Luupit

Pro gradu
Anni Keränen
Matemaattisten tieteiden laitos
Oulun yliopisto
2014

Sisältö

Johdanto

Tutkielmassa tutustutaan luuppeihin, niiden ominaisuuksiin sekä siihen, miten ne voidaan linkittää ryhmiin. Ensimmäisen luvun lähteenä on käytetty pääasiassa kurssin Algebra I luentomonistetta sekä luentomuistiinpanoja. Lukujen 2, 3, 4, 5 ja 8 lähde on Hala O. Pflugfelderin teos Quasigroups and loops introduction. Luvuissa 6 ja 7 lähteinä on käytetty R.H. Bruckin teosta Contributions to the theory of loops ja Kari Myllylän väitöskirjaa On the solvability of groups and loops.

Ensimmäisessä luvussa esitellään määritelmiä ja tuloksia kuvauksista, relaatioista, grupoidista ja osituksesta sekä hieman ryhmäteoriaa. Näitä perusmääritelmiä ja -tuloksia tarvitaan myöhemmin tutkielmassa. Yksi luvun tärkeimpiä määritelmiä on siirtokuvausten L_a ja R_a määrittely, sillä näiden avulla määritellään myöhemmin luupit.

Toisessa luvussa määritellään luupit kolmella eri tavalla. Lisäksi määritellään siirtokuvausten L_a ja R_a käänteiskuvaukset L_a^{-1} ja R_a^{-1}. Luvussa osoitetaan luupeille monia hyödyllisiä tuloksia, joita käytetään myöhemmin tutkielmassa.

Luvussa kolme tutustutaan aliluuppeihin. Heti luvun alussa todistetaan lause, joka kertoo ne kriteerit, joiden täytyy toteutua, jotta joukko olisi jonkin luupin aliluuppi. Tätä lausetta käytetään tutkielmassa useamman kerran. Lisäksi luvussa esitellään useita aliluuppeihin liittyviä määritelmiä sekä tuloksia.

Neljännessä luvussa esitellään luupin ydin ja keskus sekä niihin liittyviä lauseita.

Luvussa viisi esitellään luupin oikea ja vasen käänteisalkio. Luupin alkioiden ja käänteisalkioiden avulla määritellään esimerkiksi luupin käänteisominaisuus. Luvussa tutustutaan useisiin erikoistapauksiin luupeista, esimerkiksi käänteisominaisuuden toteuttavaan I.P. -luuppiin.

Kuudennessa luvussa määritellään kuvauksen homomorfisuus, isomorfisuus sekä automorfisuus. Lisäksi esitellään homomorfismin ydin ja kuva sekä osoitetaan, että ne ovat luuppeja.

Luvussa seitsemän tutustutaan luupin kertolaskuryhmään, joka määritellään ensimmäisessä luvussa määriteltyjen siirtokuvausten avulla. Luvussa esitellään myös sisäinen kertolaskuryhmä sekä monia näihin ryhmiin liittyviä määritelmiä ja tuloksia. Kertolaskuryhmät ja sisäiset kertolaskuryhmät ovat tärkeitä luuppien tutkimisessa, sillä ne yhdistävät luupit ryhmiin.

Viimeisessä luvussa esitetään muutama esimerkki luupeista niiden havainnollistamiseksi. Esimerkit liittyvät pääasiassa lukuihin 2 ja 5.

1 Perusteita

Tässä luvussa esitellään määritelmiä ja tuloksia kuvauksista, relaatioista, grupoidista sekä osituksesta. Luvun lopussa on myös hieman ryhmäteoriaa. Lukuun on kerätty vain sellaisia määritelmiä ja lauseita, joita tarvitaan myöhemmin tutkielmassa.

1.1 Kuvauksista

Määritelmä 1.1. Olkoot A ja B joukkoja. *Kuvaus* $f : A \to B$ kuvaa jokaisen joukon A alkion täsmälleen yhdeksi joukon B alkioksi.

Määritelmä 1.2. Olkoot A ja B joukkoja. Kuvaus $f : A \to B$ on

1. *surjektio*, jos sen arvojoukko on koko joukko B,
2. *injektio*, jos joukon A eri alkioilla on aina eri kuvapisteet eli toisin sanoen jos $x_1 \neq x_2$, niin $f(x_1) \neq f(x_2)$,
3. *bijektio*, jos se on surjektio ja injektio.

Määritelmä 1.3. Olkoon kuvaus $f : A \to B$ bijektio. Tällöin voidaan määritellä kuvauksen f *käänteiskuvaus* $f^{-1} : B \to A$ siten, että

$$x = f^{-1}(y) \Leftrightarrow y = f(x).$$

Lause 1.4. *Käänteiskuvaus f^{-1} on bijektio.*

Todistus. Olkoon $x \in A$ mielivaltainen. Tällöin $f(x) = y \in B$ ja siten $x = f^{-1}(y)$. Näin ollen käänteisfunktion arvojoukko on A eli f^{-1} on surjektio.

Olkoon $f^{-1}(y_1) = f^{-1}(y_2)$, missä $y_1, y_2 \in B$. Koska $f : A \to B$ on surjektio, niin on olemassa sellaiset $x_1, x_2 \in A$, että $f(x_1) = y_1$ ja $f(x_2) = y_2$. Koska f on injektio, saadaan

$$\begin{aligned} & f^{-1}(y_1) = f^{-1}(y_2) \\ \Leftrightarrow \quad & f^{-1}(f(x_1)) = f^{-1}(f(x_2)) \\ \Leftrightarrow \quad & x_1 = x_2 \\ \Leftrightarrow \quad & f(x_1) = f(x_2) \\ \Leftrightarrow \quad & y_1 = y_2. \end{aligned}$$

Eli f^{-1} on injektio.
Koska f^{-1} on sekä injektio että surjektio, se on myös bijektio. □

Lause 1.5. *Olkoon kuvaus $f : A \to B$ bijektio ja $f^{-1} : B \to A$ sen käänteiskuvaus. Tällöin*

$$f^{-1}(f(x)) = x \text{ aina, kun } x \in A$$

ja

$$f(f^{-1}(y)) = y \text{ aina, kun } y \in B.$$

Todistus. Osoitetaan ensin, että $f^{-1}(f(x)) = x$ aina, kun $x \in A$. Nyt $f(x) = y \Leftrightarrow f^{-1}(y) = x$. Eli $f^{-1}(f(x)) = f^{-1}(y) = x$ aina, kun $x \in A$.

Osoitetaan seuraavaksi, että $f(f^{-1}(y)) = y$ aina, kun $y \in B$. Nyt $f(f^{-1}(y)) = f(x) = y$ aina, kun $y \in B$. □

Määritelmä 1.6. Kuvausten $f : A \to B$ ja $g : C \to A$ *yhdistetty kuvaus* on $f \circ g : C \to B$. Yhdistetylle kuvaukselle on voimassa

$$(f \circ g)(x) = f(g(x))$$

aina, kun $x \in C$.

Määritelmä 1.7. Sellaista kuvausta $I_A : A \to A$, joka kuvaa jokaisen alkion itselleen, kutsutaan *identiteettikuvaukseksi*. Siis $I_A(x) = x$ aina, kun $x \in A$. Joukon B identiteettikuvaus I_B määritellään vastaavasti eli $I_B(y) = y$ aina, kun $y \in B$.

Lause 1.8. *Olkoon $f : A \to B$. Tällöin $f^{-1} \circ f = I_A$ ja $f \circ f^{-1} = I_B$.*

Todistus. Olkoon $x \in A$. Nyt $(f^{-1} \circ f)(x) = f^{-1}(f(x))$. Lauseen 1.5 nojalla $f^{-1}(f(x)) = x$ eli $f^{-1} \circ f = I_A$.

Olkoon sitten $y \in B$. Tällöin $(f \circ f^{-1})(y) = f(f^{-1}(y))$. Lauseen 1.5 perusteella $f(f^{-1}(y)) = y$ eli $f \circ f^{-1} = I_B$. □

Lause 1.9. *Olkoot kuvaukset $f : A \to B$ ja $g : C \to A$ bijektioita. Tällöin yhdistetty kuvaus $f \circ g : C \to B$ on bijektio ja $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.*

Todistus. Todistetaan ensin, että yhdistetty kuvaus $f \circ g$ on bijektio osoittamalla, että se on sekä surjektio että injektio.

Osoitetaan aluksi yhdistetyn kuvauksen $f \circ g$ surjektiivisyys. Olkoon $z \in B$ mielivaltainen. Koska f on surjektio, niin on olemassa sellainen $y \in A$, että $z = f(y)$. Koska myös g on surjektio, niin on olemassa sellainen alkio $x \in C$, että $y = g(x)$. Tällöin $(f \circ g)(x) = f(g(x)) = f(y) = z$. Näin ollen yhdistetty kuvaus $f \circ g$ on surjektio.

Osoitetaan seuraavaksi, että yhdistetty kuvaus on injektio. Oletetaan, että $(f \circ g)(x) = (f \circ g)(y)$ joillakin $x, y \in C$. Tällöin $f(g(x)) = f(g(y))$.

Koska kuvaus f on injektio, niin $g(x) = g(y)$. Toisaalta myös kuvaus g on injektio, joten $x = y$. Näin ollen yhdistetty kuvaus $f \circ g$ on injektio.

Koska yhdistetty kuvaus $f \circ g$ on sekä surjektio että injektio, niin se on myös bijektio.

Osoitetaan vielä, että $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$. Olkoon $z = (f \circ g)(x) = f(g(x))$ ja merkitään $y = g(x)$. Tällöin siis $z = f(y)$, josta määritelmän 1.3 nojalla saadaan $y = f^{-1}(z)$. Lisäksi yhtälöstä $y = g(x)$ seuraa, että $x = g^{-1}(y)$. Tällöin $x = g^{-1}(y) = g^{-1}(f^{-1}(z)) = (g^{-1} \circ f^{-1})(z)$. Toisaalta $z = (f \circ g)(x)$, josta määritelmän 1.3 nojalla saadaan $x = (f \circ g)^{-1}(z)$. Näin ollen $(f \circ g)^{-1}(z) = (g^{-1} \circ f^{-1})(z)$ aina, kun $z \in B$. Siis väite on todistettu. □

Lause 1.10. *Olkoot $g : A \to B$, $f : B \to C$ ja $h : C \to D$. Tällöin pätee*

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

Todistus. Määritelmän 1.6 nojalla $(h \circ (f \circ g))(x) = h((f \circ g)(x)) = h(f(g(x)))$.
Toisaalta $((h \circ f) \circ g)(x) = (h \circ f)(g(x)) = h(f(g(x)))$.
Näin ollen $(h \circ (f \circ g))(x) = ((h \circ f) \circ g)(x)$.
□

Voidaan siis merkitä $h \circ (f \circ g) = (h \circ f) \circ g = h \circ f \circ g$.

1.2 Relaatioista

Määritelmä 1.11. Olkoon A ei-tyhjä joukko. Tällöin joukkoa

$$A \times A = \{(a_1, a_2) \mid a_1, a_2 \in A\}$$

kutsutaan *joukon A karteesiseksi tuloksi itsensä kanssa.*

Määritelmä 1.12. Joukon $A \times A$ osajoukkoa R sanotaan *binääriseksi relaatioksi* joukossa A. Jos pari $(x, y) \in R$, niin sanotaan, että alkio x on relaatiossa R alkion y kanssa. Merkitään xRy.

Määritelmä 1.13. Binäärinen relaatio R on *ekvivalenssirelaatio* joukossa A, mikäli seuraavat ehdot toteutuvat.

- xRx aina, kun $x \in A$,
- jos xRy, niin yRx aina, kun $x, y \in A$,
- jos xRy ja yRz, niin xRz aina, kun $x, y, z \in A$.

Jos R on ekvivalenssirelaatio ja $a \in A$, niin joukko

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

on *alkion a määräämä ekvivalenssiluokka.*

Lause 1.14. *Olkoot R ekvivalenssirelaatio ja aRb. Tällöin $[a] = [b]$.*

Todistus. Olkoon $x \in [a]$, jolloin xRa. Koska aRb, niin määritelmän 1.13 nojalla myös xRb. Näin ollen $x \in [b]$ eli $[a] \subseteq [b]$.

Oletetaan seuraavaksi, että $y \in [b]$ eli yRb. Nyt aRb eli bRa, jolloin yRa eli $y \in [a]$. Siis $[b] \subseteq [a]$.

Nyt $[a] \subseteq [b]$ ja $[b] \subseteq [a]$ eli $[a] = [b]$. □

1.3 Grupoidi ja ositus

Määritelmä 1.15. Olkoon A ei-tyhjä joukko. Kuvaus $* : A \times A \to A$, $(a, b) \mapsto a * b$, on joukon A *binäärinen operaatio*, eli $(a * b) \in A$ aina, kun $a, b \in A$ ja $a * b$ on joukon A yksikäsitteinen alkio.

Määritelmä 1.16. *Grupoidi* on ei-tyhjä joukko G varustettuna binäärisellä operaatiolla $(*)$. Tällöin käytetään merkintää $(G, *)$.

Määritelmä 1.17. Olkoon G grupoidi ja H joukon G ei-tyhjä osajoukko. Jos H on grupoidi, niin silloin sanotaan, että H on grupoidin G *aligrupoidi.*

Määritelmä 1.18. Olkoot $(G, *)$ grupoidi ja a joukon G alkio. Tällöin voidaan määritellä seuraavat *siirtokuvaukset* (translation maps):

- $L_a(x) = a * x$ ja
- $R_a(x) = x * a$

kaikilla $x \in G$.
Tästä seuraa, että $L_a : G \to G$ ja $R_a : G \to G$ kaikilla $a \in G$.

Määritelmä 1.19. Olkoon G ei-tyhjä joukko. P on joukon G *ositus*, jos

- $X \neq \emptyset$ aina kun $X \in P$,
- $G = \bigcup_{X \in P} X$,
- $X = Y$ aina, kun $X \in P$, $Y \in P$ ja $X \cap Y \neq \emptyset$.

Lause 1.20. *Olkoon R joukon A ekvivalenssirelaatio ja $a \in A$. Tällöin ekvivalenssirelaation R ekvivalenssiluokat $[a]$ ovat joukon A ositus.*

Todistus. Osoitetaan ensin, että $[a] \neq \emptyset$. Nyt aRa kaikilla $a \in A$. Tällöin $a \in [a]$, joten $[a] \neq \emptyset$.

Osoitetaan seuraavaksi, että $A = \bigcup_{a \in A}[a]$. Olkoon $a \in A$, jolloin aRa eli $a \in [a]$. Siten $A = \bigcup_{a \in A}[a]$.

Osoitetaan vielä, että jos $[a] \cap [b] \neq \emptyset$ joillakin $a, b \in A$, niin $[a] = [b]$. Oletetaan, että $[a] \cap [b] \neq \emptyset$, jolloin $x \in [a] \cap [b]$. Tällöin xRa ja xRb, josta seuraa, että aRx ja siten aRb. Lauseen 1.14 nojalla $[a] = [b]$. Eli kun $[a] \cap [b] \neq \emptyset$, niin $[a] = [b]$.

Näin ollen ekvivalenssirelaation R ekvivalenssiluokat $[a]$ ovat joukon A ositus. □

1.4 Ryhmistä

Määritelmä 1.21. Olkoot $G \neq \emptyset$ ja $(*)$ binäärinen operaatio joukossa G. Pari $(G, *)$ on ryhmä, jos seuraavat ehdot toteutuvat:

1. $(*)$ on *assosiatiivinen* eli

$$(a * b) * c = a * (b * c)$$

aina, kun $a, b, c \in G$.

2. Joukossa G on olemassa *neutraalialkio* e, jolle pätee

$$a * e = e * a = a$$

aina, kun $a \in G$.

