x^2+3x+2 määrittelevät funktion, jossa x kuvautuu luvuksi $f(x) = x^2+3x+2$. Tämänkaltainen funktiokäsite on kuitenkin liian suppea, esimerkiksi funktiota $f(x) = |x|$ ei voida määritellä polynomilausekkeena. Vieläkin erikoisempi funktio saadaan määrittelemällä

$$f(x) = \begin{cases} 1 \text{ jos } x \in \mathbb{Q}, \\ 0 \text{ jos } x \notin \mathbb{Q}, \end{cases}$$

eikä ole mitenkään selvää voidaanko tällainen funktio määritellä millään lausekkeella joka koostuu kurssilla Differentiaali- ja integraalilaskenta esitetyistä alkeisfunktioista. Tässä luvussa perehdytään kaikkein yleisimpään funktion määritelmään.

1.1 Karteesinen tulo

1600-luvun alkupuolella René Descartes kehitti idean, joka mullisti matematiikan ja sittemmin myös fysiikan ja muiden luonnontieteiden kehityksen. Descartesin idea edelsi ajallisesti Newtonin ja Leibnizin differentiaalilaskentaa eikä ole täysin perusteetonta sanoa että se oli oikeastaan välttämätön työkalu differentiaalilaskennan kehittämiseksi.

Nykyajan koululaiset tuntevat Descartesin keksinnön xy-koordinaatistona, jossa yhtä tason pistettä edustaa reaalilukupari. Descartesin xy-koordinaatisto onkin tunnetuin esimerkki *karteesisesta tulosta*. Antiikin ajan matematiikan näkökulmasta ideaa voidaan luonnehtia vallankumouksselliseksi, sillä tason pisteiden esittäminen lukuparina mahdollistaa tason objektien kuten esimerkiksi suorien, ellipsien ja paraabelien esittämisen algebrallisena yhteytenä x- ja y-koordinaattien välillä. Toisaalta taas algebrallinen yhteys x ja y-koordinaattien välillä ilmenee aina jonkinlaisena tason objektina. Esimerkiksi ensimmäisen asteen polynomiyhtälö $ax+by=c$ esittää suoraa (ellei $a=b=0$), kun taas toisen asteen polynomiyhtälö voi esittää vaikkapa ympyrää, paraabelia tai hyperbeliä.

Descartes kykeni siis yhdistämään geometrian ja algebran tavalla, johon antiikin matemaatikkojen saavutukset eivät yltäneet. Sittemmin on nähty että Descartesin idea kantaa paljon kauemmaksi kuin tasogeometrian objektien kuvailuihin.

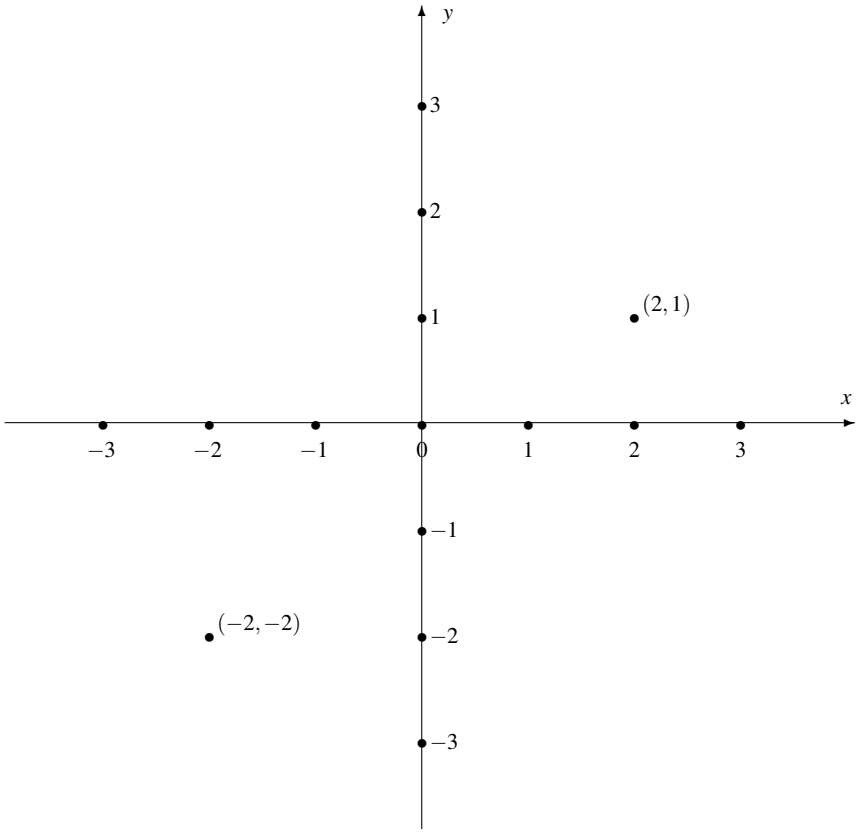
Descartesin tasoesityksessä on kaksi reaaliakselia asetettuna kohtisuoraan toisiaan vastaan. Tällaisesta tasosta käytetään merkintää $\mathbb{R}^2$ ja sitä havainnollistaa kuva 1.1. Kuvassa 1.2 puolestaan on esimerkki tasokäyrästä (origokeskinen yksikköympyrä), joka voidaan ilmaista koordinaattien välisenä algebrallisena yhtälönä $x^2+y^2=1$.

Taustatietoa

René Descartes (latin. *Renatus Cartesius*, 1596–1650) oli ranskalainen matemaatikko ja filosofi, jota pidetään nykyaikaisen filosofian perustajana. Descartes kehitti *analyyttisen geometrian* esittämällä tason pisteet reaalilukupareina. Analyyttisen geometrian perustaminen oli oleellinen edistysaskel integraali- ja differentiaalilaskentaa kohti. Descartes tutki myös mm. optiikkaa ja kehitti nykyisin käytössä olevan potenssimerkinnän.

(kuva: Wikimedia Commons)

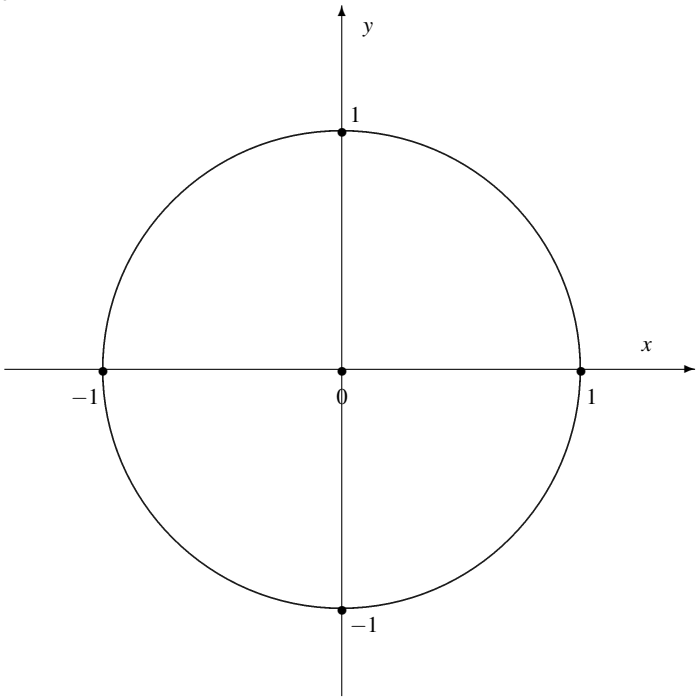
Tasoon $\mathbb{R}^2$ piirretyt käyrät toimivat itse asiassa lähtökohtana funktion käsitteen täsmälliselle määrittelylle, mutta osoittautuu tarkoituksenmukaisemmaksi käsitellä hieman yleisempiä akseleita kuin pelkästään kahta toisiaan vastaan asetettua reaaliakselia.



Kuva 1.1 Karteesinen tulo $\mathbb{R}^2$ esitetään yleensä tason pisteistönä. Tavallisesti vaaka-akselia nimitetään x-akseliksi ja pystyakselia y-akseliksi. Kuvassa on edustettuna vain joitakin pisteitä, mutta $\mathbb{R}^2$ sisältää *kaikki* tason pisteet.

Selvitetään siis mitä tason pisteen esitys koordinaattien avulla tarkoittaa matemaattisesti ja samalla yleistetään reaalitaso korvaamalla reaaliakselit akseleilla, joihin liitetään mikä hyvänsä joukko.

Joukko-opissa kahden alkion joukko on järjestämätön, millä tarkoitetaan sitä, että esimerkiksi $\{1,2\}$ ja $\{2,1\}$ esittävät samaa joukkoa. Toisinaan on kuitenkin tarpeen erotella toisistaan $\{1,2\}$ ja $\{2,1\}$ ja tätä varten otetaan käyttöön *järjestetyn parin* käsite. Järjestetystä parista käytetään merkintää (a,b).



Kuva 1.2 Yksikköympyrän $x^2 + y^2 = 1$ graafinen esitys.

Määritelmä 1 (Järjestettyjen parien yhtäsuuruus).

$$(a_1, b_1) = (a_2, b_2) \iff (a_1 = a_2) \wedge (b_1 = b_2)$$

Kuten joukon käsitteessä, ei myöskään järjestetyn parin (a,b) käsitteessä ole välttämättä tarpeen tietää mitä oliot a ja b ovat. Tässä kurssissa kuitenkin järjestetyn parin alkiot ovat useimmiten lukuja.

Huomautus 1. Joukko-opin avulla järjestetty pari voidaan määritellä täsmällisesti. esim. $(a,b) = \{a, \{a,b\}\}$. Järjestetyn parin määritelmä voidaan laajentaa järjestetyn kolmikon, nelikon, jne. määritelmäksi.

Määritelmä 2. Joukkojen A ja B *karteesinen tulo* $A \times B$ on järjestettyjen parien joukko $A \times B = \{(a,b) \mid a \in A, b \in B\}$. Samoin joukkojen A, B ja C karteesinen tulo määritellään järjestettyjen kolmikkojen joukkona $A \times B \times C = \{(a,b,c) \mid a \in A, b \in B, c \in C\}$.

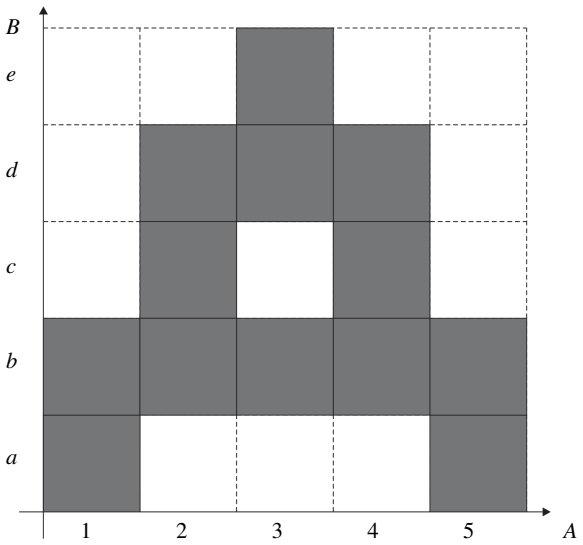
Esimerkki 1. Olkoot $A = \{1,2\}$ ja $B = \{1,2,3\}$. Silloin $A \times B = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}$. Toisaalta taas $B \times A = \{(1,1), (1,2), (2,1), (2,2), (3,1), (3,2)\}$. Voidaan siis todeta, että $A \times B$ ei aina ole sama joukko kuin $B \times A$.

Esimerkki 2. $\mathbb{R} \times \mathbb{R} = \{(x,y) \mid x, y \in \mathbb{R}\}$ on joukko, joka koostuu kaikista järjestetyistä reaalilukupareista (x,y). Joukon $\mathbb{R} \times \mathbb{R}$, jota yleensä merkitään symbolilla $\mathbb{R}^2$, graafinen tulkinta on kuvassa 1.1, jossa on erityisesti korostettu pisteitä $(2,1)$ ja $(-2,2)$ sekä akseleilla olevia pisteitä.

Usein tarvitaan sellaista karteesisen tulon erikoistapausta, jossa $A = B = C$. Tällöin merkitään $A \times A = A^2$ ja $A \times A \times A = A^3$, jne. Karteesisella tulolla $\mathbb{R}^2$ on luonnollinen tulkinta tason pisteinä ja $\mathbb{R}^3$:lla kolmiulotteisen avaruuden pisteinä. Myös karteesiset tulot $\mathbb{R}^4$, $\mathbb{R}^5$, ... ovat käyttökelpoisia lukuisissa sovelluksissa, vaikka näitä ei voidakaan visualisoida samoin kuin joukkoja $\mathbb{R}^2$ ja $\mathbb{R}^3$.

1.2 Relaatio

Joukkojen A ja B karteesinen tulo $A \times B$ koostuu määritelmän mukaan kaikista sellaisista järjestetyistä pareista (a,b), joissa $a \in A$ ja $b \in B$. Täten siis karteesinen tulo $A \times B$ ei itsessään sisällä mitään mielenkiintoista informaatiota, vaan esittää *koko AB*-tasoksi kutsuttavaa joukkoa. Tilanne voi kuitenkin muuttua oleellisesti, mikäli koko karteesisen tulon $A \times B$ sijasta tarkastellaan jotakin sen osajoukkoa. Tämä ajatus on käsitteen *relaatio* taustalla. Erityisesti äärellisten joukkojen tapauksessa on mahdollista samaistaa pikselikuva ja relaatio, jolloin relaatio on yksinkertaisesti kuvion muodostavien pikselien luettelo (katso kuva 1.3)



Kuva 1.3 Tässä kuviossa $A = \{1,2,3,4,5\}$ ja $B = \{a,b,c,d,e\}$ ja kuvan esittämä relaatio $R \subset A \times B$ koostuu pikseleistä $\{(1,a),(1,b),(2,b),(2,c),(2,d),(3,b),(3,d),(3,e),(4,b),(4,c),(4,d),(5,a),(5,b)\}$. Vaaka-akselia voidaan kutsua A-akseliksi ja pystyakselia B-akseliksi.

Määritelmä 3. Relaatio joukosta A joukkoon B on karteesisen tulon $A \times B$ osajoukko. Merkintä $R : A \to B$ tarkoittaa, että R on relaatio joukosta A joukkoon B. Joukkoa A kutsutaan *lähtöjoukoksi* ja B:tä *maalijoukoksi*. Jos $B = A$, sanotaan, että R on joukon A *binäärinen relaatio*.

Määritelmä 4. Jos R on relaatio joukosta A joukkoon B ja $(a,b) \in R$, sanotaan, että b on a:n *kuva* ja että a on b:n *alkukuva* ja että a *kuvautuu* b:ksi relaatiossa R. Tällöin käytetään myös merkintöjä $R(a,b)$, $a \xrightarrow{R} b$, tai aRb.

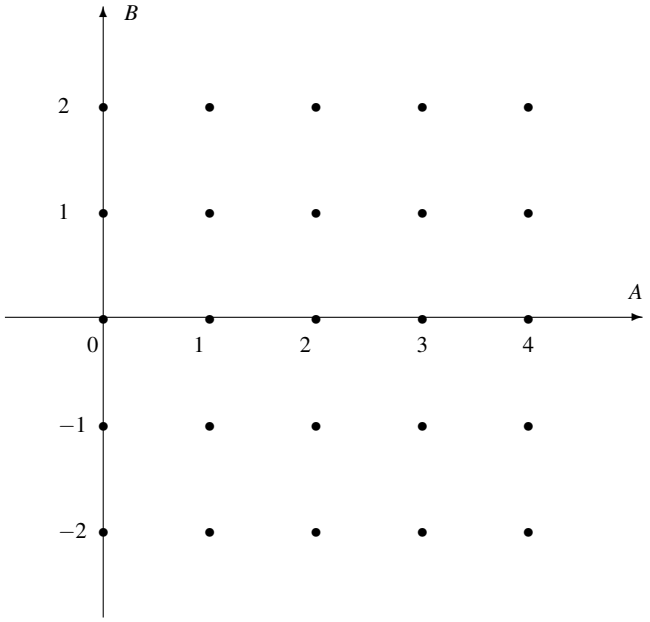
Määritelmä 5. Joukko $\{a \in A \mid (\exists b \in B)(a,b) \in R\}$ on relaation R *määrittelyjoukko*.

Esimerkki 3. Jos $R \subseteq A \times B$ on relaatio joukosta A joukkoon B, niin $(a,b) \in R$ merkitään monissa tapauksissa tavallisemmin aRb. Esimerkiksi tavallinen $<$ (pienempi kuin) on joukon $\mathbb{N}$ binäärinen relaatio, mutta on tavanomaisempaa merkitä $2 < 3$ kuin $(2,3) \in <$ tai $< (2,3)$.

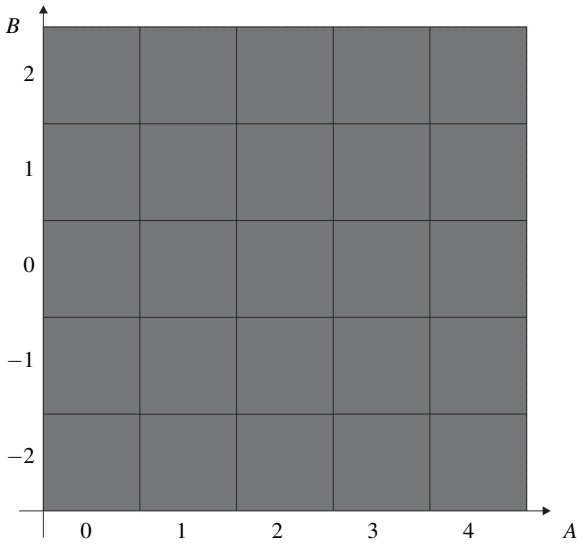
Esimerkki 4. Joukon A binääristä relaatiota $R = \{(a,a) \mid a \in A\}$ kutsutaan joukon A *identiteettirelaatioksi* tai *diagonaalirelaatioksi*.

Esimerkki 5. Olkoot $A = \{0,1,2,3,4\} \subseteq \mathbb{Z}$ ja $B = \{-2,-1,0,1,2\} \subseteq \mathbb{Z}$. Tällöin karteesinen tulo $A \times B$ muodostuu kuvassa 1.4 esitetystä pisteistöstä. Vaihtoehtoisesti, karteesinen tulo $A \times B$ voidaan esittää pikselimuodossa kuvan 1.5 mukaisesti

Tarkastellaan relaatiota



Kuva 1.4 Esimerkin 5 karteesinen tulo $A \times B$ koostuu kuvassa esitetystä $5 \cdot 5 = 25$:stä pisteestä. Vaaka-akselia voidaan kutsua A-akseliksi ja pystyakselia B-akseliksi.

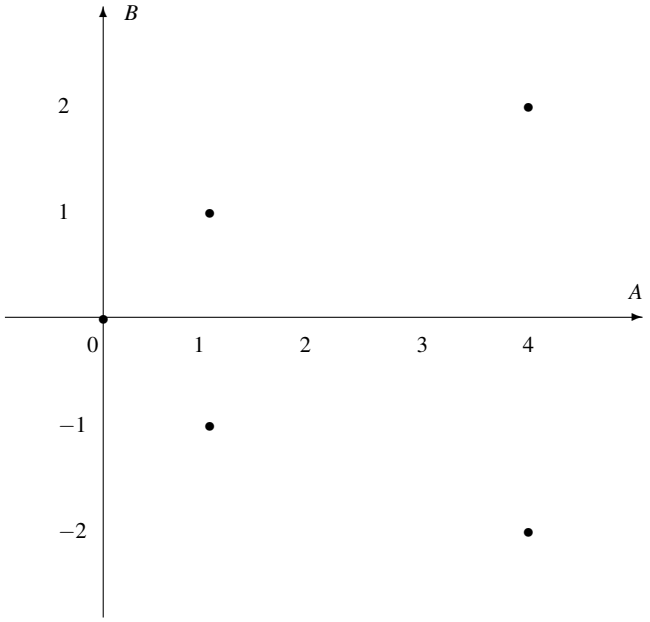


Kuva 1.5 Esimerkin 5 karteesinen tulo $A \times B$ pikselimuodossa esitettynä. Koko tasoa esittävä kuva koostuu $5 \cdot 5 = 25$:stä pikselistä. Vaaka-akselia voidaan kutsua A-akseliksi ja pystyakselia B-akseliksi.

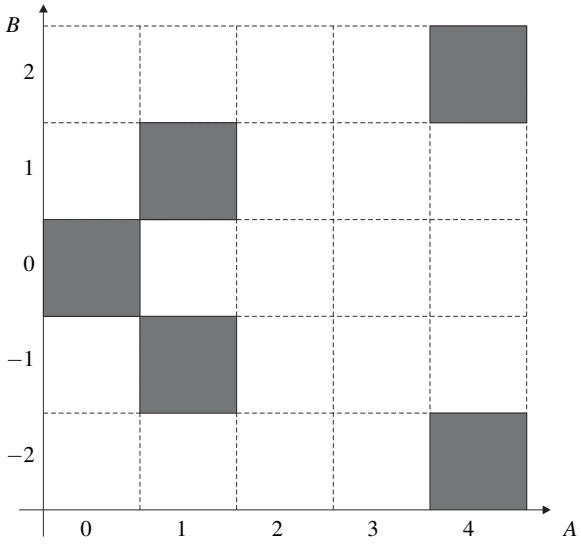
$$R = \{(0,0),(1,1),(1,-1),(4,2),(4,-2)\},$$

joka siis on karteesisen tulon $A \times B$ osajoukko. Relaatiota R edustaa kuvan 1.6 pisteistö ja samaa asiaa esittää kuvan 1.7 pikselimuoto.

Relaatio R voidaan kirjoittaa muodossa $R = \{(a,b) \mid a \in A, b \in B, b^2 = a\}$. Relaatio $R : A \to B$ edustaa siis eräänlaista neliöjuurta joukossa A . Joukon A alkioon 0 liittyy joukon B alkio 0, mikä



Kuva 1.6 Esimerkin 5 relaatio R AB-tasossa

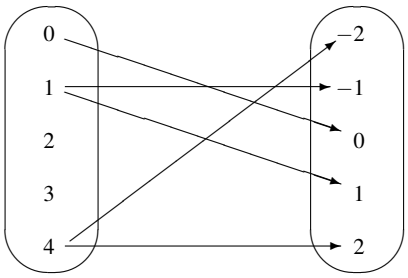


Kuva 1.7 Esimerkin 5 relaatio R pikselimuodossa esitettynä.

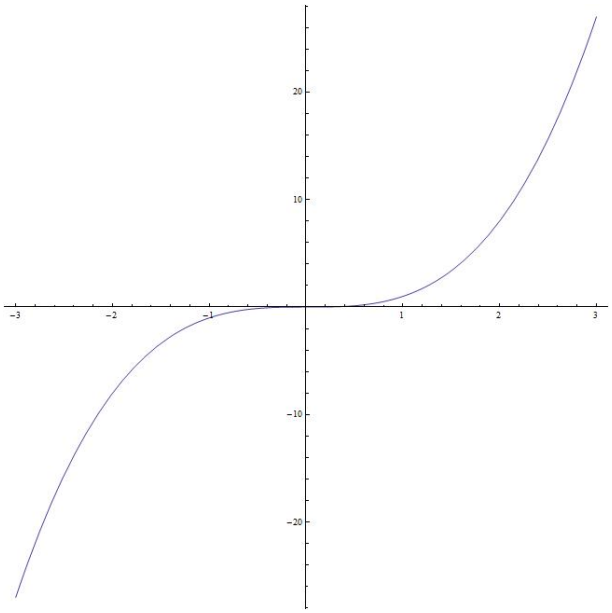
ilmaistaan siten, että pari $(0,0)$ on joukossa (relaatiossa) R. Lisäksi A:n alkioon 1 liittyvät joukon B alkiot -1 ja 1, mikä näkyy siten, että parit $(1,1)$ ja $(1,-1)$ ovat relaatiossa R ja lopulta A:n alkioon 4 liittyvät joukon B alkiot -2 ja 2, ja tämä ilmaistaan siten, että parit $(4,2)$ ja $(4,-2)$ ovat relaatiossa R.

Toisaalta taas joukon A alkioihin 2 ja 3 ei liity mikään joukon B alkio, mikä näkyy siten, että relaatiossa S ei ole muotoa $(2,b)$ tai $(3,b)$ olevia pareja. Täten siis 2 ja 3 eivät kuulu tämän relaation määrittelyjoukkoon (joka on $\{0,1,4\}$).

Äärellisten joukkojen relaatiot voidaan esittää myös (nuoli)kaavioilla, joissa $(a,b) \in R$ esitetään nuolella a:sta b:hen (kuva 1.8). Jos $A = B$, voidaan nuolikaaviossa jättää toinen joukko pois ja piirtää nuolet yhden joukon sisälle.



Kuva 1.8 Esimerkin 5 relaation nuolikaavioesitys.



Kuva 1.9 Relaation $\{(x,x^3) \mid x \in \mathbb{R}\}$ graafinen esitys.

1

Esimerkki 6. Origokeskisen yksikköympyrän yhtälö on $x^2 + y^2 = 1$. Toisin sanoen joukon $\mathbb{R} \to \mathbb{R}$ relaatio $C = \{(x,y) \mid x,y \in \mathbb{R}, x^2 + y^2 = 1\}$ koostuu niistä tason pisteistä, jotka ovat etäisyydellä 1 origosta. Relaation C graafinen esitys on kuvassa 1.2.

Esimerkki 7. Määritellään relaatio $L : \mathbb{R} \to \mathbb{R}$ seuraavasti: $L = \{(x,x^3) \mid x \in \mathbb{R}\}$. Relaation graafinen esitys on kuvassa 1.9. Tämä relaatio on itse asiassa myös funktio.

1.3 Relaatioiden yhdiste ja käänteisrelaatio

Määritelmä 6. Olkoot $R \subseteq A \times B$ ja $S \subseteq B \times C$ relaatioita. Niiden *yhdiste* on relaatio $A \to C$

$$S \circ R = \{(a,c) \mid \ (\exists b \in B)\ ((a,b) \in R \wedge (b,c) \in S)\}.$$

Määritelmä 7. Relaation $R \subseteq A \times B$ *käänteisrelaatio* $R^{-1} \subseteq B \times A$ määritellään $R^{-1} = \{(b,a) \mid (a,b) \in R\}$.

