Tampereen yliopisto

Venla Härmä

NORMAALIT ALIRYHMÄT

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Helmikuu 2020

Tiivistelmä

Venla Härmä: Normaalit aliryhmät
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Helmikuu 2020

Tutustutaan aluksi ryhmiin, aliryhmiin ja syklisiin ryhmiin. Määritellään sivuluokat ja tutustutaan seurauksiin, joiden avulla todistetaan Lagrangen lause.

Käydään läpi normaalin aliryhmän määritelmä ja sen ominaisuuksia. Todistetaan, että kun H on ryhmän G normaali aliryhmä ja joukon G/H vasemmanpuoleisille sivuluokille määritellään $(aH) \circ (bH) = abH$, niin $(G/H, \circ)$ on ryhmä.

Avainsanat: sivuluokat, Lagrangen lause, normaalit aliryhmät

Sisältö

1 Johdanto

Tässä tutkielmassa perehdytään normaaleihin aliryhmiin ja niiden ominaisuuksiin. Normaali aliryhmä on sellainen aliryhmä, jonka vasemmat ja oikeat sivuluokat ovat samat. Edetään peruskäsitteistä ryhmäteorian käsiteisiin kuten ryhmään, aliryhmään ja sykliseen ryhmään.

Luvussa 2 määritellään alustavia käsitteitä, kuten ryhmän ja aliryhmän käsitteet, ja niiden ominaisuuksia. Luvussa 3 tutustutaan normaalien aliryhmien kannalta olennaisiin käsitteisiin ja Lagrangen lauseeseen. Määritellään normaali aliryhmä ja tekijäryhmä ja tutkitaan normaalien aliryhmien ominaisuuksia.

Lukijalta oletetaan algebran alkeiden osaamista, kuten joukko-opin tuntemista ja algebran peruskäsitteitä. Lähdemateriaaleina toimivat teokset Fundamentals of Abstract Algebra, kirjoittajina D. S. Malik, John. N. Mordeson ja M. K. Sen, ja Algebra Pure and Applied, kirjoittajana Aigli Papantonopoulou.

2 Ryhmät ja aliryhmät

2.1 Tarvittavien käsitteiden määritelmiä

Käydään ensimmäiseksi läpi tämän tutkielman ymmärtämisen kannalta olennaisia peruskäsitteitä.

Määritelmä 2.1 (Järjestetty pari)**.** Olkoot A ja B epätyhjiä joukkoja ja $x \in A$, $y \in B$. Nyt *järjestetty pari* (x, y) määritellään joukkona $\{\{x\}, \{x, y\}\}$.

Määritellään seuraavaksi binäärinen laskutoimitus. Selvitetään myös mitä tarkoittaa, kun joukko on suljettu binäärisen laskutoimituksen suhteen.

Määritelmä 2.2 (Binäärinen laskutoimitus)**.** Olkoon S epätyhjä joukko. Funktiota tulojoukolta $S \times S$ joukolle S kutsutaan *binääriseksi laskutoimitukseksi joukossa* S.

Olkoon $\circ$ binäärinen laskutoimitus joukossa S. Koska laskutoimituksen $\circ$ kuvajoukko on joukon S osajoukko, sanotaan, että joukko S on *suljettu laskutoimituksen* $\circ$ *suhteen*.

2.2 Ryhmä

Tässä luvussa käydään läpi ryhmän määritelmä ja ryhmän tärkeimpiä ominaisuuksia. Määritellään ensimmäiseksi ryhmä.

Määritelmä 2.3 (Ryhmä)**.** *Ryhmä* on järjestetty pari $(G, \circ)$, missä G on epätyhjä joukko ja $\circ$ joukon G laskutoimitus. Pari $(G, \circ)$ on ryhmä, jos seuraavat ehdot ovat voimassa.

1. Kaikille alkioille $a, b, c \in G$ on voimassa $a \circ (b \circ c) = (a \circ b) \circ c$.
2. On olemassa yksikäsitteinen alkio $e \in G$ siten, että kaikille $a \in G$ on voimassa $a \circ e = a = e \circ a$.
3. Jokaiselle alkiolle $a \in G$ on olemassa jokin alkio $b \in G$ siten, että $a \circ b = e = b \circ a$.

Edellisen määritelmän ominaisuutta 1 kutsutaan *liitännäisyydeksi*, eli assosiatiivisuudeksi. Ehdossa 2 mainittua alkiota $e \in G$ kutsutaan *neutraalialkioksi* ryhmässä

$(G, \circ)$. Ehdossa 3 esiintyvästä alkiosta $b \in G$ taas käytetään nimitystä *käänteisalkio*. Tässä tapauksessa b on alkion a käänteisalkio, joten siitä käytetään merkintää a^{-1}. Ryhmää $(G, \circ)$ kutsutaan *Abelin ryhmäksi* tai *vaihdannaiseksi ryhmäksi*, jos kaikille alkioille $a, b \in G$ on voimassa $a \circ b = b \circ a$. Seuraava lause esittää ryhmän suhteen neutraalialkioon ja käänteisalkioon.

