TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Veli-Matti Nieminen

Äärellisten ryhmien hajotelmat suoriksi tuloiksi

Informaatiotieteiden yksikkö
Matematiikka
Kesäkuu 2016

Tampereen yliopisto
Informaatiotieteiden yksikkö
NIEMINEN, VELI-MATTI: Äärellisten ryhmien hajotelmat suoriksi tuloiksi
Pro gradu -tutkielma, 29 s.
Matematiikka
Kesäkuu 2016

Tiivistelmä

Tämän tutkielman päälauseessa todistetaan Krullin, Remakin ja Schmidtin lauseen erityistapaus. Tapauksessa rajoitutaan tarkastelemaan äärellisiä ryhmiä, joiden keskus on triviaali. Tulos esittää, että epätriviaalille äärelliselle ryhmälle, jonka keskus on triviaali, on olemassa tekijöiden järjestystä vaille yksikäsitteinen hajotelma epätriviaalien hajoamattomien normaalien aliryhmiensä suoraksi tuloksi. Luvussa kaksi esitetään kertausluontoisesti ja tiiviisti ryhmäteoriaa ja esitellään Oomega-ryhmät, jotka helpottavat luvun viisi käsittelyä. Luvussa kolme perehdytään ryhmien suoriin tuloihin ja esitellään tutkielmassa oleellisesti käytettävä samaistus sisäisen ja ulkoisen suoran tulon välillä. Luvussa neljä keskitytään keskuksen käsitteeseen. Viimeisen luvun aluksi esitetään tarvittavia määritelmiä ja aputuloksia, joita tarvitaan luvun päättävän päälauseen todistuksessa. Tutkielman päälähteenä on käytetty John S. Rosen teosta A Course on Group Theory.

Sisältö

1 Johdanto

Tässä tutkielmassa käsitellään äärellisten ryhmien hajotelmia suoriksi tuloiksi. Ryhmien suoria tuloja on kahdenlaisia, ulkoisia ja sisäisiä. Ulkoisen suoran tulon avulla voidaan kahdesta tai useammasta ryhmästä konstruoida uusi ryhmä. Mielenkiintoisempi tapaus on sisäinen suora tulo, joka mahdollistaa joidenkin ryhmien jakamisen tekijöihin normaalien aliryhmiensä avulla. Sisäinen ja ulkoinen suora tulo ovat keskenään isomorfiset. Ryhmän esitystä epätriviaalien normaalien aliryhmiensä sisäisenä suorana tulona kutsutaan ryhmän hajotelmaksi.

Krullin, Remakin ja Schmidtin ryhmiä koskeva lause esittää, että jos ryhmälle on olemassa kaksi hajotelmaa hajoamattomien epätriviaalien normaalien aliryhmiensä sisäisenä suorana tulona, niin suoran tulon tekijöiden lukumäärä on sama molemmissa esityksissä ja kullekin tekijälle löytyy isomorfinen vastine. Lisäksi lauseen nojalla yksittäisiä suoran tulon tekijöitä voidaan vaihtaa esitysten välillä. Tämän tutkielman päälauseena todistetaan lauseen erityistapaus, joka rajoittuu tarkastelemaan epätriviaaleja äärellisiä ryhmiä, joiden keskus on triviaali. Tässä erityistapauksessa ryhmälle saatavat kaksi esitystä ovat tekijöiden järjestystä vaille yksikäsitteiset.

Krullin, Remakin ja Schmidtin lausetta ei ole nimetty lauseen ensimmäisen esittäjän mukaan. Lauseen esitti J.M.H. Wedderbun vuonna 1909, mutta esitetty todistus oli virheellinen. R. Remak esitti vuonna 1911 ensimmäisenä pätevän todistuksen äärellisten ryhmien tapaukselle ja O.J. Schmidt yksinkertaistetumman todistuksen vuonna 1912. W. Krull laajensi tuloksen kattamaan modulit vuonna 1925 ja O.J. Schmidt Ω-ryhmät vuonna 1928. [5, s. 144]