3. Aina, kun $a \in G$, on olemassa sellainen alkio $a^{-1} \in G$, että

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

Alkiota a^{-1} kutsutaan *alkion a käänteisalkioksi.*

Määritelmä 1.22. *Alkioiden a ja b muodostama ryhmä* $< a, b >$ on pienin sellainen ryhmä, johon alkiot a ja b kuuluvat. Tällöin ryhmän määritelmän nojalla ryhmään $< a, b >$ kuuluu alkioiden a ja b lisäksi näiden käänteisalkiot a^{-1} ja b^{-1} sekä kaikki alkioiden a, b, a^{-1} ja b^{-1} väliset operaatiot.

Määritelmä 1.23. Olkoot $(G, *)$ ryhmä, $H \subseteq G$ ja $H \neq \emptyset$. Jos $(H, *)$ on ryhmä, niin sitä kutsutaan ryhmän $(G, *)$ *aliryhmäksi.* Merkitään $(H*) \leq (G, *)$.

Lause 1.24. *Olkoot G ryhmä, $H \subseteq G$ ja $H \neq \emptyset$. Tällöin H on ryhmän G aliryhmä, jos ja vain jos seuraavat ehdot toteutuvat:*

1. *Kun $a, b \in H$, niin $ab \in H$.*
2. *Kun $a \in H$, niin $a^{-1} \in H$.*

Todistus. Oletetaan, että H on ryhmän G aliryhmä. Tällöin ehdot toteutuvat, koska aliryhmänä H on myös ryhmä.

Oletetaan nyt, että ehdot totetuvat. Täytyy siis osoittaa, että tällöin H on ryhmän G aliryhmä. Todistetaan se osoittamalla, että H on ryhmä näyttämällä, että määritelmän 1.21 ehdot toteutuvat.

Nyt kyseessä on binäärinen operaatio, koska ehdon 1 mukaan $ab \in H$, kun $a, b \in H$.

Operaatio on assosiatiivinen joukossa H, koska se on assosiatiivinen ryhmässä G ja $H \subseteq G$.

Olkoon nyt $a \in H$. Ehdon 2 nojalla $a^{-1} \in H$. Nyt ehdon 1 nojalla $aa^{-1} = e \in H$.

Siis joukko H on ryhmä, jolloin se on myös ryhmän G aliryhmä.

□

1.5 Permutaatioryhmistä

Määritelmä 1.25. Olkoon $X \neq \emptyset$. Bijektiota $f : X \to X$ sanotaan joukon X *permutaatioksi*.

Lause 1.26. *Olkoon S_X joukon X kaikkien permutaatioiden joukko. Pari $(S_X, \circ)$, missä $(\circ)$ on kuvausten yhdistämisoperaatio, on ryhmä.*

Todistus. Osoitetaan, että $(S_X, \circ)$ on ryhmä näyttämällä, että kaikki määritelmän 1.21 kohdat toteutuvat.

Osoitetaan ensin, että $(\circ)$ on binäärinen operaatio joukossa S_X. Olkoon $\alpha, \beta \in S_X$. Tällöin kuvaukset $\alpha : X \to X$ ja $\beta : X \to X$ ovat bijektioita. Lauseen 1.9 nojalla yhdistetty kuvaus $\alpha \circ \beta : X \to X$ on myös bijektio eli $\alpha \circ \beta \in S_X$. Siis $(\circ)$ on joukon S_X binäärinen operaatio.

Osoitetaan seuraavaksi, että binäärinen operaatio $(\circ)$ on assosiatiivinen. Olkoon $\alpha, \beta, \gamma \in S_X$. Tällöin $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$ eli $(\circ)$ on assosiatiivinen.

Osoitetaan, että joukossa S_X on olemassa neutraalialkio. Nyt identiteettikuvaus $I : X \to X$ on bijektio eli $I \in S_X$. Lisäksi $I \circ \alpha = \alpha$ ja $\alpha \circ I = \alpha$ kaikilla $\alpha \in S_X$, joten I on joukon S_X neutraalialkio.

Osoitetaan vielä, että kun $\alpha \in S_X$, niin myös käänteisalkio $\alpha^{-1} \in S_X$. Olkoon $\alpha \in S_X$ eli $\alpha : X \to X$ on bijektio. Tällöin on olemassa käänteiskuvaus α^{-1} ja $\alpha^{-1} : X \to X$ on bijektio. Eli $\alpha^{-1} \in S_X$. Lisäksi $\alpha \circ \alpha^{-1} = I$ ja $\alpha^{-1} \circ \alpha = I$. Näin ollen α^{-1} on alkion $\alpha \in S_X$ käänteisalkio.

On siis osoitettu, että määritelmän 1.21 kaikki ehdot toteutuvat, joten $(S_X, \circ)$ on ryhmä. □

Määritelmä 1.27. Olkoon joukon X *kertaluku* eli joukon X alkioiden lukumäärä n. Tällöin merkitään $S_X = S_n$. Ryhmää S_n sanotaan *astetta n olevaksi symmetriseksi ryhmäksi.*

Symmetrisen ryhmän S_n aliryhmiä kutsutaan *permutaatioryhmiksi.*

2 Luupit

Tässä luvussa määritellään luupit kolmella eri tavalla sekä esitellään luuppeihin liittyviä määritelmiä ja tuloksia.

Määritelmä 2.1. Olkoon G ei-tyhjä joukko. Pari $(G, *)$ on *luuppi*, jos $(*)$ on binäärinen operaatio joukossa G ja kuvaukset $L_a : G \to G$ ja $R_a : G \to G$ ovat bijektioita kaikilla $a \in G$. Lisäksi joukossa G täytyy olla neutraalialkio e, jolle pätee $e * x = x * e = x$ kaikilla $x \in G$.

Luupit voidaan määritellä myös ilman siirtokuvauksia:

Määritelmä 2.2. Olkoot G ei-tyhjä joukko ja $(*)$ binäärinen operaatio joukossa G. Pari $(G, *)$ on luuppi, mikäli seuraavat ehdot toteutuvat.

1. Jos yhtälössä $x * y = z$ mitkä tahansa kaksi muuttujaa ovat joukon G alkioita, niin silloin myös kolmas muuttuja on joukon G yksikäsitteinen alkio.

2. Joukossa G on olemassa neutraalialkio e, jolle pätee $e * x = x * e = x$ kaikilla $x \in G$.

Jatkossa luuppiin $(G, *)$ viitataan vain joukolla G ja binäärinen operaatio $(*)$ jätetään merkitsemättä luupin laskutoimituksissa.

Lause 2.3. *Määritelmät 2.1 ja 2.2 ovat yhtäpitäviä.*

Todistus. Oletetaan ensin, että määritelmä 2.1 on voimassa eli $(*)$ on binäärinen operaatio joukossa G, joukossa G on olemassa neutraalialkio e ja siirtokuvaukset L_a ja R_a ovat bijektioita. Huomataan, että ainoaksi todistettavaksi kohdaksi jää määritelmän 2.2 ehto 1.

Tarkastellaan nyt yhtälöä $xy = z$.

Oletetaan, että $x, y \in G$. Nyt $L_x(y) \in G$ ja $L_x(y) = xy = z$, joten myös $z \in G$ ja on yksikäsitteinen.

Oletetaan seuraavaksi, että $y, z \in G$. Koska oletuksen perusteella R_y on bijektio eli myös surjektio, niin on olemassa sellainen alkio $x \in G$, että $R_y(x) = z$ eli $xy = z$. Koska kuvaus R_y on bijektiona myös injektio, niin x on joukon G yksikäsitteinen alkio.

Oletetaan sitten, että $x, z \in G$. Oletusten nojalla L_x on bijektio eli myös surjektio. Täten on olemassa sellainen alkio $y \in G$, että $L_x(y) = z$ eli $xy = z$. Koska kuvaus L_x on bijektiona myös injektio, niin y on joukon G yksikäsitteinen alkio.

Näin määritelmän 2.2 ehto 1 on todistettu.

Oletetaan seuraavaksi, että määritelmä 2.2 on voimassa eli kun yhtälössä $xy = z$ kaksi muuttujaa kuuluu joukkoon G, niin myös kolmas alkio on joukon G yksikäsitteinen alkio. Tavoitteena on osoittaa, että tällöin siirtokuvaukset L_a ja R_a ovat bijektioita.

Olkoon a joukon G kiinnitetty alkio. Nyt jokaiselle $y \in G$ on oletuksen mukaan olemassa sellainen $x \in G$, että $y = ax$ tai $y = xa$ eli $y = L_a(x)$ tai $y = R_a(x)$. Näin ollen kuvaukset L_a ja R_a ovat surjektioita.

Oletetaan, että $x, y \in G$ ja $L_a(x) = L_a(y)$ eli $ax = ay$. Tällöin on olemassa $z \in G$ siten, että $ax = z$ ja $ay = z$. Oletuksen nojalla näillä yhtälöillä on yksikäsitteiset ratkaisut joukossa G eli $x = y$. Näin ollen kuvaus L_a on injektio.

Oletetaan sitten, että $x, y \in G$ ja $R_a(x) = R_a(y)$ eli $xa = ya$. Tällöin joukossa G on olemassa alkio w siten, että $xa = w$ ka $ya = w$. Oletusten perusteella yhtälöillä on yksikäsitteiset ratkaisut joukossa G eli $x = y$. Täten myös kuvaus R_a on injektio.

Koska kuvaukset L_a ja R_a ovat surjektioita ja injektioita, ne ovat myös bijektioita. □

Määritelmä 2.4. Luuppi G on *assosiatiivinen*, jos $(xy)z = x(yz)$ kaikilla $x, y, z \in G$. Vastaavasti luuppi G on *kommutatiivinen*, jos $xy = yx$ kaikilla $x, y \in G$.

Määritelmä 2.5. Luupin G *kertaluku* kertoo joukon G alkioiden lukumäärän. Käytetään merkintää $|G|$.

Määritelmä 2.6. Luuppi G on *äärellinen luuppi*, jos siinä on äärellinen määrä alkioita.

Lause 2.7. *Olkoon G luuppi. Tällöin kaikille alkioille $a, x, y \in G$ on voimassa seuraavat supistamislait.*

- *Jos $ax = ay$, niin $x = y$.*
- *Jos $xa = ya$, niin $x = y$.*

Todistus. Oletetaan, että $ax = ay$ eli $L_a(x) = L_a(y)$. Koska G on luuppi, niin kuvaus L_a on bijektio. Injektiivisyydestä seuraa, että jos $ax = ay$, niin täytyy olla, että $x = y$.

Oletetaan sitten, että $xa = ya$ eli $R_a(x) = R_a(y)$. Myös kuvaus R_a on bijektio, koska G on luuppi. Täten $xa = ya$ vain jos $x = y$. □

Lause 2.8. *Olkoon $(G, *)$ luuppi. Jos luuppi G on assosiatiivinen, niin se on ryhmä.*

Todistus. Olkoon luuppi G assosiatiivinen eli $(xy)z = x(yz)$ kaikilla $x, y, z \in G$. Nyt täytyy osoittaa, että luuppi G on tällöin myös ryhmä. Tehdään se osoittamalla, että kaikki määritelmän 1.21 ehdot toteutuvat. Koska $(G, *)$ on assosiatiivinen luuppi, niin $(*)$ on binäärinen ja assosiatiivinen operaatio joukossa G ja joukossa G on olemassa neutraalialkio e. Siis määritelmän 1.21 kaksi ensimmäistä ehtoa toteutuvat. Jää siis todistettavaksi ainoastaan se, että assosiatiivisen luupin jokaisella alkiolla a on olemassa käänteisalkio $a^{-1} \in G$, jolle pätee $aa^{-1} = a^{-1}a = e$.

Osoitetaan seuraavaksi, että assosiatiivisen luupin jokaisella alkiolla a on olemassa käänteisalkio $a^{-1} \in G$. Olkoon $a \in G$ ja olkoot alkiot x ja y sellaiset yksikäsitteiset joukon G alkiot, joille pätee $xa = ay = e$. Koska luuppi G on assosiatiivinen, niin saadaan $x(ax) = (xa)x = ex = x = xe$. Eli $x(ax) = xe$, josta lauseen 2.7 kohdan 2 nojalla saadaan, että $ax = e$. Nyt $ax = e = ay$, josta saadaan, että $ax = ay$. Supistamislakien nojalla $x = y$. Merkitään $x = y = a^{-1}$. On siis osoitettu, että kun luuppi G on assosiatiivinen, niin on olemassa käänteisalkio $a^{-1} \in G$, jolle pätee $a^{-1}a = aa^{-1} = e$.

Näin ollen assosiatiivinen luuppi on ryhmä.

□

Lause 2.9. *Olkoon G luuppi. Tällöin siirtokuvauksilla L_a ja R_a on olemassa käänteiskuvaukset L_a^{-1} ja R_a^{-1}.*

Todistus. Määritelmän 2.1 mukaan G on luuppi jos ja vain jos siirtokuvaukset L_a ja R_a ovat bijektioita ja joukossa G on neutraalialkio e. Koska L_a ja R_a ovat bijektioita, niin niillä on olemassa myös käänteiskuvaukset L_a^{-1} ja R_a^{-1} määritelmän 1.3 nojalla.

□

Määritellään kaksi binääristä operaatiota $(\backslash)$ ja $(/)$ joukossa G.

Määritelmä 2.10. Olkoon L_x ja R_x bijektiivisiä kuvauksia joukossa G. Tällöin $L_x^{-1}(y) = x\backslash y$ ja $R_x^{-1}(y) = y/x$ kaikilla $x, y \in G$.

Lause 2.11. *Olkoon $x, y, z \in G$. Tällöin*

$$x\backslash y = z \quad \textit{jos ja vain jos} \quad xz = y$$

ja

$$y/x = z \quad \textit{jos ja vain jos} \quad zx = y.$$

Todistus. Oletetaan ensin, että $xz = y$ eli $L_x(z) = y$. Tällöin määritelmän 1.3 mukaan $z = L_x^{-1}(y)$ eli $z = x\backslash y$. Oletetaan sitten, että $z = L_x^{-1}(y)$ eli $z = x\backslash y$. Määritelmän 1.3 mukaan $L_x(z) = y$ eli $xz = y$.

Oletetaan seuraavaksi, että $zx = y$ eli $R_x(z) = y$. Tällöin $z = R_x^{-1}(y)$ eli $z = y/x$. Oletetaan nyt, että $z = y/x$ eli $z = R_x^{-1}(y)$. Tällöin $R_x(z) = y$ eli $zx = y$.

□

Esimerkki 2.12. Olkoon $(G, *)$ luuppi ja $(/)$ binäärinen operaatio joukossa G. Millä ehdolla pari $(G, /)$ on luuppi?

Ratkaisu. Koska pari $(G, *)$ on luuppi, niin määritelmän 2.2 nojalla kaikilla $a, b \in G$ yhtälöillä $bx = a$, $ba = y$ ja $zb = a$ on yksikäsitteinen ratkaisu joukossa G.

Lauseen 2.11 nojalla $a/x = b$, $y/a = b$ ja $a/b = z$, kun $a, b \in G$. Tällöin myös näillä yhtälöillä on yksikäsitteinen ratkaisu joukossa G.

Nyt luupin määritelmästä 2.2 kaikki muut ehdot paitsi neutraalialkion olemassaolo on tarkasteltu.

Koska pari $(G, *)$ on luuppi, niin joukossa G on olemassa neutraalialkio e siten, että $xe = ex = x$ kaikilla $x \in G$.

Oletetaan ensin, että $xe = x$ kaikilla $x \in G$. Tällöin lauseen 2.11 nojalla $x/e = x$ eli tulon neutraalialkio toimii jako-operaation neutraalialkiona oikealta.

Jotta tulon neutraalialkio olisi jako-operaation neutraalialkion myös vasemmalta eli $e/x = x$, niin lauseen 2.11 nojalla $x * x = e$ eli $x^2 = e$.

Eli pari $(G, /)$ on luuppi ainoastaan silloin, kun $x^2 = e$ kaikilla $x \in G$.

Luupit voidaan määritellä myös käyttämällä binäärisiä operaatioita $(\backslash)$ ja $(/)$.

