

Mika Hirvensalo

Insinöörimatematiikka A 2018

Sisällys

1	Johdanto	5
1.1	Matematiikasta ja sen opiskelusta	5
1.2	Matematiikan merkinnöistä	6
1.2.1	Kreikkalaiset aakkoset	6
1.2.2	Joukko-opin ja logiikan merkinnöistä	6
1.2.3	Summa- ja tulomerkinnät	7
1.3	Lausekkeiden suuruusarvioista	8
2	Logiikan alkeita	9
2.1	Matematiikan perusteista	9
2.2	Päätelyn muotoja	12
2.3	Predikaattilogiikkaa	13
2.3.1	Predikaattilogiikan syntaksi	15
2.3.2	Predikaattilogiikan semantiikka	16
2.3.3	Looginen seuraus	22
2.3.4	Gentzenin luonnollisen deduktion järjestelmä	23
2.4	Deduktion esittäminen käytännössä	28
2.5	Propositilogiikkaa	29
2.6	Induktioperiaate	31
2.7	Induktiotodistuksia	31
3	Joukko-oppia	37
3.1	Joukko-opin peruskäsitteet	37
3.2	Tärkeimmät lukujoukot	38
3.3	Joukkojen väliset suhteet ja operaatiot	39
3.4	Perusjoukko ja komplementti	40
3.5	Osittelulait ja De Morganin lait	41
3.6	Vennin Diagrammit	41
4	Relaatiot ja funktiot	43
4.1	Karteesinen tulo	43
4.2	Relaatio, relaatioiden yhdistäminen, käänteisrelaatio	45
4.3	Funktion määritelmä	51
4.4	Funktioiden ominaisuuksia	51
5	Yleisimmät reaalfunktiot	55
5.1	Reaalfunktioiden esitystapoja ja ominaisuuksia	55
5.2	Algebralliset funktiot	55
5.3	Eksponentti- ja logaritmifunktiot	57
5.4	Trigonometriset funktiot	59

6	Kompleksiluvut	63
6.1	Kompleksilukujen määritelmä ja peruslaskutoimitukset	63
6.2	Kompleksilukujen graafinen esitys, itseisarvo ja polaariesitys	64
6.3	Kompleksinen eksponenttifunktio ja logaritmi	67
6.4	Kompleksinen potenssinkerotus	68
6.5	Kompleksilukujen trigonometriset funktiot	70
6.6	Algebran peruslause	71
7	Lineaaristen yhtälöryhmien ratkaiseminen	75
7.1	Matriisilaskennan peruskäsitteet	75
7.2	Gaussin-Jordanin menetelmä	80
7.3	Ratkaisujoukon systemaattinen esittäminen	86
8	Osamurtohajotelmat	89
8.1	Polynomien tekijöihinjaosta	89
8.2	Menetelmiä tekijöihinjakoon	93
8.3	Yleinen osamurtohajotelma	94

Luku 1

Johdanto

Opintokokonaisuuden Insinöörimatematiikka A, B, C ja D tarkoitus on esittää perustiedot valikoiduista differentiaali- ja integraalilaskennan työkaluista, joita sovelletaan teknisillä aloilla. Näitä ei kuitenkaan ryhdytä käsittelemään heti osassa A, vaan tämän osan aluksi esitellään matematiikan perusteita kuten logiikkaa, matemaattista päättelyä, joukko-oppia, funktioiden peruskäsitteitä ja kompleksilukujen perusteita. Näistä lähtökohdista päästään kursseilla Insinöörimatematiikka B, C ja D käsittelemään differentiaali- ja integraalilaskennan rakennetta ja sovelluksia, Fourier-analyysiä, integraalimuunnoksia, kuin myös edellämainittujen menetelmien yhdistämistä lineaarialgebraan.

Pohjatiedoiksi kurssille Insinöörimatematiikka A tarvitaan lukiokurssien laajan matematiikan tuntemus. Osallistujien otaksutaan hallitsevan ainakin alkeellisen joukko-opin, itseisarvon käsitteen, tavanomaiset polynomit, juurenoton, murtolausekkeet, potenssi- ja eksponenttimerkinnät, algebrallisten lausekkeiden käsittely- ja sievennyssäännöt, perusmenetelmiä yhtälöiden ratkaisemiseksi, epäyhtälöiden käsittelysäännöt, yksinkertaisten epäyhtälöiden ratkaisumenetelmiä, trigonometrisien ($\sin$, $\cos$, $\tan$), eksponentti- ja logaritmifunktioiden (e^x , $\ln x$) perusominaisuudet.

1.1 Matematiikasta ja sen opiskelusta

Encyclopædia Britannican mukaan matematiikka on rakennetta, järjestystä ja suhteita käsittelevä tiede, joka on kehittynyt yksinkertaisesta lukumäärien laskemisesta, mittaamisesta ja muotojen kuvailusta.

Laskemisen taito on selvästi vanhempi kuin kirjoitustaito ja siksi matematiikan syntyä ei voida ajoittaa historian tutkimuksen keinoin. Varhaisin laskemiseen viittaava arkeologinen löydös on ajoitettu noin 35 000 vuoden taakse, mutta vanhimmat säilyneet kirjalliset dokumentit varsinaisen matematiikan harjoittamisesta ovat peräisin Egyptistä noin neljän vuosituhannen takaa. Ajanlaskumme alkua edeltävinä vuosisatoina matematiikka nousi kreikkalaisessa kulttuurissa kukoistukseen, jolle ei löytynyt vertaista ennen uuden ajan alkua. Vasta 1600-luvulla alkanut ja nykypäiviin jatkuva matematiikan nousukausi ylitti muinaisten kreikkalaisten saavutukset.

1800-luvun puolivälin jälkeen alkaneen kehityksen myötä matematiikka on jakautunut kymmeneen, jopa satoihin osa-alueisiin, ja ensikatsomalta saattaa näyttää, että joillakin alueilla on varsin vähän tekemistä toistensa kanssa. Syvällisempi perehtyminen kuitenkin paljastaa, että eri osa-alueita yhdistävät useat rakenteelliset piirteet.

Laajojen matematiikan kokonaisuuksien omaksuminen yleensä helpottuu, mikäli pelkkien laskumenetelmien lisäksi perehdytään myös perusteisiin. Insinöörimatematiikan opintokokonaisuus poikkeaa lukiomatematiikan kursseista luultavasti eniten siinä, että tällä kurssikokonaisuudella perehdytään matematiikan rakenteisiin lukiokursseja syvällisemmin. Kurssin ensimmäinen mieleenpainettava asia onkin seuraava: **ainoa keino matematiikan kunnolliseen osaamiseen kulkee perusteiden ja käsitteiden hyvän hallinnan kautta.**

Tämän kurssin opinnot jakautuvat luentoihin ja harjoitustehtäviin. Yleisesti hyväksi koetun käytännön mukaan harjoitustehtävien yhteydessä kannattaa varmistaa, että ratkaisun perustelut tulivat ymmärretyksi. Matematiikan opinnoissa pidetään yleensä oikeita perusteluja tärkeämpinä kuin virheetöntä ratkaisua, sillä oikeiden perustelujen myötä saatu virheellinen ratkaisu johtuu usein helposti korjattavissa olevasta erehdyksestä. Sen sijaan virheelliset perustelut voivat johtaa oikeaan ratkaisuun vain sattumalta.

1.2 Matematiikan merkinnöistä

1.2.1 Kreikkalaiset aakkoset

Matematiikan ohella useilla luonnontieteen aloilla käytetään kreikkalaisia aakkosia, jotka on siis syytä opetella. Joistakin pienistä kirjaimista käytetään kahta eri muotoa.

alfa	$A \alpha$	iota	$I \iota$	rho	$P \rho$
beta	$B \beta$	kappa	$K \kappa, \varkappa$	sigma	$\Sigma \sigma, \varsigma$
gamma	$\Gamma \gamma$	lambda	$\Lambda \lambda$	tau	$T \tau$
delta	$\Delta \delta$	myy	$M \mu$	ypsilon	$\Upsilon \upsilon$
epsilon	$E \varepsilon$	nyy	$N \nu$	fii	$\Phi \phi, \varphi$
zeeta	$Z \zeta$	ksii	$\Xi \xi$	khii	$X \chi$
eeta	$H \eta$	omikron	$O o$	psii	$\Psi \psi$
theeta	$\Theta \theta, \vartheta$	pii	$\Pi \pi, \varpi$	oomega	$\Omega \omega$

1.2.2 Joukko-opin ja logiikan merkinnöistä

Äärellisen tai numeroituvan äärettömän joukon merkitsemiseen käytetään aaltosulkeita: $A = \{1, 2, 3\}$, $B = \{3, 4\}$ tai $\mathbb{N} = \{1, 2, 3, \dots\}$. Joukkoon kuulumisesta käytetään merkintää $\in$ ja päinvastaisesta merkintää $\notin$. Esimerkiksi $2 \in A$, mutta $2 \notin B$. Tyhjästä joukosta, johon ei kuulu yhtään alkioa, käytetään merkintää $\emptyset$. Tätä merkintää ei tule sekoittaa kreikkalaisen aakkoston ϕ -kirjaimeen.

Tavallisimmat joukkojen väliset operaatiot ovat

- Unioni eli yhdiste. Esimerkiksi $A \cup B = \{1, 2, 3, 4\}$
- Intersektio eli leikkaus. Esimerkiksi $A \cap B = \{3\}$
- Differenssi eli erotus. Esimerkiksi $A \setminus B = \{1, 2\}$.

Joukko-oppia käsitellään enemmän luvussa 3.

Yleisimmät logiikan merkinnät ovat *konnektiivit*

- $\wedge$ (konjunktio eli looginen ja)
- $\vee$ (disjunktio eli looginen tai)
- $\neg$ (negaatio eli looginen ei)
- $\rightarrow$ (implikaatio eli looginen seuraus)

sekä *kvanttorit*

- $\forall$ (universaalikvanttori)
- $\exists$ (eksistentiaalikvanttori)

Logiikkaa käsittelevissä luvuissa täsmennetään ylläolevia merkintöjä, mutta toistaiseksi merkinnät käsitellään intuitiivisesti. Jos siis P ja Q ovat väitelauseita, merkitsee esimerkiksi $P \wedge Q$ yhdistettyä väitelausetta ” P ja Q ”, kun taas $\neg P$ tarkoittaa P :lle vastakkaista väitettä. $P \rightarrow Q$ voidaan lukea ”jos P niin Q ”.

Kvanttorit tulkitaan siten, että $(\forall x)P(x)$ tarkoittaa ”kaikille x :ille pätee $P(x)$ ” ja $(\exists x)P(x)$ ”on olemassa x jolle pätee $P(x)$ ”. On huomattava, että merkintää $\Rightarrow$ käytetään osoittamaan loogista seurausta aivan kuten konnektiivia $\rightarrow$, mutta tällä kurssilla $\rightarrow$ on varattu muodollisten loogisten väittämien yhdistämiseen, kun taas merkintää $\Rightarrow$ käytetään osana matemaattisesti varustettua suomen kieltä.

Esimerkki 1.

$$a = b \Rightarrow a + 1 = b + 1$$

on suomen kielen lause, jossa kerrotaan että ehdosta $a = b$ seuraa ehto $a + 1 = b + 1$. Sen sijaan $a + b \rightarrow a + 1 = b + 1$ on predikaattilogiikan (perehdytään myöhemmin) kaava, johon ei välttämättä katsota sisältyvän luonnollisen kielen elementtejä.

1.2.3 Summa- ja tulomerkinnät

Summa- ja tulomerkinnät Σ ja Π ja niiden käsittelysäännöt saavat lukiokurssissa yleensä vain vähän huomiota. Näitä merkintöjä käytetään kuitenkin hyvin yleisesti ja siksi niihin on syytä perehtyä.

Summa voidaan merkitä lyhyemmin

$$a_1 + a_2 + \dots + a_n = \sum_{i=1}^n a_i$$

ja tulo

$$a_1 \cdot a_2 \cdot \dots \cdot a_n = \prod_{i=1}^n a_i.$$

Tässä luvussa käsitellään jatkossa ainoastaan summamerkinnän manipulointia, koska vastaavat käsittelysäännöt voidaan saada helposti myös tulolle.

Summausindeksi i valinta ei ole tärkeä, yhtä hyvin yllä oleva summa voitaisiin kirjoittaa muodossa $\sum_{k=1}^n a_k$, tärkeää on ainoastaan, että summausindeksiä ei voi vahingossa sekoittaa johonkin toiseen lausekkeissa esiintyvään muuttujaan tai vakioon. Erityisesti kompleksilukujen yhteydessä (luku 6) pitää karta i :n käyttöä indeksinä. Summamerkinnän ideana on, että summausindeksi juoksee läpi esiintyvien lukujen $a_1, \dots, a_n$ indeksoinnin luvusta 1 lukuun n , ja tämä ilmaistaan summamerkin Σ ala- ja yläpuolella olevilla rajoitteilla ” $i = 1$ ” ja ” n ”.

Summamerkintää käyttäen voidaan vaikkapa n :n ensimmäisen kokonaisluvun summa kirjoittaa lyhyempään muotoon:

$$1 + 2 + \dots + n = \sum_{i=1}^n i.$$

On kuitenkin huomattava, että kyseessä on vain merkintätapa, eikä se anna mitään keinoa näyttää toteen, että

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

mikä kyllä pitää paikkansa. Tällä kurssilla esitetään menetelmiä, joilla yllä oleva yhtälö voidaan todistaa oikeaksi.

Summamerkinnän käsittelyyn liittyvät säännöt saadaan suoraan yleisistä summia koskevista säännöistä sekä summamerkinnän määrittelystä. Esimerkiksi tavanomainen osittelulain soveltaminen

$$c(a_1 + a_2 + \dots + a_n) = ca_1 + ca_2 + \dots + ca_n$$

voidaan summamerkintää käyttäen kirjoittaa muotoon

$$c \sum_{i=1}^n a_i = \sum_{i=1}^n ca_i.$$

Samoin summattavien jäsentely

$$(a_1 + a_2 + \dots + a_n) + (b_1 + b_2 + \dots + b_n) = (a_1 + b_1) + (a_2 + b_2) + \dots + (a_n + b_n)$$

saa muodon

$$\sum_{i=1}^n a_i + \sum_{i=1}^n b_i = \sum_{i=1}^n (a_i + b_i).$$

Edelleen, summamerkintä voidaan aina ”katkaista”: jos $1 < m < n$, voidaan tietysti kirjoittaa

$$a_1 + \dots + a_n = a_1 + \dots + a_m + a_{m+1} + \dots + a_n,$$

mikä voidaan edelleen lyhentää muotoon

$$\sum_{i=1}^n a_i = \sum_{i=1}^m a_i + \sum_{i=m+1}^n a_i.$$

Summausindeksin muutos on suora seuraus merkintätavasta:

$$\sum_{i=1}^n a_i, \quad \sum_{i=2}^{n+1} a_{i-1}, \quad \text{ja} \quad \sum_{i=0}^{n-1} a_{i+1}$$

tarkoittavat samaa asiaa. Yleisenä sääntönä pätee, että summausmerkinnän ylä- ja alarajaa voidaan nostaa yhdellä, jos summalausekkeessa esiintyvistä indeksistä vähennetään yksi. Samoin summausmerkinnän rajoja voidaan laskea yhdellä, jos summalausekkeen indeksiin lisätään ykkönen. Tarvitessa summamerkinnän rajan nostoa tai laskua voidaan tietenkin soveltaa useamman kerran peräkkäin.

1.3 Lausekkeiden suuruusarvioista

Differentiaali- ja integraalilaskennan perusteiden hallinnan vuoksi on välttämätöntä tuntee joitakin yksinkertaisia sääntöjä, joilla lausekkeiden suuruutta voidaan arvioida. Tarvittavat säännöt voidaan tiivistää seuraaviin muotoihin.

- Summa ei pienene jos summattavia ei pienennetä. Symbolein tämä voidaan merkitä seuraavasti: Jos $A \leq C$ ja $B \leq D$, niin

$$A + B \leq C + D.$$

Vastaava sääntö voidaan kirjoittaa myös tapauksessa, jossa summattavia ei suurenneta.

- Positiivisten lukujen tulo ei pienene jos tekijöitä ei pienennetä: Jos $0 \leq A \leq C$ ja $0 \leq B \leq D$, niin

$$AB \leq CD.$$

Yllä olevia sääntöjä sovellettaessa sanotaan, että A :ta on *arvioitu ylöspäin* C :ksi ja B :tä D :ksi. Säännöt yleistyvät suoraviivaisesti myös tapaukseen, jossa summattavia tai tulon tekijöitä on enemmän kuin kaksi.

- Positiivisten lukujen osamäärä ei pienene, jos osoittajaa ei pienennetä ja nimittäjää ei suurenneta: Jos $0 \leq A \leq C$ ja $B \geq D > 0$, niin

$$\frac{A}{B} \leq \frac{C}{D}.$$

Vastaava sääntö voidaan kirjoittaa myös tapaukselle, jossa osoittajaa pienennetään ja nimittäjää suurennetaan.

- Niin kutsuttu *kolmioepäyhtälö* $|A + B| \leq |A| + |B|$ seuraa edellisistä ja itseisarvon määritelmästä, mutta se on joka tapauksessa hyvä painaa mieleen jo tässä vaiheessa.

Paitsi differentiaali- ja integraalilaskennan perusteissa, voidaan edellämainittuja sääntöjä käyttää myös yksinkertaisten johtopäätösten tekemiseen.

Esimerkki 2.

$$\frac{1}{1} > \frac{1}{2} > \frac{1}{3} > \frac{1}{4} \dots$$

Esimerkki 3. Jos $0 \leq x \leq 1$, on $x^2 = x \cdot x \leq x \cdot 1 = x$, siis käyrä $y = x^2$ on suoran $y = x$ alapuolella, kun $0 \leq x \leq 1$.

Esimerkki 4. Olkoon n parillinen. Tällöin

$$\begin{aligned} 1 + 2 + 3 + \dots + n &= 1 + 2 + \dots + \frac{n}{2} + \left(\frac{n}{2} + 1\right) + \dots + n \\ &\geq 0 + 0 + \dots + 0 + \frac{n}{2} + \dots + \frac{n}{2} = \frac{n}{2} \cdot \frac{n}{2} = \frac{n^2}{4}, \end{aligned}$$

kun taas

$$1 + 2 + 3 + \dots + n \leq n + n + n + \dots + n = n \cdot n = n^2.$$

Esimerkki 5. Koska $-1 \leq \sin x, \cos x \leq 1$, on

$$\frac{4 \cos^2 x}{3 + \sin x} \leq \frac{4}{3 - 1} = 2.$$

Luku 2

Logiikan alkeita

2.1 Matematiikan perusteista

Matematiikka eroaa luonnontieteistä (esim. fysiikka, kemia, biologia) ja yhteiskuntatieteistä (esim. sosiologia, taloustiede) oleellisesti siinä, että matematiikan väitteitä ei voida todentaa (*verifoida*) tai kumota (*falsifoida*) empiirisesti, siis havaintojen perusteella. Tämä voidaan ilmaista myös siten, että matematiikan käsitteitä ei kytketä reaali maailman olioihin operationaalisesti.

Historiallisesta näkökulmasta katsoen on huomautettava että matemaattiset teoriat tosin yleensä muodostetaan jonkin konkreettisen tarpeen mukaan. Tällöin myös peruskäsitteet, -ominaisuudet ja -suhteet yleensä syntyvät reaali maailman olioista abstraktion (jota suomeksi voitaneen kutsua rakenteiden ja niiden ominaisuuksien tiivistämiseksi tai pelkistämiseksi) kautta. Esimerkiksi lukumäärän käsite on tunnettu jo ihmiskunnan esihistoriassa, mutta *lukuja* yksi, kaksi, kolme, jne. ei sellaisenaan ole fysikaalisina olioina olemassa. Ne ovat ainoastaan ihmismielen abstrakteja eli tiivistettyjä kuvia reaali maailmassa esiintyvistä konkreettisista käsitteistä. Vaikka matemaattisten objektien kuten lukujen toivotaan kuvaavan hyvin reaali maailman asiantiloja (esim. lukumääriä ja niiden yhdistämistä lisäämällä, kertomalla tai vähentämällä), ei matematiikan luku- tai muidenkaan käsitteiden ominaisuuksia voida silti yleisesti perustella havaintojen pohjalta. Havainnot voivat kyllä tukea ja joissain tapauksissa myös kumota matemaattisen väittämän, mutta tyypillisin ongelma nousee siitä tosiseikasta, että matemaattiset teoriat pyrkivät yleensä puhumaan *äärettömästä* määrästä tapauksia, kun taas havainnot voivat kattaa vain äärellisen määrän.

Esimerkki 6. Lukujen liitännäislaki eli *assosiatiivisuus* tarkoittaa sitä, että

$$(a + b) + c = a + (b + c), \quad (2.1)$$

olivatpa a , b ja c mitä hyvänsä lukuja. Kun $+$ ymmärretään tavallisena yhteenlaskuna, on hyvin ymmärrettävää, että assosiatiivisuus pätee kaikille reaali maailman lukumäärille. Sen sijaan assosiatiivisuus *matemaattisena* väittämänä ei ole itsestään selvä, sillä luvut a , b , ja c pitää ymmärtää reaali maailmasta riippumattomiksi olioiksi. Sama pätee abstraktien olioiden a , b ja c yhteenlaskulle: sen matemaattinen muoto ei ole konkreettista lukumäärien yhdistämistä, koska matemaattisessa maailmassa a , b ja c ovat vain lukumäärien ideaalisia vastineita, eivätkä lukumääriä. Tämän vuoksi liitännäislakia (2.1) ei voida matemaattista teoriaa muodostettaessa pitää itsestään selvänä, vaan se pitää kirjata teorian perusominaisuudeksi, *aksiomaksi*. Vaihtoehtoisesti perusominaisuudeksi voidaan kirjata jokin muu, josta (2.1) loogisesti seuraa.

Matemaattisessa teoriassa tärkeämpää kuin itse oliot ovat aina niiden väliset *suhteet ja operaatiot*. Juuri tämän vuoksi matematiikan sanotaan olevan *suhteen, rakenteen ja järjestyksen* tiede. Käsiteltävien perusolioiden *ontologialla* eli olemassaolon luonteella ei ole merkitystä, vaan ainoastaan sillä, miten matemaattiset objektit toisiinsa suhtautuvat. Esimerkiksi luonnollisten lukujen teorian ymmärtämisen kannalta ei ole tärkeää saavuttaa ymmärtämystä luonnollisten lukujen olemuksesta, siis siitä *mitä* objektit 1, 2, 3, ... ovat, vaan siitä, mitkä ovat niiden väliset operaatiot ja suhteet. Tietysti perusolioista määritelmien kautta rakennettavien olioiden luonteella on merkitystä, mutta vain määritelmän ymmärtämisen kannalta. Esimerkiksi *matriisi* määritellään eräntyypyisenä reaali luku-kaaviona, ja tällöin tulee ymmärtää mitä reaali lukujen sijoittuminen kaavioon merkitsee matriisiope- raatioiden kannalta.

Kaikki matemaattiset teorit voidaan esittää *aksiomaattis-deduktiivisessa* muodossa, jossa teorian perusoloiden ja -suhteiden olemassaolo esitetään määritelmänä tai *aksioomina* eli perusväittämänä. Muut teorian väittämät eli *lauseet* eli *teoreemat* johdetaan loogisesti eli *dedusoidaan* aksioomista tai jo aiemmin dedusoiduista väittämistä. Matemaattinen *teoria* tarkoittaa niiden lauseiden joukkoa, jotka voidaan aksioomista johtaa.

Esimerkki 7. Luonnollisten lukujen teoriassa voidaan peruskäsitteiksi valita luvut 1, 2, 3, ... ja niiden yhteenlasku $+$. Yhdeksi teorian aksioomaksi voidaan valita liitännäislaki (2.1). Yleensä näin ei kuitenkaan tehdä, vaan luonnollisten lukujen teoria perustetaan vielä alkeellisempiin käsitteisiin. Nämä esitetään esimerkissä 8.

Matemaattisen teorian kannalta on tärkeää, että teorian peruskäsitteet ja aksioomat olisivat mahdollisimman yksinkertaiset, sillä abstraktista olemuksesta huolimatta matemaattisen teorian toivotaan yleensä kuvaavan mahdollisimman hyvin jotain fyysiseen maailmaan liittyvää asiaa. Jos teorian peruskäsitteet ja aksioomat ovat mahdollisimman harvalukuiset ja yksinkertaiset, on helpompaa varmistua siitä, että ne kuvaavat tarkasti toivottuja fyysikaalisen maailman olioita.

Toinen syy aksioomajärjestelmien yksinkertaisuuspyrkimykseen on seuraava: osoittautuu, että jos teorian aksioomat ovat *ristiriitaiset*, voidaan niistä loogisesti johtaa mitä hyvänsä. Erityisesti voidaan johtaa mikä hyvänsä väitelause ja sen kielto. Teoriaa ei siis voida pitää hyväksyttävänä (tai edes mielenkiintoisena), jos sen aksioomat ovat keskenään ristiriitaiset.

Tämän vuoksi teorian aksioomien yksinkertaisuus on erittäin suotavaa: on uskottavaa, että ristiriitaisuudet näkyvät helpommin, mikäli aksioomat ovat yksinkertaisia. Ikävä kyllä tämä pitää paikkansa vain äärimmäisen yksinkertaisissa matemaattisissa teorioissa. Yleensä ristiriidattomuus on erittäin hankalasti (jos lainkaan) todennettavissa: 1900-luvulla matematiikan perusteiden tutkimus on osoittanut, että lähes kaikkien mielenkiintoisten matemaattisten teorioiden aksioomajoukkojen ristiriidattomuutta ei voida teoriassa itsessään lainkaan todentaa. Ns. Gödelin toisen epätäydellisyyslauseen mukaan teorian ristiriidattomuutta ei teorian puitteissa voida todentaa, jos teoria on kyllin rikas puhuakseen luonnollisista luvuista.

Esimerkki 8 (Giuseppe Peanon aksiomatisointi luonnollisille luvuille). Luonnollisten lukujen teorian *peruskäsitteet* ovat joukko $\mathbb{N}$, luonnollinen luku $1 \in \mathbb{N}$ ja luonnollisen luvun n seuraaja $s(n)$. Teorian aksioomat ovat seuraavat:

1. Jos $n \neq m$, niin $s(n) \neq s(m)$ (kahdella eri luonnollisella luvulla on eri seuraaja).
2. Kaikille joukon $\mathbb{N}$ alkioille n pätee $s(n) \neq 1$ (ykkönen ei ole minkään luonnollisen luvun seuraaja).
3. Jos joukko A sisältää luvun 1 ja jokaisen sisältämänsä luvun seuraajan, niin silloin A sisältää kaikki luonnolliset luvut (*induktioaksiooma*).

Näistä peruskäsitteistä ja aksioomista lähtien johdetaan kaikki luonnollisten lukujen ominaisuudet. Esimerkiksi yhteenlaskun määrittely voidaan aloittaa määrittelemällä $1 + n = n + 1 = s(n)$ ja laajentaa tästä koskemaan kaikkia summia $n + m$. Samoin käsitteet *suurempi kuin* ja *pienempi kuin* voidaan määritellä käyttäen pelkästään mainittuja peruskäsitteitä.

Vaikka Peanon aksioomat ovat yksinkertaiset, ei niiden ristiriidattomuutta voida todentaa perinteisen matematiikan puitteissa. Ristiriidattomuus voidaan todistaa pidemmälle viedyn matematiikan avulla, mikäli tiettyjen äärettömien objektien ominaisuuksista oletetaan riittäviä säännönmukaisuuksia.

Luonnollisten lukujen teoriaa voidaan laajentaa kokonaislukujen teoriaksi uusia käsitteitä määrittelemällä. Samoin voidaan kokonaisluvusta päästä rationaalilukuihin ja edelleen reaalinlukuihin. Toisaalta määritelmät voivat olla varsin monimutkaisia, ja siksi yleensä on perusteltua aksiomatisoida reaalinluvut erikseen.

Esimerkki 9 (Reaalilukujen aksiomatisointi). Reaalilukujen teorian peruskäsitteet ovat joukko $\mathbb{R}$, nolla $0 \in \mathbb{R}$, ykkönen $1 \in \mathbb{R}$, yhteenlasku $+$ ja kertolasku $\cdot$. Reaalilukujen aksioomat on tapana jaotella kolmeen ryhmään:

A) *Kunta-aksioomat:*

1. Kaikille reaaliluvuille a, b ja c pätee $a + (b + c) = (a + b) + c$ ja $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. Jokaiselle reaaliluvulle a pätee $0 + a = a$ ja $1 \cdot a = a$.
3. Jokaista reaalilukua a kohti on olemassa a :n vastaluku $-a$, joka toteuttaa $a + (-a) = 0$ ja jokaista nollasta eroavaa reaalilukua a kohti on olemassa käänteisluku a^{-1} , joka toteuttaa $a \cdot a^{-1} = 1$.
4. Kaikille reaaliluvuille a ja b pätee $a + b = b + a$ ja $a \cdot b = b \cdot a$.
5. kaikille reaaliluvuille a, b , ja c pätee $a \cdot (b + c) = a \cdot b + a \cdot c$.

B) *Järjestysaksioomat:* On olemassa osajoukko $\mathbb{R}_+ \subseteq \mathbb{R}$, joka toteuttaa seuraavat ehdot:

1. Jokaista reaalilukua a kohti pätee tarkalleen yksi vaihtoehdoista $a \in \mathbb{R}_+$, $a = 0$ tai $-a \in \mathbb{R}_+$.
2. Jos $a, b \in \mathbb{R}_+$, niin $a + b, a \cdot b \in \mathbb{R}_+$.

C) *Täydellisyysaksiooma:* Jokaisella epätyhjällä, ylhäältä rajoitetulla reaalilukujoukolla on pienin yläraja.

Edellä mainittuihin käsitteisiin perustuen voidaan määritellä kaikki yleensä tarvittavat reaalilukuja koskevat käsitteet ja aksioomista johdetaan reaalilukujen ominaisuudet. Esimerkiksi järjestysaksioomassa mainittua osajoukkoa kutsutaan yleensä *positiivisten reaalilukujen joukoksi* ja tämän avulla määritellään $a > b$ tarkalleen silloin, kun $a - b \in \mathbb{R}_+$.

Esimerkki 10. Tarkastellaan esimerkin vuoksi, miten ylläolevista aksioomista seuraa se tunnettu asia, että nollalla kertominen tuottaa aina nollan. Ensinnäkin $0 = 0 + 0$ kunta-aksiooman 2 perusteella, joten $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ kunta-aksiooman 5 perusteella. Edelleen kunta-aksiooman 3 perusteella reaaliluvulla $a \cdot 0$ on vastaluku $-a \cdot 0$, joka lisäämällä yhtälön kumpaankin puoleen saadaan $a \cdot 0 + (-a \cdot 0) = (a \cdot 0 + a \cdot 0) + (-a \cdot 0)$. Soveltamalla kunta-aksioomia 3 ja 1 saadaan tämä sievenemään muotoon $0 = a \cdot 0$.

Huomautus 1. Kummassakin yllä olevassa esimerkissä käytetään *joukko-oppia* (johon perehdytään luvussa 3 tarkemmin) taustateoriana. Lisäksi aksioomia esitettäessä käytetään yleensä yhtäsuuruus-symbolia ”=” jonka ajatellaan sisältyvän logiikan merkintöihin.

Insinöörimatematiikan kurssikokonaisuuden kannalta keskeisin matematiikan osa-alue on differentiaali- ja integraalilaskenta, ja sen perustana taas toimii reaalilukujen teoria. Näin ollen aksiomatisointi esimerkissä 9 toimii teoreettisena pohjana lähes koko Insinöörimatematiikan kurssikokonaisuudelle. Juuri se vastaa viime kädessä sellaisiin niihin kysymyksiin, jotka koskevat reaalilukujen ominaisuuksia. Aksioomista voidaan johtaa muun muuassa kaikkien reaalilukujen ominaisuus $a^2 \geq 0$, kunhan $a \geq b$ ensin määritellään johdonmukaisella tavalla. Sen lisäksi niistä voidaan johtaa kaikki yhtälöiden ja epäyhtälöiden käsittelysäännöt, esimerkiksi että kerrottaessa epäyhtälö negatiivisella luvulla sen epäyhtälömerkki kääntyy. Myös johdannossa esitetyt lausekkeiden suuruusarviot voidaan johtaa reaalilukujen järjestysaksioomista.

Tämän luvun lopuksi tarkastellaan lyhyesti matemaattisen teorian väitteiden *totuusarvoa*. Aksiomaattis-deduktiivisessa teoriassa teoriaa koskevat väittämät eli lauseet johdetaan loogisesti aksioomista, joten lauseiden totuus palautuu tällöin aksioomien totuuteen ja loogisten päättelysääntöjen pätevyyyteen.

Päättelysääntöjen pätevyydestä puhutaan enemmän seuraavassa luvussa, mutta jo tässä yhteydessä voidaan todeta, että *yleensä aksioomien totuusarvo on matemaattisen teorian kehittämisen kannalta täysin yhdenmukainen seikka* ja matemaattisen teorian lausetta sanotaan todeksi, mikäli se on johdettavissa aksioomista.

On kuitenkin jälleen muistutettava, että matemaattisen teorian aksioomia ei yleensä valita mielivaltaisesti, vaan niiden toivotaan kuvaavan mahdollisimman hyvin teorian objektien ominaisuuksia. Jos esimerkiksi halutaan teorian kuvaavan luonnollisia lukuja, on syytä valita aksioomat siten, että ne eivät ainakaan ole ristiriidassa luonnollisia lukuja koskevan intuition kanssa.

Totuuden käsitteen kannalta matemaattista teoriaa voidaan verrata vaikkapa shakkipeleihin: pelin alkuasetelma vastaa aksioomajoukkoa ja sääntöjen mukaiset siirrot päteviä päättelysääntöjä. Kukin säännönmukaisilla siirroilla saatu asetelma vastaa matemaattisen teorian lausetta ja tällöin matemaattisen teorian yhteydessä usein esiintyvä kysymys ”onko tämä lause tosi?” vastaa shakkipelissä kysymystä ”voidaanko tällainen asetelma saada pelisääntöjä noudattamalla?”

Shakkipelissä ei oteta kantaa siihen kysymykseen, onko pelin alkuasetelma jollakin tavalla ”tosi”, ja sama pätee myös matemaattiseen teoriaan. Oleellista on vain se, mitä aksioomista voidaan johtaa.

2.2 Päättelyn muotoja

Esimerkkinä loogisesta päättelystä toimii mainiosti esimerkki 10. Siinä reaalitylukujen aksioomista pääteltiin, että $a \cdot 0 = 0$. Looginen päättely ei kuitenkaan aina ole yhtä suoraviivaista, ja sen eri muotoihin perehdytään tässä luvussa yksityiskohtaisemmin.

Päättelyn eri muodoista voidaan mainita ainakin *deduktiivinen*, *induktiivinen* ja *abduktiivinen* päättely. Deduktiivisessa päättelyssä oletuksista johdetaan *päättelysääntöjä* käyttämällä johtopäätöksiä. Deduktiivinen päättely on tämän monisteen logiikkaosan pääasia, ja siihen perehdytään tarkemmin seuraavissa luvuissa. Induktiivisessa päättelyssä johdetaan joukosta tapauksia yleinen sääntö, ja abduktiossa taas tyypillisesti tunnetuista säännönmukaisuuksista ja seurauksesta päätellään *mitä on tapahtunut*.

Induktiivinen päättely on tyypillistä luonnontieteille, osalle yhteiskuntatieteistä ja lääketieteelle. Induktiossa päätellään, että sääntö, joka toimii havaittujen tapausten yhteydessä, pätee myös yleisesti (”kaikki joutsenet jotka olemme nähneet ovat valkoisia, siis *kaikki* joutsenet ovat valkoisia”). Induktiivinen päättely ei ole loogisesti sitovaa (Australiassa on mustia joutsenia; *Cygnus atratus*), mutta induktiivisen päättelyn epävarmuutta voidaan toisinaan arvioida tilastollisin menetelmin. Erityisen tärkeää induktion epävarmuuden arviointi on lääketieteessä: halutaan, että johtopäätös ”lääkkeellä ei ole haittavaikutuksia” pitää paikkansa mahdollisimman suurella todennäköisyydellä, vaikka lääketta on voitu testata vain rajalliseen ihmisjoukkoon.

Abduktiivinen päättely on tunnettua erityisesti salapoliisitarinoista: ”Herra X:n nähtiin poistuvan murhapaikalta, kenenkään muun ei nähty poistuvan murhapaikalta, siis herra X on murhaaja”. Abduktiivista päättelyä käytetään jossakin määrin yhteiskuntatieteissä ja humanistisissa tieteissä, mutta induktion tavoin abduktiivinen päättely ei ole loogisesti sitovaa.

