Havainnollistavaa algebraa lukiolaisille matemaattisen kielentämisen näkökulmasta

Sanni Sairanen

Pro gradu -tutkielma
Huhtikuu 2013

MATEMATIIKAN JA TILASTOTIETEEN LAITOS
TURUN YLIOPISTO

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Sairanen, Sanni: Havainnollistavaa algebraa lukiolaisille matemaattisen kielentämisen näkökulmasta
Pro gradu -tutkielma, 100 s.
Matematiikka
Huhtikuu 2013

Tämän tutkielman aiheena on lukion pitkän matematiikan syventävän kurssin laatiminen. Kurssi muodostuu algebrallisista käsitteistä lähtien joukko-opista. Tarkoituksena on tarkastella algebraan liittyviä määritelmiä ja tehtäviä erikoisesti matemaattisen kielentämisen näkökulmasta. Ryhmäteorian opiskelu on pitkän matematiikan lukio-opiskelijalle uusi ja abstrakti asia, joten teoriaa lähestytään kevyesti mahdollisia jatko-opintoja matematiikan parissa silmällä pitäen.

Tutkielman alussa tarkastellaan matemaattisen kielentämisen taustaa ja sen vaikutusta opiskelijan ja opettajan näkökulmasta. Tällöin matemaattisen kielentämisen käsite tulee lukijalle tutuksi ennen varsinaista teorian käsittelyä. Erikoisesti harjoitustehtävissä matemaattinen kielentäminen konkretisoituu.

Uutta asiaa opiskeltaessa on tärkeää käyttää erilaisia havainnollistuskeinoja. Tässä tutkielmassa kuvat ja matemaattista kielentämistä sisältävät harjoitustehtävät auttavat lisäämään ymmärrystä. Myös soveltavat laskuesimerkit tavallisesta arkielämästä motivoivat opiskelijaa.

Tutkielman loppuun on koottu kaikkia lukuja käsittävä loppukoe ja sen ratkaisut. Tämä mallikoe on opettajalle suuntaa antava. Myös kaikki harjoitustehtävät ja esimerkit ovat helposti muokattavissa. Perustehtävien lisäksi jokaisen luvun lopussa on soveltavia ja haastaviakin tehtäviä.

Asiasanat: matemaattinen kielentäminen, algebra, joukko, ryhmä.

Sisältö

1 Johdanto

Pohtiessani tutkielmani aihetta yritin parhaani mukaan samaistua 2010-luvun lukion pitkän matematiikan opiskelijaan. On hyvin todennäköistä, että lukion pitkän matematiikan opiskelija tulee tulevaisuuden opinnoissaan tarvitsemaan matematiikkaa. Lujan matemaattisen pohjan perustaminen lukiossa on edellytys esimerkiksi yliopistotason matematiikan tai muiden luonnontieteellisten aineiden opiskeluun. Tutkielmani tarkoitus on kaventaa lukion ja yliopisto-opiskelun välistä kuilua matematiikan osalta ja motivoida innokasta lukio-opiskelijaa jatkamaan matematiikan opiskelua hyvillä pohjatiedoilla varustettuna.

Matematiikan osalta lukio-opiskelu tullee tulevaisuudessa uudistumaan, monipuolistumaan ja ehkä jopa mutkistumaan ainakin aluksi. Oman osansa tähän uudistukseen tuovat opetukseen mukaan otettavat CAS -laskimet ja sähköinen ylioppilaskoe. CAS -laskinten käyttöönoton myötä soveltavat tehtävät mutkistuvat ja opiskelijoiden on opeteltava syvällisesti tällaisen laskimen käyttö. Voisi siis todeta, että muun maailman ohella myös matematiikka kehittyy teknologiassa. Mielenkiintoista on myös seurata, miten sähköinen ylioppilaskoe matematiikan osalta tulee muodostumaan. Oman erikoisuutensa matematiikan ylioppilaskokeen rakentamiseen tuovat lisäksi vielä CAS -laskimet. Onko tällä kaikella tuloksia parantava vai huonontava vaikutus? Se lienee nähtävän vasta vuosien saatossa.

Vaikka nykyteknologia imee matematiikkaa vahvasti mukaansa, keskittyy tutkielmani tarkastelemaan matemaattisia ongelmia erityisesti matemaattisen kielentämisen näkökulmasta. Lukio-opiskelijan on tärkeää laskutaidon lisäksi myös pystyä jäsentelemään kirjallisesti omia ajatuksiaan ja tuloksiaan. Ei riitä, että uusi CAS -laskin antaa tuloksen, jota ei pystytä kirjallisesti tulkitsemaan. On oltava täsmällinen ja kriittinen jatkossakin, vaikka koneet tekisivätkin laskutyön opiskelijan puolesta. Totuus kuitenkin on, että CAS -laskinten käyttöönoton myötä kynän ja paperin käyttö matemaattisten tehtävien ratkaisuissa jäävät toissijaiseksi. Vaikka CAS -laskin suorittaakin laskutyön, on opiskelijan kaikesta huolimatta tärkeää jollakin tavalla jäsen-

tää ajatuksiaan ja tuloksiaan esimerkiksi paperille. Tällä tarkoitan erityisesti matemaattista kielentämistä.

2010-luvulle tultaessa on havaittu matemaattisen osaamisen taidon laskua niin lukiossa kuin yliopistossakin. Tällaisessa tapauksessa on pohdittava ratkaisua opiskelijoiden matemaattisten taitojen parantamiseen. Syytä taitojen huonontumiselle on varmasti hankala löytää, mutta sen sijaan ratkaisuja on helpompi keksiä. Pedagogisesta näkökulmasta tarkasteltuna matemaattinen kielentäminen voisi olla yksi keino saada opiskelijat takaisin matematiikan maailmaan kirjallisen pohdinnan ja tutkiskelun kautta. On olemassa erilaisia matemaattisen kielentämisen tehtävätyyppejä, joita opiskelijat voivat ratkaisuissaan hyödyntää oman mieltymyksensä mukaan. Matemaattinen kielentäminen käsittää laajasti erilaisia näkokulmia matematiikan opiskeluun. Näitä näkökulmia opiskelija voi itse kehittää ja hyödyntää tarpeensa mukaan. Tuloksena numeerisen laskun lisäksi saadaan ratkaisuun mukaan myös kirjallista pohdintaa ja tulkintaa, mistä on hyötyä sekä itselle että muille ratkaisun lukijoille. Matemaattista kielentämistä ja sen eri muotoja olen käsitellyt tutkielmassani sekä teoreettisesti että konkreettisesti harjoitustehtävissä.

Valitsin tutkielmani aiheeksi algebran, koska se käsittää monia matematiikan aloja laajuutensa vuoksi. Opiskelija tulee matematiikkaa sisältävissä jatko-opinnoissaan tarvitsemaan algebraa varmasti. Tarkoitus on, että tutkielmaani voidaan hyödyntää lukion pitkässä matematiikassa syventävänä kurssina, joka tavallaan antaa ensivaikutelmaa yliopisto-opiskeluun. Uutena asiana pitkän matematiikan opiskelijoille opetetaan perusmääritelmiä modernin algebran käsitteestä ryhmä. Ryhmäteoriaa havainnollistetaan tässä tutkielmassa geometrian ja erilaisten kuvioiden avulla, jolloin ymmärrys ryhmäkäsitettä kohtaan helpottuu. Tutkielma käsittää myös muita ehkä hieman tutumpia algebrallisia käsitteitä kuten joukko-oppi, kuvaukset ja kongruenssi. Erityistä on, että opiskelija ratkaisee osan harjoitustehtävistä matemaattisen kielentämisen näkökulmasta, joihin esitetään myös malliratkaisut. Matemaattinen kielentäminen on käsitteenä laaja, joten opettaja pystyy myös itse oman harkintansa mukaan muokkaamaan ja kehittämään erilaisia tehtävätyyppejä.

Tutkielmani lopussa on vielä suuntaa antava mallikoe syventävän kurssin suorittamiseksi. Mukana on myös mallikokeen ratkaisut. Matemaattisen kielentämisen tehtävätyyppejä mallikokeessa on kaksi. Ensimmäinen on johonkin tutkielmani aiheeseen liittyvä todistustehtävä, johon opiskelijan tulee täyttää puuttuvat aukot ja toisessa tehtävässä ratkaisun kulkua on selitettävä kokonaisilla virkkeillä. Ratkaisun arvostelussa tulee siis ottaa huomioon myös matemaattisen kielentämisen osuus.

2 Matemaattinen kielentäminen

2.1 Mitä tarkoitetaan matemaattisella kielentämisellä?

Matematiikka kouluaineena eroaa muista oppiaineista kielellisesti melko paljon. Jo koulumatematiikassa käytetään paljon erilaisia symboleja, kun taas suurimmassa osassa muita kouluaineita työskennellään pitkälti erilaisten tekstien parissa. Matemaattisissa tehtävissä ei juurikaan käytetä tekstiä, vaan ymmärrys syntyy lähinnä symbolien, lukujen ja oman ymmärtämisen kautta. Miten opiskelijan ymmärrys ja matematiikan opiskelu muuttuisivat, jos matematiikkaan tuotaisiin laskujen rinnalle asiaa selventävää tekstiä? Entä miten muuttuu ratkaistun tehtävän analysointi opettajan näkökulmasta?

Kieli määritellään yleensä esittävien merkkien eli symboleiden järjestelmäksi, jolloin kieli käsitteenä voidaan ymmärtää hyvin laajasti. Myös ilmeet ja eleet viestittävät vastaanottajalle paljon. Voidaan esimerkiksi puhua matematiikan, musiikin tai liikunnan kielestä, yhtä hyvin ele- tai kuvakielestä. Tarkoitettiinpa mitä kielen muotoa tahansa, se konkretisoituu käyttötilanteessa. Vaikka lähettäjä ja vastaanottaja kommunikoisivatkin samalla äidinkielellä, he eivät välttämättä aina ymmärrä toisiaan. Tällaisessa tilanteessa kielenkäyttöä on jotenkin muutettava. [2]

Matematiikassa ymmärtämisen tueksi voidaan esimerkiksi tehdä erilaisia piirroksia, kuvioita ja kaavioita, mutta millä tavoin opettaja ymmärtäisi opiskelijan ajatteluprosessia tehokkaammin? Luonnollinen kirjakieli tukee oppimista myös matematiikassa. Tällöin opiskelija ratkaisee matemaattisen teh-

tävän tietenkin matemaattisin symbolein ja luvuin, mutta kirjoittaa viereen kokonaisia lauseita, joista lukijalle selviää tehtävän ratkaisijan ajatuksen kulku. Tämä ei ainoastaan edesauta opettajaa ymmärtämään opiskelijaa, vaan myös itse opiskelija ymmärtää ratkaisustaan enemmän kirjoittamansa tekstin avulla ja oppiminen saa aivan uuden näkökulman. Matemaattisella kielentämisellä tarkoitetaan siis matemaattisen ajattelun ilmaisemista kielen avulla joko suullisesti tai kirjallisesti. [7]

On kuitenkin muistettava, että opiskelijan oppiminen on pitkälti riippuvainen opiskelijan omasta asenteesta ja toiminnasta. Opiskelu on nimittäin dynaaminen tapahtuma, jossa oppiminen etenee pitkälle aikavälille sijoittuvana kehitysprosessina. [6] Matemaattisen kielentämisen tarkoitus on tukea kehitysprosessia ja sen avulla pyritään vaikuttamaan myös opiskelijan asenteeseen ja motivoitumiseen. Tärkeintä on, että opiskelija kokee onnistumisen ja osaamisen tunteen myös kirjoittamansa tekstin kautta, jolloin myös motivaatio matematiikkaa kohtaan kasvaa. [1]

2.2 Matemaattisen kielentämisen taustaa

Matemaattinen kielentäminen voi kirjallisen kielentämisen lisäksi olla myös suullista. Jos opiskelija puhuu matematiikasta, niin ajatteluprosessi on käynnissä jo ennen asian ilmaisua. Suullinen perustelu tukee kirjallista ratkaisua ja myös opettaja saa käsityksen siitä, miten opiskelija ymmärtää matemaattiset käsitteet ja ilmiöt. Tärkeintä on, että opiskelija pystyy omin sanoin selittämään ratkaisun kulkua. Matemaattinen kielentäminen suullisesti tai kirjallisesti pyrkii siis kasvattamaan opiskelijan matematiikan taitoja monipuolisesti. Koulumatematiikassa käytetään yleensä suppeasti vain matematiikan omaa symbolikieltä eikä opiskelija näin ollen pääse käyttämään kielellisiä taitojaan riittävästi.

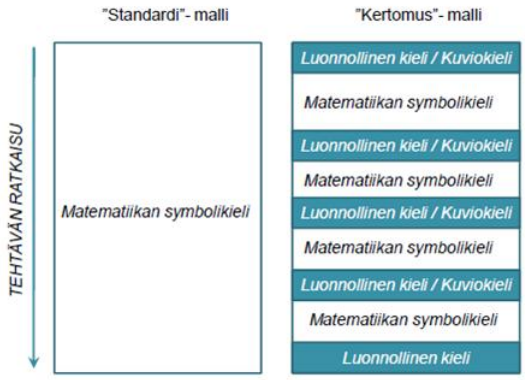
Opiskelijoita ja oppimistyylejä on olemassa yhtä paljon, mikä on otettu huomioon matemaattisessa kielentämisessäkin. Opiskelija voi käyttää tehtävien-sä kirjallisissa ratkaisuissa erilaisia matemaattisen kielentämisen malleja, joita ovat esimerkiksi standardi-, kertomus-, tiekartta-, päiväkirja- ja kommenttimalli. Edellä mainituista tyyleistä opiskelija voi valita itselleen sopivan. Esi-

tellään seuraavaksi nämä mallit. [1, 4]

2.2.1 Matemaattisen kielentämisen malleja

Standardimalli on yleinen oppikirjoissa eli se on pääpiirteiltään ainoastaan matematiikan symbolikieleen perustuva malli. Tämä malli ei siis huomioi luonnollista kieltä juuri ollenkaan, vaan keskittyy pitkälti matematiikan kielen hallintaan. Opiskelijan ja muiden lukijoiden ymmärtämisprosessi ei tässä mallissa ole keskeisimmässä roolissa.

Kertomusmallissa tehtävän ratkaisun rakenne koostuu sekä matemaattisesta symbolikielestä että luonnollisesta tekstistä. Ratkaisun eteneminen kuvataan vaiheittain sanallisesti ja/tai kuvallisesti käyttämällä väliotsikoita. Tässä mallissa siis käytetään luonnollista tekstiä ratkaisun tueksi, jotta ratkaisun lukeminen olisi helppoa ja vaivatonta. Sana "kertomus"kuvaakin hyvin tätä mallia, sillä ratkaisu etenee alkutilanteesta lopputilanteeseen niin kuin kertomuskin etenee. Useissa lukion oppikirjoissa sanallisten tehtävien esimerkit on esitelty tällä tavalla. [5]



Kuva 1: Havainnollistus standardi- ja kertomusmallista. [1]

Tiekartta -mallissa kerrotaan tehtävän ratkaisun kulku ensin sanallisessa muodossa ja kuvioiden avulla. Tällöin ratkaisun lukija pääsee jo heti alussa hyvin mukaan ratkaisun kulkuun ja näkee tarvittavat perustelut. Kun sanallinen osio ja mahdollinen kuviointi on saatu päätökseen, alkaa matemaattisen

symbolikielen osuus. Tässä kohtaa ratkaisu siis vasta lasketaan. Tässä mallissa ensin muodostettiin eräänlainen "reitti", jonka avulla saadaan ratkaisu. Tämän vuoksi mallia kutsutaan tiekartta -malliksi.

Päiväkirjamallissa opiskelija etenee suurin piirtein edellä mainitun standardimallin mukaisesti. Ongelmakohdan sattuessa opiskelija selkeyttää matemaattista ajatteluaan ja ratkaisun kulkua sanallisesti ja/tai piirtämällä ensisijaisesti oman itsensä vuoksi. Tämän vuoksi mallia kutsutaan siis päiväkirja -malliksi. Ratkaisusta muodostuva päiväkirja on usein tarkoitettu vain tehtävän ratkaisijan omaan käyttöön. Päiväkirjan avulla opiskelija on siis vuorovaikutuksessa tekstinsä kanssa, jolloin matemaattinen ymmärrys helpottuu.

Kommenttimallissa matematiikan symbolikieli ja luonnollinen kieli kulkevat rinnakkain. Tehtävän ratkaisu sisältää siis tavalliseen tapaan symbolikieltä, mutta jokaisella rivillä ratkaisun kulkua selitetään myös kirjallisesti. Tarkoitus on, että matemaattinen symbolikieli saa merkityksen myös luonnollisen kielen kautta, jolloin ratkaisu on selkeämpi ja sitä on helpompi ymmärtää.

Näistä edellä mainitusta malleista opiskelija voi siis valita itselleen sopivimman. Pääasia kuitenkin on, että tehtävien lopulliset vastaukset annetaan kokonaisina virkkeinä jokaisen mallin kohdalla. Kaikista tehokkaammin opiskelijaa itseään palvelee päiväkirja -malli, jota prosessimalliksikin kutsutaan. Muut mallit ovat enimmäkseen niin sanottuja presentaatiomalleja, joissa ratkaisu tukee sekä opiskelijan että opettajan ymmärrystä. [5]

Kaikkien edellä mainittujen tehtävämallien lisäksi mainittakoon vielä yksi käytännöllinen muista selvästi eroava kielentämismalli. Erilaisissa aukkotehtävissä opiskelija joutuu tarkasti tutkimaan kontekstia, jotta vastaus tyhjään aukkoon löytyisi. Opettaja voi nimittäin hankalimmissa tehtävissä kirjoittaa ratkaisun numeerisesti sekä kirjallisesti jättäen ratkaisuun aukkoja oleellisiin kohtiin. Tällöin opiskelija joutuu lukemaan ratkaisun läpi ehkä useitakin kertoja saadakseen ratkaisun täydennetyksi. Mitä intensiivisemmin opiskelija tutkii ratkaisua ja etsii vastauksia aukkokohtiin, sitä paremmin hän sisäistää annetun tehtävän. Tällainen aukkotehtävä -malli sopii erinomaisesti hahmottamaan opiskelijalle vaikeitakin todistuksia.

2.2.2 Kielentämistehtävien hyödyllisyydestä

Tärkein tehtävä matemaattisella kielentämisellä on edistää opiskelijan matemaattista ajattelua sekä luoda positiivinen asenne kyseistä oppiainetta kohtaan. Onnistuneesta ja ymmärretystä tehtävän ratkaisusta opiskelija saa varmasti motivaatiota matematiikan opiskeluun. Niin kuin edellä on jo tullut ilmi ei ainoastaan opiskelija hyödy matemaattisesta kielentämisestä, vaan myös opettaja ymmärtää helpommin opiskelijan ajatteluprosessia. Matemaattisen kielentämisen avulla matematiikkaa pyritään saamaan mieluisammaksi, sillä myönteinen kokemus on keskeinen oppimisen perusta.

Opettajan tehtävä on luoda opiskelijalle myönteisiä oppimiskokemuksia. Oppimiskokemus muodostuu tilanteessa, jossa opiskelija kohtaa uuden ilmiön eli tässä tapauksessa matemaattisen kielentämisen tehtävän. Tällöin opiskelija havaitsee voivansa saada aikaan sellaista toimintaa, jota hän ei ole aiemmin tuottanut. [8]

Matematiikka oppiaineena on aina ollut itsenäistä työskentelyä eikä niinkään ryhmässä oppimista. Matemaattinen kielentäminen voi kuitenkin tuoda matematiikan oppimiseen uuden näkökulman. Kun opiskelijat ovat kirjoittaneet sanallisesti kielentämistehtävien ratkaisujen perustelut, on niistä mahdollista keskustella esimerkiksi pienissä ryhmissä. Ratkaisujen perusteluja on varmasti monia erilaisia, joten opiskelijat voivat oppia muilta jotakin uutta. Tällainen käytäntö toiminnee parhaiten lukio-opetuksessa ja erityisesti pitkässä matematiikassa, sillä opiskelijat ovat itse saaneet valita syventyvänsä matematiikkaan laajasti.

Lukion jälkeen osa opiskelijoista siirtyy yliopistoon, jossa matematiikan opiskelu eroaa selvästi aikaisemmasta. Matemaattinen kielentäminen on apukeino kaventamaan lukio-opetuksen ja yliopisto-opetuksen välistä kuilua. Lukiomatematiikassa opittu kielentämisen taito auttaa opiskelijaa ratkaisemaan tehtäviä pohtivammalla otteella myös yliopistossa, jossa tehtävien ratkaisuilta vaaditaan enemmän. Matemaattista kielentämistä sisältäviä ratkaisumalleja on kokeiltu opiskelijoilla Tampereen teknillisessä yliopistossa ja Turun yliopistossa syksyllä 2012.

2.3 Esimerkkejä matematiikan kielentämistehtävistä

Esimerkki 2.1 (Standardi -malli)**.** Luokan kassassa on 400€. Opettaja ostaa 27 junalippua. Yksi lippu maksaa 12€. Kuinka paljon rahaa jää?

$$400€ - 12€ \times 27 = 76€. \quad [5]$$

Vastaus: 76€

Esimerkki 2.2 (Kertomus -malli)**.** Anna esimerkki kokonaislukukertoimisesta toisen asteen yhtälöstä, jonka juuret ovat -1 ja $\frac{2}{3}$.
Kysytty yhtälö on muotoa

$$ax^2 + bx + c = 0, a \neq 0,$$

joka myös voidaan kirjoittaa muodossa

$$ax^2 + bx + c = a\left(x - x_1\right)\left(x - x_2\right).$$

Sijoitetaan edellä mainittuun yhtälöön annetut arvot $x_1 = -1$ ja $x_2 = \frac{2}{3}$. Saadaan $a\left[x - (-1)\right]\left(x - \frac{2}{3}\right) = 0$ eli $a\left(x + 1\right)\left(x - \frac{2}{3}\right) = 0$. Kerrotaan yhtälö puolittain luvulla kolme. Nyt

$$a\left(x + 1\right)\left(3x - 2\right) = 0.$$

Yhtälö on kokonaislukukertoiminen toisen asteen yhtälö, kun a on kokonaisluku ja a eroaa nollasta. Valitaan esimerkiksi $a = 1$, jolloin saadaan yhtälö

$$\left(x + 1\right)\left(3x - 2\right) = 0.$$

Kun tämä kerrotaan auki, saadaan

$$3x^2 + x - 2 = 0. \quad [9]$$

Vastaus: $3x^2 + x - 2 = 0$

Esimerkki 2.3 (Tiekartta -malli)**.** Ratkaise itseisarvoyhtälö $|2x-4| = |5-x|$.

Lukujen $2x-4$ ja $5-x$ itseisarvot eli etäisyydet nollasta ovat yhtä suuret, jos ja vain jos luvut ovat samoja tai vastalukuja. [10]

$|2x-4| = |5-x|$
$2x-4 = 5-x$ tai $2x-4 = -(5-x)$
$3x = 9$ tai $2x-4 = -5+x$
$x = 3$ tai $x = -1$

Vastaus: $x = 3$ tai $x = -1$

Esimerkki 2.4 (Kommenttimalli)**.** Määritä raja-arvo $\lim_{x\to 2} \frac{3x^2-7x+2}{x-2}$. [11]

Rationaalifunktio $f(x) = \frac{3x^2-7x+2}{x-2}$ ei ole määritelty kohdassa $x = 2$, jolloin nimittäjä saa arvon nolla. Muokataan lauseketta ratkaisemalla ensin osoittajan nollakohdat.

$$\begin{aligned} 3x^2 - 7x + 2 &= 0 \qquad \text{| Käytetään toisen asteen yhtälön ratkaisukaavaa.} \\ x &= \frac{7 \pm \sqrt{(-7)^2 - 4 \cdot 3 \cdot 2}}{2 \cdot 3} \\ x &= \frac{7 \pm 5}{6}. \end{aligned}$$

Siis $x_1 = 2$ tai $x_2 = \frac{1}{3}$. Nyt

$\lim_{x\to 2} \frac{3x^2-7x+2}{x-2}$ | $ax^2 + bx + c = a(x-x_1)(x-x_2)$

$= \lim_{x\to 2} \frac{3(x-2)\left(x-\frac{1}{3}\right)}{x-2}$ | Termit $(x-2)$ supistuvat.

$= \lim_{x\to 2} 3\left(x-\frac{1}{3}\right)$ | Kerrotaan luku 3 sulkujen sisälle.

$= \lim_{x\to 2} (3x-1)$ | $g(x) = 3x-1$ on jatkuva kohdassa $x = 2$, joten

$= 3 \cdot 2 - 1$ | $\lim_{x\to 2} g(x) = g(2)$.

$= 5.$

Vastaus: $\lim_{x\to 2} \frac{3x^2-7x+2}{x-2} = 5.$

Esimerkki 2.5 (Tulon nollasäännön todistus (aukkotehtävä))**.** Väitetään, että tulo on nolla täsmälleen silloin, kun 1._____ on nolla.

Todistus. Tiedetään, että $b \cdot 0 = 0$ kaikilla 2._____ b. Jos nyt $b \cdot c = 0$ siten, että $b \neq 0$, niin saadaan

$$\begin{aligned} 3.\_\_\_\_\_ &= 0 \quad | \cdot b^{-1}(\text{On olemassa, koska } 4.\_\_\_\_\_). \\ b^{-1} \cdot b \cdot c &= 0 \\ 5.\_\_\_\_\_ \cdot c &= 0 \\ 6.\_\_\_\_\_ &= 0. \end{aligned}$$

Edellisen perusteella huomataan, ettei ole mahdollista lukujen b ja c 7._____, jos niiden tulo $bc = 0$. □

Oikea ratkaisu:

Väitetään, että tulo on nolla täsmälleen silloin, kun
1. *jokin tulon tekijöistä* on nolla.

Todistus. Tiedetään, että $b \cdot 0 = 0$ kaikilla 2. *reaaliluvuilla* b. Jos nyt $b \cdot c = 0$ siten, että $b \neq 0$, niin saadaan

$$\begin{aligned} 3.\ b \cdot c &= 0 \quad | \cdot b^{-1}(\text{On olemassa, koska } 4.\ b \neq 0). \\ b^{-1} \cdot b \cdot c &= 0 \\ 5.\ 1 \cdot c &= 0 \\ 6.\ c &= 0. \end{aligned}$$

Edellisen perusteella huomataan, ettei ole mahdollista lukujen b ja c
7. *eroavan nollasta*, jos niiden tulo $bc = 0$. [9] □

Seuraavissa luvuissa käsitellään algebrallisia peruskäsitteitä ja abstraktia algebraa pitkän matematiikan syventävän kurssin näkökulmasta. Edellä mainittuja tehtävämalleja matemaattisesta kielentämisestä käytetään joissakin tehtävissä. Toki oppilas voi halutessaan käyttää päiväkirja -mallia vaikka kaikissa tehtävissä. Päiväkirja -mallin tarkoituksenahan on jäsentää oppilaan ajattelua.

3 Mitä algebra on?

3.1 Historiaa

Algebra on saanut alkunsa jo muinaisesta Egyptistä ja Babyloniasta, jolloin osattiin ratkaista lineaarisia ja toisen asteen yhtälöitä. Babylonialaiset kehittivät aritmeettisen järjestelmän, jonka avulla he laskivat laskuja käyttäen algoritmeja. Tuolla aikakaudella yhtälöitä ratkaistiin pitkälti geometristen metodein, joista tutuin lienee Eukleideen Elementa.

Egyptiläiset ja babylonialaiset eivät juurikaan käyttäneet symboleita, vaan heidän matematiikkansa oli retorista. Tehtävien ratkaisuihin ei esitelty syitä tai perusteluja, vaan matematiikkaa opeteltiin esimerkkien kautta. Egyptiläisten tavoin babylonialaiset tunsivat ainoastaan positiiviset rationaaliluvut. Babylonialaiset löysivät kuitenkin approksimoituja ratkaisuja, vaikkei rationaaliluvuista muodostuvaa ratkaisua ollut saatavilla.

Merkittävin alkuaikojen matemaattikko oli kreikkalainen Diofantos, jota kutsutaan jopa algebran isäksi. Hän eli aikanaan Aleksandrian kaupungissa, joka oli aikakauden merkittävin matematiikan keskus. Yleisesti Diofantoksen arvioidaan eläneen vuoden 250 jKr tienoilla, mutta aikaisempia ja myöhäisempiäkin ajankohtia on esitetty.

