Abstraktin algebran rakenteista sekä näiden välisistä morfismeista

Pro gradu -tutkielma
Kari Kostama
Matemaattisten tieteiden laitos
Oulun yliopisto
Kevät 2014

Sisältö

Johdanto

Ensimmäinen algebrallinen rakenne, joka tulee vastaan opintojen edetessä on ryhmä. Kuitenkin ensimmäinen lukujoukko, luonnolliset luvut, ja yhteenlasku eivät muodosta ryhmää. Muita vastaavia yhdistelmiä on, jotka tulevat jo alakoululaiselle tutuksi ja niitä ohjaavat selkeät säännöt, mutta niiden luokittelu jää syvemmin algebraan perehtyvän omille harteille. Tässä työssä esitetään niitä perusteita, joilla abstraktin algebran rakenteet muodostuvat.

Ensimmäisessä luvussa määritellään, mikä on laskutoimitus ja erotetaan joukosta erityisesti kahden alkion laskutoimitus. Tämän määritelmän tekemiseksi tarvitaan hieman kuvauksiin liittyvien perusteiden läpikäyntiä ja niihin liittyviä tuloksia.

Toisessa luvussa esitellään abstraktin algebran perusrakenne, jota kutsutaan magmaksi. Magma, eli grupoidi, koostuu joukosta ja tämän joukon sisäisestä laskutoimituksesta. Toisin sanoen magma on suljettu joukko siihen liitetyn laskutoimituksen suhteen. Magmasta edetään ominaisuus kerrallaan kohti ryhmää aluksi liitännäisyyden kautta ja sitten jaettavuuden kautta.

Liitännäisyys avaa mahdollisuuden muuttaa alkioiden välisen laskutoimituksen järjestystä. Neutraalialkio on nimensä mukaisesti neutraali, eli se ei muuta sen kanssa laskettavaa alkiota. Tämän ketjun lopuksi haetaan alkioiden käänteisalkioita jolloin näiden välinen laskutoimitus tuottaa neutraalialkion. Nämä ominaisuudet löytyvät ryhmältä.

Jaettavuus mahdollistaa saman tekijän pois jakamisen alkioista, mutta ei järjestyksen muuttamista useamman alkion tapauksessa. Tämä tarkoittaa, että kahden alkion välinen suhde, joissa on eräs yhteinen tekijä, kertoo kahden muun alkion välisestä suhteesta ilman tuota yhteistä tekijää. Tämä voidaan ajatella myös niin, että alkioilla on olemassa kummallekin puolelle oma käänteisalkio ja neutraalialkio. Kaksipuolisen neutraalialkion olemassaolo ei johda kaksipuoliseen käänteisalkioon, mutta toispuoleisten käänteisalkioiden välinen erilaisuus johtuu liitännäisyyden puuttumisesta. Se onkin viimeinen ryhmältä edellytettävä ominaisuus.

Lopuksi toisessa luvussa määritellään ryhmä ja annetaan tälle muita yh-

täpitäviä määritelmiä. Muissa määritelmissä jätetään pois jokin ei kriittinen ominaisuus, joka voidaan johtaa määritelmässä esitetyistä ehdoista.

Kolmannessa luvussa esitellään algebrallisten rakenteiden välisiä suhteita. Tähän liittyen määritellään homomorfismi, eli kuvaus, joka säilyttää rakenteen kahden eri joukon välillä. Tämä tarkoittaa, että alkujoukon alkioiden välisestä laskutoimituksesta muodostettu kuva-alkio on sama kuin samoista alkioista muodostettujen kuva-alkioiden välinen laskutoimitus kuvajoukossa. Koska homomorfismi on kuvaus, niin kuvauksen ominaisuudet, injektiivisyys ja surjektiivisuus, vaikuttavat sen toimintaan. Lopuksi osoitetaan, että jokaisella monoidilla, eli neutraalialkiolla varustetulla liitännäisellä magmalla, on olemassa isomorfinen kopio sen sisäisten kuvausten muodostamassa joukossa.

1 Kahden alkion laskutoimitus eli binäärinen operaatio

Laskutoimitus on tapa, jolla laskutoimituksesta riippuen yksi tai useampi alkio tuottaa uuden alkion. Yhden alkion tapauksessa käytetään nimitystä unäärinen, kahden alkion tapaksessa binäärinen ja kolmen alkion tapauksessa trenäärinen operaatio. Tarkastellaan seuraavaksi laskutoimituksen osasia hieman tarkemmin.

1.1 Kuvauksista

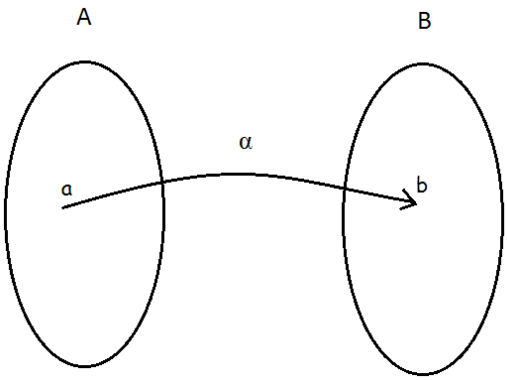
Kuvaus on yksi matematiikan keskeisiä käsitteitä, vaikka tällaisenaan nimitys ei kaikille ole tuttu. Kuvaus, tai monille tutumpi funktio, on alusta alkaen mukana yhteen- ja vähennyslaskujen muodossa. Tässä oletetaan, että joukko ja osajoukko ovat selviä käsitteitä, joten niitä ei tarvitse selventää.

Määritelmä 1.1. Olkoon A ja B joukkoja. Tällöin *kuvaus* joukolta A joukolle B on joukon A alkioiden liittäminen joukon B alkioihin niin, että jokaista joukon A alkiota kohden löytyy täsmälleen yksi alkio joukosta B. Jos α on kuvaus joukolta A joukolle B, niin tästä käytetään merkintää $\alpha : A \to B$ ja $\alpha(a)$ on *alkion a kuva* joukossa B.

Määritelmä 1.2. *Identiteettikuvaus* $\iota : A \to A$ säilyttää alkion itsellään. Siis kaikilla alkioilla $a \in A$ pätee $\iota(a) = a$.

Määritelmä 1.3. Olkoon A ja B joukkoja sekä kuvaus α joukolta A joukolle B. Tällöin joukkoa $\alpha(A) = \{y \in B \mid \alpha(x) = y,\ x \in A\}$ sanotaan *joukon A kuvaksi* joukossa B. Kuvauksen määritelmän nojalla $\alpha(A) \subseteq B$. Joukkoa $\alpha^{-1}(B) = \{x \in A \mid \alpha(x) = y,\ y \in B\}$ sanotaan *joukon B alkukuvaksi* joukossa A.

Seuraavaksi määritellään kuvauksille kolme ominaisuutta ja näissä jokaisessa oletetaan, että A ja B ovat kaksi joukkoa sekä kuvaus $\alpha : A \to B$.



Kuva 1: Kuvaus α yhdistää joukon A alkion a joukon B alkioon b.

Määritelmä 1.4. Jos joukon A kuva täyttää joukon B, eli $\alpha(A) = B$, niin tällaista kuvausta kutsutaan *surjektiiviseksi kuvaukseksi* eli lyhyesti *surjektioksi*.

Määritelmä 1.5. Jos kuvaus α kuvaa eri alkiot eri alkioiksi, toisin sanoen, jos $\alpha(a_1) \neq \alpha(a_2)$ aina, kun $a_1 \neq a_2$, niin tällaista kuvausta kutsutaan *injektiiviseksi kuvaukseksi* eli *injektioksi*.

Määritelmä 1.6. Jos kuvaus on surjektiivinen ja injektiivinen, niin sitä kutsutaan *bijektiiviseksi kuvaukseksi* eli *bijektioksi*.

Esimerkki 1.7. Identiteettikuvaus on bijektio.

Seuraavat lauseet luonnehtivat injektiivisyyttä ja surjektiivisuutta toisella tavalla sekä kertovat kuvan ja alkukuvan yhteydestä kuvauksen ominaisuuksiin.