Lause 2.4. *Olkoon $(G, \circ)$ ryhmä. Seuraavat lauseet ovat voimassa ryhmässä $(G, \circ)$.*

(i) *On olemassa yksikäsitteinen alkio $e \in G$ siten, että $e \circ a = a = a \circ e$ kaikille alkioille $a \in G$.*

(ii) *Jokaiselle alkiolle $a \in G$ on olemassa jokin alkio $b \in G$ siten, että $a \circ b = e = b \circ a$.*

Todistus. Ks. [1, s. 58]. □

Seuraavassa lauseessa käydään läpi tunnettuja ryhmien ominaisuuksia ja laskusääntöjä.

Lause 2.5. *Olkoon $(G, \circ)$ ryhmä. Silloin seuraavat lauseet ovat voimassa ryhmässä $(G, \circ)$.*

(i) $(a^{-1})^{-1} = a$ *kaikille alkioille* $a \in G$.

(ii) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ *kaikille alkioille* $a, b \in G$.

(iii) *Kaikille alkioille $a, b, c \in G$ pätee, että jos $a \circ c = b \circ c$ tai $c \circ a = c \circ b$, niin $a = b$.*

(iv) *Kaikille alkiolle $a, b \in G$ on olemassa yksikäsitteiset alkiot $x, y \in G$, joille on voimassa $a \circ x = b$ ja $y \circ a = b$.*

Todistus. Ks. [1, s. 63]. □

Seuraus 2.6. *Olkoon $(G, \circ)$ ryhmä ja $a \in G$. Jos $a \circ a = a$, niin $a = e$.*

Todistus. Koska $a = a \circ a$, saadaan $a \circ a = a \circ e$. Nyt lauseen 2.5 (iii) nojalla $a = e$. □

Ryhmää $(G, \circ)$ kutsutaan *äärelliseksi ryhmäksi*, jos joukossa G on äärellinen määrä alkioita. Ryhmän $(G, \circ)$ *kertaluvulla* tarkoitetaan joukon G alkioiden lukumäärää ja siitä käytetään merkintää $|G|$.

2.3 Aliryhmä

Tässä luvussa tutustutaan aliryhmän määritelmään ja sen tärkeimpiin ominaisuuksiin.

Määritelmä 2.7 (Aliryhmä)**.** Olkoon $(G, \circ)$ ryhmä ja epätyhjä joukko $H \subseteq G$. Jos $(H, \circ)$ on ryhmä, se on ryhmän $(G, \circ)$ *aliryhmä*.

Seuraavaksi yksinkertainen esimerkki tuttujen joukkojen ja tutun laskutoimituksen muodostamien ryhmien suhteista toisiinsa.

Esimerkki 2.8. Järjestetyt parit $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ ja $(\mathbb{R}, +)$ ovat ryhmiä, joissa laskutoimitus + on tavallinen yhteenlaskutoimitus. Ryhmä $(\mathbb{Z}, +)$ on ryhmien $(\mathbb{Q}, +)$ ja $(\mathbb{R}, +)$ aliryhmä, sillä $\mathbb{Z} \subseteq \mathbb{Q}$ ja $\mathbb{Z} \subseteq \mathbb{R}$.

Tähän asti olemme käyttäneet ryhmästä merkintää $(G, \circ)$ ja alkioiden laskutoimituksesta merkintää $a \circ b$. Jatkossa korvaamme nämä merkinnät siten, että käytämme ryhmästä merkintää G ja laskutoimituksesta ab, mikäli epäselvyyden vaaraa ei ole. Tämä mahdollistaa monimutkaisempien lauseiden, esimerkkien ja todistusten pysymisen selkeästi luettavina.

Seuraavaksi esitellään kaksi lausetta, joita voidaan hyödyntää, kun halutaan selvittää, onko kyseessä aliryhmä.

Lause 2.9. *Olkoon H joukon G epätyhjä osajoukko. Nyt H on ryhmän G aliryhmä, jos ja vain jos kaikilla alkioilla a, $b \in H$ on voimassa $ab^{-1} \in H$.*

Todistus. Ks. [1, s. 100]. □

Apulause 2.10. Olkoon G ryhmä ja olkoon H joukon G epätyhjä osajoukko. Silloin H on ryhmän G aliryhmä, jos ja vain jos kaikilla alkioilla a, $b \in H$ on voimassa $ab \in H$.

Todistus. Ks. [1, s. 101]. □

Määritellään seuraavaksi aliryhmien tulo.

Määritelmä 2.11 (Aliryhmien tulo)**.** Olkoot H ja K ryhmän G aliryhmiä. *Aliryhmien H ja K tulo* on määritelty joukoksi

$$HK = \{hk \mid h \in H, k \in K\}.$$

Olkoot $H_1, H_2, \ldots, H_n$ ryhmän G epätyhjiä osajoukkoja. Määritellään tulo $H_1H_2 \cdots H_n$ seuraavasti:

$$H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n \mid h_i \in H_i, i = 1, 2, \ldots, n\}.$$

Seuraava lause esittelee ehdon, jonka tulee toteutua, jotta ryhmän G aliryhmien tulo olisi myös ryhmän G aliryhmä. Esitellään myös kyseisen lauseen todistus.