Matemaattisten lauseiden todistamiseen käytetään ainoastaan loogisesti sitovaa deduktiivista päättelyä ja siksi siihen perehdytään jatkossa tarkemmin. Seuraavassa luvussa esitettävä predikaattilogiikka on formaali kieli matematiikassa käytettävän deduktiivisen päättelyn esittämiseksi.

*Esimerkki 11. Syllogismi on deduktion muoto, jossa kahdesta premissistä (suomeksi lähtökoh-
ta) (pääpremissi ja alipremissi) päätellään johtopäätös.*

Jokainen ihminen on kuolevainen (pääpremissi)	Sokrates on ihminen (alipremissi)
Sokrates on kuolevainen (johtopäätös)	

Harjoitustehtävä: Mitä voidaan ylläolevasta syllogismista sanoa a) jos pääpremissi poistetaan b) jos johtopäätös ei ole tosi?

Taustatietoa

Aristoteles (Ἀριστοτέλης, 384 eKr–322 eKr) oli kreikkalainen filosofi, jonka katsotaan Sokrateen ja Platonin ohella vaikuttaneen eniten länsimaiseen ajatteluun. Aristoteles käsitteli lähes kaikkea inhimillisen toiminnan piiriin kuuluvaa, luonnontieteistä valtiotieteisiin ja taiteisiin. Aristoteles analysoi loogista päättelyä ja kehitti syllogistisen logiikan. Aristotelesta sanotaan usein logiikan isäksi.

(kuva: Wikimedia Commons)

2.3 Predikaattilogiikkaa

Antiikin Kreikan ajoista logiikka on toiminut tärkeänä matematiikan rakennusosana, mutta 1800-luvun puolivälistä lähtien on esiintynyt suuntauksia, jotka korostavat matematiikan roolia logiikan perustana. Tällainen on esimerkiksi George Boolean esittämä logiikan muotoilu, johon ei kuitenkaan tässä kurssissa erityisemmin perehdytä. Boolean töiden jälkeen kävi varsin pian selväksi, että lähes kaikki matematiikkaa koskeva deduktiivinen päättely voidaan esittää kokonaan *formaalissa* (muodollisessa, tulkinnoista vapaassa) esitysasussa, ja seuraavaksi perehdytään käsitteisiin, joita tämän päämäärän saavuttamiseksi tarvitaan.

Ensimmäinen askel logiikan rakenteiden jäsentelyssä on abstrahointi. Palataan esimerkkiin 11 ja merkitään

$$I(x) = \text{”}x \text{ on ihminen”}, \quad K(x) = \text{”}x \text{ on kuolevainen”} \quad \text{ja } s = \text{”Sokrates”}.$$

Kvanttoreita (kts. johdanto) ja näitä merkintöjä käyttäen lause ”Jokainen ihminen on kuolevainen” voidaan nyt ilmaista muodossa $(\forall x)(I(x) \rightarrow K(x))$. Lause ”Sokrates on ihminen” ilmaistaan muodossa $I(s)$ ja ”Sokrates on kuolevainen” puolestaan muodossa $K(s)$. Koko päättely voidaan siis abstrakteilla merkinnöillä kirjoittaa muotoon

$$\frac{(\forall x)(I(x) \rightarrow K(x)) \quad I(s)}{K(s)}$$

Jatkossa käytetään merkintää $\models$ osoittamaan loogista seurausta, ja tällä tavalla merkittynä esimerkin 11 syllogismi saadaan muotoon

$$\{(\forall x)(I(x) \rightarrow K(x)), I(s)\} \models K(s) \quad (2.2)$$

Esitysmuodossa (2.2) tärkeää ei ole se, että se on lyhyempi kuin esimerkin 11 muoto. Sen sijaan oleellista on, että jälkimmäisessä muodossa näkyvät ainoastaan olioiden väliset *suhteet*, eivät olleet itse. Muodossa (2.2) päättelystä voidaan todellakin riisua kaikki merkitykset: esimerkiksi $I(x)$ ei tarvitse välttämättä merkitä ” x on ihminen”, eikä symbolin s tarvitse merkitä Sokratesta. Esitysmuoto (2.2) sanoo vain, että premisseistä 1) ”kaikille olioille ominaisuudesta I seuraa ominaisuus K ” ja 2) ”oliolla s on ominaisuus I ” seuraa johtopäätös ”oliolla s on ominaisuus K ”.

Muoto (2.2) selvästi yleisempi kuin esimerkki 11. Jälkimmäinen voidaan nimittäin *tulkita* esimerkin 11 päättelyksi, mutta se voidaan tulkita myös monilla muilla tavoilla. Tärkein abstraktin muodon (2.2) anti on kuitenkin se, päättelyn voidaan havaita olevan pätevää, olivatpa I :n K :n ja s :n merkitykset mitkä hyvänsä.

Havaitaan, että logiikan formaalissa esityksessä tarvitaan ainakin *ominaisuuksia* ilmoittavia määreitä kuten $I(x)$ ja $K(x)$ Sokratesta koskevassa päättelyssä. Näitä kutsutaan *predikaatti-* eli *relaatio**symboleiksi*. Matematiikassa on voitava puhua myös useamman objektin välisistä suhteista. On voitava esimerkiksi ilmoittaa ” x on pienempi kuin y ” ja tämä voidaan saavuttaa *useampipaikkaisten* predikaattisymbolien avulla. Voidaan esimerkiksi ajatella, että $P(x,y)$ tulkitaan väittämäksi ” x on pienempi kuin y ”.

Ainekset, jotka riittävät matemaattisten teorioiden esittämiseen logiikan merkinnöin luetellaan seuraavassa määritelmässä.

Näistä aineksista voidaan rakentaa predikaattilogiikan *kaavoja* tai *lauseita*, jotka voidaan tulkita matemaattisiksi väittämiksi. Tarkempi perehtyminen osoittaa, että funktiosymbolit eivät ole aivan välttämättömiä vaan ne voitaisiin kiertää käyttämällä predikaattisymboleja. Yleensä funktiosymbolien avulla voidaan kuitenkin tiivistää esitystä. Käytännössä alaindeksejä ei tarvita, vaan muuttujasymboleille käytetään merkintöjä $x, y, z, \dots$, predikaattisymboleille $A, B, C, \dots$ ja funktiosymboleille $f, g, h, \dots$. Määritelmässä alaindeksit lähinnä korostavat sitä, että muuttujasymboleja, predikaattisymboleja, ym. on olemassa rajaton määrä.

Esimerkki 12. Väite ”kaikille x :ille pätee $x^2 \geq 0$ ” kirjoitetaan logiikan kaavaksi ensin miettimällä, mitä ominaisuuksia pitää ilmaista. Yksi tällainen ominaisuus on $x \geq 0$, ja se voidaan ilmaista ainakin kahdella eri tavalla. Valitaan ensin esitystavaksi yksipaikkainen predikaattisymboli $P(x) = "x \geq 0"$. Toinen ilmaistava asia on funktio $x \mapsto x^2$, jota voidaan valita edustamaan yksipaikkainen funktiosymboli $N(x)$. Näillä merkinnöillä esimerkin väite ilmaistaan seuraavasti:

$$(\forall x)P(N(x)). \quad (2.3)$$

Toinen esitystapa voidaan perustaa kaksipaikkaiseen predikaattisymboliin $S(x, y) = "x \geq y"$ ja vakiosymboliin n , joka tulkitaan nolllaksi. Tällöin $S(x, n)$ esittää väittämää $x \geq 0$ ja koko väittämä voidaan esittää muodossa

$$(\forall x)S(N(x), n). \quad (2.4)$$

Esitystapojen suoraviivaistamiseksi voidaan kuitenkin sopia yksinkertaisemmista merkinnöistä, jotka korvaavat funktiosymbolit ja vakiosymbolit: $N(x)$ sijasta merkitään yksinkertaisesti x^2 ja n :n sijasta 0 ja $S(x, y)$:n sijasta merkitään $x \geq y$. Toisin sanoen, käytetään niitä symboleja, jotka matematiikassa on tarkoitukseen valittu jo aiemmin. Tällöin väite voidaan kirjoittaa muotoon

$$(\forall x)(x^2 \geq 0),$$

mutta tässä esitysasussa on huomioitava, että funktio-, vakio- ja predikaattisymbolista on käytetty merkintöjä, jotka eivät varsinaisesti kuulu predikaattilogiikkaan. Asia yhteydestä ne voidaan kuitenkin ymmärtää funktio-, vakio- ja predikaattisymboleiksi. On myös huomattava, että predikaatti- ja funktiosymboleita käytetään matematiikassa yleensä ns. *infix*-merkintää varsinaisen predikaattilogiikan merkinnän sijaan. Tämä tarkoittaa esim. sitä, että merkinnän $< (2, 3)$ sijaan kirjoitetaan $2 < 3$ ja $+(2, 3)$ sijaan $2 + 3$.

2.3.1 Predikaattilogiikan syntaksi

Logiikan *syntaksissa* eli lauseopissa ilmaistaan, miten aakkostosta muodostetaan *kaavoja* hyväksyttävällä tavalla. Aakkoston aineksista saadaan helposti aikaan kaikenlaisia kirjoitelmia, kuten esimerkiksi $\forall R_1 \neg x \forall \rightarrow)_C f_1 \wedge f_2$, mutta tällainen ei ole mielekäs kaava.

Esitystavan lyhentämiseksi voidaan sulkumerkkejä jättää pois erikseen sovittavilla tavoilla. Voidaan esimerkiksi sopia, että $\neg$ sitoo vahvemmin kuin $\wedge$ ja $\vee$, ja nämä puolestaan vahvemmin kuin $\leftrightarrow$ ja $\rightarrow$, jolloin kaava $\neg\phi \wedge \psi \rightarrow \eta$ on lyhennysmerkintä kaavasta $((\neg\phi) \wedge \psi) \rightarrow \eta$. Sovitaan myös, että kvantorit sitovat vahvemmin kuin $\neg$ ja $\vee$, jolloin $(\forall x)\phi \vee \psi$ tarkoittaa kaavaa $((\forall x)\phi) \vee \psi$.

Predikaattilogiikan kaavoja, jotka on muodostettu edellisen määritelmän mukaan, kutsutaan *hyvinmuodostetuiksi kaavoiksi*. Predikaattilogiikan semantiikka eli merkitysoppi koskee ainoastaan hyvinmuodostettuja kaavoja, ja muut kirjoitelmat jäävät kokonaan vaille merkitystä.

Edellisessä määritelmässä huomattavaa on, että *termit* ovat kaavan rakennusosia, jotka eivät sisällä mitään väitelausetta. Sen sijaan *kaava* pitää sisällään aina väitteen: esimerkiksi $R(t_1, t_2, \dots)$ väittää, että termit $t_1, t_2, \dots$, toteuttavat ehdon $R(t_1, t_2, \dots)$, miksi ikinä se (ehto) tulkitaankaan. Lisäksi muuttujia voidaan kvantifioida ja kaavoja voidaan yhdistää loogisilla konnektiiveilla.

Esimerkki 13. Esityksessä (2.2) s on termi, koska se on vakiosymboli ja samoin x on termi koska se on muuttujasymboli. Sen sijaan $I(x)$ ja $K(x)$ ovat kaavoja ylläolevan määritelmän mukaan. Myös $I(x) \rightarrow K(x)$ on kaava, samoin kuin $(\forall x)(I(x) \rightarrow K(x))$ ja $K(s)$.

Esimerkki 14. Esimerkissä 12 x on termi, samoin $N(x)$. Sen sijaan $P(N(x))$ on kaava, ja samoin on $(\forall x)(P(N(x)))$. Toisessa esitystavassa $x, N(x)$ ja n ovat termejä, mutta $S(N(x), n)$ on kaava, samoin kuin $(\forall x)S(N(x), n)$.

Esimerkki 15. Kaavassa $I(x) \rightarrow K(x)$ x on vapaa muuttuja, mutta $(\forall x)(I(x) \rightarrow K(x))$ on lause, koska kvanttori $(\forall x)$ sitoo muuttujan x .

Esimerkki 16. Kaavassa $x^2 \geq 0$ x on vapaa muuttuja, mutta $(\forall x)(x^2 \geq 0)$ on lause, sillä kvanttori sitoo vapaan muuttujan.

Esimerkki 17. Kaavassa $(\forall x)I(x)$ kvanttori sitoo muuttujan x , mutta kaavassa $(\forall x)I(x) \wedge K(x)$ on x :llä sekä sidottu ($I(x)$) että vapaa esiintymä $K(x)$. Jälkimmäistä x :ää kvanttori ei sido, joten kaava $(\forall x)I(x) \wedge K(x)$ ei ole lause.

Esimerkki 18. Peanon aksiomat voidaan kirjoittaa predikaattilogiikkaa käyttämällä seuraavasti: käytetään funktiosymbolia s , vakiosymbolia 1 ja relaatioymbolia $\in$ (joukkoon kuuluminen). Tällöin aksiomat saavat muodon

- $(\forall x)(\forall y)(\neg(x = y) \rightarrow \neg(s(x) = s(y)))$
- $(\forall x)\neg(s(x) = 1)$
- $(\forall A)((1 \in A \wedge (\forall x)(x \in A \rightarrow s(x) \in A)) \rightarrow (\forall x)(x \in A))$

Peanon aksiomatiikan formaalissa esitysmuodossa on oleellista huomata, että kahdessa ensimmäisessä aksiomassa kvanttori kohdistuu muuttujasymboliin x , joka tulkitaan systeemin *alkioksi*, kun taas kolmannessa aksiomassa kvanttori kohdistuu A :han, jonka tulkitaan olevan systeemin *osajoukko*.

Peanon aksiomatiikassa kaksi ensimmäistä aksiomaa ovat tyypillisiä ensimmäisen kertaluvun lauseita, mutta kolmatta, ns. induktioaksiomaa ei voida esittää ensimmäisen kertaluvun predikaattilogiikalla. Samoin voidaan havaita, että reaalilukujen aksiomatiikassa kunta-aksiomat ovat ensimmäistä kertalukua, kun taas järjestyks- ja täydellisyysaksiomat ovat toista kertalukua. Osoittautuu, että kokonaislukuja sen enempää kuin reaalilukujakaan ei voida tyydyttävällä tavalla aksiomatisoida pelkästään ensimmäisen kertaluvun predikaattilogiikan avulla.

2.3.2 Predikaattilogiikan semantiikka

Predikaattilogiikan semantiikka eli merkitysoppi on huomattavasti monimutkaisempaa kuin syntaksi. Semantiikassa predikaattilogiikan kaavoihin liitetään merkitys, jonka avulla ne tulkitaan tosiksi tai epätosiksi. On huomattava, että kaavan totuusarvo voi muuttua tulkintaa vaihdettaessa.

Esimerkki 19. Kaava $(\forall x)(\forall y)(x + y \geq 1)$ on tosi, jos muuttujien tulkitaan saavan vain luonnollisia lukuja arvoikseen. Jos sen sijaan myös negatiiviset luvut ovat mahdollisia, kaava on epätosi.

Esimerkki 20. Kaava $(\forall x)(\exists y)(x < y < x + 1)$ on epätosi, jos muuttujat saavat vain kokonaislukuarvoja. Sen sijaan reaaliarvoilla kaava on tosi.

Esimerkki 21. Kun c on vakiosymboli, x muuttujasymboli, f funktiosymboli ja R kaksipaikkainen relaatiot symboli, on kaava $R(x, f(c))$ hyvinmuodostettu. Sen totuusarvo taas riippuu täysin siitä, mikälainen tulkinta sille annetaan. Valitaan esimerkiksi tulkintaa varten tulkintajoukoksi kokonaislukujen joukko $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ ja relaatiot symbolin R tulkinnaksi $R(x, y) = "x \geq y"$ ja funktiot symbolin tulkinnaksi $f(x) = x^2$. Jos vielä valitaan vakiot symbolin c tulkinnaksi 2 ja x :n tulkinnaksi -1 , on kaavan tulkinta " $-1 \geq 2^2$ ", mikä on epätosi. Jos c :n tulkinnaksi olisi valittu 5, pitäisi kaava tulkita todeksi.

Esimerkki 22. Myös $x = c$ on hyvin muodostettu kaava, joka tulkitaan todeksi tarkalleen silloin, kun x ja c tulkitaan samaksi tulkintajoukon A alkioiksi.

Kahden edellisen esimerkin kaavat ovat muotoa $R(t_1, t_2, \dots)$ ja $t_1 = t_2$, siis atomikaavoja. Atomikaavat tulkitaan aina kuten näissä esimerkeissä. Tiivistetään tämä vielä seuraavaan määritelmään.

Monimutkaisempien kaavojen tulkinta alkaa atomikaavojen tulkinnasta, minkä jälkeen tulkitaan kvanttorit ja loogiset konnektiivit seuraavien määritelmien mukaisesti.

Huomautus 2. Edellinen määritelmä esittää tulkinnan ainoastaan ensimmäisen kertaluvun predikaattilogiikalle, jossa kvantifiointi ei ulotu tulkintajoukon osajoukkoihin, vaan ainoastaan sen alkioihin. Tästädes tässä luvussa oletetaan predikaattilogiikan tarkoittavan ensimmäisen kertaluvun logiikkaa, ellei toisin mainita.

Esimerkki 23. Sidotaan esimerkin 21 vapaa muuttuja universaalikvanttorilla ja määritetään näin syntyneen kaavan $(\forall x)R(x, f(c))$ totuusarvo. Tulkinnan ollessa sama kuin ennenkin (c tulkitaan luvuksi 2) väittää kaava seuraavasti: ”kaikille kokonaisluvuille x pätee $x \geq 2^2$ ”. Näin ollen kaava tulkitaan epätodeksi.

Esimerkki 24. Selvitetään kaavan $(\exists x)R(x, y)$ totuusarvo esimerkin 21 tulkinnassa. Tällöin $R(x, y)$ tulkitaan kokonaislukujen relaatioksi $x \geq y$, ja kaava väittää, että ”on olemassa x joka on vähintään y :n suuruinen”. Esimerkin 21 tulkinta ei kuitenkaan kiinnitä y :tä mitenkään, joten y on vielä tulkittava erikseen, esimerkiksi luvuksi 4. Tällöin lause on selvästi tosi, ja lisäksi huomataan, että y :n neloseksi tulkitseminen ei ole millään tavoin erityisasemassa, vaan lause tulkittaisiin todeksi valittiinpa y :lle mikä hyvänsä tulkinta.

Esimerkki 25. Selvitetään kaavan

$$(I(s) \wedge (\forall x)(I(x) \rightarrow K(x))) \rightarrow K(s)$$

totuusarvo tulkinnassa, jossa tulkintajoukoksi A valitaan kokonaislukujen joukko, $I(x)$ tulkitaan ” x on parillinen”, $K(x)$ ” x on suurempi kuin kymmenen”, ja s tulkitaan luvuksi 2. Tulkintaa varten selvittää ensin atomikaavojen totuusarvo. Tässä tulkinnassa $I(s)$ on väite ”2 on parillinen”, siis tosi. Seuraavaksi tarkastellaan osakaavaa $I(x) \rightarrow K(x)$, jonka tulkinta määräytyy määritelmän ?? mukaan: $I(x) \rightarrow K(x)$ tulkitaan epätodeksi vain, jos $I(x)$ tulkitaan todeksi ja $K(x)$ epätodeksi. Jos esimerkiksi x tulkitaan luvuksi 4, on $I(x)$ tulkittava todeksi, mutta $K(x)$ epätodeksi. Tällöin on siis olemassa sellainen x :n tulkinta, joka valitsemalla osakaava $I(x) \rightarrow K(x)$. Tämä havainto puolestaan riittää siihen, että osakaava $(\forall x)(I(x) \rightarrow K(x))$ on tulkittava epätodeksi.

Nyt siis konnektiivin $\wedge$ tulkinnan mukaan osakaava $I(s) \wedge (\forall x)(I(x) \rightarrow K(x))$ tulkitaan epätodeksi, ja konnektiivin $\rightarrow$ tulkinnan mukaan koko kaava todeksi.

Esimerkki 26. Osoitetaan, että edellisen esimerkin kaava on tosi *kaikissa* tulkinnoissa. Koska kaavan päämuoto on implikaatio, voi se tulla epätodeksi ainoastaan, jos osakaava $(I(s) \wedge (\forall x)(I(x) \rightarrow K(x)))$ tulkitaan todeksi ja $K(s)$ epätodeksi. Kuvitellaan sitten, että jossakin tulkinnassa näin käy. Koska ensimmäisen osakaavan päämuoto on konjunktio, on välttämättä $I(s)$ ja $(\forall x)(I(x) \rightarrow K(x))$ molemmat tulkittava todeksi. Jälkimmäisen osakaavan tulkinta todeksi tarkoittaa taas sitä, että kaikilla mahdollisilla x :n tulkinnoilla $I(x) \rightarrow K(x)$ tulkitaan todeksi, myös silloin kun x tulkitaan samaksi alkioksi kuin s . Mutta aiemmin sanotusta tiedetään, että $I(s)$ tulkitaan todeksi ja $K(s)$ epätodeksi, mikä on selvästi ristiriidassa sen kanssa, että $(\forall x)(I(x) \rightarrow K(x))$ pitää tulkita todeksi. Näin huomataan, että kuviteltua tulkintaa ei voi olla olemassa ja että kaava siis on tosi kaikissa tulkinnoissa.

Edellisen esimerkin kaavan totuusarvo ei siis riipu lainkaan tulkinnasta. Tämä merkitsee sitä, että kaava on *muotonsa vuoksi* tosi. Erityislaatuisten kaavojen nimityksiä on koottu seuraavaan määritelmään.

Esimerkki 27. Edellisessä esimerkissä todettiin, että kaava

$$(I(s) \wedge (\forall x)(I(x) \rightarrow K(x))) \rightarrow K(s)$$

on tautologia. Kun edellisen esimerkin sanallinen päättely luetaan uudelleen, huomataan, että $K(s)$ on tosi kaikissa niissä tulkinnoissa, joissa $I(s)$ ja $(\forall x)(I(x) \rightarrow K(x))$ molemmat ovat. Tällöin sanotaan, että $K(s)$ seuraa kaavoista $I(s)$ ja $(\forall x)(I(x) \rightarrow K(x))$ loogisesti. Loogista seuraussuhdetta tarkastellaan lähemmin seuraavassa luvussa.

Esimerkki 28. Kaava $\phi \wedge \neg\phi$ on kontradiktio, olipa ϕ mikä hyvänsä kaava.

2.3.3 Looginen seuraus

Tässä kurssissa termit *deduktiivinen päättely* ja *loogisesti sitova päättely* pidetään synonyymeinä. Näiden merkitys puolestaan on selvitetty seuraavassa määritelmässä predikaattilogiikan termein.

Huomautus 3. Tautologiat ovat kaavoja, jotka seuraavat *tyhjästä* premissijoukosta (miksi?) Tällöin ” ϕ on tautologia” voidaan merkitä $\emptyset \models \phi$ tai vielä lyhyemmin $\models \phi$.

Esimerkki 29. Osoita harjoitustehtävänä oikeaksi seuraava väittämä: Jos $\Gamma = \{\phi_1, \dots, \phi_n\}$, niin $\Gamma \models \phi$ tarkalleen silloin kun kaava $\phi_1 \wedge \dots \wedge \phi_n \rightarrow \phi$ on tautologia.

Edellisen määritelmän mukaan päättely on siis epäpätevää, mikäli voi esiintyä sellainen tulkinta, jossa premissit ovat kaikki tosia, mutta johtopäätös epätosi. Aivan kuten esimerkissä 26, voidaan todeta, että päättely

$$\{I(s), (\forall x)(I(x) \rightarrow K(x))\} \models K(s) \quad (2.5)$$

on pätevää: tulkinnoissa, joissa $I(s)$ ja $(\forall x)(I(x) \rightarrow K(x))$ on tosi, on myös johtopäätös $K(s)$ tosi. Päättely (2.5) on abstrahoitu versio Sokrates-esimerkistä 11, joten Sokratesta koskeva päättely on loogisesti pätevää.

Huomautus 4. Kuten luvun alussa mainittiin, matemaattisen lauseen todistaminen merkitsee sen johtamista aksioomista $A_1, \dots, A_k$. Täten siis matemaattisen lauseen ϕ todistaminen on loogisen seuraussuhteen $\{A_1, \dots, A_k\} \models \phi$ toteen näyttämistä.

Jos esimerkiksi tulee näyttää toteen, että luonnollisille luvuille pätee lause ϕ , tapahtuu tämä *periaatteessa* siten, että valitaan esimerkin 8 Peanon aksioomat oletusjoukoksi $\{P_1, P_2, P_3\}$, ja tämän jälkeen näytetään toteen, että $\{P_1, P_2, P_3\} \models \phi$. *Käytännössä* uuden matemaattisen väittämän todistuksessa ei kuitenkaan tarvitse yleensä nojautua aksioomiin asti, vaan yleensä voidaan käyttää premissinä jo todistettuja lauseita (joiden siis jo tiedetään seuraavan aksioomista).

Tämä puolestaan perustuu siihen havaintoon, että looginen seuraussuhde on *transitiivinen*, mikä puolestaan merkitsee seuraavaa:

Lause 1. Jos $\Gamma_1 \models \Gamma_2$ ja $\Gamma_2 \models \Gamma_3$, niin $\Gamma_1 \models \Gamma_3$.

Todistus. Perustuu suoraan loogisen seurauksen määritelmään (mieti miten). $\square$

Edellisen lauseen mukaan looginen päättely on mahdollista pilkkoa osiin: Jos halutaan näyttää toteen, että lausejoukosta $\Gamma = \Gamma_1$ seuraa loogisesti lause ϕ , voidaan käyttää

suoraa todistusta

$$\Gamma_1 \models \Gamma_2 \models \dots \models \Gamma_n \models \phi,$$

jossa kukin lause joukossa Γ_{i+1} on saatavissa edellisen joukon Γ_i lauseista päättelyllä, joka tiedetään päteväksi. Esimerkissä 27 on esitetty yksi loogisesti pätevä päättely, ja tällaisia esitetään jäljempänä lisää.

Toinen varsin usein matematiikassa käytetty tapa seuraussuhteen $\Gamma \models \phi$ todistamiseksi on ns.

epäsuora todistus, jossa osoitetaan, että lausejoukosta $\Gamma \cup \{\neg\phi\}$ seuraa loogisesti $\perp$,

siis lause joka on kaikissa tulkinnoissa epätosi. Vaihtoehtoisesti voidaan näyttää toteen, että lausejoukosta $\Gamma \cup \{\neg\phi\}$ seuraa loogisesti jokin lause ψ ja sen negaatio $\neg\psi$; myös tämä riittää epäsuoraan todistukseen. Tätä todistusmallia käytettiin esimerkissä 26, tosin sanallisesti eikä loogisiin merkin-töihin puettuna. Epäsuorassa todistuksessa väitettä $\neg\phi$ kutsutaan *vastaoletukseksi*.

Lause 2. Jos lausejoukosta $\Gamma \cup \{\neg\phi\}$ seuraa loogisesti $\perp$ (tai lause ψ ja sen negaatio $\neg\psi$), niin silloin lausejoukosta Γ seuraa loogisesti lause ϕ .

Todistus. Osoitetaan ensin oikeaksi aputuloks eli *lemma* joka väittää seuraavaa: Jos lausejoukosta Δ seuraa loogisesti $\perp$ tai lause ψ sekä sen negaatio $\neg\psi$, ei lausejoukolla Δ voi olla mallia.

Aputulos on seuraa melko suoraan loogisen seurauksen määritelmästä. Jos nimittäin lausejoukolla Δ olisi malli, olisi se myös $\perp$:in malli, mikä on mahdotonta. Samoin on mahdotonta, että lausejoukon Δ malli olisi yhtä aikaa ψ :n ja $\neg\psi$:n malli.

Osoitetaan sitten oikeaksi varsinainen väittämä. Loogisen seuraussuhteen $\Gamma \models \phi$ toteen näyttämiseksi on osoitettava, että mikä hyvänsä Γ :n malli on myös ϕ :n malli. Olkoon I siis jokin Γ :n malli, ja kuvitellaan, että se *ei olisi* ϕ :n malli, siis ϕ on epätosi tulkinnassa I . Tällöin $\neg\phi$ on tosi tulkinnassa I , joten I on malli lausejoukolle $\Gamma \cup \{\neg\phi\}$. Tämä on kuitenkin mahdotonta, koska tästä joukosta seuraa loogisesti $\perp$ (tai lauseet ψ ja $\neg\psi$), eikä sillä siis voi olla mallia. $\square$

Toisinaan voidaan käyttää myös

vastaesimerkkiä. Jos halutaan näyttää toteen, että lausejoukosta Γ *ei seuraa* lausetta ϕ , riittää löytää yksikin lausejoukon Γ malli, joka ei ole lauseen ϕ malli. Tällaista mallia kutsutaan *vastaesimerkiksi*.

Esimerkki 30. Lause $(\forall x)(x^2 - 4 \geq 0)$ ei seuraa reaalityökalujen aksioomista. Tämä johtuu siitä, että reaalityökalujen aksioomien luonnollinen malli toimii vastaesimerkkinä: luonnollisessa mallissa voidaan valita esimerkiksi $x = 0$, eikä lause $x^2 - 4 \geq 0$ silloin toteudu.

Esimerkki 31. Näytetään, että lauseista $K(s)$ ja $(\forall x)(I(x) \rightarrow K(x))$ ei seuraa loogisesti lause $I(s)$. Tätä varten voidaan valita tulkintajoukko kokonaislukujen joukoksi ja tulkita $K(x)$ relaatioksi ” $x \geq 0$ ” ja $I(x)$ relaatioksi ” $x \geq 2$ ”. Kun lisäksi s tulkitaan vakioksi 1, huomataan että $K(s)$ ja $(\forall x)(I(x) \rightarrow K(x))$ saavat totuusarvon 1 tässä tulkinnassa, mutta $I(s)$ totuusarvon 0.

2.3.4 Gentzenin luonnollisen deduktion järjestelmä

Teorian soveltamisen kannalta keskeiseksi ongelmaksi nousee sen selvittäminen, seuraako jokin lause aksioomista vai ei. Valitettavasti loogisen seuraussuhteen näkeminen saattaa toisinaan olla varsin hankalaa.

Tätä ongelmaa voidaan ainakin yrittää lähestyä seuraavasti: Jos on selvitettävä seuraako premisijoukosta Γ lause ϕ , voidaan ryhtyä muodostamaan lauseita, joiden *varmasti* tiedetään seuraavan tästä joukosta. Jos esimerkiksi joukossa Γ on lause $I(s)$ ja $(\forall x)(I(x) \rightarrow K(x))$, tiedetään (2.5):n perusteella, että joukosta Γ seuraa loogisesti lause $K(s)$. Jos tämänkaltaisten varmojen loogisten seuraussuhteiden avulla saavutetaan lause ϕ , on se looginen seuraus joukosta Γ .

Tätä lähestymistapaa varten tulee kehittää joukko päteviä päättelyjä, joita voidaan käyttää päätelysääntöinä. Gerhard Gentzen (1909–1945) on esittänyt vuonna 1935 päättelysäännöt, joita kutsutaan *luonnollisen deduktion järjestelmäksi*. Nimitys johtuu siitä, että Gentzenin säännöt formalisoivat tavallisen johdonmukaisen päättelyn.

Luonnollisen deduktion järjestelmä**Konnektiivien introduktio- ja eliminointisäännöt**

$$\begin{array}{l}
(I\wedge): \frac{\phi \quad \psi}{\phi \wedge \psi} \quad (I\vee): \frac{\phi}{\phi \vee \psi} \text{ ja } \frac{\psi}{\phi \vee \psi} \quad (I\rightarrow): \frac{\begin{array}{c} \phi^{\checkmark} \\ \vdots \\ \psi \end{array}}{\phi \rightarrow \psi} \\
(I\neg): \frac{\begin{array}{c} \phi^{\checkmark} \\ \vdots \\ \perp \end{array}}{\neg \phi} \quad (I\leftrightarrow): \frac{\begin{array}{c} \phi^{\checkmark} \quad \psi^{\checkmark} \\ \vdots \quad \vdots \\ \psi \quad \phi \end{array}}{\phi \leftrightarrow \psi} \\
(E\wedge): \frac{\phi \wedge \psi}{\phi} \quad \frac{\phi \wedge \psi}{\psi} \quad (E\vee): \frac{\phi \vee \psi \quad \begin{array}{c} \phi^{\checkmark} \quad \psi^{\checkmark} \\ \vdots \quad \vdots \\ \eta \quad \eta \end{array}}{\eta} \quad (E\rightarrow): \frac{\phi \quad \phi \rightarrow \psi}{\psi} \\
(E\neg): \frac{\phi \quad \neg \phi}{\perp} \quad (E\leftrightarrow): \frac{\phi \quad \phi \leftrightarrow \psi}{\psi} \quad \frac{\psi \quad \phi \leftrightarrow \psi}{\phi} \quad (E\perp): \frac{\perp}{\phi} \quad (\phi \text{ voi olla mikä hyvänsä}) \\
(RAA): \frac{\begin{array}{c} \neg \phi^{\checkmark} \\ \vdots \\ \perp \end{array}}{\phi}
\end{array}$$

Kvanttoreiden introduktio- ja eliminointisäännöt

$$\begin{array}{l}
(I\forall): \frac{\phi(x)}{(\forall x)\phi(x)} \quad (I\exists): \frac{\phi(t)}{(\exists x)\phi(x)} \\
(E\forall): \frac{(\forall x)\phi(x)}{\phi(t)} \quad (E\exists): \frac{(\exists x)\phi(x) \quad \begin{array}{c} \phi^{\checkmark} \\ \vdots \\ \psi \end{array}}{\psi}
\end{array}$$

Kvanttorisääntöjen rajoitukset: $(I\forall)$: x ei saa esiintyä vapaana missään (poistamattomassa) oletuksessa, josta $\phi(x)$ on johdettu. $(E\exists)$: x ei saa olla vapaa ψ :ssä tai johdon $\phi \dots \psi$ (poistamattomissa) oletuksissa paitsi ϕ :ssä. $(E\forall)$ ja $(I\exists)$: mikään vapaa muuttuja termissä t ei saa tulla sidotuksi, kun kaavaan $\phi(x)$ sijoitetaan x :n paikalle t (Tällöin sanotaan, että t on x -vapaa ϕ :n suhteen).

Yhtäsuuruussäännöt

$$\begin{array}{l}
(YS1): \frac{}{x = x} \quad (YS2): \frac{x = y}{y = x} \quad (YS3): \frac{x = y \quad y = z}{x = z} \\
(YS4): \frac{x_1 = y_1 \quad x_2 = y_2 \quad \dots \quad x_n = y_n}{f(x_1, x_2, \dots, x_n) = f(y_1, y_2, \dots, y_n)} \\
(YS5): \frac{x_1 = y_1 \quad x_2 = y_2 \quad \dots \quad x_n = y_n \quad R(x_1, x_2, \dots, x_n)}{R(y_1, y_2, \dots, y_n)}
\end{array}$$

Implikaation introduktiosäännössä $(I\rightarrow)$, kuten useissa muissakin säännöissä esiintyy kolme pistettä ja $\checkmark$ -merkki kaavan yläkulmassa. Kolme pistettä ϕ :n ja ψ :n välillä merkitsevät sitä, että ψ on saatu järjestelmän säännöillä käyttämällä ϕ :tä oletuksena. Merkki $\checkmark$ puolestaan tarkoittaa, että sillä merkitty kaava saadaan poistaa säännön soveltamisen jälkeen. Kaavan poistaminen saattaa olla tarpeen, jotta kvanttorisääntöjä $(I\forall)$ ja $(E\exists)$ voitaisiin soveltaa rajoitukset huomioonottaen.

Tiukasti tulkiten yhtäsuuruussääntöjen $x:t$, $y:t$ ja $z:t$ pitäisi käsittää muuttujasymboleiksi. Osoittautuu kuitenkin, että luonnollisen deduktion järjestelmän ilmaisuvoima ei muutu, vaikka ne käsitettäisiin termeiksi.

Kuva 2.1 Luonnollisen deduktion järjestelmän säännöt

Esimerkki 32 (Kvanttorisäännön väärinkäyttö). Oletuksesta $x = c$ ei voida johtaa kaavaa $(\forall x)(x = c)$, koska x esiintyy vapaana poistamattomassa oletuksessa $x = c$. ($I\forall$)-sääntöä ei siis ole käytetty oikein.

Esimerkki 33 (Kvanttorisäännön väärinkäyttö). Lauseesta $(\forall y)(-y + y = 0)$ ei voida johtaa lausetta $(\exists x)(\forall y)(x + y = 0)$, vaikka se muodollisesti saadaankin sijoittamalla edelliseen lauseeseen $-y$:n paikalle x ja lisäämällä universaalikvanttori $\forall x$. Tällä tavoin ei kuitenkaan ole käytetty ($I\exists$)-sääntöä oikein, sillä termissä $t = -y$ tulee y sidotuksi, jos kaavaan $(\forall y)(x + y = 0)$ sijoitetaan x :n paikalle $-y$.