Lause 1.8. *Olkoon kuvaus $\alpha : A \to B$. Tämä kuvaus on injektio, jos ja vain jos $\alpha^{-1}(\alpha(C)) = C$ jokaiselle joukon A osajoukolle C.*

Todistus.
Olkoon kuvaus α injektio ja joukko $C \subseteq A$ sekä alkio $x \in \alpha^{-1}(\alpha(C))$. Tällöin alkio $\alpha(x) \in \alpha(C)$. Siis on olemassa alkio $y \in C$, jolle $\alpha(y) = \alpha(x)$. Koska kuvaus α on injektio, niin $x = y$. Täten $x \in C$ ja $\alpha^{-1}(\alpha(C)) \subseteq C$.

Jos $z \in C$, niin kuvan ja alkukuvan määritelmän nojalla $z \in \alpha^{-1}(\alpha(C))$ joten $C \subseteq \alpha^{-1}(\alpha(C))$. Siis $\alpha^{-1}(\alpha(C)) = C$.
Olkoon $\alpha^{-1}(\alpha(C)) = C$ jokaiselle osajoukolle $C \subseteq A$, siis erityisesti jokaiselle yhden alkion joukolle eli *yksiölle* $\{x\} \subset A$. Olkoon $x, y \in A$, joille $\alpha(x) = \alpha(y)$. Tällöin

$$\{x\} = \alpha^{-1}(\alpha(\{x\})) = \alpha^{-1}(\{\alpha(x)\}) = \alpha^{-1}(\{\alpha(y)\}) = \alpha^{-1}(\alpha(\{y\})) = \{y\},$$

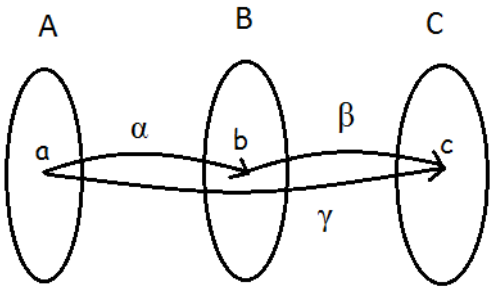
eli $x = y$. Näin ollen kuvaus α on injektio □

Lause 1.9. *Olkoon kuvaus $\alpha : A \to B$. Tämä kuvaus on surjektio, jos ja vain jos $\alpha(\alpha^{-1}(D)) = D$ jokaiselle joukon B osajoukolle D.*

Todistus.
Olkoon kuvaus α surjektio ja joukko $D \subseteq B$. Olkoon $x \in D$. Koska α on surjektio, niin on olemassa ainakin yksi alkio $y \in A$, että $\alpha(y) = x$. Toisin sanoen alkio $y \in \alpha^{-1}(D) \subseteq A$. Nyt alkion y kuva $\alpha(y) = x \in \alpha(\alpha^{-1}(D))$. Siis $D \subseteq \alpha(\alpha^{-1}(D))$.
Olkoon $x \in \alpha(\alpha^{-1}(D))$. Koska joukon D alkukuva $\alpha^{-1}(D) = \{y \in A \mid \alpha(y) \in D\}$ ja kuvaus α on surjektio, niin on olemassa ainakin yksi alkio $y \in A$, jolle $x = \alpha(y) \in D$. Tällöin $\alpha(\alpha^{-1}(D)) \subseteq D$ ja näin ollen $\alpha(\alpha^{-1}(D)) = D$.
Olkoon $\alpha(\alpha^{-1}(D)) = D$ jokaiselle joukolle $D \subseteq B$. Erityisesti tämä toimii koko joukolle B. Koska α on kuvaus joukolta A joukolle B, niin $\alpha^{-1}(B) \subseteq A$. Tällöin $\alpha(\alpha^{-1}(B) = B \subseteq \alpha(A)$ ja kuvauksen määritelmän nojalla $\alpha(A) \subseteq B$. Siis $\alpha(A) = B$, eli kuvaus α on surjektio. □

Määritelmä 1.10. Olkoot $\alpha : A \to B$ ja $\beta : B \to C$ kuvauksia. Jos a on joukon A alkio, niin sen kuva $\alpha(a) = b$ on joukon B alkio. Jatkaen tätä ketjua edelleen saadaan $\beta(b) = c$, joka on joukon C alkio. Nyt $c = \beta(\alpha(a))$, jolloin voidaan liittää joukon A alkioita joukon C alkioihin, eli on olemassa *yhdistetty kuvaus* $\gamma : A \to C$, joka voidaan ilmaista kuvausten α ja β avulla. Siis $\gamma(a) = (\beta \circ \alpha)(a) = \beta(\alpha(a)) = c$.

Määritelmä 1.11. Olkoon A ja B joukkoja sekä kuvaus $\alpha : A \to B$. Jos on olemassa kuvaus $\gamma : B \to A$, jolla $\gamma(b) = a$, jos ja vain jos $\alpha(a) = b$, niin kuvaus γ on kuvauksen α *käänteiskuvaus* ja merkitään $\gamma = \alpha^{-1}$.



Kuva 2: Kuvaus α kuvaa alkion $a \in A$ alkiolle $b \in B$, joka puolestaan kuvautuu alkiolle $c \in C$ kuvauksella β. Kuvausten α ja β yhdiste, kuvaus γ, kuvaa siis alkion $a \in A$ alkioksi $c \in C$.

Huomautus 1.12. Käänteiskuvauksen ja alkukuvan merkintää ei tule sekoittaa keskenään. Alkukuvan yhteydessä käytetään joukkoa ja käänteiskuvauksen kanssa on kyseessä alkio.

Lause 1.13. *Kuvauksella on käänteiskuvaus, jos ja vain jos se on bijektiivinen.*

Todistus.
Olkoon A ja B joukkoja sekä kuvaus $\alpha : A \to B$. Oletetaan, että kuvauksella α on käänteiskuvaus $\alpha^{-1} : B \to A$. Siis jos $\alpha(a) = b$, niin se on yhtäpitävää sen kanssa, että $\alpha^{-1}(b) = a$ kaikilla $a \in A$. Olkoon a_1,$a_2 \in A$ ja $\alpha(a_1) = \alpha(a_2)$. Tällöin $\alpha^{-1}(\alpha(a_1)) = \alpha^{-1}(\alpha(a_2))$, mistä seuraa $a_1 = a_2$. Siis kuvaus α on injektiivinen.
Jos $b \in B$, niin on olemassa $a \in A$, jolle $\alpha^{-1}(b) = a$. Tällöin $\alpha(a) = \alpha(\alpha^{-1}(b)) = b$ kaikilla $b \in B$, eli $\alpha(A) = B$ ja kuvaus α on surjektiivinen. Kuvaus α on tällöin sekä injektio että surjektio, eli bijektio.
Olkoon kuvaus $\alpha : A \to B$ bijektiivinen kuvaus. Määritellään kuvaus $\gamma : B \to A$, joka osoittautuu kuvauksen α käänteiskuvaukseksi. Jos $b \in B$, niin $\gamma(b) = a$, missä $a \in A$ on alkion b alkukuva kuvauksella α. Koska α on bijektiivinen, niin se on myös surjektiivinen, jolloin on ainakin yksi alkio $a \in A$, jolle $\alpha(a) = b$. Lisäksi α on myös injektiivinen, joten $a \in A$ on yksikäsittei-

nen. Näin määritelty kuvaus γ on kuvauksen α käänteiskuvaus, eli $\alpha(a) = b$ ja $\gamma(b) = a$ $\square$

Huomautus 1.14. Kun käänteiskuvaus on olemassa, eli kuvaus α on bijektio, niin yksiöiden tapauksessa käänteiskuvaus ja alkukuva tuottavat seuraavaa,
alkukuva: $\alpha^{-1}(\alpha(\{a\})) = \alpha^{-1}(\{\alpha(a)\}) = \{a\}$ ja
käänteiskuvaus: $(\alpha^{-1} \circ \alpha)(a) = \alpha^{-1}(\alpha(a)) = a \in \{a\}$.
Nämä muistuttavat toisiaan ja voidaankin ajatella olevan sama asia, mutta vain yksiöiden tapauksessa.