Lause 2.12. *Olkoot H ja K ryhmän G aliryhmiä. Silloin aliryhmien tulo HK on ryhmän G aliryhmä, jos ja vain jos $HK = KH$.*

Todistus. (Vrt. [1, 103].) Oletetaan ensin, että aliryhmien tulo HK on ryhmän G aliryhmä. Näin ollen HK on siis myös ryhmä. Olkoon sitten $kh \in KH$, missä $k \in K$ ja $h \in H$, ja olkoon $e \in HK$ neutraalialkio aliryhmässä HK. Silloin $e \in H$ ja $e \in K$. Nyt neutraalialkion määritelmän mukaan $k = ek \in HK$ ja $h = he \in HK$. Koska HK on aliryhmä, niin myös $kh \in HK$. Tästä seuraa, että $KH \subseteq HK$. Osoitetaan seuraavaksi, että myös $HK \subseteq KH$. Olkoon $hk \in HK$. Koska HK on ryhmä ja $hk \in HK$, niin ryhmässä HK tulee olla myös käänteisalkio $(hk)^{-1}$. Nyt siis $(hk)^{-1} \in HK$ ja on voimassa $(hk)^{-1} = h_1k_1$ joillekin alkioille $h_1 \in H$ ja $k_1 \in K$. Siispä käänteisalkion laskusäännöistä saadaan, että $hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$. Tästä seuraa, että $HK \subseteq KH$, eli ollaan siis osoitettu, että $HK = KH$.

Käänteisesti oletetaan, että $HK = KH$. Olkoot h_1k_1, $h_2k_2 \in HK$. Nyt $k_2^{-1}h_2^{-1} \in KH = HK$. Tästä seuraa, että on voimassa $k_2^{-1}h_2^{-1} = h_3k_3$ joillekin alkioille $h_3 \in H$ ja $k_3 \in K$. Yhtä lailla, $k_1h_3 = h_4k_4$ joillekin alkioille $h_4 \in H$ ja $k_4 \in K$. Tästä saadaan, että

$$\begin{aligned}(h_1k_1)(h_2k_2)^{-1} &= h_1k_1k_2^{-1}h_2^{-1} \\ &= h_1k_1h_3k_3 \\ &= h_1h_4k_4k_3 \in HK.\end{aligned}$$

Siispä lauseen 2.9 nojalla, HK on ryhmän G aliryhmä. □

Seuraus 2.13. *Jos H ja K ovat vaihdannaisen ryhmän G aliryhmiä, niin silloin HK on ryhmän G aliryhmä.*

Määritelmä 2.14. Olkoon G ryhmä ja $S \subset G$. Silloin $\langle S \rangle$ on ryhmän G kaikkien sellaisten aliryhmien H leikkaus, että $S \subseteq H$. Nyt ryhmän G aliryhmää $\langle S \rangle$ kutsutaan joukon S *virittämäksi aliryhmäksi*. Jos $G = \langle S \rangle$, joukkoa S kutsutaan ryhmän G *virittäjistöksi*.

Lause 2.15. *Olkoot H ja K ryhmän G aliryhmiä. Silloin HK on ryhmän G aliryhmä, jos ja vain jos $HK = \langle H \cup K \rangle$.*

Todistus. (Vrt. [1, 104].) Oletetaan ensin, että HK on ryhmän G aliryhmä. Olkoon $h \in H$ ja $k \in K$. Silloin $h = he \in HK$ ja $k = ek \in HK$, ja siten $H \subseteq HK$ ja $K \subseteq HK$. Siispä, $H \cup K \subseteq HK$. Koska $\langle H \cup K \rangle$ on ryhmän G pienin aliryhmä, jonka osajoukko on $H \cup K$, niin myös $\langle H \cup K \rangle \subseteq HK$. Osoitetaan seuraavaksi, että myös $HK \subseteq \langle H \cup K \rangle$. Olkoon $hk \in HK$, missä $h \in H$ ja $k \in K$. Koska $H \subseteq \langle H \cup K \rangle$ ja $K \subseteq \langle H \cup K \rangle$, on olemassa jotkin alkiot $h, k \in \langle H \cup K \rangle$. Koska $\langle H \cup K \rangle$ on aliryhmä, niin $hk \in \langle H \cup K \rangle$ ja siten $HK \subseteq \langle H \cup K \rangle$. Näin ollen, $HK = \langle H \cup K \rangle$.

Päinvastoin oletetaan, että $HK = \langle H \cup K \rangle$. Nyt koska $\langle H \cup K \rangle$ on ryhmän G aliryhmä, niin myös HK on ryhmän G aliryhmä. □

2.4 Syklinen ryhmä

Seuraavaksi esitellään ryhmien erikoistapaus, syklinen ryhmä. Syklinen ryhmä on yksittäisen alkion generoima ryhmä. Jokainen syklinen ryhmä on vaihdannainen.

Määritelmä 2.16 (Syklinen ryhmä)**.** Olkoon G ryhmä. Ryhmää G kutsutaan *sykliseksi ryhmäksi*, jos on olemassa sellainen $a \in G$, että

$$G = \langle a \rangle.$$

Merkintä $\langle a \rangle$ tarkoittaa joukkoa $\{a^n \mid n \in \mathbb{Z}\}$. Tässä merkinnällä a^n tarkoitetaan potenssia ryhmän laskutoimituksen suhteen. Esimerkiksi jos laskutoimitus ryhmässä G on $\circ$, niin $a^3 = a \circ a \circ a$. Seuraavassa lauseessa on myös huomattava, että $a^0 = e$.