Diofantoksen merkittävin teos on Arithmetica, joka muistuttaa babylonialaista algebraa geometristen menetelmien puuttumisen vuoksi. Teos sisältää suurimmaksi osaksi yksikäsitteisen ratkaisun tuottavien yhtälöiden tutkimista. Joukkoon mahtuu myös yhtälöitä, joiden ratkaisujoukko on ääretön täsmällisille ratkaisuille. Arithmeticassa esiintyvää ongelmien ratkaisua kutsutaan Diofantoksen analyysiksi, joka erityisesti nykyisin sopii paremmin lukuteorian ongelmiin kuin algebran alkeisiin.

Keskiajalla matematiikassa yleisesti ei tapahtunut juuri minkäänlaista kehitystä. Renessanssiajalla sen sijaan algebra jatkoi kehittymistään. Tuolloin algebraa alettiin soveltaa muun muassa geometriaan. Muodostettiin eriasteisia yhtälöitä soveltaen geometrisia kuvioita. Ongelmien ratkaisuun käytettiin erityisesti Eukleideen Elementaa tai al-Khwarizmin Algebraa. Merkittävä al-

gebrallinen saavutus tuohon aikaan oli myös kolmannen ja neljännen asteen yhtälöiden ratkaisu. Kaikesta huolimatta Eurooppa oppi algebraa hitaasti yliopistojen, kirkon kirjureiden ja taloudellisten toimintojen kautta.

1800-luvulla englantilaiset matemaatikot ottivat johtoaseman algebran tutkimuksessa. Englantilaiset tutkivat erilaisia matemaattisia objekteja, kuten vektoreita, matriiseja ja muunnoksia, joiden avulla he tuottivat monia uusia operaatioita matematiikkaan. Merkittävin saavutus tuolloin lienee kommutoimattoman algebran kehitys. Tällä tarkoitetaan sitä, että kertolaskuoperaation suorittamiseen algebran tietyllä alueella ei vaadita kommutatiivisuutta.

1900-luvulla alettiin puhua abstraktista algebrasta, jolla tarkoitetaan algebrallisten struktuureiden oppimista. Tällaisia struktuureita ovat esimerkiksi ryhmät, renkaat ja vektoriavaruudet. Nimitys "abstrakti algebra" luotiin, koska haluttiin erottaa edellä mainitut struktuurit alkuperäisestä algebrasta. Alkuperäisellä algebralla tarkoitetaan tässä kaavojen muodostamista ja algebrallisia ilmaisuja, jotka sisältävät tuntemattomia muuttujia sekä reaalitai kompleksilukuja. [12, 22, 24]

3.2 Algebraa yhteiskunnassa

3.2.1 Yleistä

Opettaja saattaa joutua usein tilanteeseen, jossa oppilas haluaa tietää vastauksen kysymykseen: mihin algebraa tai yleisesti matematiikkaa tarvitaan? Vastaus kysymykseen on opettajalle itselleen varmasti täysin selvä, mutta ongelma onkin, miten ilmaista se motivoivasti ja uskottavasti oppilaalle. On etsittävä mielenkiintoisia ja merkityksellisiä käytännön esimerkkejä, joita algebrakin tarjoaa runsaasti.

Algebran kehityksellä on pitkä historia, jonka avulla pystytään käsittämään abstraktin ja modernin algebran ongelmia. Nykyään erityisesti abstrakti eli moderni algebra on suosittu tutkimuskohde. Tällaisia tutkimuksia ovat muun muassa CD-levyjen virheidenkorjausalgoritmit, esimerkiksi CRC-menetelmä. Algoritmeilla on erityisen suuri merkitys myös tietokoneiden ohjelmoinnissa ja tietojenkäsittelytieteissä.

Algebran asema on yleensä aina matematiikassa ollut esimerkiksi aritmetiikkaa heikompi. Tämä johtunee siitä, ettei algebraa havaita konkreettisesti, vaikka sitä käytännössä koko ajan jollakin tavalla on esillä elinympäristössämme. Algebraa nimittäin tarvitaan fysiikassa, kemiassa, maantieteessä, taloustieteessä, psykologiassa sekä monella muulla tieteen alalla. Ensinnäkin algebran avulla pystytään ratkaisemaan monia numeerisia ja jokapäiväisiä ongelmia kuten budjetin laatimista; Kuinka paljon budjetista voi kuluttaa kuitenkaan ylittämättä sitä? Toisaalta algebran avulla pystytään muodostamaan yksinkertaisiakin yhtälöitä arkisista asioista, kun taas samasta aiheesta tehty monimutkainen taulukointi voi olla paljon hankalampi ymmärtää. Nämä kaikki yksinkertaiseltakin kuulostavat matemaattiset operaatiot ovat olleet pohjana modernin algebran kehitykselle.

Algebran oppimisen avulla pystytään matematiikassa ratkaisemaan yhä monimutkaisempia ongelmia. Matemaattisten ongelmien ratkaisemisen lisäksi algebran avulla pystytään ymmärtämään ympäröivän maailman ilmiöitä. Tällaisia ovat esimerkiksi luonnossa ilmenevät symmetriat, jotka kuuluvat ryhmäteorian tutkimusalaan.

3.2.2 Algebran asema koulumatematiikassa ennen ja nyt

Jo koulumatematiikassa oppilaat jossain mielessä käyttävät algebraa laskiessaan yhteen-, vähennys- ja kertolaskuja. Oppilaat nimittäin ratkaisevat laskujaan käyttämällä erilaisia operaatioita, numeroita ja muita symboleja. Mitä pidemmälle koulu-uralla edetään, sitä monimutkaisemmaksi muuttuvat algebralliset ongelmat. Lukiomatematiikassa tehtäviä ratkaistaan jonkin verran pelkillä symboleilla eikä niinkään numeerisilla arvoilla. Ratkaisemalla tehtävät ainoastaan symboleilla saadaan muodostettua yleisiä kaavoja, jotka voidaan ratkaista sijoittamalla symbolien paikalle jokin numeerinen arvo.

Aikaisemmin sanalla "algebra"oli keskeinen asema koulumatematiikassa. Monien oppikirjojen nimet keskikoulussa ja lukiossa sisälsivät sanan "algebra". Esimerkiksi 1960-luvun keskikoulun oppikirja on nimeltään "Keskikoulun algebran harjoituskirja" [15] ja lukion oppikirja on "Lukion algebra 1" [16]. Nyttemmin lasketaan samankaltaisia laskuja kuin edellä mainitussa keski-

koulun ja lukion oppikirjoissa, mutta sanaa "algebra"ei juurikaan käytetä enää koulumatematiikassa. Nykyajan lukiolaisista suurin osa siis laskee algebrallisia laskuja tuntematta algebran käsitettä modernista algebrasta puhumattakaan.

Modernin algebran käsite on lukiomatematiikassa vieras. Lukion opetussuunnitelman perusteetkaan eivät painota modernia algebraa. [36] Vasta yliopistossa on mahdollisuus päästä oppimaan modernin algebran peruskäsitteitä, joita siis muun muassa ovat ryhmä, rengas ja vektoriavaruus. Edellä mainittuja peruskäsitteitä voisi ottaa mukaan lukion pitkän matematiikan opetukseen ja havainnollistaa lukiolaisille algebrallisia menetelmiä. Näin oppilaat saisivat jonkunlaiset pohjatiedot myös modernista algebrasta lukion jälkeistä matematiikan opiskelua varten.

Lukion opetussuunnitelman perusteissa pitkän matematiikan osalta opiskelija pääsee tutustumaan väitelauseiden rakenteisiin ja harjoittelemaan todistamista geometrian kurssissa sekä syventävässä lukuteorian ja logiikan kurssissa. [36] Kyseinen syventävä kurssi on hyödyllinen valita, jos opiskelijan tavoitteena on jatkaa matematiikan opiskelua yliopistossa. Tällöin opiskelijalla on jonkinlainen käsitys erilaisten lauseiden todistamisesta ennen jatko-opintoja. Tässä tutkielmassa suunniteltu pitkän matematiikan syventävä kurssi perustuu pitkälti samankaltaisiin tavoitteisiin kuin lukuteorian ja logiikan syventävä kurssi. Algebran aihealueet nimittäin sisältävät useita lukio-opiskelijalle tuntemattomia käsitteitä ja väitteitä, jotka vaativat perusteluja.

Seuraavissa luvuissa esitellään algebrallisia peruskäsitteitä lukiomatematiikkaan sopivalla ja havainnollistavalla tavalla. Havainnollistavana keinona algebrallisissa käsitteissä voidaan käyttää esimerkiksi geometriaa. Tarkoitus on, että oppilaalla on entuudestaan tarvittavat geometrian tiedot. Jokaisen luvun lopussa on aiheeseen liittyviä harjoitustehtäviä. Osa harjoitustehtävistä ratkaistaan matemaattisen kielentämisen näkökulmasta niin sanottuina kielentämistehtävinä. Ratkaisut esitetään viimeisessä luvussa.

4 Joukko-oppia

Melkein jokaisella matematiikan alueella tarvitaan käsitys joukko-opin perusteista. Joukon voi sanallisesti määritellä hyvin monella eri tavalla. Se voidaan esimerkiksi kuvitella eräänlaiseksi kokoelmaksi erilaisia objekteja. Kokonaislukujen joukko $\mathbb{Z}$ on tuttu esimerkki eräästä joukosta, jossa objekteina siis ovat kaikki kokonaisluvut. Joukon objekteilla on yksi tai useampi yhteinen ominaisuus. Ulkopuolisella objektilla ei siis ole näitä ominaisuuksia. Esimerkiksi rationaaliluku $\frac{5}{7}$ ei kuulu kokonaislukujen joukkoon $\mathbb{Z}$.

4.1 Määritelmiä

Esimerkki 4.1. Oletetaan, että joukko A koostuu neljästä alkiosta 1,2,3 ja 4 toisin sanoen $A = \{1, 2, 3, 4\}$. Esimerkiksi luvun 1 kuulumista joukkoon A merkitään symbolilla $\in$. Luku 5 ei sen sijaan kuulu joukkoon A. Tällöin merkitään $5 \notin A$. Joukko voi myös olla tyhjä eli se ei sisällä ainuttakkaan alkiota. Tällaista joukkoa merkitään yleisesti symbolilla ϕ.

Esimerkki 4.2. Käytännön yksinkertaisena esimerkkinä voidaan muodostaa joukko, joka koostuu kaikista suomalaisista. Merkitään suomalaista symbolilla s. Tällöin joukko voidaan kirjoittaa muodossa

$$S = \{s \mid \text{s on suomalainen}\}.$$

Joukon S alkiot koostuvat siis niistä alkioista s, jotka täyttävät ehdon, että s on suomalainen.

Määritelmä 4.3. Olkoot C ja D joukkoja, jotka kuuluvat universaaliin joukkoon U. Jos jokainen joukon C alkio on myös joukon D alkio, niin sanotaan, että joukko C sisältyy joukkoon D tai joukko C on joukon D osajoukko. Tätä merkitään $C \subseteq D$. Jos $C \subseteq D$ ja $C \neq D$, niin joukko C on joukon D aito osajoukko, jota merkitään $C \subset D$.

Joukkojen välisiä relaatioita pystytään visualisoimaan esimerkiksi Venn - diagrammin avulla, jossa nelikulmio kuvaa universaalia joukkoa U ja ympyrät kuvaavat joukkoja C ja D. Seuraavaksi esitellään erilaisia joukko-operaatioita. [17]

a) Joukkojen C ja D *unionia* merkitään symbolilla $\cup$ ja sillä tarkoitetaan joukkoa

$$C \cup D = \{m \mid m \in C \text{ tai } m \in D \text{ tai } m \in C \text{ ja } m \in D\}.$$

b) Joukkojen C ja D *leikkaus* koostuu molemmille yhteisistä alkioista ja sitä merkitään symbolilla $\cap$:

$$C \cap D = \{m \mid m \in C \text{ ja } m \in D\}.$$

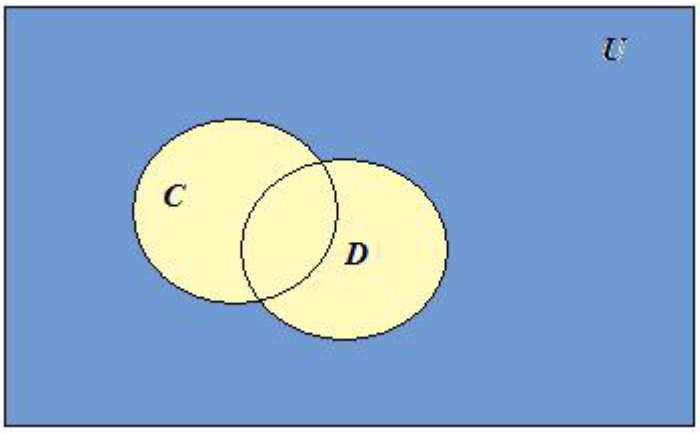
c) Jos joukko C sisältyy universaaliin joukkoon U, niin joukon C *komplementti* määritellään seuraavasti:

$$C' = \{m \mid m \in U \text{ ja } m \notin C\}.$$

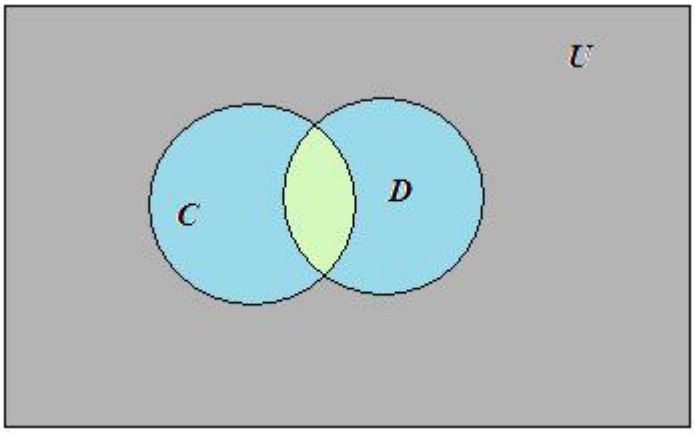
d) Joukkojen C ja D *erotus* on joukko, joka koostuu kaikista joukon C alkioista, jotka eivät sisälly joukkoon D:

$$C \backslash D = \{m \in U \mid m \in C \text{ ja } m \notin D\}.$$

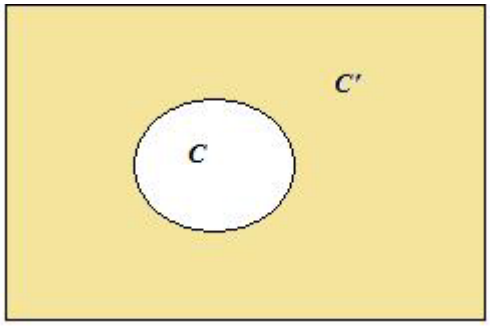
Havainnollistetaan edellä mainittuja joukko-operaatioita seuraavilla kuvilla:



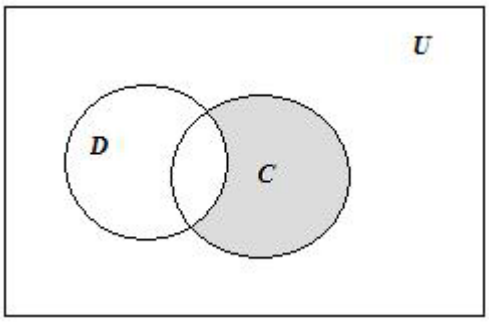
Kuva 2: Vaaleampi alue on joukkojen C ja D unioni $C \cup D$.



Kuva 3: Vaaleammaksi väritetty alue keskellä kuvaa joukkojen C ja D leikkausta $C \cap D$.



Kuva 4: Väritetty alue on joukon C komplementti C'.



Kuva 5: Väritetty alue on joukkojen C ja D erotus $C \backslash D$.

Tarkastellaan seuraavaksi joukkojen välisiä kuvauksia ja relaatioita.

4.2 Kuvaukset ja relaatiot

4.2.1 Kuvauksista

Oppilaalla on varmasti jonkunlainen käsitys funktiosta, sillä aikaisemmilla matematiikan kursseilla on ratkaistu paljon erilaisia yhtälöitä. Funktion avulla pystytään ratkaisemaan myös monia fysiikkaan liittyviä tehtäviä. Näin ollen oppilas ymmärtänee funktion toiminnan ja osaa ratkaista erilaisia yhtälöitä, mutta funktion peruskäsitteistö ja tausta on sen sijaan saattanut jäädä oppimatta.

Käsitteet *funktio* ja *kuvaus* tarkoittavat matematiikassa samaa asiaa. Tosin algebrassa käytetään yleisemmin kuvaus -nimitystä. Seuraavaksi tarkastellaan kuvaukseen liittyviä peruskäsitteitä.

Määritelmä 4.4 (Kuvaus)**.** Kuvaus f joukolta C joukkoon D liittää kaikkiin joukon C alkioihin x yksikäsitteisen joukon D alkion eli $y = f(x)$. Kuvausta merkitään $f: C \to D$. Tässä määritelmässä

i) joukkoa C kutsutaan kuvauksen f *määrittelyjoukoksi*

ii) joukko D on kuvauksen f *arvojoukko* ja

iii) alkion x *kuva* on y.

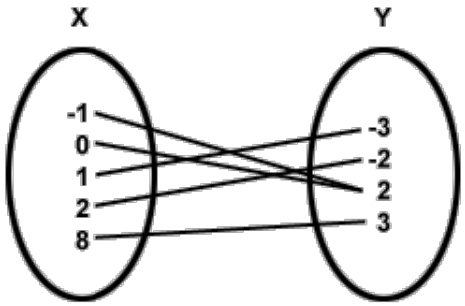
Kuvausta voidaan merkitä myös

$$f: C \to D, \quad x \mapsto y,$$

tai

$$f: C \to D, \quad f(x) = y. \text{ [13]}$$

Havainnollistetaan kuvausta myös seuraavalla kuvalla:



Kuva 6: Kuvaus joukosta X joukkoon Y. [30]

Esimerkki 4.5. Annetaan esimerkki kahdesta reaalianalyysin kuvauksesta. Merkitään $\mathbb{R}_+^o = \{x \mid x > 0\}$. Kuvaukset ovat

$$\text{a)} \quad f: \ \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2 - 1,$$

$$\text{b)} \quad g: \ \mathbb{R}_+^0 \to \mathbb{R} \quad g(x) = \log_{10} x.$$

Kohdassa a) funktioon f voidaan sijoittaa mikä tahansa reaaliluku ja funktio antaa arvoksi erään reaaliluvun. Sen sijaan kohdassa b) funktioon g voidaan sijoittaa ainoastaan reaalilukuja, jotka ovat aidosti suurempia kuin nolla. Tämä johtuu logaritmifunktion määrittelyalueesta. Funktion g arvoksi saadaan kuitenkin jokin reaaliluku.

Tarkastellaan vielä kuvaukseen $f: \ C \to D$ liittyviä ominaisuuksia [13]:

a) Kuvauksen f *arvojoukko* A_f on joukko
$f(C) = \{f(x) \mid x \in C\}$. Arvojoukosta käytetään myös merkintää $\mathrm{Im}(f)$.

b) Kohta a) voidaan esittää yleisemmin: jos $C_0 \subset C$, joukon C_0 *kuva(joukko)* on joukko $f(C_0) = \{f(x) \mid x \in C_0\}$.

c) Jos $D_0 \subset D$, joukon D_0 *alkukuva* on joukko
$f^{-1}(D_0) = \{x \in C \mid f(x) \in D_0\}$.

d) Jos $\mathrm{Im}(f)$=D, niin kuvaus f on *surjektio* (eli *surjektiivinen*). Sanotaan, että f on kuvaus joukolta C joukolle D.

e) Jos eri alkioilla on eri kuvat eli

$$x_1, x_2 \in C,\ x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2),$$

niin kuvaus f on *injektio* (eli *injektiivinen*).

f) Jos kuvaus f on injektio ja surjektio, niin kuvaus f on *bijektio* (eli *bijektiivinen*) eli *kääntäen yksikäsitteinen.*

Kohta e) voidaan esittää myös seuraavassa muodossa:

$$x_1, x_2 \in C, \quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Määritelmä 4.6 (Käänteisfunktio)**.** Jos $f : C \to D$ on bijektio, niin funktiota

$$f^{-1} : D \to C, \quad f^{-1}(y) = x, \quad \text{missä } y = f(x)$$

sanotaan funktion f *käänteisfunktioksi*, joka on funktion f tavoin myös bijektio. [20]

Esimerkki 4.7. Olkoon $g(x) = \frac{1}{x+1} + 2 : \mathbb{R} \setminus \{-1\} \to \mathbb{R} \setminus \{2\}$. Onko kyseinen kuvaus bijektio?

Funktio $g(x)$ on bijektio, jos se on sekä surjektio että injektio. Tutkitaan kohdassa a) funktion surjektiivisuus ja kohdassa b) injektiivisyys.

a) Olkoon $c \in \mathbb{R}$ ja $c \neq 2$. Tutkitaan onko olemassa sellaista muuttujaa b, joka kuuluu määrittelyjoukkoon $M_f = \mathbb{R} \setminus \{-1\}$ siten, että $g(b) = c$. Sijoitetaan muuttuja b annettuun funktioon $g(x)$ ja ratkaistaan yhtälö $g(b) = c$ muuttujan b suhteen.

$$\begin{aligned} g(b) &= \frac{1}{b+1} + 2 \\ \frac{1}{b+1} + 2 &= c \\ \frac{1}{b+1} &= c - 2 \\ b + 1 &= \frac{1}{c-2} \\ b &= \frac{1}{c-2} - 1 \\ &= \frac{3-c}{c-2} \in \mathbb{R} \setminus \{-1\} = M_f. \end{aligned}$$

Tämän perusteella funktio $g(x) = \frac{1}{x+1} + 2$ on surjektio.

b) Todetaan funktion injektiivisyys vastaoletuksen kautta. Jos muuttujat b_1 ja b_2 ovat injektiivisyyden määritelmän vastaisesti erisuuria, niin

$$g(b_1) = \frac{1}{b_1 + 1} + 2 \text{ ja } g(b_2) = \frac{1}{b_2 + 1} + 2.$$

Nämä ovat eri arvoja, sillä muuten

$$\begin{aligned} \frac{1}{b_1 + 1} + 2 &= \frac{1}{b_2 + 1} + 2 \\ b_1 + 1 &= b_2 + 1 \\ b_1 &= b_2, \end{aligned}$$

jolloin syntyy ristiriita. Siis funktio $g(x) = \frac{1}{x+1} + 2$ on injektio.

Kohtien a) ja b) perusteella funktio $g(x) = \frac{1}{x+1} + 2$ on bijektio.

Määritelmä 4.8 (Yhdistetty kuvaus)**.** Kuvausten $g : C \to D$ ja $h : D \to F$ yhdistetty kuvaus, jota tuloksikin kutsutaan, on

$$h \circ g : C \to F, \quad (h \circ g)(x) = h(g(x)).$$

Kuvaustulo on assosiatiivinen eli jos edellisten kuvausten g ja h lisäksi on kuvaus $j : F \to G$, niin

$$(j \circ h) \circ g = j \circ (h \circ g).$$

Yhdistetyn kuvauksen tapauksessa on oltava tarkkana tarkasteltaessa määrittelyjoukkoja ja arvojoukkoja. Nimittäin yhdistetyn funktion määrittely- ja arvojoukko saattaa erota alkuperäisten funktioiden määrittely- ja arvojoukoista.

Esimerkki 4.9. Olkoot $f(x) = x^2 - 4$ ($M_f = \mathbb{R}$, $A_f = [-4, \infty)$), $g(x) = \frac{1}{2}x - 3$ ($M_g = \mathbb{R}$, $A_g = \mathbb{R}$) ja $h(x) = 3x - 5$ ($M_h = \mathbb{R}$, $A_h = \mathbb{R}$). Laske

a) yhdistetty kuvaus $f(h(x))$ ja

b) yhdistetty kuvaus $h(g(f(x)))$.

Oikea ratkaisu:

a) Sijoitetaan funktio $h(x)$ funktioon $f(x)$ seuraavasti:

$$f(h(x)) = (3x-5)^2 - 4 = 9x^2 - 30x + 21 = k(x).$$

$M_k = \mathbb{R}$ ja $A_k = \mathbb{R}$.

b) Lasketaan ensin yhdistetty kuvaus $g(f(x))$:

$$g(f(x)) = \frac{1}{2}\left(x^2 - 4\right) - 3 = \frac{1}{2}x^2 - 5.$$

Lasketaan nyt yhdistetty kuvaus $h(g(f(x)))$:

$$3\left(\frac{1}{2}x^2 - 5\right) - 5 = \frac{3}{2}x^2 - 20 = j(x).$$

$M_j = \mathbb{R}$ ja $A_j = \mathbb{R}$.

Esimerkki 4.10. Olkoon $f(x) = 9x^2 - 5$ ($M_f = \mathbb{R}$, $A_f = \mathbb{R}$). Laske $(f \circ f^{-1})(x)$ eli funktion $f(x)$ ja sen käänteisfunktion $f(x)^{-1}$ yhdistetty kuvaus.

Ratkaisu:

Lasketaan ensin funktion $f(x)$ käänteisfunktio $f(x)^{-1}$. Olkoon $f(x) = y$. Ratkaistaan kyseinen yhtälö muuttujan x suhteen.

$$\begin{aligned} y &= 9x^2 - 5 \\ \frac{y+5}{9} &= x^2 \\ x &= \pm\sqrt{\frac{y+5}{9}}. \end{aligned}$$

Nyt siis muuttujanvaihdon jälkeen $f(x)^{-1} = \pm\sqrt{\frac{x+5}{9}}$ ($M_{f^{-1}} = [-5, \infty]$, $A_{f^{-1}} = \mathbb{R}$). Yhdistetty kuvaus

$$\begin{aligned} \left(f \circ f^{-1}\right)(x) & \\ &= f\left(f(x)^{-1}\right) \\ &= 9\left(\sqrt{\frac{x+5}{9}}\right)^2 - 5 \\ &= \frac{9(x+5)}{9} - 5 \\ &= x + 5 - 5 = x = g(x). \end{aligned}$$

Siis funktion ja sen käänteisfunktion yhdistetty kuvaus on aina identiteettifunktio x ($M_g = \mathbb{R}$, $A_g = \mathbb{R}$).

4.2.2 Ekvivalenssirelaatio

Tarkastellaan aluksi havainnollistavaa käytännön esimerkkiä ekvivalenssirelaatiosta:

Olkoon A junioreiden jalkapallojoukkue sekä a ja b joukkueen jäseniä. Koska a ja b molemmat kuuluvat joukkueeseen A, ovat he relaatiossa keskenään. Triviaalisti voidaan ajatella jäsenten a ja b olevan relaatiossa itsensä kanssa kyseisessä joukkueessa. Jos otettaisiin laskuihin myös kolmas jäsen c, joka siis myös kuuluu joukkueeseen A, niin jäsen c on relaatiossa sekä jäsenen a että jäsenen b kanssa. Voidaan myös ajatella, että jos jäsen c on relaatiossa jäsenen a kanssa, niin hän välttämättä on relaatiossa myös jäsenen b kanssa. Näin siksi, koska alunperin jäsenet a ja b olivat relaatiossa keskenään. Kaikissa tapauksissa voidaan ajatella tilanne myös toisin päin eli esimerkiksi jäsen b on relaatiossa jäsenen a kanssa, sillä vaihdoksesta huolimatta jäsenet edelleen pysyvät joukkueessa A ja mikään ei muutu.

Määritelmä 4.11 (Ekvivalenssirelaatio)**.** Joukkojen B_1 ja B_2 karteesisella tulolla tarkoitetaan joukkoa, jonka muodostavat kaikki järjestetyt parit (b_1, b_2), missä $b_1 \in B_1$ ja $b_2 \in B_2$. Tämä voidaan siis esittää muodossa:

$$B_1 \times B_2 = \{(b_1, b_2) \mid b_1 \in B_1, b_2 \in B_2\}.$$

Karteesisesta tulosta käytetään myös merkintää B^2.