Lause 1.15. *Olkoon kuvaus $\alpha : A \to B$ bijektio sekä kuvaus $\alpha^{-1} : B \to A$ sen käänteiskuvaus. Tällöin kuvaus α^{-1} on bijektio, $\alpha^{-1} \circ \alpha = \iota_A$ ja $\alpha \circ \alpha^{-1} = \iota_B$.*

Todistus.
Koska kuvaus α^{-1} on kuvauksen α käänteiskuvaus, niin ehdosta $\alpha(a) = b$ seuraa $\alpha^{-1}(b) = a$. Yhtälöllä $\alpha^{-1}(b) = a$ on jokaiselle $a \in A$ täsmälleen yksi ratkaisu $b \in B$. Tällöin kuvaus α^{-1} on bijektio.
Koska $\alpha(a) = b$ ja $\alpha^{-1}(b) = a$, niin kaikilla $a \in A$ pätee $(\alpha^{-1} \circ \alpha)(a) = \alpha^{-1}(\alpha(a)) = \alpha^{-1}(b) = a$ ja kaikilla $b \in B$ pätee $(\alpha \circ \alpha^{-1})(b) = \alpha(\alpha^{-1}(b)) = \alpha(a) = b$ $\square$

Lause 1.16. *Jos kuvaukset $\alpha : A \to B$ ja $\beta : B \to C$ ovat bijektioita, niin yhdistetyt kuvaukset $(\beta \circ \alpha)$ ja $(\beta \circ \alpha)^{-1} = (\alpha^{-1} \circ \beta^{-1})$ ovat bijektioita. Lisäksi jos $C = A$, niin yhdistetyt kuvaukset $(\alpha \circ \beta)$ ja $(\alpha \circ \beta)^{-1}$ ovat myös bijektioita.*

Olkoon alkiot $a_1, a_2 \in A$ ja $c \in C$. Jos kuvaukset α ja β ovat bijektioita, niin ne ovat myös surjektioita. Tällöin $\alpha(A) = B$ ja $\beta(B) = C$, siis $(\beta \circ \alpha)(A) = \beta(\alpha(A)) = \beta(B) = C$, jolloin yhdistetty kuvaus $\beta \circ \alpha$ on surjektio. Koska kuvaukset α ja β ovat bijektioita, niin ne ovat myös injektioita. Tällöin, jos $a_1 \neq a_2$, niin $\alpha(a_1) \neq \alpha(a_2)$. Tästä seuraa, että $\beta(\alpha(a_1)) \neq \beta(\alpha(a_2))$, eli $(\beta \circ \alpha)(a_1) \neq (\beta \circ \alpha)(a_2)$. Näin ollen yhdistetty kuvaus $\beta \circ \alpha$ on injektio, siis se on bijektio.
Koska yhdistetty kuvaus $\beta \circ \alpha$ on bijektio, niin lauseiden 1.13 ja 1.15 nojalla

sillä on olemassa käänteiskuvaus $(\beta \circ \alpha)^{-1}$ ja myös se on bijektio.
Nyt $(\beta \circ \alpha) \circ (\beta \circ \alpha)^{-1}(c) = \iota_C(c)$, eli $\beta(\alpha((\beta \circ \alpha)^{-1}(c))) = c$. Tästä saadaan, että $\alpha((\beta \circ \alpha)^{-1}(c)) = \beta^{-1}(c)$, josta saadaan $(\beta \circ \alpha)^{-1}(c) = \alpha^{-1}(\beta^{-1}(c))$ eli $(\beta \circ \alpha)^{-1}(c) = (\alpha^{-1} \circ \beta^{-1})(c)$.
Jos $C = A$, niin yhdistetyt kuvaukset $(\alpha \circ \beta)$ ja $(\alpha \circ \beta)^{-1}$ ovat tällöin määriteltyjä ja edelliseen nojaten bijektioita □

1.2 Laskutoimitus

Laskutoimituksesta helpoin esimerkki lienee yhteenlasku kokonaislukujen joukossa. Tarkemmin sanottuna valitaan kokonaisluvuista kaksi edustajaa, esimerkiksi luvut m ja n, jotka yhdistetään yhteenlaskulla, ja saadaan kokonaisluku $m + n$, joka on yksikäsitteinen tälle lukuparille. Yleisesti laskutoimituksen määritelmä on seuraava.

Määritelmä 1.17. Olkoon A joukko, tällöin jokainen kuvaus λ joukolta $A \times A$ joukolle A on *kahden alkion laskutoimitus* eli *binäärinen operaatio* joukossa A. Kuvauksen arvo $\lambda(a, b)$ parilla $(a, b) \in A \times A$ on tällöin laskutoimituksen *tulos* joukon A alkioilla a ja b.

Huomautus 1.18. Aina ei ole tarkoituksenmukaista kirjoittaa perusteellisesti $\lambda : A \times A \to A$ ja $\lambda(a, b) = a + b$ kaikilla $a, b \in A$. Kun joukko ja laskutoimitus ovat selviä, on riittävää käyttää joitakin seuraavista merkinnöistä kuvailemaan laskutoimitusta:

$$
\begin{gathered}
a \circ b \text{ , ”}a \text{ pallo } b\text{”}, \\
a \times b \text{ , ”}a \text{ kertaa } b\text{”}, \\
a \cdot b \text{ , ”}a \text{ kertaa } b\text{” tai ”}a \text{ piste } b\text{”}, \\
a + b \text{ , ”}a \text{ plus } b\text{”}, \\
ab \text{ , ”}a \text{ kertaa } b\text{”}, \\
a * b \text{ , ”}a \text{ tähti } b\text{” .}
\end{gathered}
$$

Esimerkki 1.19. Olkoon $\mathbb{R}_+$ positiivisten reaalilukujen joukko. Ovatko seuraavat kuvaukset laskutoimituksia joukossa $\mathbb{R}_+$?

i) $\alpha : (i, j) \to i^2$, missä $i, j \in \mathbb{R}_+$.
ii) $\beta : (i, j) \to i \cdot j$, missä $i, j \in \mathbb{R}_+$.
iii) $\gamma : (i, j) \to i - j$, missä $i, j \in \mathbb{R}_+$.
iv) $\delta : (i, j) \to i + j^2$, missä $i, j \in \mathbb{R}_+$.

Ratkaisu.

i) Kyllä. Positiivinen reaaliluku kerrottuna itsellään tuottaa aina positiivisen reaaliluvun.

ii) Kyllä. Lukujen i ja j ollessa positiivisia reaalilukuja on niiden tulokin myös positiivinen reaaliluku.

iii) Ei. On mahdollista valita luku j niin, että $j > i$, jolloin $i - j < 0 \notin \mathbb{R}_+$.

iv) Kyllä. Kohdan i) nojalla j^2 on positiivinen reaaliluku ja positiivisten reaalilukujen yhteenlasku tuottaa myös positiivisen reaaliluvun.

2 Magmoista

Alkujaan tätä abstraktin algebran rakennetta kutsuttiin grupoidiksi. Ei aivan ryhmä, mutta kuitenkin grupoidi on suljettu jonkin laskutoimituksen suhteen. Sittemmin tälle on myös keksitty nimitys magma, mikä on ehkä saanut alkunsa pienoisesta kielellisestä vitsistä. Edelleen kuitenkin käytetään grupoidi nimitystä magma nimityksen ohella. Magmassa yhdistetään epätyhjä joukko ja joukon suhteen suljettu laskutoimitus. Kun edellytetään, että magman laskutoimitus on liitännäinen eli assosiatiivinen ja magmasta löytyy neutraalialkio sekä käänteisalkio, on luotu ryhmä. Jos laskutoimitus on lisäksi vaihdannainen eli kommutatiivinen on kyseessä Abelin ryhmä. Kuitenkin ennen ryhmää on olemassa rakenteita, joihin vaaditaan vain osa ryhmään edellytetyistä ominaisuuksista.

2.1 Magma ja alimagma

Määritelmä 2.1. Olkoon M joukko ja λ laskutoimitus joukossa M. Toisin sanoen joukko M on suljettu kuvauksen λ suhteen. Tällöin paria (M,λ) kutsutaan *magmaksi*.

Esimerkki 2.2. Olkoon $M = \{1, 2, 3\}$ ja laskutoimitus λ joukossa M määritellään seuraavan taulukon mukaisesti:

λ	1	2	3
1	1	2	3
2	2	1	1
3	2	3	3

Tällöin pari (M,λ) on magma. Jos käytetään laskutoimituksesta λ merkintää $\cdot$, niin

$$1 \cdot 1 = 1, 1 \cdot 2 = 2, 2 \cdot 2 = 1, 3 \cdot 2 = 3, \ jne.$$

Esimerkki 2.3. Olkoon $M = \{0, 1, 2, ...\}$ ja kuvaus $^\wedge : M \times M \to M$. Selvästi alkioiden $a, b \in M$ tulos $a^\wedge b = a^b$ kuuluu joukkoon M, eli $^\wedge$ on laskutoimitus joukossa M. Siis $(M,^\wedge)$ on magma.