Lause 2.17. *Olkoon $\langle a \rangle$ äärellinen syklinen ryhmä kertaluvulla n. Silloin $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.*

Todistus. Ks. [1, s. 111]. □

Esimerkki 2.18. Olkoon $a \in G$ ja $n > 0$. Määritellään laskutoimitus $\circ$ seuraavan laskutoimitustaulukon mukaan:

$\circ$	a^0	a^1	a^2	$\dots$	a^{n-2}	a^{n-1}
a^0	a^0	a^1	a^2	$\dots$	a^{n-2}	a^{n-1}
a^1	a^1	a^2	a^3	$\dots$	a^{n-1}	a^0
a^2	a^2	a^3	a^4	$\dots$	a^0	a^1
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
a^{n-2}	a^{n-2}	a^{n-1}	a^0	$\dots$	a^{n-4}	a^{n-3}
a^{n-1}	a^{n-1}	a^0	a^1	$\dots$	a^{n-3}	a^{n-2}

Nyt ryhmä $(\{a^0, a^1, \dots, a^{n-1}\}, \circ)$ on alkion a määräämä syklinen ryhmä.

Lause 2.19. *Syklisen ryhmän jokainen aliryhmä on syklinen.*

Todistus. (Vrt. [1, 112].) Olkoon H syklisen ryhmän $G = \langle a \rangle$ aliryhmä. Todistetaan, että aliryhmä H on myös syklinen. Tarkastellaan ensin tapausta, jossa $H = \{e\}$. Nyt, koska e on neutraalialkio, on laskutoimituksen e^n tulos aina e. Siispä $H = \langle e \rangle$ ja siten aliryhmä H on syklinen.

Oletetaan sitten, että $\{e\} \subset H$. Silloin on olemassa $b \in H$ siten, että $b \neq e$. Koska $b \in H$, niin tietysti myös $b \in G$. Tiedetään, että ryhmä G on syklinen, joten on siis voimassa $b = a^m$ jollekin eksponentille m. Siispä, koska $b \neq e$ ja tiedetään, että $b^0 = e$, niin täytyy siis olla $m \neq 0$. Koska H on ryhmä, on alkiolla b käänteisalkio b^{-1} ryhmässä H. Käänteisalkiolle saadaan $b^{-1} = (a^m)^{-1} = a^{-m} \in H$. On siis osoitettu, että on olemassa alkiot a^m, $a^{-m} \in H$. Joko m tai $-m$ on positiivinen, joten voidaan todeta, että ryhmässä H on ainakin yksi alkion a positiivinen potenssi. Olkoon nyt n pienin positiivinen eksponentti, jolle $a^n \in H$. Osoitamme seuraavaksi, että $H = \langle a^n \rangle$.

Koska $a^n \in H$, täytyy myös olla $\langle a^n \rangle \subseteq H$. Olkoon alkio $h \in H$. Nyt $h \in G = \langle a \rangle$, joten $h = a^k$ jollekin eksponentille k. Jakoyhtälön mukaan on olemassa alkiot q, r siten, että $k = nq + r, 0 \leq r < n$. Koska a^n ja $a^k \in H$, niin $a^r = a^{k-nq} = a^k(a^n)^{-q} \in H$. Toisaalta, jos $r > 0$, muodostuu ristiriita sen oletuksen kanssa, että n olisi pienin positiivinen alkio, jolle $a^n \in H$. Sen vuoksi $r = 0$, jolloin $k = nq$ eli saadaan $a^k = (a^n)^q \in \langle a^n \rangle$. Siispä, $H \subseteq \langle a^n \rangle$ ja siten $H = \langle a^n \rangle$. On siis todistettu, että aliryhmä H on syklinen. □

3 Normaalit aliryhmät

3.1 Sivuluokat

Tässä luvussa tutustutaan aliryhmien sivuluokkiin. Sivuluokat on olennaista hallita, kun lähdetään tutustumaan Lagrangen lauseeseen ja edelleen normaaleihin aliryhmiin. Esitellään seuraavaksi sivuluokkien määritelmä.

Määritelmä 3.1 (Sivuluokat)**.** Olkoon H ryhmän G aliryhmä ja $a \in G$. Joukkoja $aH = \{ ah \mid h \in H \}$ ja $Ha = \{ ha \mid h \in H \}$ kutsutaan ryhmän G alkion a määräämiksi *vasemman- ja oikeanpuoleisiksi sivuluokiksi*.

Jos ryhmä G on vaihdannainen, niin $aH = Ha$. Kun e on neutraalialkio ryhmässä G, niin on voimassa $eH = H = He$ ja $a = ae \in aH$ ja $a = ea \in Ha$. Seuraava lause esittää sivuluokkien olennaisia laskusääntöjä.