Olkoon $R \subseteq B \times B$ jokin osajoukko. Tällöin sanotaan, että joukossa B on relaatio R. Alkio c *on relaatiossa* alkion d kanssa, kun (c, d) ovat osajoukon R alkioita. Tätä merkitään lyhyesti $c\ R\ d$.

Antamalla "sääntö" sille, milloin $c\ R\ d$ on voimassa määritellään relaatio. Tätä sääntöä voidaan hieman epätäsmällisesti kutsua relaatioksi R. [14]

Esimerkki 4.12. Annetaan esimerkki kahdesta karteesisesta tulosta:

1) Reaalilukujoukon $\mathbb{R}$ karteesinen tulo on joukko $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$.

2) Olkoon $A = \{a, b\}$ ja $B = \{1, 2, 3\}$. Nyt karteesinen tulo $A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.

Esimerkki 4.13. Määritellään kokonaislukujen joukossa $\mathbb{R}$ relaatio R asettamalla sääntö $x\ R\ y \Leftrightarrow x > y$. Nyt R on reaalilukujen tavallinen suuremmuusrelaatio. Tämä ilmaistaan sanomalla "R on relaatio $>$", mutta tarkasti relaatio R on joukko $R = \{(x, y) \in \mathbb{R}^2 \mid x > y\}$.

Määritelmä 4.14 (Ekvivalenssirelaatio)**.** Relaatio R on joukossa B määritelty *ekvivalenssirelaatio* tai *ekvivalenssi*, jos se täyttää seuraavat ehdot [13]:

E1. Kun b on joukon B alkio, niin $b\ R\ b$. (refleksiivisyys)

E2. Kun b ja c ovat joukon B alkioita ja $b\ R\ c$, niin $c\ R\ b$. (symmetrisyys)

E3. Kun b, c ja d ovat joukon B alkioita, ja $b\ R\ c$ ja $c\ R\ d$, niin $b\ R\ d$. (transitiivisuus)

Ekvivalenssirelaatiota merkitään yleensä symbolilla $\sim$. Jos $b \sim c$, niin alkio b on ekvivalentti alkion c kanssa. Sanotaan myös, että alkiot b ja c ovat ekvivalentit.

Esimerkki 4.15. Määritellään relaatio $<$ reaalilukujen joukossa $\mathbb{R}$. Nyt siis $R = \{(x, y) \in \mathbb{R}^2 \mid x < y\}$. Olkoon myös z joukon R alkio. Jos $y < z$, niin määritellyn relaation perusteella myös $x < z$. Tässä tapauksessa relaatio R on siis transitiivinen.

Esimerkki 4.16. Tutkitaan reaalilukujen joukkoa $\mathbb{R}$. Onko kyseisessä joukossa $S = \{(x, y) \mid x^2 = y^2\}$ ekvivalenssirelaatio?

Tarkastellaan ekvivalenssirelaation ehtoja E1-E3:

E1. Kaikille alkioille $x \in \mathbb{R}$ pätee $x^2 = x^2$, joten $x\ S\ x$.

E2. Kun x ja y ovat reaalilukuja, niin $x^2 = y^2 \in \mathbb{R}$ ja $y^2 = x^2 \in R$ eli $x\ S\ y$ ja $y\ S\ x$, joten symmetrisyys toteutuu.

E3. Kun x, y ja z ovat reaalilukuja, niin $x^2 = y^2 = z^2 \in R$ ja $x\ S\ y$, $y\ S\ Z$, joten $x\ S\ z$ ja transitiivisuus toteutuu.

Koska ehdot E1-E3 täyttyvät, on relaatio S ekvivalenssirelaatio.

Määritelmä 4.17 (Ekvivalenssiluokka)**.** Olkoon E ekvivalenssirelaatio joukossa B ja b sen alkio. Alkion b kanssa ekvivalenttia joukkoa sanotaan alkion b ekvivalenssiluokaksi $[b]$, jota merkitään:

$$[b] = \{c \in B \mid c \; E \; b\} .$$

Esimerkki 4.18. Määritellään kokonaislukujen joukossa $\mathbb{Z}$ relaatio $\sim$ asettamalla $n \sim m \iff n - m$ on jaollinen luvulla neljä. Tämä voidaan myös esittää muodossa $m = n + 4k$, missä k on jokin kokonaisluku. Kyseessä on ekvivalenssirelaato. Todistetaan tämä tutkimalla ekvivalenssirelaation määritelmän ehdot E1-E3.

E1 Olkoon x jokin kokonaisluku. Nyt $x - x = 0$, joka on jaollinen luvulla 4, sillä $\frac{0}{4} = 0$. Siis $x \sim x$ ja refleksiivisyys toteutuu.

E2 Symmetrisyyden osoittamiseksi oletetaan, että n ja m ovat joitakin kokonaislukuja ja $n \sim m$. Luku $n - m \in \mathbb{Z}$ on jaollinen luvulla 4 silloin ja vain silloin, kun $n = m + 4k$, missä k on jokin kokonaisluku. Ratkaisemalla kyseinen yhtälö luvun $m - n$ suhteen saadaan $m - n = -4k \in Z$, joka on jaollinen luvulla 4. Näin ollen $m \sim n$ ja symmetrisyys toteutuu.

E3 Oletetaan, että n, m ja l ovat joitakin kokonaislukuja ja $n \sim m$ sekä $m \sim l$. Silloin $n - m = 4k \in \mathbb{Z}$ ja $m - l = 4h \in \mathbb{Z}$. Nyt $n - l = 4k + m + 4h - m = 4\,(k + h)$, joka on jaollinen luvulla 4. Näin ollen siis myös $n \sim l$ ja transitiivisuus toteutuu.

Relaatio $\sim$ toteutti kaikki ekvivalenssirelaation määritelmän ehdot kokonaislukujen joukossa, joten se on ekvivalenssirelaatio. Koska ekvivalenssirelaatio voidaan myös esittää muodossa $m = n + 4k$, niin alkion n ekvivalenssiluokka on tällöin

$$[n] = \{m \in \mathbb{Z} \mid m \sim n\} = \{m + 4k \mid k \in \mathbb{Z}\} .$$

4.3 Joukko-opin harjoitustehtäviä

Harjoitustehtävä 4.1. Olkoon $U = \{10, 20, 30, 40, 50, 60, 70\}$ joukko. Muodosta ainakin neljä joukon U osajoukkoa.

Harjoitustehtävä 4.2. Olkoot $A = \{1, 2, 5, 6, 8, 10\}$, $B = \{2, 5, 7, 9, 10\}$ joukkoja ja $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ niiden universaali joukko. Muodosta seuraavat joukot:

i) $A \cup B$,

ii) $A \cap B$ ja

iii) $(A \cap B)'$.

Harjoitustehtävä 4.3. Piirrä Venn -diagrammit seuraavista joukko-operaatioista ja kirjoita omin sanoin mitä kyseiset merkinnät tarkoittavat:

a) $A \cap (B \cup C)$,

b) $(A')' = A$ ja

c) $(A \cup B)'$.

Harjoitustehtävä 4.4 (Kielentämistehtävä)**.** Olkoot A ja B perusjoukon X osajoukkoja. Todista De Morganin laki, joka on muotoa $(A \cap B)' = A' \cup B'$ täyttämällä todistuksesta puuttuvat aukot.

Todistus. Olkoon $x \in X$. Nyt $x \in$ 1._____

$$
\begin{aligned}
&\iff x \text{ 2.\_\_\_\_\_ } A \cap B \\
&\iff x \notin A \text{ tai } x \text{ 3.\_\_\_\_\_ } B \\
&\iff x \in \text{ 4.\_\_\_\_\_ tai } x \in \text{ 5.\_\_\_\_\_} \\
&\iff x \in \text{ 6.\_\_\_\_\_.}
\end{aligned}
$$

Siis $(A \cap B)' = A' \cup B'$. □

Harjoitustehtävä 4.5. Olkoon A, B ja C joukkoja jossakin universaalissa joukossa. Todista, että $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Harjoitustehtävä 4.6. Määritä seuraavien kuvausten laajin määrittelyjoukko ja arvojoukko.

a) $f(x) = x^2$,

b) $f(x) = \log_{10}(x)$,

c) $f(x) = \frac{1}{x^2-3}$ ja

d) $f(x) = \cos x + \sin x$.

Harjoitustehtävä 4.7 (Kielentämistehtävä)**.** Onko kuvaus $f : \mathbb{R} \to \mathbb{R},\ f(x) = 5x + 9$ bijektio? Entä kuvaus $g : \mathbb{R} \to \mathbb{R},\ g(x) = x^2$? Perustele vastauksesi selkeillä virkkeillä ratkaisun edetessä kertomusmallin mukaisesti (Esimerkki 2.2).

Harjoitustehtävä 4.8. Muodosta seuraavien funktioiden käänteisfunktiot. Tarkastele myös määrittelyjoukkoja ja arvojoukkoja.

a) $f(x) = \frac{x^2-4}{3}$ ja

b) $f(x) = \log_{10}(x) - 6$.

Harjoitustehtävä 4.9. Olkoot $f(x) = \sqrt{x}+6$, $g(x) = \frac{1}{x-1}$ ja $h(x) = x^3+1$. Laske

i) $g(f(x))$,

ii) $g(h(x))$ ja

iii) $f(g(h(x)))$.

Tarkastele myös alkuperäisten funktioiden ja yhdistettyjen funktioiden määrittely- ja arvojoukkoja.

Harjoitustehtävä 4.10. Olkoon $C = \{5, 11, 13\}$ ja $D = \{e, f, g\}$. Laske karteesinen tulo $C \times D$. Onko $D \times C = C \times D$? Perustele.

Harjoitustehtävä 4.11. Olkoot x ja y joitakin kokonaislukuja. Määritellään kokonaislukujen joukossa relaatio $S = \{(x, y) \mid x \sim y\}$, jossa $x \sim y$ tarkoittaa, että luku x jakaa luvun y. Onko relaatio S ekvivalenssirelaatio? Perustele ekvivalenssirelaation määritelmän avulla.

Harjoitustehtävä 4.12. Olkoot x ja y joitakin reaalilukuja. Määritellään reaalilukujen joukossa relaatio $R = \{(x, y) \mid x \sim y\}$, jossa $x \sim y$ tarkoittaa, että $x - y \in \mathbb{Z}$ eli lukujen x ja y erotus on kokonaisluku. Todista, että relaatio R on ekvivalenssirelaatio reaalilukujen joukossa $\mathbb{R}$.

Harjoitustehtävä 4.13. Määritellään kokonaislukujen joukossa relaatio $\sim$ asettamalla $a \sim b \iff a + b$ on jaollinen luvulla kolme. Mikä on alkion a ekvivalenssiluokka $[a]$?

5 Lukuteoriaa

5.1 Kokonaislukujen tekijöihinjako

Tutkitaan kokonaislukujen joukkoa $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$. Jos kokonaisluku s on jaollinen kokonaisluvulla t eli jos on olemassa jokin kokonaisluku r siten, että $s = tr$, niin merkitään $t \mid s$. Käytetään myös sanontoja: t jakaa kokonaisluvun s, t on kokonaisluvun s tekijä, kokonaisluku s on kokonaisluvun t monikerta. Kokonaislulukujen r ja t ollessa negatiivisia kokonaisluku s on kokonaisluvun t itseisarvon monikerta. Jos t ei jaa kokonaislukua s, niin merkitään $t \nmid s$. Esimerkiksi $3 \mid 12$ ja $8 \mid 24$, mutta $5 \nmid 12$.
Esitellään ja perustellaan seuraavaksi jaollisuuden yksinkertaiset ominaisuudet:

a) $s \mid s$ kaikilla kokonaisluvuilla s

   Käyttäen edellä mainittua määritelmää saadaan $s = ts$, josta ratkaisemalla t saadaan sen arvoksi $t = \frac{s}{s} = 1$ eli t on kokonaisluku.

b) jos $s \mid t$ ja $t \mid s$, niin $s = \pm t$

   Nyt $t = su$ ja $s = tv$. Kun nämä tiedot yhdistetään, saadaan $t = su = tvu$. Tämä on voimassa vain, jos $t = 0$, jolloin siis myös $s = 0$ tai $t \neq 0$ ja $uv = 1$ eli $u = v = \pm 1$.

c) jos $s \mid t$ ja $t \mid r$, niin $s \mid r$

   Nyt $t = sm$ ja $r = nt$, joten $r = nsm$. Tässä m ja n ovat joitakin

kokonaislukuja, joiden kertolaskun tuloksena saadaan myös jokin kokonaisluku l, joten $r = sl$ eli $s \mid r$.

d) jos $s \mid t$ ja $s \mid r$, niin $s \mid (t + r)$

Nyt $t = sm$ ja $r = sn$. Kun yhtälöt lasketaan puolittain yhteen, saadaan $t + r = sm + sn$. Ottamalla yhteinen tekijä yhtälö saadaan muotoon $t + r = s\,(m + n)$ eli $s \mid (t + r)$.

e) $s \mid t$ ja $s \mid r$ silloin ja vain silloin, kun $s \mid t \cdot r$ Olkoon $t = sk$ ja $r = sl$. Kun yhtälöt kerrotaan puolittain yhteen, saadaan $t \cdot r = sk \cdot sl = s^2kl$. Nyt $s \mid s^2kl$. Tarkastellaan väitettä vielä toiseen suuntaan eli oletetaan, että $s \mid t \cdot r$. Nyt $tr = sm$. Ratkaistaan yhtälöstä muuttuja t, jolloin saadaan $t = \frac{sm}{r}$. Nyt $s \mid \frac{sm}{r}$. Samoin kun yhtälöstä ratkaistaan muuttuja r, saadaan $r = \frac{sm}{t}$. Nyt $s \mid \frac{sm}{t}$.

Jos kokonaisluvun $q > 1$ ainoat tekijät ovat ± 1 ja $\pm q$, niin kokonaislukua q sanotaan alkuluvuksi tai jaottomaksi luvuksi. Yhdistetyiksi luvuiksi kutsutaan muita kokonaislukuja $m < 1$ ja ne voidaan siis hajottaa muotoon

$$m = m_1 m_2, \quad 1 < m_1 < m, \ 1 < m_2 < m.$$

Kun tekijöiden m_1 ja m_2 hajottamista jatketaan, saadaan lopulta luvun m *alkutekijähajotelma*

$$m = q_1 q_2 q_3 \cdots q_n \quad (q_1, ..., q_n \text{ alkulukuja})$$

Tämä voidaan myös kirjoittaa muodossa

$$m = h_1^{j_1} h_2^{j_2} \cdots h_r^{j_r} \quad (h_1, ..., h_r \text{ erisuuria alkulukuja}, \ j_i \geq 1)\,.$$

Alkulukujen joukkoa merkitään $\mathbb{P}$:llä eli

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 57, ...\}\,.$$

Esimerkki 5.1. $1200 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 3 = 2^4 \cdot 5^2 \cdot 3^1$.

Lause 5.2 (Jakoyhtälö)**.** Jos a ja b ovat kokonaislukuja ja b eroaa nollasta, niin on olemassa yksikäsitteiset kokonaisluvut q ja r, joille pätee

$$a = qb + r,$$

missä $0 \leq r < b$.

Jakoyhtälössä luku a on *jaettava*, b *jakaja*, q *(vaillinnainen) osamäärä* ja luku r on *jakojäännös*. [1]

Esimerkki 5.3. $31 = 6 \cdot 5 + 1, \quad 57 = 4 \cdot 13 + 5, \quad 29 = 4 \cdot 6 + 5.$

5.2 Suurin yhteinen tekijä

Olkoot u ja v kokonaislukuja siten, että ainakin toinen eroaa nollasta. Tällöin luvuilla u ja v on yksi yhteinen positiivinen tekijä, nimittäin 1. *Suurimmasta* yhteisestä tekijästä (joka siis on aina ≥ 1) käytetään merkintää $\text{syt}(u, v)$ tai (u, v). Sanotaan, että luvut u ja v ovat *suhteellisia alkulukuja* tai *keskenään jaottomia*, jos $\text{syt}(u, v)$=1.

Lemma 5.4. Kun u ja v ovat kokonaislukuja ja ainakin toinen eroaa nollasta, niin $\text{syt}(u, v)$ on joukon $\{xu + yv \mid x, y \in \mathbb{Z}\}$ pienin positiivinen luku.

Lause 5.5. Luku $d = \text{syt}\,(u, v)$ täyttää seuraavat ehdot:

(i) d on jaollinen jokaisella lukujen u ja v yhteisellä tekijällä

(ii) on olemassa sellaiset kokonaisluvut a ja b, että

$$d = au + bv \quad \text{Bezout'n identtisyys.}$$

[1] Jakoyhtälön todistus viitteessä [12] s.12.

Määritelmä 5.6 (Eukleideen algoritmi)**.** Eukleideen algoritmin avulla saadaan ratkaistua kahden kokonaisluvun u ja v suurin yhteinen tekijä. Ratkaisu perustuu toistuvaan edellä mainitun jakoalgoritmin soveltamiseen. Oletetaan, että $u \nmid v$. Saadaan

$$\begin{aligned} u &= q_1 v + r_1, \quad 0 < r_1 < |v|, \\ v &= q_2 r_1 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= q_3 r_2 + r_3, \quad 0 < r_3 < r_2, \end{aligned}$$

$$\ldots\ldots\ldots\ldots \quad \ldots\ldots$$

$$\begin{aligned} r_{n-2} &= q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n \, (+0) \, . \end{aligned}$$

Jakojäännökset r_i muodostavat aidosti vähenevän jonon positiviisia kokonaislukuja, joten menettely päättyy. Haettu suurin yhteinen tekijä (syt) on siis viimeinen jakojäännös $r_n \, (> 0)$ eli $r_n = syt\,(u, v)$. Eukleideen algoritmin menettely voidaan perustella seuraavasti. Viimeisen yhtälön mukaan $r_n \mid r_{n-1}$, joten myös $r_n \mid r_{n-2}$ ja niin edelleen. Kun yhtälöketjussa jatketaan näin ylöspäin, niin saadaan lopulta $r_n \mid v$ ja $r_n \mid u$. Nyt luku r_n on lukujen u ja v suurin yhteinen tekijä.

Eukleideen algoritmilla voidaan ratkaista myös sellaiset kokonaisluvut h ja m, että $r_n = hu + mv$. Ratkaisu saadaan, kun eliminoidaan $r_{n-1}, r_{n-2}, ..., r_1$ yhtälöketjusta esimerkiksi sijoitusmenettelyllä alhaalta lähtien.

Esimerkki 5.7. Lasketaan syt(351,603) alkutekijähajotelman avulla.

Muodostetaan ensin luvun 351 alkutekijähajotelma:

$$\begin{aligned} 351 &= 3 \cdot 117 \\ 117 &= 3 \cdot 39 \\ 39 &= 3 \cdot 13 \\ 13 &= 1 \cdot 13. \end{aligned}$$

Nyt siis $351 = 3 \cdot 3 \cdot 3 \cdot 13$. Lasketaan seuraavaksi myös luvun 603 alkutekijähajotelma:

$$\begin{aligned} 603 &= 3 \cdot 201 \\ 201 &= 3 \cdot 67 \\ 67 &= 1 \cdot 67. \end{aligned}$$

Nyt siis $603 = 3 \cdot 3 \cdot 67$. Molempien lukujen alkutekijähajotelmasta nähdään, että yhteinen tekijä muodostuu kertoimesta $3 \cdot 3$. Siis syt(351,603)=9.

Esimerkki 5.8. Lasketaan syt(202,487) Eukleideen algoritmin avulla.

$$\begin{aligned} 487 &= 2 \cdot 202 + 83 \\ 202 &= 2 \cdot 83 + 36 \\ 83 &= 2 \cdot 36 + 11 \\ 36 &= 3 \cdot 11 + 3 \\ 11 &= 3 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Nyt siis suurin yhteinen tekijä nähdään viimeisestä jakojäännöksestä eli $\text{syt}(202, 487) = 1$.

Esimerkki 5.9. Lasketaan syt(306,657) ja lausutaan se muodossa $h \cdot 306 + m \cdot 657$. Tässä siis h ja m ovat eräitä kokonaislukuja. Lasketaan ensin suurin yhteinen tekijä Eukleideen algoritmilla.

$$\begin{aligned} 657 &= 2 \cdot 306 + 45 \\ 306 &= 6 \cdot 45 + 36 \\ 45 &= 1 \cdot 36 + 9 \\ 36 &= 4 \cdot 9 + 0 \end{aligned}$$

Viimeinen jakojäännös on 9 eli $\text{syt}(306, 657) = 9$. Seuraavaksi käydään Eukleideen algoritmi läpi alhaalta ylöspäin.

$$\begin{aligned}
\text{syt}\,(306, 657) &= 9 \\
&= 45 - 1 \cdot 36 \\
&= 45 - 1 \cdot (306 - 6 \cdot 45) \\
&= -1 \cdot 306 + 7 \cdot 45 \\
&= -1 \cdot 306 + 7 \cdot (657 - 2 \cdot 306) \\
&= 7 \cdot 657 - 15 \cdot 306.
\end{aligned}$$

Nyt siis $h = -15$ ja $m = 7$, joten suurin yhteinen tekijä voidaan esittää myös muodossa $\text{syt}(306, 657) = 7 \cdot 657 - 15 \cdot 306$. On huomattava, etteivät h ja m kuitenkaan ole yksikäsitteisiä.

Määritelmä 5.10 (Pienin yhteinen jaettava, pyj)**.** Lukujen u ja v pienin yhteinen jaettava on analoginen suurimman yhteisen tekijän käsitteen kanssa. Se voidaan laskea seuraavalla tavalla:

$$\text{pyj}\,(u, v) = \frac{u \cdot v}{syt\,(u, v)}.$$

Esimerkki 5.11. Lasketaan pyj(306,657).

$\text{pyj}(306, 657) = \frac{306 \cdot 657}{9} = 22\ 338.$

5.3 Kongruenssi

Jaollisuuteen liittyviä asioita voidaan käsitellä kongruenssin määritelmän avulla, joka muistuttaa yhtälöiden käsittelyä.

Määritelmä 5.12. Olkoon m positiivinen kokonaisluku ja u ja v kokonaislukuja. Sanotaan, että u on kongruentti kokonaisluvun v kanssa *modulo* m, jos $u - v$ on jaollinen luvulla m. Tätä merkitään

$$u \equiv m \pmod{m}.$$

Edellä mainittua määritelmää kutsutaan siis kongruenssiksi ja lukua m sanotaan *moduliksi*. Vastakohtaa merkitään $u \not\equiv v \pmod{m}$ eli luku u on *epäkongruentti* (eli inkongruentti) luvun v kanssa modulo m.

Esimerkki 5.13. $22 \equiv 4 \pmod{6}$, sillä $22 - 4 = 18$ ja $6 \mid 18$. Samoin esimerkiksi $57 \equiv 2 \pmod{5}$ ja $71 \equiv -10 \pmod{9}$, kun taas $110 \not\equiv 1 \pmod{2}$.

Lemma 5.14. Olkoon m positiivinen kokonaisluku. Kaikilla kokonaisluvuilla t, u ja v on voimassa

i) $t \equiv t \pmod{m}$,

ii) Jos $t \equiv u \pmod{m}$, niin $u \equiv t \pmod{m}$,

iii) Jos $t \equiv u \pmod{m}$ ja $u \equiv v \pmod{m}$, niin $t \equiv v \pmod{m}$.

Määritelmää seuraten $t \equiv u \pmod{m}$, jos ja vain jos luku t on luvun m monikertaa vaille yhtäkuin luku u. Lyhyesti

$$t \equiv u \pmod{m} \quad \Leftrightarrow \quad t = u + mq.$$

Tässä siis q on myöskin jokin kokonaisluku. Nyt nähdään, että kongruenssi mod m hajottaa koko kokonaislukujoukon seuraavaa muotoa oleviin joukkoihin:

$$[t] = \{a + mk \mid k \in \mathbb{Z}\}.$$

Muodostunutta joukkoa [t] kutsutaan luvun [t] *jäännösluokaksi modulo* m, jota merkitään yleensä $\overline{t}$ tai $t + m\mathbb{Z}$. Luvut, jotka kuuluvat samaan jäännosluokkaan $\overline{t}$, antavat jaettaessa luvulla m saman jakojäännöksen. Kun käydään läpi kaikki mahdolliset jakojäännökset eli luvut $0, 1, ..., m-1$, muodostuu eräs jäännösluokkien edustajisto, jota kutsutaan kokonaislukujen *pienimmiksi ei-negatiivisiksi jäännöksiksi* mod m. Tämän perusteella muodostuu kaikkien jäännösluokkien mod m joukko, jota merkitään $\mathbb{Z}_m$:llä. Tämä kyseinen joukko voidaan kirjoittaa seuraavasti:

$$\mathbb{Z}_m = \left\{\overline{0}, \overline{1}, ..., \overline{m-1}\right\}.$$

Esimerkki 5.15. Valitaan esimerkiksi $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, missä

$$\begin{aligned}
\overline{0} &= 4\mathbb{Z} = \{4k \mid k \in \mathbb{Z}\} = \{..., -12, -8, -4, 0, 4, 8, 12, ...\}, \\
\overline{1} &= 1 + 4\mathbb{Z} = \{1 + 4k \mid k \in \mathbb{Z}\} = \{..., -11, -7, -3, 1, 5, 9, 13, ...\}, \\
\overline{2} &= 2 + 4\mathbb{Z} = \{2 + 4k \mid k \in \mathbb{Z}\} = \{..., -10, -6, -2, 2, 6, 10, 14, ...\}, \\
\overline{3} &= 3 + 4\mathbb{Z} = \{3 + 4k \mid k \in \mathbb{Z}\} = \{..., -9, -5, -1, 3, 7, 11, 15, ...\}.
\end{aligned}$$

Lause 5.16. a) Jos $u \equiv v \pmod{m}$ ja $s \equiv t \pmod{m}$, niin $u + s \equiv v + t$, $us \equiv vt \pmod{m}$.

b) Jos $su \equiv sv \pmod{m}$ ja $\text{syt}(s, m) = 1$, niin $u \equiv v \pmod{m}$.

c) Jos $u \equiv v \pmod{km}$, missä k on jokin positiivinen kokonaisluku, niin $u \equiv v \pmod{m}$.

Todistus. a) Luku $(u + s) - (v + t) = (u - v) + (s - t)$ on jaollinen luvulla m, koska lausekkeen tekijät $(u - v)$ ja $(s - t)$ ovat. Samalla tavalla $us - vt = (u - v)\, s + v\,(s - t)$ on jaollinen luvulla m.

b) Ehdoista $m \mid s\,(u - v)$ ja $\text{syt}(s, m) = 1$ yhdessä seuraa, että $m \mid u - v$.

c) Jos $km \mid u - v$, niin $m \mid u - v$. Tämä seuraa jaollisuuden teoriasta, sillä luku k on vain luvun m monikerta.

□

Lauseen 4.14 mukaan kongruensseja voidaan siis laskea yhteen, vähentää ja kertoa puolittain. Kohdan b) perusteella luvulla s jakaminen puolittain on mahdollista vain, jos $\text{syt}(s, m) = 1$. Tässä on ero tavalliseen yhtälöön, jonka voi kuitenkin jakaa puolittain aina, kunhan jakaja eroaa nollasta.

Esimerkki 5.17. Lasketaan jakojäännös jaettaessa $15^2 + 3^{100}$ luvulla 11. Nyt $15 \equiv 4 \pmod{11}$, koska $11 \mid 15 - 4$ tai $15 = 4 + 11 \equiv \pmod{11}$. Lauseen

4.14 perusteella saadaan

$$\begin{aligned} 15^2 &\equiv 4^2 \pmod{11} \\ 15^2 &\equiv 16 \equiv 5 \pmod{11}, \text{ koska } 11 \mid 16-5 \\ &\text{ja} \\ 3^5 &= 243 \equiv 1 \pmod{11} \\ 3^{10} &= 3^{5\cdot 2} \equiv 1^2 \pmod{11} \\ 3^{100} &= 3^{10\cdot 10} \equiv 1^{10} = 1 \pmod{11}. \end{aligned}$$

Nyt saadaan yhtälöpari

$$\begin{cases} 15^2 \equiv 5 \pmod{11} \\ 3^{100} \equiv 1 \pmod{11}. \end{cases}$$

Laskemalla yhtälöt yhteen saadaan $15^2 + 3^{100} \equiv 5 + 1 = 6 \pmod{11}$. Nyt siis jakojäännös on 6.