Kun vastaisuudessa käytetään ilmaisua 'magma M', niin tämä tarkoittaa joukkoa M sekä laskutoimitusta λ joukossa M, eli tällöin tarkoitetaan paria (M,λ). Jos λ ilmaistaan jollakin huomautuksessa 1.18 käytetyistä merkinnöistä, niin voidaan kirjoittaa, esimerkiksi $(M, \circ)$, $(M, \cdot)$ tai $(M, +)$, mikä edelleen tarkoittaa magmaa M sekä tähän liitettyä laskutoimitusta.

Määritelmä 2.4. Magmat (M, λ) ja (M', λ') *ovat yhtäsuuria*, jos ja vain jos $M = M'$ ja $\lambda = \lambda'$.

Määritelmä 2.5. Olkoon (M, λ) magma. Epätyhjää joukkoa $O \subseteq M$ sanotaan magman M *alimagmaksi*, jos se on suljettu laskutoimituksen λ suhteen, eli kaikilla alkiolla $c, d \in O$ tulos $\lambda(c, d) \in O$.

2.2 Vaihdannainen ja liitännäinen magma

Määritelmä 2.6. Olkoon $(M, *)$ magma. Jos
i) $a * b = b * a$ kaikilla $a, b \in M$, niin magma M on *vaihdannainen* eli *kommutatiivinen*.
ii) $a*(b*c) = (a*b)*c$ kaikilla $a, b, c \in M$, niin magma M on *liitännäinen* eli *assosiatiivinen*. Liitännäistä magmaa kutsutaan *puoliryhmäksi*. Vastaavasti puoliryhmän alimagma on selvästi puoliryhmä ja näin ollen sitä sanotaan *alipuoliryhmäksi*.

Esimerkki 2.7. Reaalilukujen joukossa yhteen- ja kertolasku ovat omillaan sekä liitännäisiä että vaihdannaisia laskutoimituksia. Näitä sekoitettaessa on kuitenkin huomioitava laskujärjestys, eli kertolasku on tehtävä ennen yhteenlaskua. Jos $a, b, c \in \mathbb{R}$, niin $a + b = b + a$, $(a + b) + c = a + (b + c)$, $a \cdot b = b \cdot a$ ja $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, mutta $a + (b \cdot c) \neq (a + b) \cdot c$.

Kaikki magmat eivät kuitenkaan ole vaihdannaisia, eivätkä ne välttämättä ole liitännäisiäkään. Seuraavassa esimerkissä käy ilmi, että sellaisiakin magmoja on olemassa.

Esimerkki 2.8. Olkoon $M = \{1, 2\}$ ja kuvaus $\bullet$ on laskutoimitus joukossa M, joka määritellään seuraavasti:

$\bullet$	1	2
1	1	1
2	2	1

Tällöin $1 \bullet 2 = 1 \neq 2 = 2 \bullet 1$, eli magma M ei ole vaihdannainen.
Myös $(2 \bullet 1) \bullet 2 = 2 \bullet 2 = 1 \neq 2 = 2 \bullet 1 = 2 \bullet (1 \bullet 2)$, eli magma M ei ole liitännäinen.

Esimerkki 2.9. Olkoon $M = \mathbb{C}$ ja kuvaus $*$ laskutoimitus joukossa M, jossa otetaan alkioparin a ja b tulon kompleksikonjugaatti, eli $* : (a, b) \to \overline{ab}$, kaikilla $a, b \in M$. Koska tulo on kompleksilukujen joukossa vaihdannainen operaatio, niin $a * b = \overline{ab} = \overline{ba} = b * a$. Siis tämä laskutoimitus on vaihdannainen, mutta ei liitännäinen, sillä $(a * b) * c = \overline{ab} * c = \overline{\overline{ab}c} = ab\overline{c} \neq \overline{a}bc = \overline{a\overline{bc}} = a * \overline{bc} = a * (b * c)$.

Seuraavaksi esitellään joukko M_X, jonka rakentamiseksi ei vaadita kuin jokin epätyhjä joukko X ja kuvauksia tältä joukolta itselleen. Näiden kuvausten joukko varustettuna kuvauksien yhdistämisellä toteuttaa monia vaatimuksia, joista tämä on ensimmäinen.

Lause 2.10. *Olkoon X epätyhjä joukko. Kaikki kuvaukset joukolta X itselleen muodostavat puoliryhmän M_X, jonka laskutoimituksena on kuvauksien yhdistäminen $\circ$.*

Todistus.
Olkoon X epätyhjä joukko. Olkoon $\mu : X \to X$, $\lambda : X \to X$ ja $\gamma : X \to X$. Tällöin $\mu \circ \lambda$ on kuvaus joukolta X itselleen, sillä $(\mu \circ \lambda)(x) = \mu(\lambda(x)) = \mu(y) = z \in X$ kaikilla $x \in X$. Näin ollen $\circ$ on laskutoimitus ja pari $(M_X, \circ)$ on magma.
Kuvausten yhdistäminen on myös liitännäinen, sillä

$$((\lambda \circ \gamma) \circ \mu)(x) = (\lambda \circ \gamma)(\mu(x)) = \lambda(\gamma(\mu(x))) = \lambda((\gamma \circ \mu)(x)) = (\lambda \circ (\gamma \circ \mu))(x)$$

kaikilla $x \in X$, siten $(M_X, \circ)$ on puoliryhmä $\square$

Mikäli on selvää, että kyseessä on kuvausten yhdistäminen, voidaan $\circ$ jättää pois kuvausten välistä kirjoittamisen helpottamiseksi. Tämä on yleinen käytäntö kertolaskun ($\cdot$ tai $\times$) yhteydessä. Tässä työssä kuitenkin pidetään operaatiomerkki mukana luettavuuden helpottamiseksi.

2.3 Neutraali- ja käänteisalkio magmassa

Määritelmä 2.11. Jos magmassa $(M, *)$ on alkio e, jolle pätee
i) $a * e = a$ kaikilla $a \in M$, niin tätä alkiota kutsutaan *oikeanpuoliseksi neutraalialkioksi* ja merkitään $e = e_r$.
ii) $e * a = a$ kaikilla $a \in M$, niin tätä alkiota kutsutaan *vasemmanpuoliseksi neutraalialkioksi* ja merkitään $e = e_l$.

Esimerkki 2.12. Pari $(\mathbb{Z}_+ \cup \{0\}, ^\wedge)$ tarkoittaa potenssilaskua ei negatiivisten kokonaislukujen joukossa. Tutummin tämän voi kirjoittaa $a^\wedge b = a^b$. Parin rakenteelliset ominaisuudet rajoittuvat oikeanpuoliseen neutraalialkioon 1. Vasemmalta tämä ei niin sanotusti pelaakkaan: $1^\wedge x = 1^x = 1$ kaikilla $x \in \mathbb{Z}_+ \cup \{0\}$. Potenssilasku ei ole vaihdannainen, sillä $a^\wedge b = a^b \neq b^a = b^\wedge a$, eikä liitännäinen, koska $(a^\wedge b)^\wedge c = (a^b)^c = a^{bc} \neq a^{b^c} = a^\wedge(b^\wedge c)$.

Määritelmä 2.13. Olkoon M magma. Alkiota e, joka on sekä vasemmanettä oikeanpuolinen neutraalialkio sanotaan *kaksipuoliseksi neutraalialkioksi* tai pelkästään *neutraalialkioksi*.

Lause 2.14. *Jos magmalla $(M, *)$ on neutraalialkio e, niin se on yksikäsitteinen.*

Todistus.
Olkoon M magma ja alkiot e ja e' sen neutraalialkioita. Koska e on neutraalialkio, niin $e * e' = e'$. Myös e' on neutraalialkio joten $e * e' = e$. Tästä seuraa, että $e' = e$ $\square$

Määritelmä 2.15. Liitännäistä magmaa, eli puoliryhmää, E kutsutaan *monoidiksi*, jos sillä on neutraalialkio e. Monoidin E alipuoliryhmää D sanotaan *alimonoidiksi*, mikäli $e \in D$.

Määritelmä 2.16. Olkoon $(M, *)$ magma ja e sen neutraalialkio. Jos magman M alkioille x ja x' pätee,
i) $x * x' = e$, niin alkiolla x on *oikeanpuolinen käänteisalkio*, ja merkitään $x' = x_r$.
ii) $x' * x = e$ niin alkiolla x on *vasemmanpuolinen käänteisalkio*, ja merkitään $x' = x_l$.
iii) $x * x' = e = x' * x$, niin alkio x' on alkion x *käänteisalkio*, ja merkitään $x' = x^{-1}$.