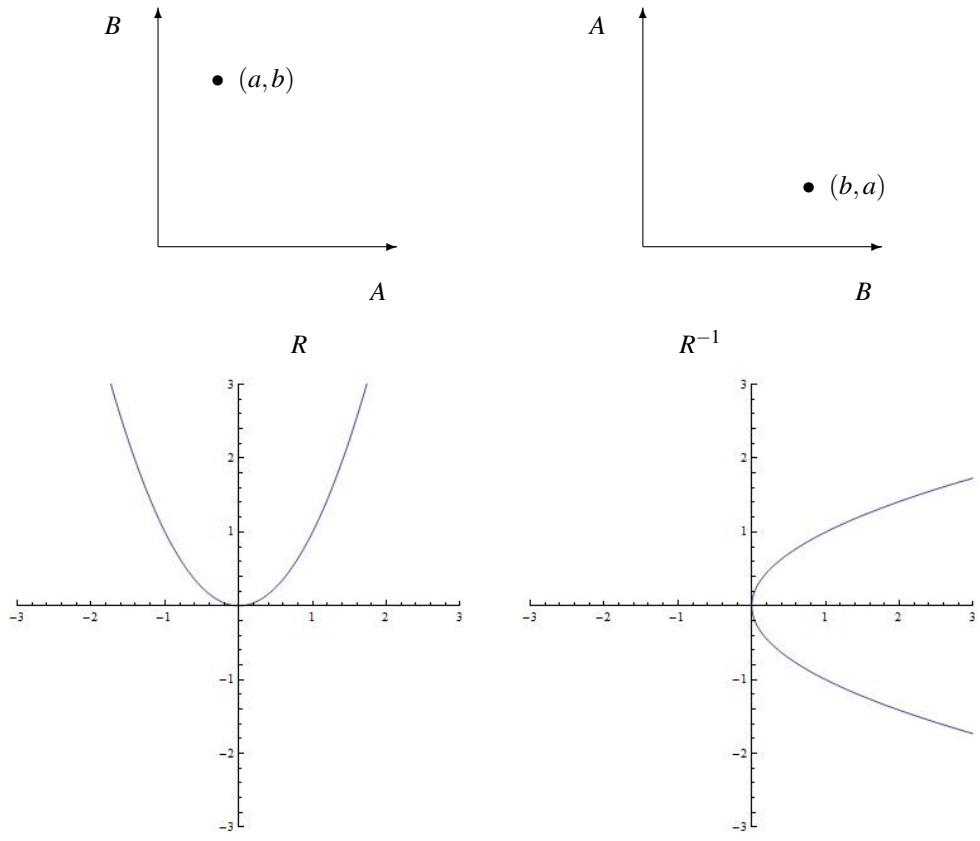
Huomautus 2. Relaatioiden R ja S yhdiste tunnetaan myös nimellä relaatioiden R ja S *tulo*. Määritelmän 6 tilanteessa relaatiotulo $S \circ R$ on siis relaatio joukosta A joukkoon C ja määritelmän 7 tilanteessa R^{-1} on relaatio joukosta B joukkoon A. Äärellisten joukkojen tapauksessa yhdistetty relaatio voidaan saada nuolikaaviota käyttäen.

Esimerkki 8. Olkoot joukot A ja B sekä relaatio R kuten esimerkissä 5 ja $C = \{0,1,2,4\}$. Määritellään relaatio $S \subseteq B \times C$ seuraavasti:

$$S = \{(-2,4),(-1,1),(0,0),(1,1),(2,4)\}.$$

Tällöin $S \circ R = \{(0,0),(1,1),(4,4)\}$. Voidaan huomata, että relaatio S on itse asiassa valikoitujen alkioiden neliöön korottaminen. Koska relaatio R toimii neliöjuuren kaltaisesti (tosin etumerkit sallien), on tulos luonteva: $S \circ R$ on joukon $\{0,1,4\}$ identiteettirelaatio.

Käänteisrelaatio R^{-1} on yksinkertaisesti määritelty vaihtamalla lähtö- ja määrittelyjoukot sekä ehdolla $(a,b) \in R \Leftrightarrow (b,a) \in R^{-1}$, minkä mukaisesti käänteisrelaation kuvaajassa pysty- ja vaakakoordinaatit vaihdetaan keskenään. Seuraavassa kuvassa on oikealla edustettuna piste relaatiossa R ja vasemmalla vastaava piste käänteisrelaatiossa R^{-1}. Siirtymä relaation kuvaajasta käänteisrelaation kuvaajaan edustaa siis peilausta suoran $a = b$ suhteen.



$$R = \{(x,x^2) \mid x \in \mathbb{R}\}, \qquad R^{-1} = \{(x^2,x) \mid x \in \mathbb{R}\}$$

Muistutetaan tässä yhteydessä että joukon A binäärinen relaatio tarkoittaa relaatiota $A \to A$. Tällöin relaation nuolikaavio voidaan piirtää ilman toista joukon A kopiota.

Määritelmä 8. Joukon A binäärinen relaatio R on *ekvivalenssirelaatio*, mikäli R toteuttaa seuraavat ehdot:

1. $(\forall a)\ aRa$ (refleksiivisyys),
2. $(\forall a)(\forall b)\ aRb \Rightarrow bRa$ (symmetria) ja
3. $(\forall a)(\forall b)(\forall c)\ aRb \wedge bRc \Rightarrow aRc$ (transitiivisuus).

Ekvivalenssirelaation tulkinta nuolikaaviossa on yksinkertainen: Refleksiivisyys merkitsee sitä, että jokaisesta alkiosta on nuoli itseensä, symmetria sitä, että nuolen $a \to b$ olemassaolosta seuraa nuolen $b \to a$ olemassaolo, ja transitiivisuus sitä, että nuolien $a \to b$ ja $b \to c$ olemassaoloista seuraa myös nuolen $a \to c$ olemassaolo.

Määritelmä 9. Olkoon R ekvivalenssirelaatio joukossa A. Määritellään alkion $a \in A$ *ekvivalenssiluokka* $[a] \subseteq R$ seuraavasti:

$$[a] = \{x \in A \mid xRa\}$$

Mikäli aRb, sanotaan, että a ja b ovat ekvivalentit (relaation R suhteen).

Huomautus 3. Määritelmän mukaan $[a]$ koostuu niistä joukon A alkioista, jotka ovat relaatiossa a:n kanssa. Nuolikaaviossa tämä merkitsee niitä joukon A alkioita, joista on nuoli a:n (ja päinvastoin symmetrian vuoksi). On helppo havaita, että jokainen ekvivalenssirelaatio R jakaa joukon A erillisiin ekvivalenssiluokkiin, jotka peittävät koko joukon A. Identiteettirelaatio $\{(a,a) \mid a \in A\}$ on aina ekvivalenssirelaatio, jossa tosin ekvivalenssiluokat ovat vain yhden alkion suuruisia. Ekvivalenssirelaatio voidaan siis nähdä yhtäsuuruuskäsitteen yleistyksenä.

Huomautus 4. Jos R on joukon A ekvivalenssirelaatio, on $[a] = [b] \Leftrightarrow aRb$.

Esimerkki 9. Tässä esimerkissä oletetaan, että joukossa $\mathbb{N}_0 = \{0,1,2,3,\ldots\}$ määritellyt yhteen- ja kertolaskuoperaatiot, vertailu $b \leq a$ ja vähennyslasku $a-b$ tapauksessa $b \leq a$ ovat hyvin määriteltyä ja tunnettuja. Tarkoitus on tämän pohjalta rakentaa joukko $\mathbb{Z}$, joka sisältää negatiiviset luvut.

Konstruktio saadaan aikaan intuitiolla, jonka mukaan yhtä lukua kuvaakin lukupari (s,v), jossa s edustaa säästöjen määrää (hallussa oleva omaisuus) ja v velan määrää (pois maksettava summa). Negatiiviset luvut rakennetaan tunnetuista objekteista käyttämällä joukko-opin käsitteitä, mukaanlukien relaatiot.

Edellämainitun intuition mukaan tilannetta $(10,5)$ jossa hallussa olevan omaisuuden arvo on 10 ja velan arvo 5 voidaan pitää samankaltaisena kuin tilannetta $(20,15)$. Kummassakin tilanteessa nimittäin velkojen maksun jälkeen päädytään tilanteeseen $(5,0)$. Molemmat näistä ovat vielä taloustilanteena lohdullisempia (positiivisempia) kuin $(3,8)$ tai $(9,14)$, jotka velkojen maksun jälkeen johtavat tilanteeseen $(0,5)$, jossa velkojen määrä on suurempi kuin hallussa oleva varallisuus.

Yllämainitun perusteella on ilmeistä, että varallisuustilanteet $(0,0)$, $(1,1)$, $(2,2)$, jne. kuvaavat kaikki yhtä ja samaa: varallisuutta ja velkoja on yhtä paljon, ja näitä lukupareja voitaisiinkin kutsua *nollan* esityksiksi. Pareja (a,b), joissa $a > b$ voidaan hyvällä syyllä kutsua *positiivisiksi* ja sellaisia pareja, joissa $a < b$ voidaan kutsua *negatiivisiksi*. Tällöin kuitenkin jokaisella taloustilanteella, olipa se positiivinen, nolla tai negatiivinen on äärettömän monta eri esitystä, mutta nämä voidaan ”liimata” yhdeksi matemaattiseksi objektiksi käyttämällä ekvivalenssirelaatioita.

Tämä tapahtuu seuraavasti: Määritellään joukossa $A = \mathbb{N}_0 \times \mathbb{N}_0$ relaatio $\sim$ seuraavasti:

$$(a,b) \sim (c,d) \Leftrightarrow a+d = b+c. \tag{1.1}$$

Huomaa, että kun a, b, c ja $d \in \mathbb{N}_0$, ei määritelmässä ole mitään ongelmallista, vaan $a+d$ ja $b+c$ ovat olemassa kaikille a, b, c, $d \in \mathbb{N}_0$. Jos sen sijaan olisi määritelmän oikea puoli kirjoitettu muotoon $a-b = c-d$, ensimmäinen ongelma syntyisi jo siitä, että vähennyslaskua $a-b$ ei ole joukossa $\mathbb{N}_0$ määritelty, kun $a < b$.

Seuraavaksi todetaan, että yhtälöllä (1.1) määritelty relaatio on todellakin ekvivalenssirelaatio. Tämä tapahtuu toteamalla ekvivalenssirelaation ehdot yksi kerrallaan:

- Refleksiivisyys tarkoittaa sitä, että mille hyvänsä $(a,b) \in A$ pätee $(a,b) \sim (a,b)$. Viimeksi mainittu puolestaan tarkoittaa, relaation $\sim$ määritelmän perusteella sitä, että $a+b = b+a$. Koska yhteenlasku on joukossa $\mathbb{N}_0$ vaihdannainen, on tämä tosi jokaiselle $(a,b) \in A$ ja siksi relaatio on refleksiivinen.
- Symmetria puolestaan tarkoittaa sitä, että $(a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$. Tulkitsemalla symboli $\sim$ eksplisiittisesti voidaan yllämainittu implikaatio kirjoittaa muotoon $a+d = b+c \Rightarrow a+b = d+a$, mikä on selvästi tosi aina kun a, b, c ja $d \in \mathbb{N}_0$.
- Transitiivisuus on voimassa, jos $(a,b) \sim (c,d) \wedge (c,d) \sim (e,f) \Rightarrow (a,b) \sim (e,f)$. Tämä voidaan nähdä oikeaksi seuraavasti: Jos premissit $(a,b) \sim (c,d)$ ja $(c,d) \sim (e,f)$ ovat voimassa, on määritelmän mukaan $a+d = b+c$ ja $c+f = d+e$. Tällöin $a+b+c+f = a+c+d+e$, mistä seuraa $a+f = b+e$ jopa ilman tietoa vähennyslaskusta. Näin ollen $(a,b) \sim (e,f)$.

Yllä tarkastettujen ehtojen perusteella $\sim$ on todellakin joukon $A = \mathbb{N}_0 \times \mathbb{N}_0$ ekvivalenssirelaatio. Määritellään kokonaisluvuksi ekvivalenssiluokka $[(a,b)] = \{(c,d) \mid (c,d) \sim (a,b)\}$, jolloin "niputetaan" yhteen esim. $(1,0)$, $(2,1)$, $(3,2)$ ... kaikki samaan luokkaan $[(1,0)]$. Sanotaan, että luokka $[(0,0)] = \{(0,0),(1,1),(2,2),\ldots\}$ on ns. *nollaluokka*, ja että esim. luokan $[(0,1)] = \{(0,1),(1,2),(2,3)\ldots\}$ kaltainen edustaa *negatiivisia* lukuja.

Määritellä *luokkien yhteenlasku* seuraavalla tavalla:

$$[(a,b)] + [(c,d)] = [(a+c, b+d)]$$

ja luokkien *kertolasku* seuraavasti:

$$[(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)].$$

(Mieti miksi kertolasku määritellään näin).

Näin määritellen pitäsi todeta, että luokkien yhteen- ja kertolasku on valitusta edustajasta riippumaton, siis jos $[(a,b)] = [(a_1,b_1)]$ ja $[(c,d)] = [(c_1,d_1)]$, on $[(a,b)]+[(c,d)] = [(a_1,b_1)]+[(c_1,d_1)]$ ja että vastaava yhtäsuuruus pätee myös kertolaskulle. Tämän jälkeen voidaan todeta, että jokaisella luokalla $[(a,b)]$ on olemassa vastaluokka $[(b,a)]$, joiden yhteenlasku tuottaa nollaluokan $[(a+b,b+a))]$. Lisäksi voidaan määritellä luokan $[(a,b)]$ *negatiivisuus* ehdolla $a < b$, vaikka koko ajan käsiteltäisiin pelkästään positiivisia kokonaislukuja.

Konstruktion lopuksi voidaan ottaa käyttöön helpommat merkinnät: Se, mitä ennen merkittiin luokalla $[(a,b)]$, merkitään uudessa järjestelmässä seuraavien vaihtoehtojen mukaan:

$$[(a,b)] \to \begin{cases} 0 \text{ jos } a = b \\ a-b \text{ jos } b < a \\ -(b-a) \text{ jos } b > a. \end{cases}$$

Edellä kuvatun konstruktion etu on se, että tunnetut lainalaisuudet kuten assosiatiivisuus $(a+b)+c = a+(b+c)$ ja distributiivisuus $a \cdot (b+c) = a \cdot b + a \cdot c$ on mahdollista näyttää toteen uudelle, ekvivalenssiluokkien päälle määritellylle järjestelmälle käyttämällä pelkästään entisen järjestelmän ($\mathbb{N}_0$) ominaisuuksia siten, että niitä sovelletaan pelkästään luokkien edustajiin:

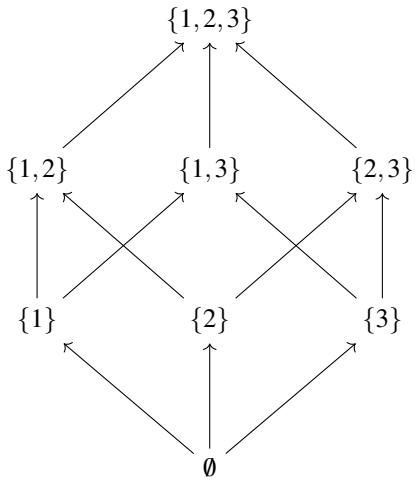
$$([(a,b)] + [(c,d)]) + [(e,f)] = [(a,b)] + ([(b,c)] + [(d,e)]).$$

Samoin voidaan todeta, että luokkien kertolasku ja yhteenlasku toteuttaa vaihdannais- assosiatiivisus- sekä distributiivilain.

Määritelmä 10. Joukon A binäärinen relaatio R on *osittainen järjestys*, mikäli R toteuttaa seuraavat ehdot:

1. $(\forall a)\ aRa$ (refleksiivisyys),
2. $(\forall a)(\forall b)\ aRb \wedge bRa \Rightarrow a = b$ (antisymmetria) ja
3. $(\forall a)(\forall b)(\forall c)\ aRb \wedge bRc \Rightarrow aRc$ (transitiivisuus).

Esimerkki 10. Alla olevaan kuvioon on sijoitettu kaikki joukon $\{1,2,3\}$ osajoukot, ja nuoli $A \to B$ merkitsee sisältymisrelaatiota $A \subseteq B$. Kaikkia nuolia ei ole piirretty näkyviin (mitkä puuttuvat?), mutta on helppo todeta, että $A \subseteq B$ on osittainen järjestys (harjoitustehtävä).



Esimerkki 11. Tavallinen järjestysrelaatio $\leq$ joukoissa $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ja $\mathbb{R}$ on osittainen järjestys.

Määritelmä 11. Olkoon A joko $\mathbb{N}$ tai $\mathbb{Z}$. Jaollisuusrelaatio $a \mid b$ (luetaan a jakaa b:n) määritellään seuraavalla tavalla:

$$a \mid b \Leftrightarrow (\exists c)(b = a \cdot c).$$

Mikäli a ei jaa b:tä, siis $\neg(a \mid b)$, merkitään myös $a \nmid b$.

Esimerkki 12. Joukossa $\mathbb{N}$ toteutuu $1 \mid 3$, sillä $3 = 1 \cdot 3$. Toisaalta $2 \nmid 3$, sillä yhtälö $3 = 2 \cdot c$ ei toteudu millekään $c \in \mathbb{N}$.

Esimerkki 13. Joukossa $\mathbb{Z}$ toteutuu $2 \mid (-2)$, sillä $-2 = 2 \cdot (-1)$ ja myös $-2 \mid 2$, sillä $2 = (-1) \cdot (-2)$.

Huomautus 5. Jaollisuusrelaatio on osittainen järjestys joukossa $\mathbb{N}$, mutta ei joukossa $\mathbb{Z}$ (Harjoitustehtävä).

Esimerkki 14. Joukossa $\mathbb{N}$ on esimerkiksi $1 \mid 2$, $2 \mid 4$, $2 \mid 6$, $1 \mid 3$, $3 \mid 6$, mutta $2 \nmid 3$ ja $3 \nmid 2$.

Määritelmä 12. Osittainen järjestys $\leq$ joukossa A on *täydellinen* eli *lineaarinen*, mikäli kaikille $x, y \in A$ on voimassa joko $x \leq y$ tai $y \leq x$.

Esimerkki 15. Tavallinen järjestysrelaatio $\leq$ joukoissa $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ja $\mathbb{R}$ on täydellinen eli lineaarinen järjestys.

Esimerkki 16. Jaollisuusrelaatio $\mid$ luonnollisten lukujen joukossa ei ole lineaarinen järjestys, sillä esim $2 \nmid 3$ ja $3 \nmid 2$, siis 2 ja 3 ovat jaollisuuden suhteen vertailukelvottomia.

Määritelmä 13. Joukossa A määritelty järjestysrelaatio $\leq$ on *hyvinjärjestys*, mikäli 1) $\leq$ on lineaarinen järjestys joukossa A ja 2) mikäli jokaisessa A:n epätyhjässä osajoukossa on olemassa pienin alkio järjestyksen $\leq$ suhteen.

Esimerkki 17. Reaalilukujen joukossa tavallinen järjestys $\leq$ ei ole hyvinjärjestys, sillä vaikka se on lineaarinen, ei esimerkiksi joukossa $(0,1)$ ole pienintä alkiota.

Esimerkki 18. Luonnollisten lukujen joukossa tavallinen järjestys $\leq$ on hyvinjärjestys, sillä se on lineaarinen ja jokaisessa epätyhjässä luonnollisten lukujen joukossa on pienin luku.

Määritelmä 14. Valitaan jokin ykköstä suurempi luku $n \in \mathbb{N}$ ja määritellään joukossa $\mathbb{Z}$ *lukuteoreettinen kongruenssirelaatio* $\equiv_n$ ehdolla

$$a \equiv_n b \Leftrightarrow n \mid (b-a).$$

Huomautus 6. Lukuteoria on matematiikan osa-alue, joka on perinteisesti keskittynyt kokonaislukuja koskevien lainalaisuuksien tutkimukseen, mutta 1800-luvulta alkaen laajentunut kokonaislukukäsitteen yleistyksiin. Edellä esitelty merkintä ei ole kaikkein tavallisin lukuteoreettisen kongruenssin merkintätavaksi, vaan perinteisesti lukuteoreettisesta kongruenssista käytetään merkintää $a \equiv b \pmod{n}$ ja luetaan "a on kongruentti b:n kanssa modulo n".

Esimerkki 19. [Jäännösluokat] Melko suoraviivaisesti voidaan todeta, että lukuteoreettinen kongruenssi on ekvivalenssirelaatio, ja vieläpä että ekvivalenssiluokille voidaan määritellä yhteen- ja kertolasku edustajien perustella: $[a]+[b]=[a+b]$ ja $[a]\cdot[b]=[a\cdot b]$ (mieti miksi määritelmä ei riipu luokkaa $[a]$ edustavan alkion a valinnasta).

Minkälaisia sitten ovat ekvivalenssiluokat? Valitaan esimerkiksi $n=6$, jolloin $a \equiv_6 b$ merkitsee sitä, että $6 \mid (b-a)$, mikä puolestaan tarkoittaa sitä, että $b-a = 6\cdot k \Leftrightarrow b = a+6\cdot k$, missä $k \in \mathbb{Z}$.

Näin ollen siis esimerkiksi luvun 0 kanssa ekvivalentit luvut saadaan lisäämällä tähän mikä hyvänsä luvun 6 monikerta. Täten

$$[0] = \{\ldots,-12,-6,0,6,12,18,\ldots\}$$

ja samoin

$$[1] = \{\ldots,-11,-5,1,7,13,19,\ldots\},$$

jne. Erityisesti on huomattava, että

$$[6] = \{\ldots,-6,0,6,12,18,24,\ldots\} = [0],$$

joten erisuuria ekvivalenssiluokkia modulo 6 on olemassa vain äärellinen määrä: [0], [1], …, [5].

Yllämainitun perusteella ekvivalenssiluokat $[a]$ ja $[b]$ ovat yhtäsuuria mikäli luokkien edustajat a ja b saadaan toisistaan vähentämällä tai lisäämällä jokin luvun 6 monikerta. Tämä voidaan ilmaista myös siten, että luokat $[a]$ ja $[b]$ ovat yhtäsuuret, mikäli lukujen a ja b jakaminen luvulla 6 tuottaa saman jakojäännöksen. Siksi näitä ekvivalenssiluokkia kutsutaan lukuteoriassa *jäännösluokiksi*.

Luokkien kerto- ja yhteenlakun määritelmien perusteella on esimerkiksi $[2]\cdot[3]=[2\cdot3]=[6]=[0]$, $[3]\cdot[3]=[3\cdot3]=[9]=[3]$, $[2]\cdot[4]=[8]=[2]$, $[4]+[2]=[6]=[0]$ jne. Tämä korostaa myös sitä, että kukin ekvivalenssiluokka voidaan esittää minkä hyvän edustajan avulla, esim. $[1]=[7]=[13]$, siis luokkaa $[1]$ kelpaa luvun 1 lisäksi edustamaan esim. luku 7 tai 13, sillä niillä on sama jakojäännös luvulla 6 jaettaessa. Kerto- ja yhteenlaskutaulukon täydentäminen jätetään harjoitustehtäväksi. Kyseessä on kuuden alkion (ekvivalenssiluokan) joukko, jolle on määritelty yhteen- ja kertolasku.

Tämän esimerkin tyyppiset algebralliset konstruktiot muodostavat perustan matematiikalle, jota käytetään digitaalisessa tiedonsiirrossa sekä tiedon salaamiseen, että tiedonsiirrossa tapahtuvien virheiden korjaamiseen.

1.4 Funktiot

Funktiot, jotka määritellään relaatioiden erikoistapauksina, ovat insinöörimatematiikan kurssikokonaisuuden kannalta keskeisimpiä matemaattisia käsitteitä.

Määritelmä 15. Relaatio $f : A \to B$ on funktio, jos jokaista joukon A alkiota a on tarkalleen yksi joukon B alkio b siten että $(a,b) \in f$.

Määritelmä 16. Edellisen määritelmän tapauksessa merkitään $f(a) = b$ ja relaatioiden yleistä terminologiaa käyttäen sanotaan, että b on a:n *kuva*, a on b:n *alkukuva*, ja että a *kuvautuu* b:ksi.

Funktion määritelmän mukaan siis jokaiselle lähtöjoukon alkiolle a on olemassa yksikäsitteinen kuva $b = f(a)$. Täten siis funktion määrittelyjoukko on sama kuin sen lähtöjoukko. Erityisesti lineaarialgebrassa käytetään termiä *kuvaus* funktion synonyyminä.

Huomautus 7. Yllä olevasta määritelmästä seuraa, että jokainen pystysuora leikkaa funktion kuvaajan tasan kerran.

Taustatietoa

Gottfried Wilhelm Leibniz (1646–1716) oli saksalainen matemaatikko, fyysikko ja filosofi, joka otti käyttöön funktion käsitteen, tosin geometrisen intuition pohjalta (nykyiseen muotoonsa funktiokäsite saatettiin 1800-luvulla). Leibniz kehitti differentiaali- ja integraalilaskennan Newtonin töistä riippumatta. Leibniz kehitteli myös ajatuksia automatisoidusta tietojenkäsittelystä.

(kuva: Wikimedia Commons)

Määritelmä 17. Olkoon $f : A \to B$ funktio. Jos $X \subseteq A$ ja $Y \subseteq B$, määritellään $f(X) = \{f(x) \mid x \in X\}$ ja $f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}$. Joukkoa $f(X)$ kutsutaan joukon X *kuvaksi* ja $f^{-1}(Y)$:tä joukon Y *alkukuvaksi*. Joukkoa $f(A)$ kutsutaan funktion $f : A \to B$ *arvojoukoksi*.

Esimerkki 20. Esimerkin 4 identiteettirelaatio on funktio.

Esimerkki 21. Esimerkin 6 relaatio C ei ole funktio, sillä $(\frac{1}{2}, \frac{\sqrt{3}}{2}) \in C$ ja $(\frac{1}{2}, -\frac{\sqrt{3}}{2}) \in C$, mikä merkitsee sitä, että luvulla $\frac{1}{2}$ on kaksi eri kuvaa vastoin funktion määritelmää. Sen lisäksi on lähtöjoukon $\mathbb{R}$ alkioita joilla ei ole lainkaan kuvaa maalijoukossa (myös $\mathbb{R}$), esimerkiksi lukua 2 ei vastaa mikään maalijoukon alkio y: tällöinhän pitäisi olla $2^2 + y^2 = 1$, toisin sanoen $y^2 = -3$, mikä ei voi toteutua millekään reaaliluvulle y.