Määritelmä 2.13. Luuppi $(G, *, /, \backslash)$ on joukko G varustettuna kolmella binäärisellä operaatiolla $(*)$, $(/)$ ja $(\backslash)$ siten, että

1. $a * (a\backslash b) = b$, $(b/a) * a = b$ kaikilla $a, b \in G$,
2. $a\backslash(a * b) = b$, $(b * a)/a = b$ kaikilla $a, b \in G$,
3. $a\backslash a = b/b$ kaikilla $a, b \in G$.

Lause 2.14. *Määritelmät 2.1 ja 2.13 ovat yhtäpitäviä.*

Todistus. Oletetaan ensin, että määritelmä 2.1 on voimassa eli $(*)$ on binäärinen operaatio joukossa G, kuvaukset L_a ja R_a ovat bijektioita sekä joukossa G on olemassa neutraalialkio e. Nyt täytyy siis osoittaa, että määritelmän 2.13 kaikki ehdot pätevät.

Osoitetaan, että määritelmän 2.10 mukaiset operaatiot toteuttavat määritelmän 2.13 ehdot.

Osoitetaan ensin, että $a(a\backslash b) = b$ kaikilla $a, b \in G$. Koska L_a on bijektio, niin on olemassa käänteiskuvaus L_a^{-1}. Nyt lauseen 1.5 nojalla $L_a(L_a^{-1}(b)) = b$ eli $a(L_a^{-1}(b)) = b$ kaikilla $a, b \in G$.

Osoitetaan seuraavaksi, että $(b/a)a = b$ kaikilla $a, b \in G$. Koska R_a on bijektio, niin on olemassa käänteiskuvaus R_a^{-1}. Tällöin $R_a(R_a^{-1}(b)) = b$ eli $(R_a^{-1}(b))a = b$ aina, kun $a, b \in G$.

Osoitetaan sitten, että $a\backslash(ab) = b$ kaikilla $a, b \in G$. Nyt $L_a^{-1}(L_a(b)) = b$ eli $L_a^{-1}(ab) = b$ aina, kun $a, b \in G$.

Osoitetaan vielä, että $(ba)/a = b$ kaikilla $a, b \in G$. Nyt $R_a^{-1}(R_a(b)) = b$ eli $R_a^{-1}(ba) = b$ aina, kun $a, b \in G$.

Nyt huomataan, että käänteiskuvaukset L_a^{-1} ja R_a^{-1} toteuttavat määritelmän 2.13 ehdot. Näin ollen $L_a^{-1}(b) = a\backslash b$ ja $R_a^{-1}(b) = a/b$.

Osoitetaan lopuksi, että $a\backslash a = b/b$ aina, kun $a, b \in G$. Oletusten mukaan joukossa G on olemassa neutraalialkio e, jolle $xe = ex = x$ aina, kun $x \in G$. Nyt $a\backslash a = L_a^{-1}(a) = L_a^{-1}(ae) = L_a^{-1}(L_a(e)) = e$. Samoin $b/b = R_b^{-1}(b) = R_b^{-1}(eb) = R_b^{-1}(R_b(e)) = e$. Eli $a\backslash a = e$ ja $b/b = e$, jolloin $a\backslash a = b/b$.

Oletetaan seuraavaksi, että määritelmä 2.13 on voimassa eli ehdot ovat voimassa. Tällöin pitää osoittaa, että kuvaukset L_a ja R_a ovat bijektioita sekä joukossa G on olemassa neutraalialkio.

Osoitetaan ensin, että kuvaukset L_a ja R_a ovat injektioita.

Oletetaan, että alkiot $b, c \in G$ ja $L_a(b) = L_a(c)$. Tällöin $ab = ac$. Operoidaan yhtälöä vasemmalta puolelta alkiolla a käyttäen operaatiota $(\backslash)$, jolloin $a\backslash(ab) = a\backslash(ac)$. Määritelmän 2.13 toisen ehdon nojalla tästä seuraa, että $b = c$. Näin ollen kuvaus L_a on injektio. Oletetaan sitten, että $R_a(b) = R_a(c)$ eli $ba = ca$. Operoidaan yhtälöä oikealta puolelta alkiolla a käyttäen operaatiota $(/)$, jolloin saadaan $(ba)/a = (ca)/a$, josta määritelmän 2.13 toisen ehdon nojalla seuraa, että $b = c$. Eli kuvaus R_a on injektio.

Osoitetaan seuraavaksi, että kuvaukset L_a ja R_a ovat surjektioita.

Olkoon a joukon G kiinnitetty alkio. Tällöin jokaiselle $b \in G$ on määritelmän 2.13 ensimmäisen ehdon nojalla olemassa sellainen alkio $a\backslash b \in G$, että $b = a(a\backslash b)$. Tällöin $b = L_a(a\backslash b)$ eli kuvaus L_a on surjektio. Toisaalta jokaiselle alkiolle $b \in G$ on olemassa alkio $b/a \in G$ siten, että $b = (b/a)a$. Siis $b = R_a(b/a)$, jolloin R_a on surjektio.

Koska kuvaukset L_a ja R_a ovat injektioita ja surjektioita, ne ovat myös bijektioita.

Osoitetaan seuraavaksi neutraalialkion olemassaolo. Nyt määritelmän 2.13 ehdon 3 nojalla $a\backslash a = b/b$ kaikilla $a, b \in G$. Nyt erityisesti $a\backslash a = a/a$ kaikilla $a \in G$. Merkitään $a\backslash a = x$ ja $a/a = x$. Lauseen 2.11 nojalla tästä seuraa, että $ax = a$ ja $xa = a$ eli $ax = xa = a$. Näin ollen $x = a\backslash a = a/a$ on neutraalialkio joukossa G. □

3 Aliluupit

Tässä luvussa määritellään luupin G aliluuppi H sekä siihen liittyviä käsitteitä ja tuloksia. Erityisen hyödyllinen on ensimmäinen lause, jossa kerrotaan ne kriteerit, joiden täytyy toteutua, jotta joukko olisi jonkin luupin aliluuppi. Tätä lausetta käytetään useasti myöhemmin tutkielmassa.

Määritelmä 3.1. Olkoon $(G, *)$ luuppi ja H joukon G ei-tyhjä osajoukko. Jos H on luuppi, niin sitä sanotaan luupin G *aliluupiksi*.

Lause 3.2. *Olkoon G luuppi. Joukon G ei-tyhjä osajoukko H on luupin G aliluuppi, jos ja vain jos $(H, *)$, $(H, /)$ ja $(H, \backslash)$ ovat grupoideja.*

Todistus. Oletetaan ensin, että $H \neq \emptyset$, $H \subseteq G$ ja H on luupin G aliluuppi. Tällöin täytyy siis osoittaa, että $(H, *)$, $(H, /)$ ja $(H, \backslash)$ ovat grupoideja.
Oletuksen mukaan $H \neq \emptyset$, joten riittää osoittaa, että operaatiot $(*)$, $(/)$ ja $(\backslash)$ ovat binäärisiä operaatioita joukossa H.

Koska H on aliluuppi, eli myös luuppi, niin määritelmän 2.1 mukaan $L_a : H \to H$ ja $R_a : H \to H$ ovat bijektioita, kun $a \in H$. Täten niillä on olemassa käänteiskuvaukset $L_a^{-1} : H \to H$ ja $R_a^{-1} : H \to H$, jotka ovat myös bijektioita. Joten kun $a, x \in H$, niin $L_a(x) = ax \in H$, $R_a^{-1}(x) = x/a \in H$ ja $L_a^{-1}(x) = a\backslash x \in H$. Näin ollen operaatiot $(*)$, $(/)$ ja $(\backslash)$ ovat binäärisiä operaatioita joukossa H. Siis $(H, *)$, $(H, /)$ ja $(H, \backslash)$ ovat grupoideja.

Oletetaan sitten, että $H \neq \emptyset$, $H \subseteq G$ sekä $(H, *)$, $(H, /)$ ja $(H, \backslash)$ ovat grupoideja. Täytyy siis osoittaa, että H on luupin G aliluuppi. Osoitetaan se näyttämällä, että kaikki määritelmän 2.2 ehdot toteutuvat.

Nyt $(*)$ on binäärinen operaatio joukossa H, koska oletusten mukaan $(H, *)$ on grupoidi.

Olkoon $a, b \in H$, jolloin $a, b \in G$. Koska G on luuppi, niin on olemassa yksikäsitteinen alkio $x \in G$ siten, että $ab = x$. Koska $a, b \in H$ ja $(H, *)$ on grupoidi, niin $ab \in H$, jolloin $x \in H$.

Samoin on olemassa yksikäsitteinen alkio $y \in G$ siten, että $ay = b$. Tällöin $a\backslash b = y$. Koska $a, b \in H$ ja $(H, \backslash)$ on grupoidi, niin $y \in H$.

Lisäksi on olemassa yksikäsitteinen alkio $z \in G$ siten, että $za = b$. Tällöin $b/a = z$. Koska $a, b \in H$ ja $(H, /)$ on grupoidi, niin $z \in H$.

Näin ollen aina, kun yhtälön $xy = z$ mitkä tahansa kaksi muuttujaa ovat joukon H alkioita, niin myös kolmas alkio on joukon H yksikäsitteinen alkio.

Osoitetaan vielä neutraalialkion olemassaolo.

Koska G on luuppi, on sillä olemassa neutraalialkio e. Nyt $H \neq \emptyset$, joten on olemassa $a \in H$. Tällöin $(a/a) * a = a = e * a$ eli $(a/a)a = ea$. Käyttämällä lauseen 2.7 toista supistamislakia, saadaan $a/a = e$. Koska $(H, /)$ on grupoidi ja $a \in H$, niin $e \in H$, joten joukossa H on olemassa neutraalialkio e.

Näin ollen lauseen 2.2 nojalla H on luuppi, eli H on luupin G aliluuppi. □

Lause 3.3. *Jos H on luupin G aliluuppi, niin aliluupilla H on sama neutraalialkio kuin luupilla G.*

Todistus. Olkoon luupin G neutraalialkio e_G ja aliluupin H neutraalialkio e_H. Nyt kaikilla $a \in H$ pätee $e_H a = a$. Tällöin myös luupissa G pätee $e_H a = a$. Toisaalta myös $e_G a = a$, jolloin saadaan, että $e_H a = a = e_G a$ eli $e_H a = e_G a$. Tästä saadaan lauseen 2.7 toisen supistamislain nojalla $e_H = e_G$. Näin ollen luupilla G ja aliluupilla H on sama neutraalialkio.

□

Lause 3.4. *Olkoot G luuppi ja H ja K sen aliluuppeja. Tällöin aliluuppien H ja K leikkaus $H \cap K$ on luupin G aliluuppi.*

Todistus. Nyt $H \cap K \subseteq G$ ja $H \cap K \neq \emptyset$, koska ainakin neutraalialkio $e \in H \cap K$.

Osoitetaan, että leikkaus $H \cap K$ on luupin G aliluuppi käyttämällä lausetta 3.2. Täytyy siis osoittaa, että $(H \cap K, *)$, $(H \cap K, \backslash)$ ja $(H \cap K, /)$ ovat grupoideja.

Oletetaan ensin, että $a, b \in H \cap K$. Tällöin $a, b \in H$. Koska H on aliluuppi, niin $(H, *)$, $(H, \backslash)$ ja $(H, /)$ ovat grupoideja. Siis $ab \in H$, $a\backslash b \in H$ ja $a/b \in H$.

Toisaalta $a, b \in K$, sillä $a, b \in H \cap K$. Koska K on luupin G aliluuppi, niin $(K, *)$, $(K, \backslash)$ ja $(K, /)$ ovat grupoideja. Tällöin $ab \in K$, $a\backslash b \in K$ ja $a/b \in K$.

Ollaan siis saatu, että $ab \in H$, $a\backslash b \in H$ ja $a/b \in H$ sekä $ab \in K$, $a\backslash b \in K$ ja $a/b \in K$. Tällöin siis $ab \in H \cap K$, $a\backslash b \in H \cap K$ ja $a/b \in H \cap K$. Näin ollen $(H \cap K, *)$, $(H \cap K, \backslash)$ ja $(H \cap K, /)$ ovat grupoideja. Lauseen 3.2 mukaan $H \cap K$ on luupin G aliluuppi.

□

Lause 3.5. *Olkoot $(G, *)$ luuppi, $\emptyset \neq S \subseteq G$ ja T jokin ei-tyhjä luupin G aliluuppien joukko, jolle $S \subseteq H$ aina, kun $H \in T$. Tällöin $\bigcap_{H \in T} H$ on luupin G aliluuppi, jolle pätee $\emptyset \neq S \subseteq \bigcap_{H \in T} H$.*

Todistus. Merkitään $D = \bigcap_{H \in T} H$. Koska $T \neq \emptyset$, niin D on joukko, jolle pätee $S \subseteq D \subseteq G$. Koska $S \neq \emptyset$, niin $D \neq \emptyset$, joten $\emptyset \neq D \subseteq G$. Olkoon nyt $a, b \in D$. Tällöin $a, b \in H$ aina, kun $H \in T$. Koska jokainen $H \in T$ on luupin G aliluuppi, niin lauseen 3.2 nojalla $(H, *)$, $(H, /)$ ja $(H, \backslash)$ ovat grupoideja. Täten $ab \in H$, $a/b \in H$ ja $a\backslash b \in H$ kaikilla $H \in T$. Tästä seuraa, että $ab, a/b$ ja $a\backslash b$ ovat joukon D alkioita. Täten $(D, *)$, $(D, /)$ ja $(D, \backslash)$ ovat grupoideja.

□

Olkoot G luuppi, $\emptyset \neq S \subseteq G$ ja T kaikkien sellaisten luupin G aliluuppien joukko, joiden osajoukko on S. Koska $G \in T$, niin $T \neq \emptyset$. Lauseen 3.5 mukaan $\bigcap_{H \in T} H$ on luupin G aliluuppi ja $S \subseteq \bigcap_{H \in T} H$. Käytetään merkintää $< S >= \bigcap_{H \in T} H$.

Määritelmä 3.6. Olkoot G luuppi ja $\emptyset \neq S \subseteq G$. Olkoon lisäksi T kaikkien niiden luupin G aliluuppien H joukko, joille $S \subseteq G$ aina, kun $H \in T$. Tällöin luupin G aliluuppia $< S >$ kutsutaan *joukon S generoimaksi aliluupiksi.*

Määritelmä 3.7. Olkoot G luuppi, H luupin G aliluuppi ja $a \in G$. Joukkoa $aH = \{ah \mid h \in H\}$ sanotaan *alkion a määräämäksi aliluupin H vasemmaksi sivuluokaksi.* Vastaavasti joukkoa $Ha = \{ha \mid h \in H\}$ sanotaan *alkion a määräämäksi aliluupin H oikeaksi sivuluokaksi.*

Määritelmä 3.8. Olkoot G luuppi ja H luupin G aliluuppi. Tällöin joukolla G on aliluupin H *vasempien sivuluokkien hajotelma* (left coset decomposition modulo H), jos kaikkien aliluupin H vasempien sivuluokkien määräämä joukko $P = \{aH \mid a \in G\}$ on luupin G ositus.

Vastaavasti joukolla G on aliluupin H *oikeiden sivuluokkien hajotelma* (right coset decomposition modulo H), jos kaikkien aliluupin H oikeiden sivuluokkien määräämä joukko $P' = \{Ha \mid a \in G\}$ on luupin G ositus.

Lause 3.9. *Olkoot G luuppi ja H luupin G aliluuppi. Tällöin joukolla G on aliluupin H vasempien sivuluokkien hajotelma, jos ja vain jos $(ah)H = aH$ kaikilla $a \in G$ ja $h \in H$.*

Vastaavasti joukolla G on aliluupin H oikeiden sivuluokkien hajotelma, jos ja vain jos $H(ha) = Ha$ kaikilla $a \in G$ ja $h \in H$.