Kuvassa 2.1 esitetään Gentzenin järjestelmän säännöt yksityiskohtaisesti samalla tavalla kuin Sokratesta koskevassa esimerkissä. Kukin sääntö on muotoa

$$\frac{\phi_1 \phi_2 \dots \phi_n}{\phi},$$

missä $\phi_1, \phi_2, \dots, \phi_n$ ovat premissejä tai johtoja ja ϕ näistä johdettava kaava.

Esimerkki 34 (Esitetään luennolla). Tulkitaan Gentzenin järjestelmän sääntöjä.

Esimerkki 35. Sääntö ($I \rightarrow$) perustuu siihen, että jos $\Gamma \cup \{\phi\} \models \psi$, niin $\Gamma \models \phi \rightarrow \psi$ (harjoitustehtävä).

Huomautus 5. Gentzenin järjestelmän mukaisen johdon esittäminen on yleensä havainnollisinta ylhäältä alaspäin etenevässä kaaviossa, jossa ylimmäksi kirjoitetaan premissit, sen jälkeen niistä saadut johtopäätökset, sitten näistä saadut johtopäätökset, jne. Kaaviossa esitetään myös, mitä sääntöjä on käytetty.

Esimerkki 36. Johdetaan kaava $\phi \rightarrow (\psi \rightarrow \phi)$ tyhjästä oletusjoukosta. Valitaan ensin (tilapäisiksi) oletuksiksi 1) ϕ ja 2) ψ . Soveltamalla näihin sääntöä ($I \rightarrow$) saadaan kaava $\psi \rightarrow \phi$, jolloin oletus 2) voidaan poistaa. Käyttämällä taas sääntöä ($I \rightarrow$) saadaan $\phi \rightarrow (\psi \rightarrow \phi)$, jolloin oletus 1) voidaan poistaa. Kaavan $\phi \rightarrow (\psi \rightarrow \phi)$ johto tyhjästä on siis jono $\phi^\vee, \psi^\vee, \psi \rightarrow \phi, \phi \rightarrow (\psi \rightarrow \phi)$, missä $\vee$ ilmaisee poistetuksi merkityt oletukset. Kaaviona tämä johto voidaan esittää seuraavasti:

$$\frac{\frac{1) \phi^\vee \quad 2) \psi^\vee}{\psi \rightarrow \phi} (I \rightarrow, 2^\vee)}{\phi \rightarrow (\psi \rightarrow \phi)} (I \rightarrow, 1^\vee)$$

Esimerkki 37. Mikäli havainnollisuuden vuoksi tarkoituksenmukaista, voidaan kaaviossa toistaa jokin premissi, vaikka sen ajatellaankin esiintyvän johdossa vain kerran. Tätä voidaan korostaa valitsemalla sama numero premissin eri esiintymille. Valitaan esimerkiksi premissiksi $\phi \wedge \psi$ ja käytetään Gentzenin järjestelmää:

$$\frac{\frac{\frac{1) \phi \wedge \psi^\vee}{\psi} (E \wedge) \quad \frac{1) \phi \wedge \psi^\vee}{\phi} (E \wedge)}{\psi \wedge \phi} (I \wedge)}{\phi \wedge \psi \rightarrow \psi \wedge \phi} (I \rightarrow, 1^\vee)$$

Viimeisintä sääntöä käyttämällä voidaan premissi $\phi \wedge \psi$ poistaa, mikä tarkoittaa sitä, että kaava $\phi \wedge \psi \rightarrow \psi \wedge \phi$ on johdettu tyhjästä oletusjoukosta.

Esimerkki 38. Johdetaan lausejoukosta $\Gamma = \{(\forall x)(I(x) \rightarrow K(x)), I(s)\}$ lause $K(s)$.

$$\frac{\frac{1) (\forall x)(I(x) \rightarrow K(x))}{I(s) \rightarrow K(s)} (E \forall) \quad 2) I(s)}{K(s)} (E \rightarrow)$$

Huomaa, että tässä esimerkissä molemmat oletukset jäivät poistamatta, mutta näin oli tarkoituskin, koska kyseessä ei ollut johto tyhjästä oletusjoukosta.

Esimerkki 39. Olkoon $+$ kaksipaikkainen funktiosymboli. Johdetaan kaava $(\forall x)(\forall y)(\forall z)(x = y \rightarrow x + z = y + z)$ tyhjästä oletusjoukosta.

$$\begin{array}{c}
\frac{1) x = y^\vee \quad \overline{z = z} \text{ (YS1)}}{\overline{x + z = y + z} \text{ (YS4)}} \\
\frac{x + z = y + z}{x = y \rightarrow x + z = y + z} \text{ (I} \rightarrow, 1^\vee \text{)} \\
\frac{x = y \rightarrow x + z = y + z}{(\forall z)(x = y \rightarrow x + z = y + z)} \text{ (I}\forall \text{)} \\
\frac{(\forall z)(x = y \rightarrow x + z = y + z)}{(\forall y)(\forall z)(x = y \rightarrow x + z = y + z)} \text{ (I}\forall \text{)} \\
\frac{(\forall y)(\forall z)(x = y \rightarrow x + z = y + z)}{(\forall x)(\forall y)(\forall z)(x = y \rightarrow x + z = y + z)} \text{ (I}\forall \text{)}
\end{array}$$

Huomautus 6. Esimerkki 39 esittää formaalissa muodossa sen tunnetun seikan, että jos yhtälön molemmille puolille lisätään sama luku, seuraa näin saatu uusi yhtälö alkuperäisestä. Koska kaksipaikkaisen funktiosymbolin $+$ olemuksesta ei ollut mitään oletuksia, pätee vastaava päättely myös esimerkiksi kertolaskulle.

Esimerkki 40. Osoitetaan, että jos muuttuja y ei esiinny kaavassa $\phi(x)$, niin kaava $(\forall x)\phi(x) \leftrightarrow (\forall y)\phi(y)$ voidaan johtaa tyhjästä oletusjoukosta.

$$\begin{array}{c}
\frac{1) (\forall x)\phi(x)^\vee}{\phi(y)} \text{ (E}\forall \text{)} \quad \frac{2) (\forall y)\phi(y)^\vee}{\phi(x)} \text{ (E}\forall \text{)} \\
\frac{\phi(y)}{(\forall y)\phi(y)} \text{ (I}\forall \text{)} \quad \frac{\phi(x)}{(\forall x)\phi(x)} \text{ (I}\forall \text{)} \\
\frac{(\forall y)\phi(y) \quad (\forall x)\phi(x)}{(\forall x)\phi(x) \leftrightarrow (\forall y)\phi(y)} \text{ (I} \leftrightarrow, 1^\vee, 2^\vee \text{)}
\end{array}$$

Säännön $(I\forall)$ oikea soveltaminen perustuu siihen, että y ei esiinny kaavassa $\phi(x)$.

Esimerkki 41. Osoitetaan, että $(\exists x)\phi(x) \vdash (\exists y)\phi(y)$, jos y esiinny kaavassa $\phi(x)$.

$$\begin{array}{c}
\frac{1) (\exists x)\phi(x) \quad \frac{2) \phi(x)^\vee}{(\exists y)\phi(y)} \text{ (I}\exists \text{)}}{(\exists y)\phi(y)} \text{ (E}\exists, 2^\vee \text{)}
\end{array}$$

Esimerkki 42. Olkoon $+$ edelleen kaksipaikkainen funktiosymboli. Osoittautuu (harjoitustehtävä), että kaavaa $x + z = y + z \rightarrow x = y$ ei voida johtaa tyhjästä oletusjoukosta. Tämän kaavan johtamiseksi otetaan käyttöön vakiosymboli 0 ja kolme oletusta: O1) $(\forall x)(x + 0 = x)$, O2) $(\forall x)(\forall y)(\forall z)(x + (y + z) = (x + y) + z)$ ja O3) $(\forall x)(\exists y)(x + y = 0)$. Näitä oletuksia käyttämällä voidaan johtaa kaava $x + z = y + z \rightarrow x = y$. Johto on pitkä ja siksi se esitetään osissa.

Osa 1: Näytetään, miten oletuksesta O3 johdetaan kaava $(\exists w)(z + w = 0)$:

$$\begin{array}{c}
\frac{O3) (\forall x)(\exists y)(x + y = 0)}{(\exists y)(z + y = 0)} \text{ (E}\forall \text{)} \\
\vdots \\
(\exists w)(z + w = 0)
\end{array}$$

Kvantifioitun muuttujan y vaihto w :ksi, jonka yksityiskohtia ei tässä ole esitetty, tapahtuu kuten esimerkissä 41.

Osa 2: Oletuksesta O1 saadaan kaava $x + 0 = x$ säännöllä $(E\forall)$, samoin siitä saadaan kaava $y + 0 = y$. Säännön $(YS2)$ perusteella näistä saadaan myös $x = x + 0$ ja $y = y + 0$.

Osa 3: Käyttämällä esimerkin 40 deduktiota kolme kertaa peräkkäin saadaan kaava

$$(\forall w_1)(\forall w_2)(\forall w_3)(w_1 + (w_2 + w_3) = (w_1 + w_2) + w_3)$$

ja tästä taas kolme kertaa $(E\forall)$ -sääntöä soveltamalla $(x + z) + w = x + (z + w)$. Samoin oletuksesta O2 johdetaan $(y + z) + w = y + (z + w)$. Soveltamalla sääntöä $(YS2)$ ja $(YS3)$ voidaan saada myös $x + (z + w) = (x + z) + w$.

Nämä osat kootaan yhteen seuraavasti:

$$\begin{array}{c}
\frac{1) x + z = y + z \quad \overline{w = w} \text{ (YS1)}}{(x + z) + w = (y + z) + w} \text{ (YS4)}
\end{array}$$

Näin saatuaan kaavaan otetaan rinnalle osassa 3 oletuksesta O2 johdettu kaava $(x + z) + w = x + (z + w)$, jolloin $(YS3)$:n perusteella saadaan $x + (z + w) = (y + z) + w$. Oletuksesta O2 voitiin myös johtaa $(y + z) + w = y + (z + w)$, mistä yhdessä edellisen kaavan ja säännön $(YS3)$ perusteella saadaan $x + (z + w) = y + (z + w)$. Valitaan tähän rinnalle uusi oletus $2) z + w = 0$. Tämän ja säännön $(YS4)$

perusteella saadaan $x + 0 = y + 0$. Kun tähän rinnalle valitaan osassa 2 johdettu kaava $x = x + 0$, saadaan $x = y + 0$. Tähän tarvitaan edelleen vain osassa 2 johdettu $y + 0 = y$, josta saadaan kaava $x = y$.

Johto ei pääty kuitenkaan tähän, sillä kaavaa $x = y$ johdettaessa valittiin ylimääräinen oletus $^2)(z + w = 0)$. Tästä päästään kuitenkin eroon sääntöä $(E\exists)$ -käyttämällä, sillä tähän asti on (osassa 1) johdettu kaava $(\exists w)(z + w = 0)$

Huomautus 7. Esimerkki 42 korostaa Gentzenin järjestelmän luonnetta kaikkiin yksityiskohtiin tarkertujana. Perusteiden kannalta tämä on tietysti tarpeen, mutta käytännössä yksityiskohtien käsittelyä voidaan välttää joustavammalla esitystavalla. Yksityiskohtien yli on hypätty esimerkiksi huomauttamalla ”Esimerkin ... mukaan voidaan tästä johtaa ...”, mutta tämänkaltaisen esitystapa ei kuulu Gentzenin järjestelmän tiukkoihin rajoituksiin.

Gentzenin järjestelmän sääntöjä tarkastelemalla voidaan melko helposti todeta (joukko harjoitustehtäviä), että järjestelmän säännöillä johdettavat lauseet ovat loogisia seurauksia oletusjoukosta. Tämä voidaan lyhyesti ilmaista seuraavasti:

Lause 3 (Deduktiojärjestelmän terveys). *Jos $\Gamma \vdash \phi$, niin $\Gamma \models \phi$.*

Huomattavasti hankalampaa on todeta päinvastainen: Luonnollisen deduktion säännöt *riittävät* kaikkien joukosta Γ loogisesti seuraavien lauseiden saavuttamiseksi. Tämä logiikan kannalta merkittävä tulos seuraa itse asiassa Kurt Gödelin vuonna 1929 esittämästä täydellisyyslauseesta, mutta sen todistus on aivan liian vaativa esitettäväksi tämän kurssin puitteissa. Symbolein ilmaistuna tämä väittämä on seuraava:

Lause 4 (Deduktiojärjestelmän riittävyys). *Jos $\Gamma \models \phi$, niin $\Gamma \vdash \phi$.*

Lauseet 3 ja 4 muodostavat yhdessä historiallisesti tärkeän kokonaisuuden logiikan kehityksen kannalta. Ne kertovat, että luonnollisen deduktion järjestelmässä premissijoukosta Γ voidaan johtaa *kaikki* siitä loogisesti seuraavat kaavat (tällöin sanotaan, että järjestelmä on *riittävä*), mutta ei mitään mikä ei Γ :sta loogisesti seuraa (tällöin sanotaan, että järjestelmä on *terve*). Deduktiojärjestelmää, joka on sekä terve että riittävä, kutsutaan *täydelliseksi*. Lauseiden 3 ja 4 perusteella Gentzenin luonnollisen deduktion järjestelmä on täydellinen deduktiojärjestelmä.

Palautetaan mieleen käsitteet syntaksi (lauseoppi) ja semantiikka (merkitysoppi). On huomattava, että loogisen seurauksen käsite $\Gamma \models \phi$ rakentuu kokonaan tulkinnoille, siis semantiikalle, kun taas käsite $\Gamma \vdash \phi$ perustuu kaavojen muodolliselle manipulaatiolle, siis syntaksille. Lauseiden 3 ja 4 merkitys voidaan siis ilmaista siten, että ne luovat kaksisuuntaisen sillan syntaksin ja semantiikan välille.

Esimerkki 43. Palataan aiempaan esimerkkiin 42 ja merkitään ϕ :llä kaavaa $x + z = y + z \rightarrow x = y$. On mahdollista löytää tulkinta, jossa ϕ ei ole tosi (harjoitustehtävä). Näin ollen kaavaa ϕ ei voida johtaa tyhjästä oletusjoukosta, sillä jos näin olisi (siis $\emptyset \vdash \phi$), niin lauseen 3 mukaan olisi myös $\emptyset \models \phi$. Tämä puolestaan merkitsisi sitä, että tyhjän joukon mallit (=kaikki tulkinnat) olisivat myös kaavan ϕ malleja, jolloin ϕ olisi siis tautologia. Näin ei kuitenkaan ole, vaan on olemassa tulkinta, jossa ϕ ei ole tosi.

Huomautus 8. $\emptyset \models \phi \Leftrightarrow \emptyset \vdash \phi$ merkitsee siis sitä, että tyhjästä oletusjoukosta voidaan johtaa tarkalleen tautologiat

Luonnollisen deduktion järjestelmän täydellisyys merkitsee sitä, että sen avulla voidaan ainakin jossain määrin *mekanisoida* deduktiivinen päättely. Joissakin tapauksissa looginen seuraussuhde $\Gamma \models \phi$ voidaan kyllä *kumota* semantiikan keinoin (esittämällä vastaesimerkki), mutta sen sijaan seuraussuhteen $\Gamma \models \phi$ *toteennäyttäminen* semantiikan keinoin on yleensä erittäin hankalaa. Tällöin voidaan käyttää lauseiden 3 ja 4 luomaa siltää, jonka avulla voidaan siirtyä semantiikan keinoista Gentzenin järjestelmän syntaktiseen lähestymistapaan.

Palautetaan edelleen mieleen, että kaavan totuus matemaattisessa teoriassa tarkoittaa sitä, että kaava on looginen seuraus teorian aksioomista. Tällöin lauseiden 3 ja 4 mukaan kaavan totuus voidaan ratkaista selvittämällä voidaanko kaava johtaa luonnollisen deduktion järjestelmällä aksioomis- tai ei.

Vaikka luonnollisen deduktion säännöt ovatkin mekaanisesti sovellettavissa, ei kysymyksen $\Gamma \vdash \phi$? ratkaiseminen tästä huolimatta ole suoraviivaista. Jos deduktio $\Gamma \vdash \phi$ (jono kaavoja ja päätelysääntöjä) on olemassa, sellainen on mahdollista löytää, mutta miten voitaisiin näyttää toteen, että deduktiota $\Gamma \vdash \phi$ ei ole olemassa? Mistä hyvänsä kaavajoukosta Γ voidaan luonnollisen deduktion sääntöjä käyttäen johtaa monenlaisia kaavoja, mutta jos ϕ näyttää jäävän deduktion keinoilla saavuttamatta, niin milloin voidaan sanoa, että ϕ :tä ei voida johtaa premissijoukosta Γ ? Kuinka monta yritelmää tarvitaan, jotta voidaan tulla vakuuttuneiksi siitä, että ϕ :tä ei voida Γ :sta johtaa?

Tähän kysymykseen on olemassa selkeä vastaus, joka voidaan johtaa Gödelin, Turingin, tai muiden 1900-luvun laskettavuuden teorian pioneerien töistä:

Lause 5. *Olko Γ äärellinen kaavajoukko ja ϕ kaava. Tällöin ongelma $\Gamma \vdash \phi$ on algoritmisesti ratkeamaton. Erityisesti siis ei ole olemassa mitään mekaanista prosessia, jolla voitaisiin yleisesti selvittää, voidaanko kaavajoukosta Γ johtaa kaava ϕ .*

Näin siis kysymyksen $\Gamma \models \phi$ selvittäminen syntaktisen keinon (deduktiojärjestelmän) kautta vaikuttaa saaneen kovan kolauksen: Vaikka deduktion säännöt ovatkin mekaanisesti sovellettavissa ja tarkistettavissa, ei siitä huolimatta voida algoritmisin keinoin yleisesti selvittää, voidaanko joukosta Γ johtaa kaava ϕ . Tätä tulosta ei kuitenkaan pidä käsittää pelkästään logiikan kannalta ikävänä, sillä ensinnäkin se selkeyttää predikaattilogiikan kokonaiskuvaa: Ilman deduktiojärjestelmää voitaisiin ajatella, että kenties kysymyksen $\Gamma \models \phi$ yleiseksi ratkaisemiseksi olisi jokin muu, toistaiseksi keksimätön algoritmien keino. Lause 5 yhdessä aiempien lauseiden 3 ja 4 kuitenkin sulkee pois kaikki tällaiset keinot.

Toiseksi, lause 5 koskee predikaattilogiikkaa yleisessä muodossa. Jos kaavojen muotoa rajoitetaan jollain tavalla, saattaa algoritmien keino kysymyksen $\Gamma \vdash \phi$? selvittämiseksi hyvinkin löytyä. Esimerkiksi klassisessa, Aristoteleen esittämässä logiikassa käytetään vain yksipaikkaisia predikaattisymboleja ja ainoastaan yhden kvanttorin lauseita. Tarkempi tutkimus paljastaa, että kumpikin näistä rajoituksista yksinään johtaa ratkeavaan logiikkaan, jossa kysymys $\Gamma \vdash \phi$? voidaan algoritmisesti aina selvittää.

Kolmas ja tämän kurssin kannalta tärkein luonnollisen deduktiojärjestelmän anti on, että se järjestelmä esittää selkein kaavioina luonnollisen päättelyn mekanismit. Looginen päättely, jota matematiikassa käytetään, on esitettävissä Gentzenin järjestelmän avulla.

2.4 Deduktion esittäminen käytännössä

Luonnollisen deduktion järjestelmän hyviin piirteisiin kuuluu, että järjestelmän säännöt ovat verrattain vähäiset ja että järjestelmän mekaanisuus on helposti nähtävissä: esimerkiksi ohjelmointitekni- nen toteutus esitetyn deduktion oikeellisuuden tarkistamiseksi on ilmeinen. Järjestelmän haittapuolet käyvät taas selvästi ilmi esimerkeistä 39 ja 42, joista nähdään, että käytännössä Gentzenin järjestelmä on äärimmäisen työläs tavallisten päättelyjen esittämiseen, sillä yleensä ihmisen on helppo mieltää vaikkapa esimerkin 42 monet yhtäsuuruuksia koskevat yksityiskohdat yhdeksi kokonaisuudeksi.

Tämän vuoksi päättelyjä ei yleensä esitetä Gentzenin järjestelmän edellyttämällä tarkkuudella, vaan ilmeiset yksityiskohdat yleensä sivuutetaan. Matemaattiset todistukset kuitenkin edellyttävät, että yksityiskohdat perustellaan huolellisesti. Tässä kurssissa ensisijaiseksi eivät nouse esitystavan muodolliset puitteet, vaan tehtävän/todistuksen loogisten vaiheiden selkeä esittäminen. Esitetään esimerkki 42 väljemmän esitystavan mukaisesti.

Esimerkki 44. Todistetaan seuraava lause:

Lause 6. *Oletuksista 1) $(\forall x)(x+0=x)$, 2) $(\forall x)(\forall y)(\forall z)(x+(y+z)=(x+y)+z)$ ja 3) $(\forall x)(\exists y)(x+y=0)$ voidaan johtaa kaava $x+z=y+z \rightarrow x=y$.*

Todistus. Oletetaan implikaation toteennäyttämistä varten sen vasen puoli $x + z = y + z$. Tästä yhtälöstä seuraa, että mille hyvänsä w :lle $(x + z) + w = (y + z) + w$ (miksi?) ja oletuksen 2 perusteella saadaan yhtälö $x + (z + w) = y + (z + w)$. Oletuksen 3 perusteella w voidaan valita siten, että $z + w = 0$, joten saadaan yhtälö $x + 0 = y + 0$. Oletuksen 1 perusteella tämä voidaan edelleen kirjoittaa muotoon $x = y$.

Vasemmasta puolesta $x + z = y + z$ on siis oletuksia käyttämällä johdettu implikaation oikea puoli $x = y$. $\square$

Esimerkki 45. Osoitetaan, että kaikille reaaliluvuille a ja b pätee $\frac{a^2+b^2}{2} \geq ab$.

Vedotaan tunnettuun ominaisuuteen $(a - b)^2 \geq 0$, joka pätee kaikille reaaliluvuille, vaikka sitä ei ole tässä yhteydessä todistettukaan. Reaalilukujen aksioomista seuraa sievennyssääntöjä, joiden perusteella em. tunnettu ominaisuus saadaan muotoon $a^2 - 2ab + b^2 \geq 0$. Sääntöjen perusteella tämä voidaan edelleen kirjoittaa muotoon $a^2 + b^2 \geq 2ab$ ja vielä $\frac{a^2+b^2}{2} \geq ab$. $\square$

Edellisessä esimerkissä halutun kaavan johto muodostuu, aivan kuten Gentzenin järjestelmässäkin, jonosta kaavoja. Pelkkä jono ei kuitenkaan riitä, vaan kaavojen väliset suhteet on esitettävä. Gentzenin järjestelmässä tämä tehdään ilmoittamalla deduktiosääntö, mutta edellisissä esimerkeissä tämä on tehty sanallisesti. Jos perustelu on ilmeinen, ei sitä tarvitse kirjata näkyviin, vaan riittää kirjoittaa loogisen seuraussuhteen ilmaiseva nuoli ($\Rightarrow$) näkyviin.

Huomautus 9. Deduktiojärjestelmän täydellisyyden perusteella kaikki tautologiat voidaan johtaa tyhjistä oletusjoukosta, joten mikä hyvänsä tautologia voidaan aina lisätä päättelyyn.

2.5 Propositiologiikkaa

Luopumalla kvanttoreista, funktiosymboleista, vakiosymboleista, muuttujasymboleista, yhtäsuuruusmerkistä ja muista kuin nollapaikkaisista relaatiotsymboleista saadaan yksinkertainen logiikan muoto, jota kutsutaan *propositio*- eli lauselogiikaksi. Propositiologiikan yhteydessä nollapaikkaisia predikaattisymboleja $p_1, p_2, p_3, \dots$ kutsutaan *propositiionmuuttujiksi* tai *atomaarisiksi propositiioiksi*. On kuitenkin huomattava, että propositiionmuuttujat eivät sisällä predikaattilogiikan muuttujasymboleja lainkaan, vaan nimitys johtuu ainoastaan siitä, että niiden totuusarvo voi muuttua tulkintaa vaihdettaessa.

Propositiologiikan syntaksi on sama kuin predikaattilogiikankin – tosin huomattavasti yksinkertaisempi, sillä aakkosto on niukempi. Koska vakio- ja funktiosymbolit puuttuvat, ei propositiologiikassa ole termejä lainkaan, vaan perusyksikön muodostavat atomikaavat p_1, p_2, p_3 , joita siis kutsutaan propositiionmuuttujiksi. Atomikaavoista voidaan muodostaa uusia kaavoja (joita kutsutaan *propositiioiksi*) konnektiiveilla aivan samoin kuin predikaattilogiikassakin. Aivan kuten predikaattilogiikassakin, ei propositiionmuuttujien olemuksen kannalta ole tärkeää, että ne esitetään symboleilla $p_1, p_2, p_3, \dots$, vaan usein käytetään merkintöjä $p, q, r, \dots$. Indeksoitu merkintä korostaa lähinnä sitä, että propositiionmuuttujia on käytettävissä ääretön määrä.

Myös propositiologiikan semantiikka on merkittävästi predikaattilogiikan semantiikkaa yksinkertaisempi, sillä vakio- ja muuttujasymbolien sekä kvanttorien puuttuessa ei tulkintajoukkoa tarvita. Riittää tulkita propositiionmuuttujat todeksi tai epätodeksi. Muiden propositioiden totuusarvo määräytyy konnektiivien tulkinnan perusteella.

Esimerkki 46. Selvitetään proposition $(p \wedge \neg q) \vee (((r \wedge \neg q) \wedge \neg r) \vee (p \wedge q))$ totuusarvo, kun p :n, q :n ja r :n totuusarvot ovat 0, 1 ja 1. Ensiksi voidaan todeta, että $\neg q$:n totuusarvo on 0, joten $p \wedge \neg q$:n totuusarvo on 0. Koska myös proposition $\neg r$ totuusarvo on 0, on tällöin proposition $(r \wedge \neg q) \wedge \neg r$ totuusarvo on 0. Seuraavaksi todetaan, että $p \wedge q$:n totuusarvo on 0, mistä seuraa, että päämuodon toisen sulkulausekkeen ja täten myös koko proposition totuusarvo on 0.

Propositiologiikkaa voidaan käyttää yksinkertaisten väitelauseiden totuusarvojen selvittämiseen. Toinen, varsin yleinen käyttötarkoitus löytyy tietotekniikasta: Koska kussakin tulkinnassa propositiionmuuttujat saavat arvon tosi (1) tai epätosi (0), voidaan propositiionmuuttujat ajatella $\{0, 1\}$ -arvoisiksi muuttujiksi. Konnektiiveilla yhdistetyt propositiot saavat myös totuusarvon 0 tai 1, ja siksi propositiot voidaan ajatella $\{0, 1\}$ -arvoisten muuttujien $\{0, 1\}$ -arvoisiksi funktioiksi. Tällöin siis propositioilla voidaan mallintaa *loogisia piirejä*, joiden rakennuspalikoina toimivat $\wedge, \vee$ ja $\neg$ -portit.

Koska propositiologiikka on predikaattilogiikan erikoistapaus, soveltuvat tietysti kaikki predikaattilogiikan termit, kuten looginen seuraus ja ekvivalenssi myös propositiologiikkaan. Lisäksi on mahdollista soveltaa Gentzenin järjestelmää; propositiologiikassa ei vain tarvita lainkaan kvanttori- tai yhtäsuuruussääntöjä. Kuitenkin loogisen seurauksen selvittäminen propositiologiikassa onnistuu aina semantiikan keinoin, nimittäin käymällä läpi kaikkien propositioissa esiintyvien propositiomuuttujien tulkinnat.

Esimerkki 47. Selvitetään, onko propositio $\neg p \rightarrow \neg q$ looginen seuraus propositiosta $p \rightarrow q$. Kirjoitetaan tätä varten totuustaulukko:

p	q	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg p \rightarrow \neg q$
0	0	1	1	1	1
0	1	1	0	1	0
1	0	0	1	0	1
1	1	0	0	1	1

Nähdään, että taulukon toisella rivillä premissi $p \rightarrow q$ on tosi, mutta johtopäätös $\neg p \rightarrow \neg q$ ei. Täten johtopäätös ei seuraa premissistä loogisesti.

Esimerkki 48. Selvitetään, onko propositio q looginen seuraus propositioista p ja $p \rightarrow q$, toisin sanoen, onko päättely $\{p, p \rightarrow q\} \models q$ pätevä. Kirjoitetaan tätä varten totuustaulukko:

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Taulukosta nähdään, että premissit p ja $p \rightarrow q$ ovat yhtäaikaaisesti tosia vain neljännellä rivillä, jolloin myös johtopäätös q on tosi. Näin ollen päättely on loogisesti sitovaa.

Esimerkki 49. Kirjoitetaan lausetta ”Siitä että jos matematiikka on helppoa niin logiikka on helppoa, seuraa että jos logiikka ei ole helppoa, niin ei matematiikka ole helppoa” vastaava propositio ja laaditaan sille totuustaulukko. Valitaan propositiomuuttujiksi p =”matematiikka on helppoa” ja q =”logiikka on helppoa”. Tällöin propositio ”jos matematiikka on helppoa niin logiikka on helppoa” kirjoitetaan $p \rightarrow q$ ja ”jos logiikka ei ole helppoa, niin matematiikka ei ole helppoa” saa muodon $\neg q \rightarrow \neg p$. Alkuperäisen lauseen muotoilu propositiologiikalla on täten $\phi = (p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$. Laaditaan tälle totuustaulukko laatimalla ensin totuustaulukot propositioille $p \rightarrow q$ ja $\neg q \rightarrow \neg p$

p	q	$p \rightarrow q$	$\neg q \rightarrow \neg p$	ϕ
0	0	1	1	1
0	1	1	1	1
1	0	0	0	1
1	1	1	1	1

Totuustaulukosta voidaan huomata, että ϕ on tosi riippumatta propositiomuuttujien p ja q totuusarvoista.

Totuustaulukon rakentaminen.

Sellaista totuustaulukkoa varten, joka esittää n :n propositiomuuttujan mahdolliset tulkinnat, tulee rakentaa kaikki mahdolliset n -pituiset jonot, jotka koostuvat vain nolista tai ykkösistä. Muodostamista varten on ensinnäkin 1-pituiset jonot on helppo luetella: $\{0, 1\}$. Tämän jälkeen 2-pituiset jonot saadaan näistä lisäämällä ensin 0 kumpaisenkin eteen: $\{00, 01\}$ ja sitten 1 kumpaisenkin eteen: $\{10, 11\}$, jolloin siis saadaan yhdistämällä joukko $\{00, 01, 10, 11\}$. Tästä saadaan 3-pituiset jonot lisäämällä 0 jokaisen eteen: $\{000, 001, 010, 011\}$ ja 1 jokaisen eteen: $\{100, 101, 110, 111\}$. Nämä yhdistämällä saadaan 3-pituisten jonojen joukko $\{000, 001, 010, 011, 100, 101, 110, 111\}$ ja samoin jatkamalla saadaan lueteltua yhä pidemmät jonot, jotka koostuvat nolista ja ykkösistä.

Totuustaulukko soveltuu myös mainiosti määritelmän ?? ominaisuuksien (toteutuvuus, kumoutuvuus, tautologisuus, kontradiktivisuus tai kontingenssi) selvittämiseen. Toisaalta taas totuustaulukon laatiminen käy työlääksi propositionmuuttujien määrän kasvaessa: jos propositionmuuttujia on n kappaletta, on tällöin mahdollisia tulkintoja 2^n kappaletta. Tähän liittyy läheisesti teoreettisen tietojenkäsittelytieteen suurin ratkaisematon ongelma, ns. **P** vs. **NP** -ongelma, joka voidaan muotoilla seuraavasti: onko proposition toteutuvuuden selvittämiseksi olemassa (oleellisesti) parempaa menetelmää kuin kaikkien tulkintojen läpikäynti? Jos proposition muotoa ei mitenkään rajoiteta, ei parempaa menetelmää tunneta, muuta joissakin erityistapauksissa päästään parempaan tehokkuuteen. Jos esimerkiksi kaikki propositionit $\phi_1, \dots, \phi_n$ ovat muotoa $p_1 \wedge \dots \wedge p_k \rightarrow q$, tunnetaan tehokas menetelmä sen selvittämiseksi, onko $\phi_1 \wedge \dots \wedge \phi_n$ toteutuva. Kyseinen menetelmä on tärkeä logiikkaohjelmoinnin kannalta (esim. Prolog-kieli). Tehokasta menetelmää proposition toteutuvuuden selvittämiseksi ei kuitenkaan tunneta, ellei proposition muotoa rajoiteta jollakin tavalla.

2.6 Induktioperiaate

Yksi tapa todistaa matemaattinen väittämä oikeaksi äärettömän monen tapauksen kohdalla on ns. *täydellinen induktio*, joka nimestään huolimatta ei ole induktiivista päättelyä, vaan yksi deduktion alalaji. Täydellinen induktio nojautuu nimittäin luonnollisten lukujen *induktioaksioomaan* (katso esimerkki 8), josta voidaan johtaa seuraava muoto:

Lause 7 (Induktioperiaate). Olkoon P yksipaikkainen predikaattisymboli ja $\mathcal{P}$ Peanon aksioomien joukko. Silloin $\mathcal{P} \cup \{P(1), (\forall n)(P(n) \rightarrow P(n+1))\} \models (\forall n)P(n)$.

Todistus. Todistus perustuu luonnollisten lukujen induktioaksioomaan, mutta sivuutetaan tässä.

Sanallisesti ilmaistuna edellinen lause sanoo, että jos jokin ominaisuus P pätee luonnolliselle luvulle 1, sekä jokaiselle luonnolliselle luvulle n on voimassa se, että $P(n)$ implikoi $P(n+1)$:n (toisin sanoen, ominaisuus P periytyy n :ltä $n+1$:lle), niin silloin ominaisuus P on jokaisella luonnollisella luvulla.

Induktioperiaatetta voidaan kuvata 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 kaatuvat. Juuri tämä on induktioperiaatteen takana piilevä intuitio.

Getzenin järjestelmän mukaan väite $(\forall n)(P(n) \rightarrow P(n+1))$ näytetään toteen osoittamalla, että $P(n) \rightarrow P(n+1)$ pätee, kun luku n ei ole sidottu missään todistuksen kaavassa. Intuitiivisesti tämä merkitsee sitä, että luku n on ”vapaa” eikä sen suhteen ole tehty mitään oletuksia. Väittämä $P(n) \rightarrow P(n+1)$ puolestaan näytetään toteen ensin olettamalla $P(n)$ ja johtamalla tästä $P(n+1)$ (vrt. Gentzenin järjestelmä).

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

2.7 Induktiotodistuksia

Sanotaan, että jono $x_1x_2\dots x_n$, on n -pituinen *bittijono*, jos kullekin muuttujalle x_i annetaan arvoksi joko 0 tai 1. Seuraavassa lauseessa selvitetään n -pituisten bittijonon määrää.

Lause 8. n -pituisia bittijonoja on 2^n kappaletta.

Todistus. Todistus voidaan suorittaa täydellisellä induktiolla. Olkoon n -pituisten bittijonon määrä $B(n)$ ja $P(n)$ väite $B(n) = 2^n$, jolloin siis induktioperiaatteen mukaan on todistettava $P(1)$ ja

$(\forall n)(P(n) \rightarrow P(n+1))$. Väite $P(1)$ tarkoittaa sitä, että $B(1) = 2^1$ (yhden pituisten bittijonojen määrä on 2), mikä on selvästi tosi.

Suoritetaan seuraavaksi induktioaskel, eli näytetään toteen implikaatio $(\forall n)(P(n) \rightarrow P(n+1))$. Tätä varten näytetään toteen implikaatio $P(n) \rightarrow P(n+1)$, 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 $P(n) \rightarrow P(n+1)$. Tästä seuraa $(\forall n)(P(n) \rightarrow P(n+1))$, sillä luku n ei esiinny missään poistamattomassa oletuksessa (siitä ei siis oletettu mitään).

On myös mahdollista määritellä käsitteitä induktiivisesti:

Edellinen määritelmä kattaa kaikki luonnolliset luvut (ja nollan), koska 1) $1!$ on määritelty ja 2) jos $n!$ on määritelty, niin myös $(n+1)!$ on määritelty.

Huomautus 10. Edellisestä määritelmästä seuraa suoraan, että $n! = n \cdot (n-1)! = n \cdot (n-1) \cdot (n-2)! = \dots = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 2 \cdot 1$. Kertoma $n!$ ilmaisee niiden jonojen määrän, jotka voidaan muodostaa luvuista $\{1, 2, \dots, n\}$ valitsemalla yksi luku vain kerran.

Tämän luvun lopuksi esitettävää binomikaavaa varten määritellään 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.