Edellisen esimerkin tilannetta hieman muutellen saadaan relaatiosta C aikaan ainakin kaksi funktiota. Ensinnäkin lähtöjoukoksi tulee ottaa $[-1,1]$ koko $\mathbb{R}$:n sijaan. Jos nimittäin valitaan mikä hyvänsä luku $x \in [-1,1]$, on $1 - x^2$ aina välillä $[0,1]$, joten lukua $x \in [-1,1]$ vastaa aina jokin maalijoukon luku y, jolle siis pätee $y^2 = 1 - x^2$. Yleensä tällaisia lukuja y on kuitenkin kaksi (paitsi tapauksissa $x \in \{-1,1\}$), joten määritellään vielä (pitäen joukkoa $[-1,1]$ sekä lähtö- että maalijoukkona) $C_1 = \{(x,y) \mid x^2 + y^2 = 1, y \geq 0\}$ ja $C_2 = \{(x,y) \mid x^2 + y^2 = 1, y \leq 0\}$. Tällöin voidaan helposti varmistua siitä, että esimerkiksi C_1 on funktio: koska joukon C_1 määritelmässä vaaditaan, että $y \geq 0$, on kutakin $x \in [-1,1]$ kohti olemassa vain yksi y:n arvo, jolle pätee $y^2 = 1 - x^2$. Vastaavasti voidaan todeta, että C_2 on funktio. Tavallista merkintätapaa käyttäen kirjoitetaan $C_1(x) = \sqrt{1-x^2}$, kun $x \in [-1,1]$ ja $C_2(x) = -\sqrt{1-x^2}$, kun $x \in [-1,1]$. Kuten helposti todetaan, $C = C_1 \cup C_2$.

Huomautus 8. Jos funktion lähtö- ja määrittelyjoukko A ja B ovat reaalisuoran osia, voidaan näitä korostaa graafisessa esityksessä piirtämällä näkyviin ainoastaan joukkoja A ja B vastaavat osat reaalisuorasta.

Lause 1. *Jos $f : A \to B$ ja $g : B \to C$ ovat funktiota, on relaatiotulo $g \circ f$ myös funktio*

Todistus. Harjoitustehtävä.

Edellisen lauseen nojalla voidaan asettaa seuraava määritelmä.

Määritelmä 18. Olkoot $f : A \to B$ ja $g : B \to C$ funktioita. *Yhdistetty funktio* $g \circ f$ on relaatiotulo $g \circ f : A \to C$, jolle siis relaatiotulon määritelmän mukaan pätee $(g \circ f)(a) = g(f(a))$. Tällöin funktiota f kutsutaan *sisäfunktioksi* ja g:tä *ulkofunktioksi*.

Esimerkki 22. Jos $h(x) = e^{-x^2}$, voidaan h kirjoittaa muodossa $h = g \circ f$, missä $g(x) = e^x$ on ulkofunktio ja $f(x) = -x^2$ on sisäfunktio.

Lauseen 1 mukaan kahdesta funktiosta yhdistämällä saatu relaatio on aina funktio. Sen sijaan vaikkapa esimerkkiä 5 tarkastelemalla voidaan todeta, että funktion käänteisrelaatio ei aina ole funktio. Sen selvittämiseksi, millaisten funktioiden käänteisrelaatio on funktio, otetaan käyttöön seuraavat käsitteet.

Määritelmä 19. Funktio $f : A \to B$ on *injektio*, jos $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$. $f : A \to B$ on *surjektio*, jos $f(A) = B$. $f : A \to B$ on *bijektio*, jos f on sekä injektio että surjektio.

Sanallisesti injektiivisyys merkitsee sitä, että eri alkukuvilla on eri kuvat. Epäsuoran todistuksen ideaa käyttäen funktion injektiivisyys voidaan kirjoittaa myös muotoon $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$. Surjektiivisuusehto taas puolestaan merkitsee sitä, että jokaisella joukon B alkiolla *on* alkukuva. Bijektiivisyys puolestaan surjektiivisuuden ja injektiivisyyden yhdistelmänä merkitsee sitä, että jokaisella joukon B alkiolla on *tarkalleen yksi* alkukuva joukossa A.

Huomautus 9. Geometrisesti tulkiten injektiivisyys tarkoittaa sitä, että jokainen vaakasuora leikkaa kuvaajan korkeintaan kerran ja surjektiivisuus sitä, että jokainen vaakasuora leikkaa kuvaajan ainakin kerran. Näin ollen bijektiivisyys merkitsee sitä, että jokainen vaakasuora leikkaa kuvaajan *tasan* kerran.

Esimerkki 23. Funktio $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ ei ole injektio eikä surjektio. Esimerkiksi $f(-1) = (-1)^2 = 1 = f(1)$, joten luvuilla -1 ja 1 on sama kuva 1, mikä on vastoin injektiivisyysehtoa. Sen lisäksi luvulla -1 ei ole lainkaan alkukuvaa, sillä $x^2 \neq -1$ kaikille reaaliluvuille x, mikä on vastoin surjektiivisuusehtoa.

Sen sijaan funktio $g : \mathbb{R} \to [0, \infty)$, $g(x) = x^2$ on surjektio, sillä jokaista lukua $y \in [0, \infty)$ kohti on olemassa alkukuva $x = \sqrt{y}$, jolle pätee $g(x) = y$. Funktio g ei kuitenkaan ole injektio, sillä $g(-1) = 1 = g(1)$.

On huomattava, että vaikka funktioiden f ja g määrittelevä lauseke on sama $f(x) = g(x) = x^2$, ovat f ja g siitä huolimatta eri funktioita. Tämä johtuu siitä, että f:n ja g:n määrittelyjoukot ovat erisuuret. Funktio nimittäin määritellään karteesisen tulon osajoukkona, jolloin siis sekä lähtö- että maalijoukkojen identtisyys on edellytys funktioiden yhtäsuuruudelle.

Lause 2. *Jos $f : A \to B$ on bijektiivinen funktio, on käänteisrelaatio $f^{-1} : B \to A$ myös funktio, ns. f:n* käänteisfunktio*. Kääntäen, jos funktion $f : A \to B$ käänteisrelaatio $f^{-1} : B \to A$ on funktio, on f bijektio.*

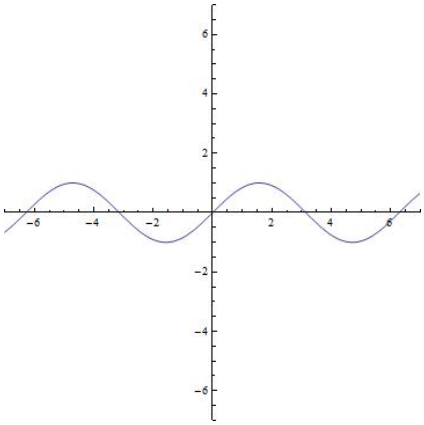
Todistus. Todistetaan ensimmäinen väite ja jätetään toinen harjoitustehtäväksi.

Oletetaan ensin, että f on bijektio. Tällöin jokaisella joukon B alkiolla b on tasan yksi alkukuva $a \in A$, mistä seuraa, että jokaisella $a \in A$ on tasan yksi kuva relaatiossa f^{-1}. Tämä puolestaan onkin jo funktion määritelmä. □

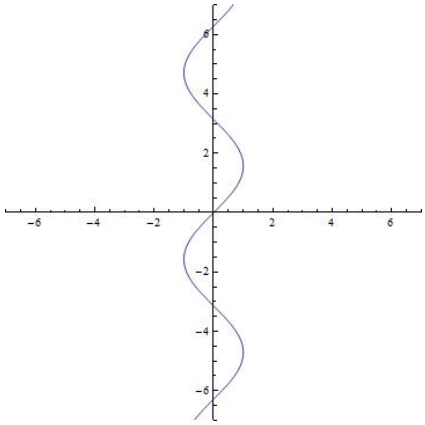
Huomautus 10. Olkoon $f : A \to B$ bijektio. Tällöin siis käänteisfunktio $f^{-1} : B \to A$ on olemassa. Määritelmän mukaan $a = f^{-1}(b)$ merkitsee, että $(b,a) \in f^{-1}$, mikä taas tapahtuu tarkalleen silloin kun $(a,b) \in f$, mikä edelleen voidaan merkitä $f(a) = b$. Näin ollen $a = f^{-1}(b) = f^{-1}(f(a)) = (f^{-1} \circ f)(a)$, mikä merkitsee siis sitä, että $f^{-1} \circ f : A \to A$ on joukon A identiteettifunktio. Samoin voidaan todeta, että $f \circ f^{-1} : B \to B$ on joukon B identiteettifunktio.

Huomautus 11. Jos $f : A \to B$ on injektio, voidaan B:tä rajoittamalla saada bijektio $f : A \to f(A)$. Tällöin on olemassa käänteisfunktio $f^{-1} : f(A) \to A$.

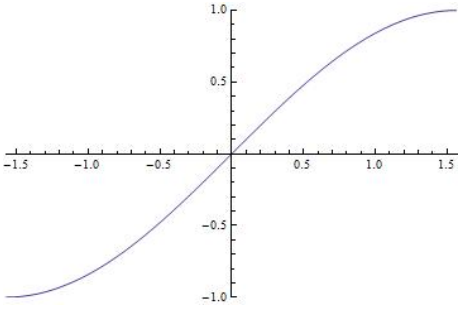
Esimerkki 24. Seuraavissa kuvaajissa on esitettynä sinifunktion ja sen käänteisrelaation kuvaaja. Ylemmällä rivilla määrittelyjoukkona toimii koko $\mathbb{R}$, ja voidaan huomata että että sinifunktiolla ilman rajoituksia ei ole käänteisfunktiota. Alemmalla rivillä on tilannetta rajoitettu sopivasti jolloin saadaan välille $[-\frac{\pi}{2}, \frac{\pi}{2}] \to [0,1]$ määritelty bijektiivinen sinifunktio, jolla on myös käänteisfunktio.



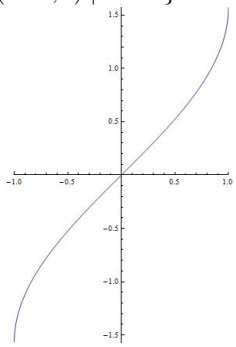
$\sin = \{(x, \sin x) \mid x \in \mathbb{R}\}$,



$\sin^{-1} = \{(\sin x, x) \mid x \in \mathbb{R}\}$



$\sin = \{(x, \sin x) \mid x \in [-\frac{\pi}{2}, \frac{\pi}{2}]\}$



$\sin^{-1} = \{(\sin x, x) \mid x \in [-\frac{\pi}{2}, \frac{\pi}{2}]\}$

1.5 Joukkojen mahtavuus

Määritelmä 20. Joukoilla A ja B on sama *kardinaliteetti* jos on olemassa bijektio $f : A \to B$. Tällöin sanotaan myös, että A ja B ovat *yhtä mahtavat* (engl. equipotent, equinumerous) ja merkitään $|A| = |B|$. Jos A on äärellinen joukko, merkintä $|A|$ tarkoittaa joukon A alkioiden lukumäärää.

Määritelmä 21. Joukon A kardinaliteetti on korkeintaan yhtä suuri kuin joukon B, mikäli on olemassa injektio $A \to B$. Tällöin sanotaan myös, että A on *korkeintaan yhtä mahtava* kuin B ja merkitään $|A| \leq |B|$.

Mikäli on olemassa injektio $A \to B$, mutta ei bijektiota $A \to B$, sanotaan, että B on *mahtavampi* kuin A ja merkitään $|A| < |B|$.

Lause 3. *Olkoon I jokin joukkojen kokoelma. Määritellään joukossa I relaatio $A \sim B$ ehdolla $|A| = |B|$. Tällöin $\sim$ on ekvivalenssirelaatio.*

Todistus. Harjoitustehtävä.

Lause 4. *Äärelliset joukot ovat yhtä mahtavat tarkalleen silloin kun niissä on sama määrä alkioita.*

Todistus. Merkitään $A = \{a_1, \ldots, a_n\}$ ja $B = \{b_1, \ldots, b_m\}$. Jos $n = m$, on $f(a_i) = b_i$ bijektio $A \to B$. Oletetaan sitten, että $m < n$ ja tehdään vastaoletus, että olisi bijektio $f : A \to B$. Koska $|B| < |A|$, on oltava alkiot $a_i \neq a_j$, joille $f(a_i) = f(a_j)$, jolloin f ei ole injektio eikä siis myöskään bijektio. □

Äärettömien joukkojen tapauksessa tilanne on mutkikkaampi. On nimittäin mahdollista, että joukko on yhtä mahtava aidon osajoukkonsa kanssa.

Esimerkki 25. Hilbertin hotelli

Lause 5. *Joukko $\mathbb{N} = \{1, 2, 3, \ldots\}$ on yhtä mahtava joukon $\mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}$ kanssa.*

Todistus. Helposti havaitaan, että $f : \mathbb{N} \cup \{0\} \to \mathbb{N}$, $f(n) = n + 1$ on bijektio.

Lause 6. *Joukko $\mathbb{N}$ on yhtä mahtava joukon $2\mathbb{N} = \{2, 4, 6, \ldots\}$ kanssa.*

Todistus. Helposti havaitaan, että $f : \mathbb{N} \to 2\mathbb{N}$, $f(n) = 2n$ on bijektio.

Määritelmä 22. Jos joukko A on yhtä mahtava joukon $\mathbb{N}$ kanssa, sanotaan että A on *numeroituva*. Tällöin on siis olemassa bijektio $f : \mathbb{N} \to A$, jolloin joukon A alkiot voidaan esittää muodossa $f(1), f(2), f(3), \ldots$ (numerointi).

Lause 7. *Joukko $\mathbb{Z}$ on numeroituva.*

Todistus. Harjoitustehtävä.

Lause 8. *Joukko $\mathbb{N} \times \mathbb{N}$ on numeroituiva.*

Todistus. Määritellään funktio $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ seuraavasti: $f(m, n) = \frac{(n+m-2)(n+m-1)}{2} + n$ ja todetaan, että tämä on bijektio. Toteaminen jätetään harjoitustehtäväksi.

Lause 9. *Joukko $\mathbb{Q}$ on numeroituva.*

Todistus. Jätetään harjoitustehtäväksi. Tässä voidaan hyödyntää edellistä lausetta.

Lause 10. *Joukko $\mathbb{R}$ ei ole numeroituva.*

Todistus. Tehdään vastaoletus, jonka mukaan $\mathbb{R}$ on numeroituva. Tällöin reaaliluvut voidaan asettaa jonoon: $\mathbb{R} = \{r_1, r_2, r_3, \ldots\}$. Olkoon $r_i = n_i.d_{i1}d_{i2}d_{i3}\ldots$ i:nnen reaaliluvun desimaalikehitelmä ja tarkastellaan näitä kaikkia yhdessä:

$$\begin{aligned} r_1 &= n_1.d_{11}d_{12}d_{13}d_{14}\ldots \\ r_2 &= n_2.d_{21}d_{22}d_{23}d_{24}\ldots \\ r_3 &= n_3.d_{31}d_{32}d_{33}d_{34}\ldots \\ r_4 &= n_4.d_{41}d_{42}d_{43}d_{44}\ldots \\ &\vdots \end{aligned}$$

ja muodostetaan desimaalikehitelmä $r = m.c_1c_2c_3\ldots$, jonka desimaalit valitaan seuraavasti: $m \neq n_1$ ja $c_i = d_1 + 1$, jos $d_i < 9$ ja $c_i = 0$ jos $d_i = 9$. Näin valitsemalla saadaan luku, jonka i:s desimaali poikkeaa yllä olevan luettelon i:nnen luvun i:nnestä desimaalista. Täten luku r ei voi olla listassa, mikä on vastoin vastaoletusta. □

Määritelmä 23. Ääretöntä joukkoa, joka ei ole numeroituva, sanotaan *ylinumeroituvaksi*.

Määritelmä 24. Joukon A *potenssijoukko* määritellään

$$2^A = \{X \mid X \subseteq A\}.$$

Toisin ilmaistuna, 2^A on joukon A kaikkien osajoukkojen joukko.

Esimerkki 26. Olkoon $A = \{1,2\}$. Tällöin $2^A = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$.

Esimerkki 27. Esimerkin 10 kuviossa esiintyvät kaikki joukon $2^{\{1,2,3\}}$ alkiot.

Lause 11. *Jos A on äärellinen, on $\left|2^A\right| = 2^{|A|}$.*

Todistus. Harjoitustehtävä.

Lause 12. *2^A on mahtavampi kuin A*

Todistus. Selvästi $a \to \{a\}$ on injektio $A \to 2^A$, joten A on korkeintaan yhtä mahtava kuin 2^A. Oletetaan sitten, että A ja 2^A olisivat yhtä mahtavat, mikä merkitsee sitä, että olisi bijektio $f : A \to 2^A$.

Tällöin voidaan määritellä $X = \{a \in A \mid a \notin f(a)\}$. Koska $X \subseteq A$, ja f on bijektio, on joukolle $X \in 2^A$ olemassa tasan yksi alkukuva $x \in A$, jolle siis $X = f(x)$. Jos $x \notin f(x)$, seuraa määritelmästä että $x \in X = f(x)$ ja jos $x \in f(x)$, seuraa määritelmästä, että $x \notin f(x)$. Tämä on ristiriita, minkä vuoksi oletettua bijektiota ei voi olla olemassa.

Huomautus 12. Edellisen lauseen perusteella on mahdollista muodostaa minkä hyvänsä joukon A avulla päättymätön ketju

$$|A| < \left|2^A\right| < \left|2^{2^A}\right| < \left|2^{2^{2^A}}\right| < \ldots,$$

jossa seuraava joukko on edellisen potenssijoukkona mahtavampi kuin edellinen.

Tämän luvun lopuksi esitetään todistuksetta lause, joka kytkee ”pienimmän” mahdollisen ääretömän joukon $\mathbb{N}$ ja joukon $\mathbb{R}$ kardinaliteetit toisiinsa.

Lause 13. *Joukko $2^{\mathbb{N}}$ on yhtä mahtava kuin $\mathbb{R}$.*

Huomautus 13. Kysymys siitä olisiko olemassa jotain joukkoa X, jonka kardinaliteetti olisi aidosti luonnollisten lukujen $\mathbb{N}$ ja reaalilukujen $\mathbb{R}$ välissä, siis $|\mathbb{N}| < |X| < |\mathbb{R}|$ askarrutti matemaatikkoja erityisesti 1900-luvun alkupuolella. Yleisesti otaksuttiin, että tällaista joukkoa ei ole olemassa, ja tämä otaksuma tunnetaan nimellä *kontinuumihypoteesi*.

Vuodesta 1940 asti on tiedetty, että kontinuumihypoteesia ei voi todistaa vääräksi ja 1963 asti että sitä ei myöskään voi todistaa oikeaksi formaalissa joukko-opissa, jota nykyään pidetään matematiikan loogisena perustana. Näin ollen voidaan sanoa, että nykymatematiikan loogisten perusteiden puitteissa ei voi ottaa mitään kantaa kontinuumihypoteesin oikeellisuuteen, ja edelleen yksi tapa ilmaista asia on sanoa että kontinuumihypoteesi on ratkeamaton (undecidable) ongelma nykyisin käytetyssä joukko-opin aksiomatisoinnissa.

Huomautus 14. Lauseen 13 todistamiseksi riitää osoittaa, että $2^{\mathbb{N}}$ on yhtä mahtava reaalilukuvälin $[0,1]$ kanssa, sillä on olemassa bijektio $[0,1] \to \mathbb{R}$. Millainen tämä bijektio voisi olla? Olisiko helpompaa etsiä ensin bijektio $(0,1) \to \mathbb{R}$?

Huomautus 15. Desimaaliesitys perustuu kymmeneen erilaiseen numeromerkintään $\{0,1,2,\ldots,9\}$, mutta yhtä lailla on mahdollista merkitä lukuja binäärimerkinnöin, käyttämällä vain numeroita 0 ja 1. Tällöin kaikki välin $[0,1]$ luvut voidaan esittää muodossa $0,b_1b_2b_3\ldots$, missä $b_i \in \{0,1\}$. Mieti miten tästä seuraa bijektio $2^{\mathbb{N}} \to [0,1]$.

Luku 2
Algebrallisista rakenteista

2.1 Määritelmä ja esimerkkejä

Määritelmä 25. Algebrallinen rakenne on joukko A, jossa on määritelty äärellinen määrä operaatioita. Operaatiot voivat olla nullaarisia (nollapaikkaisia), unaarisia (yksipaikkaisia), binäärisiä (kaksipaikkaisia), ternäärisiä (kolmipaikkaisia), jne. Operaatioiden lisäksi voi olla äärellinen määrä aksioomia.

Yllämainitussa määritelmässä nullaarinen operaatio tarkoittaa vakiota ja unaarinen eli yksipaikkainen operaatio tarkoittaa sitä, että siihen ottaa osaa vain yksi joukon A alkio, esimerkkinä voidaan mainita vastaluku reaalilukujen joukossa $\mathbb{R}$: $a \mapsto -a$ on tyypillinen unaarinen operaatio. Binäärisistä operaatioista esimerkkeinä toimivat vaikkapa yhteen- ja kertolasku reaalilukujen joukossa: kahdesta luvusta a ja b muodostetaan yksi luku operaatioilla $a+b$ ja $a \cdot b$.

Ternäärisiä tai useampipaikkaisia operaatioista ei liene koulukurssista tuttuja esimerkkejä tarjolla, mutta niitä voidaan määritellä periaatteessa aivan mielivaltaisesti, esim.

$$T(x,y,z) = 3x^2y + 3xz + z^3,$$

joka määritelee funktion $\mathbb{R}^3 \to \mathbb{R}$.

Esimerkki 28. Reaalilukujen kunta $(\mathbb{R}, +, \cdot, 0, 1)$ (kts. Matematiikan perustiedot) muodostaa algebrallisen systeemin, jonka joukossa $\mathbb{R}$ on määritelty kaksi binääristä operaatiota: yhteenlasku $+$ ja kertolasku $\cdot$. Lisäksi näihin operaatiohin liittyvät neutraalialkio yhteenlaskun suhteen (kutsutaan nolla-alkioksi ja yleensä merkitään 0) ja neutraalialkio kertolaskun suhteen (kutsutaan ykkösalkioksi ja yleensä merkitään 1). Nämä ovat nullaarisia operaatioita.

Reaalilukujen kunnan määrittelyyn liittyy myös aksioomia, joista voidaan mainita esimerkkeinä $(\forall a)(\forall b)(a+b = b+a)$, $(\forall a)(\forall b)(\forall c)(a \cdot (b+c) = a \cdot b + a \cdot c)$, jne.

Edellämainittuja luonnehdintoja tarkasteltaessa voidaan kuitenkin todeta, että käsitettä ”joukossa määritelty operaatio” ei ole erityisemmin määritelty. Tämän kurssin alkuosiin tukeutuen eksakti määrittely ei kuitenkaan ole vaikea, vaan päinvastoin: Nullaarinen operaatio määritellään joukon A alkiona, unaarinen operaatio joukossa A määritellään funktiona $A \to A$, binäärinen operaation funktiona $A \times A \to A$, ternäärinen operaatio funktiona $A \times A \times A \to A$, jne.

Tässä yhteydessä voidaan tietysti myös muistaa, että funktio on erityistapaus relaatiosta (kts. Luku 1), ja että relaatiolla, sen enempää kuin funktiollakaan, ei tarvitse olla mitään ”algebrallista lauseketta” joka määrittelisi funktion, vaan esimerkiksi äärellisissä joukoissa pelkkä taulukointi riittää (kts. Luku 1).

Edellämainitun perusteella binäärinen operaatio joukossa A voidaan määritellä funktiona $A \times A \to A$, mikä määritelmänsä vuoksi on karteesisen tulon $(A \times A) \times A$ osajoukko, joka toteuttaa funktiolle määrätyn ehdon: Jokaisella lähtöjoukon $A \times A$ alkiolla on tasan yksi kuva maalijoukossa A.

2.2 Grupoidi

Edellisen luvun perusteella algebrallisen rakenteeseen riittää joukko A ja yksikin joukossa A määritelty operaatio, mutta yleensä tarkastellaan sellaisia rakenteita, joissa on vähintään yksi binäärinen operaatio. Tämä puolestaan saattaa olla mielivaltaisesti määritelty, mitä havainnollistaa seuraava esimerkki.

Yksinkertaisin binäärisen operaation sisältävä algebrallinen rakenne esitetään seuraavassa määritelmässä.

Määritelmä 26. *Grupoidi* eli *Magma* on algebrallinen rakenne $(A,*)$, jossa on määritelty yksi binäärinen operaatio $*$.

Esimerkki 29. Joukossa $A=\{\alpha,\beta,\gamma,\delta\}$ taulukon

$*$	α	β	γ	δ
α	β	γ	β	δ
β	δ	δ	α	α
γ	α	γ	α	β
δ	β	δ	γ	δ

perustella määritelty operaatio määrittelee neljän alkion magman, jossa esimerkiksi $\alpha*\beta=\gamma$, $\beta*\alpha=\delta$, $(\alpha*\beta)*\gamma=\gamma*\gamma=\alpha$ ja $\alpha*(\beta*\gamma)=\alpha*\alpha=\beta$.

Näistä huomataan, että säännöt $x*(y*z)=(x*y)*z$ ja $x*y=y*x$ eivät siis välttämättä päde. Toisaalta ei ole syytä miksi näiden pitäisikään päteä, kun kerran magman kertolasku on määritelty täyttämällä yllä oleva kertotaulu sattumanvaraisesti.

Huomautus 16. Koska magman (eli grupoidin) algebrallinen operaatio ei ole välttämättä millään tavoin perusteltu, ei magmoilla ole mitään erityistä merkitystä matematiikan sovelluksissa tai edes teoriassa.

2.3 Puoliryhmä

Puoliryhmä (semigroup) on magma jonka operaatio $*$ toteuttaa aksiooman

$$(\forall x,y,z)((x*y)*z=x*(y*z)).$$

Tämän aksiooman toteuttavaa operaatiota $*$ kutsutaan *assosiatiiviseksi*. Voidaan siis sanoa, että puoliryhmä on siis assosiatiivinen magma.

Esimerkki 30 (Vapaa puoliryhmä). Olkoon $\Sigma=\{a,b,c\}$ kolmen alkion joukko ja merkitään karteesista tuloa Σ^2 tavallisten merkintöjen (a,a), (a,b) jne sijaan lyhyemmin $\Sigma^2=\{aa,ab,ac,ba,bb,bc,ca,cb,cc\}$ ja $\Sigma^3=\{aaa,aab,aac,aba,abb,\ldots,ccc\}$, jne.

Puoliryhmien teoriassa äärellistä joukkoa Σ kutsutaan *aakkostoksi*, ja aakkoston alkioista muodostettuja merkkijonoa *sanoiksi*. Joukko Σ^2 on 2-pituisten, Σ^3 3-pituisten, jne. sanojen joukko yli aakkoston Σ.