Todistus. Oletetaan ensin, että joukolla G on aliluupin H vasempien sivuluokkien hajotelma. On siis tarkoitus osoittaa, että $(ah)H = aH$. Nyt oletuksen nojalla kaikkien aliluupin H vasempien sivuluokkien määräämä joukko P on joukon G ositus. Koska H on aliluuppi, niin on olemassa neutraalialkio $e \in H$ siten, että $xe = ex = x$ aina, kun $x \in H$. Nyt jokaiselle alkiolle $a \in G$ ja $h \in H$ pätee, että $ah = (ah)e$. Täten $ah \in aH \cap (ah)H$. Näin ollen $aH \in P$, $(ah)H \in P$ ja $(ah)H \cap aH \neq \emptyset$. Koska P on joukon G ositus, niin määritelmän 1.19 kolmannen kohdan nojalla $(ah)H = aH$ aina, kun $a \in G$ ja $h \in H$.

Oletetaan seuraavaksi, että $(ah)H = aH$ aina, kun $a \in G$ ja $h \in H$. Tällöin täytyy osoittaa, että joukko P on luupin G ositus. Tämä osoitetaan näyttämällä, että kaikki määritelmän 1.19 ehdot pätevät.

Olkoon $X \in P$, jolloin $X = gH$ jollakin $g \in G$. Tällöin täytyy osoittaa, että $X \neq \emptyset$. Koska $X = gH$ ja aliluupilla H on olemassa neutraalialkio e, niin $g = ge \in gH$, jolloin $X \neq \emptyset$.

Osoitetaan seuraavaksi, että $G = \bigcup_{X \in P} X$. Nyt jokaiselle $g \in G$ pätee, että $g = ge \in gH$, jolloin $G = \bigcup_{X \in P} X$.

Vielä on osoitettava, että kun $X \in P$, $Y \in P$ ja $X \cap Y \neq \emptyset$, niin $X = Y$. Oletetaan, että $X \cap Y \neq \emptyset$, jolloin on olemassa $g \in X \cap Y$. Täten $g = ax = by$, joillakin $x, y \in H$ ja $a, b \in G$. Oletuksen $(ah)H = aH$ nojalla $aH = (ax)H = (by)H = bH$, josta seuraa, että $aH = bH$ eli $X = Y$.

Eli joukko P on luupin G ositus.

Jotta todistus olisi täydellinen, täytyy vielä osoittaa, että joukolla G on aliluupin H oikeiden sivuluokkien hajotelma, jos ja vain jos $H(ha) = Ha$ kaikilla $a \in G$ ja $h \in H$.

Oletetaan ensin, että joukolla G on aliluupin H oikeiden sivuluokkien hajotelma. Jää siis todistettavaksi, että $H(ha) = Ha$ kaikilla $a \in G$ ja $h \in H$. Nyt kaikkien aliluupin H oikeiden sivuluokkien määräämä joukko P' on joukon G ositus ja joukossa H on olemassa neutraalialkio e, jolle pätee $xe = ex = x$ kaikilla $x \in H$. Nyt jokaiselle alkiolle $a \in G$ ja $h \in H$ pätee $ha = e(ha)$, joten $ha \in Ha \cap H(ha)$. Tästä seuraa, että $Ha \in P'$, $H(ha) \in P'$ ja $H(ha) \cap Ha \neq \emptyset$. Näin ollen määritelmän 1.19 nojalla $H(ha) = Ha$ aina, kun $a \in G$ ja $h \in H$.

Oletetaan seuraavaksi, että $H(ha) = Ha$ aina, kun $a \in G$ ja $h \in H$. Täytyy siis osoittaa, että joukko P' on luupin G ositus.

Osoitetaan, että $X \neq \emptyset$. Oletetaan, että $X \in P'$, jolloin $X = Hg$ jollakin $g \in G$. Tällöin $g = eg \in Hg$, jolloin $X \neq \emptyset$.

Osoitetaan sitten, että $G = \bigcup_{X \in P} X$. Nyt jokaiselle $g \in G$ pätee, että $g = eg \in Hg$, jolloin $G = \bigcup_{X \in P} X$.

Osoitetaan vielä, että kun $X \in P'$, $Y \in P'$ ja $X \cap Y \neq \emptyset$, niin $X = Y$. Oletetaan, että $X \cap Y \neq \emptyset$, jolloin on olemassa $g \in X \cap Y$. Täten $g = xa = yb$, joillakin $x, y \in H$ ja $a, b \in G$. Tällöin $Ha = H(xa) = H(yb) = Hb$, josta seuraa, että $aH = bH$ eli $X = Y$.

Eli joukko P' on luupin G ositus.

Näin ollen koko lause 3.9 on todistettu.

□

Esimerkki 3.10. Olkoot G luuppi ja H luupin G aliluuppi. Osoitetaan ekvivalenssirelaatioiden avulla, että jos $(ah)H = aH$ kaikilla $a \in G$ ja $h \in H$, niin joukolla G on aliluupin H vasempien sivuluokkien hajotelma. Riittää löytää sellainen ekvivalenssirelaatio R joukossa G, että ekvivalenssirelaation R ekvivalenssiluokka $[a] = aH$ aina, kun $a \in G$, sillä lauseen 1.20 nojalla ekvivalenssiluokat ovat luupin G ositus, jolloin joukolla G on aliluupin H vasempien sivuluokkien hajotelma.

Määritellään joukon G relaatio siten, että joukon G alkio a on relaatiossa joukon G alkion b kanssa eli aRb, jos ja vain jos yhdistetty kuvaus $L_b^{-1} L_a$

on joukon H bijektio. Tarkastellaan, onko tämä relaatio ekvivalenssirelaatio käymällä läpi kaikki määritelmän 1.13 ehdot.

Tutkitaan ensin, onko aRa, kun $a \in G$. Täytyy siis tutkia onko yhdistetty kuvaus $L_a^{-1}L_a$ bijektio joukossa H. Koska kuvaukset L_a ja L_a^{-1} ovat bijektioita, niin lauseen 1.9 perusteella yhdistetty kuvaus $L_a^{-1}L_a$ on bijektio. Lauseen 1.8 nojalla $L_a^{-1}L_a = I_G$. Täten yhdistetty kuvaus $L_a^{-1}L_a$ on bijektio joukossa H, jolloin aRa.

Oletetaan seuraavaksi, että aRb, jolloin $L_b^{-1}L_a$ on joukon H bijektio. Halutaan siis osoittaa, että tällöin bRa eli yhdistetty kuvaus $L_a^{-1}L_b$ on joukon H bijektio. Koska oletuksen mukaan yhdistetty kuvaus $L_b^{-1}L_a$ on bijektio joukossa H, niin sillä on olemassa käänteiskuvaus $(L_b^{-1}L_a)^{-1}$ joukossa H. Lauseen 1.4 nojalla käänteiskuvaus $(L_b^{-1}L_a)^{-1}$ on bijektio joukossa H. Käyttämällä lausetta 1.9 saadaan, että $(L_b^{-1}L_a)^{-1} = L_a^{-1}L_b$. Näin ollen kuvaus $L_a^{-1}L_b$ on bijektio joukossa H eli bRa.

Oletetaan nyt, että aRb ja bRc eli $L_b^{-1}L_a$ ja $L_c^{-1}L_b$ ovat joukon H bijektioita. Tällöin on tarkoitus osoittaa, että aRc eli toisin sanoen täytyy osoittaa, että $L_c^{-1}L_a$ on joukon H bijektio. Nyt $L_b^{-1}L_a = L_b^{-1} \circ L_a$ ja $L_c^{-1}L_b = L_c^{-1} \circ L_b$ ja siten

$$\begin{aligned}
(L_c^{-1} \circ L_b) \circ (L_b^{-1} \circ L_a) &= L_c^{-1} \circ L_b \circ (L_b^{-1} \circ L_a) \\
&= L_c^{-1} \circ (L_b \circ (L_b^{-1} \circ L_a)) \\
&= L_c^{-1} \circ ((L_b \circ L_b^{-1}) \circ L_a) \\
&= L_c^{-1} \circ (I_G \circ L_a) \\
&= L_c^{-1} \circ L_a \\
&= L_c^{-1}L_a
\end{aligned}$$

Siten $L_c^{-1}L_a$ on joukon H bijektio ja tällöin aRc.

On siis osoitettu, että relaatio aRb, jos ja vain jos yhdistetty kuvaus $L_b^{-1}L_a$ on joukon H bijektio, on ekvivalenssirelaatio joukossa G.

Lähdetään tutkimaan seuraavaksi, millainen on alkion $a \in G$ määräämä ekvivalenssiluokka.

$$\begin{aligned}
[a] &= \{x \in G \mid xRa\} \\
&= \{x \in G \mid L_a^{-1}L_x \text{ on bijektio joukossa } H\} \\
&= \{x \in G \mid L_a^{-1}L_x(b) \in H \text{ aina, kun } b \in H\} \\
&= \{x \in G \mid L_a^{-1}(xb) = h, \text{ missä } h \text{ on yksikäsitteinen aliluupin } H \text{ alkio}\} \\
&= \{x \in G \mid a\backslash(xb) = h, \text{ missä } h \text{ on yksikäsitteinen aliluupin } H \text{ alkio ja } b \in H\} \\
&= \{x \in G \mid ah = xb, \text{ missä } h \text{ on yksikäsitteinen aliluupin } H \text{ alkio ja } b \in H\} \\
&= \{x \in G \mid aH = xH\} \\
&= \{x \in G \mid x \in aH\} \\
&= aH
\end{aligned}$$

On siis muodostettu ekvivalenssirelaation R ekvivalenssiluokka $[a] = aH$. Lauseen 1.20 nojalla ekvivalenssirelaation R ekvivalenssiluokat $[a]$ ovat luupin G ositus, eli joukolla G on vasempien sivuluokkien hajotelma.

Määritelmä 3.11. Olkoon G äärellinen luuppi ja H luupin G aliluuppi. Aliluuppi H on *Lagrangen kaltainen* (Lagrange-like), jos aliluupin H kertaluku $|H|$ jakaa luupin G kertaluvun $|G|$.

Määritelmä 3.12. Olkoon G äärellinen luuppi. Luupilla G on *heikko Lagrangen ominaisuus* (weak Lagrange property), jos jokainen luupin G aliluuppi on Lagrangen kaltainen.

Määritelmä 3.13. Olkoon G äärellinen luuppi. Luupilla G on *vahva Lagrangen ominaisuus* (strong Lagrange property), jos aliluupilla H on heikko Lagrangen ominaisuus aina, kun H on luupin G aliluuppi. Eli toisin sanoen, aina kun H on luupin G aliluuppi, niin aliluupin H aliluupin K kertaluku $|K|$ jakaa aliluupin H kertaluvun $|H|$.

Esimerkki 3.14. Olkoot G äärellinen luuppi, kertaluku $|G| = 12$ ja e luupin G neutraalialkio. Olkoot lisäksi luupin G ainoat aliluupit $\{e\}$, K ja H siten, että K on myös aliluupin H aliluuppi sekä $|H| = 6$ ja $|K| = 4$. Nyt huomataan, että sekä aliluupin H että aliluupin K kertaluku jakaa luupin G kertaluvun, mutta aliluupin K kertaluku ei jaa aliluupin H kertalukua. Näin ollen luupilla G on heikko Lagrangen ominaisuus, mutta ei vahvaa Lagrangen ominaisuutta.

Lause 3.15. *Olkoot G äärellinen luuppi ja H luupin G aliluuppi. Jos luupilla G on aliluupin H vasempien sivuluokkien hajotelma, niin aliluuppi H on Lagrangen kaltainen.*

Vastaavasti, jos luupilla G on aliluupin H oikeiden sivuluokkien hajotelma, niin aliluuppi H on Lagrangen kaltainen.

Todistus. Todistetaan lause siinä tapauksessa, että luupilla G on aliluupin H vasempien sivuluokkien hajotelma. Tapaus, jolloin luupilla G on aliluupin H oikeiden sivuluokkien hajotelma menee vastaavasti.

Olkoot luupilla G aliluupin H vasempien sivuluokkien hajotelma ja olkoon P kaikkien aliluupin H vasempien sivuluokkien joukko. Täytyy siis osoittaa, että aliluuppi H on Lagrangen kaltainen eli aliluupin H kertaluku $|H|$ jakaa luupin G kertaluvun $|G|$. Koska luupilla G on olemassa vasempien sivuluokkien hajotelma, niin määritelmän 3.8 mukaan P on luupin G ositus. Osituksen määritelmän mukaan $X \cap Y = \emptyset$, jos $X \neq Y$, ja $G = \bigcup_{X \in P} X$. Tästä saadaan, että

$$|G| = \sum_{X \in P} |X|.$$

Olkoon nyt $X \in P$, jolloin $X = aH$ jollakin $a \in G$. Määritellään seuraavaksi kuvaus $\alpha : H \to aH$ siten, että $\alpha(h) = ah$ kaikilla $h \in H$. Osoitetaan, että kuvaus α on bijektio.

Kuvauksen α surjektiivisuus seuraa suoraan vasemman sivuluokan määritelmästä, sillä jokaista alkion $a \in G$ ja $h \in H$ operaatiota ah kohtaan on olemassa alkio h siten, että $\alpha(h) = ah$.

Oletetaan nyt, että $\alpha(h_1) = \alpha(h_2)$. Tällöin $ah_1 = ah_2$. Koska G on luuppi, niin lauseen 2.7 nojalla $h_1 = h_2$ eli kuvaus α on myös injektio.

Kuvaus α on sekä surjektio että injektio, jolloin se on myös bijektio.

Kuvauksen α bijektiivisyyden takia $|H| = |aH|$ eli $|H| = |X|$. Tästä seuraa, että

$$|G| = \sum_{X \in P} |X| = |P||H|.$$

Täten aliluupin H kertaluku $|H|$ jakaa luupin G kertaluvun $|G|$. Siis aliluuppi H on Lagrangen kaltainen.

□

Lause 3.16. *Olkoot G luuppi ja H luupin G aliluuppi. Jos $(ah)H = aH$ kaikilla $a \in G$ ja $h \in H$, niin aliluuppi H on Lagrangen kaltainen.*

Vastaavasti jos $H(ha) = Ha$ kaikilla $a \in G$ ja $h \in H$, niin aliluuppi H on Lagrangen kaltainen.

Todistus. Lause seuraa suoraan lauseista 3.9 ja 3.15.

□

Määritelmä 3.17. Olkoot G luuppi ja H luupin G aliluuppi. Olkoot lisäksi luupilla G aliluupin H vasempien ja oikeiden sivuluokkien hajotelma. Aliluuppia H kutsutaan *normaaliksi aliluupiksi*, jos

$xH = Hx$, $(xH)y = x(Hy)$ ja $x(yH) = (xy)H$ aina, kun $x, y \in G$.

4 Luupin ydin ja keskus

Tässä luvussa tutustutaan luupin ytimeen N sekä luupin keskukseen Z. Luvussa osoitetaan, että ydin N ja keskus Z ovat luupin G aliryhmiä.

Määritelmä 4.1. Olkoot G grupoidi ja $a \in G$. Alkio a on grupoidin G *vasen ytimen alkio* (left nuclear), jos $L_{ax} = L_a L_x$ kaikilla $x \in G$.

Vastaavasti alkio a on grupoidin G *keskimmäinen ytimen alkio* (middle nuclear), jos $L_{xa} = L_x L_a$.

Lisäksi alkio a on grupoidin G *vasen ytimen alkio* (right nuclear), jos $R_{xa} = R_a R_x$.

Alkio a on grupoidin G *ytimen alkio* (nuclear), jos a on sekä vasen, keskimmäinen että oikea ytimen alkio.

Määritelmä 4.2. Olkoon G grupoidi. Grupoidin G *vasen ydin* (left nucleus) N_λ on kaikkien grupoidin G vasempien ytimen alkioiden joukko.

Samoin grupoidin G *keskimmäinen ydin* (middle nucleus) N_μ on kaikkien grupoidin G keskimmäisten ytimen alkioiden joukko.

Vastaavasti grupoidin G *oikea ydin* (right nucleus) N_ρ on kaikkien grupoidin G oikeiden ytimen alkioiden joukko.

Lisäksi grupoidin G *ydin* (nucleus) $N = N_\lambda \cap N_\mu \cap N_\rho$.