Määritelmä 5.18 (Diofantoksen yhtälö)**.** Diofantoksen yhtälöiksi kutsutaan yhtälöitä, joihin haetaan kokonaislukuratkaisuja. Näihin ratkaisuihin sovelletaan kongruensseja. Yleisesti lineaarisen kahden tuntemattoman muuttujan Diofantoksen yhtälön

$$lx + ny = d$$

ratkaisu on samanlainen kuin kongruenssin

$$lx \equiv d \pmod{n}$$

ratkaisu.

Esimerkki 5.19. Ratkaistaan kongruenssiyhtälö $4x \equiv 3 \pmod{7}$.

Kaikki ratkaisut ovat muotoa $x_0 + 7k$, kun k on jokin kokonaisluku. Ratkaistaan tehtävä kokeilemalla alkiot 0,1,2,...,6 kunnes jakojäännökseksi saadaan luku 3.

x	$4x \pmod 7$
0	$4 \cdot 0 = 0$
1	$4 \cdot 1 = 4$
2	$4 \cdot 2 = 8 \equiv 1 \pmod 7$
3	$4 \cdot 3 = 12 \equiv 5 \pmod 7$
4	$4 \cdot 4 = 16 \equiv 2 \pmod 7$
5	$4 \cdot 5 = 20 \equiv 6 \pmod 7$
6	$4 \cdot 6 = 24 \equiv 3 \pmod 7$

Nyt $x = 6$ on kongruenssiyhtälön eräs ratkaisu. Yleinen ratkaisu on $x = 6 + 7k$, kun k on jokin kokonaisluku.

Esimerkki 5.20. Innokas vanhojen tavaroiden keräilijä Harri osti antikvariaatista vinyylilevyjä hintaan 15€/kpl ja legendaarisia sarjakuvia hintaan 11€/kpl. Ostokset tekivät yhteensä 137 €. Montako vinyylilevyä ja sarjakuvaa Harri osti?

Merkitään vinyylilevyjä kirjaimella x ja sarjakuvia kirjaimella y. Saadaan yhtälö

$$15x + 11y = 137,$$

joka on eräs Diofantoksen yhtälö. Haetaan ensin ratkaisu vinyylilevyille eli muuttujalle x. Siirretään yhtälössä termi $11y$ toiselle puolelle, jolloin saadaan $15x = 137 - 11y$. Sovelletaan seuraavaksi kongruenssia tähän yhtälöön.

$15x \equiv 4 \pmod{11}$ ja $137 \equiv 5 \pmod{11}$. Nyt saadaan kongruenssiyhtälö $4x \equiv 5 \pmod{11}$, joka voidaan myös kirjoittaa muodossa $\overline{4x} = \overline{5}$.

Otetaan mukaan jäännösluokkaryhmän käsite. Tässä tapauksessa jäännösluokkaryhmä on $\mathbb{Z}_{11} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{10}\}$. Kokeillaan edellä mainitut ryhmän $\mathbb{Z}_{11}$ alkiot. Aloitetaan alkiosta $\overline{0}$ ja edetään järjestyksessä niin kauan kunnes saadaan alkio $\overline{5}$.

$x \in \mathbb{Z}_{11}$	$\overline{4x}$
$\overline{0}$	$\overline{4 \cdot 0} = \overline{0}$
$\overline{1}$	$\overline{4 \cdot 1} = \overline{4}$
$\overline{2}$	$\overline{4 \cdot 2} = \overline{8}$
$\overline{3}$	$\overline{4 \cdot 3} = \overline{12} = \overline{1}$
$\overline{4}$	$\overline{4 \cdot 4} = \overline{16} = \overline{5}$

Nyt siis $x = 4$ on eräs ratkaisu yhtälölle $\overline{4x} = \overline{5}$. Sijoittamalla saatu muuttujan x arvo alkuperäiseen Diofantoksen yhtälöön saadaan

$$\begin{aligned} 15 \cdot 4 + 11y &= 137 \\ 60 + 11y &= 137 \\ 11y &= 137 - 60 \\ 11y &= 77 \\ y = \tfrac{77}{11} &= 7. \end{aligned}$$

Vastaus: Harri osti vinyylilevyjä neljä kappaletta ja sarjakuvia seitsemän kappaletta.

5.4 Lukuteorian harjoitustehtäviä

Harjoitustehtävä 5.1. Ovatko seuraavat väittämät tosia? Perustele.

i) $2 \mid 52$,

ii) $3 \mid 73$,

iii) $12 \mid 252$ ja

iv) $5 \mid 117$.

Harjoitustehtävä 5.2. Muodosta lukujen a) 441, b) 237, c) 1011 ja d) 879 alkutekijähajotelmat.

Harjoitustehtävä 5.3 (Kielentämistehtävä)**.** Laske syt(207,871) lukujen alkutekijähajotelmien avulla ja perustele jokainen välivaihe yhdellä virkkeellä ratkaisun edetessä.

Harjoitustehtävä 5.4. Laske syt(120,440) Eukleideen algoritmin avulla. Entä mikä on pienin yhteinen jaettava pyj(120,440)?

Harjoitustehtävä 5.5. Laske syt(132,333) ja pyj(132,333).

Harjoitustehtävä 5.6. Laske syt(456, 661) ja lausu se muodossa $h \cdot 456 + m \cdot 661$.

Harjoitustehtävä 5.7. Ovatko seuraavat väittämät tosia? Perustele.

a) $34 \equiv 4 \pmod 7$,

b) $51 \equiv 6 \pmod 9$,

c) $64 \equiv (-8) \pmod 8$ ja

d) $100 \equiv 11 \pmod 4$.

Harjoitustehtävä 5.8. Miten muodostuu jäännösluokkien joukko $\mathbb{Z}_5$?

Harjoitustehtävä 5.9 (Kielentämistehtävä)**.** Laske jakojäännös, kun $17^3 + 5^{84}$ jaetaan luvulla 12. Selitä kokonaisilla lauseilla ratkaisun kulkua.

Harjoitustehtävä 5.10. Ratkaise kongruenssiyhtälö $5x \equiv 2 \pmod 6$.

Harjoitustehtävä 5.11. Ratkaise kongruenssiyhtälö $11x \equiv 3 \pmod 7$.

Harjoitustehtävä 5.12. Ville sai joululahjaksi lahjakortin elektroniikkakauppaan. Hän aikoo ostaa DVD -elokuvia ja CD -levyjä. DVD -elokuvat maksavat 17€ kappale ja CD-levyt 9€ kappale. Ostokset tekivät yhteensä 113€. Kuinka monta DVD -elokuvaa ja CD -levyä Ville osti?

Harjoitustehtävä 5.13 (Kielentämistehtävä)**.** Tehtävänä on todistaa kongruenssin ja Diofantoksen yhtälön teoriaan liittyvä lause täyttämällä todistuksesta puuttuvat aukot. Lause on muotoa:

Jos syt(a,m)=1, niin kongruenssilla $ax \equiv c \pmod m$ *on yksikäsitteinen ratkaisu* $x \in \mathbb{Z}$ *välillä* $0 \leq x \leq m - 1$..

Todistus. Oletuksen nojalla on olemassa sellaiset 1._____ u ja v, että $au + mv =$ 2._____ ja siis

$$a\,(uc) + m\,(vc) = c.$$

Tämän perusteella kongruenssilla on ratkaisu 3._____. Ratkaisuja ovat myös edellä mainitun ratkaisun lisäksi kongruentit luvut $x =$ 4._____, missä 5._____ on jokin kokonaisluku. Kongruessin ominaisuuksien perusteella kaikki ratkaisut ovat keskenään kongruentteja mod m, sillä

$$ax_1 \equiv ax_2 \pmod{m} \;\Rightarrow\; 6.\_\_\_\_\_ \pmod{m}.$$

Lopputuloksena siis ratkaisuista tarkalleen 7._____ on välillä $0 \leq x \leq m - 1$. [14] □

6 Ryhmät

Ryhmä on eräs abstraktin algebran peruskäsitteistä. Niin kuin muillakin algebrallisilla käsitteillä myös ryhmäteorialla on pitkä kehityshistoria. Merkittävimmät ryhmäteorian kehittäjät lienevät norjalainen matemaattiko Niels Henrik Abel ja ranskalainen matemaatikko Evariste Galois. Molemmat matemaatikot vaikuttivat 1800-luvun alkupuolella, jolloin ryhmäteoriakin kehittyi merkittävästi.

Abel tutki yhtälöiden juurien permutaatioita. Tosin nykyisin tässä tapauksessa yhtälöitä kutsutaan ryhmiksi. Abel todisti, ettei viidennen ja sitä korkeamman asteen yhtälöitä voida ratkaista algebrallisesti eli ratkaisemalla kyseisten yhtälöiden juuria. Parhaiten Abel kuitenkin tunnetaan ryhmäteorian käsitteestä "Abelin ryhmä", joka on kommutatiivinen ryhmä.

Evariste Galois kehitti kuuluisan Galoisin teorian, joka on merkittävä ryhmäteoriassa. Galois tutki Abelin tapaan erilaisten yhtälöiden ratkaisua aritmeettisen laskuoperaatioiden avulla. Hän liitti ryhmäteoriaa jokaiseen yhtälöön ja todisti, että polynomiyhtälön ratkeamiseksi määrätyssä muodossa jokaisella ryhmällä pitää olla jokin tietty ominaisuus. Galois oli myös ensimmäinen matemaatikko, joka käytti sanaa "ryhmä". [17, 29]

Ryhmäteorian avulla pystytään monipuolisesti selittämään muun muassa luonnon symmetrioita ja matemaattisia laskuoperaatioita. Tarkoitus ei ole tutkia ainoastaan esimerkiksi kokonaislukujen tai rationaalilukujen joukkoa, vaan ryhmäteoria kattaa sattumanvaraisen systeemin, jossa tietty operaatio toteuttaa esimerkiksi assosiaatiolain, joka esitetään myöhemmin. On huomattava, että ryhmäteoriaa tarvitaan matematiikan lisäksi myös fysiikassa ja tietojenkäsittelytieteissä. [18] Seuraavaksi esitellään ryhmäteorian peruskäsitteitä ja -määritelmiä. Aluksi havainnollistetaan uutta asiaa geometrian avulla.

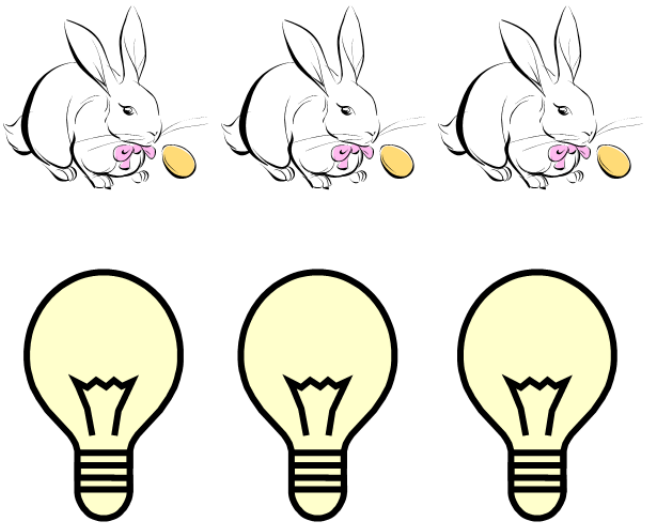
6.1 Ryhmäteorian havainnollistus geometrian avulla

Ryhmien muodostumista pystytään helposti havainnollistamaan erilaisten kuvien ja kuvioiden avulla. Tämä helpottanee lukijaa ymmärtämään abstraktia ryhmä -käsitettä hieman konkreettisemmin. Lopulta huomataan kuinka yleinen, ja laaja ryhmä käsitteenä oikeastaan on ja miten sitä voidaan havaita ympäröivässä maailmassa. Tässä aliluvussa tarkastellaan erityisesti symmetriaa.

Kuten tiedetään, matematiikan kehityksen voimakas kasvukausi alkoi 1800 -luvun alussa, jolloin tutkimusaloina olivat muun muassa funktioteoria ja ryhmäteoria. Tämän edelleenkin jatkuvan kasvukauden toinen tärkeä tutkimushaara oli symmetrian tarkastelu. Havaittiin symmetriaa löytyvän lähes kaikkialta: rakennusten seinistä, lattioista ja luonnossa perhosten siivistä. On kuitenkin huomattava, että matemaatikolle symmetria merkitsee paljon enemmän. Kuuluisin matemaatikko, joka tutki symmetriaa, oli Felix Klein. Hän tutki symmetriaa 1800-luvun loppupuolella Erlangen yliopistossa. [21] (Lisätietoa Felix Kleinista viitteestä [21] sivulta 2.)

Symmetrian tutkimisessa matemaatikkoa ei niinkään kiinnosta kuvion yksityiskohdat, vaan liikkeet, joilla symmetrian aiheuttavat toistot saadaan aikaiseksi. Kopioimalla tietokoneella esimerkiksi kuvan kukasta eri paikkaan tapahtuu juuri tällainen symmetrian aiheuttava liike. Voidaan ajatella, että tietokoneen käyttäjä muutti kukan paikkaa, mutta matemaatikon silmissä

otettiin koko sivu ja asetettiin se uudelleen, jolloin kukan paikka vaihtui. Tarkastellaan seuraavaksi alla olevaa kuvaa. Tässä kuvassa puput ja heh-



Kuva 7: Pupujen ja hehkulamppujen translaatio.

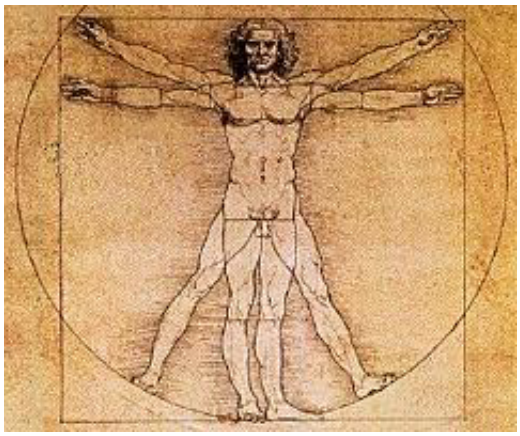
kulamput siirtyvät samalla translaatiolla. Ne vaihtavat siis paikkaa, jolloin alkuperäisellä paikalla on eri pupu ja hehkulamppu, mutta matemaatikolle translaatiolla aiheutettu symmetria pupun ja hehkulampun välillä on sama. Symmetria syntyy, kun samaa liikettä toistetaan tai iteroidaan useita kertoja. Syntynyt kuvio on symmetrinen, jos sen yksittäiset pisteet vaihtavat paikkaansa, mutta muuten kuvio säilyy entisellään. [21]

Symmetrian rotaatiota kuvaa oivallisesti esimerkiksi elintarvikepakkauksista löytyvä kierrätysmerkki.

Kuva 8: Kierrätysmerkki on symmetrinen. [31]

Tässä kuvassa on kolme nuolta, jolloin rotaatio on $\frac{360°}{3} = 120°$. Näin ollen, jos jokaista nuolta käännetään 120 asteen verran, kuvio pysyy samanlaisena, mutta nuolet ovat vaihtaneet paikkaa. [21]

Kolmas symmetrian tyyppi on molemminpuolinen symmetria, peilaus. Esimerkki tällaisesta symmetriasta on peilin edessä seisova ihminen, jonka kehon vasen ja oikea puoli on erotettu. Kuvitellaan, että vasemman puolen atomit liikkuvat horisontaalisesti samalla etäisyydellä täsmälleen samaan pisteeseen oikealle puolelle ja päinvastoin. Kuvanveistäjä ehkä näkee kasvoissa vasemmalla puolella jotakin, mitä oikealla puolella ei ole. Samoin lääkärit voivat väittää esimerkiksi sisäelinten kannalta kehon olevan ei-symmetrinen. Ulkoapäin tarkasteltuna ihmiskeho tässä tapauksessa kuitenkin on symmetrinen. Havainnollistava esimerkki molemminpuolisesta symmetriasta on kuva Leonardo Da Vincin kuuluisasta maalauksesta:



Kuva 9: Leonardo Da Vincin maalaus on molemminpuolinen symmetria. [32]

Usein symmetriakuvioissa esiintyvät kaikki kolme edellä mainittua symmetriamuotoa. Yleensä monimutkaisetkin symmetriset kuviot ovat joidenkin näiden kolmen symmetriamuodon kombinaatioita. Esimerkiksi alla olevasta kuvasta (mehiläispesästä) voidaan havaita eri symmetriamuotoja.

Kuva 10: Mehiläispesä muodostaa useita symmetrioita. [33]

Listataan, mitä symmetrioita kuvasta löytyy:

i) symmetrioiden translaatio kolmeen eri suuntaan,

ii) symmetrian rotaatio 120° kolmen kohtaavan solun ympärillä,

iii) symmetrian rotaatio 60° jokaisen solun keskuksen ympärillä,

iv) peilisymmetria reunoilla, joissa kaksi solua kohtaa ja

v) peilisymmetria kahden vastakkaisen sivun keskipisteiden välillä. [21]

Geometrisen havainnollistuksen jälkeen siirrytään tarkastelemaan ryhmäteorian perusteita tarkemmin.

6.2 Määritelmiä ja ryhmäteorian perusteita

Esimerkki 6.1. Johdantona ryhmäteoriaan tarkastellaan kokonaislukujen joukkoa $\mathbb{Z}$ ja reaalilukujen osajoukkoa $\mathbb{R}^0 = \mathbb{R}\setminus\{0\}$ eli reaalilukujoukkoa,

josta puuttuu luku nolla. Olkoot tässä kokonaisluvuilla laskutoimituksena yhteenlasku ja reaaliluvuilla kertolasku. Taulukoidaan yhteiset ominaisuudet:

$\mathbb{Z}$, laskutoimituksena $+$	$\mathbb{R}^0$, laskutoimituksena $\cdot$
(1) $a, d \in \mathbb{Z} \to a + d \in \mathbb{Z}$.	(1) $a, d \in \mathbb{R}^0 \to a \cdot d \in \mathbb{R}^0$.
(2) Kaikilla $r, s, t \in \mathbb{Z}$ on $(r + s) + t = r + (s + t)$.	(2) Kaikilla $r, s, t \in \mathbb{R}^0$ on $(r \cdot s) \cdot t = r \cdot (s \cdot t)$.
(3) On olemassa $0 \in \mathbb{Z}$, jolla $0 + i = i + 0 = i$ kaikilla kokonaisluvuilla i.	(3) On olemassa $1 \in \mathbb{R}^0$, jolla $1 \cdot i = i \cdot 1 = i$ kaikilla reaaliluvuilla $\mathbb{R}^0$:ssa.
(4) Jokaista lukua $d \in \mathbb{Z}$ vastaa $-d \in \mathbb{Z}$, jolla $d + (-d) = (-d) + d = 0$.	(4) Jokaista lukua $d \in \mathbb{R}^0$ vastaa $d^{-1} \in \mathbb{R}^0$, jolla $d \cdot d^{-1} = d^{-1} \cdot d = 1$.

Laskutoimituksilla on siis seuraavat ominaisuudet, jotka on numeroitu myös taulukossa:

(1) Vakaus laskutoimituksen suhteen eli toisin sanoen ryhmä on suljettu kyseisen laskutoimituksen suhteen,

(2) Assosiatiivisuus eli liittännäisyys,

(3) Neutraalialkion olemassaolo ja

(4) Käänteis/vasta-alkion olemassaolo.

On huomattava, etteivät edellä mainitut neljä ominaisuutta ole ainoat, jotka toteutuvat kokonaislukujen yhteenlaskussa ja nollasta poikkeavien reaalilukujen kertolaskussa. Nämä neljä ominaisuutta esiteltiin, koska ne ovat laskutoimituksien yleisimpiä ja käytetyimpiä ominaisuuksia. Myös rationaalilukujen joukko $\mathbb{Q}$ toteuttaa ominaisuudet (1)-(4), mutta esimerkiksi ominaisuus (4) ei päde kokonaislukujen kertolaskussa, sillä ei ole olemassa kokonaislukua y, jolla esimerkiksi $5 \cdot y = 1$. [13]

Määritelmä 6.2. Binäärioperaatiolla $*$ tarkoitetaan joukossa K kuvausta $K \times K \to K$, jota merkitään $(s, t) \mapsto s * t$. Jokaista joukon K alkioparia s, t kohti määräytyy yksikäsitteinen kolmas saman joukon K alkio $s * t$, jos binäärioperaatio $*$ on annettu.

Esimerkki 6.3. Kokonaislukujen joukossa $\mathbb{Z}$ on määritelty kolme tuttua binäärioperaatiota summa, tulo ja erotus $(+, \cdot, -)$. Määrittelemällä esimerkiksi joukon K alkioilla s ja t operaatio $s \,\Delta\, t = st - s - t$ saataisiin uusi binäärioperaatio Δ. [14]

Määritelmä 6.4 (Ryhmän määritelmä)**.** Ryhmällä tarkoitetaan joukkoa K, jossa on määritelty sellainen binäärioperaatio $*$, että seuraavat ehdot (K1)-(K4) ovat voimassa:

(K1) $s * t \in K$, kaikilla joukon K alkioilla s, t

(K2) $s * (t * v) = (s * t) * v$ kaikilla joukon K alkioilla s, t ja v (liitäntälaki)

(K3) On olemassa sellainen joukon K alkio a, että

$$s * a = a * s = s$$

kaikilla joukon K alkioilla s. Alkiota a kutsutaan neutraalialkioksi, ykkösalkioksi tai nolla-alkioksi.

(K4) Jokaista joukon K alkiota s kohti on olemassa sellainen joukon K alkio s^{-1}, että

$$s * s^{-1} = a = s^{-1} * a.$$

Alkiota s^{-1} kutsutaan alkion s käänteisalkioksi tai vasta-alkioksi.

Jos ehtojen (K1)-(K4) lisäksi on voimassa ehto

(K5) $s * t = t * s$ kaikilla joukon K alkiolla s, t,

sanotaan, että ryhmä K on kommutatiivinen Abelin ryhmä. [19]

Esimerkki 6.5. Kokonaislukujen joukko $\mathbb{Z}$ on Abelin ryhmä tavallisen yhteenlaskun $(+)$ suhteen. Tällöin siis kokonaislukujen joukko $\mathbb{Z}$ toteuttaa ehdot (K1)-(K5) binäärioperaationa $(+)$. Käydään seuraavaksi nämä ehdot läpi, kun $s = 3$, $t = 5$ ja $v = 1$.

(K1) $3 + 5 = 8$ ja luku 8 kuuluu kokonaislukujen joukkoon $\mathbb{Z}$.

(K2) $3 + (5 + 1) = 9 = (3 + 5) + 1$.

(K3) Kokonaislukujen tapauksessa neutraalialkio on luku 0. Nimittäin $3 + 0 = 0 + 3 = 3$.

(K4) Käänteisalkiona kokonaislukujen joukossa toimii luku -3, sillä $3 + (-3) = -3 + 3 = 0$.

(K5) $3 + 5 = 5 + 3 = 8$ eli kommutatiivisuus toteutuu.

Jos K on Abelin ryhmä, merkitään ryhmätoimitusta $*$ yleensä symbolilla $+$, neutraalialkiota luvulla 0 ja käänteisalkiota s^{-1} alkiolla $-s$, joka on niin sanottu vasta-alkio.

Lause 6.6. Ryhmän K neutraalialkio ja käänteisalkio ovat yksikäsitteisiä.

Todistus. Olkoon ryhmän K alkio a' neutraalialkio alkion a lisäksi. Tällöin ehdosta (K3) saadaan $a' = a' * a = a$. Jos alkiolla s on myös käänteisalkio s', niin kertomalla yhtälöön $s * s' = a$ vasemmalta alkiolla s^{-1} saadaan $(s^{-1} * s) * s' = s^{-1} * a$ eli $s' = s^{-1}$. Tässä tarvittiin ehtoja (K2)-(K4). [13] □

Milloin neutraalialkiota kutsutaan ykkösalkioksi tai nolla-alkioksi? Yleensä ryhmäteoriassa ryhmän K laskutoimitus $*$ merkitään kertolaskuna seuraavasti:

$$c * d = c \cdot d = cd,$$

missä alkiot c ja d ovat siis ryhmän K alkioita. Tällöin neutraalialkiota on tapana kutsua ykkösalkioksi ja sitä merkitään $e = 1 = 1_K$. Kun laskutoimitus merkitään kertolaskuna, sanotaan ryhmän K olevan *multiplikatiivinen* ryhmä.

Kertolaskuoperaation lisäksi ryhmäoperaatiolle käytetään myös yhteenlaskumerkintää:

$$c * d = c + d.$$

Yhteenlaskumerkinnässä neutraalialkiota kutsutaan nolla-alkioksi ja sitä merkitään $e = 0 = 0_K$ ja alkion c käänteisalkiota c^{-1} kutsutaan *vasta-alkioksi* $-c$. Tällöin ryhmän K sanotaan olevan *additiivinen*. Additiivista merkintätapaa käytetään usein, kun ryhmä K on Abelin ryhmä.

Ryhmän K alkioiden lukumäärää kutsutaan ryhmän K *kertaluvuksi* ja sitä merkitään $\#K$.

6.2.1 Jäännösluokkaryhmät

Olkoon m jokin positiivinen kokonaisluku. Luvussa 4 määritellyt jäännösluokat mod m muodostavat additiivisen Abelin ryhmän $(\mathbb{Z}_m, +)$, kun yhteenlasku määritellään $\overline{u} + \overline{v} = \overline{u+v}$. Koska kyseessä on Abelin ryhmä, neutraalialkio on $\overline{0}$ ja alkion $\overline{u}$ vasta-alkio on $\overline{-u}$. Jäännösluokkaryhmä on erityisesti esimerkki *äärellisestä* ryhmästä. Koska joukkona $\mathbb{Z}_m$ on $\left\{\overline{0}, ..., \overline{m-1}\right\}$, niin ryhmän $\mathbb{Z}_m$ kertaluku $\mathbb{Z}_m = m$. Ryhmällä $\mathbb{Z}_m$ on siis m alkiota, joten se on äärellinen.

Esimerkki 6.7. Ryhmä $(\mathbb{Z}_m, +)$ eli $\mathbb{Z}_m = \left\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\right\}$ on Abelin ryhmä yhteenlaskuoperaation $\overline{c} + \overline{d} = \overline{c+d}$ suhteen. Nolla-alkiona eli neutraalialkiona on $\overline{0}$, sillä $\overline{c} + \overline{0} = \overline{0} + \overline{c} = \overline{c}$. Alkion $\overline{c}$ vasta-alkiona $-\overline{c}$, sillä $\overline{c} + (\overline{-c}) = \overline{-c} + \overline{c} = \overline{0}$. Muodostetaan taulukko yhteenlaskuoperaatiosta, kun $m = 3$ ja lasketaan alkioiden vasta-alkiot.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

a) Alkion $\overline{1}$ vasta-alkio on $\overline{2}$, sillä $\overline{1} + \overline{2} = \overline{0}$ ja

b) alkion $\overline{2}$ vasta-alkio on $\overline{1}$, sillä $\overline{2} + \overline{1} = \overline{0}$.

Esimerkki 6.8. Tutkitaan onko joukko $\mathbb{Z}_m$ ryhmä kertolaskun suhteen.

1) Joukossa $\mathbb{Z}_m$ kertolasku $\overline{c} \cdot \overline{d} = \overline{cd}$, joka on assosiatiivinen, sillä

$$\left(\overline{c} \cdot \overline{d}\right) \cdot \overline{f} = \overline{cdf} = \overline{c} \cdot \left(\overline{d} \cdot \overline{f}\right).$$

2) Neutraalialkio on $\overline{1}$, sillä $\overline{1} \cdot \overline{c} = \overline{c} = \overline{c} \cdot \overline{1}$. On kuitenkin huomattava, ettei kaikilla jäännösluokilla ole käänteisalkiota. Esimerkiksi alkiolla $\overline{0}$ ei ole käänteisalkiota. Tämän perusteella siis joukko $\mathbb{Z}_m$ ei ole ryhmä kertolaskun suhteen.