Esimerkki 2.17. Nämä parit ovat monoideja:

- $(\mathbb{N}, +)$, luonnolliset luvut ja yhteenlasku muodostavat monoidin, jonka neutraalialkiona toimii luku 0.
- $(\mathbb{N}, \cdot)$, luonnolliset luvut ja kertolasku muodostavat monoidin, jonka neutraalialkiona toimii luku 1.
- $(\mathbb{Z}, \cdot)$, kokonaisluvut ja kertolasku muodostavat monoidin, joka on edellisen monoidin laajennus.

Lause 2.18. *Monoidin $(E, *)$ alkiolla x on käänteisalkio x^{-1}, jos ja vain jos sillä on vasemman- ja oikeanpuolinen käänteisalkio. Lisäksi käänteisalkio on yksikäsitteinen.*

Todistus.
Olkoon x^{-1} alkion x käänteisalkio. Tällöin määritelmän nojalla $x^{-1} * x = e$ ja $x * x^{-1} = e$, jolloin alkiolla x on vasemman- ja oikeanpuolinen käänteisalkio. Olkoon alkiolla x vasemmanpuolinen käänteisalkio x_l ja oikeanpuolinen käänteisalkio x_r. Koska E on monoidi, niin laskutoimituksen liitännäisyyden nojalla saadaan

$$x_l = x_l * e = x_l * (x * x_r) = (x_l * x) * x_r = e * x_r = x_r.$$

Siis x_l on alkion x käänteisalkio ja merkitään $x_l = x^{-1}$. Olkoon x' myös alkion x käänteisalkio. Tällöin

$$x' = x' * e = x' * (x * x^{-1}) = (x' * x) * x^{-1} = e * x^{-1} = x^{-1} \quad \square$$

Aiemmin osoitettiin, että joukko M_X ja kuvausten yhdistäminen $\circ$ muodostavat puoliryhmän. Seuraavassa lauseessa osoitetaan, että sillä on myös neutraalialkio.

Lause 2.19. *Olkoon X epätyhjä joukko, tällöin $(M_X, \circ)$ on neutraalialkiolla varustettu puoliryhmä, eli monoidi.*

Todistus.
Olkoon X epätyhjä joukko. Lauseen 2.10 mukaan $(M_X, \circ)$ on puoliryhmä. Olkoon $\iota : X \to X$ identiteettikuvaus. Jos $\mu \in M_X$, niin $(\mu \circ \iota)(x) = \mu(\iota(x)) = \mu(x) = \iota(\mu(x)) = (\iota \circ \mu)(x)$. Siis $\iota \circ \mu = \mu = \mu \circ \iota$ kaikilla $\mu \in M_X$, jolloin identiteettikuvaus ι toimii puoliryhmän $(M_X, \circ)$ neutraalialkiona. Siis $(M_X, \circ)$ on monoidi. □

Kaikilla monoidin $(M_X, \circ)$ alkioilla ei kuitenkaan ole käänteisalkiota.

Esimerkki 2.20. Olkoon $X = \{1, 2, 3\}$ ja kuvaus $\sigma \in M_X$, joka kuvaa jokaisen alkion ykköseksi, siis $\sigma(x) = 1$ kaikilla $x \in X$. Tällöin kuvauksella σ ei ole käänteiskuvausta. Jos on olemassa $\gamma \in M_X$, jolle $\gamma \circ \sigma = \iota$, niin $1 = \iota(1) = (\gamma \circ \sigma)(1) = \gamma(\sigma(1)) = \gamma(1)$ ja $2 = \iota(2) = (\gamma \circ \sigma)(2) = \gamma(\sigma(2)) = \gamma(1)$. Tällöin γ kuvaisi alkion 1 kahdelle eri alkiolle, mikä on ristiriita kuvauksen määritelmän kanssa.

Myöhemmin tarkastellaan monoidin M_X osajoukkoa M_X^*, jossa kaikilla kuvauksilla on käänteiskuvaus, toisin sanoen jokainen tämän osajoukon kuvaus on bijektiivinen. Osoittautuu, että tämä joukko varustettuna kuvausten yhdistämisellä on ryhmä.
Ennen kuin tarkastellaan ryhmän ominaisuuksia tarkemmin, tutkitaan magmoja, jotka eivät ole liitännäisiä.

2.4 Kvasiryhmä ja silmukka

Kun magman laskutoimitukselta vaaditaan jakolaskun toimivuutta, saadaan ryhmän kaltainen rakenne, jonka ei tarvitse olla liitännäinen. Tämä siis tarkoittaa, että yhtäpitävyydestä $ab = ac$ seuraa $b = c$ ja vastaavasti yhtälöstä $ba = ca$ seuraa $b = c$. Jokaiselle kvasiryhmän alkiolle on olemassa oikean- ja vasemmanpuolinen neutraalialkio, mutta usein nämä eivät ole samat. Mikäli neutraalialkio on olemassa, niin se ei välttämättä ole yksikäsitteinen. Silmukalta vaaditaan neutraalialkion yksikäsitteisyyttä, mutta oikean- ja vasemmanpuolinen käänteisalkio eivät välttämättä ole samat. Käänteisalkioiden olemassa olo edellyttää liitännäisyyden olemassaoloa.

Määritelmä 2.21. *Kvasiryhmä* on magma, jossa jakolasku 'toimii aina'. Siis jos $(Q, *)$ on kvasiryhmä, niin jokaista joukon Q alkiota a ja b kohden on olemassa yksikäsitteiset joukon Q alkiot x ja y, joille pätee
i) $a * x = b$
ii) $y * a = b$.
Näiden yhtälöiden yksikäsitteiset ratkaisut kirjoitetaan usein $x = a\backslash b$ ja $y = b/a$, missä $\backslash$ ja $/$ vastaavat vasemmalta ja oikealta jakamista.

Esimerkki 2.22. Seuraavat parit ovat kvasiryhmiä.

- $(\mathbb{Z}, -)$, kokonaisluvut varustettuna vähennyslaskulla.
- $(\mathbb{Q}^*, \div)$ ja $(\mathbb{R}^*, \div)$, nollasta poikkeavien rationaali- tai realilukujen jakolasku.

Esimerkki 2.23. Tutkitaan kokonaislukujen erotusta tarkemmin. Esimerkiksi luvun a oikeanpuolinen käänteisalkio on luku a itse, sillä $a - a = 0$. Oikeanpuolinen neutraalialkio e_r on luku 0, sillä $a - 0 = a$ kaikilla $a \in \mathbb{Z}$. Vasemmanpuolinen neutraalialkio luvulle 5 on luku 10, sillä $10 - 5 = 5$. Kuitenkaan tämä ei ole sama toisille luvuille, koska esimerkiksi $10 - 6 = 4$. Osoittautuu, että jokaisella luvulla on oma vasemmanpuolinen neutraalialkio. Jos $b \in \mathbb{Z}$, niin tämän vasemmanpuolinen neutraalialkio on luku $2b$, sillä $2b - b = b$.

Lisäksi jokaisella luvulla on oma vasemmanpuolinen käänteisalkio; luvun b vasemmanpuolinen käänteisalkio on luku $3b$, sillä $3b - b = 2b$.

Määritelmä 2.24. Kvasiryhmää kutsutaan *silmukaksi* eli *luupiksi*, jos sillä on neutraalialkio.

Lause 2.25. *Olkoon $(S, *)$ silmukka ja e sen neutraalialkio. Tällöin alkiolla $s \in S$ on oikeanpuolinen käänteisalkio s_r ja vasemmanpuolinen käänteisalkio s_l.*

Todistus.
Olkoon $s \in S$. Kvasiryhmän määritelmän nojalla yhtälöillä $s * x = e$ ja $y * s = e$ on olemassa yksikäsitteiset ratkaisut $x, y \in S$. Merkitään näitä $x = s_r$ ja $y = s_l$ □

Huomautus 2.26. Liitännäisyys ei toimi yleisesti, eli

$$s_l = s_l * e = s_l * (s * s_r) \neq (s_l * s) * s_r = e * s_r = s_r,$$

joten alkion s oikeanpuolinen ja vasemmanpuolinen käänteisalkio eivät välttämättä ole samat.