Nyt

$$\begin{aligned} N_\lambda &= \{a \in G \mid L_{ax}(y) = L_a L_x(y),\ x, y \in G\} \\ &= \{a \in G \mid (ax)y = a(xy),\ x, y \in G\}, \end{aligned}$$

$$\begin{aligned} N_\mu &= \{a \in G \mid L_{xa}(y) = L_x L_a(y),\ x, y \in G\} \\ &= \{a \in G \mid (xa)y = x(ay),\ x, y \in G\}, \end{aligned}$$

$$\begin{aligned} N_\rho &= \{a \in G \mid R_{xa}(y) = R_a R_x(y),\ x, y \in G\} \\ &= \{a \in G \mid y(xa) = (yx)a,\ x, y \in G\}. \end{aligned}$$

Lause 4.3. *Olkoon G grupoidi. Jos vasen ydin N_λ on ei-tyhjä, niin N_λ on grupoidin G aligrupoidi.*

Vastaavasti jos keskimmäinen ydin N_μ on ei-tyhjä, niin N_μ on grupoidin G aligrupoidi ja jos oikea ydin N_ρ on ei-tyhjä, niin N_ρ on grupoidin G aligrupoidi.

Todistus. Todistetaan väite keskimmäisen ytimen tapauksessa. Kun kyseessä on vasen tai oikea ydin, niin todistus menee vastaavasti.

Oletetaan, että $N_\mu \neq \emptyset$ ja olkoon $a, b \in N_\mu$. Koska $a \in N_\mu$, niin $x(ab) = (xa)b$ kaikilla $x \in G$. Tällöin $L_{x(ab)} = L_{(xa)b} = L_{xa} L_b = L_x L_a L_b = L_x L_{ab}$

kaikilla $x \in G$. Täten määritelmän 4.1 nojalla alkio ab on grupoidin G keskimmäisen ytimen alkio. Näin ollen alkio $ab \in N_\mu$, jolloin N_μ on grupoidin G aligrupoidi.

□

Lause 4.4. *Olkoon G luuppi. Tällöin ytimet N_λ, N_μ ja N_ρ ovat luupin G aliryhmiä.*

Todistus. Olkoon e luupin G neutraalialkio. Osoitetaan, että $e \in N_\lambda \cap N_\mu \cap N_\rho$.

Osoitetaan ensin, että $e \in N_\lambda$. Olkoon $x, y \in G$. Koska e on luupin G neutraalialkio, niin $e(xy) = xy = (ex)y$. Näin ollen e on joukon N_λ neutraalialkio.

Osoitetaan sitten, että $e \in N_\mu$. Koska e on luupin G neutraalialkio, niin $(xe)y = xy = x(ey)$ kaikilla $x, y \in G$. Eli $e \in N_\mu$.

Osoitetaan vielä, että $e \in N_\rho$. Olkoon $x, y \in G$. Tällöin $(xy)e = xy = x(ye)$, jolloin e on joukon N_ρ neutraalialkio.

Saatiin siis osoitettua, että $e \in N_\lambda \cap N_\mu \cap N_\rho$.

Osoitetaan seuraavaksi, että N_μ on luupin G aliluuppi. Todistetaan se käyttämällä lausetta 3.2. Lauseen 4.3 nojalla $(N_\mu, *)$ on grupoidi, joten riittää osoittaa, että $(N_\mu, /)$ ja $(N_\mu, \backslash)$ ovat grupoideja.

Olkoon $b \in N_\mu$ ja olkoot a ja c sellaisia luupin G yksikäsitteisiä alkioita, joille pätee $ab = bc = e$. Koska e on myös aligrupoidin N_μ neutraalialkio, niin alkiolle $b \in N_\mu$ pätee $a(ba) = (ab)a = ea = a = ae$. Eli $a(ba) = ae$, josta lauseen 2.7 supistamislain nojalla saadaan $ba = e$. Toisaalta myös $bc = e$, jolloin $ba = bc$. Käyttämällä lauseen 2.7 supistamislakeja saadaan, että $a = c$. Merkitään $b^{-1} = a = c$.

Nyt kaikilla $b \in N_\mu$ ja $x \in G$ pätee $((xb)b^{-1})b = (x(bb^{-1}))b = (xe)b = xb$. Olkoon jokainen $y \in G$ sellaista muotoa, että $y = xb$. Tällöin $(yb^{-1})b = y$ kaikilla $y \in G$. Huomataan, että $y = (yb^{-1})b = (R_{b^{-1}}(y))b$. Toisaalta $(R_b^{-1}(y))b = (y/b)b = y$ eli $(R_{b^{-1}}(y))b = (R_b^{-1}(y))b$, josta lauseen 2.7 supistamislakien nojalla saadaan $R_{b^{-1}}(y) = R_b^{-1}(y)$.

Vastaavasti $b(b^{-1}(bx)) = b((b^{-1}b)x) = b(ex) = bx$. Merkitään $y = bx$, jolloin $b(b^{-1}y) = y$. Nyt $y = b(b^{-1}y) = b(L_{b^{-1}}(y))$ ja $b(L_b^{-1}(y)) = b(b\backslash y) = y$. Tällöin $b(L_{b^{-1}}(y)) = b(L_b^{-1}(y))$, josta supistamislain nojalla saadaan, että $L_{b^{-1}}(y) = L_b^{-1}(y)$ kaikilla $b \in N_\mu$ ja $y \in G$.

Osoitetaan, että käänteisalkio $b^{-1} \in N_\mu$. Nyt $y = b(b^{-1}y)$. Operoidaan yhtälöä puolittain alkiolla xb^{-1} vasemmalta puolelta, jolloin saadaan $(xb^{-1})y = (xb^{-1})(b(b^{-1}y))$. Koska $b \in N_\mu$, niin $(xb^{-1})y = ((xb^{-1})b)(b^{-1}y)$. Nyt $(xb^{-1})b = x$, joten yhtälö saadaan muotoon $(xb^{-1})y = x(b^{-1}y)$. Näin ollen $b^{-1} \in N_\mu$.

Olkoon nyt $b, c \in N_\mu$. Nyt $c/b = R_b^{-1}(c) = R_{b^{-1}}(c) = cb^{-1}$ ja $b\backslash c = L_b^{-1}(c) = L_{b^{-1}}(c) = b^{-1}c$. Koska $b^{-1} \in N_\mu$, niin lauseen 4.3 nojalla $cb^{-1} \in N_\mu$

ja $b^{-1}c \in N_\mu$, jolloin myös $c/b \in N_\mu$ ja $b\backslash c \in N_\mu$. Lauseen 4.3 mukaan N_μ on grupoidi, joten aina, kun $c, b \in N_\mu$, niin $cb \in N_\mu$. Eli $(N_\mu, *)$, $(N_\mu, /)$ ja $(N_\mu, \backslash)$ ovat grupoideja.

Lauseen 3.2 nojalla N_μ on luupin G aliluuppi. Koska N_μ on assosiatiivinen, niin lauseen 2.8 nojalla N_μ on myös luupin G aliryhmä.

Aligrupoidien N_λ ja N_ρ todistaminen luupin G aliryhmiksi menee vastaavasti kuin ytimen N_μ tapauksessa. □

Määritelmä 4.5. Olkoon G grupoidi. Joukko $Z = \{a \in N \mid L_a = R_a\}$, missä N on joukon G ydin, on grupoidin G *keskus*.

Lause 4.6. *Olkoon G grupoidi, jolla on ydin N ja keskus Z. Jos ydin N ja keskus Z ovat ei-tyhjiä, niin ne molemmat ovat joukon G aligrupoideja. Lisäksi keskus Z on ytimen N kommutatiivinen aligrupoidi.*

Todistus. Oletetaan, että $N, Z \neq \emptyset$. Osoitetaan ensin, että N on grupoidin G aligrupoidi. Nyt $N = N_\lambda \cap N_\mu \cap N_\rho$. Olkoon $a, b \in N$ eli $a, b \in N_\lambda \cap N_\mu \cap N_\rho$. Tällöin $a, b \in N_\lambda$, $a, b \in N_\mu$ ja $a, b \in N_\rho$. Lauseen 4.3 nojalla N_λ, N_μ ja N_ρ ovat grupoidin G aligrupoideja, joten tällöin $ab \in N_\lambda$, $ab \in N_\mu$ ja $ab \in N_\rho$. Eli $ab \in N_\lambda \cap N_\mu \cap N_\rho = N$. Näin ollen myös N on luupin G aligrupoidi.

Osoitetaan seuraavaksi, että keskus Z on grupoidin G aligrupoidi ja ytimen N kommutatiivinen aligrupoidi.

Määritelmän 4.5 mukaan alkio $a \in G$ on keskuksen Z alkio, jos sille pätee $a(xy) = (ax)y$, $(xa)y = x(ay)$, $(xy)a = x(ya)$ ja $ax = xa$ kaikilla $x, y \in G$. Nyt siis nähdään, että Z on joukon N osajoukko.

Koska $Z \subseteq N$ ja N on grupoidin G aligrupoidi, tarvitsee enää osoittaa, että alkioille $a, b \in Z$ pätee $L_{ab}(x) = R_{ab}(x)$ eli $(ab)x = x(ab)$ kaikilla $x \in G$. Olkoon $a, b \in Z$. Tällöin $L_{ab}(x) = (ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab) = R_{ab}(x)$.

Näin ollen Z on grupoidi, eli se on grupoidin G aligrupoidi. Keskuksen määritelmän mukaan $L_x(y) = xy = yx = R_x(y)$ aina, kun $x, y \in N$, joten määritelmän 2.4 mukaan Z on kommutatiivinen grupoidi. Koska $Z \subseteq N$, niin keskus Z on ytimen N kommutatiivinen aligrupoidi.

□

Lause 4.7. *Olkoon G luuppi, jolla on ydin N ja keskus Z. Tällöin ydin N ja keskus Z ovat luupin G aliryhmiä. Lisäksi Z on ytimen N kommutatiivinen aliryhmä.*

Todistus. Osoitetaan ensin, että ydin N on luupin G aliryhmä. Nyt lauseen 4.4 mukaan ytimet N_λ, N_μ ja N_ρ ovat luupin G aliryhmiä. Koska ytimet N_λ, N_μ ja N_ρ ovat aliryhmiä, ne ovat myös luupin G aliluuppeja. Lauseen 3.4

nojalla tällöin myös leikkaus $N = N_\lambda \cap N_\mu \cap N_\rho$ on luupin G aliluuppi. Koska leikkaus N on assosiatiivinen, niin se on luupin G aliryhmä.

Osoitetaan, että keskus Z on luupin G aliryhmä näyttämällä, että lauseen 1.24 ehdot toteutuvat. Koska ydin N on luupin G aliryhmä ja $Z \subseteq N$, niin riittää osoittaa, että kun $a, b \in Z$, niin $(ab)x = x(ab)$ ja kun $a \in Z$, niin käänteisalkiolle $a^{-1} \in N$ pätee $a^{-1}x = xa^{-1}$ kaikilla $x \in G$, jolloin $a^{-1} \in Z$. Edellisessä lauseessa osoitettiin, että kun $a, b \in Z$, niin $(ab)x = x(ab)$ kaikilla $x \in G$. Osoitetaan sitten, että $a^{-1}x = xa^{-1}$. Olkoon $a \in Z$ ja $a^{-1} \in N$. Tällöin $a^{-1}x = a^{-1}(xe) = a^{-1}(x(aa^{-1})) = a^{-1}((xa)a^{-1}) = a^{-1}((ax)a^{-1}) = a^{-1}(a(xa^{-1})) = (a^{-1}a)(xa^{-1}) = xa^{-1}$ kaikilla $x \in G$. Todistuksessa on hyödynnetty sitä, että $a \in Z$ ja $a^{-1} \in N$.

□

Lause 4.8. *Olkoon G luuppi. Luupin G keskus Z on luupin G normaali aliluuppi.*

Todistus. Lauseen 4.7 nojalla keskus Z on luupin G aliryhmä. Tällöin keskus Z on myös luupin G aliluuppi.

Osoitetaan vielä, että keskus Z on normaali aliluuppi näyttämällä, että määritelmän 3.17 ehdot toteutuvat. Täytyy siis osoittaa, että $xZ = Zx$, $(xZ)y = x(Zy)$ ja $x(yZ) = (xy)Z$ aina, kun $x, y \in G$.

Määritelmän 4.5 mukaan alkio h on keskuksen Z alkio, jos sille pätee $h(xy) = (hx)y$, $(xh)y = x(hy)$, $(xy)h = x(yh)$ ja $xh = hx$ kaikilla $x, y \in G$. Näin ollen kaikille $h \in Z$ pätee $xh = hx$, $(xh)y = x(hy)$ ja $x(yh) = (xy)h$ eli $xZ = Zx$, $(xZ)y = x(Zy)$ ja $x(yZ) = (xy)Z$. Joten keskus Z on määritelmän 3.17 nojalla luupin G normaali aliluuppi.

□

5 Käänteisominaisuus

Tässä luvussa käsitellään luupin vasempia ja oikeita käänteisalkioita sekä määritellään luupin käänteisominaisuus. Lisäksi luvussa määritellään luuppien erikoistapauksia ja esitellään niihin liittyviä tuloksia.

Määritelmä 5.1. Olkoot G luuppi ja $a \in G$. Alkion a *oikea käänteisalkio* (right inverse) on sellainen alkio $a^\rho \in G$, että $aa^\rho = e$, missä e on luupin G neutraalialkio.

Vastaavasti alkion a *vasen käänteisalkio* (left inverse) on sellainen alkio $a^\lambda \in G$, että $a^\lambda a = e$.

Lause 5.2. *Olkoon G luuppi ja olkoon e luupin G neutraalialkio. Jokaisella alkiolla $a \in G$ on olemassa yksikäsitteinen vasen käänteisalkio a^λ ja yksikäsitteinen oikea käänteisalkio a^ρ, joille pätee $a^\lambda a = aa^\rho = e$.*

Todistus. Olkoot $a \in G$ ja e luupin G neutraalialkio. Määritelmän 2.2 nojalla on olemassa sellaiset alkiot a^λ ja a^ρ, että $a^\lambda a = e$ ja $aa^\rho = e$. Koska $a, e \in G$, niin määritelmän 2.2 perusteella $a^\lambda \in G$ ja $a^\rho \in G$. □

Lause 5.3. *Olkoon G luuppi. Jokaisella luupin G alkiolla a on olemassa eri käänteisalkio, sekä vasen, että oikea. Eli jos $a, b \in G$ ja $a \neq b$, niin $a^\lambda \neq b^\lambda$ ja $a^\rho \neq b^\rho$.*

Todistus. Osoitetaan väite ensin oikeille käänteisalkioille. Oletetaan, että alkiot $a, b \in G$ ja $a \neq b$. Koska $a \in G$ niin myös $a^\rho \in G$. Oletetaan, että kahdella eri alkiolla $a, b \in G$ on sama oikea käänteisalkio a^ρ eli $aa^\rho = ba^\rho = e$. Tällöin voidaan käyttää lauseen 2.7 supistuslakeja, jolloin saadaan $a = b$. Tulos on ristiriidassa oletuksen kanssa, joten jos $a, b \in G$ ja $a \neq b$, niin $a^\rho \neq b^\rho$.