Edellisen esimerkin perusteella joillakin jäännösluokilla kuitenkin on käänteisalkio. Tutkitaan minkälaisia nämä jäännösluokat ovat. Oletetaan, että $\overline{x}$ on jäännösluokan $\overline{c}$ käänteisalkio. Käänteisalkion määritelmän mukaan $\overline{c} \cdot \overline{x} = \overline{x} \cdot \overline{c} = \overline{1}$ eli $\overline{cx} = 1$. Tähän ehtoon voidaan käyttää aikaisemmin opittua kongruenssia, jolloin se saadaan muotoon $cx \equiv 1 \pmod{m}$. Kongruenssin teorian perusteella tällainen x on olemassa jos ja vain jos $\text{syt}(c, m) = 1$. Jäännösluokat, jotka toteuttavat kyseisen ehdon, ovat *alkuluokkia* mod m ja niiden joukkoa merkitään symbolilla $\mathbb{Z}_m^*$. Tätä joukkoa merkitään matemaattisesti:

$$\begin{aligned} \mathbb{Z}_m^* &= \{\overline{c} \in \mathbb{Z}_m \mid \text{syt}\,(c, m) = 1\} \\ &= \left\{\overline{c} \in \mathbb{Z}_m \mid \text{on sellainen } \overline{c} \in \mathbb{Z}_m, \text{ että } \overline{c} \cdot \overline{x} = \overline{1}\right\}. \end{aligned}$$

Alkuluokkien joukko mod m on kertolaskun suhteen Abelin ryhmä. Tällöin siis ykkösalkiona on $\overline{1}$ ja alkion $\overline{c}$ käänteisalkiona sellainen $\overline{x}$, että $cx \equiv 1 \pmod{m}$. [14]

Esimerkki 6.9. Olkoon $\mathbb{Z}_3 = \left\{\overline{0}, \overline{1}, \overline{2}\right\}$ multiplikatiivinen ryhmä ja $\mathbb{Z}_3^* = \left\{\overline{1}, \overline{2}\right\}$. Tutkitaan, millä alkuluokilla on käänteisalkio.

Nyt siis $\text{syt}(1, 3) = 1$ ja $\text{syt}(2, 3) = 1$. Alkion $\overline{1}$ käänteisalkio on $\overline{1}$, sillä $\overline{1} \cdot \overline{1} = \overline{1}$. Alkion $\overline{2}$ käänteisalkio on $\overline{2}$, sillä $\overline{2} \cdot \overline{2} = \overline{2 \cdot 2} = \overline{4} = \overline{1}$. Käänteisalkiot ovat siis alkuluokilla $\overline{1}$ ja $\overline{2}$.

6.2.2 Symmetriset ryhmät

Olkoon $J_n = \{1, 2, 3, ..., n\}$ jokin äärellinen joukko. Tällaisen joukon *permutaatioksi* kutsutaan bijektiivistä kuvausta $\alpha : J_n \to J_n$. Olkoon j jokin joukon J_n alkio. Kun $\alpha\,(j) = l_j$, permutaatiota α voidaan merkitä

$$\alpha = \begin{pmatrix} 1 & 2 & ... & n \\ l_1 & l_2 & ... & l_n \end{pmatrix}.$$

Tässä siis alkiot $l_1, l_2, ..., l_n$ ovat luvut $1, 2, ..., n$ jossakin järjestyksessä. Joukon $J_n = \{1, 2, 3, ..., n\}$ permutaatiot muodostavat symmetrisen ryhmän bijektiivisen kuvaustulon suhteen. Muodostunutta ryhmää kutsutaan $n-$alkioisen joukon *symmetriseksi ryhmäksi*, jota merkitään

$$S_n = \{\alpha : J_n \to J_n \mid \alpha \text{ on bijektio}\}.$$

Muodostuneen symmetrisen ryhmän S_n ykkösalkiona on äärellisen joukon J_n identiteettikuvaus ja permutaation α käänteisalkiona käänteiskuvaus α^{-1}. Ryhmän S_n kertaluku eli alkioiden lukumäärä $\#S_n = n!$, sillä ryhmän S_n alkiot n voidaan asettaa $n!$ eri järjestykseen. [14] Silloin esimerkiksi ryhmässä S_3 on kuusi alkiota ($3!=3 \cdot 2 \cdot 1 = 6$), joita ovat $\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ ja $\alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

Esimerkki 6.10. Olkoon $n = 3$ eli nyt symmetriset ryhmät muodostuvat äärellisestä joukosta $J_3 = \{1, 2, 3\}$. Olkoon $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ ja $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Lasketaan ryhmien α ja β kuvaustulo.

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Kuvaustulo muodostetaan seuraavasti:

1) Ensin tarkastellaan ryhmää β eli lähdetään liikkeelle oikealta vasemmalle ja katsotaan miten siellä alkio 1 kuvautuu. Huomataan, että $1 \mapsto 3$.

2) Koska ryhmässä β alkio 1 kuvautui alkioksi 3 tarkastellaan ryhmän α alkion 3 kuvautumista. Nähdään, että $3 \mapsto 3$.

3) Yhdistämällä kohdat 1) ja 2) saadaan alkion 1 kuvautumisketjuksi $1 \mapsto 3 \mapsto 3$ eli muodostuneessa kuvaustulossa alkio 1 kuvautuu alkioksi 3.

Näin edetään myös lopuille alkioille. Eli $2 \mapsto 2 \mapsto 1$ ja $3 \mapsto 1 \mapsto 2$. Siis alkio 2 kuvautuu lopulta alkioksi 1 ja alkio 3 alkioksi 2.

Esimerkki 6.11. Merkitään ryhmässä S_3 $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ ja $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Silloin

$$\tau^2 = 1, \quad \sigma^3 = 1 \text{ ja } \tau\sigma\tau = \sigma^2.$$

Lasketaan kyseiset kuvaustulot edellisen esimerkin mukaan.

1) $\tau^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Tässä siis $1 \mapsto 2 \mapsto 1, 2 \mapsto 1 \mapsto 2$ ja $3 \mapsto 3 \mapsto 3$. Näin ollen alkiot kuvautuvat takaisin itsekseen, joten $\tau^2 = 1$.

2) $\sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Lähdetään oikealta liikkeelle ja lasketaan ensin kuvaustulo $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, sillä $1 \mapsto 2 \mapsto 3, 2 \mapsto 3 \mapsto 1$ ja $3 \mapsto 1 \mapsto 2$. Lasketaan lopullinen kuvaustulo $\sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Nyt $1 \mapsto 3 \mapsto 1, 2 \mapsto 1 \mapsto 2$ ja $3 \mapsto 2 \mapsto 3$. Jälleen alkiot kuvautuvat takaisin itselleen eli $\sigma^3 = 1$.

3) $\tau\sigma\tau = \sigma^2$. Kohdan 2) perusteella $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Lasketaan kuvaustulo $\tau\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ lähtien jälleen oikealta liikkeelle. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, sillä $1 \mapsto 2 \mapsto 3, 2 \mapsto 1 \mapsto 2$ ja $3 \mapsto 3 \mapsto 1$. Nyt $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} =$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma^2, \text{ sillä } 1 \mapsto 3 \mapsto 3, 2 \mapsto 2 \mapsto 1 \text{ ja } 3 \mapsto 1 \mapsto 2.$$

Tiedetään, että ryhmällä S_3 on $3! = 3 \cdot 2 \cdot 1 = 6$ alkiota. Voidaan todeta esimerkiksi laskemalla, että nämä alkiot ovat ovat $S_3 = \{1, \tau, \sigma, \sigma\tau, \sigma^2, \sigma^2\tau\}$, jolloin ne osoittautuvat erisuuriksi. [14] Tämän toteaminen on harjoitustehtävänä luvun lopussa.

On olemassa myös helpompi tapa osoittaa edellä mainitun esimerkin alkioiden olevan erisuuret. Otetaan avuksi seuraava lause, jonka todistus on harjoitustehtävänä.

Lause 6.12. Olkoon K ryhmä. Kun a ja b ovat joitakin ryhmän K alkioita, niin

a) yhtälöllä $ax = b$ on ryhmässä K yksikäsitteinen ratkaisu $x = a^{-1}b$;

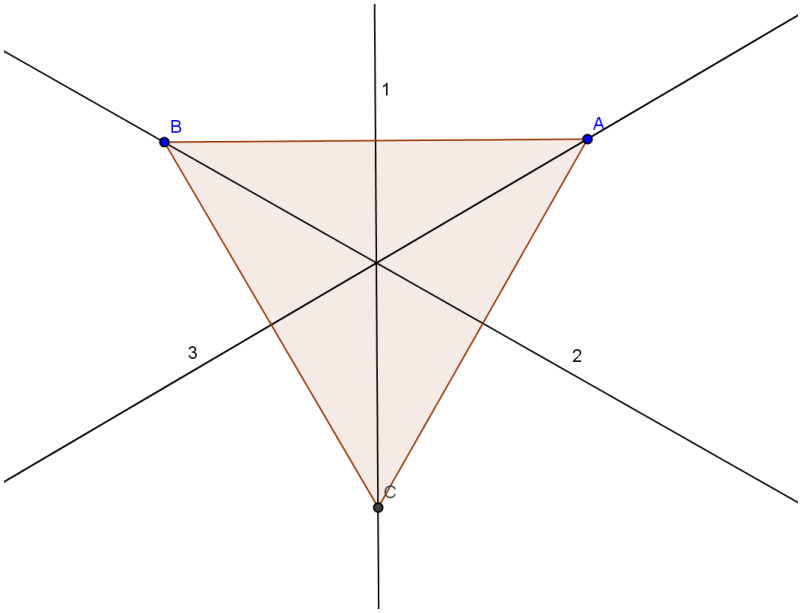
b) yhtälöllä $xa = b$ on ryhmässä K yksikäsitteinen ratkaisu $x = ba^{-1}$.

Esimerkki 6.13. Permutaatioryhmien avulla voidaan tarkastella monikulmioiden symmetriaa. Tarkastellaan esimerkiksi tasasivuista kolmioita ja sellaisia tason etäisyyden säilyttäviä kuvauksia, jotka kuvaavat kyseisen kolmion itselleen. Kierrot kulman 0°, 120° ja 240° verran kolmion keskipisteen ympäri ovat tällaisia kuvauksia sekä peilaukset alla olevan kuvan keskinormaaleissa 1, 2 ja 3. Kuvassa (seuraavalla sivulla) kolmion kärkiä merkitään symboleilla A, B ja C. Tällöin kyseiset symmetriakuvaukset ovat seuraavat permutaatiot:

$$\alpha_{0^\circ} = \begin{pmatrix} 1 & 2 & 3 \\ A & B & C \end{pmatrix}, \ \alpha_{120^\circ} = \begin{pmatrix} 1 & 2 & 3 \\ B & C & A \end{pmatrix}, \ \alpha_{240^\circ} = \begin{pmatrix} 1 & 2 & 3 \\ C & A & B \end{pmatrix},$$

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ A & C & B \end{pmatrix}, \ \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ B & A & C \end{pmatrix} \text{ ja } \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ C & B & A \end{pmatrix}.$$

Nämä edellä mainitut kuvaukset muodostavat ryhmän S_3, jota kutsutaan kyseisen kolmion symmetriaryhmäksi. Oletettavasti mitä säännöllisempi kuvio on kyseessä sitä suurempi on myös sen symmetriaryhmä. Erityisesti



Kuva 11: Tasasivuinen kolmio muodostaa symmetriaryhmän.

kemiassa ja fysiikassa käytetään kyseistä teoriaa molekyylien symmetriatarkasteluissa. [19]

6.2.3 Ryhmätaulu

Ryhmätaulujen avulla pystytään havainnollistamaan tehokkaasti *äärellisessä* ryhmässä tapahtuvia operaatioita ja algebrallista rakennetta. Tällaisia ovat esimerkiksi yhteenlasku ja kertolasku. Ryhmätauluun muodostuu selkeästi kyseessä olevan ryhmän alkiot operaatiosta riippuen. Taulukossa vaaka- ja pystyriveille merkitään ryhmän alkiot ja jokaiseen risteyskohtaan muodostuu kyseisestä operaatiosta saatu alkio. Esimerkiksi jäännösluokka $\mathbb{Z}_2$ muodostuu alkioista $\overline{0}$ ja $\overline{1}$. Muodostetaan additiivisen ryhmän $(\mathbb{Z}_2, +)$ ryhmätaulu. [17]

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

Additiivisessa ryhmässä $(\mathbb{Z}_2, +)$ on siis voimassa operaatiot $\overline{0} + \overline{0} = \overline{0}$, $\overline{0} + \overline{1} = \overline{1}$, $\overline{1} + \overline{0} = \overline{1}$ ja $\overline{1} + \overline{1} = \overline{0}$.

Esimerkki 6.14. Muodostetaan multiplikatiivisen ryhmän $(\mathbb{Z}_3^*, \cdot)$ ryhmätaulu. Tämän jäännösluokkaryhmän alkioita ovat ainoastaan alkiot $\overline{1}$ ja $\overline{2}$.

$\cdot$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{1}$

Multiplikatiivisessa ryhmässä $(\mathbb{Z}_3^*, \cdot)$ on siis voimassa operaatiot $\overline{1} \cdot \overline{1} = \overline{1}$, $\overline{1} \cdot \overline{2} = \overline{2}$, $\overline{2} \cdot \overline{1} = \overline{2}$ ja $\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$.

Esimerkki 6.15. Muodostetaan tässä esimerkissä ryhmätaulu jäännösluokasta $\mathbb{Z}_5$ ja yhteenlaskuoperaatiota $+$. Tässä siis lasketaan yhteen jäännösluokan $\mathbb{Z}_5$ alkioita $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ ja $\overline{4}$. [17]

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Taulukossa on laskettu yhteen esimerkiksi alkiot $\overline{1}$ ja $\overline{2}$, jolloin jäännösluokassa $\mathbb{Z}_5$ saadaan $\overline{1} + \overline{2} = \overline{3}$. Jos suoritetaan yhteenlasku alkioille $\overline{2}$ ja $\overline{3}$, niin saadaan $\overline{2} + \overline{3} = \overline{5} = \overline{0}$ jäännösluokassa $\mathbb{Z}_5$.

6.3 Aliryhmät

Olkoon $\mathbb{Q}^*$ nollasta eroavien rationaalilukujen ryhmä tavallisen kertolaskun suhteen. Näin ollen ryhmä $\mathbb{Q}^*$ sisältää nollasta eroavien reaalilukujen ryhmän $\mathbb{R}^*$ tavallisen kertolaskun suhteen. Jos ryhmän osajoukko on itsessään ryhmä alkuperäisen ryhmän operaation suhteen, niin osajoukkoa sanotaan *aliryhmäksi*. Tässä siis ryhmä $\mathbb{R}^*$ on ryhmän $\mathbb{Q}^*$ *aliryhmä*.

Määritelmä 6.16 (Aliryhmä)**.** Olkoon G ryhmä. Epätyhjä joukko H on ryhmän G aliryhmä, jos joukko H on ryhmä ryhmässä G määritellyn operaation suhteen. Merkitään $H \leq G$. Jos $H \neq G$, niin ryhmä H on ryhmän G

aito aliryhmä. Tätä merkitään $H < G$. [17]

Aliryhmän määritelmä voidaan esittää myös toisin. Jos H on ryhmän G osajoukko ja jos H on ryhmä ryhmän G binäärioperaation $G \times G \longrightarrow G$ restriktion suhteen, niin ryhmä H on ryhmän G *aliryhmä*.

Lause 6.17. Muutetaan edellinen määritelmä 6.12 lauseeksi ja todistetaan se.

Kun G on ryhmä ja H sen osajoukko, niin joukko H on ryhmän G aliryhmä täsmälleen silloin, kun seuraavat ehdot toteutuvat:

A1. Olkoot c ja d joukon H alkioita. Jos $a, b \in H$, niin myös $ab \in H$.

A2. Ryhmän G ykkösalkio 1_G on myös joukon H ykkösalkio.

A3. Olkoon b jokin joukon H alkio. Tällöin myös käänteisalkio b^{-1} on joukon H alkio.

Todistus on esitettävä kahdessa osassa. Ensin oletetaan, että ryhmä H on ryhmän G aliryhmä eli $H \leq G$ ja tutkitaan toteutuvatko ehdot A1-A3. Tämä ei kuitenkaan vielä riitä, vaan on myös todistettava väite toiseen suuntaan. Toisessa osassa oletetaan ehtojen A1-A3 olevan voimassa ja tutkitaan niiden perusteella onko ryhmä H ryhmän G aliryhmä. Tämä suunta on edellistä suoraviivaisempi todistaa.

Todistus. Oletetaan, että ryhmä H on ryhmän G aliryhmä. Käydään läpi ehdot A1-A3.

A1. Koska oletuksen mukaan ryhmä H on ryhmän G aliryhmä, niin ryhmän G binäärioperaatio $G \times G \longrightarrow G$ antaa rajoittumana binäärioperaation eli kuvauksen $H \times H \longrightarrow H$. Siis ehto A1 on voimassa.

A2. Osoitetaan, että ryhmän G ja ryhmän H ykkösalkiot ovat samat eli $1_G = 1_H$, jolloin ehto A2 seuraa. Kun lasketaan ryhmässä H tulo $1_H 1_H = 1_H$, niin tämä yhtäsuuruus on voimassa myös ryhmässä G,

sillä ykkösalkioiden oletettiin olevan samat. Siis ykkösalkio 1_H toteuttaa ryhmässä G yhtälön $x^2 = x$ ($1_H 1_H = 1_H$). Ainoa ryhmän G alkio, joka toteuttaa kyseisen yhtälön, on $x = 1_G$. Nimittäin kun kerrotaan yhtälö $x^2 = x$ puolittain termillä x^{-1}, niin saadaan $x = 1_G$. Nyt siis $1_G = 1_H$ ja ehto A2 toteutuu.

A3. Oletetaan, että c on jokin ryhmän H alkio ja d alkion c käänteisalkio ryhmässä H. Nyt $cd = dc = 1_H = 1_G$, joten alkio d on alkion c käänteisalkio myös ryhmässä G. Käänteisalkion yksikäsitteisyyden nojalla $c^{-1} = d \in H$. Siis ehto A3 toteutuu.

Oletetaan toiseksi, että ehdot A1-A3 ovat voimassa. Ehdon A1 perusteella ryhmän G binäärioperaatio antaa rajoittumana binäärioperaation ryhmälle H. Koska assosiatiivilaki on voimassa ryhmässä G, niin se on voimassa myös ryhmässä H. Ehdon A2 perusteella ryhmässä H on ykkösalkio. Tämän ykkösalkio on siis juurikin 1_G. Ehdon A3 mukaan jokaisella ryhmän H alkiolla on käänteisalkio ryhmässä H ja tämä käänteisalkio on täsmälleen sama kuin ryhmän G käänteisalkio. Näin ollen siis $H \leq G$. [14] □

Lause 6.18 (Aliryhmäkriteeri)**.** Olkoon K ryhmä ja H sen epätyhjä osajoukko eli $H \subseteq K$.

i) Olkoon ryhmä K äärellinen ja a, b joitakin osajoukon H alkioita. Jos $ab \in H$ kaikilla osajoukon alkioilla a ja b, niin osajoukko H on ryhmän K aliryhmä.

ii) Olkoot c ja d joitakin osajoukon H alkioita. Jos $cd^{-1} \in H$ kaikilla osajoukon alkioilla c ja d, niin osajoukko H on ryhmän K aliryhmä.

Todistus. i) Valitaan jokin osajoukon H alkio s. Saadaan oletuksen nojalla $1_K = ss^{-1} \in H$. Kun a, b ovat joitakin osajoukon H alkioita, niin $b^{-1} = 1_G b^{-1} \in H$, joten $ab = a\left(b^{-1}\right)^{-1} \in H$. Nyt aliryhmän määritelmän ehdot ovat voimassa, joten $H \leq K$.

ii) Olkoon ryhmä K äärellinen ja cd jokin osajoukon H alkio kaikilla osajoukon H alkioilla c ja d. Osoitetaan, että kun $d \in H$, niin myös käänteisalkio $d^{-1} \in H$. Tällöin seuraa, että $cd^{-1} \in H$ ja väite saadaan edellisestä kohdasta i). Kun d on jokin osajoukon H alkio, niin $d, d^2, d^3... \in H$. Koska ryhmä K on oletuksen mukaan äärellinen, niin jotkin alkioista d^i $(i = 1, 2, 3...)$ ovat samoja. Olkoon $d^k = d^j$, missä $k > j > 0$. Kertomalla yhtälö puolittain alkiolla d^{-j} saadaan $d^{k-j} = 1_K$ ja kertomalla vielä alkiolla d^{-1} saadaan $d^{-1} = d^{k-j-1} \in H$. [14]

□

Esimerkki 6.19. Olkoot $H = (\mathbb{Z}, +)$ ja $G = (\mathbb{R}, +)$ additiivisia ryhmiä. Osoitetaan, että ryhmä H on ryhmän G aliryhmä tarkistamalla ehdot A1-A3.

Todistus. A1. Olkoot a ja b joitakin ryhmän H alkioita eli kokonaislukuja. Nyt myös kokonaislukujen a ja b summa on kokonaisluku eli $a + b = c$, joten myös alkio c kuuluu ryhmään H ja ehto A1 toteutuu.

A2. Olkoon a ryhmän H jokin alkio ja b jokin ryhmän G alkio. Nyt yksikösalkiona (tässä pikemminkin neutraalialkiona) toimii alkio 0, sillä $a + 0 = 0 + a = a$. Neutraalialkio 0 toteutuu myös ryhmässä G, sillä $b + 0 = 0 + b = 0$. Nyt siis $0_H + 0_G = 0$ ja ehto A2 toteutuu.

A3. Olkoon c jokin ryhmän H alkio. Koska on kyse additiivisista ryhmistä, niin käänteisalkiona toimii ryhmän H alkion c vastaluku $-c$. Nyt $c + (-c) = 0_H = 0_G$, joten alkio $-c$ on alkion c käänteisalkio myös ryhmässä G. Tällöin ehto A3 toteutuu.

Ehdot A1-A3 toteutuivat, joten ryhmä H on ryhmän G aliryhmä. □

Esimerkki 6.20. Jokaisessa ryhmässä G on niin sanotut *triviaalit* aliryhmät $\{1\}$ ja G itsessään. [17]

6.4 Ryhmäteorian harjoitustehtäviä

Harjoitustehtävä 6.1. Hahmottele kuvio seuraavista symmetriamuodoista:

a) rotaatiosymmetria,

b) translaatiosymmetria ja

c) molemminpuolinen symmetria, peilaus.

Harjoitustehtävä 6.2. Määritellään kokonaislukujen joukossa $\mathbb{Z}$ uusi binäärirelaatio Δ asettamalla $a\Delta b = a + b + 1$, kun a ja b ovat joitakin kokonaislukuja. Osoita, että $(\mathbb{Z}, \Delta)$ on Abelin ryhmä.

Harjoitustehtävä 6.3. Onko $(\mathbb{Z}_{15}, \cdot)$ ryhmä? Entä $(\mathbb{Z}_{15}^*, +)$?

Harjoitustehtävä 6.4. Olkoon $\mathbb{Z}_5 = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\right\}$ multiplikatiivinen ryhmä ja $\mathbb{Z}_5^* = \left\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\right\}$. Millä alkuluokilla on käänteisalkio?

Harjoitustehtävä 6.5. Olkoon ryhmässä S_4 $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ ja $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$. Laske kuvaustulo $\alpha\beta\alpha$.

Harjoitustehtävä 6.6 (Kielentämistehtävä)**.** Tehtävänä on todistaa lause 6.12 laittamalla annetut todistuksen osat oikeaan järjestykseen. Lause 6.12 on muotoa

Olkoon K ryhmä. Kun a ja b ovat joitakin ryhmän K alkioita, niin

a) *yhtälöllä $ax = b$ on ryhmässä K yksikäsitteinen ratkaisu $x = a^{-1}b$;*

b) *yhtälöllä $xa = b$ on ryhmässä K yksikäsitteinen ratkaisu $x = ba^{-1}$.*

Todistetaan ensin a) -kohta eli osat 1)-6) ja sen jälkeen b) -kohta järjestämällä osat i)-vi). Todistukseen kuuluvat ovat osat sattumanvaraisessa järjestyksessä:

1) koska $a\,(a^{-1}b) = b$.

2) Kääntäen, $x = a^{-1}b$

3) Kertomalla yhtälö $ax = b$

4) saadaan $x = a^{-1}b$.

5) vasemmalta alkiolla a^{-1}

6) toteuttaa yhtälön $ax = b$,

ja

i) toteuttaa yhtälön $xa = b$,

ii) Kertomalla yhtälö $xa = b$

iii) Kääntäen, $x = ba^{-1}$

iv) saadaan $x = ba^{-1}$.

v) oikealta alkiolla a^{-1}

vi) koska $(ba^{-1})\,a = b$.

Harjoitustehtävä 6.7 (Kielentämistehtävä)**.** Olkoon S_3 ryhmä, jossa $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ ja $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Silloin $\tau^2 = 1, \sigma^3 = 1$ ja $\tau\sigma\tau = \sigma^2$, mikä perusteltiin esimerkissä 6.11. Osoita, että ryhmän $S_3 = \{1, \tau, \sigma, \sigma\tau, \sigma^2, \sigma^2\tau\}$ alkiot ovat erisuuria. Liitä vastaukseesi selkeät perustelut kokonaisilla virkkeillä ratkaisun edetessä. (Vihje: Edellistä lausetta käytettäessä ei tarvitse laskea kuvaustuloja.)

Harjoitustehtävä 6.8. Olkoot edelleen S_3, τ ja σ kuten edellisessä tehtävässä. Saata tulot $(\sigma\tau)\,(\sigma^2)$ ja $(\sigma^2\tau)\,(\sigma\tau)$ johonkin seuraavista muodoista

$$1, \tau, \sigma, \sigma\tau, \sigma^2, \sigma^2\tau$$

käyttäen ainoastaan ominaisuuksia $\tau^2 = 1$, $\sigma^3 = 1$ ja $\sigma\tau\sigma = \sigma^2$.

Harjoitustehtävä 6.9. Muodosta multiplikatiivisen ryhmän $(\mathbb{Z}_4^*, \cdot)$ ryhmätaulu. Mitkä ovat kyseisen jäännösluokkaryhmän alkiot?

Harjoitustehtävä 6.10. Olkoot $K = (\mathbb{Z}, +)$ ja $H = (2\mathbb{Z}, +)$. Osoita aliryhmän määritelmän avulla, että ryhmä H on ryhmän K aliryhmä eli $H \leq K$.

Harjoitustehtävä 6.11 (Kielentämistehtävä)**.** Tehtävänä on todistaa seuraava lause täyttämällä puuttuvat aukot todistuksesta. Lauseen todistuksessa tarvitaan lausetta 6.18.

Olkoon K ryhmä ja $\{H_i \mid i \in I\}$ ryhmän K aliryhmien joukko (tässä indeksit i kuuluvat erääseen joukkoon I). Tällöin aliryhmien joukon leikkaus $\underbrace{\cap}_{i \in I} H_i$ on myös ryhmän K aliryhmä.

Todistus. Merkitään $H = \underbrace{\cap}_{i \in I} H_i$. Koska jokainen 1._____ on aliryhmä, sisältävät ne ryhmän 2._____ ykkösalkion 1. Tällöin 3._____, joten ryhmä H on epätyhjä. Olkoon nyt x ja y joitakin ryhmän H alkioita. Tällöin x, y 4._____ kaikilla indeksin i arvoilla. Lauseen 6.18 perusteella 5._____ $\in H_i \ \forall \ i$. Näin ollen 6._____ $\in H$, joten lauseen 6.18 mukaan joukko H on ryhmän K 7._____. □

7 Harjoitustehtävien malliratkaisut

7.1 Joukko-opin harjoitustehtävien malliratkaisut

Harjoitustehtävä 4.1

Tehtävänä oli muodostaa annetun joukon $U = \{10, 20, 30, 40, 50, 60, 70\}$ neljä osajoukkoa. Tällaisia osajoukkoja ovat mitkä tahansa joukot, jotka sisältävät joitakin alkioita joukosta U. Merkitään joukon U osajoukkoja A, B, C ja D. Esimerkiksi $A = \{20, 30, 40, 50\}$, $B = \{10, 40\}$, $C = \{20, 50, 70\}$ ja $D = \{10, 30, 50, 70\}$.