Esimerkki 50.

$$\binom{m}{0} = \frac{m!}{0! \cdot (m-0)!} = \frac{m!}{m!} = 1, \quad \binom{m}{1} = \frac{m!}{1! \cdot (m-1)!} = \frac{m \cdot (m-1)!}{(m-1)!} = m, \\ \binom{m}{2} = \frac{m!}{2 \cdot (m-2)!} = \frac{m(m-1) \cdot (m-2)!}{2 \cdot (m-2)!} = \frac{m(m-1)}{2}.$$

Lause 9. 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:

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

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 11. Lauseen 9 mukaisesti binomikertoimet muodostavat ns. *Pascalin kolmion*, jonka kukin alkio askemalla yläoikealla ja ylävasemmalla olevat alkioit yhteen:

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

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

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

mistä jakolaskulla ja määritelmiä soveltamalla saadaan

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

Esimerkki 51. Joukosta $\{1, 2, 3, \dots, 39\}$ voidaan valita 7 numeroa $\binom{39}{7} = \frac{39!}{7!32!} = 15380937$ eri tavalla.

Lause 10 (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 $(\forall n)(P(n) \rightarrow P(n+1))$: 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 $(I \rightarrow)$ -säännön nojalla on johdettu $P(n) \rightarrow P(n+1)$ 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 $(\forall n)(P(n) \rightarrow P(n+1))$. 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 Arkhimedeeseen ohella maailmanhistorian merkittävimpien matemaatikkojen joukkoon.

(kuva: Wikimedia Commons)

Luvun oleellisia asioita:

- Matematiikan perustana toimivat aksioomat, lauseita eli teorian väittämiä johdetaan päättelämällä.
- Deduktio on ainoa matematiikassa käytettävä päättelyn muoto.
- Predikaattilogiikka formalisoi väittämiä, joissa väitelauseilla voi olla sisäinen rakenne: perusosina toimivat termit, joista voidaan rakentaa kaavoja, joita voidaan yhdistää konnektiiveilla ja kvantifioida.
- Predikaattilogiikan tulkinnan peruspilarit ovat tulkintajoukko sekä funktio- ja predikaattisymbolien tulkinta.
- Looginen seuraus: $\Gamma \models \phi$, jos Γ :n mallit ovat myös ϕ :n malleja.
- Luonnollisen deduktion järjestelmä on tavallisten päättelymekanismien formaalinen (muodollinen) esitys.

- Propositiologiikassa ei esiinny termejä eikä kvanttoareita, vaan ainoastaan nollapaikkaisia predikaatisymboleja, joita kutsutaan propositiomuuttujiksi.
- Propositiologiikan tulkinta perustuu propositiomuuttujien tulkintaan todeksi tai epätodeksi.
- Matemaattinen induktio (osattava!) on yksi tapa osoittaa väittämä todeksi äärettömän monelle arvolle, mutta nimestään huolimatta on yksi deduktion muoto.

Luku 3

Joukko-oppia

3.1 Joukko-opin peruskäsitteet

Käsite *joukko* on yksi matematiikan tärkeimmistä. Matemaattisia teorioita esittäessä predikaattilogiikan avulla tulee aina valita tarvittavat predikaatti- ja funktiosymbolit, joilla teorian objekteista voidaan puhua. Osoittautuu, että lähestulkoon kaikki matematiikka voidaan rakentaa joukko-opin varaan, jolloin siis periaatteessa riittää esittää joukko-oppi aksiomatisoituna teoriana ja sopia, että muut matemaattiset käsitteet ovat lyhennysmerkintöjä joukko-opin merkinnöistä.

Tämän kurssin tavoitteiden kannalta ei ole mielekäästä esittää aksiomaattista perustaa joukko-opille, joten tyydytään sen sijaan intuitiiviseen käsitykseen.

***Joukko** koostuu mistä hyvänsä olioista, mutta on voitava tarkoin määritellä ainakin periaatteessa, kuuluuko jokin olio joukkoon vai ei. Olioita, joista joukko koostuu, kutsutaan alkioiksi.*

Esimerkki 52. Joukon merkintänä käytetään aaltosulkuja $\{ \}$. Äärellinen joukko voidaan määritellä aina luettelemalla sen alkiot. Täten siis $A = \{1, 2, 3\}$ merkitsee sitä, että joukko A koostuu luvuista 1, 2 ja 3, jotka ovat siis joukon A alkiot.

Joukon merkinnässä alkioden järjestyksellä ei ole väliä. Täten siis $\{2, 3, 1\}$ on sama joukko kuin $\{1, 2, 3\}$. Joukko ei myöskään sisällä samaa alkioita kahteen kertaan, joten on sovittu, että esimerkiksi myös merkintä $\{1, 1, 2, 3\}$ tarkoittaa joukkoa $\{1, 2, 3\}$.

Joskus myös ääretön joukko määritellään ”esittelemällä” sen alkiot. Näin voidaan tehdä, mikäli on olemassa jokin *induktiivinen sääntö*, joka määrittää kaikki alkiot.

Esimerkki 53. Luonnollisilla luvuilla tarkoitetaan joukkoa $\mathbb{N} = \{1, 2, 3, \dots\}$.

Käsitteen joukko kuvailussa on oleellista, että voidaan aina määrittää kuuluuko jokin alkio joukkoon vai ei. Tähän liittyvät matemaattiset merkinnät esitellään seuraavassa määritelmässä.

Esimerkki 54. $B = \{x \in A \mid x \leq 2\}$ tarkoittaa joukkoa, joka sisältää joukkoon A kuuluvat alkiot x , jotka ovat suuruudeltaan korkeintaan 2. Jos siis A on esimerkin 52 joukko, on $B = \{1, 2\}$.

Joukko-opin tärkein anti matematiikalle on mahdollisuus laskea käsitteet yksinkertaiselle pohjalle. Yleensä matemaattisen teorian esittämisessä käytetään funktio- ja relaatiotymboleja, mutta periaatteessa lähes kaikki matematiikka on mahdollista rakentaa käyttämällä vain yhtä relaatiota ($\in$) ja sopimalla pidemmälle menevät määritelmät lyhennysmerkinnöiksi.

Esimerkki 55. Tyhjä joukko $\emptyset$ on eri asia, kuin joukko $\{\emptyset\}$, jonka ainoa alkio on tyhjä joukko. Edelleen eri käsite on joukko $\{\emptyset, \{\emptyset\}\}$, joka sisältää kaksi edellistä joukkoa. Näistä esitetyistä joukoista voidaan rakentaa yhä uusia muodostamalla joukko, jonka jäseninä ovat kaikki entiset joukot. Listan seuraava jäsen on täten $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}$ ja yleinen sääntö on seuraava: $N_0 = \emptyset$, $N_i = N_{i-1} \cup \{N_{i-1}\}$.

Jos joukko-opille on luotu kestävä perusta, on sen nojalla yllämainittujen joukkojen olemassaolo ja uusien muodostaminen edellämaitulla tavalla ongelmattonta. Tällöin voidaan sopia, että joukosta $\emptyset$ käytetään merkintää 0, joukosta $\{\emptyset\}$ merkintää 1, joukosta $\{\emptyset, \{\emptyset\}\}$ merkintää 2 jne. Tällä tavoin on mahdollista esittää luonnolliset luvut pelkästään joukko-opin käsitteiden avulla.

Lähes kaikki matemaattiset kaavat, lauseet ja todistukset voidaan kirjoittaa ja niiden merkitys voidaan periaatteessa ymmärtää ainoastaan joukko-opin merkintöjä käyttäen. Monet oleelliset käsitteet kuten funktio *määritellään* joukkojen avulla (Luvussa 4.3 nähdään kuinka tämä tapahtuu).

Voidaan oikeutetusti kysyä miksi sitten joukot ja joukko-oppi eivät näytä olevan erityisen tärkeitä matematiikan opiskelussa eivätkä edes kovinkaan usein matemaatikkojen työskentelyssä. Vastaus on varsin yksinkertainen: pelkästään joukko-opin merkintöjä ja käsitteitä käyttäen kaavoista, todistuksista ja käsitteistä tulisi varsin pitkiä ja työläitä ymmärtää, minkä vuoksi tarvitaan selkeämpiä merkintöjä ja käsitteitä.

Samankaltainen ilmiö nähdään myös ohjelmoinnissa: nykyisin enää aniharva ohjelmoi konekielellä, koska korkeamman tason ohjelmointikielillä työ on selkeämpää ja usein tarkoituksenmukaisempaa. Kuitenkin korkean tason ohjelmointikielten toiminta voidaan selittää konekielen avulla. Matematiikassa voidaan joukko-opin käsitteiden ajatella vastaavan konekieltä ja tavallisesti esiintyvien käsitteiden vastaavan korkean tason ohjelmointikieltä. Joukko-opin peruskäsitteet kuitenkin esiintyvät matematiikassa toisinaan, minkä vuoksi niihin pitää perehtyä.

3.2 Tärkeimmät lukujoukot

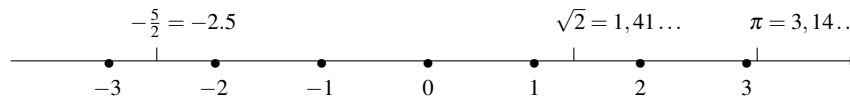
Joukko on käsitteenä tarkoin määritelty, kun sen alkiot tunnetaan. Tällöin ei siis ole tarpeen perehtyä alkoiden sisäiseen rakenteeseen tai olemukseen, ei siis tarvitse tietää minkälaisia ”olioita” joukon alkiot ovat, riittää tietää sisältyykö jokin alkio joukkoon vai ei.

Perinteisesti matematiikassa *lukujoukot* ovat olleet erityisasemassa jo historiallisista syistä. Tämän kurssin kannalta tärkeimmät lukujoukot luetellaan seuraavassa määritelmässä.

Luonnollisten lukujen ja reaalilukujen aksioomat on esitetty aiemmin luvussa 2, mutta yllä esitetyt joukot käsitetään tässä kurssista kaikesta huolimatta intuitiivisella tasolla, sillä todistusten esittäminen aksioomista lähtien veisi kohtuuttomasti resursseja. Joukkoa $\mathbb{Z}$ pidämme intuitiivisesti selvänä käsitteinä ja kommentoimme lyhyesti lukujoukkoja $\mathbb{Q}$ ja $\mathbb{R}$. Kompleksilukujen joukkoa $\mathbb{C}$ tarkastellaan luvussa 6.

Määritelmien ?? ja ?? mukaan $\mathbb{Q}$ koostuu siis sellaisista osamääristä $\frac{a}{b}$, joissa a ja b ovat kokonaislukuja, ja $b \neq 0$. Samaa osamäärää voidaan esittää monella tavalla: $\frac{1}{2} = \frac{2}{4} = \frac{4}{8} = \dots$, mutta kuten aiemmin on mainittu, alkion useat mahdolliset esitykset eivät muuta joukkoa: $\{\frac{1}{2}, \frac{2}{4}, \frac{4}{8}\} = \{\frac{1}{2}\}$. Rationaalilukujen joukko $\mathbb{Q}$ voidaan katsoa kokonaislukujen joukon $\mathbb{Z}$ laajennukseksi, sillä jokainen kokonaisluku a voidaan esittää osamääränä $a = \frac{a}{1}$.

Reaaliluvut $\mathbb{R}$ täydentävät rationaalilukujen joukkoa siten, että lukusuorasta muodostuu yhtenäisen jatkumo (kuva 3.1).



Kuva 3.1 Lukujen ajatellaan sijoittuvan lukusuoralle suuruusjärjestyksessä vasemmalta oikealle. Kokonaisluvut muodostavat tasavälisen pisteistön, kun taas rationaaliluvut levittäytyvät lukusuoralle tiheänä joukkona. Aukoton lukusuorasta tulee kuitenkin vasta, kun reaaliluvut tuodaan mukaan.

Jokaisella reaaliluvulla on olemassa desimaaliesitys, joka useimmissa tapauksissa on päättymätön. Sanotaan, että desimaaliesitys on päättävä, jos kaikki desimaalit ovat nollija jostakin rajasta lähtien, jolloin voidaan tietenkin jättää loputon nollien jono merkitsemättä.

Esimerkki 56. Rationaaliluvulla $\frac{1}{3}$ on päättymätön desimaaliesitys $\frac{1}{3} = 0,333\dots$, sen sijaan rationaaliluvulla $\frac{1}{5}$ on päättävä esitys $\frac{1}{5} = 0,2000\dots$, mikä yleensä merkitään $\frac{1}{5} = 0,2$.

Päättävä desimaaliesitys (toisin sanoen sellainen desimaaliesitys, jossa kaikki desimaalit ovat nollija jostakin kohdasta lähtien) voi olla vain rationaaliluvulla. Mikäli rationaaliluvun desimaaliesitys ei ole päättävä, se on jaksollinen. Toisaalta taas rationaaliluvun desimaaliesitys ei välttämättä ole yksikäsitteinen: Esimerkiksi kokonaisluvulla 1 on sekä päättävä desimaaliesitys $1,000\dots$ että päättymätön jaksollinen desimaaliesitys $0,999\dots$. Itse asiassa jokaista päättävää desimaaliesitystä kohti voidaan löytää samaa lukua esittävä päättymätön esitys samoin kuin esimerkiksi luvulle $0,5000\dots = 0,4999\dots$.

Tavanomaisia merkintöjä ovat myös seuraavat:

- $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$ (suljettu väli)
- $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$ (avoin väli)
- $[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$ (puoliavoin väli, analogisesti $(a, b]$)
- $[a, \infty) = \{x \in \mathbb{R} \mid a \leq x\}$ (suljettu puolisuora, analogisesti $(-\infty, a]$)
- $(a, \infty) = \{x \in \mathbb{R} \mid a < x\}$ (avoin puolisuora, analogisesti $(-\infty, a)$)

3.3 Joukkojen väliset suhteet ja operaatiot

Luvun alussa mainittiin, että lähes kaikki matematiikka voidaan periaatteessa palauttaa joukkooppiin. Tämä tietysti edellyttää, että joukoille voidaan määritellä operaatiota, joiden avulla entisistä joukoista voidaan rakentaa uusia. Tässä ja seuraavassa luvussa määritellään kurssin kannalta tarpeellisia joukko-opillisia operaatiota.

Huomautus 12. Joissakin oppikirjoissa aito sisältyminen merkitään $A \subset B$, kun taas toisissa kirjoissa $A \subset B$ saattaa tarkoittaa myös tilannetta, joissa joukot A ja B ovat yhtäsuuret. Joukkojen sisällymistä koskevat merkinnät on tarkistettava kirjan johdannosta. Tässä kurssissa käytetään yllä olevan määritelmän mukaisia merkintöjä.

Esimerkki 57. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

Esimerkki 58. Olkoon $A = \{1, 2\}$, $B = \{1, 2, 3\}$ ja $C = \{2, 3\}$. Tällöin $A \subseteq B$, $C \subseteq B$, mutta sen sijaan $A \not\subseteq C$ ja $C \not\subseteq A$.

Esimerkki 59. Olkoot A , B ja C kuten esimerkissä 58. A :n ja C :n yhdiste $A \cup C = \{1, 2, 2, 3\} = \{1, 2, 3\} = B$, kun taas A :n ja C :n leikkaus $A \cap C = \{2\}$.

Esimerkki 60. Olkoot A , B ja C kuten esimerkissä 58. Tällöin $B \setminus A = \{3\}$, $B \setminus C = \{1\}$ ja $A \setminus B = \emptyset$.

Huomautus 13. On helppo huomata, että joukkojen yhdiste eikä leikkaus riipu järjestyksestä, siis

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

Tällöin voidaan useampikertaisissa yhdisteissä ja leikkauksissa jättää sulkeet kirjoittamatta ja merkitä ainoastaan $A \cup B \cup C$ sekä $A \cap B \cap C$. Sama pätee myös mikäli joukkoja on enemmän kuin kolme.

Lisäksi käytetään merkintöjä $\bigcup_{i=1}^k A_i = A_1 \cup A_2 \cup \dots \cup A_k$ sekä $\bigcap_{i=1}^k A_i = A_1 \cap A_2 \cap \dots \cap A_k$.

Esimerkki 61. $\bigcup_{n=1}^{\infty} (n, n+1] = (1, \infty)$, kun taas $\bigcap_{n=1}^{\infty} (-\frac{1}{n}, \frac{1}{n}) = \{0\}$.

Edellisessä määritelmässä joukkoja oli ääretön jono A_1, A_2, A_3 , jolloin siis luonnolliset luvut $\mathbb{N}$ indeksoivat joukot. Äärettömän monen joukon yhdiste ja leikkaus voidaan yleistää tästäkin.

Esimerkki 62. Jos $A = \{1, 2\}$, ovat A :n osajoukot $\emptyset$, singletonit $\{1\}$ ja $\{2\}$, sekä A itse. Täten siis $2^A = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

Potenssijoukon erikoiselta vaikuttava merkintä ja nimi saavat selityksensä seuraavan lauseen myötä.

Lause 11. Jos $|A|$ on äärellinen, niin $|2^A| = 2^{|A|}$.

Todistus. Täydellisellä induktiolla: Montako osajoukkoa on yhden, kahden, kolmen, jne. alkion joukolla? (harjoitustehtävä).

3.4 Perusjoukko ja komplementti

Usein tarkastelun kohteena on jonkin tietyn joukon osajoukot. Insinöörimatematiikan kursseissa on yleensä hyödyllistä valita tällaiseksi kiinteäksi tarkastelun kohteeksi reaalityöjoukko $\mathbb{R}$ tai kompleksilukujen joukko $\mathbb{C}$.

Tarkasteltaessa joukon P (tässä kurssissa yleensä $\mathbb{R}$ tai $\mathbb{C}$) osajoukkoja kutsutaan P :tä yleensä *perusjoukoksi*. Perusjoukko ei siis ole kiinteästi määritelty matemaattinen käsite, vaan riippuu asiayhteydestä.

Lause 12. Olkoon $A \subseteq P$. Tällöin $A \cap \bar{A} = \emptyset$ ja $A \cup \bar{A} = P$, missä $\bar{A}$ tarkoittaa komplementtia perusjoukon P suhteen.

Todistus. Ensimmäisen väitteen todistus perustuu siihen, että tyhjä joukko on määritelmän mukaan joukko, jossa ei ole yhtään alkia. Tällöin siis tulee näyttää toteen, että mille tahansa x :lle pätee $x \notin A \cap \bar{A}$. Jos $x \notin A$, ei x myöskään voi olla leikkauksessa $A \cap \bar{A}$. Oletetaan sitten, että $x \in A$. Tällöin määritelmän mukaan $x \notin P \setminus A = \bar{A}$, joten $x \notin A \cap \bar{A}$.

Toista väitettä varten taas osoitetaan, että joukoilla P ja $A \cup \bar{A}$ on samat alkiot, siis kaikille x :ille $x \in P \Leftrightarrow x \in A \cup \bar{A}$.

Ekvivalenssia varten oletetaan ensin, että $x \in P$. Tällöin on kaksi vaihtoehtoa: $x \in A$ tai $x \notin A$. Jos $x \in A$, on myös $x \in A \cup \bar{A}$, sillä $A \subseteq A \cup \bar{A}$. Jos taas $x \notin A$, on $x \in P \setminus A = \bar{A}$ ja siis $x \in A \cup \bar{A}$. Nähtiin siis että oletuksesta $x \in P$ seuraa $x \in A \cup \bar{A}$ kummassakin tapauksessa.

Oletetaan sitten, että $x \in A \cup \bar{A}$ ja näytetään, että $x \in P$. Taas on kaksi vaihtoehtoa: $x \in A \subseteq P$, jolloin selvästi $x \in P$, tai $x \in \bar{A} = P \setminus A$, jolloin taas $x \in P$. Nähtiin siis että oletuksesta $x \in A \cup \bar{A}$ seuraa $x \in P$. $\square$

Huomautus 14. Lause 12 kertoo sen yksinkertaisen tosiasian, että perusjoukon P osajoukon A komplementti $\bar{A}$ sisältää tarkalleen ne alkiot, joita A ei sisällä. Tällöin A :lla ja $\bar{A}$:lla ei ole yhteisiä alkioita, ja A ja $\bar{A}$ yhdessä muodostavat tarkalleen koko perusjoukon P .

Lause 13. $\overline{\bar{A}} = A$.

Todistus. Väitettä varten osoitetaan, että kaikille x :ille $x \in A \Leftrightarrow x \in \overline{\bar{A}}$.

Oletetaan ensin, että $x \in \overline{\bar{A}} = P \setminus \bar{A}$, jolloin $x \notin \bar{A} = P \setminus A$. Tällöin on oltava $x \in A$.

Oletetaan sitten, että $x \in A$. Tästä seuraa, että $x \notin P \setminus A = \bar{A}$. Edelleen tästä seuraa, että $x \in P \setminus \bar{A} = \overline{\bar{A}}$. $\square$

Huomautus 15. Lause 13 voidaan sanallisesti ilmaista sanomalla että komplementin komplementti on alkuperäinen joukko itse.

3.5 Osittelulait ja De Morganin lait

Kertolasku toteuttaa distribuutio- eli osittelulain yhteenlaskun suhteen: $a(b+c) = ab+ac$. Joukko-opissa leikkaus toteuttaa samankaltaisen lain unionin suhteen ja päinvastoin. Tämä on ilmaistu seuraavassa lauseessa.

Lause 14. *Kaikille joukoille A , B ja C pätee $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ja $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.*

Todistus. Harjoitustehtävä.

Osittelulakien lisäksi on syytä mainita seuraavat *De Morganin* lait.

Lause 15. *Olko A ja B jonkin perusjoukon P osajoukkoja. Tällöin $\overline{A \cup B} = \bar{A} \cap \bar{B}$ ja $\overline{A \cap B} = \bar{A} \cup \bar{B}$.*

Todistus. Harjoitustehtävä.

Esimerkki 63. Olko A , B ja C perusjoukon P osajoukkoja. Tällöin seuraavat säännöt pätevät:

1. $A \cap (B \cap C) = (A \cap B) \cap C$ ja $A \cup (B \cup C) = (A \cup B) \cup C$ (lause 7)
2. $A \cap B = B \cap A$ ja $A \cup B = B \cup A$ (Huomautus 3.3)
3. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ja $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (lause 14)
4. $A \cap P = A$ ja $A \cup \emptyset = A$ (seuraa suoraan ehdosta $A \subseteq P$ ja tyhjän joukon määritelmästä)
5. $A \cap \bar{A} = \emptyset$ ja $A \cup \bar{A} = P$ (lause 9)

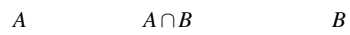
Edellisen esimerkin säännöt kertovat, että joukot muodostavat ns. Boolean algebran. Samankaltainen rakenne saadaan aikaan propositiomuuttujien ekvivalenssiluokille korvaamalla leikkaus $\wedge$:illa, unioni $\vee$:illa ja komplementti $\neg$:illa.

3.6 Vennin Diagrammit

Vennin diagrammi on joukon käsitettä havainnollistava graafinen esitys. Perusjoukkoa kuvataan yleensä suorakulmiolla, jonka sisällä olevat ympyrät esittävät osajoukkoja. Tällöin unioni, leikkaus ja komplementti saavat kuviosta havainnollisen tulkinnan (kuva 3.2).

Luvun oleellisia asioita:

- Teoreettisesti joukko on tärkeä käsite matematiikassa: sen varaan voidaan perustaa suurin osa matematiikasta.
- Lukujoukot $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ (viimeisintä käsitellään myöhemmin)
- Operaatiot leikkaus, unioni, erotus, komplementti, potenssijoukko.
- Osittelulait ja De Morganin lait



A $A \cap B$ B

Kuva 3.2 Vennin diagrammissa suorakulmio esittää perusjoukkoa, ympyrät A ja B sen osajoukkoja. Alue, jonka kumpikin ympyrä peittää, esittää leikkausta $A \cap B$, kun taas alue, jonka ympyrät kokonaisuudessaan peittävät, esittää unionia $A \cup B$.

Luku 4

Relaatiot ja funktiot

Polynomilausekkeet, kuten $x^2 + 3x + 2$ määrittelevät funktion, jossa x kuvautuu luvuksi $f(x) = x^2 + 3x + 2$. Tämänkaltaisen 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 itsestään selvää voidaanko tällainen funktio määritellä millään lausekkeella. Tässä luvussa perehdytään yleisimpään mahdolliseen funktion määritelmään.

4.1 Karteesinen tulo

1600-luvun alkupuolella René Descartes kehitti idean, joka mullisti matematiikan ja fysiikan kehityksen. Nykyajan koululaiset tuntevat Descartesin keksinnön xy -koordinaatistona, jossa tason pisteitä edustaa kaksi koordinaattia. Descartesin xy -koordinaatisto onkin tunnetuin esimerkki *karteesisesta tulosta*. Ideaa voidaan luonnehtia vallankumoukselliseksi, 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. Kyseessä on siis geometrian ja algebran yhdistäminen. Tässä luvussa voidaan kuitenkin havaita, että Descartesin idea kantaa paljon kauemmaksi kuin tason käyrien kuvailuihin.

Taustatietoa

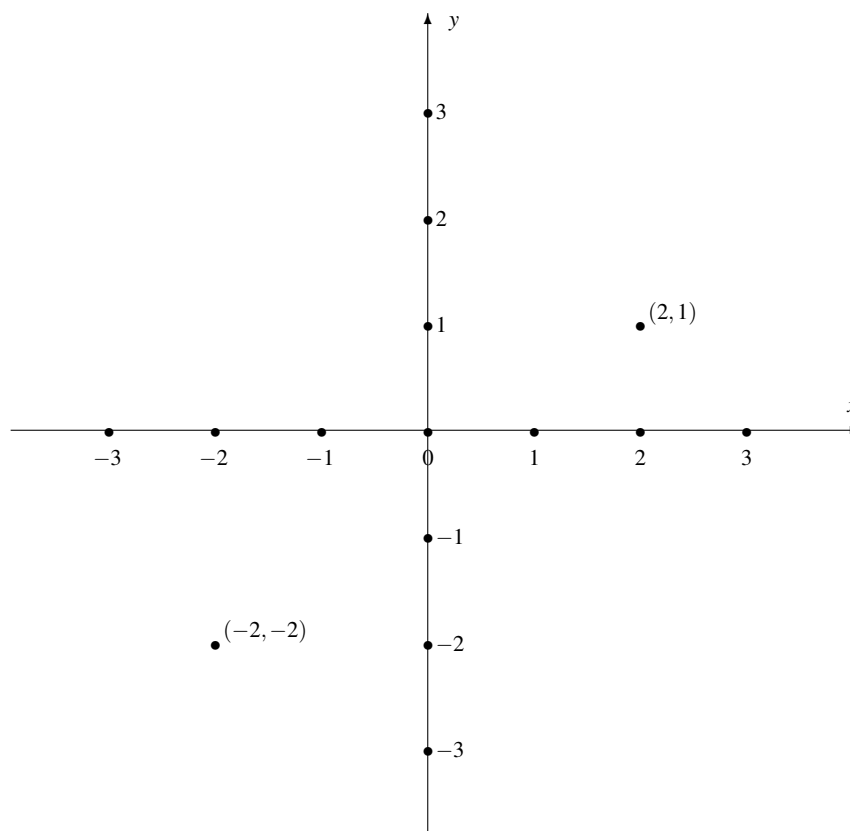


René Descartes (latin. *Renatus Cartesius*, 1596–1650) oli ranskalainen matemaatikko ja filosofi, jota pidetään nykyaikaisen filosofian perustajana. Descartes kehitti *analyttisen geometrian* esittämällä tason pisteet reaalitylukupareina. Analyttisen geometrian perustaminen oli oleellinen edistysaskel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

(kuva: Wikimedia Commons)

Descartesin tasossa on siis itse asiassa kaksi reaaliakselia asetettuna kohtisuoraan toisiaan vastaan. Tällaisesta tasosta käytetään merkintää $\mathbb{R}^2$ ja sitä havainnollistaa kuva 4.1. Kuvassa 4.2 puolestaan on esimerkki tasokäyrästä (origokeskinen yksikköympyrä), joka voidaan ilmaista koordinaattien välisenä algebrallisena yhtälönä $x^2 + y^2 = 1$.

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.



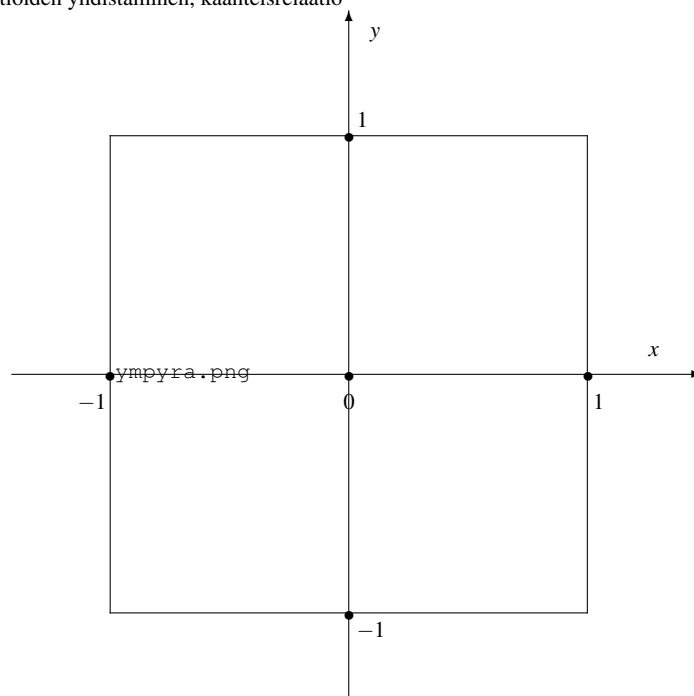
Kuva 4.1 Karteesinen tulo $\mathbb{R}^2$ esitetään yleensä tason pisteistönä. Tavallisesti vaaka-akselia nimitetään x -akseliksi ja pystyakselia y -akseliksi. Kuvassa on edustettuna vain joitakin pisteitä, mutta $\mathbb{R}^2$ sisältää *kaikki* tason pisteet.

Lähdetään siis selvittämään, mitä tason piste (x, y) tarkoittaa matemaattisesti ja samalla yleistetään reaalitaso korvaamalla reaaliakselit akseleilla, joihin liitetään mikä hyvänsä joukko.

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) .

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



Kuva 4.2 Yksikköympyrän $x^2 + y^2 = 1$ graafinen esitys.

Esimerkki 64. Olkoot A ja B edelleen kuten esimerkissä 58. 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 65. $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$ 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 4.1.

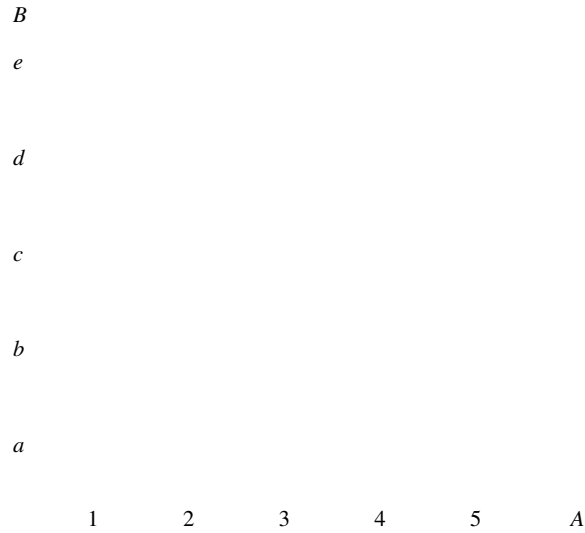
Usein tarvitaan sellaista karteesisen tulon erikoistapausta, jossa $A = B = C$. Tällöin merkitään $A \times A = A^2$ ja $A \times A \times A = A^3$, jne. Karteesisella tulolla $\mathbb{R}^2$ on luonnollinen tulkinta tason pisteinä (Kuva 4.1) ja $\mathbb{R}^3$:lla kolmiulotteisen avaruuden pisteinä. Myös karteesiset tulot $\mathbb{R}^4, \mathbb{R}^5, \dots$ ovat käyttökelpoisia lukuisissa sovelluksissa, vaikka näitä ei voidakaan visualisoida samoin kuin joukkoja $\mathbb{R}^2$ ja $\mathbb{R}^3$.

4.2 Relaatio, relaatioiden yhdistäminen, käänteisrelaatio

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 esitä mitään mielenkiintoista yhteyttä joukkojen A ja B välillä, vaan *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 4.3)

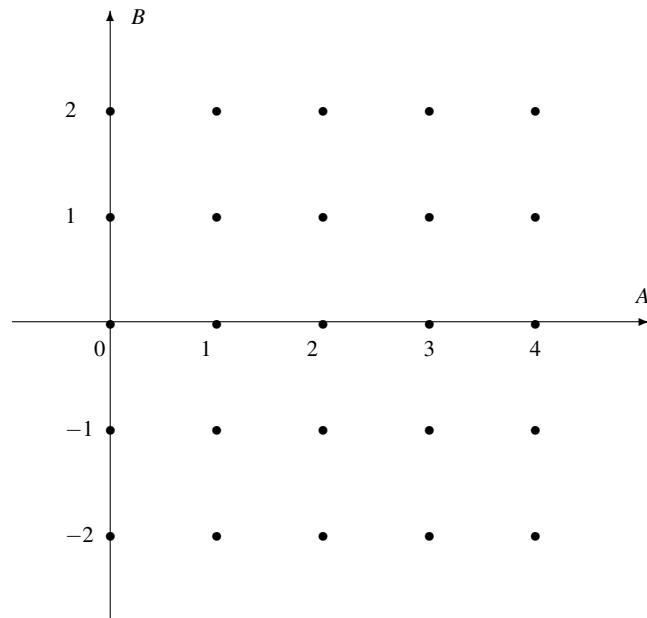
Esimerkki 66. Jos $R \subseteq A \times B$ on relaatio joukosta A joukkoon B , niin $(a, b) \in R$ merkitään tavallisemmin aRb . Esimerkiksi tavallinen $<$ (pienempi kuin) on joukon $\mathbb{N}$ binäärinen relaatio, mutta on tavanomaisempaa merkitä $2 < 3$ kuin $(2, 3) \in <$ tai $< (2, 3)$.

Esimerkki 67. Joukon A binääristä relaatiota $R = \{(a, a) \mid a \in A\}$ kutsutaan joukon A *identiteettirelaatioksi* tai *diagonaalirelaatioksi*.

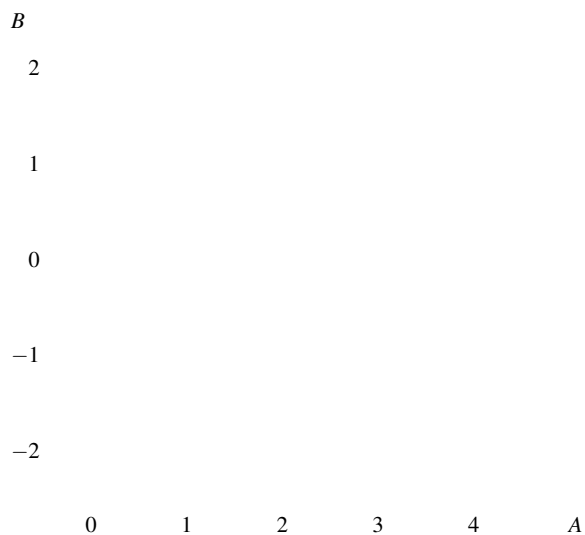


Kuva 4.3 Tässä kuviossa $A = \{1, 2, 3, 4, 5\}$ ja $B = \{a, b, c, d, e\}$ ja kuvan esittämä relaatio $R \subset A \times B$ koostuu pikseleistä $\{(1, a), (1, b), (2, b), (2, c), (2, d), (3, b), (3, d), (3, e), (4, b), (4, c), (4, d), (5, a), (5, b)\}$. Vaaka-akselia voidaan kutsua A -akseliksi ja pystyakselia B -akseliksi.

Esimerkki 68. Olkoon $A = \{0, 1, 2, 3, 4\}$ ja $B = \{-2, -1, 0, 1, 2\}$. Tällöin karteesinen tulo $A \times B$ muodostuu kuvassa 4.4 esitetystä pisteistöstä. Vaihtoehtoisesti, karteesinen tulo $A \times B$ voidaan esittää pikselimuodossa kuvan 4.5 mukaisesti



Kuva 4.4 Esimerkin 68 karteesinen tulo $A \times B$ koostuu kuvassa esitetystä $5 \cdot 5 = 25$:stä pisteestä. Vaaka-akselia voidaan kutsua A -akseliksi ja pystyakselia B -akseliksi.