Lause 3.2. *Olkoon H ryhmän G aliryhmä ja $a, b \in G$. Nyt*

(i) *$aH = bH$, jos ja vain jos $b^{-1}a \in H$,*

(ii) *$Ha = Hb$, jos ja vain jos $ab^{-1} \in H$.*

Todistus. (Vrt. [1, 118].) (i) Oletetaan ensin, että $aH = bH$. Nyt koska $a \in aH$ ja $aH = bH$, niin $a \in bH$, joten täytyy olla olemassa jokin alkio $h' \in H$ siten, että $a = bh'$. Kerrotaan yhtälö puolittain alkion b käänteisalkiolla b^{-1}, jolloin saadaan $b^{-1}a = bh'b^{-1}$, eli $b^{-1}a = h' \in H$.

Käänteisesti oletetaan, että $b^{-1}a \in H$. Silloin on olemassa jokin alkio $h' \in H$ siten, että $b^{-1}a = h'$. Voidaan jälleen kertoa yhtälö puolittain alkiolla b, jolloin saadaan $b^{-1}ab = bh'$ ja edelleen $a = bh'$. Olkoon nyt $ah \in aH$. Yhdistämällä edellinen yhtälö tähän, saadaan $ah = bh'h \in bH$. Tästä seuraa, että $aH \subseteq bH$. Seuraavaksi tulee osoittaa, että $bH \subseteq aH$, jotta lopulta saataisiin $aH = bH$. Aikaisemmin muodostettiin yhtälö $a = bh'$ ja kertomalla alkiolla h'^{-1} saadaan, että $ah'^{-1} = b$. Olkoon nyt $bh \in bH$. Käyttämällä edellistä yhtälöä saadaan siis $bh = ah'^{-1}h \in aH$. Tästä seuraa, että $bH \subseteq aH$. Nyt koska $aH \subseteq bH$ ja $bH \subseteq aH$, niin $aH = bH$.

(ii) Tehdään oletus, että $Ha = Hb$. Nyt koska $a \in Ha$ ja $Ha = Hb$, täytyy olla olemassa jokin alkio $h' \in H$ siten, että $a = h'b$. Voidaan kertoa yhtälö puolittain alkioilla b^{-1}, jolloin saadaan $ab^{-1} = b^{-1}h'b$, eli $ab^{-1} = h' \in H$.

Käänteisesti oletetaan, että $ab^{-1} \in H$. Silloin on olemassa jokin alkio $h' \in H$ siten, että $ab^{-1} = h'$. Kerrotaan yhtälö puolittain alkiolla b, jolloin saadaan $bab^{-1} = h'b$ ja edelleen $a = h'b$. Olkoon nyt $ha \in Ha$. Yhdistämällä edelliseen yhtälöön, saadaan $ha = hh'b \in Hb$. Tästä seuraa, että $Ha \subseteq Hb$. Seuraavaksi osoitetaan, että $Hb \subseteq Ha$. Lisätään yhtälöön $a = h'b$ alkio h'^{-1}, jolloin saadaan $h'^{-1}a = b$. Olkoon nyt $hb \in Hb$. Yhdistämällä edelliseen yhtälöön saadaan $hb = hh'^{-1}a \in Ha$. Tästä seuraa, että $Hb \subseteq Ha$. Nyt koska $Ha \subseteq Hb$ ja $Hb \subseteq Ha$, niin $Ha = Hb$. □

Seuraava lause kertoo sen, että ryhmässä G kahden eri alkion määräämät sivuluokat ovat joko samat tai sitten niiden leikkaus on tyhjä joukko. Esitellään sen jälkeen seuraukset 3.5 ja 3.7, joita tullaan tarvitsemaan seuraavassa luvussa Lagrangen lauseen todistuksessa. Määritellään ensin seurauksessa 3.5 esiintyvä käsite ositus.

Määritelmä 3.3 (Ositus)**.** Olkoon A joukko ja $\mathcal{P}$ jokin joukon A epätyhjien osajoukkojen kokoelma. Nyt $\mathcal{P}$ on joukon A *ositus*, jos seuraavat ehdot ovat voimassa.

(i) Kaikille $B, C \in \mathcal{P}$, joko $B = C$ tai $B \cap C = \phi$.

(ii) $A = \cup_{B \in \mathcal{P}} B$.

Lause 3.4. *Olkoon H ryhmän G aliryhmä. Nyt kaikille alkioille $a, b \in G$ on voimassa joko $aH = bH$ tai $aH \cap bH = \phi$.*

Todistus. Ks. [1, s. 118]. □

Seuraus 3.5. *Olkoon H ryhmän G aliryhmä. Nyt joukkojen kokoelma $\{aH \mid a \in G\}$ muodostaa joukon G osituksen.*

Todistus. (Vrt. [1, 118].) Olkoon $\mathcal{P} = \{aH \mid a \in G\}$. Tämä tarkoittaa sitä, että $\mathcal{P}$ on kaikkien ryhmän G vasemmanpuoleisten sivuluokkien joukko. Lauseen 3.4 mukaan kaikille sivuluokille aH, $bH \in \mathcal{P}$ on voimassa joko $aH = bH$ tai $aH \cap bH = \phi$. Siispä, $\mathcal{P}$ täyttää ehdon (i) määritelmästä 3.3. Koska $aH \subseteq G$ kaikille $a \in G$, $\cup_{aH \in \mathcal{P}} aH \subseteq G$. Jos $a \in G$, niin $a \in aH \subseteq \cup_{aH \in \mathcal{P}} aH$. Siten, $G \subseteq \cup_{aH \in \mathcal{P}} aH$. Siispä, $G = \cup_{aH \in \mathcal{P}} aH$. Tämä osoittaa, että $\mathcal{P}$ täyttää ehdon (ii) määritelmästä 3.3. Näin ollen, $\mathcal{P}$ on joukon G ositus. □