Harjoitustehtävä 4.2

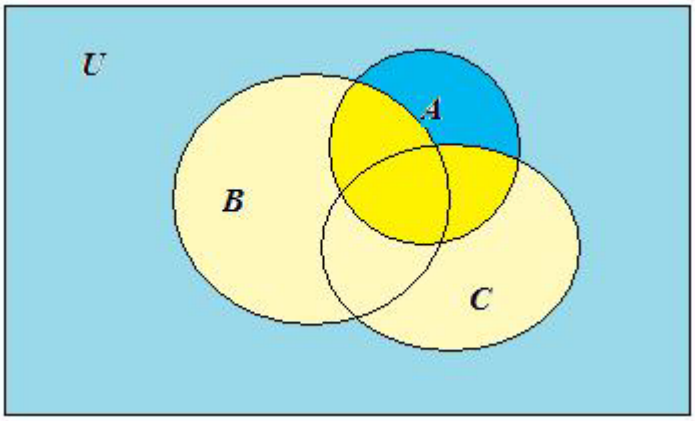
i) $A \cup B = \{1, 2, 5, 6, 7, 8, 9, 10\}$. Kyseessä on osajoukkojen A ja B muodostama *unioni*, johon siis lasketaan kaikki osajoukkojen A ja B alkiot, jotka kuuluvat jompaan kumpaan osajoukkoon tai molempiin osajoukkoihin. On kuitenkin syytä huomata, että alkiot esiintyvät unionissa vain kerran.

ii) $A \cap B = \{2, 5, 10\}$. Osajoukkojen A ja B *leikkaus* muodostuu osajoukkojen A ja B yhteisistä alkioista.

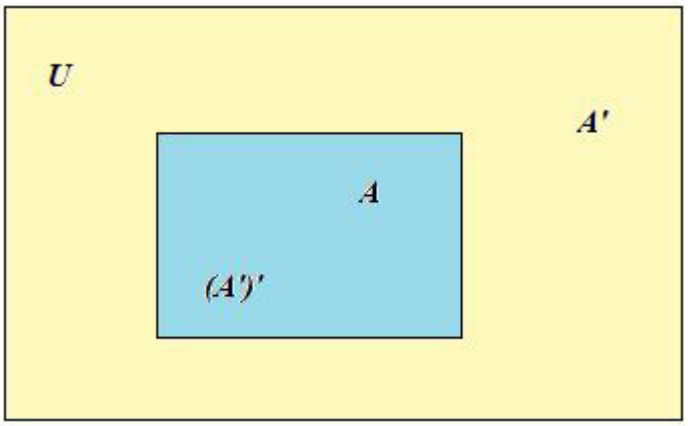
iii) $(A \cap B)' = \{1, 3, 4, 6, 7, 8, 9\}$. Osajoukkojen A ja B leikkauksen *komplementtijoukko* muodostuu osajoukkojen A ja B leikkauksen ulkopuolisista alkioista.

Harjoitustehtävä 4.3

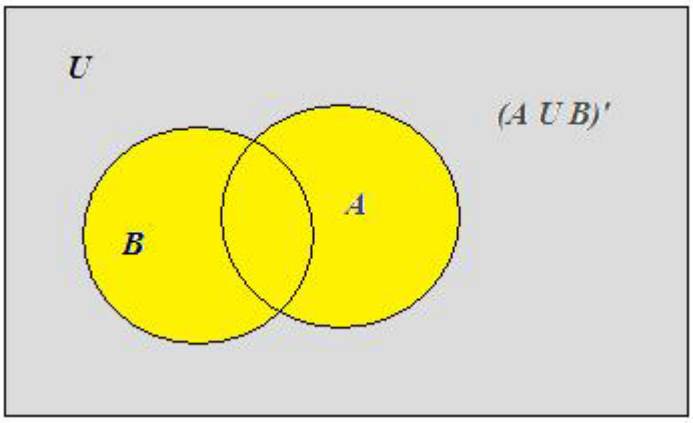
Kaikissa Venn -diagrammeissa joukko U on joukkojen A, B ja C universaalijoukko.



Kuva 12: a) Keltaisella väritetty alue kuvaa operaatiota $A \cap (B \cup C)$.



Kuva 13: b) Kuvassa näkyy joukon A komplementin komplementti, joka itseasissa on joukko A.



Kuva 14: c) $(A \cup B)$'.

Tehtävässä oli myös kerrottava omin sanoin, mitä edellä mainitut merkinnät tarkoittavat.

a) $A \cap (B \cup C)$ = Joukon A leikkaus joukkojen B ja C unionin kanssa.

b) $(A')' = A$ = Joukon A komplementin komplementti on joukko A itse.

c) $(A \cup B)'$ = Joukkojen A ja B unionin komplementti.

Harjoitustehtävä 4.4

Olkoot A ja B perusjoukon X osajoukkoja. Todista De Morganin laki, joka on muotoa $(A \cap B)' = A' \cup B'$ täyttämällä todistuksesta puuttuvat aukot.

Todistus. Olkoon $x \in X$. Nyt $x \in 1.\ \underline{(A \cap B)'}$

$$\begin{aligned} &\iff x\ 2.\ \underline{\notin}\ A \cap B \\ &\iff x \notin A \text{ tai } x\ 3.\ \underline{\notin}\ B \\ &\iff x \in\ 4.\ \underline{A'} \text{ tai } x\ \in 5.\ \underline{B'} \\ &\iff x \in\ 6.\ \underline{A' \cup B'}. \end{aligned}$$

Siis $(A \cap B)' = A' \cup B'$. □

Harjoitustehtävä 4.5

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

Todistus. Todistetaan edellä mainittu kaava oikeaksi osoittamalla sisältyvyys molempiin suuntiin. Tutkitaan ensin $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$:

Jos $A \cap (B \cup C) = \emptyset$ eli tyhjä joukko, niin asia on selvä. Olkoon sitten x mielivaltainen joukon $A \cap (B \cup C)$ alkio. Leikkauksen määritelmän mukaan $x \in A$ ja $x \in B \cup C$, josta edelleen unionin määritelmän mukaan $x \in B$ tai $x \in C$. Nyt

$$\begin{aligned} &\text{jos } x\ \in\ B, \text{ niin } A \cap B\, (A \cap B) \cup (A \cap C) \text{ ja} \\ &\text{jos } x\ \in\ C, \text{ niin } A \cap C\, (A \cap B) \cup (A \cap C)\,. \end{aligned}$$

Siis molemmissa tapauksissa $x \in (A \cap B) \cup (A \cap C)$. Seuraavaksi tutkitaan toinen puoli $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. Jälleen jos $(A \cap B) \cup (A \cap C) = \emptyset$, niin asia on selvä. Olkoon x joukon $(A \cap B) \cup (A \cap C)$ mielivaltainen alkio. Unionin määritelmän mukaan $x \in A \cap B$ tai $x \in A \cap C$. Nyt

$$\begin{aligned} &\text{jos } x\ \in\ A \cap B, \text{ niin } x \in A \text{ ja } x \in B \subset B \cup C \text{ eli } x \in A \cap (B \cup C) \text{ ja} \\ &\text{jos } x\ \in\ A \cap C, \text{ niin } x \in A \text{ ja } x \in C \subset B \cup C \text{ eli } x \in A \cap (B \cup C)\,. \end{aligned}$$

Molemmissa tapauksissa siis $x \in A \cap (B \cup C)$. $\square$

Harjoitustehtävä 4.6

Merkitään määrittelyjoukkoa symbolilla C ja arvojoukkoa symbolilla D.

a) Tässä funktio on muotoa $f(x) = x^2$. Kyseiseen funktioon voidaan sijoittaa mitä tahansa reaalilukuja, jolloin se antaa arvoksi jonkin positiivisen reaaliluvun toiseen potenssiin korotuksen vuoksi. Näin ollen $C = \mathbb{R}$ ja $D = \mathbb{R}_+$.

b) Nyt funktio on muotoa $f(x) = \log_{10}(x)$. Tässä tapauksessa logaritmifunktioon voi syöttää vain positiivisia muuttujan x arvoja (x $>$ 0), joten $C = \mathbb{R}_+ \setminus \{0\}$. Logaritmifunktio voi saada mitä tahansa reaalilukuarvoja, joten $D = \mathbb{R}$.

c) Funktio on muotoa $f(x) = \frac{1}{x^2-3}$. Nyt on tärkeää huomioida, ettei nimittäjä voi saada arvoa nolla, sillä nollalla ei voi jakaa! Tämä siis rajaa kyseisen funktion määrittelyjoukon. Siis $x^2 - 3 \neq 0$. Haetaan siis funktion $g(x^2 - 3)$ nollakohdat.

$$\begin{aligned} x^2 - 3 &= 0 \\ x^2 &= 3 \\ x &= \pm\sqrt{3}. \end{aligned}$$

Nyt siis nollakohdat ovat $x_1 = -\sqrt{3}$ ja $x_2 = \sqrt{3}$, joten ne on rajattava pois määrittelyjoukosta. Näin ollen $C = \mathbb{R} \setminus \left\{-\sqrt{3}, \sqrt{3}\right\}$. Funktio $f(x) = \frac{1}{x^2-3}$ voi arvoikseen saada mitä tahansa reaalilukuja paitsi nollaa. Siis arvojoukko on $D = \mathbb{R} \setminus \{0\}$.

d) Tarkastellaan funktiota $f(x) = \cos x + \sin x$. Tunnetusti sekä kosinifunktion että sinifunktion määrittelyjoukko muodostuu reaaliluvuista ja arvojoukko on väli [-1,1]. Siis kyseisen funktion $f(x) = \cos x + \sin x$ määrittelyjoukko on $C = \mathbb{R}$, mutta tutkittaessa arvojoukkoa pitää olla

tarkkana. Kosinifunktio ja sinifunktio eivät tässä tapauksessa voi saada samanaikaisesti arvoa 1, sillä niillä on sama muuttuja x. Näin ollen siis arvojoukko on väli $D =$[-1,1].

Harjoitustehtävä 4.7

Tehtävänä on tutkia ovatko funktiot $f : \mathbb{R} \to \mathbb{R},\ f(x) = 5x + 9$ ja $g : \mathbb{R} \to \mathbb{R},\ g(x) = x^2$ bijektiivisiä. Funktiot ovat bijektioita täsmälleen silloin, kun ne ovat sekä injektioita että surjektioita. Tarkastellaan ensin funktiota $f(x) = 5x + 9$. Tarkastellaan a) -kohdassa surjektiivisuus ja b) -kohdassa injektiivisyys.

a) Olkoon d jokin reaaliluku. Tutkitaan onko olemassa sellaista muuttujaa c, joka kuuluu annetun funktion määrittelyjoukkoon $M_f = \mathbb{R}$ siten, että $f(c) = d$. Sijoitetaan muuttuja c funktioon $f(x)$ ja ratkaistaan yhtälö $f(c) = d$ muuttujan c suhteen.

$$\begin{aligned} 5c + 9 &= d \quad \text{Ratkaistaan yhtälöstä muuttuja } c. \\ 5c &= d - 9 \quad \text{Jaetaan luvulla 5.} \\ c &= \frac{d-9}{5}. \end{aligned}$$

Nyt muuttuja c on jokin reaaliluku eli se kuuluu annetun funktion $f(x) = 5x + 9$ määrittelyjoukkoon $M_f = \mathbb{R}$. Näin ollen funktio $f(x) = 5x + 9$ on surjektio.

b) Todetaan annetun funktion injektiivisyys vastaesimerkin kautta. Jos muuttujat a_1 ja a_2 ovat injektiivisyyden määritelmän vastaisesti erisuuria, niin

$$f(a_1) = 5a_1 + 9 \text{ ja } f(a_2) = 5a_2 + 9.$$

Nämä ovat eri arvoja, sillä muuten

$$\begin{aligned} 5a_1 + 9 &= 5a_2 + 9 \quad \text{Luvut 9 kumoavat toisensa.} \\ 5a_1 &= 5a_2 \quad \text{Jakamalla luvulla 5 saadaan} \\ a_1 &= a_2, \end{aligned}$$

jolloin syntyy ristiriita. Siis funktio $f(x) = 5x + 9$ on injektio.

Kohtien a) ja b) perusteella annettu funktio $f(x) = 5x + 9$ on bijektio.

Tarkastellaan vielä funktiota $g(x) = x^2$. Tämä funktio ei ole injektio, koska se saa saman arvon kahdella eri muuttujan x arvolla. Esimerkiksi $g(2) = 4 = g(-2)$. Toisaalta kyseinen funktio ei ole myöskään surjektio, sillä ei ole olemassa reaalilukua x, jolle $x^2 = -4$. Funktio $g(x) = x^2$ ei siis ole bijektio. Tämän osoittamiseksi riittää todeta jompi kumpi edellä mainituista seikoista.

Huom! Ratkaisussa vaadittiin selkeät kirjalliset selitykset ratkaisun edetessä.

Harjoitustehtävä 4.8

Oletetaan, että $y = f(x)$. Käänteisfunktio saadaan, kun ratkaistaan annetusta funktiosta muuttuja x muuttujan y suhteen.

a) Tarkastellaan funktiota $f(x) = \frac{x^2-4}{3}$ ($M_f = \mathbb{R}$, $A_f = \mathbb{R}$). Ratkaistaan funktiosta muuttuja x.

$$\begin{aligned} y &= \frac{x^2-4}{3} \\ 3y &= x^2 - 4 \\ 3y + 4 &= x^2 \\ x &= \pm\sqrt{3y+4}. \end{aligned}$$

Nyt siis käänteisfunktio $f(x)^{-1} = f(y) = \pm\sqrt{3y+4}$ ($M_{f^{-1}} = \left[-\frac{4}{3}, \infty\right)$, $A_f = \mathbb{R}$).

b) Nyt funktio on muotoa $f(x) = \log_{10}(x) - 6$ ($M_f = (0, \infty)$, $A_f = \mathbb{R}$). Ratkaistaan funktiosta muuttuja x.

$$\begin{aligned} y &= \log_{10}(x) - 6 \\ y + 6 &= \log_{10}(x) \\ x &= 10^{y+6}. \end{aligned}$$

Nyt siis käänteisfunktio $f(y) = 10^{y+6}$. Kun tehdään muuttujanvaihto, saadaan $f(x)^{-1} = 10^{x+6}$ ($M_{f^{-1}} = \mathbb{R}$, $A_{f^{-1}} = \mathbb{R}$).

Harjoitustehtävä 4.9

Nyt $f(x) = \sqrt{x} + 6$ ($M_f = [0, \infty)$, $A_f = [6, \infty)$), $g(x) = \frac{1}{x-1}$ ($M_g = \mathbb{R} \setminus \{1\}$, $A_g = \mathbb{R} \setminus \{0\}$) ja $h(x) = x^3 + 1$ ($M_h = \mathbb{R}$, $A_h = \mathbb{R}$).

i) $g(f(x)) = \frac{1}{\sqrt{x}+5} = k(x)$, ($M_k = [0, \infty)$, $A_k = \mathbb{R}_+$),

ii) $g(h(x)) = \frac{1}{x^3+1-1} = \frac{1}{x^3} = j(x)$, ($M_j = \mathbb{R} \setminus 0$, $A_j = \mathbb{R} \setminus 0$) ja

iii) $f(g(h(x))) = \sqrt{\frac{1}{x^3}} + 6 = \frac{1}{\sqrt{x^3}} + 6 = m(x)$, ($M_m = \mathbb{R}_+ \setminus \{0\}$, $A_m = \mathbb{R}_+ \setminus \{0\}$).

Harjoitustehtävä 4.10

Tehtävässä annettiin kaksi joukkoa $C = \{5, 11, 13\}$ ja $D = \{e, f, g\}$. Tarkoitus on laskea karteesinen tulo $C \times D$.

$C \times D = \{(5, e), (5, f), (5, g), (11, e), (11, f), (11, g), (13, e), (13, f), (13, g)\}$.

$D \times C = \{(e, 5), (e, 11), (e, 13), (f, 5), (f, 11), (f, 13), (g, 5), (g, 11), (g, 13)\}$.

Koska joukot C ja D sisältävät eri alkiot, niin $C \times D \neq D \times C$ eli tässä karteesiset tulot eivät ole kommutatiivisia. Tällöin järjestetyt parit kääntyvät.

Harjoitustehtävä 4.11

Tehtävässä on tarkoitus tutkia onko relaatio $S = \{(x, y) \mid x \sim y\}$, jossa $x \sim y$ tarkoittaa luvun y jakamista luvulla x, ekvivalenssirelaatio. Käydään läpi ekvivalenssirelaation määritelmän ehdot E1-E3.

E1 Koska nollalla ei voi jakaa, ei ole voimassa $0\ S\ 0$. Näin ollen refleksiivisyys ei toteudu.

E2 Luku 2 jakaa luvun 4, sillä $\frac{4}{2} = 2$. Nyt siis $2\ S\ 4$. Luku 4 ei kuitenkaan jaa lukua 2, joten ei ole voimassa $4\ S\ 2$. Näin ollen symmetrisyys ei toteudu.

E3 Transitiivisuuden osoittamiseksi oletetaan, että muuttujat a, b ja c ovat joitakin kokonaislukuja ja $a\ S\ b$ sekä $b\ S\ c$. Nyt siis luku a jakaa luvun b ja luku b jakaa luvun c, joten on olemassa sellaiset kokonaisluvut k ja l, jolloin $b = ak$ ja $c = bl$. Tämän perusteella $c = bl = (ak)\, l = a\,(kl)$. Näin ollen siis myös $a\ S\ c$ ja transitiivisuus toteutuu.

Ekvivalenssirelaation määritelmän ehdoista ainoastaa ehto E3 toteutui. Tämän perusteella siis relaatio $S = \{(x, y) \mid x \sim y\}$ ei ole ekvivalenssirelaatio. Tehtävässä olisi riittänyt osoittaa ehdon E1 tai ehdon E2 perusteella, ettei relaatio ole ekvivalenssirelaatio. Ekvivalenssirelaation olemassaoloon nimittäin vaaditaan kaikkien kolmen ehdon toteutuminen.

Harjoitustehtävä 4.12

Tehtävässä tarkastellaan relaatiota $R = \{(x, y) \mid x \sim y\}$, jossa $x \sim y$ tarkoittaa, että $x - y \in \mathbb{Z}$ eli lukujen x ja y erotus on kokonaisluku. Tarkoitus on osoittaa, että kyseinen relaatio on ekvivalenssirelaatio eli se toteuttaa ekvivalenssirelaation määritelmän ehdot E1-E3.

Todistus. E1 Olkoon x jokin reaaliluku. Nyt $x - x = 0$ ja luku 0 kuuluu kokonaislukuihin, joten $x\ R\ x$. Näin ollen refleksiivisyys siis toteutuu.

E2 Symmetrisyyden osoittamiseksi oletetaan, että muuttuja a ja b ovat joitakin reaalilukuja ja $a\ R\ b$. Silloin lukujen a ja b erotuksena saadaan jokin kokonaisluku m eli $a - b = m \in \mathbb{Z}$. Nyt $b - a = -(a - b) = -m \in Z$, joten $b\ R\ a$ ja symmetrisyys toteutuu.

E3 Transitiivisuuden osoittamiseksi oletetaan, että muuttujat a, b ja c ovat joitakin reaalilukuja ja $a\ R\ b$ sekä $b\ R\ c$. Silloin $a - b = m \in \mathbb{Z}$ ja $b - c = n \in \mathbb{Z}$. Nyt $a - c = (a - b) + (b - c) = m + n$. Koska muuttujat

m ja n ovat kokonaislukuja, niin myös niiden yhteenlasku $m + n$ on kokonaisluku eli $a - c \in Z$. Siis $a \; R \; c$ ja transitiivisuus toteutuu.

Relaatio $R = \{(x, y) \mid x \sim y\}$ toteutti ehdot E1-E3, joten se on ekvivalenssirelaatio. □

Harjoitustehtävä 4.13

Tehtävässä tarkastellaan kokonaislukujen joukossa relaatiota $\sim$. Olkoot a ja b joitakin kokonaislukuja. Nyt $a \sim b$ tarkoittaa, että lukujen a ja b yhteenlasku on jaollinen luvulla 2 eli $2 \mid a + b$. Tarkoitus on muodostaa alkion a ekvivalenssiluokka $[a]$ ja ensinnäkin todeta, että kyseinen relaatio on ekvivalenssirelaatio. Todistetaan tämä tutkimalla ekvivalenssirelaation määritelmän ehdot E1-E3.

E1 Olkoon a jokin kokonaisluku. Nyt $a + a = 2a \in Z$, joka on jaollinen luvulla 2. Näin ollen $a \sim a$ ja refleksiivisyys toteutuu.

E2 Olkoot a ja b joitakin kokonaislukuja ja $a \sim b$. Luku $a + b \in \mathbb{Z}$ on jaollinen luvulla 2 silloin ja vain silloin, kun $a+b = 2k$, missä k on jokin kokonaisluku. Nyt siis $b + a = 2k$ ja $b \sim a$. Näin ollen symmetrisyys toteutuu.

E3 Olkoot a, b ja c joitakin kokonaislukuja ja $a \sim b$ sekä $b \sim c$. Silloin $a + b = 2k$, missä k on jokin kokonaisluku ja $b + c = 2l$, missä l on jokin kokonaisluku. Nyt $a + c = 2k - b + 2l - b = 2k + 2l - 2b = 2\,(k + l - b) \in \mathbb{Z}$, joka on jaollinen luvulla 2. Näin ollen siis myös $a \sim c$ ja transitiivisuus toteutuu.

Nyt relaatio $\sim$ toteuttaa kaikki ekvivalenssirelaation määritelmän ehdot, joten se on ekvivalenssirelaatio. Koska alkio a voidaan myös esittää muodossa $a = 2k - b$, niin alkion a ekvivalenssiluokka on tällöin

$$[a] = \{b \in \mathbb{Z} \mid b \sim a\} = \{b + 2k \mid k \in \mathbb{Z}\}\,.$$

7.2 Lukuteorian harjoitustehtävien malliratkaisut

Harjoitustehtävä 5.1

i) Koska $52 = 2 \cdot 26$ eli $\frac{52}{26} = 2$, niin $2 \mid 52$.

ii) Jakamalla luku 73 luvulla 3 ei saada tasalukua, joten $3 \nmid 73$.

iii) Koska $252 = 12 \cdot 21$ eli $\frac{252}{21} = 12$, niin $12 \mid 252$.

iv) Jakamalla luku 117 luvulla 5 ei saada tasalukua, joten $5 \nmid 117$.

Harjoitustehtävä 5.2

a) $441 = 3 \cdot 147 = 3 \cdot 21 \cdot 7 = 3 \cdot 3 \cdot 7 \cdot 7 = 3^2 \cdot 7^2$.

b) $237 = 3 \cdot 79$. Tässä luku 79 on alkuluku eli sitä ei saada hajotetuksi.

c) $1100 = 11 \cdot 100 = 11 \cdot 10 \cdot 10 = 11 \cdot 2 \cdot 5 \cdot 2 \cdot 5 = 2^2 \cdot 5^2 \cdot 11$.

d) $876 = 3 \cdot 292 = 3 \cdot 2 \cdot 146 = 3 \cdot 2 \cdot 2 \cdot 73 = 2^2 \cdot 3 \cdot 73$.

Harjoitustehtävä 5.3

Tässä tehtävässä suurimman yhteisen tekijän löytämiseksi on ensin selvitettävä molempien lukujen alkutekijähajotelmat. Lasketaan ensin luvun 207 alkutekijähajotelma:

$$\begin{aligned} 207 &= 3 \cdot 69 \quad \text{Seuraavaksi lasketaan luvun 69 alkutekijähajotelma} \\ 69 &= 3 \cdot 23 \quad \text{ja jatketaan niin kauan kunnes päädytään alkulukuun.} \\ 23 &= 1 \cdot 23. \text{ Nyt luku 23 on alkuluku, joten laskeminen päättyy.} \end{aligned}$$

Nyt luvun 207 alkutekijä hajotelma muodostuu niistä kertoimista, jotka ovat alkulukuja eli $207 = 3 \cdot 3 \cdot 23 = 3^2 \cdot 23$. Lasketaan seuraavaksi vielä luvun 871

alkutekijähajotelma samalla tavalla kuin luvun 207:

$$\begin{aligned} 871 &= 13 \cdot 67 \\ 67 &= 1 \cdot 67. \end{aligned}$$

Luvun 871 alkutekijähajotelma on siis $13 \cdot 67$. Kertoimista nähdään, ettei luvuilla 207 ja 871 ole muita yhteisiä tekijöitä kuin luku 1. Näin ollen suurin yhteinen tekijä syt(207,871)=1.

Huom! Ratkaisussa vaadittiin selkeät kirjalliset selitykset ratkaisun edetessä.

Harjoitustehtävä 5.4

Lasketaan syt(120,440) Eukleideen algoritmin avulla.

$$\begin{aligned} 440 &= 3 \cdot 120 + 80 \\ 120 &= 1 \cdot 80 + 40 \\ 80 &= 2 \cdot 40 + 0. \end{aligned}$$

Nyt suurin yhteinen tekijä syt(120,440) nähdään viimeisestä jakojäännöksestä eli syt(120,440)=40.

Lasketaan vielä pyj(120,440). Pienin yhteinen jaettava saadaan kaavalla:

$$\text{pyj}(120,440) = \frac{120 \cdot 440}{\text{syt}(120,440)} = \frac{52800}{80} = 660.$$

Harjoitustehtävä 5.5

Lasketaan syt(132,333) ensin lukujen alkutekijähajotelmien avulla. Ensin luvun 101 alkutekijähajotelma:

$$\begin{aligned} 132 &= 2 \cdot 66 \\ 66 &= 3 \cdot 22 \\ 22 &= 2 \cdot 11 \\ 11 &= 1 \cdot 11. \end{aligned}$$

Luvun 132 alkutekijähajotelma saadaan kertoimista eli $132 = 2^2 \cdot 3 \cdot 11$. Seuraavaksi luvun 333 alkutekijähajotelma:

$$\begin{aligned} 333 &= 3 \cdot 111 \\ 111 &= 3 \cdot 37 \\ 37 &= 1 \cdot 37. \end{aligned}$$

Luvun 333 alkutekijähajotelma on $333 = 3^2 \cdot 37$. Nyt suurin yhteinen tekijä syt(132,333) nähdään alkutekijähajotelmien yhteisistä kertoimista. Luvuilla 132 ja 333 on luku 3 yhteisenä kertoimena. Näin ollen syt(132,33)=3.

Lasketaan suurin yhteinen tekijä vielä Eukleideen algoritmin avulla:

$$\begin{aligned} 333 &= 2 \cdot 132 + 69 \\ 132 &= 1 \cdot 69 + 63 \\ 69 &= 1 \cdot 63 + 6 \\ 63 &= 10 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

Nyt suurin yhteinen tekijä syt(132,333) nähdään viimeisestä jakojäännöksestä eli syt(132,333)=3.

Lasketaan vielä pienin yhteinen jaettava pyj(132,333):

$$\text{pyj}(132{,}333) = \frac{132 \cdot 333}{\text{syt}(132{,}333)} = \frac{43956}{3} = 14652.$$

Harjoitustehtävä 5.6

Lasketaan suurin yhteinen tekijä syt(456,661) Eukleideen algoritmin avulla:

$$\begin{aligned} 661 &= 1 \cdot 456 + 205 \\ 456 &= 2 \cdot 205 + 46 \\ 205 &= 4 \cdot 46 + 21 \\ 46 &= 2 \cdot 21 + 4 \\ 21 &= 5 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

Suurin yhteinen tekijä syt(456,661) saadaan viimeisestä jakojäännöksestä eli syt(456,661)=1. Seuraavaksi käydään Eukleideen algoritmi läpi alhaalta ylöspäin.

$$\begin{aligned}
\text{syt}(456,661) &= 1 \\
&= 21 - 5 \cdot 4 \\
&= 21 - 5 \cdot (46 - 2 \cdot 21) \\
&= -5 \cdot 46 + 11 \cdot 21 \\
&= -5 \cdot 46 + 11 \cdot (205 - 4 \cdot 46) \\
&= 11 \cdot 205 - 49 \cdot 46 \\
&= 11 \cdot 205 - 49 \cdot (456 - 2 \cdot 205) \\
&= -49 \cdot 456 + 109 \cdot 205 \\
&= -49 \cdot 456 + 109 \cdot (661 - 1 \cdot 456) \\
&= -158 \cdot 456 + 109 \cdot 661.
\end{aligned}$$

Nyt siis $h = -158$ ja $m = 109$, joten suurin yhteinen tekijä voidaan esittää myös muodossa syt(456,661)=$-158 \cdot 456 + 109 \cdot 661$.