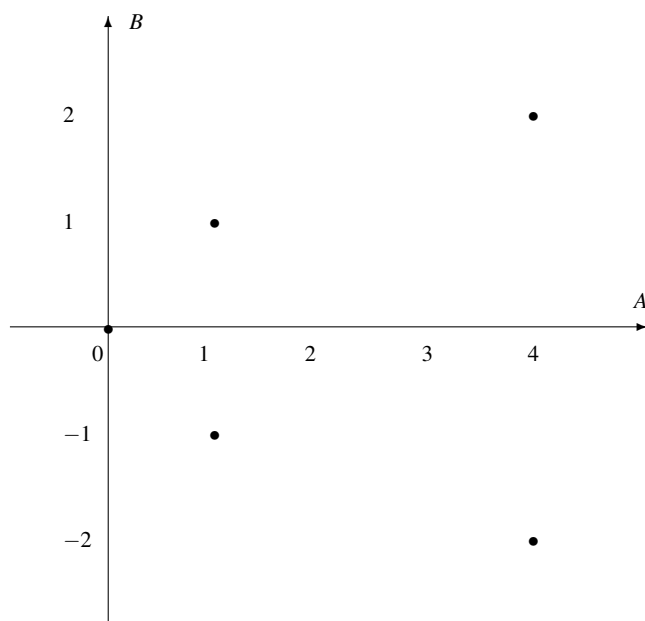


Kuva 4.5 Esimerkin 68 karteeminen tulo $A \times B$ pikselimuodossa esitettynä. Koko tasoa esittävä kuva koostuu $5 \cdot 5 = 25$:stä pikselistä. Vaaka-akselia voidaan kutsua A -akseliksi ja pystyakselia B -akseliksi.

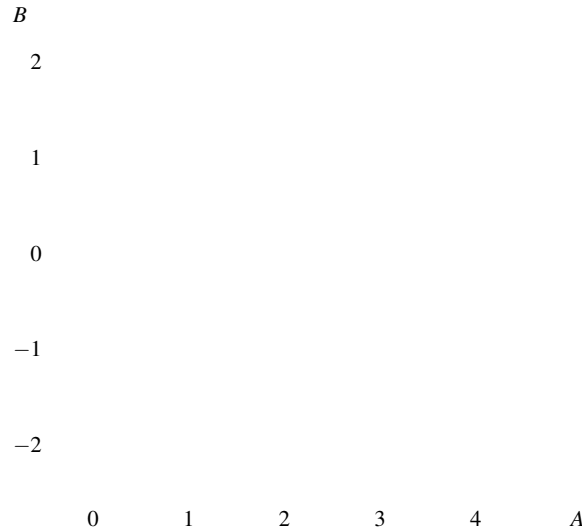
Tarkastellaan relaatiota

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

joka siis on karteesisen tulon $A \times B$ osajoukko. Relaatiota R edustaa kuvan 4.6 pisteistö ja samaa asiaa esittää kuvan 4.7 pikselimuoto.



Kuva 4.6 Esimerkin 68 relaatio R AB -tasossa

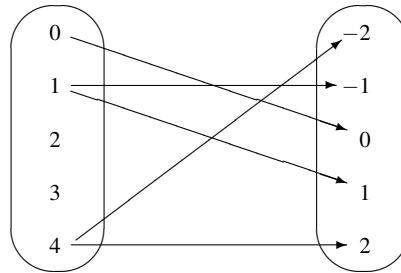


Kuva 4.7 Esimerkin 68 relaatio R pikselimuodossa esitettynä.

Relaatio R voidaan kirjoittaa muodossa $R = \{(a, b) \mid a \in A, b \in B, b^2 = a\}$. Relaatio $R : A \rightarrow B$ edustaa siis eräänlaista neliöjuuren ottoa joukon A alkioista. Joukon A alkioon 0 liittyy joukon B alkio 0, mikä ilmaistaan siten, että pari $(0, 0)$ on joukossa (relaatiossa) R . Lisäksi A :n alkioon 1 liittyvät joukon B alkio -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 alkio -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 4.8). Jos $A = B$, voidaan nuolikaaviossa jättää toinen joukko pois ja piirtää nuolet yhden joukon sisälle.



Kuva 4.8 Esimerkin 68 relaation nuolikaavioesitys.

Relaatio on siis funktiota (joka määritellään täsmällisesti seuraavassa luvussa) väljempi käsite. Funktio joukosta A joukkoon B ei esimerkiksi salli sellaista mahdollisuutta, että joukon A alkioon liitettäisiin useampi kuin yksi joukon B alkio (edellisessä esimerkissä lukuun $1 \in A$ liitettiin sekä -1 että 1 kuin myös lukuun $4 \in A$ liitettiin sekä -2 että 2). Funktion käsite ei myöskään salli sitä, että joukossa A olisi alkioita, joita ei vastaa yksikään joukon B alkio. Edellisessä esimerkissä 2 ja 3 olivat tällaisia joukon A alkioita.

Esimerkki 69. Origokeskisen yksikköympyrän yhtälö on $x^2 + y^2 = 1$. Toisin sanoen joukon $\mathbb{R} \rightarrow \mathbb{R}$ 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 4.2.

Esimerkki 70. Määritellään relaatio $L : \mathbb{R} \rightarrow \mathbb{R}$ seuraavasti: $L = \{(x, x^3) \mid x \in \mathbb{R}\}$. Relaation graafinen esitys on kuvassa 4.9. Tämä relaatio on itse asiassa myös funktio.

Kuva 4.9 Relaatian $\{(x, x^3) \mid x \in \mathbb{R}\}$ graafinen esitys.

Huomautus 18. Jokainen ekvivalenssirelaatio R jakaa joukon A erillisiin *ekvivalenssiluokkiin*, jotka koostuvat keskenään relaatiossa olevista alkioista. Identiteettirelaatio on aina ekvivalenssirelaatio, jossa tosin ekvivalenssiluokat ovat vain yhden alkion suuruisia.

Huomautus 19. Luonnollisten lukujen tavallinen järjestysrelaatio $\leq$ on osittainen järjestys. Osittainen järjestys R on *totaalinen järjestys*, jos lisäksi aina jompikumpi vaihtoehdoista aRb tai bRa on voimassa.

4.3 Funktion määritelmä

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

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

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 kehitti myös ajatuksia automatisoidusta tietojenkäsittelystä.

(kuva: Wikimedia Commons)

Esimerkki 72. Esimerkin 67 identiteettirelaatio on funktio.

Esimerkki 73. Esimerkin 69 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 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 20. 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.

4.4 Funktioiden ominaisuuksia

Lause 16. Jos $f : A \rightarrow B$ ja $g : B \rightarrow C$ ovat funktiota, on relaatiotulo $g \circ f$ myös funktio

Todistus. Harjoitustehtävä.

Edellisen lauseen nojalla voidaan asettaa seuraava määritelmä.

Esimerkki 74. Jos $h(x) = e^{-x^2}$, voidaan h kirjoittaa muodossa $h = g \circ f$, missä $g(x) = e^x$ on ulko-funktio ja $f(x) = -x^2$ on sisäfunktio.

Lauseen 16 mukaan kahdesta funktiosta yhdistämällä saatu relaatio on aina funktio. Sen sijaan vaikkapa esimerkkiä 68 tarkastelemalla voidaan todeta, että funktion käänteisrelaatio ei aina ole funktio. Sen selvittämiseksi, millaisten funktioiden käänteisrelaatio on funktio, otetaan käyttöön seuraavat käsitteet.

Sanallisesti injektiivisuus merkitsee sitä, että eri alkukuvilla on eri kuvat. Epäsuoran todistuksen ideaa käyttäen funktion injektiivisuus 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. Bijektiivisuus puolestaan surjektiivisuuden ja injektiivisyyden yhdistelmänä merkitsee sitä, että jokaisella joukon B alkiolla on *tarkalleen yksi* alkukuva joukossa A .

Esimerkki 75. Funktio $f : \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2$ 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 injektiivisuusehtoa. Sen lisäksi luvulla -1 ei ole lainkaan alkukuvaa, sillä $x^2 \neq -1$ kaikille reaaliluvuille x , mikä on vastoin surjektiivisuusehtoa.

Sen sijaan funktio $g : \mathbb{R} \rightarrow [0, \infty)$, $g(x) = x^2$ 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 17. Jos $f : A \rightarrow B$ on bijektiivinen funktio, on käänteisrelaatio $f^{-1} : B \rightarrow A$ myös funktio, ns. f :n käänteisfunktio. Kääntäen, jos funktion $f : A \rightarrow B$ käänteisrelaatio $f^{-1} : B \rightarrow A$ 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.

Olkon $f : A \rightarrow B$ bijektio. Tällöin siis käänteisfunktio $f^{-1} : B \rightarrow A$ 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 $f^{-1} \circ f : A \rightarrow A$ on joukon A identiteettifunktio. Samoin voidaan todeta, että $f \circ f^{-1} : B \rightarrow B$ on joukon B identiteettifunktio.

Huomautus 21. Jos $f : A \rightarrow B$ on injektio, voidaan B :tä rajoittamalla saada bijektio $f : A \rightarrow f(A)$. Tällöin on olemassa käänteisfunktio $f^{-1} : f(A) \rightarrow A$.

Lause 18. Merkitään $A \sim B$ jos A ja B ovat yhtä mahtavat. Tällöin $\sim$ on ekvivalenssirelaatio.

Todistus. Harjoitustehtävä.

Lause 19. Äärelliset joukot ovat yhtä mahtavat tarkalleen silloin kun niissä on sama määrä alkioita.

Todistus. Merkitään $A = \{a_1, \dots, a_n\}$ ja $B = \{b_1, \dots, b_m\}$. Jos $n = m$, on $f(a_i) = b_i$ bijektio $A \rightarrow B$. Jos myös joukossa B on n alkioita, on olemassa bijektio $g : \{1, 2, \dots, n\} \rightarrow B$. Oletetaan sitten, että $m < n$ ja tehdään vastaoletus, että olisi bijektio $f : A \rightarrow B$. Koska $|B| < |A|$, on oltava alkio $a_i \neq a_j$, joille $f(a_i) = f(a_j)$, jolloin f ei ole injektio eikä siis myöskään bijektio. $\square$

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

Lause 20. Joukko $\mathbb{N} = \{1, 2, 3, \dots\}$ on yhtä mahtava joukon $\mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \dots\}$ kanssa.

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

Lause 21. Joukko $\mathbb{N}$ on yhtä mahtava joukon $2\mathbb{N} = \{2, 4, 6, \dots\}$ kanssa.

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

Lause 22. Joukko $\mathbb{Z}$ on numeroituva.

Todistus. Harjoitustehtävä.

Lause 23. Joukko $\mathbb{N} \times \mathbb{N}$ on numeroituva.

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

Lause 24. Joukko $\mathbb{Q}$ on numeroituva.

Todistus. Jätetään harjoitustehtäväksi. Tässä voidaan hyödyntää edellistä lausetta.

Lause 25. Joukko $\mathbb{R}$ ei ole numeroituva.

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

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

ja muodostetaan desimaalikehitelmä $r = 0.c_1c_2c_3\dots$, jonka desimaalit valitaan seuraavasti: $c_i = d_i + 1$, 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. $\square$

Luku 5

Yleisimmät reaalifunktiot

Varsinkin reaalifunktioiden yhteydessä jätetään usein sekä määrittelyjoukko että maalijoukko ilmoittamatta. Tällöin määrittelyjoukoksi valitaan *laajin mahdollinen* reaalilukujoukko, ellei toisin sovita.

Esimerkki 76. Olkoon $f(x) = \frac{1}{x(x-1)}$. Funktion f määrittelevän lausekkeen nimittäjä saa arvon 0 kun $x \in \{0, 1\}$, joten reaalifunktion f laajin mahdollinen määrittelyjoukko on $\mathbb{R} \setminus \{0, 1\}$.

5.1 Reaalifunktioiden esitystapoja ja ominaisuuksia

Esimerkki 77. Palataan esimerkin 69 yhtälöön $x^2 + y^2 = 1$. Tämä on implisiittimuotoinen yhtälö, mutta kuten aiemmin jo huomattiin, ei implisiittimuoto välttämättä määrittele funktiota, vaan relaation. Tämän kaltaisissa tapauksissa tarvitaan jokin lisäehto, jotta saataisiin määriteltyksi funktio. Tässä tapauksessa tällainen lisäehto voi olla vaikkapa $y \geq 0$.

Jos asetetaan rajoitus $y \geq 0$, saadaan eksplisiittimuotoinen funktio $f(x) = \sqrt{1-x^2}$, jonka laajimpana määrittelyjoukkona toimii $[-1, 1]$. Parametriesitys samalle funktiolle puolestaan on esimerkiksi $f = \{(\cos t, \sin t) \mid t \in [0, \pi]\}$.

Myös parametrimuoto voi määritellä funktion sijasta relaation. Jos edellisessä esimerkissä olisi parametrin annettu kulkea väli $[0, 2\pi]$ välin $[0, \pi]$ sijaan, olisi tuloksena esimerkin 69 relaatio. Parametrin arvoa rajoittamalla voidaan kuitenkin usein saada aikaan funktio.

Lause 26. *Aidosti monotoninen funktio $f : A \rightarrow \mathbb{R}$ on injektio.*

Todistus. Harjoitustehtävä.

Kuten esimerkissä 21 todettiin, voidaan jokaista joukossa A määriteltyä injektiivistä funktiota f kohti määritellä bijektio $f : A \rightarrow f(A)$ rajoittamalla maalijoukkoa.

Lause 27. *Jos funktio $f : A \rightarrow f(A)$ on aidosti kasvava, niin myös sen käänteisfunktio $f^{-1} : f(A) \rightarrow A$ on aidosti kasvava. Vastaava tulos pätee aidosti väheneville funktioille.*

Todistus. Harjoitustehtävä.

5.2 Algebralliset funktiot

Polynomifunktiot ovat tiettyssä mielessä kaikkein yksinkertaisimpia reaalifunktioita. Ainakin niiden arvojen laskeminen perustuu suoraan reaalilukujen operaatioihin: kun x on annettu, arvo $p(x)$ voidaan laskea pelkästään kerto- ja yhteenlaskujen perusteella.

Kaikille mahdollisille reaaliluvuille on määritelty vähennyslasku, sillä jokaisella reaaliluvulla on *vastaluku*. Tällöin erotus $a - b$ voidaan aina määritellä $a - b = a + (-b)$. Jos $b \neq 0$, on reaaliluvuille määritelty myös jakolasku $\frac{a}{b} = ab^{-1}$, ja näitä operaatioita käyttämällä saadaan polynomifunktioita laajempi funktioluokka, ns. *rationaalifunktiot*. Yleisemmin yhteen-, vähennys-, kerto- ja jakolaskua kutsutaan *rationaalisiksi* operaatioiksi.

y an encoding such as `\[latin1]inputenc` in the document preamble. Alternatively, save the file in UTF-8 using your editor or another toolReaalifun

Esimerkki 78. $f(x) = 5 \cdot 1 + 4 \cdot x = 5 + 4x$ on rationaalifunktio, samoin $f(x) \cdot f(x) = (5 + 4x) \cdot (5 + 4x) = 25 + 40x + 16x^2$. Myös $g(x) = \frac{1+2x+3x^2}{2+x+x^2}$ on rationaalifunktio. Kaikki rationaalifunktiot voidaan esittää kahden polynomin osamääränä.

Rationaaliset operaatiot eivät kuitenkaan ole ainoita, joilla tunnetuista reaalifunktioista saadaan uusia: aiemmin on jo todettu, että esimerkiksi myös yhdistämällä ja käänteisfunktioina saadaan uusia funktiota. Myöhemmin esitellään lisää tapoja uusien reaalifunktioiden muodostamiseksi.

Esimerkki 79. Olkoon $k \in \mathbb{N}$. Tällöin reaalifunktio $f : [0, \infty) \rightarrow [0, \infty)$, $f(x) = x^k$ on bijektio. Sen käänteisfunktioita kutsutaan *juurifunktioksi* ja merkitään $f^{-1}(x) = \sqrt[k]{x}$.

Esimerkki 80. $f(x) = \sqrt{1-x^2}$ on algebrallinen funktio, koska se on kahden muuttujan polynomiyhtälön $x^2 + y^2 - 1 = 0$ määrittelemän relaation osa, jossa $x \in [-1, 1]$ ja $y \geq 0$.

Esimerkki 81. Jokainen rationaalifunktio $f(x) = \frac{p(x)}{q(x)}$ on algebrallinen, koska se voidaan määritellä polynomiyhtälöllä $q(x)y - p(x) = 0$.

Esimerkki 82. Funktio $f(x) = |x|$ on algebrallinen, koska se on polynomiyhtälön $y^2 - x^2 = 0$ määrittelemän relaation osa.

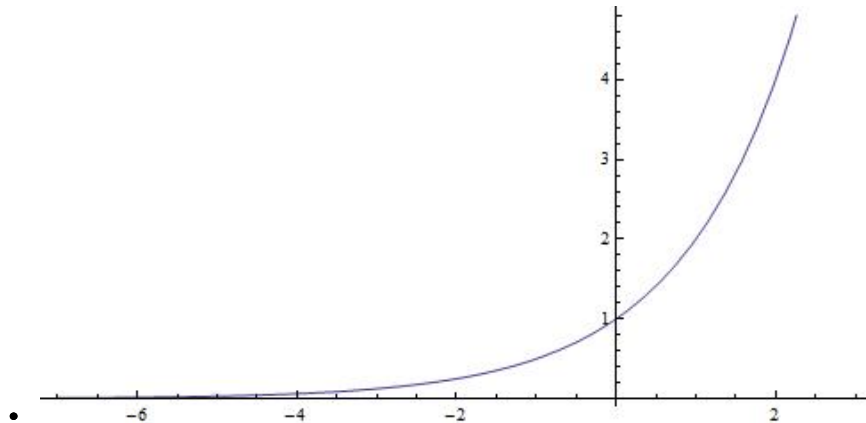
5.3 Eksponentti- ja logaritmifunktiot

Tavanomainen potenssimerkintä

$$a^n = \underbrace{a \cdot \dots \cdot a}_{n \text{ kpl}}$$

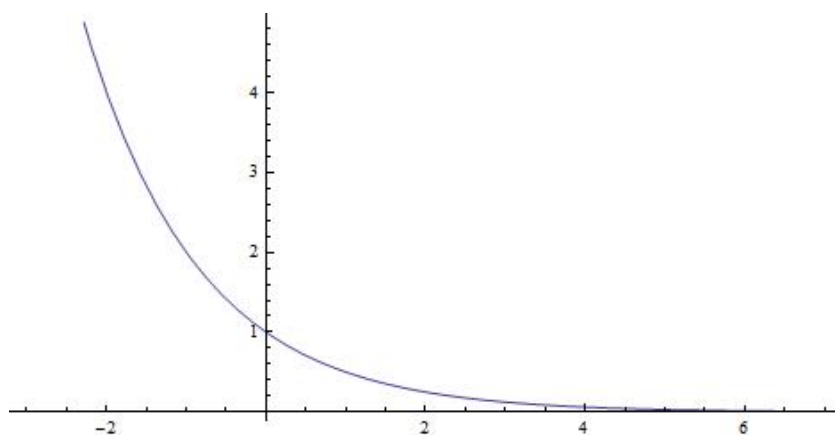
laajennetaan yleensä koskemaan negatiivisia lukuja $-n$ määrittelemällä $a^{-n} = \frac{1}{a^n}$ ja rationaalieksponentteja seuraavasti: $a^{\frac{m}{n}} = \sqrt[n]{a^m}$.

Viimeistään rationaalilukueksponentteja määriteltäessä tulee yleensä rajoittautua tapauksiin $a \geq 0$, jotta juuren olemassaolon suhteen ei olisi ongelmaa. Reaaliluvulle x potenssimerkintä a^x voidaan määritellä täsmällisesti vain raja-arvokäsitteen kautta. Yleinen tapa tämän saavuttamiseksi on valita jokin jono rationaalilukuja $r_1, r_2, r_3, \dots$, joka lähestyy reaalilukua x ja määritellä a^x lukuna, jota jono $a^{r_1}, a^{r_2}, a^{r_3}, \dots$ lähestyy. Näin määriteltäessä pitää varmistua yksityiskohdista, kuten raja-arvojen olemassaoloista ja määriteltävän objektin yksikäsitteisyydestä. Nämä teknisluontoiset yksityiskohdat kuitenkin sivuutetaan tässä yhteydessä ja esitetään vain seuraava määritelmä ja siihen liittyvät väitteet todistuksetta.



Kuva 5.1 $y = 2^x$

Aiemmin todetun mukaan kaikilla bijektioilla on olemassa käänteisfunktio, myös eksponenttifunktiolla $\mathbb{R} \rightarrow (0, \infty)$.



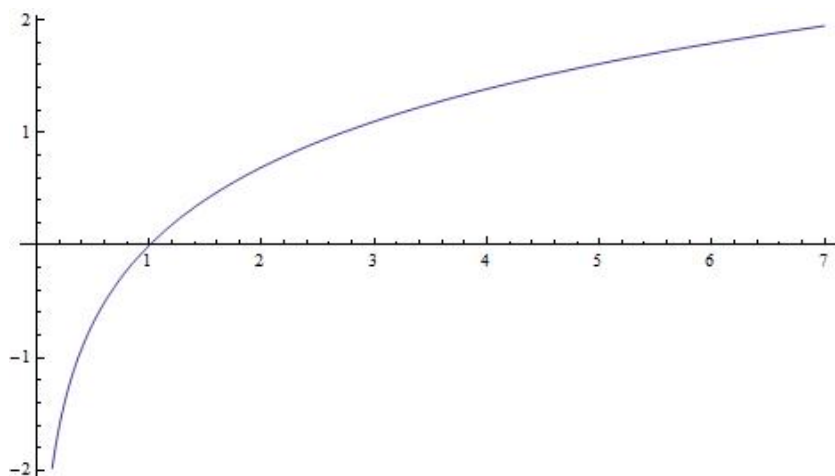
Kuva 5.2 $y = \left(\frac{1}{2}\right)^x$

Lause 28. Logaritmifunktiot toteuttavat $\log_a(xy) = \log_a x + \log_a y$ ja $\log_a x^y = y \log_a x$.

Todistus. Harjoitustehtävä. Käytä eksponenttifunktion ominaisuuksia todistuksessa.

Lause 29. Jos $a > 1$, on $f(x) = \log_a x$ aidosti kasvava. Jos taas $0 < a < 1$, on $f(x) = \log_a x$ aidosti vähenevä.

Todistus. Harjoitustehtävä. Käytä eksponenttifunktion ominaisuuksia todistuksessa.



Kuva 5.3 $y = \ln x$

Periaatteessa kaikki eksponenttifunktiot voidaan esittää yhden ainoan eksponenttifunktion avulla, ja sama pätee logaritmifunktioihin. Tämä perustuu seuraavaan tulokseen, jota ei kuitenkaan ryhdytä todistamaan.

Lause 30 (Kantaluvun vaihto). Jos $b = a^c$, on

$$b^x = (a^c)^x = a^{cx}$$

ja

$$\log_b x = \frac{\log_a x}{c}.$$

Jälkimmäinen väittämä tietysti seuraa edellisestä (harjoitustehtävä).

Syistä jotka selviävät Insinöörimatematiikan kurssikokonaisuuden myöhemmissä osissa, valitaan eksponenttifunktiolle ja logaritmifunktiolle kantaluvuksi irrationaaliluku

$$e = 2,71828182845904523536\dots,$$

niin sanottu *Neperin luku*. Tässä kurssissa eksponentti- ja logaritmifunktiot, joiden kantalukua ei erikseen mainita, oletetaan *e*-kantaisiksi.

5.4 Trigonometriset funktiot

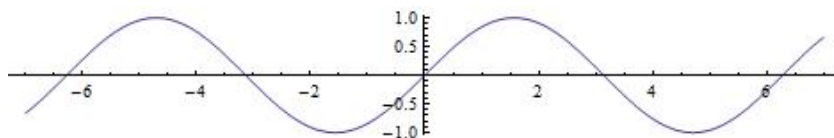
Edelläkuvattujen lisäksi yksi varsin yleisesti esiintyvän reaalifunktiotyypin muodostavat *trigonometriset funktiot*. Trigonometriset funktiot voidaan määritellä täsmällisesti sarjaopin avulla, mutta tässä yhteydessä tyydytään intuitiivisempaan kuvailuun.

Kuvailu tarvitsee tuekseen kulman suuruuden määritelmän absoluuttisissa yksiköissä eli *radiaaneissa*.

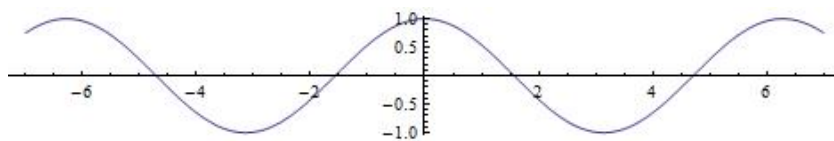
Käyttämällä moninkertaisia kierroksia sekä myötäpäivään kiertymistä voidaan sini ja kosini määritellä kaikille mahdollisille reaaliluvuille. Edelleen huomataan, että sini ja kosini voivat saada arvoja vain väliltä $[-1, 1]$, mutta huomattavin ominaisuus on, että kumpikin funktio on *jaksollinen*:

$$\sin x = \sin(x + 2\pi) \quad \text{ja} \quad \cos x = \cos(x + 2\pi)$$

kaikille mahdollisille reaaliluvuille x . Trigonometriset funktiot toteuttavat lukuisia identiteettejä (yhtäsuuruuksia, jotka pätevät kaikille muuttujan arvoille) joita on listattu taulukoihin. Näistä tunnetuimpia ovat $\sin^2 x + \cos^2 x = 1$ ja $\sin(x + y) = \sin x \cos y + \cos x \sin y$. Myös identiteetti $\sin x = \cos(x - \frac{\pi}{2})$ on huomattava, sillä siitä ilmenee että kosini ja sini ovat itse asiassa koordinaatiston siirtoa vaille samat funktiot.



Kuva 5.4 $y = \sin x$



Kuva 5.5 $y = \cos x$

Määritelmästä nähdään helposti myös oikeaksi seuraava tulos.

Lause 31 (Sinin ja kosinin nollakohdat).

- $\sin x = 0 \Leftrightarrow x \in \{n\pi \mid n \in \mathbb{Z}\}$
- $\cos x = 0 \Leftrightarrow x \in \{\frac{\pi}{2} + n\pi \mid n \in \mathbb{Z}\}$

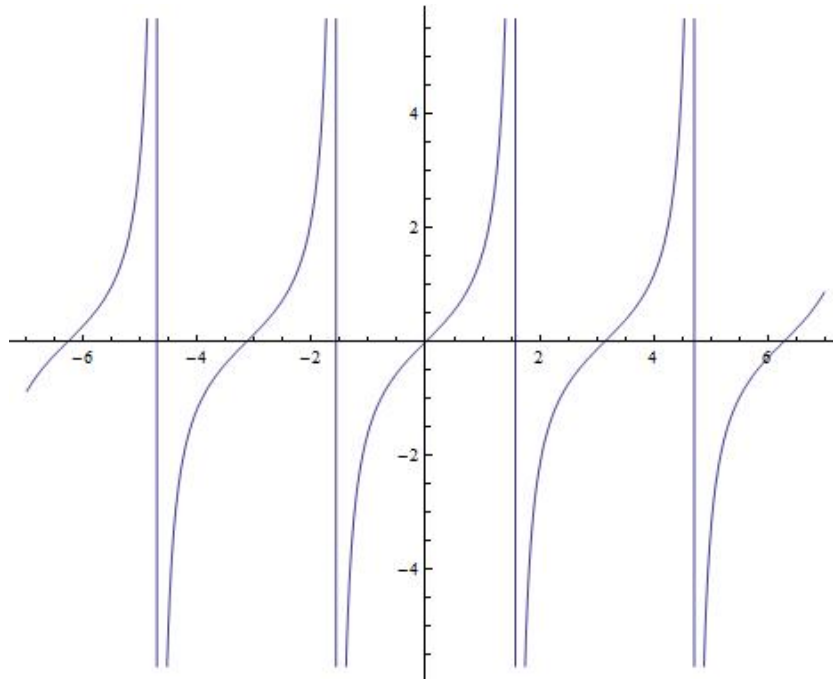
Funktiona $\mathbb{R} \rightarrow \mathbb{R}$ sini ei ole surjektio, sillä se saa vain välillä $[-1, 1]$ olevia arvoja. Sini ei myöskään ole injektio, sillä se on jaksollinen ja saa täten samoja arvoja 2π :n välein. Näin ollen sini ei ole bijektio eikä sillä siis ole käänteisfunktioita. Sopivasti lähtö- ja maalijoukkoa rajoittamalla sinistä saadaan aikaan bijektio, esimerkiksi

funktio $\sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \rightarrow [-1, 1]$ on bijektio, jonka käänteisfunktioita kutsutaan *arkussiniksi* ja merkitään $\arcsin x$ tai $\sin^{-1} x$.

Arkuskosini $\arccos : [0, \pi] \rightarrow [-1, 1]$ määritellään analogisesti.

Tangentti voidaan määritellä kaavalla $\tan x = \frac{\sin x}{\cos x}$, jolloin saadaan kaikilla muilla reaaliarvoilla paitsi joukossa $\{\frac{\pi}{2} + k\pi \mid k \in \mathbb{Z}\}$ määritelty funktio. Osoittautuu, että tangentti on π -jaksollinen funktio, joka on kasvava välillä $(-\frac{\pi}{2}, \frac{\pi}{2})$ ja saa kaikki reaaliarvot tällä välillä.

Funktio $\tan : (-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R}$ on bijektio ja sen käänteisfunktioita kutsutaan *arkustangentiksi*.



Kuva 5.6 $y = \tan x$

Kurssin seuraavassa osassa perehdytään pintapuolisesti Matlab-ohjelmistoon, joka kykenee monipuoliseen reaalifunktioiden numeeriseen käsittelyyn, mukaanlukien graafiset esitykset. Reaalifunktioiden ominaisuuksia voi myös valottaa Wolfram Alphan avulla. Wolfram Alpha on osoitteesta <http://www.wolframalpha.com/> löytyvä matemaattisen tiedon hakukone, joka pystyy myös symboliseen sekä numeeriseen laskentaan ja kuvaajien piirtämiseen ja osaa tulkita hyvinkin summittaisesti annettuja syötteitä. Kokeile!

Seuraavan määritelmän mukainen funktioluokka riittää jo varsin pitkälle, mutta ei kuitenkaan sisällä kaikkia Insinöörimatematiikan kurssikokonaisuudessa tarvittavia funktioita.

Esimerkki 83.

$$f(x) = \frac{\ln(1+x) \sin^2 x - \sqrt{3+4x^2}}{\arctan(\cos x)}$$

on alkeisfunktio.

Esimerkki 84. Voidaan osoittaa, että ns. *normaalijakauman kertymäfunktio*

$$\Psi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{t^2}{2}} dt$$

ei ole alkeisfunktio.

Luku 6

Kompleksiluvut

Lukualueiden laajentamista luonnollisten lukujen joukosta $\mathbb{N}$ laajempiin joukkoihin voidaan tarkastella monelta kannalta. Algebrallinen lähestymistapa kiinnittää huomiota polynomi yhtälöiden ratkeavuuteen, esimerkiksi yhtälöllä $x + 2 = 1$ ei ole ratkaisua luonnollisten lukujen joukossa, mutta kokonaislukujen joukossa $\mathbb{Z}$ sillä on ratkaisu $x = -1$. Vastaavasti yhtälö $2x = 1$ on kokonaislukujen joukossa ratkeamaton, mutta laajennettaessa kokonaislukujen joukkoa rationaalilukujen joukoksi $\mathbb{Q}$ saadaan yhtälölle ratkaisu $x = \frac{1}{2}$. Samoin yhtälö $x^2 - 2 = 0$ on rationaalilukujen joukossa ratkeamaton, mutta reaalilukujen joukossa $\mathbb{R}$ sillä on kaksikin ratkaisua, nimittäin $\sqrt{2}$ ja $-\sqrt{2}$.

Helposti huomataan, että reaaliluvutkaan eivät takaa polynomi yhtälön ratkeavuutta: esimerkiksi yhtälöllä $x^2 + 1 = 0$ ei ole ratkaisua joukossa $\mathbb{R}$. Tämän puutteen korvaamiseksi otetaan käyttöön *kompleksiluvut*.

6.1 Kompleksilukujen määritelmä ja peruslaskutoimitukset

Edellisen määritelmän mukaan kompleksiluku $x + yi$ voidaan käsittää reaalilukuparina (x, y) . Koska jokainen reaaliluku voidaan kirjoittaa muotoon $x = x + 0i$, voidaan reaaliluvut käsittää kompleksilukujen erikoistapauksiksi ja siis $\mathbb{R} \subseteq \mathbb{C}$.

Huomautus 22. Koska imaginaariyksikkö toteuttaa yhtälön $i^2 = -1$, voidaan periaatteessa merkitä $i = \sqrt{-1}$. Tällöin pitäisi kuitenkin olla $(-i)^2 = (-i)(-i) = (-1 \cdot i)(-1 \cdot i) = (-1)^2 i^2 = i^2 = -1$. Täten siis näyttää siltä, että myös $-i$ toteuttaa yhtälön $(-i)^2 = -1$ eikä neliöjuuri $\sqrt{-1}$ olisi yksikäsitteinen. Tähän ongelmaan palataan myöhemmin.

Huomautus 23. Symbolia i käytetään toisinaan merkitsemään vaihtovirtaa, ja siksi erityisesti sähkötekniikan yhteydessä imaginaariyksiköstä käytetään j :n sijaan merkintää j .

Esimerkki 85. Yhtälöllä $x^2 - 2x + 5 = 0$ ei ole reaalisia ratkaisuja, koska $x^2 - 2x + 5 = (x - 1)^2 + 4 \geq 4$ aina kun $x \in \mathbb{R}$. Sen sijaan yhtälöllä on kaksi kompleksista ratkaisua, jotka saadaan seuraavasti: $x^2 - 2x + 5 = 0 \Leftrightarrow (x - 1)^2 = -4 \Leftrightarrow (x - 1)^2 = 4i^2 \Leftrightarrow x - 1 = \pm 2i \Leftrightarrow x = 1 \pm 2i$.

Yhteenlasku kompleksiluvuilla on suoraviivainen: $(x_1 + y_1 i) + (x_2 + y_2 i) = (x_1 + x_2) + (y_1 + y_2)i$, ja kertolaskua varten muistetaan, että $i^2 = -1$. Tällöin

$$\begin{aligned}(x_1 + y_1 i)(x_2 + y_2 i) &= x_1 x_2 + x_1 y_2 i + y_1 i x_2 + y_1 i y_2 i \\ &= x_1 x_2 + y_1 y_2 i^2 + x_1 y_2 i + y_1 x_2 i \\ &= (x_1 x_2 - y_1 y_2) + (x_1 y_2 + y_1 x_2)i.\end{aligned}$$

Vähennyslasku on yhteenlaskun kanssa analoginen, ja jakolaskun helpottamiseksi otetaan ensin käyttöön *liittoluvun* käsite.

Lause 32. Jos z_1 ja $z_2 \in \mathbb{C}$, niin $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ ja $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.

Todistus. Harjoitustehtävä.

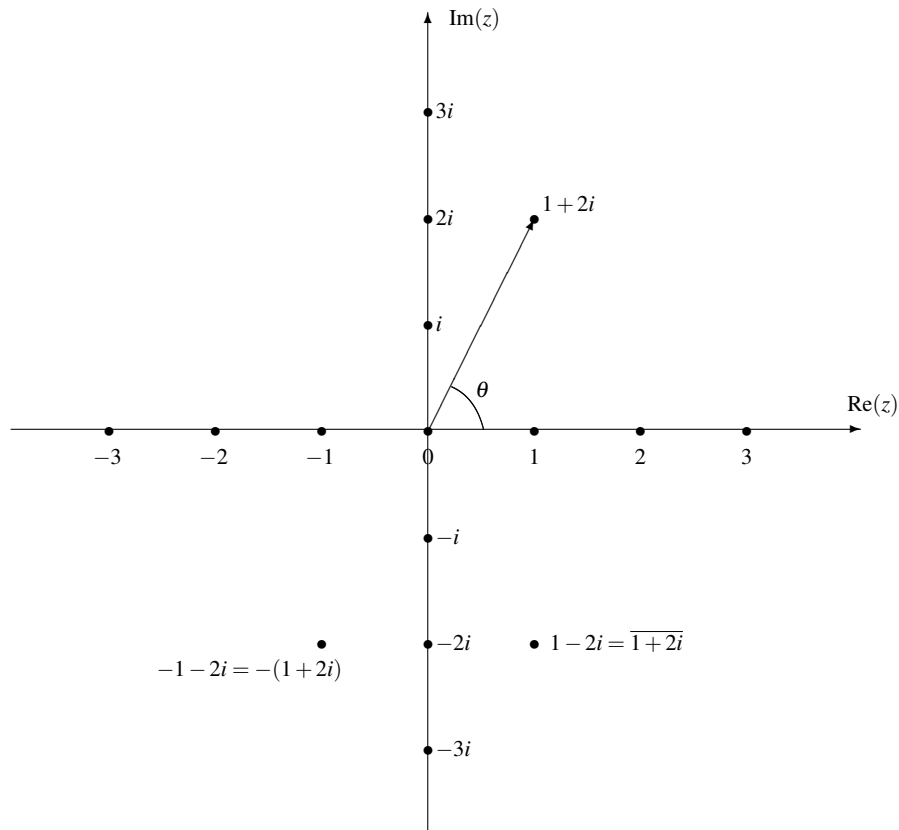
Kompleksilukujen jakolaskussa kannattaa usein laventaa jakajan liittoluvulla:

$$\begin{aligned}\frac{x_1 + y_1 i}{x_2 + y_2 i} &= \frac{(x_1 + y_1 i)(x_2 - y_2 i)}{(x_2 + y_2 i)(x_2 - y_2 i)} = \frac{x_1 x_2 + y_1 y_2 + x_2 y_1 i - x_1 y_2 i}{x_2^2 + y_2^2} \\ &= \frac{x_1 x_2 + y_1 y_2}{x_2^2 + y_2^2} + \frac{x_2 y_1 - x_1 y_2}{x_2^2 + y_2^2} i.\end{aligned}$$

Kompleksiluvuilla on siis monia reaalilukujen kaltaisia ominaisuuksia: niille voidaan määritellä summa, erotus, tulo ja osamäärä, jotka vielä toteuttavat samankaltaisia sääntöjä kuin reaalilukujen vastaavat operaatiot. On esimerkiksi helppo tarkistaa, että kompleksiluvuille z_1 , z_2 ja z_3 pätevät sekä *vaihdantalaki eli kommutatiivisuus* $z_1 z_2 = z_2 z_1$ sekä *osittelulaki eli distributiivisuus* $z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3$. Lisäksi kompleksiluvuille pätee tulon nollasääntö eli $z_1 z_2 = 0$ tarkalleen silloin kun joko $z_1 = 0$, $z_2 = 0$, tai $z_1 = z_2 = 0$ (tulon nollasääntö on itse asiassa seuraus siitä, että jokaisella nolasta eroavalla luvulla on käänteisluku). Voidaan itse asiassa näyttää toteen, että kompleksiluvut toteuttavat esimerkin 9 kunta-aksioomat.