Kaikkien sanojen joukko yli aakkoston Σ saadaan äärettömänä unionina

$$\Sigma^+=\Sigma\cup\Sigma^2\cup\Sigma^3\cup\ldots$$

Määritellään operaatio $*$ (ns. konkatenaatio) joukossa Σ^+ seuraavasti: Jos $w_1,w_2\in\Sigma^+$ ovat n_1- ja n_2-pituisia sanoja, niin w_1*w_2 on n_1+n_2-pituinen sana joka saadaan kirjoittamalla sanat w_1 ja w_2 peräkkäin. Tällöin sanotaan myös, että aakkosto $\Sigma=\{a,b,c\}$ *generoi* puoliryhmän Σ^+.

Esimerkki 31. Vapaassa puoliryhmässä $\{a,b,c\}^+$ on

$$(abbca*ccab)*abcc=abbcaccab*abcc=abbcaccababcc \quad \text{ja}$$
$$abbca*(ccab*abcc)=abbca*ccababcc=abbcaccababcc,$$

mikä havainnollistaa operaation $*$ assosiatiivisuutta. Puoliryhmien teoriassa on myös tapana käyttää operaatiosymbolin $*$ sijasta pistettä $\cdot$ samoin kuin kertolaskussa, tai jättää symboli kokonaan kirjoittamatta, siis $abbca * ccab = abbca \cdot ccab = abbcaccab$.

Huomautus 17. Tarkastellaan edelleen (vapaata) puoliryhmää, jonka generoivat alkiot $\{a,b,c\}$. Edellä mainitun perusteella tämän puoliryhmän alkiot voidaan esittää yksikäsitteisesti merkkijonoina yli aakkoston $\{a,b,c\}$, esim. *aabcbaab* ja *abca* ovat mainitun vapaan puoliryhmän alkioita, ja näille puoliryhmän operaatio vastaa konkatenaatiota.

Hyvinkin moninaisista syistä voidaan joutua tarkastelemaan puoliryhmää, jossa jokin yhtäsuuruus, esim. $ab = bc$ on voimassa. Tämä merkitsee sitä, että puoliryhmän alkioille määritellään ekvivalenssirelaatio $w_1 \sim w_2$ mikäli $w_1 = w_2$ tai w_2 saadaan w_1:stä korvaamalla merkkijono ab merkkijonolla bc:llä tai päinvastoin ja toistamalla korvaamista uudelleen.

Tällä tavoin saadut ekvivalenssiluokat otetaan uuden järjestelmän alkioiksi. Mitä hyvänsä ekvivalenssiluokkaa voidaan toki esittää jollakin alkiolla $w \in \{a,b,c\}^+$, mutta esittävä alkio voidaan aina korvata toisella yllä mainitun säännön perusteella.

Näin saadusta puoliryhmästä käytetään merkintää $\langle \Sigma \mid ab = bc \rangle$, ja sanotaan että se ei ole vapaa, vaan sitä sitoo ehdon $ab = bc$ indusoima ekvivalenssirelaatio. Koska varsinainen konstruktio kulkee ekvivalenssirelaatioiden kautta, kutsutaan määritelmässä esiintyviä yhtäsuuruuksia $ab = bc$ myös *relaatioksi*. Käytännnössä siis tämä tarkoittaa, että sanat w_1 ja w_2 ovat ekvivalentteja, jos ne ovat samat tai saadaan toisistaan kirjoittamalla ab:n paikalle bc tai päinvastoin ja soveltamalla uudelleenkirjoitusta uudelleen niin monta kertaa kuin halutaan.

Relaation sitoma puoliryhmä tarkoittaa ekvivalenssiluokkien joukkoa, ja ekvivalenssiluokkia esitetään luonnollisestikin edustajan avulla, eikä niiden esityksissä ylensä käytetä hakasulkumerkintää $[w]$. Tällöin esimerkiksi puoliryhmässä $\langle \Sigma \mid ab = bc \rangle$ on voimassa $\underline{ab}bccab = bcbcc\underline{ab} = bc\underline{bc}cbc = bcabcbc$.

Huomautus 18. Vapaita puoliryhmiä käytetään mm. merkkijonojen mallintamiseen ja siksi näillä on erityisen suuri merkitys teoreettisessa tietojenkäsittelyopissa. Puoliryhmien teorian tutkimus on viimeistään 1950-luvulta lähtien ollut merkittävä osa diskreettiä matematiikkaa.

Ei-vapaiden puoliryhmien teorian puitteissa voidaan myös esittää elementaarinen laskennan malli, ns. Turingin kone.

2.4 Monoidi

Määritelmä 27. Puoliryhmän A alkio ε on *neutraalialkio* eli *identiteettialkio* eli *ykkösalkio*, jos $\varepsilon * w = w * \varepsilon$ kaikille $w \in A$.

Huomautus 19. Puoliryhmän neutraalialkiosta käytetään myös merkintää 1 tai λ, ja sitä kutsutaan *tyhjäksi sanaksi*.

Määritelmä 28. *Monoidi* on puoliryhmä, jossa on neutraalialkio.

Huomautus 20. Mikä hyvänsä puolirymä voidaan täydentää monoidiksi yksinkertaisesti lisäämällä ykkösalkio 1.

Määritelmä 29 (Vapaa monoidi). Jos $\Sigma = \{a_1, \ldots, a_n\}$ on äärellinen joukko, merkitään $\Sigma^0 = \{1\}$ (tyhjä sana) ja

$$\Sigma^* = \{1\} \cup \Sigma^+ = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \ldots.$$

Σ^* on ns. *vapaa monoidi*. Joukot Σ^+ ja Σ^* eroavat siis toisistaan ainoastaan siinä, että Σ^* sisältää tyhjän sanan, mutta Σ^* ei. Algebrallinen eroavaisuus on se, että Σ^* on neutraalialkion sisältävä 1 monoidi, kun taas puoliryhmässä Σ^+ ei neutraalialkiota ole.

2.5 Ryhmä

Määritelmä 30. Olkoon A monoidi, jonka ykkösalkiota merkitään symbolilla on 1. Alkio y on x:n *käänteisalkio*, jos $x * y = y * x = 1$ ja tällöin merkitään $y = x^{-1}$.

Määritelmä 31. Ryhmä (group) on monoidi, jossa jokaisella alkiolla on käänteisalkio.

Huomautus 21. Monoidin määritelmään perustuen edellinen määritelmä voidaan purkaa auki seuraavalla tavalla:

Ryhmä on algebrallinen rakenne, johon kuuluu joukko G ja yksi binäärinen joukossa G määritelty operaatio $*$ joka toteuttaa seuraavat aksioomat:

1. $(\forall x,y,z \in G)\ ((x*y)*z = x*(y*z))$ (assosiatiivisuus)
2. $(\exists 1 \in G)(\forall x \in G)\ (x*1 = 1*x = x)$ (neutraalialkion olemassaolo)
3. $(\forall x \in G)(\exists y \in G)\ (x*y = y*x = 1)$ (käänteisalkion olemassaolo)

Huomautus 22. Jokainen puoliryhmä voidaan täydentää monoidiksi lisäämällä neutraalialkio. Joissakin tapauksissa monoidi voidaan täydentää ryhmäksi lisäämällä jokaiselle alkiolle x käänteisalkio x^{-1}.

Voidaan kuitenkin huomata, että jos ryhmässä toteutuu yhtälö $xy = xz$, saadaan tästä x:n käänteisalkiolla x^{-1} vasemmalta kertomalla yhtälö $x^{-1}(xy) = x^{-1}(xz)$, josta seuraa $(x^{-1}x)y = (x^{-1}x)z$ ja tästä edelleen $y = z$. Näin ollen ryhmissä pätee aina ns. *vasenmmanpuoleinen supistuvuus* [1] $xy = xz \Rightarrow y = z$. Samoin voidaan todeta, että ryhmissä pätee niinikään *oikeanpuoleinen supistuvuus* $xy = zy \Rightarrow x = y$

Oikea tai vasen supistuvuus ei kuitenkaan ole kaikille monoideille voimassa, eikä tällaisia monoideja voida täydentää ryhmiksi. Monoideja, joille pätee sekä oikean- että vasemmanpuoleinen supistuvuus, sanotaan *supistuviksi monoideiksi* (cancellative monoids). Mikäli ainoastaan toinen, esimerkiksi oikeanpuoleinen supistuvuus on voimassa, sanotaan, että monoidi on *oikealta supistuva*.

Esimerkki 32. Vapaat monoidit ovat supistuvia. Jos nimittäin $xy = xz$ joillekin merkkijonoille x, y ja $z \in \Sigma^*$, niin tällöin merkkijonoilla xy ja xz on sama ensimmäinen kirjain. Poistamalla ensimmäiset kirjaimet molemmista jonoista saadaan yhtäsuuruus $x_1 y = x_1 z$, ja samoin jatkamalla lopulta $y = z$.

Esimerkki 33. Olkoon $\Sigma = \{a,b\}$. Vapaa monoidi Σ^* voidaan täydentää ryhmäksi seuraavalla tavalla: Merkitään $\Sigma^{-1} = \{a^{-1}, b^{-1}\}$ ja määritellään joukon $\Sigma \cup \Sigma^{-1} = \{a,b,a^{-1},b^{-1}\}$ yli puoliryhmä relaatioilla $aa^{-1} = a^{-1}a = bb^{-1} = b^{-1}b = 1$.

Aiemmin mainittiin, että puoliryhmien (ja monoidien) teorialla on erityisen suuri merkitys teoreettisessa tietojenkäsittelyssä esimerkkinä merkkijonojen matemaattisena mallina (vapaa puoliryhmä tai monoidi). Mikäli vapaaseen monoidiin määritellään sopivia relaatioita (kts. Esimerkki 17), voidaan saadulla ei-vapaalla monoidilla mallintaa yksinkertaista mutta yleispätevää laskennan mallia, ns. Turingin konetta.

Ryhmäteorialla sen sijaan huomattava merkitys erityisesti fysiikassa; ryhmäteoriaa voidaan nimittäin pitää matemaattisena symmetrian mallina ja erityisen tärkeinä voidaan pitää erilaisia *matriisiryhmiä*, joita käsitellään kurssikokonaisuuden lineaarialgebran osiossa. Ryhmäteorialla on lukuisa määrä sovelluksia erityisesti kvanttifysiikassa, mutta myös perinteisessa mekaniikassa.

Huomautus 23. Samoin kuin puoliryhmien ja monoidien kohdalla, myös ryhmäteoriassa jätetään usein operaatiosymboli $*$ kirjoittamatta ja merkitään $x*y$:n sijasta xy. Näin tehdään erityisesti mikäli ryhmä ei ole kommutatiivinen.

Määritelmä 32. Jos Määritelmän 31 lisäksi pätee $x*y = y*x$ kaikilla x, $y \in G$, sanotaan että G on *kommutatiivinen ryhmä* eli *Abelin ryhmä*.

Huomautus 24. Kommutatiivisissa ryhmissä operaatiosta käytetään usen merkintää $+$, identiteettialkiosta merkintää 0 ja alkion x käänteisalkiosta merkintää $-x$ sekä nimitystä *vasta-alkio*.

Huomautus 25. Kommutatiivisissa ryhmissä, joissa ryhmäoperaatiota merkitään symbolilla $+$, saa supistuvuus muodot $x+y = x+z \Rightarrow y = z$ ja $x+y = z+y \Rightarrow x = z$.

Esimerkki 34. $\mathbb{Z}$ on kommutatiivinen eli Abelin ryhmä, kun ryhmäoperaatioksi valitaan tavallinen yhteenlasku $+$, neutraalialkioksi 0 ja luvun a vasta-alkioksi vastaluku $-a$. Seuraavat ehdot pätevät joukossa $\mathbb{Z}$.

1. $(a+b)+c = a+(b+c)$ (assosiatiivisuus)

[1] Left cancellation property, ei pidä sekoittaa murtolukujen supistamiseen.

2. $a+0=0+a=a$ (neutraalialkio eli nolla-alkio)
3. $a+(-a)=-a+a=0$ (vasta-alkio)
4. $a+b=b+a$ (kommutatiivisuus)

Esimerkki 35. $\mathbb{Q}\setminus\{0\}$ on kommutatiivinen ryhmä, kun ryhmäoperaatioksi valitaan tavallinen kertolasku $\cdot$, neutraalialkioksi 1, ja käänteisalkioksi käänteisluku a^{-1}. Seuraavat ehdot pätevät joukossa $\mathbb{Q}$.

1. $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ (assosiatiivisuus)
2. $a\cdot 1=1\cdot a=a$ (neutraalialkio eli ykkösalkio)
3. $a\cdot a^{-1}=a^{-1}\cdot a=1$ (käänteisalkio)
4. $a\cdot b=b\cdot a$ (kommutatiivisuus)

On syytä huomata, että esimerkkien 34 ja 35 ehdot ovat samankaltaiset, niitä erottavat ainoastaan algebrallisen operaation, neutraalialkion, sekä vasta-alkion (käänteisalkion) merkintätapa. Tästä huolimatta kommutatiivisia ryhmiä on hyvinkin monenkaltaisia eivätkä edellämainittujen ryhmien algebralliset rakenteet ole toisiaan vastaavat.

Erityisesti on syytä huomata, että ryhmän $\mathbb{Z}$ kaikki alkiot saadaan lukua 1 tai sen vasta-alkiota monistamalla, mutta ryhmässä $\mathbb{Q}$ ei ole yhtä alkiota, jota itsensä kanssa kertomalla saataisiin kaikki rationaaliluvut.

2.6 Rengas

Tähän asti esitetyt algebralliset systeemit ovat rakentuneet joukosta, jossa on määritelty vain yksi binäärinen operaatio. Toisaalta jo matematiikan varhaisvaiheessa on osoittautunut, että vähintään kaksi binääristä operaatiota, yhteen- , ja kertolasku ovat käyttökelpoisia. Siksi on perusteltua määritellä kahdella binäärisellä operaatiolla varusteltu matemaattinen rakenne, *rengas*.

Määritelmä 33. Rengas (ring) $(R,+,\cdot,0)$ on algebrallinen rakenne, jossa joukossa R on määritelty kaksi binääristä operaatiota $+$ ja $\cdot$ ja alkio 0, jotka toteuttavat seuraavat ehdot:

1. $(R,+,0)$ on kommutatiivinen ryhmä.
2. $(R,\cdot)$ on puoliryhmä.
3. $a\cdot(b+c)=a\cdot b+a\cdot c$ ja $(a+b)\cdot c=a\cdot c+b\cdot c$ (distributiivisuus)

Renkaan operaatiota $+$ kutsutaan tyypillisesti yhteenlaskuksi ja operaatiota $\cdot$ kertolaskuksi.

On huomattava, että renkaan $+$-operaation (yhteenlaskun) vaaditaan olevan aina kommutatiivinen, mutta $\cdot$-operaatiolle (kertolaskulle) tätä vaatimusta ei esitetä. Jos kuitenkin rengas on myös kertolaskun suhteen kommutatiivinen, sanotaan että kyseessä on *kommutatiivinen* rengas.

Huomautus 26. Jokaisessa renkaassa pitää olla neutraalialkio yhteenlaskun $+$ suhteen (ns. nolla-alkio) ja niinikään vasta-alkio yhteenlaskun suhteen.

Kirjallisuudessa esiintyy hyvin yleisesti myös sellainen renkaan määritelmä, jossa vaaditaan, että rengas on kertolaskun $\cdot$ suhteen monoidi, mikä siis tarkoittaa sitä että on olemassa neutraalialkio 1 myös operaation $\cdot$ suhteen (ns. ykkösalkio).

Tällä kurssilla ei kuitenkaan vaadita renkaan ykkösalkion olemassaoloa, mutta mikäli renkaassa on ykkösalkio, voidaan tätä korostaa sanomalla, että kyseessä on *ykkösalkiolla varustettu rengas* (ring with identity).

Esimerkki 36. $(\mathbb{Z},+,\cdot,0)$ on kommutatiivinen ykkösalkiolla varustettu rengas, koska

1. $(\mathbb{Z},+,0)$ on kommutatiivinen ryhmä.
2. $(\mathbb{Z},\cdot)$ on kommutatiivinen puoliryhmä ($(\mathbb{Z},\cdot,1)$ jopa monoidi).

Esimerkki 37. Parillisten kokonaislukujen joukko $2\mathbb{Z}=\{\ldots,-4,-2,0,2,4,\ldots\}$ muodostaa niinikään kommutatiivisen renkaan tavallisen yhteen- ja kertolaskun suhteen. Tätä varten pitää varmistaa että joukko $2\mathbb{Z}$ on suljettu yhteen- ja kertolaskun suhteen, siis että $x+y$, x, $y\in 2\mathbb{Z}$ aina kun x, $y\in 2\mathbb{Z}$ (ei kovin hankalaa). Tässä renkaassa ei kuitenkaan ole ykkösalkiota.

Esimerkki 38. Liitetään reaalilukujen joukkoon alkio $\{-\infty\}$ ja sovitaan, että $-\infty < x$ ja että $-\infty + x = -\infty$ aina kun $x \in \mathbb{R}$. Totea, että joukosta $\mathbb{R} \cup \{-\infty\}$ tulee tällöin ns. *puolirengas* (rengas jossa ei välttämättä ole additiivista vasta-alkioita), kun yhteenlaskuksi $\oplus$ valitaan $x \oplus y = \max\{x, y\}$ ja kertolaskuksi valitaan $x \otimes y = x + y$. Mieti miten tilanne muuttuu, jos maksimi max korvataan minimillä min.

Esimerkki 39. Jos R on jokin rengas, voidaan määritellä $R[x] = \{r_0 + r_1 x + r_2 x^2 + \ldots + r_k x^k \mid r_i \in R\}$ ja näin määriteltyä rengasta kutsutaan *polynomirenkaaksi* yli R:n. Se koostuu kaikista R-kertoimisista polynomeista, joille yhteen- ja kertolasku määritellään tavalliseen tapaan.

2.7 Kunta

Tärkeä erikoistapaus renkaasta on *kunta*.

Määritelmä 34. *Kunta (Field)* $(\mathbb{K}, +, \cdot, 0, 1)$ on ykkösalkiolla varustettu kommutatiivinen rengas, jossa jokaisella nollasta eroavalla alkiolla a on multiplikatiivinen käänteisalkio a^{-1}, joka siis toteuttaa ehdon $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Esimerkki 40. Rationaaliluvut $(\mathbb{Q}, +, \cdot, 0, 1)$ muodostavat kunnan yhteen- ja kertolaskun suhteen, samoin reaaliluvut $(\mathbb{R}, +, \cdot, 0, 1)$. Sen sijaan $(\mathbb{Z}, +, \cdot, 0, 1)$ ei ole kunta, koska nollasta eroavilla kokonaisluvuilla ei ole kertolaskun suhteen käänteisalkioita (poikkeuksena luvut 1 ja -1).

Rationaalilukujen kunta $\mathbb{Q}$ voidaan ajatella kokonaislukujen renkaan $\mathbb{Z}$ laajennukseksi, jossa jokaiselle alkiolle $x \in \mathbb{Z} \setminus \{0\}$ lisätään multiplikatiivinen käänteisalkio x^{-1}. Tämänkaltainen laajennus renkaasta kunnaksi ei aina ole kuitenkaan mahdollinen.

Aiemmin mainittiin, että jokainen puoliryhmä voidaan täydentää monoidiksi lisäämällä ykkösalkio, mutta monoidin täydentäminen ryhmäksi ei välttämättä onnistu, sillä monoidi ei välttämättä ole supistuva, kun taas ryhmä on. Monoidien supistuvuuskäsitettä kunnissa vastaa tulon nollasääntö ja sen avulla voidaan määrittää ne renkaat, jotka voidaan täydentää kunnaksi.

Luonnehdintaa varten esitetään ensin helposti todistettava ominaisuus:

Lause 14. *Jokaisessa renkaassa* $0 \cdot x = x \cdot 0 = 0$.

Todistus. Todistus on sama kuin kurssilla Matematiikan perustiedot reaaliluvuille esitetty, mutta tässä luvussa esitettyjen käsitteiden avulla se voidaan esittää lyhyemmin:

$$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0.$$

Koska rengas on yhteenlaskun suhteen ryhmä ja siksi supistuva, voidaan ylläolevasta päätellä $0 = x \cdot 0$. Analogisesti voidaan päätellä $0 \cdot x = 0$. □

Lause 15 (Tulon nollasääntö). *Jos kunnassa* $\mathbb{K}$ *on* $xy = 0$*, niin joko* $x = 0$ *tai* $y = 0$.

Todistus. Jos $x = 0$, on lause todistettu. Jos taas $x \neq 0$, on kunnan määritelmän mukaan x:llä multiplikatiivinen käänteisalkio x^{-1}, ja kertomalla yhtälö $xy = 0$ vasemmalta saadaan $x^{-1} \cdot (xy) = x^{-1} \cdot 0$, mistä puolestaan seuraa $(x^{-1}x)y = 0$ ja tästä edelleen $y = 0$. □

Koska edellisen lauseen mukaan kunnissa pätee tulon nollasääntö, on uskottavaa, että renkaita, joissa kyseinen sääntö ei päde, ei voida laajentaa kunnaksi.

Tulon nollasäännön toteutumista renkaissa luonnehditaan yleensä seuraavilla käsitteillä:

Määritelmä 35. Renkaan R alkio a on *nollanjakaja*, jos on olemassa sellainen $b \in R \setminus \{0\}$, että $a \cdot b = 0$.

Määritelmä 36. Rengas R on *kokonaisalue (integral domain)*, jos renkaassa ei ole muita nollanjakajia kuin itse nolla-alkio 0.

Esimerkki 41. Rengas $\mathbb{Z}$ on kokonaisalue, sillä yhtälöstä $ab = 0$ seuraa $a = 0$ tai $b = 0$, siis luku 0 on ainoa nollanjakaja joukossa $\mathbb{Z}$.

On mahdollista todistaa, että kokonaisalueet voidaan laajentaa kunniksi, mutta muita renkaita ei välttämättä voi.

Esimerkki 42. Esimerkin 19 kuuden alkion algebrallinen rakenne on kommutatiivinen ykkösalkiolla varustettu rengas, mutta ei kokonaisalue, sillä $\overline{2} \cdot \overline{3} = \overline{0}$. Näin ollen tätä joukkoa ei voi laajentaa kunnaksi.

2.8 Vektoriavaruus, Algebra

Insinöörimatematiikan kurssikokonaisuuden kannalta on syytä mainita vielä *vektoriavaruudeksi kutsuttu* algebrallinen rakenne, jota tullaan tarkastelemaan yksityiskohtaisemmin kurssin loppuosassa.

Määritelmä 37. *Vektoriavaruus* on algebrallinen rakenne, jossa alkiojoukko koostuu kahdesta osasta: skalaarikunnasta $\mathbb{K}$ ja avaruudesta V, sekä operaatiosta $K \times V \to V$ (skalaarikertolasku) jotka toteuttavat alla olevat aksioomat (merkitään skalaarikertolaskua ilman kertomerkkiä: $a\mathbf{v}$ ja sovitaan, että $\mathbf{v}a = a\mathbf{v}$).

- $(V, +, \mathbf{0})$ on kommutatiivinen ryhmä
- $1\mathbf{v} = \mathbf{v}$
- $a(\mathbf{v} + \mathbf{w}) = a\mathbf{v} + a\mathbf{w}$
- $(a+b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$
- $a(b\mathbf{v}) = (ab)\mathbf{v}$

Määritelmä 38. Vektoriavaruuden skalaarikunnan alkioita kutsutaan *skalaareiksi* ja avaruuden V alkioita *vektoreiksi*.

Mikäli vektoriavaruudessa on vielä vektoreiden joukossa määritelty tietyt ehdot täyttävä algebrallinen operaatio, sanotaan vektoriavaruutta *algebraksi*.

Määritelmä 39. Kunnan $\mathbb{K}$ yli määritelty *algebra* V on vektoriavaruus, jossa muiden rakenteiden lisäksi vektoreille on määritelty kertolasku $\cdot\, V \times V \to V$, joka on *bilineaarinen*, siis toteuttaa ehdot

- $(a\mathbf{u} + b\mathbf{v}) \cdot \mathbf{w} = a \cdot \mathbf{u} \cdot \mathbf{w} + b \cdot \mathbf{u} \cdot \mathbf{w}$
- $\mathbf{u} \cdot (a\mathbf{v} + b\mathbf{w}) = a \cdot \mathbf{u} \cdot \mathbf{v} + b \cdot \mathbf{u} \cdot \mathbf{w}$
- $a\mathbf{u} \cdot b\mathbf{v} = ab \cdot \mathbf{u} \cdot \mathbf{v}$

Esimerkki 43. $\mathbb{R}^3$:sta tulee vektoriavaruus, kun määritellään vektoreiden $V = \mathbb{R}^3$, $\mathbb{K} = \mathbb{R}$ ja vektoreiden yhteenlasku määritellään ehdolla $(x_1, x_2, x_3) + (y_1, y_2, y_3) = (x_1 + y_1, x_2 + y_2, x_3 + y_3)$ ja skalaarikertolasku ehdolla $a(x, y, z) = (ax, ay, az)$.

2.9 Karteesinen tulo

Toisinaan on tarpeellista luoda uusi algerallinen rakenne olemassaolevien varaan, ja tällaisesta menettelytavasta yksi esimerkki on karteesinen tulo, jossa jokaista koordinaattia kohti sovelletaan samaa operaatiota.

Esimerkki 44. Tapauksessa $A = B = \mathbb{R}$, voidaan määritellä yhteenlasku joukossa $\mathbb{R}^2$ ehdolla $(a,b) + (c,d) = (a+c, b+d)$. Tämänkaltainen yhteenlasku yhdessä sopivasti määritellyn skalaarikertolaskun kanssa tuottaa vektoriavaruuden $\mathbb{R}^2$.

Toisinaan karteesisen tulon määrittämässä systeemissä voi olla ”liikaa” alkioita. Tälllöin on toisinaan mahdollista samaistaa alkioita käyttämällä ekvivalenssirelaatiota.

Esimerkki 45. Olkoon $(R, +, \cdot, 0, 1)$ kommutatiivinen kokonaisalue ja määritellään joukossa $R \times (R \setminus \{0\})$ kertolasku ja yhteenlasku seuraavasti: $(a,b) \cdot (c,d) = (ac, bd)$ ja $(a,b) + (c,d) = (ad + bc, bd)$.

Määritellään ekvivalenssi joukossa $R \times (R \setminus \{0\})$ ehdolla $(a,b) \equiv (c,d) \leftrightarrow ad = bc$.

Näin määritelty ekvivalenssi on kongruenssi joukossa $R \times (R \setminus \{0\})$ ja ekvivalenssiluokat määrittävät ns. *osamääräkunnan*.

2.10 Tekijäsysteemi

Sovellusten kannalta hyödyllisten algebrallisten rakenteiden luomiseksi yksi hyvin käyttökelpoinen menetelmä on turvautua ns. tekijärakenteeseen, jota voidaan kuvailla siten, että laajemman algebrallisen rakenteen alkioita samaistetaan yhdeksi joukoksi, ja joukkojen joukosta muodostetaan uusi algebrallinen rakenne.