Lause 2.27. *Olkoon $(A, *)$ liitännäinen silmukka. Tällöin alkiolla $a \in A$ on yksikäsitteinen käänteisalkio a^{-1}.*

Todistus.
Lauseen 2.25 nojalla alkiolla $a \in A$ on olemassa oikeanpuolinen ja vasemmanpuolinen käänteisalkio, eli on olemassa alkiot $a_r, a_l \in A$, joille $a * a_r = e$ ja $a_l * a = e$. Koska silmukka A on liitännäinen, niin huomautuksen 2.26 yhtälö muuttuu muotoon

$$a_l = a_l * e = a_l * (a * a_r) = (a_l * a) * a_r = e * a_r = a_r,$$

eli $a_l = a_r$. Merkitään $a_l = a_r = a^{-1}$.
Olkoon $a' \in A$ myös alkion a käänteisalkio. Tällöin

$$a' = a' * e = a' * (a * a^{-1}) = (a' * a) * a^{-1} = e * a^{-1} = a^{-1},$$

eli $a' = a^{-1}$ jolloin a^{-1} on yksikäsitteinen □

2.5 Ryhmä

Ryhmän rakenteeseen päädytään kahta reittiä. Liitännäinen magma, josta löytyy neutraalialkio on monoidi. Kun monoidille vaaditaan käänteisalkioiden olemassaoloa, päädytään ryhmän rakenteeseen. Vaihtoehtoisesti oletetaan magmassa olevan aina toimiva jakolasku ja vaaditaan neutraalialkion olemassaoloa jolloin saadaan silmukka. Kun lopuksi vaaditaan, että silmukassa oleva laskutoimitus on liitännäinen, saavutaan jälleen ryhmän rakenteeseen.

Määritelmä 2.28. Monoidia G sanotaan *ryhmäksi*, mikäli sen jokaisella alkiolla on käänteisalkio. Kootusti voidaan sanoa, että ryhmä on kolmikko $(G, *, e)$, jolle

- G on joukko,
- $* : G \times G \to G$ on laskutoimitus joukossa G,
- $*$ on assosiatiivinen, eli $g*(h*k) = (g*h)*k$ kaikilla alkioilla $g, h, k \in G$,
- e on neutraalialkio joukossa G, eli $g * e = g = e * g$ kaikilla alkioilla $g \in G$ ja
- kaikilla alkioilla $g \in G$ on olemassa alkio $h \in G$, jolle $g * h = e = h * g$. Tätä yksikäsitteisesti alkion g määräämää alkiota h sanotaan alkion g käänteisalkioksi ja sitä merkitään g^{-1}.

Jos lisäksi $*$ on vaihdannainen, eli $g * h = h * g$ kaikilla alkioilla $g, h \in G$, niin tällaista ryhmää kutsutaan *Abelin ryhmäksi*.

Esimerkki 2.29. Seuraavat kolmikot ovat ryhmiä:

- $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$ ja $(\mathbb{R}, +, 0)$,
- $(\mathbb{Q}^*, \cdot, 1)$ ja $(\mathbb{R}^*, \cdot, 1)$.

Seuraavissa lauseissa osoitetaan, että ryhmärakenne seuraa, vaikka kaikkia määritelmän ehtoja ei vaadittaisi, sillä ne ovat johdettavissa annetuista ehdoista.

Lause 2.30. *Olkoon $(G, *)$ puoliryhmä ja oletetaan, että sillä on oikeanpuolinen neutraalialkio $e_r \in G$. Lisäksi jokaisella joukon G alkiolla on oikeanpuolinen käänteisalkio. Tällöin $(G, *, e_r)$ on ryhmä.*

Todistus.
Osoitetaan ensiksi, että $(G, *, e_r)$ on monoidi. Koska $(G, *)$ on puoliryhmä ja $x * e_r = x$ kaikilla $x \in G$, riittää osoittaa, että $x = e_r * x$ kaikilla $x \in G$. Olkoon x' alkion x oikeanpuolinen käänteisalkio, jolloin $x * x' = e_r$. Tällöin saadaan

$$\begin{aligned} e_r * x &= (e_r * x) * e_r = e_r * (x * e_r) = e_r * (x * (x' * (x')')) \\ &= e_r * ((x * x') * (x')') = e_r * (e_r * (x')') = (e_r * e_r) * (x')' \\ &= e_r * (x')' = (x * x') * (x')' = x * (x' * (x')') = x * e_r = x. \end{aligned}$$

Siis $e_r * x = x * e_r = x$, eli e_r onkin neutraalialkio ja voidaan merkitä $e_r = e$. Tällöin $(G, *, e)$ on monoidi.
Oletusten nojalla kaikille alkioille $x \in G$ on olemassa alkio $x' \in G$, jolla $x * x' = e$. Osoitetaan seuraavaksi, että myös $x' * x = e$ kaikilla $x \in G$. Nyt

$$\begin{aligned} x' * x = (x' * x) * e = (x' * x) * (x' * (x')') = (x' * (x * x')) * (x')' = \\ (x' * e) * (x')' = x' * (x')' = e. \end{aligned}$$

Näin ollen alkio x' on käänteisalkio ja voidaan merkitä $x' = x^{-1}$. Tällöin $(G, *, e)$ on ryhmä $\square$

Lause 2.31. *Olkoon $(G, *)$ puoliryhmä ja oletetaan, että sillä on vasemmanpuolinen neutraalialkio e_l joukossa G. Lisäksi jokaisella joukon G alkiolla on vasemmanpuolinen käänteisalkio. Tällöin $(G, *, e_l)$ on ryhmä.*

Todistus.
Olkoon x' alkion x vasemmanpuolinen käänteisalkio, eli $x' * x = e_l$. Koska $(G, *)$ on puoliryhmä ja $e_l * x = x$ kaikilla $x \in G$, niin

$$x * e_l = e_l * (x * e_l) = (e_l * x) * e_l = (((x')' * x') * x) * e_l$$
$$= ((x')' * (x' * x)) * e_l = ((x')' * e_l) * e_l = (x')' * (e_l * e_l)$$
$$= (x')' * e_l = (x')' * (x' * x) = ((x')' * x') * x = e_l * x = x.$$

Nyt $e_l * x = x * e_l = x$, eli alkio e_l on neutraalialkio ja voidaan merkitä $e_l = e$. Tällöin $(G, *, e)$ on monoidi.
Kaikille alkioille $x \in G$ on olemassa alkio $x' \in G$, jolla $x' * x = e$. Osoitetaan, että myös $x * x' = e$ kaikilla $x \in G$. Nyt

$$x * x' = e * (x * x') = (x')' * x' * (x * x') = (x')' * (x' * x) * x' =$$
$$(x')' * (e * x') = (x')' * x' = e.$$

Siis alkio x' on käänteisalkio ja tätä voidaan merkitä $x' = x^{-1}$. Tällöin $(G, *, e)$ on ryhmä □

Lause 2.32. *Olkoon $(G, *)$ liitännäinen kvasiryhmä. Tällöin on olemassa alkio e, jolle $(G, *, e)$ on ryhmä.*

Todistus.
Muistetaan, että kvasiryhmä on magma, jonka alkioilla $a, b \in G$ on ratkaisut $x, y \in G$ yhtälöille $a * x = b$ ja $y * a = b$. Valitaan alkio a_0 joukosta G. Yhtälölle $a_0 * x = a_0$ on olemassa ratkaisu. Merkitään tätä ratkaisua $x = e$.
1) Koska yhtälöllä $y * a_0 = g$ on ratkaisu joukossa G, niin merkitään tätä ratkaisua $y = h$, eli $h * a_0 = g$, jolloin saadaan $g * e = (h * a_0) * e = h * (a_0 * e) = h * a_0 = g$. Siis jokaiselle alkiolle $g \in G$ pätee $g * e = g$, eli e on oikeanpuolinen neutraalialkio kvasiryhmässä G.
2) Oletuksen nojalla yhtälöllä $g * x = e$ on ratkaisu joukossa G. Tällöin jokaiselle alkiolle $g \in G$ löytyy alkio $g' \in G$, jolle $g * g' = e$. Alkiota g' voidaan siis sanoa oikeanpuoliseksi käänteisalkioksi.
Tällöin kohtien 1) ja 2) sekä lauseen 2.30 nojalla $(G, *, e)$ on ryhmä □

Lause 2.33. *Olkoon $(G, *, e)$ ryhmä. Tällöin sen jokaiselle alkiolle $a, b \in G$ on olemassa ratkaisu yhtälöihin $a * x = b$ ja $y * a = b$. Lisäksi nämä ovat yksikäsitteiset.*