Lause 3.6. *Olkoon H ryhmän G aliryhmä. Silloin on olemassa bijektio aliryhmän H ja sen jokaisen vasemmanpuoleisen (ja oikeanpuoleisen) sivuluokan välillä.*

Todistus. Ks. [1, s. 119]. □

Seuraus 3.7. *Olkoon H ryhmän G aliryhmä. Nyt kaikille alkioille $a \in G$ on voimassa $|H| = |aH| = |Ha|$.*

3.2 Lagrangen lause

Lagrangen lause on ryhmäteorian tärkeimpiä lauseita. Lagrangen lause osoittaa, että aliryhmän kertaluku jakaa äärellisen ryhmän kertaluvun.

Lause 3.8 (Lagrangen lause)**.** *Olkoon H äärellisen ryhmän G aliryhmä. Silloin aliryhmän H kertaluku jakaa ryhmän G kertaluvun, eli $|H| \mid |G|$. Merkitään*

$$|G| = [G : H]|H|.$$

Todistus. (Vrt. [1, 120].) Koska G on äärellinen ryhmä, sen vasemmanpuoleisten sivuluokkien lukumäärä on myös äärellinen. Olkoon nyt $A = \{a_1H, a_2H, \ldots, a_rH\}$ kaikkien ryhmän G vasemmanpuoleisten sivuluokkien joukko. Nyt seurauksen 3.5 nojalla $G = \bigcup_{i=1}^{r} a_iH$ ja $a_iH \cap a_jH = \phi$ kaikilla $i \neq j$, $1 \leq i, j \leq r$. Näin ollen saadaan, että $[G : H] = r$ ja

$$|G| = |a_1H| + |a_2H| + \ldots + |a_rH|.$$

Seurauksen 3.7 nojalla $|H| = |a_iH|$ kaikilla i, $1 \leq i \leq r$. Näin ollen

$$\begin{aligned} |G| &= \underbrace{|H| + |H| + \ldots + |H|}_{r \text{ kpl}} \\ &= r|H| \\ &= [G : H]|H|. \end{aligned}$$

Nyt on todistettu, että aliryhmän H kertaluku jakaa ryhmän G kertaluvun. □

Lause 3.9. *Olkoot H ja K ryhmän G äärellisiä aliryhmiä. Silloin*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Todistus. (Vrt. [1, 122].) Merkitään aluksi, että $A = H \cap K$. Koska H ja K ovat ryhmän G aliryhmiä, myös aliryhmien leikkaus A on ryhmän G aliryhmä. Saadaan myös, että koska $A \subseteq H$, niin A on myös ryhmän H aliryhmä. Lagrangen lauseen mukaan kertaluku $|A|$ jakaa kertaluvun $|H|$. Käytetään näiden kertalukujen suhteesta merkintää n, eli olkoon $n = \frac{|H|}{|A|}$. Silloin $[H : A] = n$ ja siten aliryhmällä A on n kappaletta erilaisia vasemmanpuoleisia sivuluokkia ryhmässä H. Olkoon nyt $\{x_1A, x_2A, \ldots, x_nA\}$ kaikkien ryhmän A eri vasemmanpuoleisten sivuluokkien joukko ryhmässä H. Silloin $H = \bigcup_{i=1}^{n} x_iA$. Koska $A \subseteq K$, saadaan, että

$$HK = (\cup_{i=1}^{n} x_iA)K = \cup_{i=1}^{n} x_iK.$$

Seuraavaksi osoitetaan, että $x_iK \cap x_jK = \phi$, jos $i \neq j$. Tehdään vastaoletus, että joillekin alkioille $i \neq j$ on voimassa $x_iK \cap x_jK \neq \phi$. Silloin siis sivuluokat ovat samat, eli $x_jK = x_iK$. Siispä, $x_i^{-1}x_j \in K$. Koska $x_i^{-1}x_j \in H$, niin myös $x_i^{-1}x_j \in A$ ja siten $x_jA = x_iA$. Tämä on ristiriidassa oletuksen kanssa, että $x_1A, \ldots, x_nA$ ovat eri suuria vasemmanpuoleisia sivuluokkia. Siten $x_1K, \ldots, x_nK$ ovat erillisiä vasemmanpuoleisia ryhmän K sivuluokkia. Myös seurauksen 3.7 mukaan $|K| = |x_iK|$ kaikille $i = 1, 2, \ldots, n$, joten saadaan

$$\begin{aligned} |HK| &= |x_1K| + \ldots + |x_nK| \\ &= \underbrace{|K| + \ldots + |K|}_{n \text{ kpl}} \\ &= n|K| \\ &= \frac{|H||K|}{|A|} \\ &= \frac{|H||K|}{|H \cap K|}. \end{aligned}$$

□

3.3 Normaali aliryhmä ja tekijäryhmä

Tässä luvussa tutustutaan normaaleihin aliryhmiin. Normaaliksi aliryhmäksi kutsutaan sellaista tapausta, kun vasemman- ja oikeanpuoleiset sivuluokat ovat samat.