Harjoitustehtävä 5.7

a) $34 \not\equiv 4 \pmod 7$, sillä 34-4=30 ja $7 \nmid 30$.

b) $51 \equiv 6 \pmod 9$, sillä 51-6=45 ja $9 \mid 45$.

c) $64 \equiv (-8) \pmod 8$, sillä 64-(-8)=72 ja $8 \mid 72$.

d) $100 \not\equiv 11 \pmod 4$, sillä 100-11=89 ja $4 \nmid 89$.

Harjoitustehtävä 5.8

Jäännösluokkien joukko $\mathbb{Z}_5$ on muotoa $\mathbb{Z}_5 = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\right\}$, missä

$$\begin{aligned}
\overline{0} &= 5\mathbb{Z} = \{5k \mid k \in \mathbb{Z}\} = \{..., -15, -10, -5, 0, 5, 10, 15, ...\}, \\
\overline{1} &= 1 + 5\mathbb{Z} = \{1 + 5k \mid k \in \mathbb{Z}\} = \{..., -14, -9, -4, 1, 6, 11, 16, ...\}, \\
\overline{2} &= 2 + 5\mathbb{Z} = \{2 + 5k \mid k \in \mathbb{Z}\} = \{..., -13, -8, -3, 2, 7, 12, 17, ...\}, \\
\overline{3} &= 3 + 5\mathbb{Z} = \{3 + 5k \mid k \in \mathbb{Z}\} = \{..., -12, -7, -2, 3, 8, 13, 18, ...\} \text{ ja} \\
\overline{4} &= 4 + 5\mathbb{Z} = \{4 + 5k \mid k \in \mathbb{Z}\} = \{..., -11, -6, -1, 4, 9, 14, 19, ...\}.
\end{aligned}$$

Harjoitustehtävä 5.9

On laskettava jakojäännös, kun luku $17^3 + 5^{84}$ jaetaan luvulla 12. Otetaan aluksi selvää, millä jakojäännöksillä luvut 17^3 ja 5^{84} jakautuvat luvulla 12. Tämä tapahtuu kongruenssin avulla. Tutkitaan ensin lukua 17^3. Kongruenssin ominaisuuksien perusteella voidaan lähteä liikkeelle kuitenkin luvusta 17, sillä potenssiin korotuksella ei ole mitään vaikutusta kongruenssissa. Nyt siis

$$\begin{aligned}
17 &\equiv 5, \pmod{12}, \text{ sillä } 12 \mid 17 - 5 = 12. \text{ Seuraavaksi potenssiin korotus.} \\
17^3 &\equiv 5^3 \pmod{12} \text{ Luvut voidaan korottaa potenssiin, kongruenssi säilyy.} \\
17^3 &\equiv 125 \equiv 5 \pmod{12}, \text{ sillä } 12 \mid 125 - 5 = 120. \text{ Avattiin luku } 5^3 \text{ auki.}
\end{aligned}$$

Kun luku 17^3 jaetaan luvulla 12, jää jakojäännökseksi luku 5. Lasketaan seuraavaksi luvun 5^{84} jakojäännös, kun se jaetaan luvulla 12.

$$\begin{aligned}
5^2 &\equiv 1, \pmod{12}, \text{ sillä } 12 \mid 5^2 - 1 = 24. \text{ Seuraavaksi potenssiin korotus.} \\
5^{2 \cdot 21 = 42} &\equiv 1^{21} \pmod{12} \text{ Korotetaan potenssiin, kongruenssi säilyy.} \\
5^{42 \cdot 2 = 84} &\equiv 1^{42} \pmod{12}. \text{ Jakojäännöstä 1 korotetaan potenssiin,} \\
5^{84} &\equiv 1 \pmod{12} \text{ joten se ei muutu.}
\end{aligned}$$

Luvun 5^{84} jakojäännös luvulla 12 jaettaessa on 1. Koska tehtävässä kysyttiin lukujen 17^3 ja 5^{84} summan jakojäännöstä, saadaan yhtälöpari

$$\begin{cases} 17^3 \equiv 5 \pmod{12} \\ 5^{84} \equiv 1 \pmod{12}. \end{cases}$$

Nyt siis yhteinen jakojäännös on lukujen 17^3 ja 5^{84} jakojäännöksien summa 5+1=6. Siis jakojäännös on luku 6.

Harjoitustehtävä 5.10

Tehtävässä ratkaistaan kongruenssiyhtälö $5x \equiv 2 \pmod 6$. Kaikki ratkaisut ovat muotoa $x_0 + 6k$, missä k on jokin kokonaisluku. Kokeillaan alkioita 0, 1, 2, 4, 5 ja 6 niin kauan, että jakojäännökseksi saadaan luku 2. Käytetään seuraavaa taulukkoa:

x	$5x \pmod 6$
0	$5 \cdot 0 = 0$
1	$5 \cdot 1 = 5$
2	$5 \cdot 2 = 10 \equiv 4 \pmod 6$
3	$5 \cdot 3 = 15 \equiv 3 \pmod 6$
4	$5 \cdot 4 = 20 \equiv 2 \pmod 6$

Nyt $x = 4$ on kongruenssiyhtälön eräs ratkaisu. Yleinen ratkaisu on $x = 4 + 6k$, kun k on jokin kokonaisluku.

Harjoitustehtävä 5.11

Tehtävänä on ratkaista kongruenssiyhtälö $11x \equiv 3 \pmod 7$. Kaikki ratkaisut ovat muotoa $x_0 + 7k$, missä k on jokin kokonaisluku. Kokeillaan alkioita 0, 1, 2, 3, 4, 5, 6 ja 7 niin kauan, että jakojäännökseksi saadaan luku 2. Käytetään taulukkoa:

x	$11x \pmod 7$
0	$11 \cdot 0 = 0$
1	$11 \cdot 1 = 11 \equiv 4 \pmod 7$
2	$11 \cdot 2 = 22 \equiv 1 \pmod 7$
3	$11 \cdot 3 = 33 \equiv 5 \pmod 7$
4	$11 \cdot 4 = 44 \equiv 2 \pmod 7$
5	$11 \cdot 5 = 55 \equiv 6 \pmod 7$
6	$11 \cdot 6 = 66 \equiv 3 \pmod 7$

Nyt $x = 6$ on eräs kongruenssiyhtälön ratkaisu. Yleinen ratkaisu on $x = 6 + 7k$, kun k on jokin kokonaisluku.

Harjoitustehtävä 5.12

Merkitään DVD -elokuvia muuttujalla x ja CD -levyjä muuttujalla y. Saadaan yhtälö

$$17x + 9y = 113,$$

joka on eräs Diofantoksen yhtälö. Haetaan ensin ratkaisu DVD -elokuville eli muuttujalle x. Siirretään yhtälössä termi $9y$ toiselle puolelle, jolloin saadaan $17x = 113 - 9y$. Sovelletaan seuraavaksi kongruenssia saatuun yhtälöön.

$17x \equiv 8 \pmod 9$ ja $113 \equiv 5 \pmod 9$. Nyt saadaan kongruenssiyhtälö $8x \equiv 5 \pmod 9$, joka voidaan myös kirjoittaa muodossa $\overline{8x} = \overline{5}$.

Otetaan mukaan jäännösluokkaryhmän käsite. Tässä tehtävässä jäännösluokkaryhmä on $\mathbb{Z}_9 = \{\overline{0}, \overline{1}, \overline{3}, ..., \overline{8}\}$. Kokeillaan nämä alkiot alusta alkaen ja edetään järjestyksessä niin kauan kunnes saadaan alkio $\overline{5}$. Saadaan seuraava taulukko:

$x \in \mathbb{Z}_9$	$\overline{8x}$
$\overline{0}$	$\overline{8 \cdot 0} = \overline{0}$
$\overline{1}$	$\overline{8 \cdot 1} = \overline{8}$
$\overline{2}$	$\overline{8 \cdot 2} = \overline{16} = \overline{7}$
$\overline{3}$	$\overline{8 \cdot 3} = \overline{24} = \overline{6}$
$\overline{4}$	$\overline{8 \cdot 4} = \overline{32} = \overline{5}$

Nyt siis $x = 4$ on eräs ratkaisu. Sijoittamalla saatu muuttujan x arvo alkuperäiseen Diofantoksen yhtälöön saadaan

$$\begin{aligned} 17 \cdot 4 + 9y &= 113 \\ 68 + 9y &= 113 \\ 9y &= 113 - 68 \\ 9y &= 45 \\ y &= \frac{45}{9} = 5. \end{aligned}$$

Ville sai DVD -elokuvia 4 kappaletta ja CD -levyjä 5 kappaletta.

Harjoitustehtävä 5.13

Jos syt(a,m)=1, niin kongruenssilla $ax \equiv c \pmod{m}$ *on yksikäsitteinen ratkaisu* $x \in \mathbb{Z}$ *välillä* $0 \leq x \leq m - 1$..

Todistus. Oletuksen nojalla on olemassa sellaiset 1. *kokonaisluvut* u ja v, että $au + mv = 2$. 1 ja siis

$$a\,(uc) + m\,(vc) = c.$$

Tämän perusteella kongruenssilla on ratkaisu 3. $x = uc$. Ratkaisuja ovat myös edellä mainitun ratkaisun lisäksi kongruentit luvut $x = 4$. $uc + km$, missä 5. k on jokin kokonaisluku. Kongruenssin ominaisuuksien perusteella kaikki ratkaisut ovat keskenään kongruentteja mod m, sillä

$$ax_1 \equiv ax_2 \pmod{m} \Rightarrow 6.\ x_1 \equiv x_2 \pmod{m}.$$

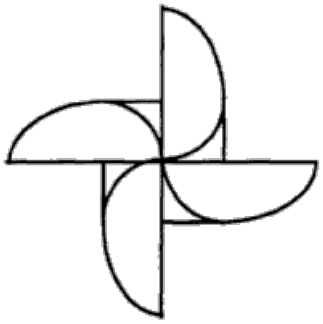
Lopputuloksena siis ratkaisuista tarkalleen 7. *yksi* on välillä $0 \leq x \leq m - 1$. [14] □

7.3 Ryhmäteorian harjoitustehtävien malliratkaisut

Harjoitustehtävä 6.1

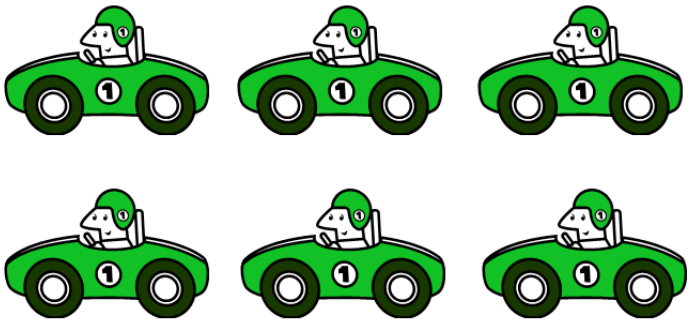
Tehtävän tarkoituksena oli hahmotella kuviot rotaatiosymmetriasta, translaatiosymmetriasta ja molemminpuolisesta symmetriasta. Ratkaisuja tehtävään on monia, mutta tässä esimerkkiratkaisut:

a) Rotaatiosymmetriaa kuvaavaksi kuvioksi sopii kaikki sellaiset kuviot, joita kääntämällä tietyn asteen verran kuvio pysyy muuttumattomana.



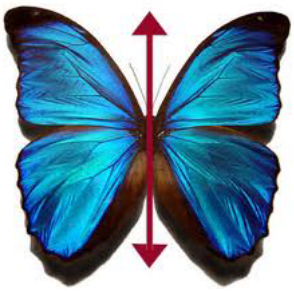
Kuva 15: Kääntämällä kuvan neljää komponenttia 90 asteen verran saadaan aikaan rotaatiosymmetria. [34]

b) Translaatiosymmetrian muodostavat kuviot, joita voidaan siirtää tiettyyn suuntaan etäisyys säilyttäen.



Kuva 16: Ralliautoja siirtämällä paikasta toiseen kuvio pysyy muuttumattomana.

c) Molemminpuolinen symmetria muodostuu, kun kuvioon voidaan hahmotella niin sanottu symmetria-akseli. Kuvio peilautuu symmetria-akselin suhteen. Tästä hyvä esimerkki on esimerkiksi perhosen siivet, jotka ovat toistensa peilikuvat.



Kuva 17: Perhosen siipiä halkoo symmetria-akseli.

Harjoitustehtävä 6.2

Kokonaislukujen joukossa $\mathbb{Z}$ määriteltiin uusi binäärirelaatio Δ asettamalla $a \Delta b = a + b + 1$, kun a ja b ovat joitakin kokonaislukuja. Tehtävänä oli osoittaa, että ryhmä $(\mathbb{Z}, \Delta)$ on Abelin ryhmä. Todistetaan tämä tarkista-

malla ryhmän määritelmän ehdot K1-K4 ja niiden lisäksi vielä ehto K5, joka määrittelee Abelin ryhmän.

K1 Ensimmäinen ehto on selvä, sillä oletuksen mukaan alkiot a ja b ovat kokonaislukuja eli $a, b \in \mathbb{Z}$.

K2 Oletetaan, että alkioiden a ja b lisäksi myös alkio c on kokonaisluku. Lasketaan ensin liitäntälain oikea puoli ja todetaan, että se on sama kuin vasen puoli. Siis $a\Delta\,(b\Delta c) = a\Delta\,(b+c+1) = a+b+c+2$, joka on kokonaisluku. Lasketaan seuraavaksi vasen puoli eli $(a\Delta b)\,\Delta c = (a+b+1)\,\Delta c = a+b+1+c+1 = a+b+c+2$, joka on yhtäsuuri kuin oikea puoli. Ehto K2 siis toteutuu.

K3 Olkoon e jokin kokonaisluku. Ehdon K3 mukaan pitää olla voimassa $a\Delta e = e\Delta a = a$. Kun tämä yhtälö ratkaistaan alkion e suhteen, saadaan $a+e+1 = a$, josta alkiot a kumoutuvat ja alkion e arvoksi saadaan $e = -1$. Sijoitetaan saatu alkion e arvo liitäntälakiin ja suoritetaan lasku. Nyt $a\Delta\,(-1) = (-1)\,\Delta a = a$ kaikilla kokonaisluvuilla a. Ehto K3 toteutuu.

K4 Ehdon K4 mukaan jokaista kokonaislukua a kohti on olemassa sellainen kokonaisluku a^{-1} siten, että $a\Delta a^{-1} = a^{-1}\Delta a = e$. Ratkaistaan tämä yhtälö alkion a^{-1} suhteen. Siis vasenta puolta käyttäen saadaan

$$\begin{aligned} a\Delta a^{-1} &= e \quad | \text{ Aiemmin laskettiin, että } e = -1. \\ a + a^{-1} + 1 &= -1 \\ a^{-1} &= -a - 2. \end{aligned}$$

Nyt $a\Delta\,(-a-2) = (-a-2)\,\Delta a = -1 = e$. Näin ollen ehto K4 toteutuu.

K5 Jotta ryhmä $(\mathbb{Z}, \Delta)$ olisi Abelin ryhmä, on oltava $a\Delta b = b\Delta a$ kaikilla kokonaisluvuilla a ja b. Lasketaan ensin vasen puoli eli $a\Delta b = a+b+1$. Oikea puoli on $b\Delta a = b+a+1 = a+b+1$ eli yhtäsuuri kuin vasen puoli. Siis ryhmä $(\mathbb{Z}, \Delta)$ on Abelin ryhmä.

Harjoitustehtävä 6.3

Tutkitaan ensin onko $(\mathbb{Z}_{15}, \cdot)$ ryhmä kertolaskun suhteen tarkastamalla ryhmän määritelmän ehdot K1-K4.

K1 Joukko $(\mathbb{Z}_{15}, \cdot)$ muodostuu alkioista $(\mathbb{Z}_{15}, \cdot) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, ..., \overline{14}\}$. Oletetaan, että a, b ja c ovat kyseisen joukon eräitä alkioita.

K2 Liitäntälaki kertolaskun suhteen on muotoa $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$. Nyt vasen puoli on $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{abc}$, joka on yhtäsuuri kuin oikea puoli $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{abc}$. Siis ehto K2 toteutuu.

K3 Neutraalialkio on $\overline{1}$, sillä $\overline{1} \cdot \overline{a} = \overline{a} \cdot \overline{1} = \overline{a}$. Näin ollen ehto K3 toteutuu.

K4 On huomattava, että kyseisessä joukossa on alkio $\overline{0}$, jolla ei ole käänteisalkiota. Käänteisalkion olemassaolon ehto ei siis toteudu ja näin ollen joukko $(\mathbb{Z}_{15}, \cdot)$ ei ole ryhmä.

Tutkitaan samalla tavalla onko $(\mathbb{Z}_{15}^*, +)$ ryhmä yhteenlaskun suhteen.

K1 Joukko $(\mathbb{Z}_{15}^*, +)$ koostuu alkioista $(\mathbb{Z}_{15}^*, \cdot) = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$. Tässä siis esimerkiksi syt(1,15)=1 ja syt(7,15)=1. Oletetaan, että a, b ja c ovat tämän joukon eräitä alkioita.

K2 Liitäntälain toteutuminen todetaan samalla tavalla kuin edellisessä tapauksessa. Nyt $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$. Tässä vasen puoli on $\overline{a} + (\overline{b} + \overline{c}) = \overline{a + b + c}$ ja oikea puoli $(\overline{a} + \overline{b}) + \overline{c} = \overline{a + b + c}$, joten ehto K2 toteutuu.

K3 Neutraalialkiota ei ole olemassa, sillä $\overline{a} + \overline{b} = \overline{b} + \overline{a} \neq \overline{b}$. Tilanne olisi erilainen, jos joukossa olisi myös alkio $\overline{0}$. Näin ollen joukko $(\mathbb{Z}_{15}^*, +)$ ei myöskään ole ryhmä.

Harjoitustehtävä 6.4

Tehtävänä oli tarkastella multiplikatiivista ryhmää $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ ja joukkoa $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Tutkitaan, millä alkuluokilla on käänteisalkio.

Nyt siis syt(1,5)=1, syt(2,5)=1, syt(3,5)=1 ja syt(4,5)=1.

i) Alkion $\overline{1}$ käänteisalkio on $\overline{1}$, sillä $\overline{1} \cdot \overline{1} = \overline{1}$.

ii) Alkion $\overline{2}$ käänteisalkio on $\overline{3}$, sillä $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$.

iii) Alkion $\overline{3}$ käänteisalkio on $\overline{2}$, sillä $\overline{3} \cdot \overline{2} = \overline{6} = \overline{1}$.

iv) Alkiolla $\overline{4}$ ei ole käänteisalkiota kyseissä ryhmässä, sillä kertomalla alkiota $\overline{4}$ millä tahansa alkiolla $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ ei saada tulokseksi alkiota $\overline{1}$.

Käänteisalkiot ovat siis alkuluokilla $\overline{1}, \overline{2}$ ja $\overline{3}$.

Harjoitustehtävä 6.5

Tehtävänä oli laskea kuvaustulo $\alpha\beta\alpha$, kun ryhmässä S_4 määritellään $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ ja $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$. Lähdetään liikkeelle oikealta vasemmalle ja lasketaan ensin kuvaustulo $\beta\alpha$.

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix},$$

sillä $1 \mapsto 3 \mapsto 1, 2 \mapsto 2 \mapsto 4, 3 \mapsto 1 \mapsto 2$ ja $4 \mapsto 4 \mapsto 3$. Lasketaan seuraavaksi koko kuvaustulo $\alpha\beta\alpha$.

$$\alpha\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix},$$

sillä $1 \mapsto 1 \mapsto 3, 2 \mapsto 4 \mapsto 4, 3 \mapsto 2 \mapsto 2$ ja $4 \mapsto 3 \mapsto 1$.

Harjoitustehtävä 6.6

Tehtävässä todistettava lause on muotoa

Olkoon K ryhmä. Kun a ja b ovat joitakin ryhmän K alkioita, niin

a) *yhtälöllä $ax = b$ on ryhmässä K yksikäsitteinen ratkaisu $x = a^{-1}b$;*

b) *yhtälöllä $xa = b$ on ryhmässä K yksikäsitteinen ratkaisu $x = ba^{-1}$.*

Todistetaan ensin a) -kohta laittamalla annetut todistuksen osat oikeaan järjestykseen, joka on

3) Kertomalla yhtälö $ax = b$

5) vasemmalta alkiolla a^{-1}

4) saadaan $x = a^{-1}b$.

2) Kääntäen, $x = a^{-1}b$

6) toteuttaa yhtälön $ax = b$,

1) koska $a\,(a^{-1}b) = b$.

Oikea järjestys a) -kohdassa on siis 3), 5), 4), 2), 6) ja 1). Todistetaan seuraavaksi b) -kohta.

ii) Kertomalla yhtälö $xa = b$

v) oikealta alkiolla a^{-1}

iv) saadaan $x = ba^{-1}$.

iii) Kääntäen, $x = ba^{-1}$

i) toteuttaa yhtälön $xa = b$,

vi) koska $(ba^{-1})\,a = b$.

Oikea järjestys b) -kohdassa on siis ii), v), iv), iii), i) ja vi). Selvennyksen vuoksi kirjoitetaan todistus vielä helpommin luettavaksi.

Todistus. a) -kohta: Kertomalla yhtälö $ax = b$ vasemmalta alkiolla a^{-1} saadaan $x = a^{-1}b$. Kääntäen, $x = a^{-1}b$ toteuttaa yhtälön $ax = b$, koska $a\left(a^{-1}b\right) = b$.

b) -kohta: Kertomalla yhtälö $xa = b$ oikealta alkiolla a^{-1} saadaan $x = ba^{-1}$. Kääntäen, $x = ba^{-1}$ toteuttaa yhtälön $xa = b$, koska $\left(ba^{-1}\right)a = b$. □

Harjoitustehtävä 6.7

Osoitetaan ryhmän S_3 alkiot $\{1, \tau, \sigma, \sigma\tau, \sigma^2, \sigma^2\tau\}$ erisuuriksi käyttämällä ensin edellisen harjoitustehtävän lausetta. Tässä $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\tau^2 = 1, \sigma^3 = 1$ ja $\tau\sigma\tau = \sigma^2$. On selvää, että $1 \neq \sigma$, $1 \neq \tau$ ja $\sigma \neq \tau$. Asetetaan seuraavaksi ryhmän S_3 alkiot vuorotellen yhtäsuuriksi ja osoitetaan, että kyseessä on ristiriita. Tapauksia on yhteensä 12.

1 ja $\sigma\tau$:

$$\begin{aligned} 1 &= \sigma\tau \quad \text{Kerrotaan vasemmalta alkiolla } \tau\text{, jolloin saadaan} \\ \tau &= \sigma\tau^2. \quad \text{Oletuksen mukaan } \tau^2 = 1\text{. Tällöin} \\ \tau &= \sigma, \quad \text{mikä on ristiriita, sillä } \tau \text{ ja } \sigma \text{ ovat erisuuria. Siis } 1 \neq \sigma\tau. \end{aligned}$$

1 ja σ^2:

$$\begin{aligned} 1 &= \sigma^2 \quad \text{Kerrotaan vasemmalta alkiolla } \sigma\text{, jolloin saadaan} \\ \sigma &= \sigma^3. \quad \text{Oletuksen mukaan } \tau^3 = 1\text{, jolloin syntyy ristiriita eli } 1 \neq \sigma^2. \end{aligned}$$

1 ja $\sigma^2\tau$:

$$\begin{aligned} 1 &= \sigma^2\tau \text{ Kerrotaan vasemmalta alkiolla } \sigma, \text{ jolloin saadaan} \\ \sigma &= \sigma^3\tau. \text{ Oletuksen mukaan } \sigma^3 = 1. \text{ Tällöin} \\ \sigma &= \tau, \text{ mikä on ristiriita, sillä } \tau \text{ ja } \sigma \text{ ovat erisuuria. Siis } 1 \neq \sigma^2\tau. \end{aligned}$$

τ ja $\sigma\tau$:

$$\begin{aligned} \tau &= \sigma\tau \text{ Kerrotaan oikealta alkiolla } \tau, \text{ jolloin saadaan} \\ \tau^2 &= \sigma\tau^2. \text{ Oletuksen mukaan } \tau^2 = 1. \text{ Tällöin} \\ 1 &= \sigma, \text{ mikä on ristiriita. Siis } \tau \neq \sigma\tau. \end{aligned}$$

τ ja σ^2:

$$\begin{aligned} \tau &= \sigma^2 \text{ Kerrotaan vasemmalta alkiolla } \sigma, \text{ jolloin saadaan} \\ \sigma\tau &= \sigma^3. \text{ Oletuksen mukaan } \sigma^3 = 1. \text{ Tällöin} \\ \sigma\tau &= 1, \text{ mikä on ristiriita. Tämän perustelee ensimmäinen tapaus 1 ja } \sigma\tau. \end{aligned}$$

τ ja $\sigma^2\tau$:

$$\begin{aligned} \tau &= \sigma^2\tau \text{ Kerrotaan oikealta alkiolla } \tau, \text{ jolloin saadaan} \\ \tau^2 &= \sigma^2\tau^2. \text{ Oletuksen mukaan } \tau^2 = 1. \text{ Tällöin} \\ 1 &= \sigma^2, \text{ mikä on ristiriita aiemman tapauksen 1 ja } \sigma^2 \text{ perusteella.} \end{aligned}$$

σ ja $\sigma\tau$:

$$\begin{aligned} \sigma &= \sigma\tau \text{ Kerrotaan vasemmalta alkiolla } \sigma^2, \text{ jolloin saadaan} \\ \sigma^3 &= \sigma^3\tau. \text{ Oletuksen mukaan } \sigma^3 = 1. \text{ Tällöin} \\ 1 &= \tau, \text{ mikä on ristiriita.} \end{aligned}$$

σ ja σ^2:

$$\begin{aligned} \sigma &= \sigma^2 \text{ Kerrotaan vasemmalta alkiolla } \sigma, \text{ jolloin saadaan} \\ \sigma^2 &= \sigma^3. \text{ Oletuksen mukaan } \sigma^3 = 1. \text{ Tällöin} \\ \sigma^2 &= 1, \text{ mikä on ristiriita aiemman tapauksen 1 ja } \sigma^2 \text{ perusteella.} \end{aligned}$$

σ ja $\sigma^2\tau$:

$$\begin{aligned}
\sigma &= \sigma^2\tau \text{ Kerrotaan vasemmalta alkiolla } \sigma, \text{ jolloin saadaan} \\
\sigma^2 &= \sigma^3\tau. \text{ Oletuksen mukaan } \sigma^3 = 1. \text{ Tällöin} \\
\sigma^2 &= \tau, \text{ mikä on ristiriita aiemman tapauksen } \tau \text{ ja } \sigma^2 \text{ mukaan.}
\end{aligned}$$

$\sigma\tau$ ja σ^2:

$$\begin{aligned}
\sigma\tau &= \sigma^2 \text{ Kerrotaan vasemmalta alkiolla } \sigma, \text{ jolloin saadaan} \\
\sigma^2\tau &= \sigma^3. \text{ Oletuksen mukaan } \sigma^3 = 1. \text{ Tällöin} \\
\sigma^2\tau &= 1, \text{ mikä on ristiriita aiemman tapauksen 1 ja } \sigma^2\tau \text{ perusteella.}
\end{aligned}$$

$\sigma\tau$ ja $\sigma^2\tau$:

$$\begin{aligned}
\sigma\tau &= \sigma^2\tau \text{ Kerrotaan vasemmalta alkiolla } \sigma, \text{ jolloin saadaan} \\
\sigma^2\tau &= \sigma^3\tau. \text{ Oletuksen mukaan } \sigma^3 = 1. \text{ Tällöin} \\
\sigma^2\tau &= \tau, \text{ mikä on ristiriita aiemman tapauksen } \tau \text{ ja } \sigma^2\tau \text{ perusteella.}
\end{aligned}$$

σ^2 ja $\sigma^2\tau$:

$$\begin{aligned}
\sigma^2 &= \sigma^2\tau \text{ Kerrotaan vasemmalta alkiolla } \sigma, \text{ jolloin saadaan} \\
\sigma^3 &= \sigma^3\tau. \text{ Oletuksen mukaan } \sigma^3 = 1. \text{ Tällöin} \\
1 &= \tau, \text{ mikä on ristiriita aiemman tapauksen 1 ja } \tau \text{ perusteella.}
\end{aligned}$$

Toinen tapa osoittaa alkiot erisuuriksi on laskea alkioiden kuvaustulot. Lasketaan ensin alkioiden $\sigma\tau, \sigma^2$ ja $\sigma^2\tau$ kuvaustulot ja verrataan niitä toisiinsa sekä muihin alkioihin.