Tämänkaltaseen menettelyyn on olemassa systemaattinen menetelmä, jota pohjustaaa seuraava määritelmä:

Määritelmä 40. Olkoon $\equiv$ ekvivalessirelaatio joukossa A. Joukossa A määritelty algebrallinen operaatio $*$ on yhteensopiva relaation $\equiv$ kanssa, mikäli $a \equiv c \wedge b \equiv d \to a * b \equiv c * d$.

Jos kaikki algebrallisen rakenteen operaatiot ovat yhteensopivia ekvivalenssirelaation $\equiv$ kanssa, sanotaan että relaatio $\equiv$ on *kongruenssi*.

Esimerkki 46. Lukuteoreettinen kongruenssi (kts. Määritelmä 14) on kongruenssirelaatio, sillä jos $a \equiv_n b \wedge c \equiv_n d$, niin $a + c \equiv_n c + d$ ja $ac \equiv_n cd$.

Kongruenssin määritelmä vaikuttaa lähtökohtaisesti melko vaativalta: Kongruenssin pitää olla lähtökohtaisesti ekvivalenssirelaatio, mutta sen lisäksi yhteensopiva algebrallisten operaatioiden suhteen. Näin ollen ei ole mitenkään itsestään selvää, että kongruensseja olisi helppo löytää. Osoittautuu kuitenkin, että algebrallisen rakenteen alirakenne määrittelee kongruenssin tietyillä ehdoilla.

Määritelmä 41. Ryhmä $H \subseteq G$ on G:n *aliryhmä*, jos $a, b \in H \to ab \in G$, ja $a^{-1} \in G$.

Aliryhmä on siis ryhmän osajoukko, joka on suljettu ryhmäoperaatioiden suhteen (ryhmä ryhmän sisällä)

Määritelmä 42. Aliryhmä $H \subseteq G$ on *normaali*, jos $(\forall g \in G)$

$$gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = Hg.$$

Aliryhmän normaalius merkitsee sitä, että $(\forall g \in G)(\forall h \in H)(\exists h_1 \in H)\ (gh = h_1 g)$.

Huomaaa, että kommutatiivisessa ryhmässä jokainen aliryhmä on normaali.

Ryhmien teoriassa kytkös alisysteemien ja kongruenssien välillä esitetään seuraavassa lauseessa:

Lause 16. *Jos H on G:n normaali aliryhmä, niin ehdolla $a \equiv b \Leftrightarrow ab^{-1} \in H$ määritelty relaatio $\equiv$ on kongruenssi ryhmässä G.*

Määritelmä 43. Olkoon G ryhmä ja $H \subseteq G$ normaali aliryhmä.

Kongruenssin $a \equiv b \Leftrightarrow ab^{-1} \in H$ ekvivalenssiluokat muodostavat ryhmän, kun määritellään $[a] \cdot [b] = [a \cdot b]$ ja $[a]^{-1} = [a^{-1}]$. Tätä ryhmää sanotaan *tekijäryhmäksi* ja merkitään G/H.

Tässä tapauksessa merkitään usein myös $[a] = aH$. Tämän merkinnän mukaisesti $aH \cdot bH = a \cdot bH$.

Näitä merkintöjä voidaan hyvinkin verrata esimerkin 19 merkintään, jossa esim. $[2]$ esitti joukkoa $2 + 6\mathbb{Z}$ ja $[5]$ joukkoa $5 + 6\mathbb{Z}$. Näiden summaa esittää luokka $[2] + [5] = [2 + 5] = [7] = [1]$, mikä voidaan yhtä hyvin merkitä muodossa

$$(2 + 6\mathbb{Z}) + (5 + 6\mathbb{Z}) = 7 + 6\mathbb{Z} = 1 + 6\mathbb{Z}.$$

Myös kahden algebrallisen operaation rakenteessa voidaan kongruensseja löytää alirakenteista. Tätä varten otetaan käyttöön seuraavat määritelmät.

Määritelmä 44. $S \subseteq R$ on renkaan R *alirengas*, jos $a, b \in S \to a + b$, ab, $-a \in S$.
Alirengas $I \subseteq R$ on renkaan R *ihanne* (ideal), jos ri, $ir \in I$ aina, kun $r \in R$ ja $i \in I$. Renkaan ihanne on siis alirengas joka "vetää" kertolaskulla kaikki renkaan alkiot ihanteeseen.

Kaikissa renkaissa on ainakin ihanteet $\{0\}$ ja R.

Lause 17. *Jos I on renkaan R ihanne, on ehdolla $a \equiv b \Leftrightarrow a - b \in I$ määrittyvä relaatio on kongruenssi.*

Määritelmä 45. Olkoon $I \subseteq S$ renkaan S ihanne. Kongruenssin $a \equiv b \Leftrightarrow a-b \in I$ ekvivalenssiluokat muodostavat renkaan, kun määritellään $[a]+[b] = [a+b]$, $[a]\cdot[b] = [a\cdot b]$ ja $-[a] = [-a]$. Tätä rengasta sanotaan *tekijärenkaaksi* ja merkitään R/I.

Tällöin merkitään usein myös $[a] = a+I$. Näillä merkinnöillä $(a+I)+(b+I) = (a+b)+I$ sekä $(a+I)(b+I) = ab+I$.

Esimerkki 47. Olkoon $n \in \mathbb{N}$. Tällöin $n\mathbb{Z} = \{n \cdot m \mid m \in \mathbb{Z}\}$ on renkaan $\mathbb{Z}$ ihanne. Se muodostuu kokonaisluvuista, jotka ovat jaollisia luvulla n.

Ihanne $I = n\mathbb{Z}$ määrittää edellämainitun mukaan ekvivalenssirelaation $a \equiv b \Leftrightarrow a - b \in I$, mikä tarkoittaa sitä, että $a - b = nk$ jollekin $k \in \mathbb{Z}$. $a - b = nk$ puolestaan tarkoittaa sitä, että $n \mid a - b$, mistä seuraa edelleen, että $n \mid b - a$. Kyseessä on siis lukuteoreettinen kongruenssi.

Määritelmä 46. Renkaan R ihanne $I \subsetneq R$ on *maksimaalinen*, jos ei ole suurempaa ihannetta $J \subsetneq R$ johon I sisältyy aidosti, siis $I \subsetneq J$.

Lause 18. *Jokaisessa renkaassa on ainakin yksi maksimaalinen ihanne*

Lause 19. *Jos R on multiplikatiivisen ykkösalkion sisältävä kommutatiivinen rengas, on tekijärengas R/I on kunta tarkalleen silloin kuin I on maksimaalinen ihanne.*

Esimerkki 48. Renkaan $\mathbb{Z}$ ihanne $6\mathbb{Z}$ ei ole maksimaalinen, koska se sisältyy suurempiin ihanteisiin $2\mathbb{Z}$ ja $3\mathbb{Z}$. Tämän vuoksi $\mathbb{Z}/6\mathbb{Z}$ ei ole kunta. Sen sijaan ihanteet $2\mathbb{Z}$ ja $3\mathbb{Z}$ ovat maksimaalisia, samoin kuin samoin kuin $5\mathbb{Z}$.

Esimerkki 49. Näytetään toteen, että x^2+x+1 on jaoton polynomi yli kahden alkion kunnan $\mathbb{F}_2$, jolloin polynomirenkaan ihanne $I\langle x^2+x+1\rangle = \{p(x)(x^2+x+1) \mid p(x) \in \mathbb{F}_2[x]\}$ on maksimaalinen ja rakennetaan neljän alkion kunta $\mathbb{F}_4$.

Esimerkki 50. Esimerkin merkintä $\mathbb{R}[x]$ tarkoittaa kaikkien reaalikertoimisten polynomien joukkoa (kts. Esimerkki 39) Tässä renkaassa voidaan määritellä polynomin x^2+1 generoima ihanne $I = \langle x^2+1\rangle$. Tällöin esim. $(x+I)(x+I) = -1+I$, miksi?

Luku 3
Rekursio ja induktio

Käsitteissä rekursio ja induktio on samankaltaisia piirteitä, mutta matematiikassa ne eivät ole toistensa synonyymejä. Rekursio tarkoittaa järjestettyjen matemaattisten objektien määrittelemistä siten, että pienimmät (ns. rekursion pohja) määritellään erikseen, esimerkiksi luettelemalla, ja pohjaa suuremmat määritellään pienempien, siis jo aiemmmin määriteltyjen objektien perusteella.

Matemaattinen induktio puolestaan on menetelmä, jolla voidaan todistaa väittämiä oikeaksi rekursiivisesti määritellyille objekteille. Nimestään huolimatta matemaattinen induktio ei ole tieteenfilosofian kannalta induktiivista päättelyä vaan yksi deduktion muoto.

3.1 Rekursio

Esimerkki 51. Kun $n \in \mathbb{N}_0 = \{0,1,2,\ldots\}$, voidaan kertomafunktio $n!$ määritellä rekursiivisesti määrittelemällä ensin $0! = 1$ (rekursion pohja) ja tämän jälkeen $(n+1)! = (n+1) \cdot n!$.

Huomautus 27. Edellinen määritelmä kattaa kaikki joukon $\mathbb{N}_0$ alkiot, koska $0!$ on määritelty, ja $(n+1)! = (n+1)\cdot!$ tulee määritellyksi rekursiivisesti pienemmän arvon $n!$ perusteella.

Tämä toteama että $n!$ on määritelty kaikille joukon $\mathbb{N}_0$ alkiolle, on puolestaan luonteeltaan rekursiivinen ja perustuu siihen, että joukko $\mathbb{N}_0$ voidaan itsessään määritellä joukkona, jossa on pienin alkio 0, ja muut saadaan tästä rekursiivisesti *seuraajafunktiolla*: $s(0)$, $s(s(0))$, $s(s(s(0)))$, ... Jotta näin saataisiin aikaan $\mathbb{N}_0$, pitää seuraajafunktiolle asettaa tiettyjä ehtoja (kts. Matematiikan perustiedot).

Huomautus 28. Kertomafunktion määritelmästä seuraa suoraan, että $n! = n \cdot (n-1)! = n \cdot (n-1) \cdot (n-2)! = \ldots = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$, joten kertomafunktio voitaisiin määritellä myös $0! = 1$ ja

$$n! = \prod_{i=1}^{n} i, \tag{3.1}$$

mutta määritelmä (3.1) ei ole rekursiivinen. Kertoma $n!$ ilmaisee niiden jonojen määrän, jotka voidaan muodostaa luvuista $\{1,2,\ldots,n\}$ valitsemalla yksi luku vain kerran.

Huomautus 29. Kertomafunktion rekursiivisessa määritelmässä suurempi arvo $(n+1)!$ määritellään vain yhden pienemmän arvon $n!$ perusteella, mutta näin ei välttämättä tarvitse olla.

Esimerkki 52. Fibonaccin luvut määritellään ehdoilla $F_0 = 0$, $F_1 = 1$ (rekursion pohja) ja $F_{n+2} = F_{n+1} + F_n$, kun $n > 0$. Näin ollen siis $F_2 = F_1 + F_0 = 1 + 0 = 1$, $F_3 = F_2 + F_1 = 1 + 1 = 2$, $F_4 = F_2 + F_1 = 2 + 1 = 3$, $F_5 = F_4 + F_3 = 3 + 2 = 5$, $F_6 = F_5 + F_4 = 5 + 3 = 8$, jne.

Huomautus 30. Edellisten esimerkkien rekursiossa suuremmuus määriteltiin joukon $\mathbb{N}_0$ perusteella. Joukko $\mathbb{N}_0$ on määriteltävissä hyvin yksinkertaisella rekursiolla, jossa kukin suurempi alkio $s(n)$ määritellään ainoastaan yhden pienemmän alkion n perusteella. Näin ei kuitenkaan tarvitse aina olla, vaan järjestysrelaatio voi olla myös monimutkaisempi.

Seuraavissa esimerkeissä määritellään ns. *propositiologiikan* alkeiskäsitteet. Propositiologiikkaa voidaan paitsi käyttää mallintamaan yksinkertaisia kyllä/ei -väitelauseita sekä niiden yhdistelmiä, myös loogisia piirejä, jotka koostuvat yksinkertaisista AND, OR, ja NOT-porteista. Klassista informaatiota käsittelevien tietokoneiden toimintaa voidaan kuvailla hyvinkin monilla eri tasoilla, mutta

siirryttäessä fysikaalisesta esitystasosta loogiseen yleensä ensimmäiseksi valitaan nimenomaan loogiset portit ja niiden suorittamat operaatiot.

Kehityshistoriaan liittyen on syytä kuitenkin mainita, että mainitut loogiset operaatiot ja niiden ominaisuudet olivat tunnettuja jo huomattavasti ennen ensimmäisten puolijohdepiirien valmistamista, ja fysikaalisen toteutusmuodon kehitystä ohjasi tarve toteuttaa tunnettuja loogisia operaatioita.

Määritelmä 47. Propositiologiikan aakkosto koostuu

1. Numeroituvasti äärettömästä joukosta *propositiomuuttujia* $x_1, x_2, x_3, \ldots$
2. *Loogisista konnektiiveista* $\wedge, \vee, \neg$
3. Sulkumerkeistä (ja).

Ylläamainitun aakkoston perusteella voidaan kirjoittaa monenlaisia merkkijonoja, esimerkiksi $x_1)\neg x_3)x_5 \vee ($. Propositiologiikan kaavat eli *propositiot* ovat yllämainitun aakkoston avulla kirjoitettuja merkkijonoja, mutta eivät mielivaltaisia, vaan niiden muodostamiseksi on tarkka sääntö, jonka ilmaisee seuraava määritelmä

Määritelmä 48. Propositiologiikan hyvinmuodostetut kaavat (propositiot) määritellään seuraavasti

- Propositiomuuttujat $x_1, x_2, x_3, \ldots$ ovat kaavoja.
- Jos φ ja ψ ovat kaavoja, niin myös $(\neg\varphi)$, $(\varphi \wedge \psi)$ ja $(\varphi \vee \psi)$ ovat kaavoja.
- Ylläolevat ehdot määrittelevät kaikki propositiologiikan kaavat.

Esimerkki 53. Ylläolevan määritelmän mukaan propositiologiikan kaavoja ovat esimerkiksi x_1, x_2, x_3, $(x_1 \wedge x_2)$ $(\neg x_3)$, $((x_1 \wedge x_2) \vee (\neg x_3))$, $(x_1 \wedge (\neg x_4))$ ja $(((x_1 \wedge x_2) \vee (\neg x_3)) \wedge (x_1 \vee (\neg x_4)))$.

Huomautus 31. Ylläolevaa määritelmää voidaan verrata luonnollisten lukujen aksiomaattiseen määrittelyyn (kts. Matematiikan perustiedot), jossa rekursiivisen rakenteen pohjan muodosti yksi ainoa alkio 1, mutta tässä äärettömän monta propositiomuuttujaa $x_1, x_2, x_3, \ldots$.

Toinen analoginen seikka on uusien alkioiden muodostus edellisten avulla. Luonnollisten lukujen rakenteessa oli tosin ainoastaan seuraajafunktio $s(n)$, jolla saadaan uusi luku kun n tunnetaan. Propositiologiikassa sen sijaan on peräti kolme mahdollisuutta $\neg$, $\wedge$ ja $\vee$ muodostaa aiemmista kaavoista uusia.

Kolmas analoginen piirre on viimeisin ehto, jonka mukaan muita kaavoja kuin edellämainituilla ehdoilla saatavia ei ole. Tämä vastaa luonnollisten lukujen ns. induktioaksioomaa, jonka mukaan kaikki luonnolliset luvut saadaan, kun lähdetään liikkeelle luvusta 1 ja otetaan mukaiseen jokaisen luvun seuraaja.

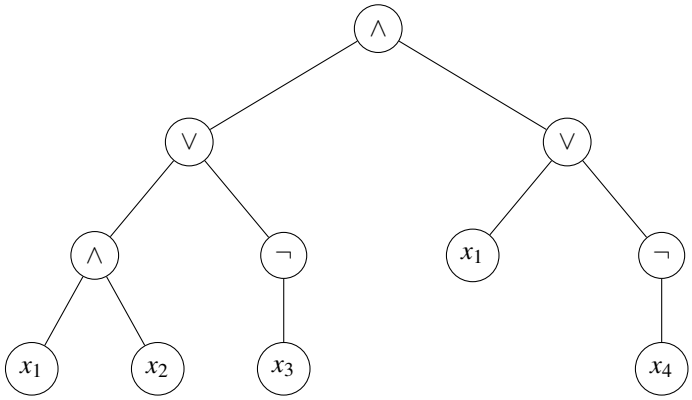
Puurakenne esittää propositiologiikan kaavan muodostamistapaa. Esimerkiksi alhaalla vasemmalla lehtinä olevat propositiomuuttujat x_1 ja x_2 liitetään toisiinsa $\wedge$-konnektiivilla, jolloin saadaan osakaava $(x_1 \wedge x_2)$. Samoin kolmanneksi vasemmalta oleva propositiomuuttuja x_3 saa eteensä konnektiivin $\neg$, jolloin saadaan osakaava $\neg x_3$, ja puurakenteessa ylöspäin siirryttäessä seuraavaksi huomataa, että edelliset osarakenteet liitetään toisiinsa konnektiivilla $\vee$, jolloin saadaan osakaava $((x_1 \wedge x_2) \vee (\neg x_3))$, jne.

Huomautus 32. Propositiologiikan kaavojen esitysasua yksinkertaistetaan yleensä sopimuksilla, joiten avulla voidaan vähentää sulkeita tulkinnan (esitetään myöhemmin) kärsimättä. Esimerkiksi sovitaan, että $(\neg x_1) \vee x_2$ voidaan kirjoittaa muodossa $\neg x_1 \vee x_2$ eikä sitä pidä sekoittaa merkintään $\neg(x_1 \vee x_2)$. Tällöin sanotaan, että on sovittu konnektiivin $\neg$ *sitovan vahvemmin* kuin konnektiivin $\vee$.

Huomautus 33. Edellämainitun kaltaisia sopimuksia operaatiomerkintöjen sitovuudesta esiintyy paljonkin perinteisessä matematiikassa: On esimerkiksi sovittu, että $a \cdot b + c$ tarkoittaa kaavaa $(a \cdot b) + c$, eikä kaavaa $a \cdot (b + c)$.

Esimerkki 54. Sopimalla sulkeiden poistoista johdonmukaisesti voidaan $(((x_1 \wedge x_2) \vee (\neg x_3)) \wedge (x_1 \vee (\neg x_4)))$ kirjoittaa muodossa $((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$.

Huomautus 34. Ylläolevan esimerkin propositio $(((x_1 \wedge x_2) \vee (\neg x_3)) \wedge (x_1 \vee (\neg x_4)))$ voidaan esittää seuraavanlaisen, ns. puurakenteen avulla. Rekursion pohjina toimivia propositiomuuttujia kutsutaan tässä esitystavassa *lehdiksi* ja ylinnä esiintyvää konnektiivia *juureksi*.



Huomautus 35. Ylläolevan puurakenteen tulkinta tulee ilmeisemmäksi myöhemmin kun perehdytään propositiologiikan syntaksin sijasta semantiikkaan. Tässä yhteydessä on kuitenkin jo huomattava, että propositiologiikan rekursiivisesti määritellyn syntaksin vuoksi kaikki propositiologiikan kaavat voidaan tietysti esittää yllä olevan puukaavion muodossa.

3.2 Induktio

Yksi tapa todistaa matemaattinen väittämä oikeaksi äärettömän monen tapauksen kohdalla on ns. *matemaattinen induktio*, joka nimestään huolimatta ei ole induktiivista päättelyä, vaan yksi deduktion alalaji. Matemaattisessa induktiossa väitämä todistetaan rekursiivisesti määritellyille objekteille todistamalla se ensin oikeaksi rekursion pohjan muodostaville alkiolle ja sen jälkeen osoittamalla, että rekursion soveltaminen säilyttää väittämän totuusarvon.

Matemaattinen induktio rinnastetaan usein *täydelliseen induktioon*, jossa käydään läpi kaikki tarkasteltavan joukon yksittäistapaukset. Täydellinen induktio ja matemaattinen induktio eivät kuitenkaan ole tieteenfilosofian kannalta sama käsite, mutta tästä huolimatta ne toisinaan samaistetaan ja varsinkin matematiikan kirjallisuudessa termit sekaantuvat usein. Nimestään huolimatta matemaattinen induktio ei ole induktiivista vaan deduktiivista päättelyä.

Luonnollisten lukujen joukko on yksinkertaisin ääretön rekursiivinen rakenne: Luku 1 toimii rekursion pohjana, ja luvun n seuraaja $s(n)$ saadaan lisäämällä 1, siis $s(n) = n+1$. Soveltamalla seuraajafunktiota lukuun 1 rekursiivisesti saadaan jono 1, $2 = s(1)$, $3 = s(2) = s(s(1))$, ... Luonnollisten lukujen induktioaksiooman (kts. Matematiikan perustiedot) perusteella näin muodostettu jono sisältää kaikki luonnolliset luvut, joten induktioperiaate luonnollisille luvuille (tai samankaltaiselle rekursiiviselle rakenteelle) toimii seuraavan lauseen mukaisella tavalla.

Seuraavassa lausessa P viittaa johonkin ominaisuuteen joka voi olla luonnollisilla luvuilla, ja sanotaan, että $P(n)$ on tosi, mikäli luvulla n on ominaisuus P.

Lause 20 (Induktioperiaate joukossa $\mathbb{N}$). *Jos voidaan näyttää toteen että*

- $P(1)$ *on tosi*
- $(\forall n)(P(n) \to P(n+1))$ *on tosi,*

niin ominaisuus $P(n)$ on tosi kaikilla $n \in \mathbb{N}$.

Sanallisesti ilmaistuna edellinen lause sanoo, että jos jokin ominaisuus P pätee luonnolliselle luvulle 1 (rekursion pohja), sekä jokaiselle luonnolliselle luvulle n on voimassa se, että $P(n)$ implikoi

$P(n+1)$:n. Toisin sanoen, ominaisuus P periytyy luvulta n tästä rekursiolla saatavalle luvulle $n+1 = s(n)$. Mikäli näin tapahtuu, niin silloin ominaisuus P on tosi jokaiselle luonnolliselle luvulle.

Luonnollisia lukuja koskevaa induktioperiaatetta voidaan kuvata myös dominopalikoiden avulla: ajatellaan, että dominopalikat on numeroitu luonnollisten lukujen mukaan 1, 2, 3, ... (ääretön määrä palikoita!) ja että seuraava väittämä pätee: palikan n kaatuessa kaatuu myös seuraava palikka $n+1$. Mitä tällöin tapahtuu, jos palikka 1 kaatuu? silloin kaatuu myös palikka $1+1=2$, ja tästä seuraa, että myös palikka $2+1=3$ kaatuu, mistä jälleen seuraa, että palikka $3+1=4$ kaatuu, jne. Johtopäätöksenä on, että *kaikki palikat* (ääretön määrä) 1:sta eteenpäin umeroituvasti kaatuvat. Juuri tämä on luonnollisia lukuja koskevan induktioperiaatteen takana piilevä intuitio.

Väite $(\forall n)(P(n) \to P(n+1))$ näytetään toteen osoittamalla, että $P(n) \to P(n+1)$ pätee, kunhan lukua n ei ole sidottu mihinkään ominaisuuteen (esim. parillisuuteen, olemaan pienempi kuin 100, tms.). Tämä voidaan ilmaista myös siten, siten, että luku n on "vapaa" eikä sen suhteen siis ole tehty mitään oletuksia. Väittämä $P(n) \to P(n+1)$ puolestaan näytetään toteen ensin olettamalla $P(n)$ ja johtamalla tästä $P(n+1)$.

Edelisin merkinnöin sanotaan, että $P(1)$ on *induktion lähtökohta*, johtopäätös $(\forall n)(P(n) \to P(n+1))$ on *induktioaskel*, $P(n)$ on *induktio-oletus* ja $P(n+1)$ *induktioväite*.

Huomautus 36. Joukolla $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$ on samankaltainen rekursiivinen rakenne kuin joukolla $\mathbb{N}$, joten induktion lähtökohdaksi voitaisiin valita yhtä hyvin 0 luvun 1 sijaan. Tämä ajatus voidaan yleistää ja valita itse asiassa mikä tahansa kokonaisluku $k \in \mathbb{Z}$ induktion lähtökohdaksi, jolloin lause 20 seuraavaan muotoon:

Lause 21. *Mikäli voidaan näyttää toteen, että*

1. $P(k)$ *on tosi ja*
2. $(\forall n \geq k)(P(n) \to P(n+1))$ *on tosi,*

niin ominaisuus $P(n)$ *on tosi joukossa* $\{k, k+1, k+2, \ldots, \}$.

3.3 Induktiotodistuksia joukossa $\mathbb{N}$

Esimerkki 55. Sanotaan, että jono $x_1 x_2 \ldots x_n$, on n-pituinen *bittijono*, jos kullekin muuttujalle x_i annetaan arvoksi joko 0 tai 1. Seuraavassa lauseessa selvitetään n-pituisten bittijonojen määrä.

Lause 22. *n-pituisia bittijonoja on 2^n kappaletta.*

Todistus. Todistus voidaan suorittaa täydellisellä induktiolla. Olkoon n-pituisten bittijonojen määrä $B(n)$ ja $P(n)$ ominaisuus $B(n) = 2^n$, jolloin siis induktioperiaatteen mukaan on todistettava $P(1)$ ja $(\forall n)(P(n) \to P(n+1))$. $P(1)$ tarkoittaa sitä, että $B(1) = 2^1$ (yhden pituisten bittijonojen määrä on 2), mikä on selvästi tosi.

Suoritetaan seuraavaksi induktioaskel, eli näytetään toteen implikaatio $(\forall n)(P(n) \to P(n+1))$. Tätä varten näytetään toteen implikaatio $P(n) \to P(n+1)$, kun luvusta n ei oleteta mitään erityistä. Tätä varten taas oletetaan $P(n)$ (induktio-oletus) ja johdetaan siitä $P(n+1)$ (induktioväite).

Oletus $P(n)$ tarkoittaa, että $B(n) = 2^n$, siis n-pituisten bittijonojen määrä on 2^n. $P(n+1)$ puolestaan puhuu $n+1$-pituisten bittijonojen määrästä, joten on mietittävä, miten se suhtautuu n-pituisten jonojen määrään. Helposti huomataan, että kaikki $n+1$-pituiset jonot saadaan n-pituisista lisäämällä eteen joko 0 tai 1, määrä siis kaksinkertaistuu kun pituutta lisätään yhdellä. Näin ollen $B(n+1) = 2 \cdot B(n) = 2 \cdot 2^n = 2^{n+1}$, mikä onkin väite $P(n+1)$.