6.2 Kompleksilukujen graafinen esitys, itseisarvo ja polaariesitys

Kompleksiluku voidaan käsittää reaalilukuparina, joten luonteva graafinen esitys kompleksiluvuille on tason piste (Kuva 6.1).



Kuva 6.1 Kompleksilukujen graafinen esitys. Kuviossa näkyvän nuolen pituus kuvaa kompleksiluvun $1 + 2i$ itseisarvoa ja θ sen vaihekulmaa. Vaaka-akselia kutsutaan *reaaliakseliksi* ja pystyakselia *imaginaariakseliksi*. Reaaliakselilla olevat luvut ovat reaalisia, kun taas imarinääriakselin lukuja kutsutaan *puhtaiksi* imaginaariluvuiksi. Liittoluku saadaan peilaamalla reaaliakselin suhteen ja vastaluku origon suhteen.

Kompleksilukuja ei kuitenkaan voida yleisesti ottaen järjestää suuruusjärjestykseen kuten reaalilukuja. Ei voida määritellä milloin kompleksiluku on suurempi kuin toinen, mistä seuraa, että

kompleksilukujen kohdalla ei voi puhua epäyhtälöistä. Sen sijaan kompleksiluvuille voidaan määrittellä *itseisarvo* ja kahden eri kompleksiluvun itseisarvoa voidaan verrata.

Huomautus 24. Edellisen määritelmän merkinnöin $z\bar{z} = x^2 + y^2 = |z|^2$. Tästä seuraa lauseen 32 perusteella, että $|z_1 z_2|^2 = z_1 z_2 \overline{z_1 z_2} = z_1 \overline{z_1} z_2 \overline{z_2} = |z_1|^2 |z_2|^2$, mistä edelleen seuraa, että $|z_1 z_2| = |z_1| |z_2|$ pitää myös kompleksiluvuille paikkansa. Myös kolmioepäyhtälö

$$|z_1 + z_2| \leq |z_1| + |z_2|$$

pätee kompleksiluvuille, vaikka sitä ei tässä yhteydessä todistetaakaan.

Kompleksiluku $z = x + yi$ voidaan esittää paitsi reaalilukuparina (x, y) , myös antamalla pisteen (x, y) etäisyys origosta (mikä on siis yhtä kuin $|z|$, kompleksiluvun z itseisarvo) sekä origon ja pisteen (x, y) kautta kulkevan suoran ja reaaliakselin välinen kulma θ (ns. *vaihekulma*) (Kuva 6.1). Tästä esityksestä käytetään nimeä *polaariesitys* tai *napakoordinaattiesitys*. Kompleksiluvun esitystä muodossa $z = x + iy$ kutsutaan *karteesiseksi* tai *xy-esitykseksi*.

Huomautus 25 (Polaariesityksen etsiminen). Kompleksiluvun karteesisesta esityksestä $z = x + yi$ saadaan polaariesitys seuraavasti: Itseisarvon laskeminen määritelmän ?? mukaan suoraan: $|z| = \sqrt{x^2 + y^2}$. Tämän lisäksi alkeistigonometrian mukaan $\tan \theta = \frac{y}{x}$ (kts. kuva 6.1), joten pääteltäväksi jää θ . Määritelmän mukaan nimittäin funktion $\arctan$ arvot ovat aina välillä $(-\frac{\pi}{2}, \frac{\pi}{2})$, mutta selvästikin kompleksilukujen vaihekulmia on olemassa myös tämän välin ulkopuolella. Tämä tulee ymmärrettäväksi siten, että tangentifunktio saa samat arvot kulman π välein: $\tan(x + \pi) = \tan x$.

Vaihekulman θ valinta tehdään seuraavasti:

1. Tapauksessa $x = 0$ voidaan vaihekulmaksi valita $\theta = \frac{\pi}{2}$, jos $y > 0$, ja $\theta = -\frac{\pi}{2}$, jos $y < 0$.
2. Tapauksessa $x > 0$ voidaan vaihekulmaksi valita $\theta = \arctan \frac{y}{x}$, ja
3. Tapauksessa $x < 0$ voidaan vaihekulmaksi valita $\theta = \arctan \frac{y}{x} + \pi$.

Reaalilukujen ($y = 0$) vaihekulmaksi voidaan siis edellämainitun perusteella aina valita 0 (positiiviset reaaliluvut) tai π (negatiiviset reaaliluvut).

On kuitenkin huomattava, että kompleksiluvun vaihekulma *ei ole koskaan yksikäsitteinen*, sillä siihen voidaan lisätä tai siitä vähentää niin monta täyden ympyrän (2π) monikertaa kuin halutaan.

Esimerkki 86. Vaihekulman $-\frac{\pi}{2}$ sijaan voidaan yhtä hyvin valita vaihekulma $-\frac{\pi}{2} + 2\pi = \frac{3\pi}{2}$. Piirrä kuva ja havaitse itse!

Esimerkki 87. Kuvan 6.1 tilanteessa $z = 1 + 2i$, joten $|z|^2 = 1^2 + 2^2$, ja siis $|z| = \sqrt{5}$. Vaihekulma θ on yhtälön $\tan \theta = \frac{2}{1} = 2$ ratkaisu, ja tälle saadaan likiarvo $\theta = 1, 10715 \dots$ (radiaaneina).

Huomautus 26 (Polaarimuodosta karteesiseen). Jos $r = |z|$ on kompleksiluvun z itseisarvo ja θ sen vaihekulma, voidaan alkeistigonometrian perusteella (katso kuva 6.1) kirjoittaa $x = r \cos \theta$ ja $y = r \sin \theta$, joten kompleksiluku $z = x + yi$ voidaan kirjoittaa muotoon

$$z = r \cos \theta + ir \sin \theta.$$

Näin saadusta muodosta voidaan lisäksi huomata, että

$$|z| = |r(\cos \theta + i \sin \theta)| = \underbrace{|r|}_{|z|} |\cos \theta + i \sin \theta|,$$

ja jos $z \neq 0$, nähdään välittömästi että

$$|\cos \theta + i \sin \theta| = 1,$$

mikä tarkoittaa sitä, että kompleksiluku $\cos \theta + i \sin \theta$ on yksikköympyrällä.

Näin saatu esitys ei kuitenkaan ole muotoa jossa kompleksilukujen polaariesitys yleensä kirjoitetaan. Yleensä käytetään vielä *Eulerin kaavaa* (vaihtoehtoinen nimitys: *Eulerin identiteetti*).

Lause 33 (Eulerin kaava). $e^{i\theta} = \cos \theta + i \sin \theta$

(kaavassa e on neperin luku, kaava määrittelee e -kantaisen potenssin ns. pääarvon).

Todistus. Perustelu Eulerin kaavalle esitetään kurssikokonaisuuden myöhemmässä osassa, sarjakehitelmien yhteydessä.

Huomautus 27. Trigonometrinen funktioiden yhteenlaskukaavoista seuraa, että kaava

$$e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1 + \theta_2)} \quad (6.1)$$

pätee, vaikka eksponentit ovat imaginaarilukuja. Itse asiassa olisi mahdollista valita toisenlainen lähestymistapa: kaava (6.1) on mahdollista todistaa käyttämättä trigonometrinen funktioiden yhteenlaskukaavoja, jotka puolestaan voitaisiin johtaa kaavasta (6.1).

Taustatietoa



Leonhard Euler (1707–1783) oli 1700-luvun merkittävin matemaatikko ja lienee kaikkien aikojen tuottelia matemaatikko julkaisujen määrän suhteen. Hänen kaikki työnsä voitaneen esittää n. 80:ssä kirjassa, mutta nykyisin, yli 230 vuotta Eulerin kuoleman jälkeen vuonna 1911 aloitettu työ on vielä kesken ja vasta 76 kokoomateosta on julkaistu Sveitsin tiedeakatemia rahoittamassa Opera Omnia-sarjassa. Euler syntyi Baselissa, mutta toimi suurimman osan urastaan professorina Pietarissa ja Berliinissä.

(kuva: Wikimedia Commons)

Eulerin kaavaa käyttäen voidaan kompleksiluvun polaari- eli napakoordinaattiesitys kirjoittaa seuraavaan muotoon.

Lause 34 (Eksponenttimuotoinen polaariesitys). Jos kompleksiluvun z itseisarvo on r ja vaihekulma θ , niin

$$z = re^{i\theta}.$$

Esimerkki 88. Luvun $z = 1 - i\sqrt{3}$ itseisarvo on $|z| = \sqrt{1^2 + (-\sqrt{3})^2} = 2$. Vaihekulma θ toteuttaa yhtälön $\tan \theta = \frac{-\sqrt{3}}{1}$, joten voidaan valita $\theta = -\frac{\pi}{3}$ (yhtä hyvin voitaisiin valita $\theta = -\frac{\pi}{3} + 2\pi = \frac{5\pi}{3}$). Tällöin siis

$$1 - i\sqrt{3} = 2e^{-i\frac{\pi}{3}}.$$

Polaariesitys antaa kompleksilukujen tulolle selkeän tulkinnan: Olkoon $z_1 = |z_1|e^{i\theta_1}$ ja $z_2 = |z_2|e^{i\theta_2}$. Tällöin

$$z_1 z_2 = |z_1| |z_2| e^{i\theta_1} e^{i\theta_2} = |z_1| |z_2| e^{i(\theta_1 + \theta_2)},$$

mikä siis merkitsee sitä, että

tulon $z_1 z_2$ itseisarvo on kompleksilukujen z_1 ja z_2 itseisarvojen tulo, ja että tulon $z_1 z_2$ vaihekulma on kompleksilukujen z_1 ja z_2 vaihekulmien summa.

Huomautus 28. Koska $\sin \pi = 0$ ja $\cos \pi = -1$, seuraa Eulerin kaavasta yhtälö

$$e^{i\pi} = -1,$$

mitä pidetään yhtenä informatiivisimmista klassisen matematiikan kaavoista: siinä yhdistyvät merkittävät luvut e , π ja i hyvin yksinkertaisella tavalla. Selvitä (harjoitustehtävä) mitä ovat luvut $e^{i\frac{\pi}{4}}$, $e^{i\frac{\pi}{2}}$ ja $e^{i\frac{3\pi}{2}}$ ilmoitettuna reaali- ja imaginaariosien avulla.

Toinen kompleksilukujen yhteydessä usein esiintyvä kaava on ns. de Moivre'n kaava, jota ei kuitenkaan tällä kurssilla paljon käytetä. Se luo kuitenkin mielenkiintoisen kytköksen trigonometriaan.

Lause 35 (de Moivre'n kaava). $(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta$.

Todistus. Kaavasta (6.1) seuraa (miten?), että kaikille kokonaisluvuille n pätee $(e^{i\theta})^n = e^{in\theta}$. Tällöin Eulerin kaavan perusteella saadaan

$$(\cos \theta + i \sin \theta)^n = (e^{i\theta})^n = e^{in\theta} = \cos n\theta + i \sin n\theta.$$

Muistamalla Eulerin kaava saadaan helposti monia trigonometrian kaavoja.

Esimerkki 89. $e^{2i\theta} = \cos 2\theta + i \sin 2\theta$, mutta toisaalta

$$e^{2i\theta} = (e^{i\theta})^2 = (\cos \theta + i \sin \theta)^2 = \cos^2 \theta - \sin^2 \theta + 2i \cos \theta \sin \theta.$$

Yhdistämällä näin saadut esitykset huomataan, että $\cos 2\theta = \cos^2 \theta - \sin^2 \theta$ ja $\sin 2\theta = 2 \cos \theta \sin \theta$.

Muistutetaan lopuksi yksinkertaisesta mutta tärkeästä tosiasiasta, jolla on merkittäviä seurauksia mm. kompleksilukujen logaritmikäsittelylle.

Huomautus 29. Koska kompleksiluvun vaihekulma ei ole yksikäsitteinen, ei myöskään eksponenttimuotoinen polaariesitys ole yksikäsitteinen, vaan

$$e^{i\theta} = \cos \theta + i \sin \theta = \cos(\theta + n \cdot 2\pi) + i \sin(\theta + n \cdot 2\pi) = e^{i(\theta + n \cdot 2\pi)},$$

missä $n \in \mathbb{Z}$.

Edellisen yhtälön perusteella $e^{n \cdot 2\pi i} = 1$ aina kun n on kokonaisluku.

6.3 Kompleksinen eksponenttifunktio ja logaritmi

Kompleksisen, e -kantaisen eksponenttifunktion lähtökohtana toimii luonnollisesti Eulerin kaava.

Esimerkki 90.

$$e^{\ln 2 - \frac{\pi}{2}i} = e^{\ln 2} e^{-\frac{\pi}{2}i} = 2(\cos(-\frac{\pi}{2}) + i \sin(-\frac{\pi}{2})) = -2i.$$

Edellisestä määritelmästä seuraa, että kompleksinen eksponenttifunktio toteuttaa reaalialueella tunnetun yhtälön $e^{z_1+z_2} = e^{z_1}e^{z_2}$, mutta muiden vastaavanlaisten kaavojen suhteen tulee olla huolellinen, kuten jatkossa tullaan näkemään. Huomautuksesta 29 seuraa suoraan, että jos $n \in \mathbb{Z}$, niin

$$e^{z+n \cdot 2\pi i} = e^z e^{n \cdot 2\pi i} = e^z,$$

mikä merkitsee sitä, että kompleksinen eksponenttifunktio ei ole injektio, vaan $2\pi i$ -jaksoinen funktio, joka saa saman arvon äärettömän monella kompleksiluvulla. Tästä seuraa, että kompleksilukujen eksponenttifunktiolla ei voi olla käänteisfunktiota, vaan että *kompleksinen logaritmi* on välttämättä relaatio.

Suoraviivaisimman tien kompleksisen logaritmin määrittelyyn tarjoaa polaariesitys: Jos $z = |z|e^{i\theta}$, voidaan kompleksiluku z kirjoittaa vaihekulman monikäsitteisyyden vuoksi äärettömän monella eri tavalla:

$$z = |z|e^{i(\theta+n \cdot 2\pi)},$$

missä $n \in \mathbb{Z}$. Nämä esitysasut antavat aiheen seuraavaan määritelmään.

Esimerkki 91. Lasketaan luvun -2 logaritmin arvot. Tätä varten etsitään luvun -2 polaariesitys: $-2 = 2e^{\pi i}$, mutta on otettava huomioon, että vaihekulmaan voidaan lisätä mikä hyvänsä 2π :n monikerta, jolloin siis $-2 = 2e^{i(\pi+n \cdot 2\pi)}$, missä $n \in \mathbb{Z}$. Tällöin siis kaikki logaritmin $\text{Log}(-2)$ arvot ovat

$$\text{Log}(-2) = \{\ln 2 + i(\pi + n \cdot 2\pi) \mid n \in \mathbb{Z}\}.$$

Esimerkki 92. Lasketaan luvun i logaritmin arvot. Tätä varten käytetään polaariesitystä: $i = e^{i\frac{\pi}{2}} = e^{i(\frac{\pi}{2}+n \cdot 2\pi)}$, missä $n \in \mathbb{Z}$. Näin ollen

$$\text{Log } i = \{i(\frac{\pi}{2} + n \cdot 2\pi) \mid n \in \mathbb{Z}\}.$$

Logaritmin monikäsitteisyyden poistamiseksi voidaan ottaa käyttöön seuraava käsite:

Esimerkki 93. $\overline{\text{Log}}(-2) = \ln 2 + \pi i$ ja $\overline{\text{Log}} i = i\frac{\pi}{2}$.

6.4 Kompleksinen potenssiinkorotus

Potenssiinkorotus, jossa sekä kantaluku että eksponentti voivat olla kompleksilukuja määritellään logaritmi- ja eksponenttifunktion avulla. Koska reaaliluvuille $a \neq 0$ ja b pätee

$$a^b = e^{\ln a^b} = e^{b \ln a},$$

käytetään tätä lähtökohtana kompleksista potenssia määriteltäessä. Haittapuolena kompleksilukujen yhteydessä on tietenkin logaritmin monikäsitteisyys, mutta osoittautuu, että joissakin tapauksissa eksponenttifunktion epäinjektiivisyys poistaa monikäsitteisyyttä jonkin verran. Lähtökohtaisesti kuitenkin hyväksytään, että kompleksinen potenssiinkorotus $(a, b) \mapsto a^b$ ei ole funktio, vaan relaatio.

Esimerkki 94. Lasketaan potenssin i^i kaikki arvot. Aiemman esimerkin mukaan logaritmin $\text{Log } i$ kaikki arvot ovat

$$\text{Log } i = \{i(\frac{\pi}{2} + n \cdot 2\pi) \mid n \in \mathbb{Z}\},$$

joten

$$i \log i = \{-\frac{\pi}{2} - n \cdot 2\pi \mid n \in \mathbb{Z}\}.$$

Tällöin siis

$$i^i = e^{\text{Log } i^i} = e^{i \log i} = \{e^{-\frac{\pi}{2} - n \cdot 2\pi} \mid n \in \mathbb{Z}\}.$$

Esimerkki 95. Lasketaan potenssin 3^2 kaikki arvot.

$$3^2 = e^{\text{Log } 3^2} = e^{2 \text{Log } 3},$$

joten on siis selvitettävä kaikki logaritmin $\text{Log } 3$ arvot. Luvun 3 polaariesitys on $3 = 3e^{i \cdot 0} = 3e^{n \cdot 2\pi i}$, missä $n \in \mathbb{Z}$, mistä saadaan

$$\text{Log } 3 = \{\ln 3 + n \cdot 2\pi i \mid n \in \mathbb{Z}\}.$$

Näin ollen potenssin 3^2 kaikki arvot ovat

$$\{e^{2\ln 3 + 4n\pi i} \mid n \in \mathbb{Z}\} = \{e^{\ln 3^2} e^{4n\pi i} \mid n \in \mathbb{Z}\} = \{3^2\} = \{9\}.$$

Tässä siis eksponenttifunktio kumoaa logaritmifunktion tuottaman monikäsitteisyyden. On helppo huomata, että näin tapahtuu aina, kun eksponentti on kokonaisluku, jolloin potenssi voidaan aina määritellä toistettuna kertolaskuna.

Esimerkki 96. Lasketaan kaikki potenssin $8^{\frac{1}{3}}$ arvot.

$$8^{\frac{1}{3}} = e^{\text{Log } 8^{\frac{1}{3}}} = e^{\frac{1}{3} \text{Log } 8},$$

joten on selvitettävä kaikki $\text{Log } 8$:n arvot. $8 = 8e^{n \cdot 2\pi i}$, mistä

$$\text{Log } 8 = \{\ln 8 + n \cdot 2\pi i \mid n \in \mathbb{Z}\}$$

ja potenssin $8^{\frac{1}{3}}$ kaikki arvot ovat

$$\{e^{\frac{1}{3}(\ln 8 + n \cdot 2\pi i)} \mid n \in \mathbb{Z}\} = \{e^{\frac{1}{3} \ln 8} e^{\frac{n \cdot 2\pi i}{3}} \mid n \in \mathbb{Z}\} = \{2e^{\frac{n \cdot 2\pi i}{3}} \mid n \in \mathbb{Z}\}.$$

Nyt tulee vielä selvittää, mitä arvoja $e^{\frac{n \cdot 2\pi i}{3}}$ saa, kun $n \in \mathbb{Z}$. Jaetaan tätä varten tarkastelu kolmeen osaan: 1) $n = 3k$, missä $k \in \mathbb{Z}$. Tällöin $e^{\frac{n \cdot 2\pi i}{3}} = e^{\frac{2 \cdot 3k \cdot \pi i}{3}} = e^{2k\pi i} = 1$. 2) $n = 3k + 1$, missä $k \in \mathbb{Z}$. Tällöin $e^{\frac{n \cdot 2\pi i}{3}} = e^{\frac{2 \cdot (3k+1) \cdot \pi i}{3}} = e^{2k\pi i} e^{\frac{2\pi i}{3}} = e^{\frac{2\pi i}{3}}$. 3) $n = 3k + 2$, missä $k \in \mathbb{Z}$. Tällöin $e^{\frac{n \cdot 2\pi i}{3}} = e^{\frac{2 \cdot (3k+2) \cdot \pi i}{3}} = e^{2k\pi i} e^{\frac{4\pi i}{3}} = e^{\frac{4\pi i}{3}}$.

Näin ollen kaikki potenssin $8^{\frac{1}{3}}$ arvot ovat

$$\{2, 2e^{\frac{2\pi i}{3}}, 2e^{\frac{4\pi i}{3}}\},$$

jotka voidaan vielä Eulerin kaavan avulla kirjoittaa muotoon

$$\{2, -1 + i\sqrt{3}, -1 - i\sqrt{3}\}.$$

Tämä on sopusoinnussa sen kanssa, että mikä hyvänsä näistä luvuista potenssiin kolme korotettuna antaa luvun 8.

Tässä esimerkissä eksponenttifunktio ei kumoa kokonaan logaritmin tuottamaa monikäsitteisyyttä, sillä eksponentilla on nimittäjä 3.

Edellisissä esimerkeissä havaitut seikat on mahdollista yleistää suoraviivaisesti: Koska kompleksisen potenssin määritelmän (määritelmä ??) mukaan kaikki arvot ovat muotoa

$$e^{b(\ln r + i(\theta + n \cdot 2\pi))} = e^{b \ln r + b\theta i} e^{b \cdot n \cdot 2\pi i},$$

missä $n \in \mathbb{Z}$, voidaan toimia kuten edellisissä esimerkeissä ja todeta seuraava tulos.

Lause 36.

- Jos $b \in \mathbb{Z}$, kompleksinen potenssi a^b on yksikäsitteinen ja yhtyy kertolaskun avulla saatuun määritelmään:

$$a^b = \underbrace{a \cdot \dots \cdot a}_{b \text{ kpl}}$$

- Jos $b = \frac{p}{q} \in \mathbb{Q}$ on supistetussa muodossa, on kompleksisella potenssilla a^b q eri arvoa, jotka saadaan yhdestä arvosta kertomalla luvuilla $e^{\frac{n \cdot 2\pi i}{q}}$, $n \in \{0, 1, \dots, q-1\}$.
- Jos $b \notin \mathbb{Q}$, on kompleksisella potenssilla a^b äärettömän monta eri arvoa, jotka saadaan yhdestä arvosta kertomalla luvuilla $e^{b \cdot n \cdot 2\pi i}$, $n \in \mathbb{Z}$.

Huomautus 30. Kokonaislukueksponentin $b = n$ kannalta polaarimuoto voi toisinaan olla käyttökelpoinen:

$$z^b = (|z|e^{i\theta})^n = |z|^n e^{in\theta},$$

mikä siis merkitsee sitä, että itseisarvo korotetaan potenssiin n ja vaihekulma kerrotaan luvulla n .

Esimerkki 97. Lasketaan $(\frac{1}{\sqrt{2}}(1+i))^{105}$. Tätä varten selvitetään ensin polaariesitys: $\frac{1}{\sqrt{2}}(1+i) = e^{i\frac{\pi}{4}}$, josta $(\frac{1}{\sqrt{2}}(1+i))^{105} = e^{i\frac{\pi}{4} \cdot 105} = e^{i\frac{\pi}{4} \cdot (13 \cdot 8 + 1)} = e^{13 \cdot 2\pi i} e^{i\frac{\pi}{4}} = e^{i\frac{\pi}{4}} = \frac{1}{\sqrt{2}}(1+i)$.

Aiemmat määritelmät johtavat myös siihen, että n :s juuri kompleksiluvusta saadaan juurtamalla itseisarvo (reaalinen juuri) ja *jakamalla* vaihekulma luvulla n . Tällöin on vain huomioitava, että kompleksiluvulla on ääretön määrä esitysmuotoja (vaihekulmaan voidaan aina lisätä 2π :n monikerä).

Esimerkki 98. Koska $-1 = e^{\pi i} = e^{3\pi i}$, ovat luvun -1 kaikki toiset juuret $e^{\frac{\pi}{2}i} = i$ ja $e^{\frac{3\pi}{2}i} = -i$.

Nimensä mukaan n :nnet ykkösenjuuret potenssiin n korotettuna tuottavat ykkösen, mikä nähdään suoraan lausekkeista. Vaihekulmista nähdään lisäksi, että ykkösenjuuret sijaitsevat tasavälein yksikköympyrällä. Lisäksi 1 on aina niiden joukossa (kts. kuva 6.4). Vielä yksi merkittävä huomio on, että kaikki n :nnet ykkösenjuuret saadaan ns. *primitiivisen ykkösenjuuren* potensseina.

Kompleksista potenssia voidaan myös rajoittaa samoin kuin logaritmiakin:

Kompleksisen potenssin pääarvolle ei ole vakiintunutta merkintää, mutta yleensä kompleksisesta potenssista puhuttaessa tarkoitetaan sen pääarvoa, ellei toisin ilmoiteta.

Esimerkki 100. Koska $\overline{\text{Log}} i = i\frac{\pi}{2}$, on potenssin i^i pääarvo

$$e^{\overline{\text{Log}} i^i} = e^{i\overline{\text{Log}} i} = e^{-\frac{\pi}{2}}.$$

Esimerkki 101. Kompleksilukujen neliöjuuret voidaan aina löytää xy -muodossa seuraavasti: Suoralla laskulla todetaan, että $(x+yi)^2 = (x^2-y^2) + 2xy \cdot i$, joten luvun $a+bi$ neliöjuuren $x+yi$ pitää toteuttaa $a = x^2 - y^2$ sekä $b = 2xy$. Ratkaisemalla x ja y yhtälöparista

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$

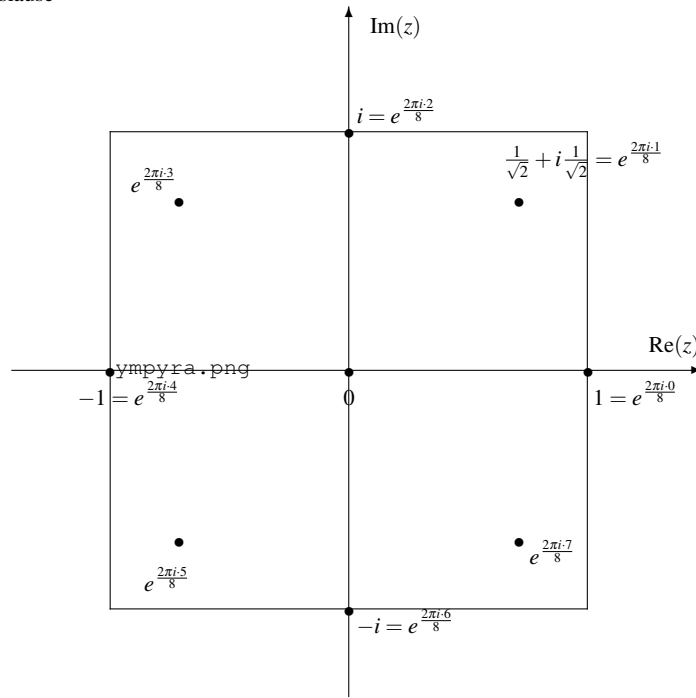
saadaan luvun $a+bi$ neliöjuuret muodossa $x+yi$.

6.5 Kompleksilukujen trigonometriset funktiot

Trigonometrysten funktioiden laajentaminen kompleksialueelle perustuu Eulerin kaavaan

$$e^{i\theta} = \cos \theta + i \sin \theta.$$

Jos tähän sijoitetaan θ :n paikalle $-\theta$, saadaan



Kuva 6.2 Kahdeksannet ykkösenjuuret ovat kaikki yhtälön $z^8 = 1$ ratkaisut eli polynomin $z^8 - 1$ nollakohdat.

$$e^{-i\theta} = \cos \theta - i \sin \theta.$$

Laskemalla yhteen näin saadut kaksi yhtälöä saadaan $e^{i\theta} + e^{-i\theta} = 2 \cos \theta$, kun taas vähennyslasku tuottaa $e^{i\theta} - e^{-i\theta} = 2i \sin \theta$. Koska eksponenttifunktio on jo määritelty kaikille kompleksiluvuille, voidaan asettaa seuraava määritelmä:

Muut trigonometriset funktiot kuten tangenti määritellään samoin kuin reaali-luvuille, esim. $\tan z = \frac{\sin z}{\cos z}$. Koska kompleksinen eksponenttifunktio on yksikäsitteinen, samoin ovat sini ja kosini. Lisäksi on huomattava, että eksponenttifunktion jaksosta $2\pi i$ seuraa sinille ja kosinille jakso 2π . Tunnettu trigonometrinen identiteetti $\sin^2 z + \cos^2 z = 1$ voidaan huomata oikeaksi jo heti määritelmän perusteella. Trigonometrian summakaavat puolestaan voidaan johtaa eksponenttifunktion ominaisuudesta $e^{z_1+z_2} = e^{z_1} e^{z_2}$.

Esimerkki 102.

$$\cos i = \frac{1}{2}(e^{i \cdot i} + e^{-i \cdot i}) = \frac{1}{2}(e^{-1} + e^1) \approx 1,54,$$

joten trigonometristen funktioiden arvo kompleksialueella *ei rajoitu* välille $[-1, 1]$. Itse asiassa trigonometristen funktioiden arvo ei välttämättä ole reaalinen, kuten helposti nähdään laskemalla $\sin i$.

6.6 Algebran peruslause

Kun kompleksiluvut on otettu käyttöön, voidaan tietenkin kysyä olisiko syytä laajentaa lukujoukkoja vielä tästäkin. Kompleksilukuja koskevan osion alussa esitetty tarve ainakin poistuu seuraavan tuloksen myötä.

Lause 37 (Algebran peruslause). *Olkoon $P(z)$ mikä hyvänsä polynomi, joka ei ole vakio ja jonka kertoimet ovat kompleksilukuja. Tällöin polynomiyhtälöllä $P(z) = 0$ on aina olemassa ratkaisu joukossa $\mathbb{C}$.*

Todistus. Vaatii esitietoja, jotka eivät kuulu tähän kurssiin ja on muutenkin mutkikas, sivuutetaan.

Edellinen tulos kertoo, että kompleksiluvut muodostavat ns. *algebrallisesti suljetun kunnan*, jossa kaikilla polynomeilla on nollakohta, eikä siksi polynomiyhtälöiden ratkaisun kannalta tarvitse laajentaa lukualuetta enempää.

Tästä huolimatta voidaan kuitenkin ajatella kompleksilukujen kuntaa laajennettavaksi edelleen. Yksi mahdollinen laajennustapa nousee esille kompleksilukujen määritelmästä: Kompleksiluvuthan ovat oleellisesti ottaen reaalilukupareja, joten voitaisiin otaksua, että laajempi lukujoukko saataisiin tarkastelemalla reaalilukukolmikoita, -nelikoita, jne. ja määrittelemällä näille yhteen- ja kertolaskut siten, että reaalilukujen tutut laskusäännöt (vaihdannaisuus, liitännäisyys, käänteisluvut, jne., katso esimerkki 9) säilyisivät.

Tarkempi algebran tutkimus osoittaa kuitenkin, että tämä ei ole mahdollista. Käy ilmi, että kaikki tällaiset kolmikoihin, nelikoihin, jne. perustuvat laajennukset olisivat reaalilukujen kunnan *algebraalisia* laajennuksia, ja algebran peruslauseesta seuraa, että kompleksilukujen kunnalla ei ole algebraalisia laajennuksia.

Huomautus 31. Algebran peruslause takaa, että jokaisella kompleksikertoimisella polynomilla $P(z)$ on olemassa nollakohta $c \in \mathbb{C}$, ei sitä, että nollakohdat saataisiin polynomin kertoimista algebrallisesti. Korkeintaan astetta 4 oleville polynomeille nollakohdat kuitenkin voidaan löytää polynomin kertoimien algebrallisina funktioina, toisin sanoen korkeintaan astetta 4 oleville polynomeille on olemassa *algebraallinen* ratkaisukaava. Viidettä tai sitä korkeampaa astetta oleville polynomeille ei ole yleistä algebraalista ratkaisukaavaa, mutta minkä hyvänsä polynomin nollakohdille voidaan aina löytää niin tarkat likiarvot kuin halutaan.

Taustatietoa

Girolamo Cardano (1501–1576) oli italialainen lääkäri ja matemaatikko, jonka julkistamat ratkaisukaavat 3. ja 4. asteen yhtälöille johtivat kompleksilukujen yleiseen käyttöön. Cardano ei kuitenkaan keksinyt kaavoja itse, vaan oli saanut tietoonsa 3. asteen ratkaisukaavat, jotka Niccolò Tartaglia (n. 1499–1557) ja Scipio del Ferro (n. 1465–1526) olivat kehittäneet toisistaan tietämättä aiemmin. Cardano kehitti 4. asteen yhtälön ratkaisukaavan yhdessä oppilaansa Lodovico Ferrarin (1522–1565) kanssa ja julkisti kaikki ratkaisukaavat teoksessaan *Ars magna* (1554). Siksi mainitut kaavat tunnetaan nykyisin *Cardanon kaavoina* (kuva: Wikimedia Commons)

Lause 38. Jos polynomilla $P(z)$ on nollakohta c_1 , niin $P(z)$ on jaollinen polynomilla $z - c_1$.

Todistus. Jakolaskulla (polynomien jakolaskua käsitellään tarkemmin monisteen viimeisessä luvussa) saadaan $P(z) = (z - c_1)P_1(z) + r(z)$, missä $P_1(z)$ on osamäärä ja $r(z)$ jakojäännös. Koska jakojäännöksen $r(z)$ aste on pienempi kuin jakajan $z - c$ aste, on $r(z)$ välttämättä vakiopolynomi, merkitään $r(z) = r$. Nyt siis $P(z) = (z - c_1)P_1(z) + r$, ja sijoittamalla c_1 saadaan $0 = P(c_1) = (c_1 - c_1)P_1(c_1) + r = r$, siis $r = 0$ ja $P(z) = (z - c_1)P_1(z)$.

Huomautus 32. Huomaa, että vastakkainen tulos pätee ilman muuta: jos $P(z)$ on jaollinen polynomilla $z - c_1$, on sillä nollakohta c_1 . Tämä seuraa suoraan sijoittamalla c_1 hajotelmaan $P(z) = (z - c_1)P_1(z)$.

Huomautus 33. Olkoon $P_1(z)$ edellisen lauseen osamäärä. Se on polynomi, jonka aste on yhtä pienempi kuin $P(z)$:n aste, ja jos se ei ole vakio, on sillä algebran peruslauseen nojalla nollakohta c_2 . Edelleen, lauseen 38 nojalla $P_1(z) = (z - c_2)P_2(z)$, missä $P_2(z)$:n aste on yhtä pienempi kuin $P_1(z)$:n. Tällöin siis $P(z) = (z - c_1)(z - c_2)P_2(z)$, ja samaa menettelyä voidaan soveltaa edelleen polynomiin $P_2(z)$, ellei se ole vakio (siis astetta 0). Lopulta päädytään lausekkeeseen $P(z) = (z - c_1)(z - c_1) \cdots (z - c_d)a$, missä $a \in \mathbb{C}$ on vakiopolynomi ja d polynomin $P(z)$ aste. Hajotelma

$$P(z) = a(z - c_1)(z - c_2) \cdots (z - c_d) \quad (6.2)$$

kertoo sen, että *jokainen polynomi jakautuu kompleksilukujen joukossa ensimmäisen asteen tekijöihin*. Vastaava ei pidä paikkansa reaalityyppisille: jos esimerkiksi polynomilla $x^2 + 1$ olisi reaalin ensimmäisen asteen tekijä, olisi sillä myös huomautuksen 32 mukaan reaalin nollakohta.