Väite todistetaan vastaavasti myös vasemmille käänteisalkioille. Oletetaan, että $a, b \in G$ ja $a \neq b$, jolloin $a^\lambda \in G$. Oletetaan, että $a^\lambda a = a^\lambda b = e$ kaikilla $a, b \in G$. Tällöin lauseen 2.7 nojalla $a = b$, joka on ristiriidassa oletuksen kanssa. Näin ollen, jos $a, b \in G$ ja $a \neq b$, niin $a^\lambda \neq b^\lambda$. □

Määritelmä 5.4. Olkoon G luuppi. Luupilla G on *vasen käänteisominaisuus* (left inverse property), jos on olemassa joukon G bijektiivinen kuvaus $J_\lambda : a \to a^\lambda$ siten, että $a^\lambda(ax) = x$ kaikilla $x \in G$. Tällaista luuppia kutsutaan *L.I.P. -luupiksi.*

Vastaavasti luupilla G on *oikea käänteisominaisuus* (right inverse property), jos on olemassa joukon G bijektiivinen kuvaus $J_\rho : a \to a^\rho$ siten, että $(xa)a^\rho = x$ kaikilla $x \in G$. Tällaista luuppia kutsutaan *R.I.P. -luupiksi.*

Sellaisella luupilla, jolla on sekä vasen että oikea käänteisominaisuus, on *käänteisominaisuus* (inverse property). Tällaista luuppia sanotaan *I.P. -luupiksi.*

Lause 5.5. *Jos G on L.I.P. -luuppi tai R.I.P. -luuppi, niin $a^\lambda = a^\rho = a^{-1}$, missä $aa^{-1} = a^{-1}a = e$ ja e on luupin G neutraalialkio.*

Todistus. Olkoon G L.I.P. -luuppi eli luuppi, jolla on vasen käänteisominaisuus ja jonka neutraalialkio on e. Tällöin $aa^\rho = e$, $a^\lambda a = e$ ja $a^\lambda(aa^\rho) = a^\rho$. Toisaalta $a^\lambda(aa^\rho) = a^\lambda e = a^\lambda$. Siis $a^\lambda = a^\rho = a^{-1}$.

Olkoon sitten G R.I.P. -luuppi eli luuppi, jolla on oikea käänteisominaisuus ja jonka neutraalialkio on e. Nyt $(a^\lambda a)a^\rho = a^\lambda$ ja $(a^\lambda a)a^\rho = ea^\rho = a^\rho$, jolloin $a^\rho = a^\lambda = a^{-1}$.

On siis osoitettu, että jos G on L.I.P. -luuppi tai R.I.P. -luuppi, niin $a^\lambda = a^\rho = a^{-1}$.

□

Lause 5.6. *Olkoon G I.P. -luuppi ja $a, b \in G$. Tällöin $(ab)^{-1} = b^{-1}a^{-1}$.*

Todistus. Olkoon $ab = c$, missä $a, b \in G$. Koska $a, b, c \in G$, niin myös $a^{-1}, b^{-1}, c^{-1} \in G$. Operoidaan yhtälöä $ab = c$ oikealta alkiolla b^{-1}, jolloin saadaan $(ab)b^{-1} = cb^{-1}$. Koska G on I.P. -luuppi, niin $a = cb^{-1}$. Operoidaan tätä yhtälöä vasemmalta puolelta alkiolla c^{-1}. Nyt $c^{-1}a = c^{-1}(cb^{-1})$ eli $c^{-1}a = b^{-1}$. Operoidaan saatua yhtälöä oikealta alkiolla a^{-1}. Tällöin $b^{-1}a^{-1} = (c^{-1}a)a^{-1}$, josta saadaan $c^{-1} = b^{-1}a^{-1}$. Aluksi määriteltiin, että $c = ab$, jolloin $c^{-1} = (ab)^{-1}$. Näin ollen $(ab)^{-1} = b^{-1}a^{-1}$.

□

Lause 5.7. *Olkoot G I.P. -luuppi ja $a \in G$. Tällöin $(a^{-1})^{-1} = a$.*

Todistus. Olkoon $a \in G$. Koska G on I.P. -luuppi, niin $(a^{-1})^{-1}(a^{-1}(ax)) = ax$. Toisaalta $a^{-1}(ax) = x$, jolloin $(a^{-1})^{-1}x = ax$. Käyttämällä lauseen 2.7 supistamislakeja saadaan $(a^{-1})^{-1} = a$.

□

Lause 5.8. *Olkoon luuppi G I.P. -luuppi, eli luuppi, jolla on sekä vasen että oikea käänteisominaisuus. Tällöin ytimille N_λ, N_ρ ja N_μ pätee $N_\lambda = N_\rho = N_\mu = N$.*

Todistus. Olkoon N_λ, N_ρ ja N_μ I.P. -luupin G ytimiä. Osoitetaan ensin, että $N_\lambda = N_\rho$.

Olkoon $l \in N_\lambda$ ja $r \in N_\rho$. Tällöin täytyy osoittaa, että $l \in N_\rho$ ja $r \in N_\lambda$. Koska $l \in N_\lambda$ ja N_λ on ryhmä, niin myös käänteisalkio $l^{-1} \in N_\lambda$ ja $l^{-1}(b^{-1}a^{-1}) = (l^{-1}b^{-1})a^{-1}$ kaikilla $a, b \in G$. Ottamalla puolittain käänteisalkio saadaan

$$\begin{aligned} & l^{-1}(b^{-1}a^{-1}) = (l^{-1}b^{-1})a^{-1} \\ \text{eli} \quad & (l^{-1}(b^{-1}a^{-1}))^{-1} = ((l^{-1}b^{-1})a^{-1})^{-1} \\ \text{eli} \quad & (b^{-1}a^{-1})^{-1}l = a(l^{-1}b^{-1})^{-1} \\ \text{eli} \quad & (ab)l = a(bl). \end{aligned}$$

Näin ollen $l \in N_\rho$.

Osoitetaan seuraavaksi, että kun $r \in N_\rho$, niin saadaan $r \in N_\lambda$. Olkoon $r \in N_\rho$, jolloin myös $r^{-1} \in N_\rho$ ja $a^{-1}(b^{-1}r^{-1}) = (a^{-1}b^{-1})r^{-1}$ kaikilla $a, b \in G$. Nyt

$$\begin{aligned} & a^{-1}(b^{-1}r^{-1}) = (a^{-1}b^{-1})r^{-1} \\ \text{eli} \quad & (a^{-1}(b^{-1}r^{-1}))^{-1} = ((a^{-1}b^{-1})r^{-1})^{-1} \\ \text{eli} \quad & (b^{-1}r^{-1})^{-1}a = r(a^{-1}b^{-1})^{-1} \\ \text{eli} \quad & (rb)a = r(ba). \end{aligned}$$

Näin ollen $r \in N_\lambda$.

On siis osoitettu, että kun $l \in N_\lambda$ ja $r \in N_\rho$, niin $l \in N_\rho$ ja $r \in N_\lambda$ eli $N_\rho = N_\lambda$.

Osoitetaan seuraavaksi, että $N_\lambda = N_\mu$. Olkoon $l \in N_\lambda$ ja $m \in N_\mu$. Tällöin täytyy osoittaa, että $l \in N_\mu$ ja $m \in N_\lambda$ kaikilla $x \in G$.

Koska G on I.P. -luuppi, niin $a^{-1}(ax) = x$ eli $L_{a^{-1}}L_a(x) = x$ kaikilla $a, x \in G$. Toisaalta $L_a^{-1}L_a(x) = x$ kaikilla $a, x \in G$. Siis $L_{a^{-1}}L_a(x) = L_a^{-1}L_a(x)$ kaikilla $x \in G$. Tällöin $L_{a^{-1}}(y) = L_a^{-1}(y)$ kaikilla $y \in G$ eli $L_{a^{-1}} = L_a^{-1}$ kaikilla $a \in G$.

Olkoon $m \in N_\mu$, jolloin myös $m^{-1} \in N_\mu$. Tällöin kaikilla $x, y \in G$ pätee:

$$\begin{aligned} & (x^{-1}m^{-1})y = x^{-1}(m^{-1}y) \\ \text{eli} \quad & L_{x^{-1}m^{-1}}(y) = L_{x^{-1}}L_{m^{-1}}(y) \\ \text{eli} \quad & L^{-1}_{x^{-1}m^{-1}}(y) = L^{-1}_{m^{-1}}L^{-1}_{x^{-1}}(y) \\ \text{eli} \quad & L_{(x^{-1}m^{-1})^{-1}}(y) = L_{(m^{-1})^{-1}}L_{(x^{-1})^{-1}}(y) \\ \text{eli} \quad & L_{mx}(y) = L_mL_x(y) \\ \text{eli} \quad & (mx)y = m(xy). \end{aligned}$$

Näin ollen $m \in N_\lambda$.

Osoitetaan seuraavaksi, että kun $l \in N_\lambda$, niin $l \in N_\mu$. Olkoon siis $l \in N_\lambda$, jolloin myös $l^{-1} \in N_\lambda$. Tällöin kaikille $x, y \in G$ pätee:

$$\begin{aligned} & (l^{-1}x^{-1})y = l^{-1}(x^{-1}y) \\ \text{eli} \quad & L_{l^{-1}x^{-1}}(y) = L_{l^{-1}}L_{x^{-1}}(y) \\ \text{eli} \quad & L_{(xl)^{-1}}(y) = L_{l^{-1}}L_{x^{-1}}(y) \\ \text{eli} \quad & L^{-1}_{xl}(y) = L^{-1}_l L^{-1}_x(y) \\ \text{eli} \quad & L_{xl}(y) = L_xL_l(y) \\ \text{eli} \quad & (xl)y = x(ly). \end{aligned}$$

Näin ollen $l \in N_\mu$.

On siis osoitettu, että kun $l \in N_\lambda$ ja $m \in N_\mu$, niin $l \in N_\mu$ ja $m \in N_\lambda$ eli $N_\mu = N_\lambda$.

Koska $N_\rho = N_\lambda$ ja $N_\mu = N_\lambda$, niin $N_\mu = N_\lambda = N_\rho = N$ eli väite on todistettu. □

Määritelmä 5.9. Olkoon G luuppi ja e luupin G neutraalialkio. Luuppia G kutsutaan *ristikkäisen käänteisominaisuuden toteuttavaksi luupiksi* (cross inverse property loop), jos alkioille $x, y \in G$ pätee

$$(xy)x^\rho = y.$$

Tällaista luuppia kutsutaan lyhyemmin *C.I.P. -luupiksi.*

Lause 5.10. *Olkoon G C.I.P. -luuppi. Tällöin kaikilla $x, y \in G$*

$$(xy)^\rho = x^\rho y^\rho$$

ja

$$x(yx^\rho) = y.$$

Todistus. Osoitetaan, että $(xy)^\rho = x^\rho y^\rho$. Koska G on C.I.P. -luuppi, niin $(xy)x^\rho = y$ kaikilla $x, y \in G$. Operoidaan yhtälöä oikealta puolelta alkiolla $(xy)^\rho$, jolloin yhtälö saadaan muotoon $((xy)x^\rho)(xy)^\rho = y(xy)^\rho$. Koska G on C.I.P. -luuppi, niin $((xy)x^\rho)(xy)^\rho = x^\rho$. Sijoittamalla tämä yhtälöön $((xy)x^\rho)(xy)^\rho = y(xy)^\rho$ saadaan $x^\rho = y(xy)^\rho$. Operoidaan yhtälöä oikealta puolelta alkiolla y^ρ, jolloin $x^\rho y^\rho = (y(xy)^\rho)y^\rho$. Näin ollen $x^\rho y^\rho = (xy)^\rho$ kaikilla $x, y \in G$.

Osoitetaan sitten, että kun G on C.I.P. -luuppi, niin $x(yx^\rho) = y$ kaikilla $x, y \in G$. Olkoon $x, y \in G$. Tällöin $(xy)x^\rho = y$ eli $R_{x^\rho}L_x(y) = y$. Toisaalta $L_x^{-1}L_x(y) = y$ kaikilla $x, y \in G$. Siis $R_{x^\rho}L_x(y) = L_x^{-1}L_x(y)$, josta saadaan $R_{x^\rho} = L_x^{-1}$.

Nyt $x(yx^\rho) = L_xR_{x^\rho}(y) = L_xL_x^{-1}(y) = y$ kaikilla $y \in G$ eli väite on todistettu.

□

Määritelmä 5.11. Olkoon G luuppi ja e luupin G neutraalialkio. Jos luuppi G toteuttaa yhtälön $y(xy)^\rho = x^\rho$ kaikilla $x, y \in G$, niin luupilla G on *heikko käänteisominaisuus* (weak inverse property loop). Tällaista luuppia kutsutaan lyhyemmin *W.I.P. -luupiksi.*

Lause 5.12. *Jokaisella C.I.P -luupilla on heikko käänteisominaisuus.*

Todistus. Täytyy siis osoittaa, että kun luupin G alkiot x, y toteuttavat yhtälön $(xy)x^\rho = y$, niin ne toteuttavat myös yhtälön $y(xy)^\rho = x^\rho$.

Oletetaan, että G on C.I.P. -luuppi eli $(xy)x^\rho = y$, kun $x, y \in G$. Tällöin lauseen 5.10 nojalla $x(yx^\rho) = y$ ja $(xy)^\rho = x^\rho y^\rho$. Täten $y(xy)^\rho = y(x^\rho y^\rho) = x^\rho$. Eli C.I.P. -luuppi on myös W.I.P. -luuppi. □

Lause 5.13. *Olkoon G luuppi ja e luupin G neutraalialkio. Tällöin seuraavat väitteet ovat yhtäpitäviä.*

1. *G on W.I.P. -luuppi.*
2. *Jos $(xy)z = e$, niin $x(yz) = e$ kaikilla $x, y \in G$.*
3. *Luuppi G toteuttaa yhtälön $(xy)^\lambda x = y^\lambda$ aina, kun $x, y \in G$.*

Todistus. Osoitetaan ensin, että väitteestä 1 seuraa väite 2. Oletetaan siis, että luuppi G on W.I.P. -luuppi eli $y(xy)^\rho = x^\rho$ kaikilla $x, y \in G$. Olkoon x, y ja z sellaisia luupin G alkioita, että ne toteuttavat yhtälön $(xy)z = e$. Tästä seuraa, että $z = (xy)^\rho$. Tällöin $x(yz) = x(y(xy)^\rho) = xx^\rho = e$. Siis $x(yz) = e$, eli väite 2 pätee.

Osoitetaan seuraavaksi, että väitteestä 2 seuraa väite 3. Oletetaan, että väite 2 on voimassa eli kun $(xy)z = e$, niin $x(yz) = e$ kaikilla $x, y, z \in G$. Tällöin $x = (yz)^\lambda$ ja $xy = z^\lambda$. Nyt $(yz)^\lambda y = xy = z^\lambda$. Näin ollen on osoitettu, että kun väite 2 on voimassa, niin $(yz)^\lambda y = z^\lambda$ aina, kun $y, z \in G$.

Osoitetaan vielä, että kun väite 3 on voimassa, niin myös väite 1 pätee. Oletetaan siis, että $(yz)^\lambda y = z^\lambda$ aina, kun $y, z \in G$. Operoidaan yhtälöä alkiolla z oikealta puolelta, jolloin saadaan $((yz)^\lambda y)z = z^\lambda z = e$. Koska $((yz)^\lambda y)z = e$, niin $z = ((yz)^\lambda y)^\rho$. Merkitään $(yz)^\lambda = x$, jolloin $z = (xy)^\rho$. Operoidaan yhtälöä alkiolla y vasemmalta puolelta, jolloin saadaan $yz = y(xy)^\rho$.

Toisaalta $(yz)^\lambda = x$. Operoidaan yhtälöä alkiolla (yz) oikealta puolelta, jolloin $(yz)^\lambda(yz) = x(yz)$. Siis $x(yz) = e$, jolloin täytyy olla, että $yz = x^\rho$.

Ollaan siis saatu, että $y(xy)^\rho = yz = x^\rho$ eli $y(xy)^\rho = x^\rho$, jolloin määritelmän 5.11 nojalla G on W.I.P. -luuppi eli lauseen 5.13 ensimmäinen väite toteutuu.

On siis osoitettu, että kaikki kolme väitettä ovat yhtäpitäviä.

□

6 Homomorfismi

Tässä luvussa määritellään kuvauksen $f : G \to Q$, missä G ja Q ovat luuppeja, homomorfisuus ja isomorfisuus. Lisäksi määritellään kuvauksen $f : G \to G$ automorfisuus.

Näiden lisäksi tutkitaan homomorfismin f ydintä ja kuvaa sekä osoitetaan, että myös ne ovat luuppeja.

Määritelmä 6.1. Olkoot G ja Q luuppeja. Kuvaus $f : G \to Q$ on *homomorfismi*, jos

$$f(x)f(y) = f(xy)$$

kaikilla $x, y \in G$.