Täten on todistettu seuraussuhde $P(n) \to P(n+1)$. Tästä seuraa $(\forall n)(P(n) \to P(n+1))$, sillä luvusta n ei oletettu mitään.

Esimerkki 56 (Bernoullin epäyhtälö). Olkoon $x \geq -1$ ja näytetään toteen, että aina kun $n \in \mathbb{N}$, on voimassa $(1+x)^n \geq 1+nx$. Merkitään $P(n)$:llä tätä ominaisuutta ja näytetään ensiksi induktion lähtökohta $P(1)$ todeksi.

$P(1)$ on siis sama kuin $(1+x)^1 \geq 1+1 \cdot x$, mikä pitää selvästi paikkansa, näin ollen induktion lähtökohta on tosi.

Osoitetaan sitten oikeaksi induktioaskel $(\forall n)(P(n) \to P(n+1))$, mikä tapahtuu siten, että näytetään toteen $P(n) \to P(n+1)$ olettamatta luvusta n mitään erityistä. Implikaatio $P(n) \to P(n+1)$ puolestaan osoitetaan oikeaksi olettamalla vasen puoli todeksi ja johtamalla tästä oikea puoli.

Oletetaan siis, että $P(n)$ on tosi, toisin sanoen, että $(1+x)^n \geq 1+nx$. Tästä oletuksesta on johdettava $P(n+1)$, siis epäyhtälö $(1+x)^{n+1} \geq 1+(n+1)x$. Johtaminen voi tapahtua seuraavasti:

$$(1+x)^{n+1} = (1+x)(1+x)^n \geq (1+x)(1+nx) = 1+nx+x+nx^2 = 1+(n+1)x+nx^2 \geq 1+(n+1)x.$$

Esimerkki 57. Osoitetaan induktiolla todeksi, että

$$\sum_{i=1}^{n} i = \frac{1}{2}n(n+1) \tag{3.2}$$

Ominaisuus $P(n)$ tässä yhteydessä tarkoittaa sitä, että yhtälö (3.2) toteutuu luvulle n, ja induktiotodistuksessa onkin ensiksi tarkistettava lähtökohta $P(1)$. Tämä tarkoittaa yhtälöä

$$\sum_{i=1}^{1} i = \frac{1}{2} \cdot 1 \cdot (1+1),$$

mikä on selvästi tosi.

Induktioaskelta $(\forall n)(P(n) \to P(n+1))$ varten oletetaan ensin $P(n)$ (induktio-oletus) ja johdetaan tästä $P(n+1)$ (induktioväite). Tämä voidaan tehdä seuraavasti:

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + n + 1 = \frac{1}{2}n(n+1) + n + 1 = \frac{1}{2}n(n+1) + \frac{1}{2}(2n+2) = \frac{1}{2}(n+1)(n+2).$$

Koska luvusta n ei oletettu mitään erityistä, on implikaatio tosi kaikille $n \in \mathbb{N}$.

Esimerkki 58. Palauta mieleen Fibonaccin lukujen rekursiivinen määritelmä: $F_0 = 0$, $F_1 = 1$ ja $F_{n+2} = F_{n+1} + F_n$, kun $n \geq 0$. Osoitetaan matemaattisella induktiolla todeksi, että $F_n \leq 2^n$ aina, kun $n \in \mathbb{N}_0$.

Ominaisuus $P(n)$, jota tässä yhteydessä ollaan näyttämässä toteen, on siis $F_n \leq 2^n$ ja koska rekursion pohjana toimivat F_0 ja F_1, pitää induktion lähtökohta varmistaa oikeaksi molempien osalta. Havaitaan että $F_0 = 0 \leq 2^0 = 1$ sekä $F_1 = 1 \leq 2^1 = 2$ ovat molemmat tosia.

Induktioaskelta varten oletetaan, että $P(n)$ on tosi aina, kun $n \geq 1$ ja tämän pohjalta näytetään todeksi myös $P(n+1)$. Tämä voi tapahtua seuraavasti: Olkoon $n \geq 2$. Tällöin

$$F_n = F_{n-1} + F_{n-2} \leq 2^{n-1} + 2^{n-2} \leq 2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n.$$

Tämän osion lopuksi esitettävää binomikaavaa varten kerrataan kurssista Matematiikan perustiedot ns. *binomikertoimet* ja tarkastellaan joitakin niiden ominaisuuksia. Johdantona binomikaavaan voidaan tarkastella binomin $a+b$ potensseja

$$(a+b)^1 = a+b, \quad (a+b)^2 = a^2+2ab+b^2, \quad (a+b)^3 = a^3+3a^2b+3ab^2+b^3,$$
$$(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4, \quad \text{jne.}$$

Edellisissä esimerkeissä $(a+b)^n$ on summalauseke, jossa esiintyvät termit $C_{n,i}a^{n-i}b^i$ ja jokaisessa termissä $C_{n,i}$ on jokin tietty kerroin. Newtonin binomikaava selvittää kertoimien $C_{n,i}$ muodon.

Määritelmä 49. Olkoon $0 \leq n \leq m$. Binomikerroin $\binom{m}{n}$ määritellään

$$\binom{m}{n} = \frac{m!}{n!(m-n)!}.$$

Esimerkki 59.

$$\binom{m}{0} = \frac{m!}{0! \cdot (m-0)!} = \frac{m!}{m!} = 1, \quad \binom{m}{1} = \frac{m!}{1! \cdot (m-1)!} = \frac{m \cdot (m-1)!}{(m-1)!} = m,$$

$$\binom{m}{2} = \frac{m!}{2 \cdot (m-2)!} = \frac{m(m-1) \cdot (m-2)!}{2 \cdot (m-2)!} = \frac{m(m-1)}{2}.$$

Lause 23. *Jos* $1 \leq n \leq m-1$, *niin* $\binom{m}{n} = \binom{m-1}{n} + \binom{m-1}{n-1}$

Todistus. Tässä todistuksessa esiintyy ainoastaan yhtäsuuruuksia, jotka on perusteltavissa määritelmillä tai (reaali)lukujen perusominaisuuksilla:

$$\begin{aligned}
&\binom{m-1}{n} + \binom{m-1}{n-1} \\
&= \frac{(m-1)!}{n!(m-1-n)!} + \frac{(m-1)!}{(n-1)!(m-1-(n-1))!} \\
&= \frac{(m-1)!(m-n)}{n!(m-n)!} + \frac{(m-1)!n}{n!(m-n)!} \\
&= \frac{(m-1)!(m-n+n)}{n!(m-n)!} = \frac{m!}{n!(m-n)!} \\
&= \binom{m}{n}.
\end{aligned}$$

Taustatietoa

Blaise Pascal (1623–1662) oli ranskalainen matemaatikko, fyysikko ja filosofi, jonka katsotaan perustaneen todennäköisyyslaskennan. Hän tutki myös projektiivista geometriaa. Pascalin mukaan on nimetty paineen yksikkö ja ohjelmointikieli.

(kuva: Wikimedia Commons)

Huomautus 37. Lauseen 23 mukaisesti binomikertoimet muodostavat ns. *Pascalin kolmion*, jonka kukin alkio askemalla yläoikealla ja ylävasemmalla olevat alkiot yhteen:

$$\begin{array}{ccccccccc}
 & & & \binom{0}{0} & & & & & \\
 & & \binom{1}{0} & & \binom{1}{1} & & & & \\
 & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & \\
\binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & \\
 & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \\
 & & & \dots & & & & &
\end{array}
=
\begin{array}{c}
1 \\
1\ \ 1 \\
1\ 2\ 1 \\
1\,3\ \ 3\,1 \\
1\,4\ 6\ 4\,1 \\
\dots
\end{array}$$

Binomikertoimen merkitys kombinatoriikassa (yhdistelmiä tutkiva matematiikan haara) on seuraava: $\binom{m}{n}$ ilmaiseen niiden tapojen määrän, joilla m:n alkion joukosta voidaan valita n alkiota, kun valintajärjestykseen ei kiinnitetä huomiota. Tämä voidaan havaita oikeaksi seuraavasti: Olkoon $C(m,n)$ mainittu tapojen määrä. Koska valitut n alkiota voidaan järjestää jonoon $n!$ eri tavalla, on $n!C(m,n)$ niiden tapojen määrä, joilla voidaan m:n alkion joukosta valita n alkiota järjestys huomioon ottaen. Koska ensimmäinen alkio voidaan valita m:llä tavalla, toinen $m-1$:llä, jne., on tämä määrä $m(m-1)(m-2)\cdot\ldots\cdot(m-n+1)$. Näin ollen

$$n!C(m,n) = m(m-1)\cdot\ldots\cdot(m-n+1),$$

mistä jakolaskulla ja määritelmiä soveltamalla saadaan

$$C(m,n) = \frac{m(m-1)\cdot\ldots\cdot(m-n+1)}{n!} = \frac{m(m-1)\cdot\ldots\cdot(m-n+1)\cdot(m-n)!}{n!(m-n)!} = \frac{m!}{n!(m-n)!} = \binom{m}{n}.$$

Esimerkki 60. Joukosta $\{1,2,3,\ldots,39\}$ voidaan valita 7 numeroa $\binom{39}{7} = \frac{39!}{7!\cdot 32!} = 15380937$ eri tavalla.

Lause 24 (Newtonin binomikaava).

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i,$$

kun n on positiivinen kokonaisluku.

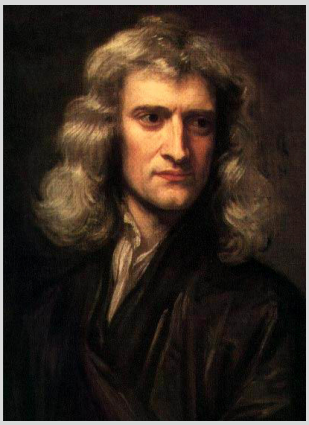
Todistus. Todistetaan väittämä induktiolla. Induktion lähtökohta $P(1)$: Kun $n = 1$, on vasen puoli $(a+b)^1 = a+b$ ja oikea puoli $\binom{1}{0}a^{1-0}b^0 + \binom{1}{1}a^{1-1}b^1 = a+b$, joten väite pätee tapauksessa $n = 1$.

Induktioaskel $(\forall n)(P(n) \to P(n+1))$: Oletetaan ensin $P(n)$ ja johdetaan $P(n+1)$. Suora lasku ja $P(n)$ antaa

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i \\
&= a\sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i + b\sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i \\
&= \sum_{i=0}^{n}\binom{n}{i}a^{n+1-i}b^i + \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^{i+1} \\
&= \sum_{i=0}^{n}\binom{n}{i}a^{n+1-i}b^i + \sum_{i=1}^{n+1}\binom{n}{i-1}a^{n-(i-1)}b^{i-1+1} \\
&= a^{n+1} + \sum_{i=1}^{n}\binom{n}{i}a^{n+1-i}b^i + \sum_{i=1}^{n}\binom{n}{i-1}a^{n+1-i}b^i + b^{n+1} \\
&= a^{n+1} + \sum_{i=1}^{n}\left(\binom{n}{i} + \binom{n}{i-1}\right)a^{n+1-i}b^i + b^{n+1} \\
&= a^{n+1} + \sum_{i=1}^{n}\binom{n+1}{i}a^{n+1-i}b^i + b^{n+1} \\
&= \sum_{i=0}^{n+1}\binom{n+1}{i}a^{n+1-i}b^i.
\end{aligned}$$

Näin saatu yhtäsuuruus on väite $P(n+1)$. Tällöin $(I\to)$-säännön nojalla on johdettu $P(n) \to P(n+1)$ ja $P(n)$ voidaan poistaa oletuksista. Kvanttori $(\forall n)$ voidaan $(I\forall)$-säännön mukaan lisätä, sillä luku n ei esiinny vapaana missään poistamattomassa oletuksessa. Näin ollen on johdettu kaava $(\forall n)(P(n) \to P(n+1))$. Induktioperiaatteen mukaan on siis todistettu $(\forall n)P(n)$.

Taustatietoa



Sir Isaac Newton (1643–1728) oli englantilainen matemaatikko, fyysikko, filosofi ja alkemisti. Newton esitti mekaniikan perustavat liikelait sekä yleisen gravitaatiolain. Hän kehitti differentiaali- ja integraalilaskennan riippumatta Gottfried Leibnizin samanaikaisesta työstä. Newtonin katsotaan kuuluvan Gaussin ja Arkhimedeen ohella maailmanhistorian merkittävimpien matemaatikkojen joukkoon.

(kuva: Wikimedia Commons)

Määritelmä 50. Matemaattinen induktio on menetelmä, jolla rekursiivista rakennetta koskeva väittämä voidaan todistaa oikeaksi äärettömälle määrälle erikoistapauksia.

Matemaattinen induktio perustuu kahteen askeleeseen:

1) Väittämän todistaminen rekursion pohjimmaisille alkioille (induktion lähtökohta)
2) Väittämän totuusarvon siirtäminen rekursiossa ylöspäin (induktioaskel).

3.4 Propositiologiikan semantiikkaa

Määritelmä 51. Olkoon HMK propositiologiikan hyvinmuodostettujen kaavojen joukko (kts. Määritelmä 48). Propositiologiikan *totuusarvotus* eli *arvotus* on funktio $\alpha : \text{HMK} \to \{0,1\}$, joka voidaan määritellä rekursiivisesti seuraavalla tavalla:

- Propositiomuuttujille $x_1, x_2, x_3, \ldots$ arvot $\alpha(x_i) \in \{0,1\}$ kiinnitetään mielivaltaisella tavalla.
- Jos ϕ ja ψ ovat propositioita, niin $\alpha((\neg\phi)) = 1 - \alpha(\phi)$, $\alpha((\phi \wedge \psi)) = \min\{\alpha(\phi), \alpha(\psi)\}$, ja $\alpha((\phi \vee \psi))) = \max\{\alpha(\phi), \alpha(\psi)\}$.

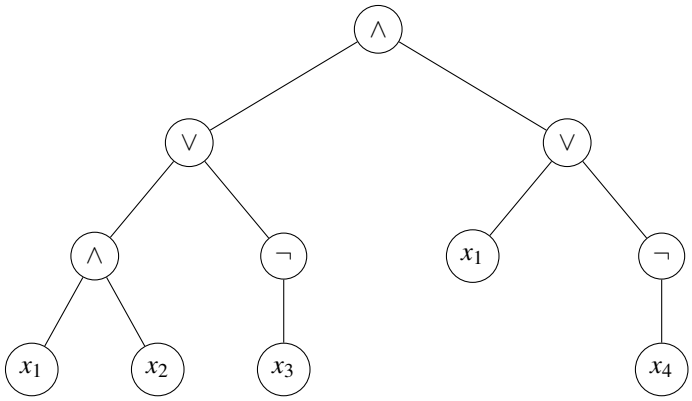
Määritelmä 52. Olkoon ϕ jokin propositio ja α jokin arvotus. Jos $\alpha(\phi) = 0$, sanotaan, että ϕ on *epätosi* arvotuksessa α. Jos $\alpha(\phi) = 1$, sanotaan, että ϕ on *tosi* arvotuksessa α.

Huomautus 38. Totuusarvotus $\alpha : \text{HMK} \to \{0,1\}$ tulee edellämainitulla tavalla yksikäsitteisesti määritellyksi joukossa HMK.

Todistus. Huomautus voidaan todistaa oikeaksi induktiolla. Induktion lähtökohta: Määritelmän mukaan α kiinnittää arvon jokaiselle propositiomuuttujalle x_i, joten induktion lähtökohta on tosi.

Induktioaskel: Esitetään induktio-oletus, jonka mukaan väittämä pitää paikkansa propositiolle ϕ ja ψ.

Tällöin arvotuksen α määritelmästä seuraa, että $\alpha((\neg\phi)) = 1 - \alpha(\phi)$, ja että $\alpha((\phi \wedge \psi)) = \min\{\alpha(\phi), \alpha(\psi)\}$. Samoin ja $\alpha((\phi \vee \psi)) = \max\{\alpha(\phi), \alpha(\psi)\}$. Koska kaikki propositiot saadaan aikaan aiemmista osita negaatioilla, konjunktioilla tai disjunktioilla, voidaan todeta, että väite on tosi kaikille propositioille.



Esimerkki 61. $\phi = ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$ ja arvotus α, jolle $\alpha(x_1) = 1$, $\alpha(x_2) = 1$, $\alpha(x_3) = 0$, ja $\alpha(x_4) = 1$.

Esimerkki 62. $\phi = ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$ ja arvotus α, jolle $\alpha(x_1) = 1$, $\alpha(x_2) = 1$, $\alpha(x_3) = 0$, ja $\alpha(x_4) = 1$.

Esimerkki 63. $\phi = ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$ ja arvotus α, jolle $\alpha(x_1) = 1$, $\alpha(x_2) = 1$, $\alpha(x_3) = 0$, ja $\alpha(x_4) = 1$.

Esimerkki 64. Esimerkki $\phi = ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$ ja arvotus α, jolle $\alpha(x_1) = 1$, $\alpha(x_2) = 1$, $\alpha(x_3) = 0$, ja $\alpha(x_4) = 1$.

Esimerkki 65. $\phi = ((x_1 \wedge x_2) \vee \neg x_3) \wedge (x_1 \vee \neg x_4)$ ja arvotus α, jolle $\alpha(x_1) = 1$, $\alpha(x_2) = 1$, $\alpha(x_3) = 0$, ja $\alpha(x_4) = 1$.

Määritelmä 53. Arvotus α on *pienempi tai yhtäsuuri kuin* arvotus β (merkitään $\alpha \preceq \beta$), jos $\alpha(x_i) \leq \beta(x_i)$ jokaiselle propositiomuuttujalle x_i.

Huomautus 39. $\alpha \preceq \beta$ on osittainen järjestys arvotusten joukossa. (miksi?)

Määritelmä 54. Propositio ϕ on *monotoninen*, jos ehdosta $\alpha \preceq \beta$ seuraa $\alpha(\phi) \leq \beta(\phi)$.

Lause 25. *Jos propositio ϕ muodostetaan rekursiivisesti käyttämällä vain konnektiiveja $\wedge$ ja $\vee$, eikä lainkaan konnektiivia $\neg$, on ϕ monotoninen.*

Todistus. Olkoot α ja β arvotuksia ja $\alpha \preceq \beta$.
Induktion lähtökohta: Jos $\phi = x_i$ (propositiomuuttuja), on määritelmän mukaan $\alpha(x_i) \leq \beta(x_i)$, joten $\phi = x_i$ on monotoninen.
Induktioaskel. Oletetaan, että väittämä pitää paikkansa propositiolle ϕ ja ψ ja näytetään toteen, että se pitää paikkansa myös propositiolle $(\phi \wedge \psi)$ ja $(\phi \vee \psi)$.

Todistus:

$$\alpha(\phi \wedge \psi) = \min\{\alpha(\phi), \alpha(\psi)\} \leq \min\{\beta(\phi), \beta(\psi)\} = \beta(\phi \wedge \psi).$$

Samoin

$$\alpha(\phi \vee \psi) = \max\{\alpha(\phi), \alpha(\psi)\} \leq \max\{\beta(\phi), \beta(\psi)\} = \beta(\phi \vee \psi).$$

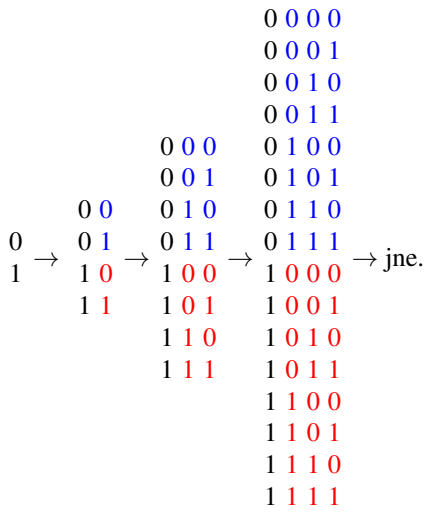
Induktioperiaatteen nojalla voidaan todeta, että väittämä pitää paikkansa kaikille propositioille, jotka voidaan muodostaa käyttämällä konnektiiveja $\wedge$ ja $\vee$. □

Propositiologiikan semantiikan keskeinen kysymys kuuluu: onko jokin annettu propositio ψ toteutuva vai ei. Tämä voidaan periaatteessa aina selvittää käymällä läpi kaikki mahdolliset arvotukset niiden muuttujien osalta, jotka propositiossa esiintyvät. Tätä voidaan havainnollistaa seuraaavan taulukon avulla: Totuustaulukon sarakkeet

x_2	x_2	…	x_{n-1}	x_n	$\phi(x_1, \ldots, x_n)$
0	0	…	0	0	$*$
0	0	…	0	1	$*$
0	0	…	1	0	$*$
0	0	…	1	1	$*$
⋮	⋮	⋱	⋮	⋮	⋮
1	1	…	1	1	$*$

rakennetaan siten, että propositiomuuttujien $x_1, \ldots, x_n$ kaikki arvot käydään läpi. Tämä on mahdollista varmistaa monilla eri tavoilla, joista yksinkertaisin lienee aloittaminen yhden bitin systeemista (0 tai 1) ja tämän jälkeen voidaan lisätä mahdollisten arvojen eteen 0 tai 1, jolloin bittijonon pituus kasvaa yhdellä ja lukumäärä kaksinkertaistuu.

Seuraava kuva havainnollistaa tätä prosessia:



Ensimmäisessä vaiheessa on siis vain yksi propositiomuuttuja (bitti), joka voi saada arvon 0 tai 1, ja kun nämä arvot kirjoitetaan allekkain, saadaan 2×1-taulukko jossa on kaksi riviä ja yksi sarake. Tätä voidaan laajentaa 4×2-taulukoksi, joka muodostetaan edellisessä vaiheessa olleen 2×1-taulukon kahdesta kopiosta (sininen ja punainen). Sinisen kopion eteen kirjoitetaan 0 ja punaisen kopion eteen 1. Konstruktiota voidaan laajentaa kolmen sarakkeen taulukoksi samalla idealla: 4×2-taulukosta otetaan kaksi kopiota (sininen ja punainen), sinisen kopion eteen asetetaan 0 ja punaisen eteen 1. Tällä tavoin jatkettaessa nähdään että muuttujien määrän lisääntyessä yhdellä mahdollisten arvotusten määrä tuplaantuu: Yhdellä propositiomuuttujalla on $2^1 = 2$ mahdollista arvotusta, kahdella $2^2 = 4$ ja $2^3 = 8$, jne.

3.5 Toteutuvuus

Yksi merkittävimmistä kysymyksistä propositiologiikassa lienee seuraava: Jos on annettuna kaava $\phi(x_1, \ldots, x_n)$, onko olemassa sellaista arvotusta propositiomuuttujille x_1 , …, x_n, että $\phi(x_1, \ldots, x_n)$ tulisi todeksi? Tätä kutsutaan *propositiologiikan toteutuvuusongelmaksi*.

Tämän kysymyksen selvittämiseksi on periaatteessa aina mahdollista käydä läpi kaikki 2^n vaihtoehtoa propositiomuuttujille, mutta käytännön hankaluudeksi muodostuu eksponenttifunktion 2^n arvon kasvaminen suureksi jo melko pienillä luvun n arvoilla. Täten siis kaikkien vaihtoehtojen läpi käyminen suurilla n:n arvoilla muodostuu laskennallisesti haastavaksi ongelmaksi.

Toisaalta monien käytännön ongelmien, kuten lukujärjestys- tai aikataulutusongelmien optimaaliseksi ratkaisemiseksi ei ole tiedossa mitään oleellisesti parempaa menetelmää kuin kaikkien ratkaisuvaihtoehtojen vaihtoehtojen läpikäyminen. Laskenta-ajan puitteissa tämä muodostaa suuren ongelman, sillä 2^n kasvaa suureksi jo varsin pienillä n:n arvoilla. Jos esimerkiksi $n = 300$, on 2^n jo suunnilleen suuruusluokkaa 10^{90}, kutakuinkin saman verran kuin arvioitu atomien määrä havaittavissa olevassa maailmankaikkeudessa.

Jos siis proposition ratkeavuusongelman selvittämiseksi pitää käydä läpi kaikki mahdolliset vaihtoehdot, tulee n:n propositionmuuttujan tapauksessä käydä läpi 2^n eri totuusarvotusta, ja kutakin arvotusta kohti pitää vielä laskea kyseisen proposition arvo (tosi/epätosi). Täten siis joudutaan käyttämään ainakin aika, joka on verrannollinen lukuun 2^n, ja käytetty aika siis kasvaa ainakin eksponentiaalisesti lukuun n nähden.

Jo 1970-luvulta asti asiaa tutkittaessa on havaittu, että monet merkittävät laskennallisesti merkittävät ongelmat voidaan palauttaa (redusoida) propositiologiikan ratkeavuusongelmaan. Tämä tarkoittaa sitä, että mikäli propositiologiikan ratkeavuusongelmalle löydettäisiin laskennallisesti tehokas ratkaisu, tästä seuraisi myös tehokas ratkaisu monille muille tärkeille ongelmille.

Siksi onkin hyvin perusteltua kysyä olisiko olemassa oleellisesti tehokkaampaa menetelmää propositiologiikan toteutuvuusongelmaksi? Erityisesti, olisiko olemassa jokin sellainen menetelmä, joka toimisi ajassa $p(n)$, missä p on jokin polynomi? On huomattava, että mille hyvänsä polynomille $p(n)/2^n \xrightarrow{n\to\infty} 0$, joten mikä tahansa polynomi $p(n)$ on suurilla n:n arvoilla mitättömän suuruinen lukuun 2^n nähden.

Vaikka kysymys on hyvin perusteltu, myös käytännölliseltä kannalta mielenkiintoinen ja asiaa on tutkittu n. 50 vuotta, ei vastausta siihen tiedetä vielä. Kysymys on tapana formalisoida määrittelemällä **P** niiden ongelmien luokaksi, jotka voidaan ratkaista ns. *deterministisellä Turingin koneella* polynomiajassa ja **NP** ongelmien luokaksi jotka voidaan ratkaista *epädetermisistisellä Turinin koneella* polynomiajassa. Tällöin ongelman muotoilu saa asun

$$\mathbf{P} \neq \mathbf{NP}?$$

Clay Mathematics Institute tarjoaa $1000000 palkinnon tämän ongelman selvittämisestä.

Luvun oleellisia asioita:

- Rekursio ja rekursiivinen rakenne.
- Matemaattinen induktio (osattava!) on yksi tapa osoittaa väittämä todeksi äärettömän monelle arvolle, mutta nimestään huolimatta on yksi deduktion muoto.