$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, sillä $1 \mapsto 2 \mapsto 3, 2 \mapsto 1 \mapsto 2$ ja $3 \mapsto 3 \mapsto 1$. (Tässä siis $\mapsto$ tarkoittaa alkion kuvautumista toiseksi alkioksi.)

$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, sillä $1 \mapsto 2 \mapsto 3, 2 \mapsto 3 \mapsto 1$

ja $3 \mapsto 1 \mapsto 2$.
$\sigma^2\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, sillä $1 \mapsto 2 \mapsto 1, 2 \mapsto 1 \mapsto 3$ ja $3 \mapsto 3 \mapsto 2$.

Vertaamalla edellä mainittuja kuvaustuloja toisiinsa havaitaan kaikkien olevan erisuuria. Näin käy myös, kun verrataan laskettuja kuvaustuloja alkioihin 1, τ ja σ. Täten kaikki alkiot ovat erisuuria.

On huomattava, että tehtävä on kielentämistehtävä, jolloin tarkat kirjalliset perustelut vaaditaan.

Harjoitustehtävä 6.8

Tehtävän oletukset ovat samat kuin edellisessä harjoitustehtävässä 6.7. Tarkoitus on saattaa tulot $(\sigma\tau)(\sigma^2)$ ja $(\sigma^2\tau)(\sigma\tau)$ joihinkin seuraavista muodoista

$$1, \tau, \sigma, \sigma\tau, \sigma^2, \sigma^2\tau$$

käyttämällä ainoastaan ominaisuuksia $\tau^2 = 1, \sigma^3 = 1$ ja $\tau\sigma\tau = \sigma^2$. Tarkastellaan ensin kuvaustuloa $(\tau\sigma)(\sigma^2)$.

$(\tau\sigma)\,(\sigma^2)$ Käytetään ominaisuutta $\sigma^2 = \tau\sigma\tau$.
$= \sigma\tau\tau\sigma\tau$
$= \sigma\tau^2\sigma\tau$ Oletuksen mukaan $\tau^2 = 1$.
$= \sigma^2\tau$.

Tutkitaan seuraavaksi kuvaustuloa $(\sigma^2\tau)(\sigma\tau)$.

$(\sigma^2\tau)\,(\sigma\tau)$ Käytetään jälleen ominaisuutta $\sigma^2 = \tau\sigma\tau$.
$= \tau\sigma\tau\tau\sigma\tau$
$= \tau\sigma\tau^2\sigma\tau$ Oletuksen mukaan $\tau^2 = 1$.
$= \tau\sigma^2\tau$ Käytetään uudelleen ominaisuutta $\sigma^2 = \tau\sigma\tau$.
$= \tau\tau\sigma\tau\tau$ Nyt $\tau^2 = 1$, joten
$= \sigma$.

Harjoitustehtävä 6.9

Muodostetaan multiplikatiivisen ryhmän $(\mathbb{Z}_4^*, \cdot)$ ryhmätaulu. Sen alkiot ovat $(\mathbb{Z}_4^*, \cdot) = \{\overline{1}, \overline{2}, \overline{3}\}$.

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Kyseisessä taulukossa esimerkiksi $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$ ja $\overline{3} \cdot \overline{2} = \overline{6} = \overline{2}$ multiplikatiivisessa ryhmässä $(\mathbb{Z}_4^*, \cdot)$.

Harjoitustehtävä 6.10

Tehtävässä annettiin ryhmät $K = (\mathbb{Z}, +)$ ja $H = (2\mathbb{Z}, +)$. Osoitetaan aliryhmän määritelmän avulla, että ryhmä H on ryhmän K aliryhmä.

A1 Olkoot a ja b ryhmän H alkioita. Koska alkiot a ja b ovat parillisia kokonaislukuja, myös niiden summa $a+b = c$ on parillinen kokonaisluku eli myös alkio c on ryhmän H alkio.

A2 Ryhmän K neutraalialkio on 0_k, sillä $0+a = a+0 = a$. Myös ryhmällä H on sama neutraalialkio, sillä $0+2a = 2a+0 = 2a$. Jakamalla luvulla 2 saadaan ryhmän K alkio ja erikoisesti luku 2 jakaa luvun nolla. Ehto A2 toteutuu.

A3 Olkoon d ryhmän H alkio. Nyt alkion d käänteisalkio ryhmässä H on $-d$, sillä $d + (-d) = 0 = -d + d$. Siis ehto A3 toteutuu.

Ehdot A1-A3 toteutuivat, joten ryhmä H on ryhmän K aliryhmä.

Harjoitustehtävä 6.11

Tehtävänä on todistaa seuraava lause täyttämällä puuttuvat aukot todistuksesta. Lauseen todistuksessa tarvitaan lausetta 6.18.

Olkoon K ryhmä ja $\{H_i \mid i \in I\}$ ryhmän K aliryhmien joukko (tässä indeksit i kuuluvat erääseen joukkoon I). Tällöin aliryhmien joukon leikkaus $\underbrace{\cap}_{i\in I} H_i$ on myös ryhmän K aliryhmä.

Todistus. Merkitään $H = \underbrace{\cap}_{i\in I} H_i$. Koska jokainen 1. $\underline{H_i}$ on aliryhmä, sisältävät ne ryhmän 2. $\underline{K}$ ykkösalkion 1. Tällöin 3. $\underline{1 \in H}$, joten ryhmä H on epätyhjä. Olkoon nyt x ja y joitakin ryhmän H alkioita. Tällöin x, y 4. $\underline{\in H_i}$ kaikilla indeksin i arvoilla. Lauseen 6.18 perusteella 5. $\underline{xy, x^{-1}} \in H_i$ kaikilla indekseillä i. Näin ollen 6. $\underline{xy, x^{-1}} \in H$, joten lauseen 6.18 mukaan joukko H on ryhmän K 7. $\underline{aliryhmä}$. □

8 Mallikoe

1. Olkoon U joukkojen A, B ja C universaali joukko. Piirrä Venn -diagrammit seuraavista joukko-operaatioista:

   a) $A \cap B \cap C$,

   b) $(A' \cup C) \setminus B$ ja

   c) $(A \cup B)' \cap C$.

2. Määritellään joukossa $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ relaatio säännöllä

   $$(x_1, y_1)\, R\, (x_2, y_2) \;\Leftrightarrow\; x_1 - y_1 = x_2 - y_2.$$

   Osoita, että R on ekvivalenssirelaatio.

3. Tämä koetehtävä suoritetaan kielentämistehtävänä. Laske Eukleideen algoritmin avulla lukujen 432 ja 762 suurin yhteinen tekijä syt(432,

762). Mikä on lukujen pienin yhteinen jaettava pyj? Selitä ratkaisun kulkua kokonaisilla virkkeillä ratkaisun edetessä kertomus -mallin mukaisesti.

4. Mikä on jakojäännös, kun jaetaan luvulla 13 luku

   i) $20^4 + 20^{20}$ ja

   ii) $1000 - 11^8$?

5. Määritellään joukossa $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ seuraava binäärioperaatio λ:

$$a \lambda b = \frac{ab}{3},$$

   missä a ja b ovat joukon $\mathbb{Q}^*$ alkioita. Tässä ab tarkoittaa lukujen tavallista kertolaskua. Näytä, että $(\mathbb{Q}^*, \lambda)$ on ryhmä ja vieläpä Abelin ryhmä.

6. Tämä koetehtävä suoritetaan kielentämistehtävänä. Olkoon G ryhmä ja a sen alkio. Osoita, että ryhmä $H = \{x \in G \mid xa = ax\}$ on ryhmän G aliryhmä täyttämällä todistuksesta puuttuvat aukot.

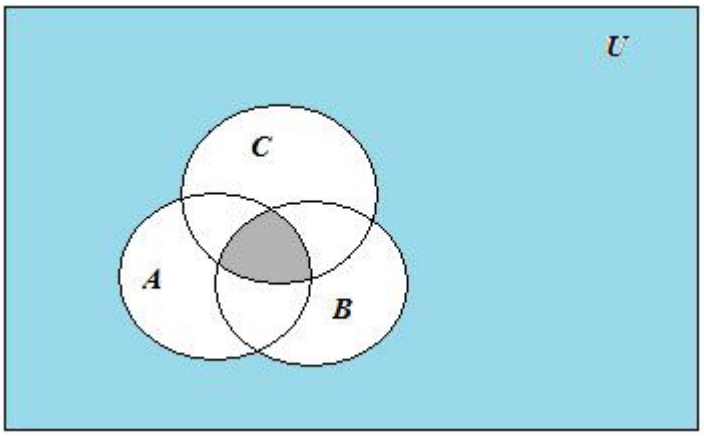
   A1 Olkoon x ja y ryhmän H alkioita. On tutkittava onko myös 1._____ ryhmän H alkio. Nyt 2._____$= x\,(ya) = x\,(ay) = (xa)\,y = (ax)\,y =$3._____. Koska 4._____, niin ryhmä on suljettu ryhmän G operaation suhteen.

   A2 Tarkastellaan onko ryhmällä H 5._____alkiota e. Nyt $ea =$6._____$= ae$. Siis e 7._____ H.

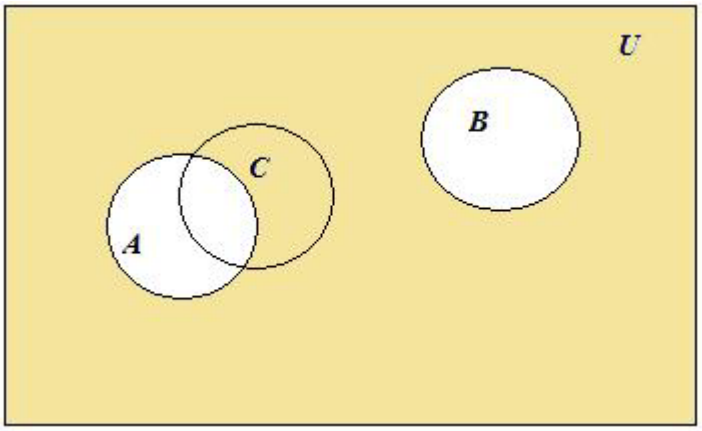
   A3 Olkoon x ryhmän H alkio. Tarkistetaan, että 8._____ x^{-1} on myös ryhmän H alkio. Koska $x \in H$, niin 9._____. Kertomalla tämä vasemmalta alkiolla 10._____ saadaan $a =$ 11._____. Kun nyt kerrotaan oikealta alkiolla 12._____, niin $ax^{-1} =$ 13._____. Näin ollen 14._____ $\in H$ eli ryhmä H on ryhmän G aliryhmä.

8.1 Mallikokeen ratkaisut

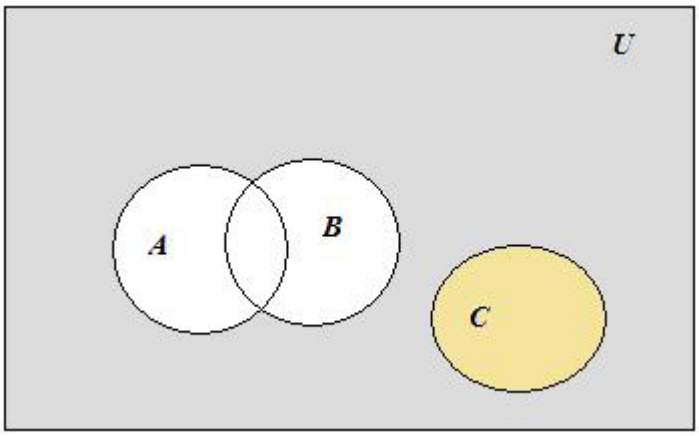
1. Alla Venn -diagrammit kohdista a) - c).



Kuva 18: a) Tummalla väritetty alue kuvaa operaatiota $A \cap B \cap C$.



Kuva 19: b) Tummalla väritetty alue kuvaa operaatiota $(A' \cup C) \setminus B$.



Kuva 20: c) Tummalla väritetty alue kuvaa operaatiota $(A \cup B)' \cap C$.

2. Määritellään joukossa $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ relaatio säännöllä

$$(x_1, y_1)\, R\, (x_2, y_2) \;\Leftrightarrow\; x_1 - y_1 = x_2 - y_2.$$

Osoitetaan, että R on ekvivalenssirelaatio tarkistamalla ekvivalenssirelaation määritelmän ehdot E1-E3.

E1 Tutkitaan refleksiivisyyttä. Nyt $x-y = x-y$ kaikilla reaaliluvuilla x ja y, joten refleksiivisyys toteutuu.

E2 Nyt $x_1 - y_1 = x_2 - y_2$. Yhtäsuuruus säilyy, jos vaihdetaan puolia $x_2 - y_2 = x_1 - y_1$ eli symmetrisyys toteutuu.

E3 Oletetaan, että $x_1 - y_1 = x_2 - y_2$, $x_2 - y_2 = x_3 - y_3$ ja $(x_2, y_2)\, R\, (x_3, y_3)$. Tällöin myös $x_1 - y_1 = x_3 - y_3$, joten $(x_1, y_1)\, R\, (x_3, y_3)$ ja transitiivisuus toteutuu.

Ehdot E1-E3 toteutuivat, joten R on ekvivalenssirelaatio.

3. Tehtävä suoritetaan kielentämistehtävänä. Lasketaan syt(432,762) Eukleideen algoritmin avulla ja selitetään ratkaisun kulkua kirjallisesti selkeillä virkkeillä. Tarkastellaan aluksi kuinka monta kertaa luku 432

sisältyy lukuun 762 ja mikä on jakojäännös.

$$\begin{aligned}
762 &= 1 \cdot 432 + 330 \quad \text{Nyt jakojäännös on 330, joka sisältyy lukuun 432} \\
432 &= 1 \cdot 330 + 102 \quad \text{vain kerran ja jakojäännökseksi jää 102.} \\
330 &= 3 \cdot 102 + 24 \quad \text{Näin edetään} \\
102 &= 4 \cdot 24 + 6 \quad \text{kunnes jakojäännökseksi saadaan luku 0.} \\
24 &= 4 \cdot 6 + 0. \quad \text{Algoritmi lopetetaan, jakojäännökseksi saatiin luku 0.}
\end{aligned}$$

Lukujen 432 ja 762 suurin yhteinen tekijä syt(432,762) nähdään viimeisestä jakojäännöksestä, joka tässä tapauksessa on luku 6. Siis syt(432,762)=6. Lasketaan pienin yhteinen jaettava pyj seuraavalla kaavalla:

$$\text{pyj}\,(432, 762) = \frac{432 \cdot 762}{\text{syt}\,(432, 762)} = \frac{329184}{6} = 54864.$$

Lukujen 432 ja 762 pienin yhteinen jaettava pyj(432,762)=54864.

4. Tässä tehtävässä tarkastellaan jakojäännoksiä, kun luvut $20^4 + 20^{20}$ ja $1000 - 11^8$ jaetaan luvulla 13. Jakojäännökset saadaan ratkaistuksi kongruenssin (mod 13) avulla.

   i) Lasketaan ensin luvun 20^4 jakojäännös.

   $$\begin{aligned}
   20 &\equiv 7 \pmod{13}, \text{ sillä } 13 \mid 20 - 7 = 13. \\
   20^2 &\equiv 7^2 = 49 \equiv 10 \pmod{13}, \text{ sillä } 13 \mid 49 - 10 = 39. \\
   20^4 &\equiv 10^2 = 100 \equiv 9 \pmod{13}, \text{ sillä } 13 \mid 100 - 9 = 91.
   \end{aligned}$$

   Kun luku 20^4 jaetaan luvulla 13, jakojäännökseksi saadaan luku 9. Lasketaan seuraavaksi luvun 20^{20} jakojäännös.

   $$\begin{aligned}
   20^2 &\equiv 10 \pmod{13}, \text{ aiemman perusteella.} \\
   20^{10} &\equiv 10^5 = 100000 \equiv 4 \pmod{13}, \text{ sillä } 13 \mid 100000 - 4 = 99996. \\
   20^{20} &\equiv 4^2 = 16 \equiv 3 \pmod{13}, \; sill13 \mid 16 - 3 = 3.
   \end{aligned}$$

   Kun luku 20^{20} jaetaan luvulla 13, jakojäännökseksi saadaan luku 3. Luvun $20^4 + 20^{20}$ jakojäännös saadaan laskemalla lukujen 20^4 ja 20^{20} jakojäännökset yhteen. Siis luvun $20^4 + 20^{20}$ jakojäännös luvulla 13 jaettaessa on 9+3=12.

ii) Lasketaan ensin luvun 10000 jakojäännös.

$$1000 \equiv 12 \pmod{13}, \text{ sillä } 13 \mid 1000 - 12 = 988.$$

Kun luku 1000 jaetaan luvulla 13, saadaan jakojäännökseksi luku 12. Lasketaan seuraavaksi luvun 11^8 jakojäännös luvulla 13 jaettaessa.

$$\begin{aligned} 11 &\equiv -2 \pmod{13}, \text{ sillä } 13 \mid 11 - (-2) = 13. \\ 11^4 &\equiv (-2)^4 = 16 \equiv 3 \pmod{13}, \text{ sillä } 13 \mid 16 - 3 = 13. \\ 11^8 &\equiv 3^2 = 9 \pmod{13}. \end{aligned}$$

Kun luku 11^8 jaetaan luvulla 13, saadaan jakojäännökseksi luku 9. Luvun $1000 - 11^8$ jakojäännös luvulla 13 jaettaessa saadaan vähentämällä lukujen 1000 ja 11^8 jakojäännökset toisistaan. Siis luvun $1000 - 11^8$ jakojäännös on 12-9=3 luvulla 13 jaettaessa.

5. Tehtävässä määriteltiin joukossa $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ seuraava binäärioperaatio:

$$a \lambda b = \frac{ab}{3},$$

missä a ja b ovat joukon $\mathbb{Q}^*$ alkioita. Tässä ab tarkoittaa lukujen tavallista kertolaskua. Osoitetaan, että joukko $\mathbb{Q}^*$ on Abelin ryhmä tarkastamalla ryhmän määritelmän ehdot K1-K5.

K1 Olkoon a ja b joukon $\mathbb{Q}^*$ alkioita. Tällöin luku ab on rationaaliluku ja erikoisesti myös luku $\frac{ab}{2}$ sisältyy joukkoon $\mathbb{Q}^*$. Näin ollen binäärioperaatio λ on suljettu joukon $\mathbb{Q}^*$ suhteen ja ehto K1 toteutuu.

K2 Olkoot a, b ja c joukon $\mathbb{Q}^*$ alkioita. Tarkastellaan liitäntälain toteutumista. Nyt

$$a \lambda (b \lambda c) = a \lambda \left(\frac{bc}{3} \right) = \frac{a \left(\frac{bc}{3} \right)}{3} = \frac{a\,(bc)}{9}$$

ja

$$(a \lambda b)\, \lambda c = \left(\frac{ab}{3} \right) \lambda c = \frac{\frac{(ab)}{3} c}{3} = \frac{(ab)\, c}{9}.$$

Siis liitäntälaki toteutuu.

K3 Olkoon e jokin joukon $\mathbb{Q}^*$ alkio. Ehdon K3 mukaan pitää olla voimassa $a\lambda e = e\lambda a$. Nyt $e = 3$, sillä vasen puoli

$$a\lambda 3 = \frac{a3}{3} = a \text{ ja oikea puoli}$$

$$3\lambda a = \frac{3a}{3} = a \text{ ovat yhtäsuuria.}$$

Ehto K3 toteutuu.

K4 Ehdon K4 mukaan jokaista joukon $\mathbb{Q}^*$ alkiota a kohti on olemassa sellainen rationaaliluku a^1 siten, että $a\lambda a^{-1} = a^{-1}\lambda a = e$. Ratkaistaan kyseinen yhtälö alkion a^{-1} suhteen.

$$\begin{aligned} a\lambda a^{-1} &= e. \text{ Aiemmin saatiin, että } e = 3. \\ \frac{aa^{-1}}{3} &= 3 \text{ Kerrotaan yhtälö luvulla 3 puolittain} \\ aa^{-1} &= 9 \\ a^{-1} &= \frac{9}{a}. \end{aligned}$$

Nyt $a\lambda a^{-1} = \frac{a\frac{9}{a}}{3} = 3 = e$. Näin ollen ehto K4 toteutuu.

K5 Jotta ryhmä $(\mathbb{Q}^*, \lambda)$ olisi Abelin ryhmä, on oltava $a\lambda b = b\lambda a$ kaikilla nollasta eroavilla rationaaliluvuilla a ja b. Lasketaan ensin vasen puoli eli $a\lambda b = \frac{ab}{3}$. Oikea puoli on $b\lambda a = \frac{ba}{3}$ eli yhtäsuuri kuin oikea puoli. Siis ryhmä $(\mathbb{Q}^*, \lambda)$ on Abelin ryhmä.

6. Osoitetaan, että ryhmä $H = \{x \in G \mid xa = ax\}$ on ryhmän G aliryhmä täyttämällä todistuksesta puuttuvat aukot.

A1 Olkoon x ja y ryhmän H alkioita. On tutkittava onko myös 1. $\underline{xy}$ ryhmän H alkio. Nyt 2. $\underline{(xy)\,a}$=$x\,(ya) = x\,(ay) = (xa)\,y = (ax)\,y$ =3. $\underline{a\,(xy)}$. Koska 4. $\underline{xy \in H}$, niin ryhmä on suljettu ryhmän G operaation suhteen.

A2 Tarkastellaan onko ryhmällä H 5. *identiteetti*alkiota e. Nyt ea =6. $\underline{a}$= ae. Siis e 7. $\underline{\in}$ H.

A3 Olkoon x ryhmän H alkio. Tarkistetaan, että 8. *käänteisalkio* x^{-1} on myös ryhmän H alkio. Koska $x \in H$, niin 9. $\underline{xa = ax}$. Kertomalla tämä vasemmalta alkiolla 10. $\underline{x^{-1}}$ saadaan a = 11. $\underline{x^{-1}ax}$.

Kun nyt kerrotaan oikealta alkiolla 12. $\underline{x^{-1}}$, niin $ax^{-1} = 13.\ \underline{x^{-1}a}$.
Näin ollen 14. $\underline{x^{-1}} \in H$ eli ryhmä H on ryhmän G aliryhmä.

Viitteet

[1] Joutsenlahti, J. (2009). *Matematiikan kielentäminen kirjallisessa työssä.* Teoksessa Raimo Kaasila (toim.)
Matematiikan ja luonnontieteiden opetuksen tutkimuspäivät Rovaniemellä 7.-8.11.2008.
Rovaniemi: Lapin yliopisto, 71-86. (Lapin yliopiston kasvatustieteellisiä raportteja 9).

[2] Joutsenlahti, Jorma. (2003). *Kielentäminen matematiikan opiskelussa.* Teoksessa Virta Arja & Marttila Outi (toim.) (toim.) Opettaja, asiantuntijuus ja yhteiskunta (Ainedidaktinen symposium 7.2.2003).
Turku: Turun opettajankoulutuslaitos, 188-196. (Turun yliopiston kasvatustieteiden tiedekunnan julkaisuja B:72).

[3] Joutsenlahti J, Kulju P. (2010). *Kieliteoreettinen lähestymistapa koulumatematiikan sanallisiin tehtäviin ja niiden kielennettyihin ratkaisuihin.* Teoksessa Eero Ropo, Harry Silfverberg & Tiina Soini (toim.) Toisensa kohtaavat ainedidaktiikat.
Ainedidaktiikan symposiumi Tampereella 13.2.2009. Tampere: Tampereen yliopisto, 77-89.
(Tampereen yliopiston opettajankoulutuslaitoksen julkaisuja. A 31).

[4] Joutsenlahti J. (2010). *Matematiikan kirjallinen kielentäminen lukiomatematiikassa.* Teoksessa Mervi Asikainen, Pekka E. Hirvonen ja Kari Sormunen (toim.) Ajankohtaista matemaattisten aineiden opetuksen ja oppimisen tutkimuksessa.
Joensuu: University of Eastern Finland, 3-15. (Reports and Studies in Education, Humanities, and Theology 1).

[5] Joutsenlahti, Jorma. *Kirjallisen kielentämisen malleja.* Tampereen yliopisto, 2009 & 2010.

[6] Koppinen, Marja-Leena. *Lapsen kieli ja vuorovaikutustaidot.* Jyväskylä, 1989.

[7] Seppälä, Reino. *Matematiikka -taitoa ajatella.* Jyväskylä, 1994.

[8] Yrjönsuuri, Raija. *Matematiikka mieluisaksi.* Oppilo, 2007.

[9] Kontkanen, Pekka & Liira, Riitta. *Pyramidi 2, Polynomifunktiot.* 1-2. painos, Tammi, 2005.

[10] Kontkanen, Pekka & Liira, Riitta. *Pyramidi 4, Analyyttinen geometria.* 1-2. painos, Tammi, 2005.

[11] Kontkanen, Pekka & Liira, Riitta. *Pyramidi 7, Derivaatta.* 1-2. painos, Tammi, 2006.

[12] Boyer, Carl. *Tieteiden kuningatar, matematiikan historia osa 1.* Juva, 1994.

[13] Metsänkylä, Tauno. *Algebra.* Helsinki, 2003.

[14] Koppinen, Markku. *Algebran peruskurssi 1.* Turun yliopisto, 2005.

[15] Virtanen, Kalervo & Österdahl, Lasse. *Keskikoulun algebran harjoituskirja.* Porvoo, 1969.

[16] Pekkala, Kalervo & Oinas-Kukkonen, Heikki. *Lukion algebra 1.* Porvoo, 1969.

[17] Reis, Clive. *Abstract algebra An introduction to groups, rings and fields.* University of Western Ontario, Canada, 2011.

[18] Cohn, P.M. *Algebra volume 1.* University College London, 1989.

[19] Neuvonen, Timo. *Algebra (TKO).* Turun yliopisto, 1994.

[20] Neuvonen, Timo *Analyysi 1.* Turun yliopisto, 2009.

E-kirja:

[21] Mumford, David. *Indraś Pearls: the vision of Felix Klein/David Mumford, Caroline Series and David Wright; with cartoons by Larry Gonick.* Cambridge University Press, 2002.

Internet -lähteet:

[22] http://www.algebra.com/algebra/about/history/ (28.9.2012)

[23] http://en.wikipedia.org/wiki/Algebra (1.10.2012)

[24] http://www.ucs.louisiana.edu/ sxw8045/history.htm (5.10.2012)

[25] http://en.wikipedia.org/wiki/Abstract_algebra (5.10.2012)

[26] http://www.math.niu.edu/ beachy/abstract_algebra/guide/guide.pdf (5.10.2012)

[27] http://www.garnermath.com/downloads/Usiskin_Why-is-Algebra-Important.pdf (10.10.2012)

[28] http://www.mathgoodies.com/articles/why_learn_algebra.html (10.10.2012)

[29] http://library.thinkquest.org/22584/temh3002.htm (12.11.2012)

[30] http://www.sparknotes.com/math/algebra2/functions/section1.rhtml (30.11.2012)

[31] http://britton.disted.camosun.bc.ca/jbescher1.htm (18.2.2013)

[32] http://4e7221.medialib.glogster.com/media/
6f946ea2f8bf00ed175ee314c023692b15b4f
5e1779006ed1533ff0a956adc2f/
bilateral-symmetry.jpg (18.2.2013)

[33] http://nothingvia.tumblr.com/post/30256866714/cocoroachchanel-wasp-nest-apartment-houses-of (18.2.2013)

[34] http://dev.physicslab.org/Document.aspx?doctype=5&filename=
ModernAtomicNuclear_RotationalReflectionSymmetries.xml (20.2.2013)

[35] http://scienceforkids.kidipede.com/math/geometry/pictures/butterfly.jpg (20.2.2013)

[36] http://www.oph.fi/download/47345_lukion_opetussuunnitelman_perusteet_2003.pdf (18.3.2013)