Määritelmä 3.10 (Normaali aliryhmä)**.** Olkoon G ryhmä ja H sen aliryhmä. Aliryhmää H sanotaan *normaaliksi aliryhmäksi*, jos joukon G alkioiden määräämät oikean- ja vasemmanpuoleiset sivuluokat ovat samoja, eli jos

$$aH = Ha \text{ kaikilla } a \in G.$$

Normaalin aliryhmän määritelmästä seuraa, että jokaiselle ryhmälle $G \neq \{e\}$ on olemassa ainakin kaksi normaalia aliryhmää. Nämä ovat ryhmä G itse ja $\{e\}$. Jos H on ryhmän G normaali aliryhmä, niin välttämättä ei ole voimassa $ah = ha$ kaikille alkioille $h \in H$ ja $a \in G$. Seuraava esimerkki osoittaa tämän.

Esimerkki 3.11. Oletetaan tässä esimerkissä lukijalta permutaatioryhmän ja joukon S_3 tunteminen. Olkoon nyt $H = \left\{e, \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right)\right\}$ ryhmän S_3 normaali aliryhmä. Merkitään $h = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) \in H$ ja $a = \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right) \in S_3$. Silloin

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} h = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

ja

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

Nyt ei ole voimassa $ah = ha$ kaikille $a \in S_3$ ja $h \in H$, eli

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} h \neq h \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

vaikka

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

Normaalin aliryhmän testaamista varten on olemassa useita kriteerejä. Seuraava lause sisältää niistä yhden.

Lause 3.12. *Olkoon H ryhmän G aliryhmä. Nyt H on ryhmän G normaali aliryhmä, jos ja vain jos kaikilla alkioilla $a \in G$ on voimassa $aHa^{-1} \subseteq H$.*

Todistus. (Vrt. [1, 128].) Tehdään ensin oletus, että H on ryhmän G normaali aliryhmä. Olkoon sitten $a \in G$. Tarkoituksena on nyt osoittaa, että $aHa^{-1} \subseteq H$. Olkoon nyt $aha^{-1} \in aHa^{-1}$, missä $h \in H$. Koska H on ryhmän G normaali aliryhmä, niin $aH = Ha$. Tiedetään siis, että koska $ah \in aH$, niin $ah \in Ha$, joten on voimassa $ah = h'a$ jollekin alkiolle $h' \in H$. Kun lisätään alkion a käänteisalkio a^{-1} yhtälön molemmin puolin, saadaan $aha^{-1} = h' \in H$. Saadaan siis, että $aHa^{-1} \subseteq H$.

Käänteisesti oletetaan, että on voimassa $aHa^{-1} \subseteq H$ kaikille alkioille $a \in G$. Olkoon siis $a \in G$, ja osoitetaan, että $aH = Ha$. Olkoon $ah \in aH$, missä $h \in H$. Nyt $aha^{-1} \in aHa^{-1}$ ja siten $aha^{-1} \in H$. Voidaan siis merkitä, että $aha^{-1} = h'$ jollekin alkiolle $h' \in H$. Kun kerrotaan yhtälö puolittain alkiolla a, saadaan $ah = h'a \in Ha$. Näin ollen, $aH \subseteq Ha$. Osoitetaan seuraavaksi, että myös $Ha \subseteq aH$. Olkoon $ha \in Ha$, missä $h \in H$. Nyt $a^{-1}ha \in a^{-1}Ha$ ja siten $a^{-1}ha \in H$. Siis $a^{-1}ha = h'$ jollekin $h' \in H$. Yhtälöstä saadaan $ha = ah' \in aH$. Näin ollen myös $Ha \subseteq aH$ ja siten $aH = Ha$. Siispä, H on ryhmän G normaali aliryhmä. □

Seuraava lause esittelee normaalien aliryhmien tärkeitä ominaisuuksia. Todistetaan sitten kaikki lauseen kolme alakohtaa.

Lause 3.13. *Olkoon G ryhmä ja olkoot H ja K sen normaaleja aliryhmiä. Silloin*

(i) *$H \cap K$ on ryhmän G normaali aliryhmä,*

(ii) *$HK = KH$ on ryhmän G normaali aliryhmä,*

(iii) $\langle H \cup K \rangle = HK$.

Todistus. (Vrt. [1, 129].) (i) Tiedetään, että aliryhmien leikkaus on myös aliryhmä. Koska H ja K ovat ryhmän G aliryhmiä, niin myös leikkaus $H \cap K$ on ryhmän G aliryhmä. Olkoon nyt $g \in G$, ja todistetaan, että $g(H \cap K)g^{-1} \subseteq H \cap K$. Olkoon nyt gag^{-1} jokin alkio, jossa $a \in H \cap K$. Koska $a \in H \cap K$, niin $a \in H$ ja $a \in K$. Voidaan siis kirjoittaa, että $gag^{-1} \in H$ ja $gag^{-1} \in K$, ja tästä seurauksena $gag^{-1} \in H \cap K$. Tämä osoittaa, että $g(H \cap K)g^{-1} \subseteq H \cap K$. Siispä, lauseen 3.12 nojalla $H \cap K$ on normaali aliryhmä.