Määritelmä 6.2. Olkoot G ja Q luuppeja sekä $f : G \to Q$ homomorfismi. Joukkoa $Im(f) = f(G) = \{f(x) \mid x \in G\}$ sanotaan *homomorfismin f kuvaksi* (the image of f).

Luupin G osajoukkoa $Ker(f) = \{x \in G \mid f(x) = f(e)\}$, kutsutaan *homomorfismin f ytimeksi* (the kernel of f).

Lause 6.3. *Olkoot G ja Q luuppeja sekä kuvaus $f : G \to Q$ homomorfismi. Tällöin homomorfismin f kuva $Im(f)$ on luuppi.*

Todistus. Koska f on homomorfismi, niin $f(x)f(y) = f(xy)$ kaikilla $x, y \in G$. Näin ollen kun alkiot $f(x), f(y) \in Im(f)$, niin myös kuvausten operaatio $f(x)f(y) \in Im(f)$, sillä $f(xy) \in Im(f)$.

Koska G on luuppi, niin jos yhtälössä $xy = z$ mitkä tahansa kaksi muuttujaa ovat joukon G alkioita, niin silloin myös kolmas muuttuja on joukon G yksikäsitteinen alkio.

Oletetaan, että $f(x)u = f(z)$, missä $f(x)$ ja $f(z)$ ovat joukon $Im(f)$ alkioita. Tällöin kuvaukset $f(x)$ ja $f(y)$ ovat myös luupin Q alkioita. Sen vuoksi yhtälöllä $f(x)u = f(z)$ on olemassa yksikäsitteinen ratkaisu $u \in Q$. Tarkastellaan nyt yhtälöä $xy = z$, missä x ja z ovat luupin G alkiota. Luupin määritelmän nojalla myös y on luupin G yksikäsitteinen alkio. Nyt $f(x)f(y) = f(xy) = f(z)$ eli alkion $f(y)$ täytyy olla luupin Q yksikäsitteinen alkio, jolloin $u = f(y)$. Lisäksi koska $y \in G$, niin $f(y)$ on joukon $Im(f)$ alkio.

Oletetaan seuraavaksi, että $uf(x) = f(z)$, missä $f(x)$ ja $f(z)$ ovat joukon $Im(f)$ alkioita. Edelleen $f(x)$ ja $f(z)$ ovat luupin Q alkioita, jolloin u on luupin määritelmän nojalla luupin Q yksikäsitteinen alkio. Olkoon $yx = z$, missä $x, z \in G$. Tällöin myös y on luupin G yksikäsitteinen alkio. Nyt $f(y)f(x) = f(yx) = f(z)$, jolloin alkio $f(y)$ on luupin Q yksikäsitteinen alkio eli $u = f(y)$. Lisäksi koska y on luupin G alkio, niin $f(y) \in Im(f)$.

Oletetaan vielä, että $f(x)f(z) = u$, missä $f(x)$ ja $f(z)$ ovat joukon $Im(f)$ alkioita. Koska $f(x)$ ja $f(z)$ ovat myös luupin Q alkioita, niin u on luupin Q yksikäsitteinen alkio. Tutkitaan yhtälöä $xz = y$, missä $x, z \in G$. Luupin määritelmään nojalla myös y on luupin G yksikäsitteinen alkio. Tällöin $f(x)f(z) = f(xz) = f(y)$, joten $f(y)$ on luupin Q yksikäsitteinen alkio. Siis $u = f(y)$. Koska $y \in G$, niin $f(y) \in Im(f)$.

Lisäksi $f(e)f(x) = f(ex) = f(x)$ ja $f(x)f(e) = f(xe) = f(x)$, missä e on luupin G neutraalialkio ja $x \in G$. Näin ollen $f(e)$ on joukon $Im(f)$ neutraalialkio.

Lauseen 2.2 nojalla homomorfismin f kuva $Im(f)$ on luuppi.

□

Lause 6.4. *Olkoot G ja Q luuppeja ja kuvaus $f : G \to Q$ homomorfismi. Tällöin homomorfismin f ydin $Ker(f)$ on luupin G aliluuppi.*

Todistus. Olkoot x ja y ytimen $Ker(f)$ alkiota, jolloin $f(x) = f(y) = f(e)$, missä e on luupin G neutraalialkio. Koska kuvaus f on homomorfismi, niin $f(xy) = f(x)f(y) = f(e)f(e) = f(e)$. Täten xy on myös homomorfismin f ytimen $Ker(f)$ alkio.

Koska G on luuppi, niin jos yhtälössä $xy = z$ mitkä tahansa kaksi muuttujaa ovat joukon G alkioita, niin silloin myös kolmas muuttuja on joukon G yksikäsitteinen alkio. Osoitetaan, että sama pätee myös ytimen $Ker(f)$ alkioille.

Olkoot $xy = z$ ja $x, y \in Ker(f)$. Tällöin myös $z \in Ker(f)$, sillä aiemman mukaan $f(z) = f(xy) = f(e)$.

Olkoot seuraavaksi $x, z \in Ker(f)$ ja $xy = z$. Tällöin $f(xy) = f(x)f(y) = f(e)f(y) = f(y) = f(z) = f(e)$, joten myös $y \in Ker(f)$.

Vastaavasti, jos $y, z \in Ker(f)$ ja $xy = z$, niin $f(xy) = f(x)f(y) = f(x)f(e) = f(x) = f(z) = f(e)$, joten $x \in Ker(f)$.

Lisäksi neutraalialkio e on homomorfismin f ytimen $Ker(f)$ alkio, sillä $f(e) = f(e)$.

Lauseen 2.2 nojalla homomorfismin f ydin $Ker(f)$ on luuppi. □

Määritelmä 6.5. Olkoon G ja Q luuppeja. Luuppien G ja Q sanotaan olevan *isomorfisia* (isomorphic), jos on olemassa bijektiivinen kuvaus $f : G \to Q$ siten, että $f(xy) = f(x)f(y)$ kaikille $x, y \in G$. Tällöin sanotaan, että kuvaus f on *isomorfismi* (isomorphism).

Toisin sanoen isomorfismi on bijektiivinen homomorfismi.

Määritelmä 6.6. Olkoon G luuppi. Bijektiivinen kuvaus $f : G \to G$ on *automorfismi* (automorphism), jos $f(a)f(b) = f(ab)$ kaikilla $a, b \in G$.

Toisin sanoen automorfismi on isomorfismi $f : G \to G$.

Määritelmä 6.7. Olkoon G ryhmä ja x ryhmän G kiinnitetty alkio. Tällöin kuvaus $f : G \to G$ on *sisäinen automorfismi* (inner automorphism), jos kaikilla $a \in G$ pätee:

$$f(a) = xax^{-1}.$$

7 Kertolaskuryhmät

Tässä luvussa esitellään luupin G kertolaskuryhmä $M(G)$, joka määritellään siirtokuvausten L_a ja R_a avulla. Lisäksi määritellään luupin G sisäinen kertolaskuryhmä $I(G)$.

Nämä ryhmät ovat tärkeitä luuppien tutkimisessa, sillä ne toimivat linkkinä luuppien ja ryhmien välillä.

Olkoot G luuppi ja $a \in G$. Siirtokuvaukset $L_a : G \to G$, $L_a(x) = ax$, ja $R_a : G \to G$, $R_a(x) = xa$, ovat joukon G permutaatioita.

Lauseen 1.26 nojalla siirtokuvaukset R_a ja L_a ovat kaikkien joukon G permutaatioiden muodostaman symmetrisen ryhmän S_G alkioita.

Määritelmä 7.1. Olkoot G luuppi ja $x \in G$. Luupin G permutaatioiden L_x ja L_x^{-1} muodostamaa ryhmää $M_\lambda(G)$ kutsutaan *luupin G vasemmaksi kertolaskuryhmäksi* (left multiplication group).

Vastaavasti luupin G permutaatioiden R_x ja R_x^{-1} muodostamaa ryhmää $M_\rho(G)$ kutsutaan *luupin G oikeaksi kertolaskuryhmäksi* (right multiplication group).

Lisäksi luupin G permutaatioiden R_x, L_x, R_x^{-1} ja L_x^{-1} muodostamaa ryhmää $M(G)$ kutsutaan *luupin G kertolaskuryhmäksi* (multiplication group).

Määritelmä 7.2. Olkoot G luuppi ja $M(G)$ sen kertolaskuryhmä. Permutaatioiden $R_{x,y} = R_{xy}^{-1} R_y R_x$ ja $M_{x,y} = R_{xy}^{-1} L_x R_y$ muodostamaa kertolaskuryhmän $M(G)$ aliryhmää sanotaan *sisäiseksi kertolaskuryhmäksi* (inner mapping group) ja merkitään $I(G)$.

Lause 7.3. *Olkoot G luuppi ja $I(G)$ sen sisäinen kertolaskuryhmä. Tällöin jokaiselle ryhmän $I(G)$ alkiolle T pätee $T(e) = e$, missä e on luupin G neutraalialkio.*

Todistus. Olkoon $x, y \in G$. Tällöin käyttämällä määritelmiä 2.10 ja 2.13 saadaan $R_{x,y}(e) = R_{xy}^{-1} R_y R_x(e) = R_{xy}^{-1}(xy) = (xy)/(xy) = e$ ja $R_{x,y}^{-1}(e) = R_x^{-1} R_y^{-1} R_{xy}(e) = R_x^{-1} R_y^{-1}(xy) = R_x^{-1}((xy)/y) = R_x^{-1}(x) = x/x = e$.

Samoin $M_{x,y}(e) = R_{xy}^{-1} L_x R_y(e) = R_{xy}^{-1}(xy) = (xy)/(xy) = e$ ja $M_{x,y}^{-1}(e) = R_y^{-1} L_x^{-1} R_{xy}(e) = R_y^{-1} L_x^{-1}(xy) = R_y^{-1}(x\backslash(xy)) = R_y^{-1}(y) = y/y = e$.

Koska permutaatiot $R_{x,y}$ ja $M_{x,y}$ muodostavat koko sisäisen kertolaskuryhmän $I(G)$, niin jokaiselle $T \in I(G)$ pätee $T(e) = e$. □

Lemma 7.4. *Olkoot G luuppi ja $x, y \in G$. Tällöin seuraavat kohdat pätevät.*

1. $R_y R_x = R_{xy} R_{x,y}$,
2. $L_y R_x = R_{yx} M_{y,x}$,

3. $R_y^{-1}R_x = R_pR_{p,y}^{-1}$, *missä* $p = R_y^{-1}(x)$,

4. $L_y^{-1}R_x = R_qM_{y,q}^{-1}$, *missä* $q = L_y^{-1}(x)$,

5. $L_y = R_yM_{y,e}$,

6. $R_y^{-1} = R_uR_{u,y}^{-1}$, *missä* $u = R_y^{-1}(e)$,

7. $L_y^{-1} = R_vM_{y,v}^{-1}$, *missä* $v = L_y^{-1}(e)$.

Todistus. Todistetaan ensin kohta 1. Määritelmän mukaan $R_{x,y} = R_{xy}^{-1}R_yR_x$. Operoidaan yhtälöä vasemmalta puolelta permutaatiolla R_{xy}, jolloin saadaan $R_yR_x = R_{xy}R_{x,y}$.

Kohta 2 todistetaan samoin kuin kohta 1. Määritelmän mukaan $M_{y,x} = R_{yx}^{-1}L_yR_x$. Operoidaan yhtälöä puolittain vasemmalta puolelta permutaatiolla R_{yx}, jolloin $L_yR_x = R_{yx}M_{y,x}$.

Osoitetaan lemman väite numero kolme. Olkoon $p = R_y^{-1}(x)$ eli $x/y = p$, josta seuraa, että $py = x$. Tällöin $R_{p,y} = R_{py}^{-1}R_yR_p = R_x^{-1}R_yR_p$. Otetaan yhtälöstä käänteisalkio puolittain, jolloin saadaan $R_{p,y}^{-1} = R_p^{-1}R_y^{-1}R_x$. Operoidaan saatua yhtälöä puolittain vasemmalta alkiolla R_p. Tällöin $R_pR_{p,y}^{-1} = R_y^{-1}R_x$, missä $p = R_y^{-1}(x)$ ja $x, y \in G$.

Osoitetaan seuraavaksi kohta 4. Olkoon $q = L_y^{-1}(x)$ eli $y\backslash x = q$, josta saadaan, että $yq = x$. Tällöin $M_{y,q} = R_{yq}^{-1}L_yR_q = R_x^{-1}L_yR_q$. Otetaan yhtälöstä puolittain käänteisalkio, jolloin saadaan $M_{y,q}^{-1} = R_q^{-1}L_y^{-1}R_x$. Operoidaan tätä yhtälöä puolittain vasemmalta permutaatiolla R_q, jolloin $R_qM_{y,q}^{-1} = L_y^{-1}R_x$, kun $q = L_y^{-1}(x)$ ja $x, y \in G$.

Osoitetaan, että kohdan 5 väite pätee. Olkoon $x = e$. Tällöin kohdan 2 nojalla $L_yR_e = R_{ye}M_{y,e}$ eli $L_y = R_yM_{y,e}$ kaikilla $y \in G$.

Todistetaan väite 6. Olkoon edelleen $x = e$. Kohdan 3 nojalla $R_y^{-1}R_e = R_uR_{u,y}^{-1}$, missä $u = R_y^{-1}(e)$. Eli $R_y^{-1} = R_uR_{u,y}^{-1}$, missä $u = R_y^{-1}(e)$ ja $y \in G$.

Osoitetaan vielä kohta 7. Olkoon $x = e$. Tällöin kohdan 4 perusteella $L_y^{-1}R_e = R_vM_{y,v}^{-1}$, missä $v = L_y^{-1}(e)$. Joten $L_y^{-1} = R_vM_{y,v}^{-1}$, missä $v = L_y^{-1}(e)$ ja $y \in G$. □

Lause 7.5. *Olkoon G luuppi. Jos $X \in M(G)$, niin se voidaan esittää yksikäsitteisessä muodossa $X = R_xT$, missä $T \in I(G)$ ja $x = X(e)$.*

Todistus. Osoitetaan ensin yksikäsitteisyys. Jos $X = R_xT$, $T \in I(G)$, niin $X(e) = R_xT(e) = R_x(e) = ex = x$, joten alkio x on yksikäsitteinen, jolloin myös kuvaus R_x on yksikäsitteinen. Nyt $T = R_x^{-1}X$, joten myös kuvaus T on yksikäsitteinen.

Osoitetaan seuraavaksi, että jokaisella $X \in M(G)$ on olemassa ainakin yksi esitys, joka on muotoa $X = R_xT$, missä $T \in I(G)$.

Kertolaskuryhmän $M(G)$ määritelmän mukaan jokaisella $X \in M(G)$ on olemassa ainakin yksi esitys, joka on muotoa $X = X_r...X_2X_1$, missä $r \geq 1$ ja jokainen X_i on jokin alkioista R_y, L_y, R_y^{-1} tai L_y^{-1}, missä y on luupin G mielivaltainen alkio.

Osoitetaan induktiolla luvun r suhteen, että $X = R_xT$, missä $T \in I(G)$.

Jos $r = 1$, niin lemman 7.4 kohtien 5,6 ja 7 nojalla $X = X_1$ on haluttua muotoa.

Oletetaan, että väite on tosi, kun operaatiossa $X_r...X_2X_1$ on vähemmän kuin r alkiota ja $r > 1$. Tällöin $X = X_rR_xV$, missä $V \in I(G)$, $x \in G$ ja X_r on jokin permutaatioista R_y, L_y, R_y^{-1} ja L_y^{-1}.

Lemman 7.4 kohtien 1,2,3 ja 4 perusteella nähdään, että $X_rR_x = R_zW$, $W \in I(G)$ ja $z \in G$. Täten $X = R_zWV = R_zT$, $T \in I(G)$. Näin ollen lause 7.5 on todistettu.