Seuraus 1. *Astetta $d \geq 1$ olevalla polynomilla $P(z)$, on korkeintaan d nollakohtaa.*

Todistus. Hajotelmassa (6.2) luvut $c_1, c_2, \dots, c_d$ ovat kaikki $P(z)$:n nollakohdat. Koska d on polynomin $P(z)$ aste, on nollakohtia korkeintaan d .

Huomautus 34. Kertomalla tulo (6.2) auki nähdään helposti, että a on polynomin $p(z)$ korkeimman asteen termin vakiokerroin.

Milloin sitten astetta d olevalla polynomilla voi olla *vähemmän* kuin d nollakohtaa? Tarkastelemalla hajotelmaa (6.2) huomataan, että näin voi käydä vain silloin, kun jotkin luvuista $c_1, c_2, \dots, c_d$ ovat keskenään yhtäsuuria. Esimerkkinä käy toisen asteen polynomi $z^2 - 2z + 1 = (z - 1)(z - 1)$, jolla on vain yksi nollakohta $z = 1$. Tämän kaltaisessa tapauksessa sanotaan kuitenkin, että $z = 1$ on polynomin $z^2 - 2z + 1$ *kaksinkertainen* nollakohta. Vastaavasti määritellään *kolminkertainen* nollakohta, jne.

Kompleksiluvut annetaan **Matlabille** seuraavan esimerkin mukaisesti:

```
>> (5+3i)/(1+2i)
```

```
ans =
```

```
11/5 - 7/5i
```

Vastaus siis tulkitaan siten, että $\frac{5+3i}{1+2i} = \frac{11}{5} - \frac{7}{5}i$.

Kompleksikonjugaatin tuottaa $\text{conj}(z)$ ja itseisarvon $\text{abs}(z)$. Vaihekulma puolestaan saadaan komennolla $\text{angle}(z)$. Reaali- ja imaginaariosat saadaan eroteltua komennoilla $\text{real}(z)$ ja $\text{imag}(z)$.

Selitä vastaus seuraavaan syötteeseen:

```
>> imag(log(-1))
```

```
ans =
```

```
3.1416
```

```
>>
```

Luvun oleellisia asioita:

- Imaginaariyksikkö, kompleksilukujen summa, tulo ja osamäärä.
- Liittoluku.
- Kompleksilukujen itseisarvo ja polaariesitys.
- Eulerin kaava.
- Kompleksilukujen eksponenttifunktio, sini, kosini, potenssi, juuret ja logaritmi; pääarvo.
- Algebran peruslause.

Luku 7

Lineaaristen yhtälöryhmien ratkaiseminen

Lineaariset yhtälöryhmät esiintyvät monenlaisissa sovelluksissa. Tässä luvussa käsitellään niiden yleistä ratkaisumenetelmää, jota voidaan käyttää myöhemmin monissa yhteyksissä. Varsinaiseen lineaarialgebraan ei kuitenkaan perehdytä tässä luvussa, vaan vasta kurssilla Insinöörimatematiikka D. Matriisin käsite liittyy kuitenkin lineaarisiin yhtälöryhmiin niin kiinteästi, että tarvittava terminologia on syytä esittää ja omaksua jo tässä yhteydessä.

7.1 Matriisilaskennan peruskäsitteet

Mikä hyvänsä $m \times n$ -matriisi voidaan siis esittää rivivektoreiden kokoelmana (m kpl) tai sarakevektoreiden kokoelmana (n kpl). Rivivektorin koordinaatit on tapana erottaa pilkulla. Vektoreita on tapana merkitä myös lihavoiduilla kirjaimilla ja yksinkertaisella indeksoinnilla, esimerkiksi

$$\vec{x} = (x_1, x_2, \dots, x_n) \text{ ja } \vec{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}. \text{ Jos koordinaattien määrä on korkeintaan kolme, voidaan vektori tulkitä geometrisesti kolmi- tai pienempiulotteisen avaruuden pisteinä. Tätä tulkintaa on yleensä tapana laajentaa suuntajanaaksi origosta kyseiseen pisteeseen ja jopa kaikkien samansuuntaisten ja -pituisten suuntajanojen joukoksi.}$$

Esimerkki 103. $A = \begin{pmatrix} 2 & -1 & 0 \\ 0 & 1 & 3 \end{pmatrix}$ on 2×3 -matriisi ja $5A = \begin{pmatrix} 10 & -5 & 0 \\ 0 & 5 & 15 \end{pmatrix}$

Esimerkki 104. $A = \begin{pmatrix} 2 & -1 & 0 \\ 0 & 1 & 3 \end{pmatrix}$ on 2×3 -matriisi ja $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \\ -1 & 3 \end{pmatrix}$ 3×2 -matriisi, joten summaa $A + B$ ei ole määritelty.

Esimerkki 105. $A = \begin{pmatrix} 2 & -1 & 0 \\ 0 & 1 & 3 \end{pmatrix}$ on 2×3 -matriisi ja $B = \begin{pmatrix} 1 & 2 & -1 \\ 0 & 1 & 3 \end{pmatrix}$ on 2×3 -matriisi, joten summa $A + B$ on määritelty:

$$A + B = \begin{pmatrix} 2 & -1 & 0 \\ 0 & 1 & 3 \end{pmatrix} + \begin{pmatrix} 1 & 2 & -1 \\ 0 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 & -1 \\ 0 & 2 & 6 \end{pmatrix}$$

Esimerkki 106.

$$(-x + 3, -x - 1, x) = (-x, -x, x) + (3, -1, 0) = x(-1, -1, 1) + (3, -1, 0).$$

Matlab-ohjelmistoon (versio 6.5) matriisit syötetään siten, että rivit erotetaan toisistaan puolipisteellä ja alkiot pilkuilla. Esimerkiksi matriisit

$$A = \begin{pmatrix} 1 & 3 & -3 & -2 \\ 0 & 2 & 1 & -2 \\ -4 & 1 & 2 & -3 \end{pmatrix} \text{ ja } B = \begin{pmatrix} 2 & 0 & -1 & -1 \\ 1 & 0 & 3 & 3 \\ -1 & 5 & 0 & -2 \end{pmatrix}$$

Syötetään seuraavasti:

```
>> A=[1,3,-3,-2;0,2,1,-2;-4,1,2,-3]
```

```
>> B=[2,0,-1,-1;1,0,3,3;-1,5,0,-2]
```

Matriisien summa lasketaan seuraavasti:

```
>> A+B
```

```
ans =
     3     3    -4    -3
     1     2     4     1
    -5     6     2    -5
```

```
>>
```

Matriisitulon merkitys esitellään varsinaisesti vasta osassa Insinöörimatematiikka D, mutta muiden kurssien vuoksi matriisitulon määritelmä pitää esittää jo tässä vaiheessa.

Matriisitulo on siis määritelty vain silloin, kun tulon ensimmäisen tekijän sarakkeiden määrä on yhtä suuri kuin jälkimmäisen tekijän rivien määrä.

Esimerkki 107.

$$\begin{aligned} & \begin{pmatrix} 2 & 1 & 1 \\ -1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 1 \\ 1 & 2 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 2 \cdot 1 + 1 \cdot 2 + 1 \cdot 1 & 2 \cdot 0 + 1 \cdot 1 + 1 \cdot 2 & 2 \cdot 0 + 1 \cdot 1 + 1 \cdot 2 \\ -1 \cdot 1 + 2 \cdot 2 + 3 \cdot 1 & -1 \cdot 0 + 2 \cdot 1 + 3 \cdot 2 & -1 \cdot 0 + 2 \cdot 1 + 3 \cdot 2 \end{pmatrix} \\ &= \begin{pmatrix} 5 & 3 & 3 \\ 6 & 8 & 8 \end{pmatrix}. \end{aligned}$$

Esimerkki 108.

$$\begin{aligned} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix} &= \begin{pmatrix} 4 & 8 \\ 3 & 5 \end{pmatrix}, \\ \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} &= \begin{pmatrix} 5 & 4 \\ 6 & 4 \end{pmatrix}. \end{aligned}$$

Edellinen esimerkin osoittaa, että matriisitulo ei ole yleisesti *kommutatiivinen* (vaihdannainen), toisin sanoen voi olla $AB \neq BA$.

Esimerkki 109.

$$\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Tämä esimerkki puolestaan osoittaa, että *tulon nollasääntö* ei päde matriiseille, mikä siis merkitsee sitä, että $AB = O$ on mahdollinen, vaikka $A \neq O$ ja $B \neq O$.

Lause 39. *Matriisitulolle on voimassa seuraavat yhtäsuuruudet:*

1. $A(BC) = (AB)C$
2. $A(B+C) = AB+AC$
3. $(A+B)C = AC+BC$
4. $a(AB) = (aA)B = A(aB)$
5. $AO = OA = O$
6. $AI = IA = A$,
7. $(AB)^T = B^T A^T$,

edellyttäen että kunkin yhtälön vasen puoli on määritelty.

Todistus. Suoraviivainen, mutta työläs. Jätetään harjoitustehtäväksi.

Huomautus 35. Suoraan määritelmästä seuraa, että matriisitulo voidaan laskea myös lohkoittain:

$$\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix} = \begin{pmatrix} A_1 B_1 + A_2 B_3 & A_1 B_2 + A_2 B_4 \\ A_3 B_1 + A_4 B_3 & A_3 B_2 + A_4 B_4 \end{pmatrix},$$

mikäli lohkojen A_i ja B_i koot on valittu siten, että kaikki tulot ovat määriteltyjä.

Matlab-ohjelmistossa matriisikertolasku ilmaistaan asteriskilla $*$ ja potenssi nuolella $^$

```
>> A*B
```

```
ans =
```

```
    -20     12     6  
     -9     -1     3  
    -18     -5     8
```

```
>>
```

7.2 Gaussin-Jordanin menetelmä

Lineaaristen yhtälöryhmien ratkaisuja voidaan löytää lukiokurssista tutulla *muuttujien eliminointimenetelmällä*, jossa yhtälö kerrotaan jollakin luvulla ja lisätään toiseen muuttujien määrän vähentämiseksi. Vaihtoehtoisesti voidaan jokin muuttuja esittää muiden muuttujien avulla ja sijoittaa ryhmään. Kumpikin tapa toimii, mikäli alkuperäisellä yhtälöryhmällä on yksikäsitteinen ratkaisu, mutta ratkaisujoukon ollessa ääretön kumpikaan ei välttämättä johda selkeästi päättyvään prosessiin. Tässä luvussa esiteltävä Gaussin-Jordanin eliminointimenetelmä ei tuo mitään uutta käytettäviin operaatioihin nähden, vaan sen erityinen piirre on selkeästi hallittava, arvioitava ja päättyvä prosessi.

Esimerkki 110. Lisätään yhtälöparin

$$\begin{cases} 2x_1 - x_2 + x_3 = 7 \\ x_1 + 3x_2 + 4x_3 = 0 \end{cases}$$

toinen yhtälö ensimmäiseen -2 :lla kerrottuna, jolloin saadaan

$$\begin{cases} -7x_2 - 7x_3 = 7 \\ x_1 + 3x_2 + 4x_3 = 0 \end{cases}.$$

Kerrotaan tämän jälkeen ensimmäinen yhtälö luvulla $-\frac{1}{7}$ ja vaihdetaan yhtälöiden järjestystä. Näin saadaan

$$\begin{cases} x_1 + 3x_2 + 4x_3 = 0 \\ x_2 + x_3 = -1 \end{cases}.$$

Lisätään nyt toinen yhtälö ensimmäiseen luvulla -3 kerrottuna. Tuloksena saadaan yhtälöpari

$$\begin{cases} x_1 + x_3 = 3 \\ x_2 + x_3 = -1 \end{cases},$$

jonka ratkaisut (x_1, x_2, x_3) ovat ilmeiset: ensimmäisen yhtälön perusteella $x_1 = -x_3 + 3$ ja toisen yhtälön nojalla $x_2 = -x_3 - 1$. Täten siis viimeisimmän yhtälöparin ratkaisut ovat muotoa $(x_1, x_2, x_3) = (-x_3 + 3, -x_3 - 1, x_3) = x_3(-1, -1, 1) + (3, -1, 0)$, missä x_3 on mikä tahansa reaaliluku. Ratkaisut ovat siis muotoa $t(-1, -1, 1) + (3, -1, 0)$, missä $t \in \mathbb{R}$ ja täten ratkaisuja on ääretön määrä.

Nyt kuitenkin puhuttiin *viimeisimmän* yhtälöparin ratkaisuksista, mutta helposti voidaan nähdä, että nämä ovat myös alkuperäisen yhtälöparin ratkaisut. Ensinnäkin, alkeisoperaatiot ovat selvästi totuusarvon säilyttäviä siinä mielessä, että jos yhtälöryhmä S' saadaan yhtälöryhmästä S jotakin näistä operaatioista hyödyntämällä, on ryhmällä S' välttämättä *ainakin* ne ratkaisut, jotka ryhmällä S on. Toisin sanoen, jos ryhmä S toteutuu joillakin muuttujien arvoilla, niin myös ryhmä S' toteutuu samoilla arvoilla.

Toisaalta taas alkeisoperaatiot ovat *kääntyviä*, sillä ryhmästä S' voidaan saada jälleen S alkeisoperaatioilla. Jos nimittäin suoritettu alkeisoperaatio oli yhtälöiden järjestyksen vaihto, voidaan samainen vaihto suorittaa uudelleen alkuperäisen yhtälöryhmän palauttamiseksi. Jos taas alkeisoperaatio oli yhtälön kertominen nolasta eroavalla vakiolla, saadaan alkuperäinen ryhmä kertomalla vakion käänteisluvulla. Yhtälön lisääminen toiseen vakiolla kerrottuna voidaan puolestaan kääntää lisäämällä sama yhtälö vakion vastaluvulla kerrottuna.

Kuten aiemmin todettiin, ryhmällä S' on *ainakin* ne ratkaisut, jotka ryhmällä S on, mutta koska ryhmästä S' voidaan alkeisoperaatiota käyttäen saada jälleen ryhmä S , saadaan seuraava lause:

Lause 40. *Jos yhtälöryhmään sovelletaan mitä hyvänsä alkeisoperaatiota, on tuloksena yhtälöryhmä, jolla on tarkalleen samat ratkaisut kuin alkuperäisellä ryhmällä. Tällöin sanotaan, että ryhmät ovat ekvivalentit.*

Lauseen 40 mukaan yhtälöryhmän ratkaisemiseksi voidaan ryhmään soveltaa alkeisoperaatiota, kunnes saadaan niin yksinkertainen ryhmä, että sen ratkaisut nähdään suoraan. Juuri näin tehtiin esimerkissä 110.

Menettelytapaa tarkastelemalla huomataan helposti, että muuttujien ja yhtäsuuruusmerkkien kirjoittaminen joka vaiheeseen ei anna mitään lisäinformaatiota. Esimerkissä 110 voidaan yhtälöparin sijaan yhtä hyvin käyttää *kerroinmatriiseja*, joka on $\begin{pmatrix} 2 & -1 & 1 \\ 1 & 3 & 4 \end{pmatrix}$. Lisäämällä tähän oikealla puolella esiintyvät vakiot omaksi sarakkeekseen saadaan ns. *augmentoitu* eli laajennettu kerroinmatriisi $\begin{pmatrix} 2 & -1 & 1 & 7 \\ 1 & 3 & 4 & 0 \end{pmatrix}$.

Välttömästi huomataan, että esitettäessä yhtälöryhmiä tällä tavalla matriisimuodossa ilman muuttujia alkeisoperaatiot voidaan tulkita *matriisien alkeisoperaatioiksi* jotka siis määritellään seuraavasti:

Huomaa, että esimerkin 110 toisen yhtälöparin (augmentoitu) matriisi on

$$\begin{pmatrix} 0 & -7 & -7 & 7 \\ 1 & 3 & 4 & 0 \end{pmatrix},$$

mikä saadaan ensimmäisen yhtälöparin augmentoidusta matriisista lisäämällä toinen rivi ensimmäiseen -2 :lla kerrottuna. Vastaavasti esimerkin toinen yhtälöpari saatiin ensimmäisestä lisäämällä toisen yhtälö ensimmäiseen -2 :lla kerrottuna. Tämä on varsin ymmärrettävää, koska *augmentoidut matriisit esittävät yhtälöryhmiä täsmällisesti*, ainoastaan muuttujat ja yhtäsuuruusmerkit on jätetty kirjoittamatta. Täten siis yhtälöryhmiä ratkaistaessa voidaan yhtä hyvin tarkastella augmentoituja matriiseja ja suorittaa niille alkeisoperaatioita.

Ylläolevasta tarkastelusta seuraa välittömästi seuraava tulos:

Lause 41. Jos lineaaristen yhtälöryhmien S_1 ja S_2 augmentoidut matriisit A ja B ovat riviekvivalentteja, on ryhmällä S_1 ja S_2 samat ratkaisut.

Yhtälöryhmien yleinen ratkaisustrategia onkin etsiä ryhmän alkuperäisen (augmentoidun) matriisin A kanssa riviekvivalentti matriisi B , jossa on mahdollisimman paljon nollia. Tällöin ratkaisut on helppo selvittää. Mitä sitten tarkoittaa ”mahdollisimman paljon nollia”? Tätä ryhdytään selvittämään seuraavaksi.

Esimerkki 111. Ratkaistaan yhtälöryhmä

$$\begin{cases} 2x - y + 3z = 4 \\ 3x + 2y + z = 6 \\ -5x + y - 2z = 3 \end{cases}.$$

Ryhmän augmentoitu matriisi on $\begin{pmatrix} 2 & -1 & 3 & 4 \\ 3 & 2 & 1 & 6 \\ -5 & 1 & -2 & 3 \end{pmatrix}$. Kertomalla ensimmäinen rivi vakiolla $\frac{1}{2}$ saa-

daan $\begin{pmatrix} 1 & -\frac{1}{2} & \frac{3}{2} & 2 \\ 3 & 2 & 1 & 6 \\ -5 & 1 & -2 & 3 \end{pmatrix}$, missä edelleen voidaan lisätä ensimmäinen rivi toiseen -3 :lla kerrottuna

ja kolmanteen 5 :llä kerrottuna. Tuloksena saadaan matriisi $\begin{pmatrix} 1 & -\frac{1}{2} & \frac{3}{2} & 2 \\ 0 & \frac{7}{2} & -\frac{7}{2} & 0 \\ 0 & -\frac{3}{2} & \frac{11}{2} & 13 \end{pmatrix}$. Kerrotaan näin

saadun matriisin toinen rivi $\frac{2}{7}$:llä. Näin saadaan $\begin{pmatrix} 1 & -\frac{1}{2} & \frac{3}{2} & 2 \\ 0 & 1 & -1 & 0 \\ 0 & -\frac{3}{2} & \frac{11}{2} & 13 \end{pmatrix}$, minkä jälkeen lisätään toinen rivi ensimmäiseen $\frac{1}{2}$:lla kerrottuna ja kolmanteen $\frac{3}{2}$:lla kerrottuna. Tuloksena saatava matriisi

on $\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 4 & 13 \end{pmatrix}$, josta kolmas rivi $\frac{1}{4}$:lla kertomalla saadaan $\begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & \frac{13}{4} \end{pmatrix}$. Lisäämällä kolmas rivi ensimmäiseen -1 :llä kerrottuna ensimmäiseen ja 1 :llä kerrottuna toiseen saadaan matriisi

$\begin{pmatrix} 1 & 0 & 0 & -\frac{5}{4} \\ 0 & 1 & 0 & \frac{13}{4} \\ 0 & 0 & 1 & \frac{13}{4} \end{pmatrix}$, jota vastaava yhtälöryhmä on

$$\begin{cases} x &= -\frac{5}{4} \\ y &= \frac{13}{4} \\ z &= \frac{13}{4} \end{cases},$$

mistä ratkaisu voidaan suoraan lukea: $(x, y, z) = (-\frac{5}{4}, \frac{13}{4}, \frac{13}{4})$. Tässä esimerkissä on siis tasan yksi ratkaisu.

Esimerkki 112. Yhtälöryhmää

$$\begin{cases} x + 3y + 2z = 7 \\ 2x + y - z = 5 \\ -x + 2y + 3z = 4 \end{cases}$$

vastaava agmentoitu matriisi on $\begin{pmatrix} 1 & 3 & 2 & 7 \\ 2 & 1 & -1 & 5 \\ -1 & 2 & 3 & 4 \end{pmatrix}$, mistä alkeisoperaatioilla saadaan matriisi $\begin{pmatrix} 1 & 3 & 2 & 7 \\ 0 & 1 & 1 & \frac{9}{5} \\ 0 & 0 & 0 & 2 \end{pmatrix}$.

Viimeisintä matriisia vastaavan yhtälöryhmän kolmas yhtälö on muotoa $0 \cdot z + 0 \cdot y + 0 \cdot z = 2$, siis $0 = 2$, mikä ei voi toteutua millään muuttujien x , y ja z arvoilla. Koska viimeisimmällä ryhmällä ei ole ratkaisua, ei sellaista voi olla ensimmäiselläkään, sillä ryhmiä vastaavat (augmentoidut) matriisit ovat riviekvivalentteja.

Esimerkin 110 ratkaisumenetelmää voidaan kuvailla seuraavasti: Ensin matriisi saatetaan alkeisoperaatioilla *porrasmuotoon* ja tämä edelleen *redusoituun porrasmuotoon*. Juuri redusoitu porrasmuoto on se, jossa katsotaan olevan ”mahdollisimman paljon nollia” (ainakin monia tarkoituksia varten).

Esimerkki 113. Redusoitu porrasmatriisi on siis muotoa

$$\begin{pmatrix} \cdot & \cdot & 1 & \cdot & \cdot & * & * & \cdot & \cdot & * & * & \cdot & * \\ \cdot & \cdot & \cdot & 1 & \cdot & * & * & \cdot & \cdot & * & * & \cdot & * \\ \cdot & \cdot & \cdot & \cdot & 1 & * & * & \cdot & \cdot & * & * & \cdot & * \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & * & * & \cdot & * \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & * & * & * & \cdot & * \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & * & * \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix},$$

missä pisteet merkitsevät nollia ja asteriskit mitä tahansa lukuja. Pelkkä porrasmatriisi taas tarkoittaa sitä, että ykkösten sijasta saa esiintyä mitä hyvänsä nollasta poikkeavia lukuja ja niiden yläpuolella mitä hyvänsä lukuja.

Porrasmuodon saavuttamiseksi voidaan käyttää seuraavaa menetelmää (algoritmia):

1. Jos kaikki rivit ovat nollarivejä, lopeta. Samoin jos rivejä on vain yksi, on A valmiiksi porrasmuotoa ja voidaan lopettaa.
2. Jos A :ssa enemmän kuin yksi rivi, etsi rivi $\vec{c} = (0, \dots, c, *, \dots, *)$, jolla on vähiten alkunollia ja vaihda se ylimmäksi. Jos tällaisia rivejä on useampia, valitse niistä mikä hyvänsä. Näin saadaan matriisi

$$A_1 = \begin{pmatrix} 0 & \dots & c & * & \dots & * \\ 0 & \dots & * & * & \dots & * \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & * & * & \dots & * \end{pmatrix},$$

jossa $c \neq 0$ ja asteriskit ovat mitä hyvänsä lukuja.

3. Jokaista ylimmän rivin alapuolella olevaa riviä $\vec{d} = (0, \dots, d, \dots, *)$ kohti toimi seuraavasti (d on siis alkio, joka on ylimmän rivin alkion c alapuolella): lisää ylin rivi tähän riviin kerrottuna vakiolla $-c^{-1}d$. Tällöin d siis korvautuu luvulla $d - c \cdot c^{-1}d = 0$ ja näin saadaan matriisi

$$A_2 = \begin{pmatrix} 0 & \dots & c & * & \dots & * \\ 0 & \dots & 0 & * & \dots & * \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & * & \dots & * \end{pmatrix} \xrightarrow{\text{merk.}} \begin{pmatrix} 0 & \dots & c & * & \dots & * \\ 0 & \dots & 0 & & & \\ \vdots & \ddots & \vdots & & B & \\ 0 & \dots & 0 & & & \end{pmatrix},$$

jossa c :n alapuolella on vain nollia.

4. Sovella tätä samaa menetelmää matriisiin B .

Edellä kuvattu algoritmia kutsutaan *Gaussin* menetelmäksi ja se päättyy varmasti, sillä matriisi B , johon menetelmää sovelletaan rekursiivisesti uudelleen, on riviluvultaan pienempi kuin alkuperäinen matriisi. Jossain vaiheessa siis päädytään kokonaan nollista koostuvaan tai yksiriviseen matriisiin, jolloin menetelmä päättyy. Menetelmän perusteella on lisäksi selvää, että menetelmä todella tuottaa porrasmatriisin.

Porrasmatriisista saadaan redusoitu muoto täydentämällä Gaussin menetelmää seuraavasti:

1. Kerro jokainen rivi ensimmäisen nollasta poikkeavan luvun (jos olemassa) käänteisluvulla. Tämän jälkeen jokainen rivi, joka ei kokostu kokonaan nollista, alkaa ykkösellä.
2. Jos rivin i aloittavan ykkösen yläpuolella on $d \neq 0$ rivillä j , lisää rivi i riviin $j - d$:llä kerrottuna. Toista tätä uudelleen niin kauan rivien alkuykkösten yläpuolelta löytyy nollasta poikkeavia alkioita.

Gaussin menetelmä saattaa siis matriisin porrasmuotoon alkeisoperaatioita käyttämällä. Täydentämällä tätä yllä kuvattua menetelmällä, joka saattaa matriisin redusoituun porrasmuotoon, saadaan niin kutsuttu *Gaussin-Jordanin* eliminointimenetelmä. Se on valmiiksi ohjelmoitu useimpiin tavallisiin matematiikkaohjelmiin.

Taustatietoa

(Johann) Carl Friedrich Gauss (Gauß) (latin. *Carolus Fridericus Gauss* 1777–1855) oli saksalainen matemaatikko, jota Arkhimedeen ja Newtonin ohella pidetään yhtenä maailmanhistorian merkittävimpänä matematiikan kehittäjänä. Gaussia pidetään mm. ensimmäisen *algebran peruslauseen* aukottoman todistuksen esittäjänä. Gauss saavutti huomattavia tuloksia suurella osalla nykymatematiikan aloista.

(kuva: Wikimedia Commons)

Syötetään esimerkin 111 augmentoitu matriisi **Matlab**-ohjelmistoon:

```
>> A=[2,-1,3,4;3,2,1,6;-5,1,-2,3]
```

Komento `format rat` asettaa Matlabin laskemaan desimaaliesitysten sijaan murtoluvuilla ja `rref(A)` muuntaa matriisin A redusoituun porrasmuotoon:

```
>> rref(A)
```

```
ans =
```

```

      1      0      0     -5/4
      0      1      0     13/4
      0      0      1     13/4
```

```
>>
```

Lause 42. *Redusoidut porrasmatriisit ovat riviekvivalentteja keskenään vain silloin kun ne ovat samat.*

Todistus. Siivutetaan. Todistus on monivaiheinen, mutta ei erityisen syvälinen.

Edellisestä lauseesta seuraa, että jokainen matriisi A on riviekvivalentti *tarkalleen yhden* redusoidun porrasmatriisin kanssa.

Määritelmän perusteella on selvää, että matriisin aste on korkeintaan sen rivien määrä, mutta ei myöskään ole vaikeaa nähdä, että matriisin astetta rajoittaa lisäksi sarakkeiden määrä, toisin sanoen $m \times n$ -matriisille pätee $r(A) \leq \min\{m, n\}$.

7.3 Ratkaisujoukon systemaattinen esittäminen

Tarkastellaan lähinnä esimerkkien valossa miten redusoidusta porrasmatriisista saadaan *kaikki* yhtälöryhmän ratkaisut. Ensinnäkin voidaan todeta, että ratkaisujen puuttuminen havaitaan, mikäli (augmentoitu) matriisi redusoituu esimerkissä 112 olevaan muotoon, siis muotoon, jossa esiintyy yhtälö $0 = c \neq 0$.

Ratkaisujen systemaattinen esittäminen perustuu yksinkertaisesti siihen, että redusoidussa porrasmuodossa olevan yhtälöryhmän ”portaan aloittavat” muuttujat esitetään muiden avulla, kun taas muut muuttujat ”jäävät ratkaisuun”.

Esimerkki 114. Olkoon augmentoidusta yhtälöryhmän matriisista saatu redusoitua matriisi

$$\begin{pmatrix} 1 & 0 & 2 & 0 & 4 \\ 0 & 1 & -1 & 0 & -3 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}.$$

Tätä matriisia vastaa yhtälöryhmä

$$\begin{cases} x_1 + 2x_3 = 4 \\ x_2 - x_3 = -3 \\ x_4 = -1 \end{cases},$$

jonka kaikki ratkaisut (x_1, x_2, x_3, x_4) voidaan suoraviivaisesti lukea redusoidusta porrasmuodosta: Ensimmäisen yhtälön perusteella $x_1 = -2x_3 + 4$, toisen yhtälön perusteella $x_2 = x_3 - 3$, ja kolmannen yhtälön perusteella $x_4 = -1$. Täten siis yhtälöryhmän yleinen ratkaisu on muotoa $(x_1, x_2, x_3, x_4) = (-2x_3 + 4, x_3 - 3, x_3, -1) = (-2x_3, x_3, x_3, 0) + (4, -3, 0, -1) = x_3(-2, 1, 1, 0) + (4, -3, 0, -1)$, missä x_3 on mikä hyvänsä reaaliluku.

Esimerkki 115. Tarkastellaan toisena esimerkkinä redusoitua (augmentoitua) porrasmatriisia

$$\begin{pmatrix} 1 & 0 & 0 & -4 & -6 & -2 \\ 0 & 1 & 0 & 3 & 0 & 3 \\ 0 & 0 & 1 & 1 & 2 & 7 \end{pmatrix},$$

jota vastaava yhtälöryhmä on

$$\begin{cases} x_1 - 4x_4 - 6x_5 = -2 \\ x_2 + 3x_4 = 3 \\ x_3 + x_4 + 2x_5 = 7 \end{cases}$$

Nyt muuttujat x_1 , x_2 ja x_3 ovat kukin ”portaansa aloittavia” muuttujia, joten ne esitetään muiden avulla. Ensimmäisen yhtälön perusteella $x_1 = 4x_4 + 6x_5 - 2$, toisen perusteella $x_2 = -3x_4 + 3$, ja kolmannen perusteella $x_3 = -x_4 - 2x_5 + 7$. Täten siis yleinen ratkaisu $(x_1, x_2, x_3, x_4, x_5)$ voidaan kirjoittaa muodossa

$$\begin{aligned} (x_1, x_2, x_3, x_4, x_5) &= (4x_4 + 6x_5 - 2, -3x_4 + 3, -x_4 - 2x_5 + 7, x_4, x_5) \\ &= (4x_4 + 6x_5, -3x_4, -x_4 - 2x_5, x_4, x_5) + (-2, 3, 7, 0, 0) \\ &= (4x_4, -3x_4, -x_4, x_4, 0) + (6x_5, 0, -2x_5, 0, x_5) + (-2, 3, 7, 0, 0) \\ &= x_4(4, -3, -1, 1, 0) + x_5(6, 0, -2, 0, 1) + (-2, 3, 7, 0, 0), \end{aligned}$$

missä x_4 ja x_5 ovat mitä hyvänsä reaalilukuja.

Esimerkissä 114 yleinen ratkaisu saatiin muodossa $x_3(-2, 1, 1, 0) + (4, -3, 0, -1)$, ja esimerkin 115 tapauksessa yleinen ratkaisu on muotoa $x_4(4, -3, -1, 1, 0) + x_5(6, 0, -2, 0, 1) + (-2, 3, 7, 0, 0)$. Kummassakin tapauksessa ratkaisu voidaan esittää sellaisessa muodossa, jossa äärettömään vektorijoukkoon lisätään yksittäinen vektori: Esimerkin 114 tapauksessa kyseinen yksittäinen vektori on $(4, -3, 0, -1)$ ja esimerkin $(2, 3, 7, 0, 0)$. Lisättyä yksittäistä vektoria kutsutaan *yksityisratkaisuksi*.

Kuten aiemmin huomattiin, esimerkin 115 ratkaisut ovat muotoa

$$t(4, -3, -1, 1, 0) + s(6, 0, -2, 0, 1) + (-2, 3, 7, 0, 0),$$

missä $t, s \in \mathbb{R}$. Voidaan lisäksi huomata, että esimerkin 115 ääretön ratkaisujoukko $\{t(4, -3, -1, 1, 0) + s(6, 0, -2, 0, 1) \mid s, t \in \mathbb{R}\}$ on ns. *homogenisoitun* yhtälöryhmän

$$\begin{cases} x_1 - 4x_4 - 6x_5 = 0 \\ x_2 + 3x_4 = 0 \\ x_3 + x_4 + 2x_5 = 0 \end{cases}$$

ratkaisujoukko. Tämänkaltainen jäsentely pätee yleisestikin. Seuraava lause onkin edellisten esimerkkien yleistys.

Lause 43. Jos A on lineaarisen yhtälöryhmän $m \times n$ -matriisi (ei siis augmentoitu), jonka aste on r , voidaan ryhmän ratkaisut esittää muodossa $\vec{x} = x_{r+1}\vec{c}_{r+1} + \dots + x_n\vec{c}_n + \vec{c}$, missä $\vec{c}_i, \vec{c} \in \mathbb{R}^n$ ovat vakiovektoreita ja $x_i \in \mathbb{R}$. Kaikilla kertoimien x_i valinnoilla $x_{r+1}\vec{c}_{r+1} + \dots + x_n\vec{c}_n$ on alkuperäisestä yhtälöryhmästä saatavan homogeenisen yhtälöryhmän ratkaisu.

Todistus (Todistuksen idea). Muistetaan, että aste r merkitsee A :sta saatavan redusoidun porrasmatriisin P porraskukua (määritelmä ??), ja että jokainen lineaarinen yhtälöryhmä on ekvivalentti sellaisen yhtälöryhmän kanssa jonka matriisi on redusoitua porrasmuotoa. Kuten esimerkeissä 114 ja 115 nähtiin, voidaan kunkin portaan aloittava muuttuja $x_1, \dots, x_r$ esittää muiden muuttujien $x_{r+1}, \dots, x_n$ avulla (muuttujat voidaan numeroida uudelleen siten, että nimenomaan $x_1, \dots, x_r$ aloittavat portaan). Samoin kuin esimerkeissä 114 ja 115, voidaan ratkaisuvektori $\vec{x}$ (jossa siis esiintyy $n - r$ muuttujaa $x_{r+1}, \dots, x_n$) hajottaa ensin muotoon $\vec{x} = \vec{x}_{r+1} + \dots + \vec{x}_n + \vec{c}$, missä vektorissa $\vec{x}_i$ ainoa esiintyvä muuttuja on x_i ja $\vec{c}$ on vakiovektori. Tämän jälkeen muuttuja x_i voidaan ottaa vektorin $\vec{x}_i$ kertoimeksi, joten $\vec{x}_i = x_i \vec{c}_i$, missä $\vec{c}_i \in \mathbb{R}^n$ on vakiovektori. Näin saadaan haluttu esitys $\vec{x} = x_{r+1} \vec{c}_{r+1} + \dots + x_n \vec{c}_n + \vec{c}$. Jälkimmäinen väite seuraa suoraan siitä, että ratkaisussa esiintyvä vakiovektori $\vec{c}$ on nolla tarkalleen silloin kun yhtälöryhmän oikean puolen luvut ovat nollia.

Edellinen lause voidaan ilmaista myös seuraavassa muodossa:

Lause 44. *Linearisen yhtälöryhmän kaikki ratkaisut ovat muotoa $\vec{x} = \vec{x}_1 + \vec{c}$, missä $\vec{c}$ on jokin yksittäinen ratkaisu ja $\vec{x}_1$ on mikä hyvänsä alkuperäisestä ryhmästä saatavan homogeenisen ryhmän ratkaisu.*

Voidaan huomata, että esimerkin 114 yhtälöryhmässä homogenisoidun ryhmän ratkaisut saadaan yhden vektorin skalaarimonikertoina $\{t(-2, 1, 1, 0) \mid t \in \mathbb{R}\}$, kun taas yhtälöryhmää 115 vastaavan homogeenisen ryhmän ratkaisut ovat muotoa $\{t(4, -3, -1, 1, 0) + s(6, 0, -2, 0, 1) \mid s, t \in \mathbb{R}\}$.