(ii) Osoitetaan ensin, että $HK = KH$. Olkoon $hk \in HK$, missä $h \in H$ ja $k \in K$. Koska K on ryhmän G normaali aliryhmä ja $h \in G$, niin $hK = Kh$. Siispä, $hk \in hK = Kh$. Koska $Kh \subseteq KH$, niin $hk \in KH$, ja näin ollen $HK \subseteq KH$. Osoitetaan sitten, että myös $KH \subseteq HK$. Olkoon $kh \in KH$, missä $k \in K$ ja $h \in H$. On siis jälleen $Kh = hK$, ja nyt $kh \in Kh = hK$. Koska $hK \subseteq HK$, niin $kh \in HK$, eli $KH \subseteq HK$. Ollaan siis saatu $HK = KH$. Koska H ja K ovat aliryhmiä ja $HK = KH$, lauseen 2.12 nojalla HK on ryhmän G aliryhmä.

Seuraavaksi osoitetaan, että HK on normaali aliryhmä. Olkoon $g \in G$. Silloin $gHg^{-1} \subseteq H$ ja $gKg^{-1} \subseteq K$, koska H ja K ovat normaaleja aliryhmiä. Nyt

$$\begin{aligned} g(HK)g^{-1} &= g(Hg^{-1}gK)g^{-1} \\ &= (gHg^{-1})(gKg^{-1}) \\ &\subseteq HK. \end{aligned}$$

Näin ollen, lauseen 3.12 nojalla, HK on ryhmän G aliryhmä.

(iii) Kohdan (ii) mukaan HK on ryhmän G aliryhmä. Tästä saadaan, että lauseen 2.15 nojalla

$$HK = \langle H \cup K \rangle.$$

□

Lause 3.14. *Olkoon H ryhmän G normaali aliryhmä. Merkitään kaikkien vasemmanpuoleisten sivuluokkien joukkoa $\{aH \mid a \in G\}$ notaatiolla G/H, ja määritellään laskutoimitus $\circ$ joukossa G/H siten, että kaikille sivuluokille aH, $bH \in G/H$ on voimassa*

$$(aH) \circ (bH) = abH.$$

Nyt $(G/H, \circ)$ *on ryhmä.*

Todistus. (Vrt. [1, 131].) Ensin osoitetaan, että $\circ$ on hyvinmääritelty. Olkoot aH, bH, $a'H$, $b'H \in G/H$ ja oletetaan, että $(aH, bH) = (a'H, b'H)$. Silloin $aH = a'H$ ja $bH = b'H$. Nyt tulee osoittaa, että $aH \circ bH = a'H \circ b'H$ tai $abH = a'b'H$. Nyt koska $aH = a'H$ ja $bH = b'H$, niin joillekin alkioille h_1, $h_2 \in H$ on voimassa $a = a'h_1$ ja $b = b'h_2$. Saadaan

$$\begin{aligned}(a'b')^{-1}(ab) &= b'^{-1}a'^{-1}ab \\ &= b'^{-1}a'^{-1}a'h_1b'h_2 \\ &= b'^{-1}h_1b'h_2.\end{aligned}$$

Koska H on normaali aliryhmä ja $h_1 \in H$, on voimassa $b'^{-1}h_1b'h_2 = (b'^{-1}h_1b')h_2 \in H$. Siten myös $(a'b')^{-1}(ab) \in H$. Tämän seurauksena, lauseen 3.2 (i) nojalla $abH = a'b'H$, eli $\circ$ on hyvinmääritelty.

Seuraavaksi osoitetaan, että $\circ$ on liitännäinen. Olkoot aH, bH, $cH \in G/H$. Nyt $(aH) \circ [(bH) \circ (cH)] = (aH) \circ (bcH) = a(bc)H = (ab)cH = (abH) \circ (cH) = [(aH) \circ (bH)] \circ (cH)$. Siispä, $\circ$ on liitännäinen.

Nyt $eH \in G/H$ ja

$$(aH) \circ (eH) = aeH = aH = eaH = (eH) \circ (aH)$$

kaikille $aH \in G/H$. Siispä eH on neutraalialkio joukossa G/H.

Lisäksi kaikille $aH \in G/H$ on olemassa $a^{-1}H \in G/H$ ja

$$(aH) \circ (a^{-1}H) = aa^{-1}H = eH = a^{-1}aH = (a^{-1}H) \circ (aH).$$

Kaikille $aH \in G/H$ on siis käänteisalkio $a^{-1}H$ joukossa aH. Näin ollen $(G/H, \circ)$ on ryhmä. □

Määritelmä 3.15 (Tekijäryhmä)**.** Olkoon H ryhmän G normaali aliryhmä. Nyt sivuluokkaryhmää G/H kutsutaan aliryhmän H määräämäksi ryhmän G *tekijäryhmäksi*.

Lähteet

[1] Malik, D. S., Mordeson, J. N., Sen, M. K. *Fundamentals of Abstract Algebra*. United States of America: The McGraw-Hill Companies, Inc, 1997.

[2] Papantonopoulou, Aigli, *Algebra Pure and Applied*. University of California, Prentice Hall, 2002.