Todistus.
Olkoon $a, b \in G$, tällöin pätee

$$a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b,$$
$$(b * a^{-1}) * a = b * (a^{-1} * a) = b * e = b.$$

Siis $a^{-1} * b$ on ratkaisu yhtälöön $a * x = b$ ja $b * a^{-1}$ on ratkaisu yhtälöön $y * a = b$. Olkoon $c \in G$ sellainen alkio, jolle $a * c = b$. Tällöin $c = e * c = (a^{-1} * a) * c = a^{-1} * (a * c) = a^{-1} * b$. Vastaavasti olkoon $d \in G$, jolle $d * a = b$. Tällöin $d = d * e = d * (a * a^{-1}) = (d * a) * a^{-1} = b * a^{-1}$ □

Huomautus 2.34. Lauseiden 2.30, 2.31, 2.32 ja 2.33 nojalla voidaan antaa ryhmälle muita yhtäpitäviä määritelmiä

- Ryhmä on monoidi, jonka jokaisella alkiolla on kaksipuolinen käänteisalkio.
- Ryhmä on puoliryhmä, jolla on oikeanpuolinen neutraalialkio sekä jokaisella alkiolla on oikeanpuolinen käänteisalkio.
- Ryhmä on puoliryhmä, jolla on vasemmanpuolinen neutraalialkio sekä jokaisella alkiolla on vasemmanpuolinen käänteisalkio.
- Ryhmä on kvasiryhmä, jonka laskutoimitus on liitännäinen.

Aikaisemmin mainittiin monoidin $(M_X, \circ)$ osajoukko M_X^*, jonka jokaisella kuvauksella oli olemassa käänteiskuvaus. Samassa yhteydessä esitettiin väite, että tämä alimonoidi on ryhmä. Tarkastellaan nyt tuota väittämää.

Lause 2.35. *Joukko* $M_X^* = \{\alpha \in M_X \mid \exists\ \alpha^{-1} \in M_X,\ \alpha \circ \alpha^{-1} = \iota = \alpha^{-1} \circ \alpha\}$ *varustettuna kuvausten yhdistämisellä on ryhmä.*

Todistus.
Osoitetaan aluksi, että $(M_X^*, \circ)$ on alimagma. Olkoon $\alpha, \beta \in M_X^*$. Tällöin kuvaukset α ja β ovat bijektioita. Lauseen 1.16 nojalla yhdistetty kuvaus $\alpha \circ \beta$ on bijektiivinen, eli sille on olemassa käänteiskuvaus $(\alpha \circ \beta)^{-1}$. Tällöin

$\alpha \circ \beta \in M_X^*$.
Lauseen 2.10 nojalla kuvausten yhdistäminen on liitännäinen operaatio. Identiteettikuvaus ι toteuttaa neutraalialkion vaatimuksen, sillä $\iota^{-1} = \iota$ ja $\iota \circ \alpha = \alpha \circ \iota = \alpha$ kaikilla $\alpha \in M_X^*$. Jos $\alpha \in M_X^*$, niin joukon M_X^* määrittelyn nojalla myös $\alpha^{-1} \in M_X^*$ ja $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = \iota$.
Tällöin $(M_X^*, \circ, \iota)$ on ryhmä $\square$

Määritelmä 2.36. Olkoon G ja H ryhmiä ja $G \neq \emptyset$ ja $H \neq \emptyset$. Jos $H \subseteq G$ ja sen laskutoimitus on sama kuin ryhmässä G, niin sanotaan, että H on ryhmän G *aliryhmä* ja merkitään $H \leq G$.

Lause 2.37. *(Aliryhmäkriteeri)*
Olkoon G ryhmä. Joukko $H \subseteq G$ on ryhmän G aliryhmä, mikäli seuraavat ehdot ovat voimassa:

1. *ryhmän G neutraalialkio kuuluu joukkoon H,*
2. *joukon H alkioille h ja k pätee $hk \in H$,*
3. *jokaisella $h \in H$ on olemassa $h^{-1} \in H$.*

Todistus.
Olkoon G ryhmä ja $\emptyset \neq H \subseteq G$ sekä ehdot 1, 2 ja 3 voimassa. Kohdan 2 nojalla joukon H sisäinen laskutoimitus on suljettu. Olkoon alkiot $a, b, c \in H$. Koska $H \subseteq G$, niin $a, b, c \in G$. Koska G on ryhmä, niin sen laskutoimitus on liitännäinen ja $(ab)c = a(bc)$. Lisäksi $(ab)c \in H$ ja $a(bc) \in H$, joten laskutoimitus joukon H sisällä on liitännäinen. Kohdista 1 ja 3 saadaan puuttuvat ehdot. Siis H on ryhmä ja $H \subseteq G$, eli $H \leq G$.
Jos $H \leq G$, niin se on myös ryhmä. Tällöin ehdot 1, 2 ja 3 toteutuvat $\square$

Huomautus 2.38. Olkoon G ryhmä. Tällöin sillä on aliryhmät $\{e\}$ ja G, joita kutsutaan ryhmän G *triviaaleiksi aliryhmiksi*. Aliryhmää H sanotaan *aidoksi aliryhmäksi*, mikäli $H \neq G$, ja sitä merkitään $H < G$. Jos $G \neq \{e\}$, niin aliryhmä $\{e\}$ on myös aito aliryhmä.

Seuraava lause helpottaa aliryhmyyden tarkistamista, sillä riittää osoittaa, että joukko H ei ole tyhjä ja hk^{-1} on joukon H alkio kaikilla alkioilla $h, k \in H$.

Lause 2.39. *Olkoon G ryhmä ja joukko $H \subseteq G$. Tällöin H on ryhmän G aliryhmä, jos ja vain jos $H \neq \emptyset$ ja $hk^{-1} \in H$ kaikilla $h, k \in H$.*

Todistus.
Oletetaan, että H on aliryhmä. Tällöin siihen kuuluu ainakin ryhmän G neutraalialkio, eli $H \neq \emptyset$. Jos alkiot $h, k \in H$, niin käänteisalkio $k^{-1} \in H$, jolloin $h(k^{-1}) \in H$ kaikilla $h, k \in H$.
Oletetaan, että H on joukon G osajoukko, $H \neq \emptyset$ ja jokaisella alkiolla $h, k \in H$ pätee $hk^{-1} \in H$. Koska H ei ole tyhjä, voidaan valita alkio $h_0 \in H$, jolloin $h_0 h_0^{-1} \in H$. Koska $H \subseteq G$, niin $h_0 h_0^{-1} = e \in G$. Siis $e \in H$. Olkoon $h \in H$, tällöin $h^{-1} = e \cdot h^{-1} \in H$. Jos $k \in H$, niin $hk = h(k^{-1})^{-1} \in H$ ja lauseen 2.37 ehdot täyttyvät $\square$

3 Morfismeista

Tässä luvussa kuvauksella yhdistetään algebrallisia rakenteita toisiinsa ja osoitetaan, että mille tahansa monoidille A on olemassa isomorfinen kopio joukossa M_X.

Määritelmä 3.1. Olkoon $(A, *)$ ja $(B, \bullet)$ magmoja.
Tällöin kuvaus $f : A \to B$ on *homomorfismi*, mikäli kaikilla $x, y \in A$ toimii $f(x * y) = f(x) \bullet f(y)$.

Esimerkki 3.2. Olkoon $A = \{[0], [1], [2]\}$ jäännösluokkien joukko modulo 3, $B = \{[0], [3], [6]\}$ jäännösluokkien joukko modulo 9 ja varustetaan nämä joukot yhteenlaskulla sekä kuvaus $f : A \to B$, $f(x) = 3x$. Tällöin
$f([1] + [2]) = f([3]) = [9] = [3] + [6] = f([1]) + f([2])$,
$f([1] + [1]) = f([2]) = [6] = [3] + [3] = f([1]) + f([1])$,
$f([2] + [2]) = f([4]) = [12] = [6] + [6] = f([2]) + f([2])$,
$f([0]_A + [2]) = f([2]) = [6] = [0]_B + [6] = f([0]_A) + f([2])$,
$f([1] + [0]_A) = f([1]) = [3] = [3] + [0]_B = f([1]) + f([0]_A)$ ja
$f([0]_A + [0]_A) = f([0]_A) = [0]_B = [0]_B + [0]_B = f([0]_A) + f([0]_A)$.
Jäännösluokkien yhteenlasku on vaihdannainen, joten tämä riittää. Siis kuvaus f on homomorfismi.