Ensiksi mainitussa yhtälöryhmässä 114 on neljä tuntematonta ja kolme yhtälöä. Redusoidusta porrasmatriisista nähdään, että sen aste on 3. Vastaavasti yhtälöryhmässä 115 on viisi tuntematonta ja kolme yhtälöä, redusoidun porrasmatriisin asteen ollessa 3.

Etsittäessä ratkaisuja näille esimerkeille olemme huomanneet, että ratkaisujen joukko homogenisoidulle yhtälöryhmälle voidaan esimerkin 114 tapauksessa ilmoittaa $4 - 3 = 1$ vektorin avulla, ja esimerkin 115 tapauksessa $5 - 3 = 2$ vektorin avulla. Nämä lukumäärät eivät ole sattumaa, vaan vastaava yleinen sääntö pätee:

Huomautus 36. Lauseen 43 mukaan homogeenisella yhtälöryhmällä (m yhtälöä ja n tuntematonta) on $n - r(A)$ (toisistaan) riippumatonta ratkaisua (käsite täsmennetään osassa Insinöörimatematiikka D) $\vec{c}_{r+1}, \dots, \vec{c}_n$, joiden avulla kaikki muut ratkaisut voidaan esittää.

Esimerkin 114 kerroinmatriisi (ei augmentoitu versio) on 3×4 -matriisi, jonka aste on 3; täten kyseistä ryhmää vastaavalla homogeenisella ryhmällä $4 - 1 = 1$ riippumatonta ratkaisua. Vastaavasti esimerkin 115 ei-augmentoitu matriisi on 3×5 -matriisi, jonka porraskuku on 3; täten ryhmää vastaavalla homogeenisella ryhmällä on $5 - 3 = 2$ riippumatonta ratkaisua.

Luvun oleellisia asioita:

- Peruskäsitteet matriiseista
- Gaussin-Jordanin menetelmä yhtälöryhmän ratkaisemiseksi ja ratkaisun esittäminen systemaattisesti.

Luku 8

Osamurtohajotelmat

Osamurtohajotelmat ovat rationaalilausekkeiden summamuotoisia esitystapoja, joille on tyypillistä, että osoittajien aste on nimittäjien astetta pienempi. Tämä on eduksi monissa sovelluksissa, kuten Insinöörimatematiikka B:ssä esiintyvien määräämättömien integraalien laskemisessa ja C:ssä esiintyvien integraalimuunnosten kääntämisessä.

Esimerkki 116. Tyypillinen osamurtohajotelma on muotoa

$$2x + 1 + \frac{1}{x+2} - \frac{2}{x+1}.$$

Suoralla laskulla saadaan ylläoleva lauseke muotoon

$$\frac{2x^3 + 7x^2 + 6x - 1}{x^2 + 3x + 2},$$

mutta keskeisin tehtävä osamurtohajotelmien yhteydessä onkin yleensä selvittää miten jälkimmäisestä muodosta saadaan ensimmäinen. Tällöin joudutaan aluksi perehtymään polynomien tekijöihinjakoon.

8.1 Polynomien tekijöihinjaosta

Kahden luvun jakolasku voidaan aina suorittaa koulukurssilta tutussa jakokulmassa ja saada tulos: 25 jaettuna luvulla 3 tuottaa osamääräksi 8 ja jakojäännökseksi jää 1. Symbolisesti merkittynä tämä voidaan kirjoittaa seuraavalla tavalla: $\frac{25}{3} = 3 + \frac{1}{3}$ tai $25 = 3 \cdot 8 + 1$. Yhden muuttujan polynomien jakolaskussa voidaan havaita täsmälleen sama ilmiö, ja jakokulman soveltaminenkin tapahtuu samoin kuin luvuille:

Esimerkki 117. Lasketaan $\frac{x^4+3x^2-x+1}{x^2+3x+1}$ jakokulmassa.

$$\begin{array}{r} x^2 - 3x + 11 \\ x^2 + 3x + 1 \overline{) \begin{array}{r} x^4 + 3x^2 - x + 1 \\ x^4 + 3x^3 + x^2 \\ \hline -3x^3 + 2x^2 - x + 1 \\ -3x^3 - 9x^2 - 3x \\ \hline 11x^2 + 2x + 1 \\ 11x^2 + 33x + 11 \\ \hline -31x - 10 \end{array}} \end{array}$$

Osamäärä on $x^2 - 3x + 11$ ja jakojäännös $-31x - 10$, mikä merkitsee sitä, että

$$\frac{x^4 + 3x^2 - x + 1}{x^2 + 3x + 1} = x^2 - 3x + 11 + \frac{-31x - 10}{x^2 + 3x + 1}.$$

Tässä pykälässä tarkasteltavat polynomit ovat joko reaali- tai kompleksilukukertoimisia. Reaalikertoimisten polynomien joukosta käytetään merkintää $\mathbb{R}[x]$ ja kompleksikertoimisten polynomien

joukosta $\mathbb{C}[x]$ (jos polynomin muuttuja on z , on myös joukon merkintä $\mathbb{C}[z]$) Polynomin p asteesta käytetään merkintää $\deg(p)$ ja polynomien tulolle pätee $\deg(pq) = \deg(p) + \deg(q)$. Nollapolynomin asteesta käytetään symbolista merkintää $\deg(0) = -\infty$.

Esimerkki 118. $x^2 - 1 = (x+1)(x-1)$, joten $x^2 - 1$ on jaollinen polynomeilla $x-1$ ja $x+1$. Toisaalta $x^2 - 1 = 2(x+1)\frac{1}{2}(x-1)$, joten $x^2 - 1$ on jaollinen myös polynomeilla $2(x+1)$ ja $\frac{1}{2}(x-1)$.

Itse asiassa, jos q on jaollinen polynomilla p , siis $q = pr$, ja $c \neq 0$ on vakio, voidaan kirjoittaa myös $q = cp \cdot c^{-1}r$, joten q on jaollinen myös polynomilla cp . Sama idea ei toimi, jos c on polynomi, jonka aste on suurempi kuin 0, sillä tällöin c^{-1} ei ole polynomi.

Kuten edellisestä esimerkistä huomataan, polynomien jaollisuuskäsitteissä p ja cp , missä c on nollasta poikkeava vakio, ovat samankaltaisessa asemassa.

Esimerkki 119. Koska $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$, on ensimmäisen asteen polynomin $ax + b$ tekijöistä toinen välttämättä vakio. Täten siis ensimmäisen asteen polynomin ainoa vakiosta poikkeava tekijä on polynomi itse.

Jos polynomi d toteuttaa ylläolevat ehdot, niin tällöin myös mikä hyvänsä d :stä nollasta poikkeavalla vakiolla kertomalla saatava polynomi toteuttaa myös ne, joten polynomeille $\text{sy}(p, q)$ ei ole yksikäsitteisesti määritetty. Voidaan kuitenkin todistaa, että $\mathbb{R}[x]$:n ja $\mathbb{C}[x]$:n polynomeille $\text{sy}(p, q)$ määrittyy *vakiotekijää vaille* yksikäsitteisesti, siis jos d_1 ja d_2 molemmat toteuttavat sy :n määritelmän ehdot, niin d_1 ja d_2 saadaan toisistaan nollasta poikkeavalla vakiolla kertomalla.

Esimerkki 120. $\text{sy}(x-1, x+1) = 1$, koska esimerkin 119 mukaan $x-1$ ja $x+1$ eivät voi jakaa toisiaan. Edellisten esimerkkien valossa voidaan toisaalta yhtä hyvin kirjoittaa $\text{sy}(x-1, x+1) = c$, missä $c \neq 0$ on mikä hyvänsä nollasta poikkeava vakio, mutta tapana on käyttää merkintää $\text{sy}(x-1, x+1) = 1$.

Polynomien suurimman yhteisen tekijän löytämiseksi voidaan käyttää samanlaista menettelyä kuin kokonaislukujen tapauksessa. Prosessi tunnetaan nimellä *Eukleideen algoritmi* ja on varhaisin tunnettu algoritmien menetelmä.

Eukleideen algoritmi polynomien sy :n löytämiseksi

Syöte: Polynomit p ja q

Tuloste: $\text{sy}(p, q)$

1. Jos $\deg(p) < \deg(q)$, vaihdetaan merkintöjä $p \leftrightarrow q$, minkä jälkeen $\deg(p) \geq \deg(q)$.
2. Jos $q = 0$, annetaan vastaus $\text{sy}(p, q) = p$ ja päätetään prosessi. Jos $\deg(q) = 0$, annetaan vastaus $\text{sy}(p, q) = 1$ ja päätetään prosessi.
3. Jos $\deg(q) \geq 1$, suoritetaan jakolasku $p = aq + r$ (a on osamäärä ja r jakojäännös, $\deg(r) < \deg(q)$). Tällöin $\text{sy}(p, q) = \text{sy}(q, r)$, ja jälkimmäinen sy määritetään tätä samaa menetelmää käyttäen.

Esimerkki 121. Lasketaan $\text{sy}(x^3 - 1, x^2 - 1)$. Ensimmäinen jakolasku antaa

$$x^3 - 1 = x(x^2 - 1) + x - 1,$$

siis osamäärä on x ja jakojäännös $x - 1$. Tällöin $\text{sy}(x^3 - 1, x^2 - 1) = \text{sy}(x^2 - 1, x - 1)$, minkä selvittämiseksi suoritetaan uusi jakolasku:

$$x^2 - 1 = (x + 1)(x - 1),$$

missä osamäärä on $x + 1$ ja jakojäännös 0. Tällöin $\text{sy}(x^2 - 1, x - 1) = \text{sy}(x - 1, 0)$, ja vastaus $x - 1$ saadaan suoraan menetelmän toisesta vaiheesta.

Esimerkki 122. Lasketaan $\text{sy}(x^3 - 1, x^3 + 1)$. Ensimmäinen jakolasku antaa

$$x^3 - 1 = 1 \cdot (x^3 + 1) - 2,$$

missä siis 1 on osamäärä ja -2 jakojäännös. Tällöin siis $\text{sy}(x^3 - 1, x^3 + 1) = \text{sy}(x^3 + 1, 2) = 1$.

Esimerkki 123. Polynomi $x - 1$ on jaoton, koska esimerkin 119 mukaan sen kaikki tekijät ovat muotoa $c(x - 1)$, missä $c \neq 0$ tai vakioita. Polynomi $x^2 - 1$ ei ole jaoton, koska sillä on tekijä $x - 1$, joka ei ole vakio, ja josta alkuperäistä polynomia ei saada vakiolla kertomalla.

Polynomin jaollisuus voi kuitenkin riippua siitä, missä joukossa tekijöiden halutaan olevan. On mahdollista, että sama polynomi on jaoton joukossa $\mathbb{R}[x]$, mutta jaollinen joukossa $\mathbb{C}[x]$.

Esimerkki 124. Tarkastellaan, onko $x^2 + 1$ jaollinen joukossa $\mathbb{R}[x]$. Jos näin olisi, pitäisi sillä olla ensimmäisen asteen tekijä $x + a \in \mathbb{R}[x]$ (johtava kerroin voidaan olettaa ykköseksi). Tällöin pitäisi olla myös toinen tekijä $x + b \in \mathbb{R}[x]$, joille pätee

$$x^2 + 1 = (x + a)(x + b) = x^2 + (a + b)x + ab,$$

siis $a + b = 0$ ja $ab = 1$. Edellisestä yhtälöstä saadaan $b = -a$ ja sijoittamalla tämä jälkimmäiseen $a^2 = -1$, mikä ei toteudu millekään reaaliluvulle a , mutta toteutuu kompleksiluvulla $a = i$. Polynomi $x^2 + 1$ on siis jaoton joukossa $\mathbb{R}[x]$, mutta jaollinen joukossa $\mathbb{C}[x]$: $x^2 + 1 = (x - i)(x + i)$.

Itse asiassa polynomin $x^2 + 1$ jaottomuus yli reaalilukujen juontaa juurensa yleisemmästä periaatteesta, jonka mukaan polynomin ensimmäisen asteen tekijät ja nollakohdat vastaavat toisiaan täydellisesti. Tämän ilmaisee kompleksilukujen yhteydessä esitetty lause 38:

Jos $p(a) = 0$, niin $p(x)$ on jaollinen polynomilla $x - a$.

Lauseen 38 mukaan siis polynomin p hajottaminen ensimmäisen asteen tekijöihin on yhtä hankala tehtävä kuin p :n nollakohtien löytäminen. Nollakohtia ei aina voida löytää algebrallisesti, vaikka nollakohtien *olemassaolo* voidaan taata Algebran peruslauseen 37 mukaan.

Huomautuksen 6.2 mukaan polynomille $p(z)$ saadaan lopulta esitys

$$p(z) = (z - z_1) \dots (z - z_n) p_n(z),$$

missä $p_n(z) = c$ on vakio ja siis

$$p(z) = c(z - z_1) \dots (z - z_n) \quad (8.1)$$

Esitys (8.1) ratkaisee täydellisesti kysymyksen siitä, mitkä ovat kompleksikertoimisen polynomin jaottomat tekijät:

Jokainen kompleksikertoiminen polynomi jakautuu ensimmäisen asteen tekijöihin $z - z_k$, joille lisäksi pätee $\text{sy}(z - z_k, z - z_l) = 1$, jos $z_k \neq z_l$ ja $\text{sy}(z - z_k, z - z_k) = z - z_k$.

Tämä ei pidä paikkansa reaaliluvuille, kuten nähtiin esimerkissä 124: polynomi $x^2 + 1$ on jaoton joukossa $\mathbb{R}[x]$. Joukon $\mathbb{C}[x]$ polynomien jaollisuudesta voidaan kuitenkin johtaa myös tuloksia reaalikertoimisten polynomien jaollisuuteen.

Lause 45. Jos polynomilla $p \in \mathbb{R}[x]$ on nollakohta $w \in \mathbb{C}$, niin myös kompleksikonjugaatti $\bar{w}$ on polynomin p nollakohta.

Todistus. Merkitään $p(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$, missä $c_i \in \mathbb{R}$. Tällöin suoraan sijoittamalla saadaan $p(\bar{w}) = c_n \bar{w}^n + c_{n-1} \bar{w}^{n-1} + \dots + c_1 \bar{w} + c_0$. Koska jokainen kerroin c_i on reaalinen, on $\bar{c_i} = c_i$, mistä seuraa, että $p(\bar{w}) = \overline{p(w)} = 0$.

Edellisen lauseen mukaan *reaalikertoimisen* polynomin kompleksiset nollakohdat esiintyvät pareittain: Jos w on nollakohta (mitä kutsutaan myös *juureksi*), niin myös w :n kompleksikonjugaatti $\bar{w}$ on. Tarkastellaan siis minkälainen on reaalikertoimisen polynomin $p(x)$ algebran peruslauseesta seuraava hajotelma:

$$p(x) = c(x - x_1) \dots (x - x_k)(x - w_1)(x - \bar{w}_1) \dots (x - w_l)(x - \bar{w}_l), \quad (8.2)$$

missä $x_1, \dots, x_k$ ovat polynomin p reaaliset juuret ja $w_1, \bar{w}_1, \dots, w_l, \bar{w}_l$ sen kompleksiset juuret. Tarkasteltaessa paria $(x - w_i), (x - \bar{w}_i)$ huomataan, että polynomilla

$$(x - w_i)(x - \bar{w}_i) = x^2 - (w_i + \bar{w}_i)x + w_i \bar{w}_i$$

on reaaliset kertoimet. Tämä nähdään siitä, että $\overline{w_i + \bar{w}_i} = \bar{w}_i + w_i$ ja $\overline{w_i \bar{w}_i} = \bar{w}_i w_i$. Tällöin siis merkitsemällä $u_i = w_i + \bar{w}_i$ ja $v_i = w_i \bar{w}_i$ saadaan

$$(x - w_i)(x - \bar{w}_i) = x^2 + u_i x + v_i,$$

jolloin myös polynomille p saadaan reaalikertoiminen hajotelma kertomalla kukin tekijä $x - w_i$ konjugaattitekijänsä $x - \bar{w}_i$ kanssa:

$$p(x) = c(x - x_1) \dots (x - x_k)(x^2 + u_1 x + v_1) \dots (x^2 + u_l x + v_l). \quad (8.3)$$

On lisäksi huomattava, että kukin tekijä $x^2 + u_i x + v_i = (x - w_i)(x - \bar{w}_i)$ on jaoton $\mathbb{R}[x]$:ssä, sillä jaollisuudesta yli $\mathbb{R}$:n seuraisi reaalinen nollakohta. Edelleen voidaan todeta, että esityksessä (8.3) $\text{synt}(x - x_i, x - x_j) = 1$, jos $x_i \neq x_j$ ja $\text{synt}(x^2 + u_i x + v_i, x^2 + u_j x + v_j) = \text{synt}((x - w_i)(x - \bar{w}_i), (x - w_j)(x - \bar{w}_j)) = 1$, jos $w_i \neq w_j$. Yhteenvetona voidaan siis mainita:

Jokainen reaalkertoiminen polynomi jakautuu korkeintaan astetta kaksi oleviin jaottomiin tekijöihin $\mathbb{R}[x]$:ssä.

8.2 Menetelmiä tekijöihinjakoon

Lauseen 38 perusteella polynomin p ensimmäisen asteen tekijä voidaan löytää polynomin p nollakohdan avulla.

Esimerkki 125. Jaetaan polynomi $x^2 + 3x + 1$ tekijöihin. Nollakohdat ovat $\frac{-3 \pm \sqrt{5}}{2}$, joten

$$x^2 + 3x + 1 = \left(x - \frac{-3 + \sqrt{5}}{2}\right) \left(x - \frac{-3 - \sqrt{5}}{2}\right)$$

Yli neljännen asteen polynomeille ei kuitenkaan ole välttämättä olemassa algebrallista ratkaisua, siis sellaista, jossa nollakohta voitaisiin esittää polynomin kertoimista saatavana lausekkeena yhteen-, kerto-, vähennys- ja jakolaskun sekä juurenoton avulla. Toisaalta taas rationaalisia nollakohtia voidaan etsiä kokeilemalla seuraavaan lauseeseen perustuen:

Lause 46. *Olkoon*

$$p(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$$

kokonaislukukertoiminen polynomi. Jos $p(x)$:llä on rationaalinen juuri $r = \frac{p}{q}$, missä $\text{synt}(p, q) = 1$, niin silloin osoittaja p jakaa vakiokertoimen c_0 ja nimittäjä q korkeimman asteen kertoimen c_n .

Todistus. Koska $r = \frac{p}{q}$ on nollakohta, on

$$0 = c_n \left(\frac{p}{q}\right)^n + c_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + c_1 \frac{p}{q} + c_0,$$

ja kertomalla yhtälö puolittain luvulla q^n saadaan

$$0 = c_n p^n + c_{n-1} p^{n-1} q + \dots + c_1 p q^{n-1} + c_0 q^n, \quad (8.4)$$

ja $c_0 q^n$ toiselle puolelle siirtämällä saadaan

$$-c_0 q^n = c_n p^n + c_{n-1} p^{n-1} q + \dots + c_1 p q^{n-1}.$$

Tästä nähdään, että p jakaa luvun $c_0 q^n$. Koska $\text{synt}(p, q) = 1$, ei p voi jakaa lukua q^n , siis p jakaa luvun c_0 . Siirtämällä yhtälössä (8.4) $c_n p^n$ toiselle puolelle nähdään samalla tavalla, että q jakaa luvun c_n .

Esimerkki 126. Olkoon $p(x) = 6x^3 - 37x^2 + 72x - 45$. Jos $p(x)$:llä on rationaalijuuri $r = \frac{p}{q}$, on $q \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ (luvun 6 tekijät) ja $p \in \{\pm 1, \pm 3, \pm 5, \pm 9, \pm 15, \pm 45\}$ (luvun 45 tekijät). Kokeilemalla eri vaihtoehtoja havaitaan, että esim $p(3) = 0$, jolloin siis $x - 3$ jakaa polynomin $p(x)$. Jakolaskulla saadaan $p(x) = (x - 3)(6x^2 - 19x + 15)$. Edelleen polynomin $p_1(x) = 6x^2 - 19x + 15$ mahdollisen rationaalijuuren osoittaja jakaa luvun 15 ja nimittäjä luvun 6. Kokeilemalla saadaan tälle nollakohdaksi $x = \frac{3}{2}$, jolloin siis $p_1(x)$ on jaollinen polynomilla $x - \frac{3}{2}$. Jakolaskulla saadaan $p_1(x) = (x - \frac{3}{2})(6x - 10) = 6(x - \frac{3}{2})(x - \frac{5}{3})$, jolloin alkuperäiselle polynomille $p(x)$ saadaan tekijöihinjako

$$p(x) = 6(x - \frac{3}{2})(x - \frac{5}{3})(x - 3).$$

Esimerkki 127. Myös erilaisia ryhmittelyjä on toisinaan mahdollista käyttää tekijöiden löytämiseen:

$$\begin{aligned} & x^4 - 2x^3 - 2x^2 + 5x - 2 \\ &= x^4 - 2x^3 - 2x^2 + 4x + x - 2 \\ &= x^3(x - 2) - 2x(x - 2) + x - 2 \\ &= (x^3 - 2x + 1)(x - 2) \end{aligned}$$

ja edelleen

$$\begin{aligned} x^3 - 2x + 1 &= x^3 - x^2 + x^2 - x - x + 1 \\ &= x^2(x - 1) + x(x - 1) - (x - 1) \\ &= (x^2 + x - 1)(x - 1), \end{aligned}$$

mutta sopivia ryhmittelyjä on yleensä hankala löytää.

Esimerkki 128.

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

Esimerkki 129. Joitakin tekijöihinjakoja on myös valmiiksi taulukoituna (esim. MAOL).

$$x^6 - 1 = (x^3)^2 - 1^2 = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1).$$

polynomeilla $x^2 + x + 1$ ja $x^2 - x + 1$ ei ole reaalisia nollakohtia, joten ne ovat jaottomia $\mathbb{R}[x]$:ssä. Joukossa $\mathbb{C}[x]$ ne sen sijaan jakautuvat tekijöihin: polynomilla $x^2 + x + 1$ on nollakohdat $\frac{-1 \pm i\sqrt{3}}{2}$, joten

$$x^2 + x + 1 = \left(x - \frac{-1 + i\sqrt{3}}{2}\right)\left(x - \frac{-1 - i\sqrt{3}}{2}\right)$$

ja samalla tavalla

$$x^2 - x + 1 = \left(x - \frac{1 + i\sqrt{3}}{2}\right)\left(x - \frac{1 - i\sqrt{3}}{2}\right).$$

8.3 Yleinen osamurtohajotelma

Osamurtohajotelmia etsittäessä oletetaan ensiksi, että rationaalilausekkeessa $\frac{p(x)}{q(x)}$ nimittäjä on korkeampaa astetta kuin osoittaja, siis $\deg(p) < \deg(q)$. Jos tämä ei toteudu, on ensiksi suoritettava jakolasku:

$$\frac{p(x)}{q(x)} = a(x) + \frac{p_1(x)}{q(x)},$$

jossa $a(x)$ on osamäärä ja $p_1(x)$ jakojäännös, jonka aste on pienempi kuin jakajan aste. Tämän jälkeen etsitään osamurtohajotelma rationaalilausekkeelle $\frac{p_1(x)}{q(x)}$. Tähän puolestaan sovelletaan kahta strategiaa, jotka esitellään seuraavissa lauseissa.

Lause 47 (Nimittäjän tekijöillä syt 1). Olkoon $f(x) = \frac{p(x)}{q(x)}$ kahden polynomin osamäärä, $\deg(p) < \deg(q)$ ja

$$q(x) = q_1(x) \cdot q_2(x),$$

sellainen nimittäjän hajotelma, että $\text{syt}(q_1(x), q_2(x)) = 1$. Silloin on olemassa sellaiset (yksikäsitteiset) polynomit $p_1(x)$ ja $p_2(x)$, että

$$f(x) = \frac{p_1(x)}{q_1(x)} + \frac{p_2(x)}{q_2(x)}, \quad (8.5)$$

$$\text{ja } \deg(p_i) < \deg(q_i).$$

Edellisessä lauseen polynomit $p_1(x)$ ja $p_2(x)$ pitää yleensä etsiä määräämättömien kertoimien avulla.

Esimerkki 130.

$$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1),$$

ja helposti todetaan, että $\text{sy}(x^2 + x + 1, x^2 - x + 1) = 1$. Tällöin

$$\frac{1}{x^4 + x^2 + 1} = \frac{A_1 + B_1x}{x^2 + x + 1} + \frac{A_2 + B_2x}{x^2 - x + 1},$$

mistä kertoimet A_1, B_1, A_2 ja B_2 saadaan seuraavasti: Aluksi lavennetaan oikean puolen termit samannimisiksi ja lasketaan yhteen, jolloin saadaan

$$\begin{aligned} & \frac{1}{x^4 + x^2 + 1} \\ &= \frac{A_1 + A_2 + (-A_1 + B_1 + A_2 + B_2)x + (A_1 - B_1 + A_2 + B_2)x^2 + (B_1 + B_2)x^3}{(x^2 + x + 1)(x^2 - x + 1)}. \end{aligned}$$

Kertoimet A_1, B_1, A_2 ja B_2 saadaan siis ratkaisemalla yhtälöryhmä

$$\begin{cases} A_1 + A_2 = 1 \\ -A_1 + B_1 + A_2 + B_2 = 0 \\ A_1 - B_1 + A_2 + B_2 = 0 \\ B_1 + B_2 = 0 \end{cases}.$$

Ryhmän augmentoitu kerroinmatriisi

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ -1 & 1 & 1 & 1 & 0 \\ 1 & -1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Saadaan Gaussin-Jordanin eliminointimenetelmällä muotoon

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 1 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 1 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 1 & -\frac{1}{2} \end{pmatrix},$$

joten $A_1 = A_2 = B_1 = \frac{1}{2}$ ja $B_2 = -\frac{1}{2}$ ja tulokseksi saadaan

$$\frac{1}{x^4 + x^2 + 1} = \frac{\frac{1}{2}(1+x)}{x^2 + x + 1} + \frac{\frac{1}{2}(1-x)}{x^2 - x + 1}.$$

Esimerkki 131. Esimerkin 122 mukaan $\text{sy}(x^3 - 1, x^3 + 1) = 1$, joten rationaalifunktio $f(x) = \frac{1}{x^6 - 1}$ voidaan hajottaa osamurtoihin

$$\frac{1}{x^6 - 1} = \frac{p_1(x)}{x^3 - 1} + \frac{p_2(x)}{x^3 + 1},$$

missä polynomien p_1 ja p_2 asteet ovat korkeintaan 2. Polynomit p_1 ja p_2 saadaan määräämättömien kertoimien menetelmällä kuten edellisessäkin esimerkissä ja hajotelma on

$$\frac{1}{x^6 - 1} = \frac{\frac{1}{2}}{x^3 - 1} + \frac{-\frac{1}{2}}{x^3 + 1}.$$

On huomattava, että lauseessa (47) ei oleteta nimittäjän tekijöiden $q_1(x), \dots, q_k(x)$ olevan jaottomia, ainoastaan, että niillä ei ole yhteisiä tekijöitä. Esimerkin 131 tilanne onkin juuri tällainen:

$x^3 - 1$ on jaollinen $x - 1$:llä ja $x^3 + 1$ jaollinen $x + 1$:llä. Niinpä esimerkin 131 osamurtohajotelmaa on mahdollista jatkaa edelleen.

Jos nimittäjässä esiintyy jaottoman polynomin potenssi, ei nimittäjää voida jakaa tekijöihin, joiden syt on 1. Tällöin voidaan turvautua seuraavaan lauseeseen.

Lause 48 (Nimittäjän tekijöillä syt > 1). Olkoon $\deg(r) < \deg(q^n)$. Tällöin on olemassa polynomit $r_1, \dots, r_n$, joille pätee $\deg(r_i) < \deg(q)$ ja

$$\frac{r(x)}{q(x)^n} = \frac{r_1(x)}{q(x)} + \frac{r_2(x)}{q(x)^2} + \dots + \frac{r_n(x)}{q(x)^n}.$$

Esimerkki 132. Etsitään lausekkeelle $\frac{3x^2-8x+7}{(x-1)(x-2)^2}$ osamurtohajotelma. Koska $\text{syt}(x-1, (x-2)^2) = 1$, voidaan aluksi lauseen 47 perusteella löytää muotoa

$$\frac{3x^2-8x+7}{(x-1)(x-2)^2} = \frac{p_1(x)}{x-1} + \frac{p_2(x)}{(x-2)^2}$$

oleva hajotelma, missä $\deg(p_1) < 1$ ja $\deg(p_2) < 2$. Merkitään siis $p_1(x) = A$ ja $p_2(x) = B + Cx$, ja määrätään luvut $A = 2$, $B = 1$ ja $C = 1$, jolloin

$$\frac{3x^2-8x+7}{(x-1)(x-2)^2} = \frac{2}{x-1} + \frac{1+x}{(x-2)^2}. \quad (8.6)$$

Hajotelmaa (8.6) voidaan vielä lauseen 48 perusteella jatkaa:

$$\frac{1+x}{(x-2)^2} = \frac{D}{x-2} + \frac{E}{(x-2)^2},$$

mistä saadaan $D = 1$, $E = 3$ ja siis

$$\frac{1+x}{(x-2)^2} = \frac{1}{x-2} + \frac{3}{(x-2)^2}.$$

Hajotelmaa

$$\frac{3x^2-8x+7}{(x-1)(x-2)^2} = \frac{2}{x-1} + \frac{1}{x-2} + \frac{3}{(x-2)^2}$$

ei enää voida jatka, mutta tämä olisi voitu löytää suoraankin käyttämällä määräämättömiä kertoimia.

Esimerkki 133. Jos nimittäjän ensimmäisen asteen tekijät ovat yksinkertaiset, ei välttämättä tarvitse turvautua määräämättömien kertoimien keinoon. Esimerkiksi hajotelman

$$\frac{1}{x(x-1)(x+1)} = \frac{A}{x} + \frac{B}{x-1} + \frac{C}{x+1} \quad (8.7)$$

kertoimet saadaan seuraavasti: kerrotaan yhtälö (8.7) x :llä, jolloin saadaan

$$\frac{1}{(x-1)(x+1)} = A + \frac{Bx}{x-1} + \frac{Cx}{x+1}$$

ja sijoittamalla $x = 0$ nähdään, että $A = -1$. Kertomalla yhtälö (8.7) $x - 1$:llä puolestaan saadaan

$$\frac{1}{x(x+1)} = \frac{A(x-1)}{x} + B + \frac{C(x-1)}{x+1},$$

ja sijoittamalla $x = 1$ nähdään, että $B = \frac{1}{2}$. Yhtälön (8.7) kertominen $x + 1$:llä taas antaa

$$\frac{1}{x(x-1)} = \frac{A(x+1)}{x} + \frac{B(x+1)}{x-1} + C,$$

josta sijoitus $x = -1$ antaa $C = \frac{1}{2}$.

Aina ei kuitenkaan ole tarpeen löytää hajotelmaa, jossa palaudutaan nimittäjän ensimmäisen asteen tekijöihin. Esimerkiksi määräämätöntä integraalia etsittäessä voidaan toisinaan tyytyä nimittäjän toisen asteen tekijöihin, jolloin etuna on lisäksi se, että ei tarvitse käyttää kompleksilukuhajotelmia, vaan voidaan pysyä reaalilukujen joukossa.

Esimerkki 134. Polynomille $q(x) = x^6 + x^4 - x^2 - 1$ voidaan löytää seuraava hajotelma:

$$\begin{aligned} x^6 + x^4 - x^2 - 1 &= x^4(x^2 + 1) - (x^2 + 1) = (x^4 - 1)(x^2 + 1) \\ &= (x^2 - 1)(x^2 + 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)^2. \end{aligned}$$

Tekijä $x^2 + 1$, joka esiintyy kaksi kertaa, ei enää jakaudu tekijöihin reaalilukujen joukossa, koska sillä ei ole reaalista nollakohtaa. Nyt $\text{sy}(x^2 - 1, x^2 + 1) = 1$, joten voidaan löytää osamurtohajotelma

$$\frac{1}{(x^2 - 1)(x^2 + 1)^2} = \frac{A + Bx}{x^2 - 1} + \frac{C + Dx + Ex^2 + Fx^3}{(x^2 + 1)^2},$$

josta kertoimet ratkaisemalla saadaan

$$\frac{1}{(x^2 - 1)(x^2 + 1)^2} = \frac{1}{4} \frac{1}{x^2 - 1} - \frac{1}{4} \frac{3 + x^2}{(x^2 + 1)^2}. \quad (8.8)$$

Jälkimmäinen termi voidaan edelleen kehittää muotoon

$$\frac{x^2 + 3}{(x^2 + 1)^2} = \frac{A + Bx}{x^2 + 1} + \frac{C + Dx}{(x^2 + 1)^2},$$

mistä kertoimet ratkaisemalla saadaan

$$\frac{x^2 + 3}{(x^2 + 1)^2} = \frac{1}{x^2 + 1} + \frac{2}{(x^2 + 1)^2},$$

siis saadaan

$$\frac{1}{(x^2 - 1)(x^2 + 1)^2} = \frac{1}{4} \frac{1}{x^2 - 1} - \frac{1}{4} \frac{1}{x^2 + 1} - \frac{1}{4} \frac{2}{(x^2 + 1)^2}. \quad (8.9)$$

Vaikka näin saadun hajotelman ensimmäisen termin nimittäjä jakaantuu reaaliin tekijöihin $x^2 - 1 = (x - 1)(x + 1)$, on (8.9) jo käyttökelpoinen vasemman puolen määräämättömän integraalin löytämiseksi: Oikean puolen termien antiderivaatat on esitetty mm. matematiikan kaavakokoelmassa kohdissa (28) ja (29).

Huomautus 37. Kehitelmä

$$\frac{x^2 + 3}{(x^2 + 1)^2} = \frac{1}{x^2 + 1} + \frac{2}{(x^2 + 1)^2}$$

voidaan löytää myös käyttämättä määräämättömiä kertoimia. Miten?

Matlab-ohjelmistossa polynomit esitetään jonona kertoimia muuttujan suurimmasta potenssista alaspäin. Esimerkiksi polynomit $p(x) = x^3 + 2x - 1$ ja $q(x) = x^2 - 1$ syötetään muodossa

```
>> p=[1,0,2,-1]
```

```
>> q=[1,0,-1]
```

Polynomien arvo jossakin pisteessä lasketaan komennolla `polyval`. Esimerkiksi $q(2) = 2^2 - 1 = 3$ lasketaan seuraavasti:

```
>> polyval(q,2)
```

```
ans =
```

```
>>
```

Polynomien tulo lasketaan komennolla `conv`:

```
>> conv(p,q)
```

```
ans =
```

```
1      0      1     -1     -2      1
```

```
>>
```

Vastaus tulkitaan polynomiksi $x^5 + x^3 - x^2 - 2x + 1$. Nollakohtien etsiminen puolestaan tapahtuu seuraavasti:

```
>> roots(p)
```

```
ans =
```

```
-0.2267 + 1.4677i  
-0.2267 - 1.4677i  
0.4534
```

```
>>
```

Matlabissa on symbolisen matematiikan työkalut myös tekijöihinjakoa varten. Tällöin tulee luoda `syms`-komennolla tarvittavat muuttujasymbolit. Esimerkiksi

```
>> syms x
```

```
>> factor(x^6-1)
```

```
ans =
```

```
(x-1)*(x+1)*(x^2+x+1)*(x^2-x+1)
```

```
>>
```

Pelkkä polynomien jakolasku taas saadaan aikaan komennolla `deconv`. Jos esimerkiksi on jaettava polynomi $p(x) = x^3 + 2x - 1$ polynomilla $q(x) = x^2 - 1$ toimitaan seuraavasti:

```
>> [a,r]=deconv(p,q)
```

```
a =
```

```
1      0
```

```
r =
```

```
0      0      3     -1
```

```
>>
```

Vastaus tulkitaan siten että osamäärä on x ja jakojäännös $3x - 1$.

Matlabissa on myös työkalu osamurtojen löytämiseksi:

```
>> [r,p,k]=residue(p,q)
```

```
r =
```

```
2  
1
```

```
p =
```

$$\begin{array}{r} -1 \\ 1 \\ k= \\ 1 \quad 0 \end{array}$$

>>

tulkitaan siten, että

$$\frac{p(x)}{q(x)} = \frac{2}{x+1} + \frac{1}{x-1} + x.$$

Pystyvektori r ilmaisee siis osoittajat 2 ja 1, kun puolestaan pystyvektori p ilmaisee nimittäjien nollakohdat -1 ja 1 . Nimittäjät ovat siis $x - (-1) = x + 1$ ja $x - 1$. k on osamääräpolynomi $1 \cdot x + 0$.

Luvun oleellisia asioita:

- Polynomien jaollisuus, Eukleideen algoritmi, syt.
- Lauseen 47 hajotelma.
- Lauseen 48 hajotelma.