Luku 4
Boolen algebra

4.1 Propositiologiikan sovelluksia

Jo 1900-luvun alkupuolelta asti on osattu käyttää elektroniputkia sähkötekniikan komponentteina, joiden avulla on voitu esim. jännitettä käsitellä on/off-syötteenä ja elektroniputkien ulosantia loogisena tulosteena.

- Jännite on mahdollista mieltää 0 / 1 –suureena (0 V vs. 5 V).
- Virtapiireissä on mahdollista rakentaa $\neg$, $\wedge$, ja $\vee$ -rakenteita.
- Nykyaikaisten klassisen informaation tietokoneiden toiminta on perustasolla kuvattavissa näistä rakentuvien funktioiden avulla.

Esimerkki 66. Jos käytettävissä on $\vee$, $\wedge$ ja $\neg$-portit, mieti minkälaisella piirillä toteutetaan yhteenlasku $x_1 + x_2$ (ja muistinumero), kun $x_1, x_2 \in \{0,1\}$.

1900-luvun loppupuolelta alkaen on komponentteja osattu rakentaa ns. mikropiireihin, joiden looginen rakenne perustuu puolijohdekomponenttien sähköiseen toimintaan. Nykyisellä tekniikalla voidaan rakentaa yli sata miljoonaa komponenttia (esim. transistoria) neliömillimetrin kokoiselle alueelle. Tämä mahdollistaa hyvin monimutkaisen tietojenkäsittelyn pienessä tilassa.

Voidaan kuitenkin huomata, että monenlaiset propositiologiikan kaavat voivat määritellä saman funktion ja jonkin fysikaalisen toteutuksen puitteissa saattaa olla hyvinkin perusteltua valita jokin tietty kaava esittämään kyseistä funktiota. Yleensä toivotaan optimaalista toteutusta, mutta optimaalisuuden kriteerit voivat vaihdella eri fysikaalisissa toteutuksissa.

4.2 Propositioiden ekvivalenssi

Esimerkki 67. Aiemmassa luvussa määritellyt propositiologiikan kaavat ovat merkkijonoja, joihin sisältyy propositiomuuttujia, konnektiiveja sekä sulkumerkkejä. Näin ollen kaavat $x \wedge (y \wedge z)$ ja $(x \wedge y) \wedge z$ eivät ole yhtäsuuret, koska ne ovat erilaisia merkkijonoja.

Kuitenkin propositio $x \wedge (y \wedge z)$ saa totuusarvon 1 tarkalleen silloin kun jokainen propositiomuuttuja x, y ja z saa arvon 1, ja samoin on proposition $(x \wedge y) \wedge z$ laita. Näin ollen kyseisiä propositioita voidaan pitää tietyssä mielessä samankaltaisina.

Esimerkki 68. Propositiot $x \wedge \neg y$ ja $\neg(\neg x \vee y)$ eivät ole yhtäsuuret, mutta saavat samat totuusarvot kaikissa mahdollisissa totuusarvotuksissa, kuten seuraava taulukko osoittaa,

x	y	$x \wedge \neg y$	$\neg(\neg x \vee y)$
0	0	0	0
0	1	0	0
1	0	1	1
1	1	0	0

Matemaattinen ekvivalenssin käsite on omiaan täsmentämään mainittua samankaltaisuutta.

Määritelmä 55. Propositiot ϕ ja ψ ovat *ekvivalentit*, mikäli $\alpha(\phi) = \alpha(\psi)$ kaikille totuusarvotuksille α. Tällöin merkitään $\phi \equiv \psi$. On suoraviivaista nähdä, että $\equiv$ on ekvivalenssirelaatio (miksi?)

Lause 26. *Edellisen määritelmän $\equiv$ on paitsi ekvivalenssi(relaatio), myös kongruenssi operaatioiden $\neg$, $\wedge$ ja $\vee$ suhteen.*

Huomautus 40. Ylläolevan lauseen kongruenssiominaisuus merkitsee sitä, että jos $\phi_1 \equiv \phi_2$ ja $\psi_1 \equiv \psi_2$, niin $\neg\phi_1 \equiv \neg\phi_2$ ja $\phi_1 \wedge \psi_1 \equiv \phi_2 \wedge \psi_2$ ja $\phi_1 \vee \psi_1 \equiv \phi_2 \vee \psi_2$. Nämä pitää kaikki tarkistaa jotta voitaisiin olla varmoja siitä, että $\equiv$ on kongruenssi.

Määritelmän 55 mukaisen ekvivalenssikäsitteen avulla voidaan laajentaa konjunktion ja disjuktion määritelmää tapaukseen, jossa on useita rinnakkaisia konjunktioita.

Määritelmä 56. Lyhennysmerkintä $x \wedge y \wedge z$ tarkoittaa propositiota $(x \wedge y) \wedge z$ tai propositiota $x \wedge (y \wedge z)$. Lyhennysmerkintä $x \vee y \vee z$ niinikään tarkoittaa propositiota $(x \vee y) \vee z$ tai propositiota $x \vee (y \vee z)$.

Huomautus 41. Ylläolevassa määritelmässä sulkeilla varustetut konjunktiot (kuin myös disjunktiot) ovat ekvivalentteja, joten on yhdentekevää kumpi niistä valitaan määrittelemään sulkeistamatonta konjunktiota (tai sulkeistamatonta disjunktiota).

Tätä voi varsin hyvin verrata summamerkintöihin $(x+y)+z$ ja $x+(y+z)$. Nämäkään eivät merkkijonoina ole yhtäsuuret, mutta reaalilukujen teoriassa näillä summilla on täsmälleen sama lukuarvo, olipa reaaliluvuilla x, y ja z mitkä arvot hyvänsä. Tämä perustuu viime kädessä reaalilukujen aksiomatiikkaan. Näin ollen molemmista summista voidaan periaatteessa käyttää merkintää $x+y+z$ ilman sulkeita. Tästä merkinnästä on melko helppo johtaa induktiivinen yleistys, josta käytetään merkintää $x_1 + x_2 + \ldots + x_n$ ilman sulkeita, olipa yhteenlaskettavien määrä mikä hyvänsä.

Samoin voidaan toimia predikaattilogiikan kaavojen kohdalla.

Määritelmä 57. $x_1 \wedge x_2 \wedge \ldots \wedge x_n$ on propositiologiikan kaava, joka voidaan rekursiivisesti määritellä kaavana $x_1 \wedge (x_2 \wedge \ldots \wedge x_n)$ tai kaavana $(x_1 \wedge \ldots \wedge x_{n-1}) \wedge x_n$. Kaava $x_1 \vee x_2 \vee \ldots \vee x_n$ määritellään samoin. Huomaa että määritelmässä ei ole välttämätöntä että x_i:t olisivat propositiomuuttujia.

Huomautus 42. Jos $\alpha : \{x_1, x_2, x_3, \ldots\} \to \{0,1\}$ on jokin totuusarvotus, on $\alpha(x_1 \wedge x_2 \wedge \ldots \wedge x_n) = \min\{\alpha(x_1), \alpha(x_2), \ldots, \alpha(x_n)\}$ ja $\alpha(x_1 \vee x_2 \vee \ldots \vee x_n) = \max\{\alpha(x_1), \alpha(x_2), \ldots, \alpha(x_n)\}$.

Esimerkki 69. Kaava $x \wedge \neg y \wedge z$ saa arvon 1 tarkalleen silloin, kun $(x,y,z) = (1,0,1)$ ja kaava $x \wedge y \wedge \neg z$ saa arvon 1 tarkalleen silloin $(x,y,z) = (1,1,0)$. Näin ollen kaava $(x \wedge \neg y \wedge z) \vee (x \wedge y \wedge \neg z)$ saa arvon 1 tarkalleen kun $(x,y,z) = (1,0,1)$ tai $(x,y,z) = (1,1,0)$.

4.3 Boolen funktiot

Edellä esitettyjen merkintöjen avulla nähdään melko helposti oikeaksi varsin merkittävä tulos ns. Boolen funktioiden esittämisestä.

Määritelmä 58. n-paikkainen *Boolen funktio* eli *totuusfunktio* f on funktio $f : \{0,1\}^n \to \{0,1\}$.

Lause 27. *Jokainen n-paikkainen Boolen funktio f voidaan esittää propositiologiikan kaavana, jossa esiintyvät propositiomuuttujat x_1, …, x_n, ja konnektiivit $\neg$, $\wedge$ ja $\vee$.*

Todistus. Funktio $f : \{0,1\}^n \to \{0,1\}$ joka saa arvon 1 tarkalleen alkukuvissa $\mathbf{a}_1, \ldots, \mathbf{a}_N \in \{0,1\}^n$ ja nollan muualla voidaan määritellä ns. *disjunktiivisella* muodolla

$$f = \eta_1 \vee \eta_2 \vee \ldots \vee \eta_N,$$

missä kukin η_i on *konjunktiivista* muotoa $\eta_i = y_{i1} \wedge y_{i2} \wedge \ldots \wedge y_{in}$, missä edelleen $y_{ij} = x_j$ jos $(\mathbf{a}_i)_j = 1$ ja $y_{ij} = \neg x_j$ jos $(\mathbf{a}_i)_j = 0$.

Todistusta voidaan havainnollistaa havainnollistaa seuraavilla esimerkeillä.

Esimerkki 70. Muodostetaan Boolen funktio $f : \{0,1\}^3 \to \{0,1\}$, jolle $f(0,0,1) = f(0,1,0) = 1$, $f(1,0,0) = 1$ ja $f(x_1,x_2,x_3) = 0$ kaikille muille $(x_1,x_2,x_3) \in \{0,1\}^3$. Tällöin on siis kolme alkukuvaa, $\mathbf{a}_1 = (0,0,1)$, $\mathbf{a}_2 = (0,1,0)$ ja $\mathbf{a}_3 = (1,0,0)$, joissa f saa arvon 1. Valitaan siis $\eta_1 = \neg x_1 \wedge \neg x_2 \wedge x_3$, $\eta_2 = \neg x_1 \wedge x_2 \wedge \neg x_3$ ja $\eta_3 = x_1 \wedge \neg x_2 \wedge \neg x_3$, jolloin η_1 saa arvon 1 ainoastaan kun $(x_1,x_2,x_3) = (0,0,1)$, η_2 arvon 1 ainoastaan kun $(x_1,x_2,x_3) = (0,1,0)$ ja η_3 arvon 1 ainoastaan kun $(x_1,x_2,x_3) = (1,0,0)$. Näin ollen

$$f(x_1,x_2,x_3) = \eta_1 \vee \eta_2 \vee \eta_3 = (\neg x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge \neg x_3) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3)$$

saa arvon 1 tarkalleen silloin kun $(x_1,x_2,x_3) = (0,0,1)$, $(0,1,0)$ tai $(1,0,0)$.

Esimerkki 71. Muodostetaan Boolen funktio $f : \{0,1\}^2 \to \{0,1\}$, jolle pätee $f(x_1,x_2) = 0$, jos $x_1 = x_2$ ja $f(x_1,x_2) = 1$, jos $x_1 \neq x_2$, siis $f(0,0) = f(1,1) = 0$ ja $f(1,0) = f(0,1) = 1$. Tämä funktio voidaan muodostaa osakaavoista $x_1 \wedge \neg x_2$ ja $\neg x_1 \wedge x_2$, joista ensimmäinen saa arvon 1, kun $(x_1,x_2) = (1,0)$ ja toinen arvon 1, kun $(x_1,x_2) = (0,1)$. Näin ollen haluttu funktio saadaan osakaavojen disjunktiona $(x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2)$.

Huomautus 43. Jokainen funktio $f : \{0,1\}^n \to \{0,1\}^m$ voidaan koostaa m:stä Boolen funktiosta f_1, …, f_m: $\{0,1\}^m \to \{0,1\}$.

4.4 Boolen algebran aksioomat

Määritellään kaksi nollapaikkaista propositiota seuraavasti:

Määritelmä 59. *Verum* $\top$ on propositio, joka on tosi kaikissa tulkinnoissa ja *Falsum* $\bot$ on propositio, joka on epätosi kaikissa tulkinnoissa.

Esimerkki 72. Kaikille mahdollisille tulkinnoille α on $\alpha(x \wedge \top) = \alpha(x)$ ja $\alpha(x \vee \bot) = \alpha(x)$ (miksi?). Näin ollen $x \wedge \top \equiv x$ ja $x \vee \bot \equiv x$.

Kun otetaan huomioon muita edellä esitettyjä ekvivalensseja, voidaan esittää seuraava ominaisuuksien lista, joka tunnetaan *Boolen algebran* määrittelevänä aksioomalistana.

Määritelmä 60. Boolen algebra on joukko B jossa on määritelty kaksi binääristä operaatiota $\wedge$ ja $\vee$, yksi unaarinen operaatio $\neg$ ja kaksi nollapaikkaista operaatiota (eli vakiota) $\bot$ ja $\top$ jotka toteuttavat seuraavat aksioomat:

- $a \vee (b \vee c) = (a \vee b) \vee c$ ja $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (assosiatiivisuus).
- $a \vee b = b \vee a$ ja $a \wedge b = b \wedge a$ (kommutatiivisuus)
- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ ja $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ (distributiivisuus)
- $a \vee \bot = a$, $a \wedge \top = a$ (neutraalialkiot)
- $a \vee \neg a = \top$ ja $a \wedge \neg a = \bot$ (vasta-alkiot)

Huomautus 44. On myös tapana merkitä 1 verumin $\top$ ja 0 falsumin $\bot$ sijasta.

Huomautus 45. Boolen algebrassa ovat kummankin operaation $\wedge$ ja $\vee$ suhteen analogiset distributiivisäännöt voimassa, siis

- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ ja
- $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Näin ei ole esimerkiksi kokonaislukujen renkaassa, jossa kertolasku on distributiivinen yhteenlaskun yli: $a \cdot (b+c) = a \cdot b + a \cdot c$, mutta päinvastoin $a + (b \cdot c) = (a+b) \cdot (a+c)$ ei yleensä pidä paikkansa.

Huomautus 46. Tyypillisenä esimerkkinä Boolen algebrasta toimii nimenomaan määritelmän 55 mukaiset propositiologiikan ekvivalenssiluokat.

Lause 28 (De Morganin lait). *Boolen algebrassa pätee* $\neg(a \wedge b) = \neg a \vee \neg b$ *ja* $\neg(a \vee b) = \neg a \wedge \neg b$

Huomautus 47. De Morganin lait voidaan johtaa suoraan Boolen funktioiden aksioomista (miten?)

Esimerkki 73. Boolen algebran ominaisuudet voivat joskus tarjota mahdollisuuksia “sieventää“ propositiologiikan lausekkeita.

$$\begin{aligned}
& (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2) \\
\equiv\ & (x_1 \vee (\neg x_1 \wedge x_2)) \wedge (\neg x_2 \vee (\neg x_1 \wedge x_2)) \\
\equiv\ & ((x_1 \vee \neg x_1) \wedge (x_1 \vee x_2)) \wedge ((\neg x_2 \vee \neg x_1) \wedge (\neg x_2 \vee x_2)) \\
\equiv\ & (\top \wedge (x_1 \vee x_2)) \wedge (\neg(x_1 \vee x_2) \wedge \top) \\
\equiv\ & ((x_1 \vee x_2)) \wedge (\neg(x_1 \wedge x_2))
\end{aligned}$$

Mieti mitä Boolen algebran ominaisuutta on kussakin kohdassa käytetty.

Propositiologiikan ekvivalenssiluokkien ohella toinen tunnettu esimerkki Boolen algebrasta on jonkin perusjoukon X osajoukkojen joukossa määritellyt operaatiot.

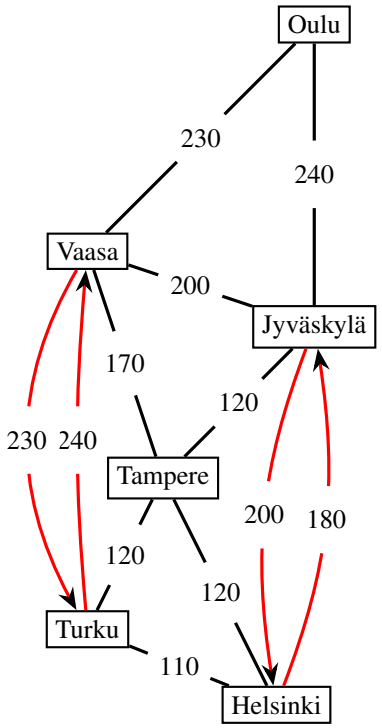
Esimerkki 74. Olkoon X jokin joukko ja sen osajoukkojen joukossa $\mathscr{P}(X)$ määritellyt $A \cup B$, $A \cap B$, $\overline{A} = P \setminus A$, jne. Minkälaisina Boolen algebran aksioomat näyttäytyvät, kun operaatiota $\wedge$, $\vee$ ja $\neg$ vastaavat $\cap$, $\cup$, ja joukko-opillinen komplementti. Mitkä joukot vastaavat vakioita $\bot$ ja $\top$?

Luku 5
Graafiteoriaa

5.1 Graafit

Matemaattisen graafi-käsitteen esityksiä hyödynnetään visualisoitaessa monenlaisia suhteita (relaatioita), joten ei liene yllätys, että käsitteellä graafi on hyvinkin vahva yhteys relaatiohin. Toisaalta taas joissain tapauksissa on tarpeen lisätä visuaaliseen esitysasuun ominaisuuksia, joita ei yksinkertaisimmissa relaation esityksissä ole.

Esimerkki 75. Alla oleva kuvio on tyypillinen esimerkki graafista. Siinä on esitetty kuusi suomalaista kaupunkia ja keskimääräisiä ajoaikoja minuutteina kaupunkien välillä erään vuoden heinäkuussa. Epäsymmetria matka-ajoissa Turun ja Vaasan sekä Jyväskylän ja Helsingin välillä on merkitty punaisella ja johtuu tien kunnostustöistä joiden vuoksi nopeusrajoitusta on alennettu vain moottoritien toisella puolella.



Graafiteorian keskeiset käsitteet on mahdollista kuvailla yllä olevan esimerkin valossa: Kaupunkeja kutsutaan graafin *pisteiksi* tai *solmuiksi* (engl. *vertices*, *nodes*), teitä kaupunkien välillä kutsutaan *nuoliksi*, tai *viivoiksi* tai *kaariksi*, (engl. *edges*), ja nuoliin tai viivoihin liitettyjä lukuarvoja kutsutaan näiden *leimoiksi* (engl. *labels*).

Ylläoleva kuva on siis visuaalinen esitys graafista, jossa pisteinä toimivat kaupungit, nuolina (viivoina) näiden väliset tieyhteydet, ja jälkimmäisiin liittyvinä leimoina matka-ajat. Graafi siis ilmaisee esimerkiksi sen, että ajomatka Helsingistä Turkuun kestää n. 110 minuuttia, Turusta Vaasaan n. 240 minuuttia, ja Vaasasta takaisin Turkuun n. 230 minuuttia.

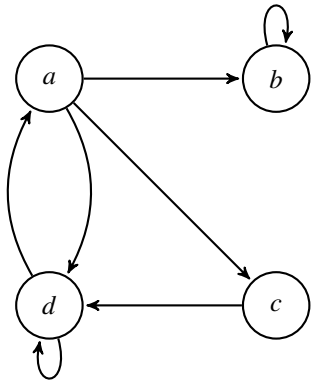
Lukuisat käsitteen graafi määritelmät johtavat omilla sovellusalueillaan yleensä matemaattisesti analogiseen tulokseen, eikä tällä kurssilla ole syytä yrittää tavoitella kaikkein yleisintä määritelmää, vaan sellaista joka riittää tämän kurssin kannalta oleellisiin sovelluksiin. Yleisenä periaatteena kannattaa valita määritelmä mahdollisimman yksinkertaiseksi, kunhan sen perusteella kuitenkin kyetään ilmaisemaan tarkasteltavan objektin halutut ominaisuudet riittävän tarkasti. Riittävä tarkkuus riippuu ilman muuta siitä, millaista objektia on tarkoitus mallintaa.

Yksi monissa yhteyksissä ja myös tämän kurssin kannalta käyttökelpoinen graafin määritelmä on seuraava:

Määritelmä 61. Graafi G on pari $G = (V,E)$, missä G on graafin *pisteiden* (engl. *vertices* tai *nodes*) joukko ja $E \subseteq V \times V$ graafin *nuolien* eli *viivojen* (engl. *edges*) joukko.

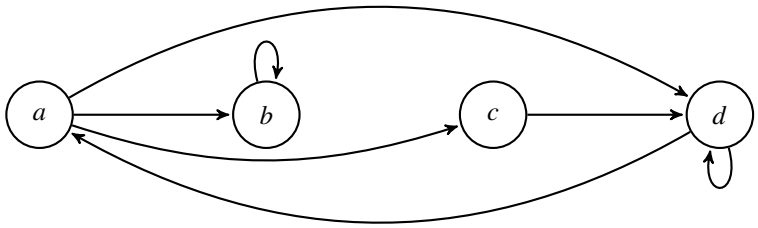
Tämän määritelmän mukaista graafia (tai sen osaa) visualisoidaan esittämällä graafin pisteet tasolla jossain järjestyksessä, ja viivat nuolina pisteiden välillä.

Esimerkki 76. Olkoon G graafi, jonka pisteiden joukko on $V = \{a,b,c,d\}$ ja nuolien joukko $E = \{(a,b),(a,c),(a,d),(b,b),(c,d),(d,a),(d,d)\}$. Graafin visuaalinen esitys on alla olevassa kuvassa:



Tarkkaavainen lukija voi tässä yhteydessä huomata suoran yhteyden aiemmassa luvussa esitetyn relaatiokäsitteen ja graafin välillä: Määritelmän 61 mukaisen graafin viivat on tosiaankin täsmälleen sama asia kuin binäärinen relaatio joukossa V, mikä siis tarkoittaa joukon $V \times V$ osajoukkoa.

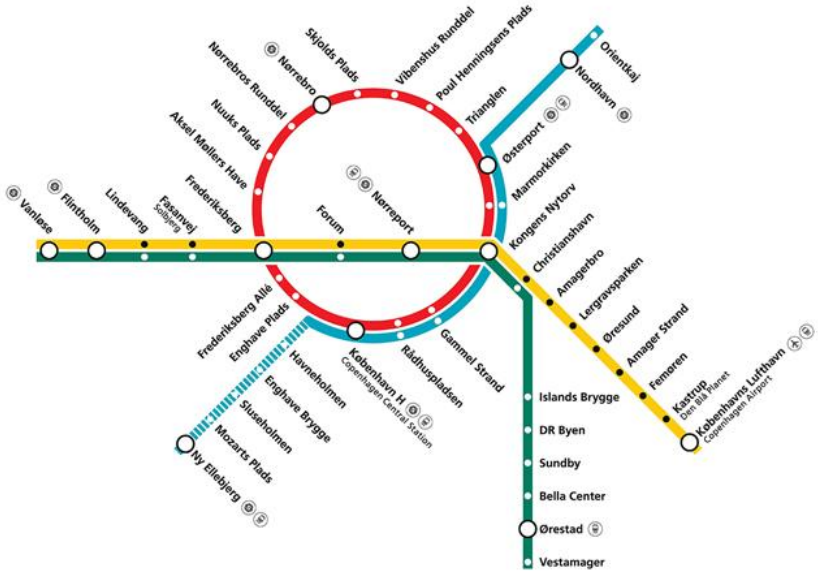
Huomautus 48. Graafin visuaalinen esitysasu ei ole yksikäsitteisesti määrätty. Edellisen esimerkin graafissa voitaisiin pisteet järjestää kuvioon periaatteessa miten hyvänsä, jolloin saadaan uudenlainen visuaalinen esitysasu samalle graafille:



Vaikka graafeja käytetään tyypillisesti visualisoimaan reaalimaailman objekteja ja niiden välisiä suhteita, ei graafin matemaattinen määritelmä kerro millä tavalla graafi pitäisi visualisoida. Tästä on toisinaan hyötyäkin:

Metrokartat ovat tyyppiesimerkkejä graafeista, eikä niiden visuaalisessa esityksessä ole useinkaan tarpeen esittää miten asemat (graafin pisteet) sijaitsevat metrimääräisillä etäisyyksillä mitattuina toistensa suhteen. Erityisesti suurkaupunkien keskusta-alueella metroasemia on hyvin tiheästi, kun taas asemien välit kohti esikaupunkialuetta mennessä yleensä pitenevät.

Metroverkoston käyttäjän kannalta eksaktia välimatkaa tärkeämpi informaatio on asemien väliset linjat (graafin viivat), joista voi päätellä miten kannattaa asemalta toiselle kulkea. Suurkaupungin metrokartassa on keskusta-alueen asemien välit yleensä esitetty pidempinä kuin niiden maantieteellinen etäisyys edellyttäisi, mikä selkeyttää metrokartan (graafin) tulkitsemista.

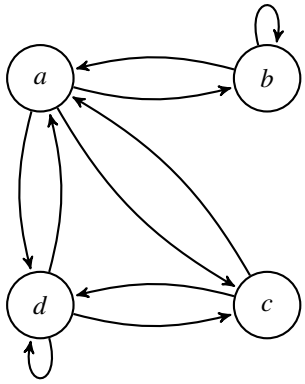


Kuva 5.1 Kööpenhaminan metrokartassa jokainen piste vastaa yhtä metroasemaa. Mittasuhteet eivät vastaa todellisia maantieteellisiä etäisyyksiä vaan erityisesti keskusta-alueen asemavälit on esitetty suhteellisesti paljon suurempina kuin linjojen ääripäiden asemavälit.

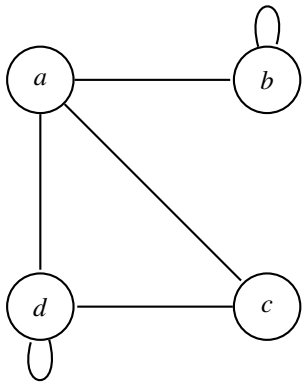
Määritelmä 62. Graafi $V = (G,E)$ on *suuntaamaton* tai *symmetrinen* (engl. undirected), mikäli jokaista $(v,u) \in E$ kohti on olemassa myös $(u,v) \in E$, toisin sanoen graafin määrittelevä relaatio on symmetrinen. Koska symmetrisessä graafissa on aina nuolta $u \to v$ kohti myös nuoli $v \to u$, ei visuaalisessa esitysasussa ole tarpeen piirtää kahteen suuntaan kulkevia nuolia, vaan korvata ne yhdellä ainoalla viivalla johon ei piirretä nuolen kärkiä kumpaankaan suuntaan. Erityisesti tässä tapauksessa on graafin nuolia tapana kutsua *viivoiksi*.