Koska homomorfismi on kuvaus, niin luonnollisesti kuvauksen ominaisuudet antavat sille lisäominaisuuksia. Oletetaan seuraavaan kolmeen määritelmään, että kuvaus f on homomorfismi magmalta A magmalle B.

Määritelmä 3.3. Jos kuvaus f on surjektio, niin kuvausta f sanotaan *epimorfismiksi* tai *epimorfiseksi kuvaukseksi.*

Määritelmä 3.4. Jos kuvaus f on injektio, niin kuvausta f sanotaan *monomorfismiksi* tai *monomorfiseksi kuvaukseksi.*

Määritelmä 3.5. Jos kuvaus f on sekä injektio että surjektio, eli bijektio, niin kuvausta f sanotaan *isomorfismiksi* tai *isomorfiseksi kuvaukseksi.* Jos on olemassa isomorfismi magmalta A magmalle B, niin sanotaan, että A ja B

ovat *isomorfisia keskenään* tai magma A on *isomorfinen* magman B kanssa. Tällöin merkitään $A \cong B$. Isomorfista kuvausta joukolta itselleen sanotaan *automorfismiksi*.

Seuraavaksi osoitetaan epimorfismin säilyttävän joitakin ominaisuuksia siirryttäessä magmasta toiseen. Seuraavan neljän lauseen kohdalla oletetaan, että $(A, *)$ ja $(B, \bullet)$ ovat magmoja sekä kuvaus $f : A \to B$ on epimorfismi.

Lause 3.6. *Jos magmalla A on neutraalialkio u, niin myös magmalla B on neutraalialkio $f(u)$. Jos alkio $y \in A$ on alkion $x \in A$ käänteisalkio, niin alkio $f(y) \in B$ on alkion $f(x) \in B$ käänteisalkio.*

Todistus.
Olkoon $z \in B$. Osoitetaan, että alkio $f(u)$ on magman B neutraalialkio, eli $f(u) \bullet z = z = z \bullet f(u)$. Koska kuvaus f on epimorfismi, niin se on surjektio jolloin on olemassa alkio $x \in A$, jolle $f(x) = z$. Tällöin

$$f(u) \bullet z = f(u) \bullet f(x) = f(u * x) = f(x) = z,$$
$$z \bullet f(u) = f(x) \bullet f(u) = f(x * u) = f(x) = z.$$

Siis $f(u)$ on magman B neutraalialkio.
Osoitetaan seuraavaksi säilyvyys käänteisalkioille.
Olkoon alkiolla $x \in A$ käänteisalkio y, siis $x * y = u = y * x$. Tällöin

$$f(x) \bullet f(y) = f(x * y) = f(u) = f(y * x) = f(y) \bullet f(x).$$

Siis alkiolla $f(x) \in B$ on käänteisalkio $f(y)$ □

Lause 3.7. *Jos A on puoliryhmä, niin myös B on puoliryhmä.*

Todistus.
Osoitetaan, että magman B laskutoimitus on liitännäinen. Olkoon alkiot $z, y, z \in B$. Koska f on epimorfismi, niin se on surjektio jolloin on olemassa alkiot $a, b, c \in A$, joille $f(a) = x$, $f(b) = y$ ja $f(c) = z$. Tällöin

$$x \bullet (y \bullet z) = f(a) \bullet (f(b) \bullet f(c)) = f(a) \bullet (f(b * c)) = f(a * (b * c)) =$$
$$f((a * b) * c) = f(a * b) \bullet f(c) = (f(a) \bullet f(b)) \bullet f(c) = (x \bullet y) \bullet z.$$

Siis B on puoliryhmä $\square$

Lause 3.8. *Jos A on vaihdannainen magma, niin B on vaihdannainen magma.*

Todistus.
Olkoon $x, y \in B$. Koska f on epimorfismi, niin on olemassa alkiot $a, b \in A$, joille $f(a) = x$ ja $f(b) = y$. Tällöin

$$x \bullet y = f(a) \bullet f(b) = f(a * b) = f(b * a) = f(b) \bullet f(a) = y \bullet x.$$

Siis B on vaihdannainen magma $\square$

Lause 3.9. *Jos A on silmukka, niin myös B on silmukka.*

Todistus.
Osoitetaan ensiksi, että kvasiryhmästä seuraa kvasiryhmä. Olkoon alkio $b \in B$. Koska f on epimorfismi, niin on olemassa ainakin yksi alkio $a \in A$, että $f(a) = b$. Koska A on kvasiryhmä, niin voidaan valita alkio $c \in A$, jolloin on olemassa yksikäsitteiset ratkaisut $x, y \in A$, että $c * x = a$ ja $y * c = a$.
Koska f on homomorfismi, niin $b = f(a) = f(c * x) = f(c) \bullet f(x)$ ja $b = f(a) = f(y * c) = f(y) \bullet f(c)$. Siis B on kvasiryhmä.
Jos A on silmukka eli kvasiryhmällä A on neutraalialkio, niin lauseen 3.6 nojalla myös kvasiryhmällä B on neutraalialkio. $\square$

Toisessa luvussa esitetyn joukon M_X tärkeys käy ilmi seuraavasta lauseesta, joka osoittaa, että millä tahansa puoliryhmällä S on olemassa isomorfinen kopio jossakin joukossa M_X, joka koostuu kaikista epätyhjän joukon X kuvauksista itselleen, eli $M_X = \{\lambda \mid \lambda : X \to X\}$.

Lause 3.10. *(Cayleyn lause)*
Olkoon $(S, *)$ monoidi. Tällöin on olemassa monomorfismi joukolta S joukolle M_S.

Todistus.
Olkoon $s \in S$ ja kuvaus $f_s : S \to S$ määritelty niin, että $f_s(x) = s * x$ kaikilla $x \in S$. Olkoon kuvaus $h : S \to M_S$ määritelty niin, että $h(s) = f_s$. Osoitetaan, että kuvaus h on monomorfismi. Olkoon $s, s' \in S$. Nyt

$$h(s * s') = f_{ss'} \text{ ja } h(s) \circ h(s') = f_s \circ f_{s'}.$$

Jos $x \in S$, niin $(f_s \circ f_{s'})(x) = f_s(f_{s'}(x)) = f_s(s' * x) = s * (s' * x) = (s * s') * x = f_{ss'}(x)$. Siis $f_{ss'}(x) = (f_s \circ f_{s'})(x)$ kaikilla $x \in S$, eli $h(s * s') = h(s) \circ h(s')$, joten kuvaus h on homomorfismi.
Vielä pitää osoittaa, että kuvaus h on injektiivinen. Olkoon $h(s) = h(s')$. Tällöin $f_s(x) = f_{s'}(x)$, kaikilla $x \in S$. Tämä toimii etenkin neutraalialkiolla $e \in S$, jolloin $f_s(e) = s * e = s = f_{s'}(e) = s' * e = s'$. Siis $s = s'$ ja kuvaus h on monomorfismi $\square$

Vaikka tämä lause ei sisälläkkään suoraan isomorfiaa, niin se seuraa kuvauksen määritelmästä, kuten seuraavasta käy ilmi.

Lause 3.11. *Monoidilla S on olemassa isomorfinen kopio joukossa M_S.*

Todistus.
Edellisen lauseen nojalla on olemassa monomorfinen kuvaus $h : S \to M_S$. Koska monomorfismi h on kuvaus, niin sen joukosta S muodostama kuvajoukko $h(S)$ on joukon M_S osajoukko. Selvästi $h : S \to h(S)$ on surjektio ja tällöin joukot S ja $h(S)$ ovat isomorfisia, eli $S \cong h(S) \subseteq M_S$ $\square$

Lähdeluettelo

[1] Baumslag B., Chandler B.: *Shaum's outline of theory and problems of group theory*, McGraw-Hill 1968.

[2] Hungerford T. W.: *Algebra. Graduate Texts in Mathematics 73*, Springer-Verlag 1974.

[3] Lang S.: *Algebra. Revised Third Edition, Graduate Texts in Mathematics 211*, Springer-Verlag 2002.

[4] Menini C., van Oystaeyen F.: *Abstract algebra, a comprehensive treatment*, Marcel Dekker 2004.

[5] Myrberg L.: *Algebra, korkeakouluja varten*, Vaasa Oy 1978.

[6] Rotman J.J.: *Advanced Modern Algebra.* Prentice Hall 2002.