□

Lause 7.6. *Olkoon G luuppi ja $M(G)$ sen kertolaskuryhmä. Kertolaskuryhmän $M(G)$ alkio T on sisäisen kertolaskuryhmän $I(G)$ alkio, jos ja vain jos $T(e) = e$, missä e on luupin G neutraalialkio.*

Todistus. Osoitetaan ensin, että jos $T \in I(G)$, niin $T(e) = e$, missä e on luupin G neutraalialkio. Oletetaan, että $T \in I(G)$. Tällöin lauseen 7.3 nojalla $T(e) = e$.

Osoitetaan seuraavaksi, että jos $T(e) = e$, niin $T \in I(G)$. Olkoon $X(e) = e$, missä X on jokin kertolaskuryhmän $M(G)$ alkio. Lauseen 7.5 nojalla $X(e) = R_xT(e) = R_x(e) = ex = x$. Oletuksen $X(e) = e$ nojalla täytyy olla, että $x = e$, jolloin $X = R_eT = T$. Näin ollen permutaatio X on sisäisen kertolaskuryhmän $I(G)$ alkio. □

Lause 7.7. *Olkoon G luuppi ja $M(G)$ sen kertolaskuryhmä. Kaikilla alkioilla $X \in M(G)$ on olemassa yksikäsitteinen esitys, joka on muotoa $X = L_xV$, missä $V \in I(G)$ ja $x = X(e)$.*

Todistus. Olkoon $X(e) = x$ ja merkitään $V = L_x^{-1}X$. Tällöin saadaan $V(e) = L_x^{-1}X(e) = L_x^{-1}(x) = e$, jolloin $V \in I(G)$. Kun operoidaan yhtälöä $V = L_x^{-1}X$ puolittain vasemmalta puolelta permutaatiolla L_x, niin saadaan $X = L_xV$ ja väite on todistettu. □

Lause 7.8. *Olkoot G luuppi, $a \in G$, $M(G)$ luupin G kertolaskuryhmä ja $X \in M(G)$. Tällöin $X(a) = T(a)x = xV(a)$, missä T ja V ovat sisäisen kertolaskuryhmän alkioita ja $x = X(e)$.*

Todistus. Olkoon $a \in G$. Lauseen 7.5 nojalla $X(a) = R_xT(a) = T(a)x$, missä $T \in I(G)$. Vastaavasti lauseen 7.7 nojalla $X(a) = L_xV(a) = xV(a)$, $V \in I(G)$. Näin ollen $X(a) = T(a)x = xV(a)$ eli väite on todistettu. □

Lause 7.9. *Olkoon G luuppi ja $a \in G$. Jos $T(a) = a$ kaikilla $T \in I(G)$, niin*

$$Y(ax) = aY(x)$$

aina, kun $x \in G$ ja $Y \in M(G)$.

Todistus. Olkoon $x, y \in G$ ja a sellainen luupin G alkio, että $T(a) = a$ kaikilla $T \in I(G)$. Nyt $R_y(ax) = (ax)y = R_y R_x(a)$. Koska permutaatiot R_y ja R_x ovat kertolaskuryhmän $M(G)$ alkioita, niin $R_y R_x \in M(G)$. Lauseen 7.5 mukaan alkio $X \in M(G)$ voidaan esittää yksikäsitteisessä muodossa $X = R_x T$, missä $T \in I(G)$ ja $x = X(e)$. Nyt $R_y R_x(e) = R_y(ex) = (ex)y = xy$. Tämän nojalla $R_y(ax) = R_y R_x(a) = R_{xy}T(a) = a(xy) = aR_y(x)$. Tämän nojalla $R_y(aR_y^{-1}(x)) = aR_y R_y^{-1}(x) = ax$. Kun operoidaan saatua yhtälöä vasemmalta permutaatiolla R_y^{-1} saadaan $aR_y^{-1}(x) = R_y^{-1}(ax)$, missä $x, y, a \in G$

Vastaavasti $L_y(ax) = y(ax) = L_y R_x(a)$ kaikilla $x, y \in G$. Nyt $L_y R_x$ on kertolaskuryhmän $M(G)$ alkio, koska L_y ja R_x ovat kertolaskuryhmän $M(G)$ alkioita. Lauseen 7.5 mukaan permutaatio $X \in M(G)$ voidaan esittää yksikäsitteisessä muodossa $X = R_x(T)$, missä $T \in I(G)$ ja $x = X(e)$. Nyt $L_y R_x(e) = y(ex) = yx$. Näin ollen $L_y(ax) = L_y R_x(a) = R_{yx}T(a) = a(yx) = aL_y(x)$. Tämän nojalla $L_y(aL_y^{-1}(x)) = aL_y L_y^{-1}(x) = ax$, josta saadaan, että $L_y^{-1}(ax) = aL_y^{-1}(x)$.

On siis saatu, että $R_y(ax) = aR_y(x)$, $R_y^{-1}(ax) = aR_y^{-1}(x)$, $L_y(ax) = aL_y(x)$ ja $L_y^{-1}(ax) = aL_y^{-1}(x)$ aina, kun $x, y \in G$ ja a on sellainen alkio, että $T(a) = a$. Koska permutaatiot R_y, L_y, R_y^{-1} ja L_y^{-1} muodostavat koko kertolaskuryhmän $M(G)$, niin aina kun $Y \in M(G)$, niin $Y(ax) = aY(x)$. □

Lause 7.10. *Olkoon G luuppi. Luupin keskus Z sisältää sellaiset alkiot $a \in G$, että $T(a) = a$ kaikilla $T \in I(G)$.*

Todistus. Osoitetaan ensin, että jos $a \in Z$, niin $T(a) = a$ kaikilla $T \in I(G)$. Olkoon siis $a \in Z$. Tällöin

$$R_{x,y}(a) = R_{xy}^{-1} R_y R_x(a) = R_{xy}^{-1}((ax)y) = R_{xy}^{-1}(a(xy)) = R_{xy}^{-1} R_{xy}(a) = a.$$

Samoin

$$M_{x,y}(a) = R_{xy}^{-1} L_x R_y(a) = R_{xy}^{-1}(x(ay)) = R_{xy}^{-1}(a(xy)) = R_{xy}^{-1} R_{xy}(a) = a.$$

Koska permutaatiot $R_{x,y}$ ja $M_{x,y}$ muodostavat sisäisen kertolaskuryhmän $I(G)$, niin $T(a) = a$ kaikilla $a \in Z$ ja $T \in I(G)$.

Osoitetaan seuraavaksi, että kun $T(a) = a$ kaikilla $T \in I(G)$, niin $a \in Z$. Kaikille luupin G alkioille x pätee, että $xa = L_x(a) = R_{xe}T(a) = R_x T(a) =$

$R_x(a) = ax$. Olkoon x ja y luupin G alkioita. Lauseen 7.9 nojalla $R_y(ax) = aR_y(x)$ eli $(ax)y = a(xy)$. Samoin lauseen 7.9 nojalla $L_y(ax) = aL_y(x)$ eli $y(ax) = a(yx)$. Käyttämällä sitä tietoa, että alkio a on kommutatiivinen ja yhtälöä $(ax)y = a(xy)$ saadaan $y(ax) = a(yx) = (ay)x = (ya)x$. Käyttämällä yhtälöitä $(ax)y = a(xy)$ ja $y(ax) = (ya)x$ sekä alkion a kommutatiivisuutta saadaan $(xy)a = a(xy) = (ax)y = (xa)y = x(ay) = x(ya)$. On siis saatu, että $(ax)y = a(xy)$, $(xa)y = x(ay)$ ja $(xy)a = x(ya)$. Näin ollen alkio a on luupin G keskuksen alkio.

□

Lause 7.11. *Olkoon luuppi G ryhmä. Tällöin ryhmän G sisäinen kertolaskuryhmä $I(G)$ on ryhmä, joka muodostuu sisäisistä automorfismeista.*

Todistus. Sisäinen kertolaskuryhmä on ryhmä, joka muodostuu permutaatioista $R_{x,y}$ ja $M_{x,y}$, missä $x, y \in G$. Koska G on ryhmä, niin $R_x^{-1} = R_{x^{-1}}$ ja $L_x^{-1} = L_{x^{-1}}$. Tällöin

$$R_{x,y}(a) = R_{xy}^{-1} R_y R_x(a) = R_{xy}^{-1}((ax)y) = R_{xy}^{-1}(a(xy)) = R_{xy}^{-1} R_{xy}(a) = a$$

ja

$$\begin{aligned} M_{x,y}(a) &= R_{xy}^{-1} L_x R_y(a) = R_{(xy)^{-1}}(x(ay)) = (x(ay))(xy)^{-1} \\ &= x(ay)y^{-1}x^{-1} = xax^{-1} \end{aligned}$$

kaikilla $a \in G$. Siis permutaatio $R_{x,y}$ on identiteettikuvaus ja permutaatio $M_{x,y}$ on sisäinen automorfismi.

Tutkitaan sitten sisäistä automorfismia $f(a) = xax^{-1}$, missä $x, a \in G$. Nyt sisäiselle automorfismille f pätee

$$\begin{aligned} f(a) &= xax^{-1} = xa(yy^{-1})x^{-1} = x(ay)y^{-1}x^{-1} = x(ay)(xy)^{-1} \\ &= R_{(xy)^{-1}}(x(ay)) = R_{(xy)^{-1}} L_x(ay) = R_{xy}^{-1} L_x R_y(a) = M_{x,y}(a). \end{aligned}$$

Eli jokainen sisäinen automorfismi kuuluu sisäiseen kertolaskuryhmään $I(G)$.

Näin ollen kun G on ryhmä, niin sisäinen kertolaskuryhmä $I(G)$ on ryhmä, joka muodostuu sisäisistä automorfismeista.

□

Lause 7.12. *Luuppi G on kommutatiivinen ryhmä, jos ja vain jos sen sisäinen kertolaskuryhmä $I(G)$ sisältää vain identiteettikuvauksen I.*

Todistus. Oletetaan ensin, että luuppi G on kommutatiivinen ryhmä. Tällöin lauseen 7.11 nojalla $I(G)$ on ryhmä, joka koostuu sisäisistä automorfismeista. Koska ryhmä G on kommutatiivinen, niin sisäiselle automorfismille $f : G \to G$ pätee $f(a) = xax^{-1} = xx^{-1}a = a$ kaikilla $a \in G$. Näin ollen kaikki sisäiset

automorfismit ovat identiteettikuvauksia eli sisäinen kertolaskuryhmä $I(G)$ sisältää ainoastaan identiteettikuvauksen.

Oletetaan seuraavaksi, että sisäinen kertolaskuryhmä $I(G)$ sisältää vain identiteettikuvauksen. Pitää siis osoittaa, että tällöin luuppi G on kommutatiivinen ryhmä. Koska identiteettikuvaus muodostaa koko sisäisen kertolaskuryhmän $I(G)$, niin $T(a) = a$ kaikilla luupin G alkioilla a ja kaikilla sisäisen kertolaskuryhmän $I(G)$ alkioilla T. Lauseen 7.10 nojalla $G = Z$. Koska lauseen 4.7 nojalla keskus Z on kommutatiivinen ryhmä, niin myös luuppi G on kommutatiivinen ryhmä eli väite on todistettu. □

8 Esimerkkejä luupeista

Tässä luvussa esitellään muutama havainnollistava esimerkki luupeista. Esimerkeissä käsitellään lähinnä luvuissa 2 ja 5 esiteltyä teoriaa.

Esimerkki 8.1. Olkoon $G = \{1, 2, 3, 4, 5\}$ ja $(*)$ sellainen joukon G operaatio, että

$*$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	2	3	1

.

Osoitetaan, että G on luuppi näyttämällä, että lauseen 2.2 ehdot toteutuvat.

Operaatio $(*)$ on binäärinen operaatio joukossa G, sillä $a * b \in G$ aina, kun $a, b \in G$.

Tarkastellaan sitten yhtälöä $a * b = c$. Jos kaksi yhtälön muuttujaa ovat joukon G alkioita, niin taulukosta nähdään, että myös kolmas alkio on tällöin joukon G yksikäsitteinen alkio.

Joukon G neutraalialkio on 1, sillä $1 * a = a * 1 = a$ aina, kun $a \in G$.

Näin ollen lauseen 2.2 nojalla G on luuppi.

Tutkitaan vielä, voisiko luuppi G olla ryhmä eli toisin sanoen tutkitaan, onko joukko G assosiatiivinen. Nyt esimerkiksi $3 * (2 * 4) = 3 * 5 = 4$ ja $(3 * 2) * 4 = 5 * 4 = 3$. Koska $3 * (2 * 4) \neq (3 * 2) * 4$, niin luuppi G ei ole assosiatiivinen eli se ei ole ryhmä.

Esimerkki 8.2. Olkoon $G = \{1, 2, 3, 4, 5\}$ ja $(*)$ sellainen joukon G operaatio, että

$*$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	3	5	1	2	4
4	4	3	5	1	2
5	5	4	2	3	1

.

Esimerkin 8.1 nojalla G on luuppi.

Huomataan, että $x * x = 1$ kaikilla $x \in G$. Näin ollen $x = x^{\rho} = x^{\lambda}$ eli toisin sanoen $x = x^{-1}$.

Tutkitaan, onko luupilla G käänteisominaisuutta eli päteekö luupin G alkioille x ja y yhtälöt $y^{-1}(yx) = x$ ja $(xy)y^{-1} = x$. Aiemman nojalla $x = x^{-1}$ kaikilla $x \in G$. Tällöin esimerkiksi $(3 * 4) * 4 = 2 * 4 = 5 \neq 3$ ja $3 * (3 * 4) = 3 * 2 = 5 \neq 4$, joten luupilla G ei ole käänteisominaisuutta.

Tutkitaan seuraavaksi onko luuppi G C.I.P. -luuppi eli toteuttaako luuppi G ristikkäisen käänteisominaisuuden. Toisin sanoen täytyy tutkia päteekö kaikille alkiolle $x, y \in G$ yhtälö $(xy)x^{\rho} = y$.

Tutkitaan tämä käymällä läpi kaikki luupin G alkiot.

Olkoon $y = 1$ ja $x \in G$. Tällöin $(x1)x = xx = 1$ eli yhtälö pätee.

Olkoon sitten $x, y \in G$ ja $x = y$. Tällöin $(xx)x = 1x = x$.

Tutkitaan vielä erikseen loput luupin G alkiot.

Olkoon $y = 2$ ja $x \in \{3, 4, 5\}$. Tällöin

$$(3 * 2) * 3 = 5 * 3 = 2,$$
$$(4 * 2) * 4 = 3 * 4 = 2,$$
$$(5 * 2) * 5 = 4 * 5 = 2.$$

Olkoon $y = 3$ ja $x \in \{2, 4, 5\}$. Tällöin

$$(2 * 3) * 2 = 4 * 2 = 3,$$
$$(4 * 3) * 4 = 5 * 4 = 3,$$
$$(5 * 3) * 5 = 2 * 5 = 3.$$

Olkoon $y = 4$ ja $x \in \{2, 3, 5\}$. Tällöin

$$(2 * 4) * 2 = 5 * 2 = 4,$$
$$(3 * 4) * 3 = 2 * 3 = 4,$$
$$(5 * 4) * 5 = 3 * 5 = 4.$$

Olkoon $y = 5$ ja $x \in \{2, 3, 4\}$. Tällöin

$$(2 * 5) * 2 = 3 * 2 = 5,$$
$$(3 * 5) * 3 = 4 * 3 = 5,$$
$$(4 * 5) * 4 = 2 * 4 = 5.$$

Näin ollen kaikilla $x, y \in G$ pätee $(xy)x^{\rho} = y$, joten luuppi G on C.I.P. -luuppi.

Lähdeluettelo

[1] Bruck, R.H.: *Contributions to the theory of loops*, American Mathematical Society, vol 60, 1946, s. 245-354.

[2] Myllylä, K.: *On the solvability of groups and loops*, Acta Univ. Oul. A396, 2002.

[3] Niemenmaa, M., Myllylä, K., Tirilä, J-M.: *Algebra I, luentomoniste*, Oulun yliopisto, 2010.

[4] Pflugfelder, H.O.: *Quasigroups and loops introduction*, Sigma series in pure mathematics 7, Heldermann Berlin, 1990.