Huomautus 49. Mistä hyvänsä Määritelmän 61 mukaisesta graafista G on mahdollista tehdä symmetrinen graafi lisäämällä jokaista nuolta $u \to v$ kohti myös nuoli $v \to u$, ellei sitä jo aiemmin graafissa ole. Näin saatua uutta graafia G_1 kutsutaan graafin G *symmetriseksi sulkeumaksi*. Samoin graafia G_1 vastaavaa relaatiota kutsutaan graafia G vastaavan relaation symmetriseksi sulkeumaksi.

Esimerkki 77. Alla oleva graafi on Esimerkin 76 graafin symmetrinen sulkeuma. Joukon $V = \{a,b,c,d\}$ symmetrinen relaatio on tässä tapauksessa $E = \{(a,b),(b,a),(a,c),(c,a),(a,d),(d,a),(b,b),(c,d),(d,c),(d,d)\}$.



Koska ylläoleva graafi on symmetrinen, on se yleensä tapana esittää visuaalisesti ilman kahteen suuntaan kulkevia nuolia allaolevan kuvion mukaisesti.



Huomautus 50. Symmetrisen sulkeuman lisäksi on mahdollista määritellä käsite *refleksiivinen sulkeuma*, jossa kutakin alkiota a kohti lisätään nuoli $a \to a$, sekä *transitiivinen sulkeuma*, jossa jokaista nuoliparia $a \to b$ ja $b \to c$ kohti lisätään nuoli $a \to c$, ja lisäämistä toistetaan kunnes nuolikaavion määrittämä relaatio on kokonaisuudessaan transitiivinen.

Edellämainitun perusteella näyttää siis siltä, että käsite graafi ainakin perusmuodossaan sisältyisi matemaattisesti keskeiseen relaatio-käsitteeseen, jota on aiemmin käsitelty. Siksi onkin perusteltua kysyä miksi ylipäänsä pitäisi olla jokin muunlainen teoreettinen määritelmä käsitteelle graafi.

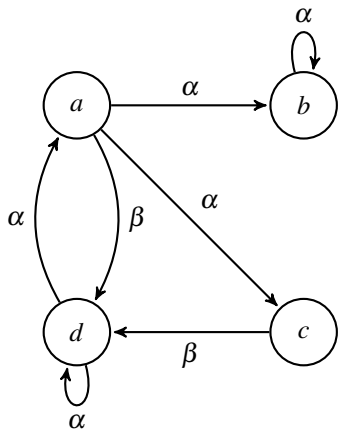
Vastauksena yllä esitettyyn pohdintaan voidaan esittää jo pelkästään käytännön tarpeista liittää jotain suureita relaationuoliin, kuten matka-ajat esimerkissä 75 sekä linjojen värit metrokartassa.

Määritelmä 63. Olkoon $G = (V,E)$ graafi ja L jokin joukko, jonka alkioita kutsutaan *leimoiksi* (eng. *labels*). Tällöin sanotaan, että funktio $l : E \to L$ varustaa nuolet *leimoilla*, jolloin saadaan *leimattu graafi* (eng. *labelled graph*).

Esimerkki 78. Olkoon $G = (V,E)$ sama kuin esimerkissä 76 ja $L = \{\alpha, \beta\}$. Määritellään funktio $l : E \to L$ seuraavan taulukon mukaisesti:

e	(a,b)	(a,c)	(a,d)	(b,b)	(c,d)	(d,a)	(d,d)
$l(e)$	α	α	β	α	β	α	α

Näin saadaan leimattu graafi, jonka visualisaatio on alla olevassa kuvassa.



Huomautus 51. Jos $G = (V,E)$ on leimattu graafi ja $(a,b) \in V$ nuoli jonka leima on α, merkitään $a \xrightarrow{\alpha} b$.

Esimerkki 79. Esimerkin 75 graafissa pisteiden joukko on $V = \{\text{Helsinki}, \text{Jyväskylä}, \text{Oulu}, \text{Tampere}, \text{Turku}, \text{Vaasa}\}$ ja nuolien joukko on $E = \{(\text{Helsinki}, \text{Jyväskylä}), (\text{Helsinki}, \text{Tampere}), (\text{Helsinki}, \text{Turku}), \ldots (\text{Tampere}, \text{Helsinki}), \ldots, (\text{Turku}, \text{Vaasa}), \ldots, (\text{Vaasa}, \text{Turku})\}$.

Esimerkin 75 graafi on siis siinä mielessä symmetrinen, että nuolta $(a,b) \in E$ kohti on myös aina nuoli (b,a). Epäsymmetria nousee kuitenkin esille kun määritellään leimafunktio nuolille: Esimerkiksi $l(\text{Helsinki}, \text{Jyväskylä}) = 180$, mutta $l(\text{Jyväskylä}, \text{Helsinki}) = 200$, mutta toisaalta $l(\text{Helsinki}, \text{Tampere}) = l(\text{Tampere}, \text{Helsinki}) = 120$.

Graafin visuaalinen esitys esimerkissä 75 onkin piirretty siten, että niiden kaupunkien välille, joissa matka-aika on symmetrinen, ei ole piirretty kahdensuuntaisia nuolia joilla olisi sama aikaleima (tämäkin olisi mahdollinen esitys), vaan yksi ainoa viiva, jolla on aikaleima.

Sen sijaan epäsymmetristen matka-aikojen kohdalla graafiin on piirretty kahdensuuntaiset nuolet, ja kummankin suunnan kohdalla merkitty leimaksi matka-aika.

Huomautus 52. Esimerkin 75 graafissa on osa nuolista värjätty punaisella. Tämänkaltaista värjäystä ei tarvitse jättää pelkästään mielivaltaiseksi visuaalisen esitysasun funktioksi, vaan myös väri voidaan "koodata" sisään leimafunktioon: Sen sijaan että määriteltäisiin leimafunktio $l(e) = d$, missä $d \in \mathbb{R}$ on etäisyys, voidaan määritellä leimafunktio $l \to \mathbb{R} \times \{\text{punainen}, \text{musta}\}$, siis kullekin nuolelle voidaan määritellä väri laajennetun leimafunktion avulla

Esimerkin 75 tapauksessa olisi siis $l(\text{Jyväskylä}, \text{Helsinki}) = (200, \text{punainen})$ ja $l(\text{Turku}, \text{Helsinki}) = (110, \text{musta})$. Mieti miten graafin *pisteiden* väri (vrt. metrokartta) otetaan huomioon määritelmässä (Tähän on ainakin kaksi toisistaan oleellisesti poikkeavaa mahdollisuutta).

Määritelmä 64. Olkoon $G = (V,E)$ graafi ja $\Pi : v_0, v_1, \ldots, v_n$ sellainen pisteiden joukko, että $(v_i, v_{i+1}) \in E$ ja kaikki pisteet mahdollisesti v_0:aa ja v_n:ää lukuunottamatta ovat erisuuria. Tällöin sanotaan, että

$$\Pi : v_0 \to v_1 \to \ldots \to v_n$$

on n-pituinen *polku* (eng. *path*) graafissa G.

Jos graafi on symmetrinen, määritellään polku P^{-1} seuraavasti:

$$\Pi^{-1} : v_n \to v_{n-1} \to \ldots \to v_0,$$

Π^{-1} saadaan siis kulkemalla polku Π "takaperin".

Esimerkki 80. Esimerkin 75 graafissa on 3-pituinen polku

$$\Pi : \text{Turku} \to \text{Tampere} \to \text{Jyväskylä} \to \text{Oulu}$$

ja tämän käänteinen polku Π^{-1} on

$$\Pi^{-1} : \text{Oulu} \to \text{Jyväskylä} \to \text{Tampere} \to \text{Turku}$$

Määritelmä 65. Suuntaamaton graafi $G = (V,E)$ on *yhtenäinen* jos kaikille u, $v \in V$ on olemassa polku $u \to v$.

Suunnatuille graafeille G määritellään yleensä ainakin kaksi erilaista yhtenäisyyden käsitettä. *Vahva yhtenäisyys* merkitsee, että kaikille pistepareilla u, $v \in V$ on olemassa polut $u \to v$ ja $v \to u$, kun taas *heikko yhtenäisyys* merkitsee sitä, että G:n symmetrinen sulkeuma on yhtenäinen.

Määritelmä 66. Olkoon G leimattu graafi ja

$$\Pi : v_0 \xrightarrow{e_1} \ldots \xrightarrow{e_n} v_n$$

n-pituinen polku G:ssä missä $e_i = l(v_{i-1}, v_i)$ on nuolen (v_{i-1}, v_i) leima. Tällöin polun Π leima $l(\Pi)$ on jono $(e_1, \ldots, e_n)$

Esimerkki 81. Esimerkin 75 graafissa 3-pituisen polun

$$\Pi : \text{Turku} \to \text{Tampere} \to \text{Jyväskylä} \to \text{Oulu},$$

leima on $(120, 120, 240)$. Tässä tapauksessa leima-alkioiden summa edustaa matka-aikaa polun alkupisteestä päätepisteeseen.

Määritelmä 67. Polku $\Pi : v_0 \to v_1 \to \ldots \to v_n$ graafissa G on *sykli*, jos $v_0 = v_n$.

Esimerkki 82. Esimerkin 75 graafissa on mm. sykli (leimat merkitty myös)

$$\text{Tampere} \xrightarrow{170} \text{Vaasa} \xrightarrow{200} \text{Jyväskylä} \xrightarrow{200} \text{Helsinki} \xrightarrow{120} \text{Tampere}.$$

Tämän syklin leima on $(170, 200, 200, 120)$, ja leima-alkioiden summa edustaa syklin läpikulkuun menevää aikaa.

Kurssikokonaisuuden seuraavassa osassa nähdään minkälainen yhteys kahden näennäisesti erilaisen matematiikan käsitteen: graafin ja matriisin välillä vallitsee. Tässä osiossa tyydytään toistaiseksi edellämainittuun deskriptiiviseen esitykseen, josta seuraavassa luvussa esitetään tärkeä erikoistapaus.

5.2 Puut

Teoreettisessa tietojenkäsittelyssä, erityisesti tietorakenteissa käytettävä käsite *puu* (eng. *tree*) on erittäin tärkeä erikoistapaus graafista ja ansaitsee siksi oman osionsa.

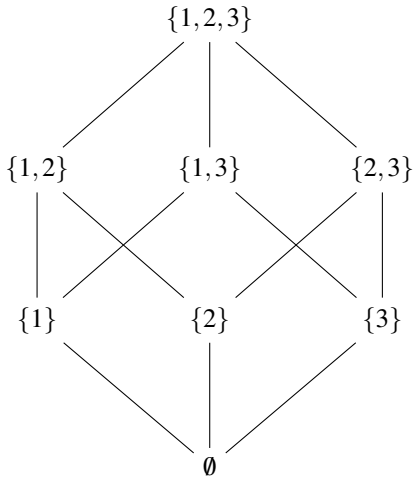
Seuraavassa määritelmässä käsitetään graafi leimattomana ja suuntaamattomana.

Määritelmä 68. Puu on yhtenäinen graafi, jossa ei ole syklejä.

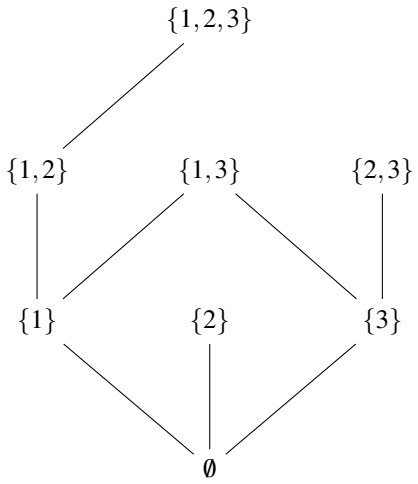
Huomautus 53. Ylläoleva määritelmä on yhtäpitävä seuraavan kanssa: Puu on yhtenäinen (suuntaamaton) graafi, jossa kahden eri pisteen välillä on tarkalleen yksi polku. Jos nimittäin kahden pisteen u ja v välillä olisi kaksi erilaista polkua $u \xrightarrow{P_1} v$, ja $u \xrightarrow{P_2} v$, saataisiin sykli $u \xrightarrow{P_1 P_2^{-1}} u$, missä $P_1 P_2^{-1}$ tarkoittaa polkua, jossa ensin kuljetaan P_1 ja sen jälkeen P_2 takaperin.

Jos taas (suuntaamattomassa) graafissa olisi sykli $u \xrightarrow{C} u$, voidaan valita mikä hyvänsä sykliin kuuluva piste v ja jakaa sykli kahteen osaan: $u \xrightarrow{C_1} v \xrightarrow{C_2} u$, jolloin pisteiden u ja v välillä on kaksi eri polkua, C_1 ja C_2^{-1}.

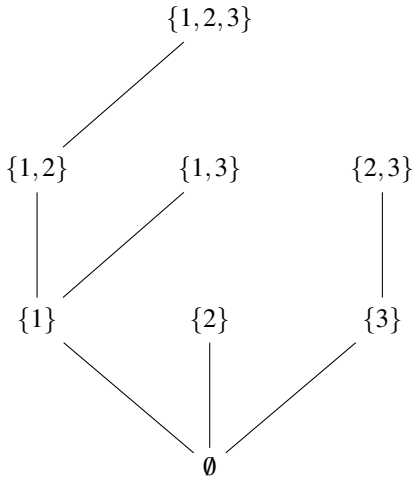
Esimerkki 83. Esimerkin 10 kuvio on suunnattu graafi, jonka symmetrinen sulkeuma voidaan esittää alla olevan kuvan mukaisesti. Kyseessä ei ole puu, koska esim. $\{1,2,3\} \to \{2,3\} \to \{3\} \to \{1,3\} \to \{1,2,3\}$ on sykli.



Esimerkki 84. Myöskään seuraava graafi ei ole puu, koska $\{1,3\} \to \{3\} \to \emptyset \to \{1\} \to \{1,3\}$ on sykli.



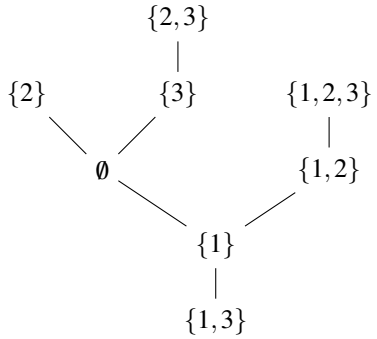
Esimerkki 85. Alla oleva graafi on puu, koska siinä ei ole yhtään sykliä.



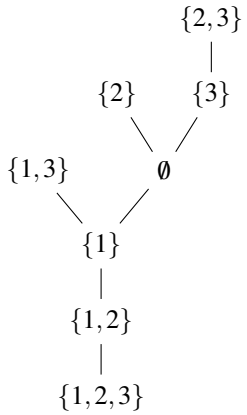
Huomautus 54. Jos graafi T on puu, voidaan mikä hyvänsä T:n piste valita ns. *juureksi*, josta on yksikäsitteinen polku mihin hyvänsä muuhun graafin pisteeseen. Juuresta lähtevien polkujen päätepisteitä kutsutaan *lehdiksi*.

Esimerkki 86. Jos esimerkin 85 puussa valitaan juureksi $\emptyset$, ovat lehtiä $\{1,2,3\}$, $\{1,3\}$, $\{2\}$ ja $\{2,3\}$.

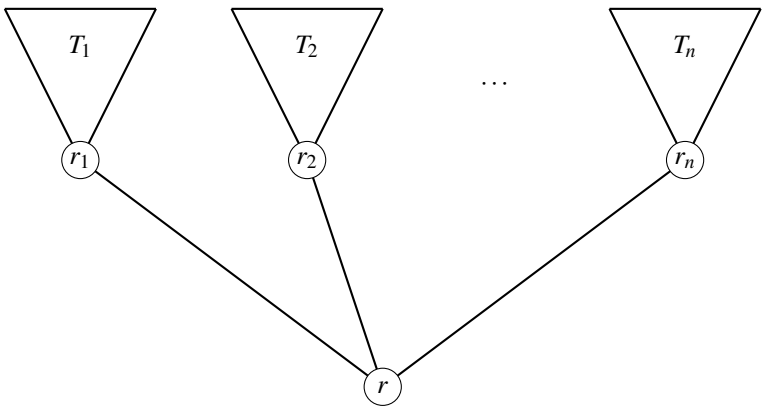
Jos taas juureksi valitaan $\{1,3\}$, ovat lehtinä pisteet $\{2\}$ ja $\{2,3\}$, $\{1,2,3\}$. Havainnollisuuden vuoksi tällöin piirretään graafi uudelleenjärjestettynä alla olevaan visuaaliseen esitysasuun:



Jos juureksi valitaan $\{1,2,3\}$, ovat lehtiä $\{1,3\}$, $\{2\}$ ja $\{2,3\}$ ja tyypillinen visuaalinen esitysasu saa allaolevan muodon:

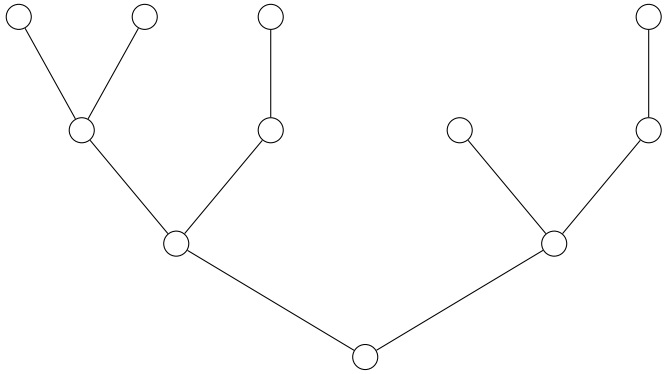


Huomautus 55. Edellisten esimerkkien valossa puun graafinen esitysasu voidaan aina saattaa allaolevaan muotoon: Kiinnitetään jokin pisteistä r juureksi ja sijoitetaan se alimmalle tasolle. Tästä seuraavaksi ylemmälle tasolle sijoitetaan kaikki ne pisteet $r_1, \ldots, r_n$, joille on olemassa viiva $r - r_i$ ja näin jatketaan alipuille $T_1, \ldots, T_n$. Alipuulla T_i tarkoitetaan alkuperäisen graafin osaa, joihin on olemassa polku pisteestä r_i.



Tämä menetelmä puun graafisen esitysasun tuottamiseksi toimii, koska alunperinkin graafi oli puu, eli syklejä ei ole olemassa. Tästä seuraa, että $T_1, \ldots, T_n$ ovat paitsi erillisiä graafeja, myös puita, ja niiden juuriksi voidaan valita $r_1, \ldots, r_n$.

Piirrosprosessin päättyessä puun graafinen esitysasu näyttää tyypillisesti seuraavalta: Juuri on alinna ja lehdet ylinnä, juuresta on yksikäsitteinen polku jokaiseen lehteen.



Huomautus 56. Olkoon $T = (V,E)$ on puu, jonka juureksi on kiinnitetty piste r. Tällöin T määrittelee osittaisen järjestyksen $\preceq$ pisteidensä V joukossa seuraavasti:

$v_1 \preceq v_2$
$\Leftrightarrow$ Joko $v_1 = v_2$ tai on olemassa polku $r \to v_1 \to v_2 \to l$ juuresta r lehteen l.
Voi olla myös $v_2 = l$.

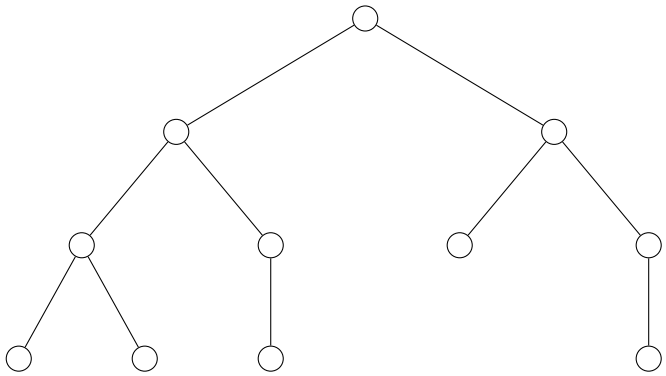
Huomautus 57. Oletetaan, että puussa $T = (V,E)$ on määritelty Huomautuksen 56 mukainen järjestys $\preceq$. Tällöin seuraavat ehdot toteutuvat:

- Kaikille $v \in V$ joukko $V_v = \{u \in V \mid u \preceq v\}$ on hyvinjärjestetty.
- Kaikilla hyvinjärjestetyillä joukoilla V_v on sama minimaalinen alkio (juuri).

Puukäsite on itse asiassa mahdollista määritellä tässä huomautuksessa mainituilla ominaisuuksilla.

Edellä esitetty tapa kuvata puita visuaalisesti juuri alhalla ja lehdet ylhäällä on toki sopusoinnussa kasvitieteellisen puun käsitteen kanssa, ja siihenhän matemaattiseen puukäsitteeseen liittyvät nimitykset juuri ja lehdet ilman muuta perustuvat.

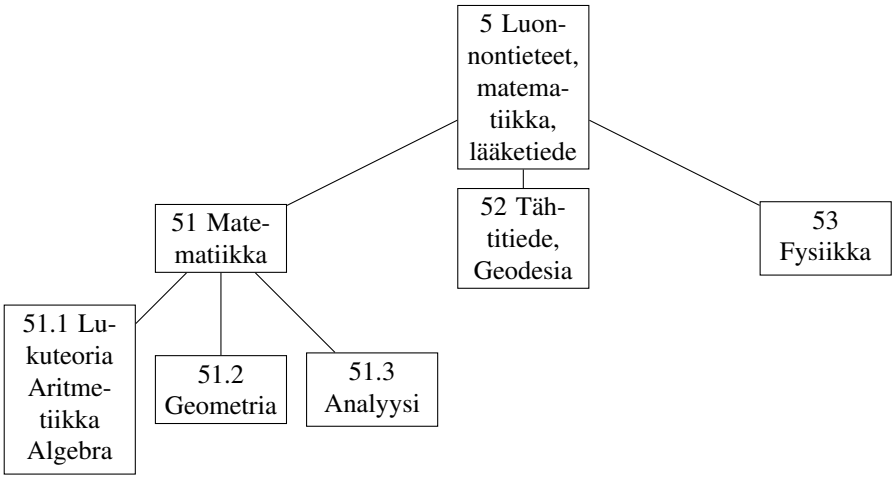
Vaikka kasvitieteen näkökulmasta puut suuntaavat juurensa alaspäin ja lehtensä ylöspäin, ei näin ole kuitenkaan useissa matematiikan tai teoreettisen tietojenkäsittelyn malleisssa. Näissä päinvastoin on tapana kuvata puita biologisen esikuvan peilikuvana, juuri ylhäällä ja lehdet alhaalla seuraavan kuvan mukaisesti.



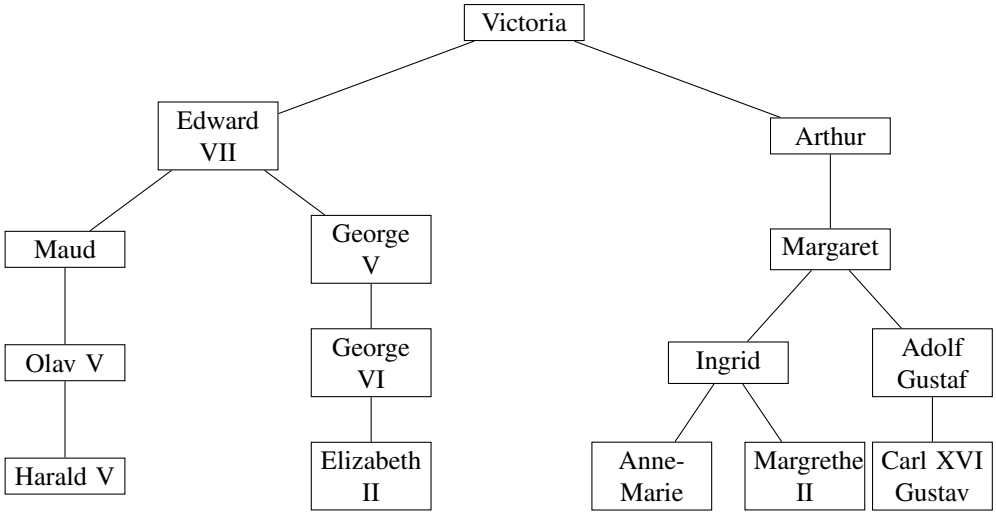
Graafeja ja puurakennetta voidaan käyttää jäsentelemään monia erilaisia suhteita. Usein esiintyviä ovat esimerkiksi

Tietokoneen kovalevyn hakemistohierarkia (juurikansio > kansio > kansio > ... > tiedosto (lehti))

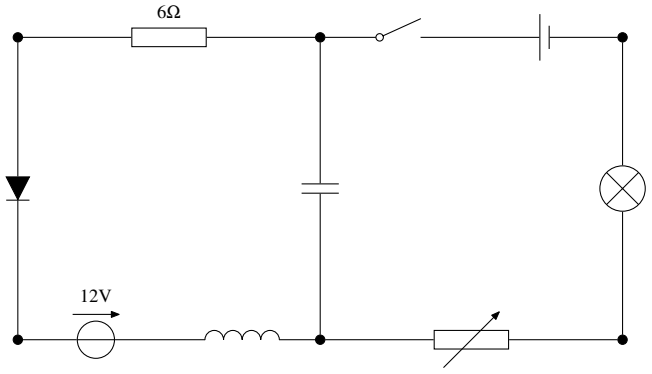
Kirjaston luokitukset:



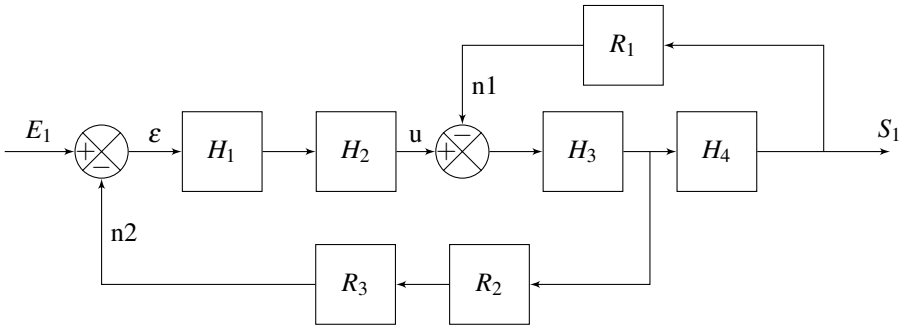
Sukupuu:



Piiirikaaviot ovat graafeja. Mieti mitä ovat pisteet ja mitä viivat.



Tekniikassa esiintyvät lohkokaaviot ovat niinikään graafeja. Mieti miten nämä jäsennellään graafiteorian käsitteiksi.



Propositiologiikan kaavat voidaan esittää puurakenteen avulla.

5.3 Graafin vierusmatriisi