Lukijan oletetaan tuntevan algebran perusteet. Luvun kaksi ensimmäisessä alaluvussa kuitenkin kerrataan tälle tutkielmalle oleellisimmat algebran peruskäsitteet ja tulokset. Kertausluontoisuuden vuoksi käsittelyyn ei käytetä paljoa aikaa. Luvun kaksi jälkimmäisessä alaluvussa tutustutaan pääluvun käsittelyä oleellisesti yksinkertaistavan Ω-ryhmän käsitteeseen. Luku kolme keskittyy ryhmien suoriin tuloihin, jotka ovat tämän tutkielman oleellista antia. Ulkoisen ja sisäisen suoran tulon määrittelyn jälkeen esitetään loppututkielman käsittelyä helpottava samaistus sisäisen ja ulkoisen suoran tulon välillä, jota havainnollistetaan esimerkein. Luku neljä keskittyy erityisesti keskuksen käsitteeseen, sillä keskusta koskeva oletus oleellinen päälausetta ajatellen. Lukujen kolme ja neljä viimeisimpinä tuloksina esitetään päälauseen todistuksessa tarvittavia apulauseita. Luvun viisi alussa esitetään tarvittavia käsitteitä ja tuloksia, joita hyödynnetään luvun päättävän päälauseen todistuksessa.

Suurin osa esitetyistä havainnollistavista esimerkeistä ovat joko tutkielman tekijän itse kehittämiä tai lähdeteosten harjoitustehtäviä. Myös osa esitetyistä apulauseista on lähdeteosten harjoitustehtäviä. Tutkielman päälähteenä on käytetty John S. Rosen teosta *A Course on Group Theory* [4].

2 Ryhmäteorian peruskäsitteitä ja -tuloksia

Tässä luvussa esitellään tutkielmassa myöhemmin tarvittavia ryhmäteorian peruskäsitteitä ja -tuloksia. Alaluvussa 2.1 esitellään kertauksenomaisesti ryhmiin, kuvauksiin ja homomorfismeihin liittyviä määritelmiä ja tuloksia, joiden oletetaan olevan lukijalla ennalta tuttuja. Näin ollen käsittelyyn ei käytetä paljoa aikaa, eikä tulosten yhteydessä esitetä juurikaan esimerkkejä. Lähteinä alaluvussa 2.1 on käytetty Bhattacharyan, Jainin ja Nagpaulin teosta *Basic Abstract Algebra* [1], Eien ja Changin teosta *A Course on Abstract Algebra* [2], Rosen teosta *A Course on Group Theory* [4] sekä Scottin teosta *Group Theory* [6].

Alaluvussa 2.2 esitellään Ω-ryhmien käsite ja niihin liittyviä perustuloksia, joiden ei oleteta olevan lukijalle ennalta tuttuja. Ω-ryhmät tulevat olemaan merkittävässä roolissä päälauseen todistuksessa. Tämän alaluvun lähteinä on käytetty Rosen teoksen *A Course on Group Theory* [4] sivuja 22 ja 137-138 sekä Rotmanin teoksen *An Introduction to the Theory of Groups* [5] sivua 151 .

2.1 Ryhmäteorian kertausta

Aloitetaan kertaamalla ryhmäteorian perustkäsitteitä, kuten ryhmä, aliryhmä ja normaali aliryhmä.

Määritelmä 2.1. *Puoliryhmä* on epätyhjä joukko varustettuna liitännäisellä laskutoimituksella. *Ryhmä* on puoliryhmä, jolla on neutraalialkio, ja jonka jokaisella alkiolla on käänteisalkio. Vain neutraalialkion sisältävää ryhmää kutsutaan *triviaaliksi* ryhmäksi. Jos ryhmä ei ole triviaali, sitä kutsutaan *epätriviaaliksi*. Jatkossa merkitään ryhmän neutraalialkiota symbolilla 1 ja ryhmän alkion g käänteisalkiota symbolilla g^{-1}.

Määritelmä 2.2. Ryhmä G on *äärellinen*, jos se sisältää äärellisen määrän alkioita. Ryhmän G sisältämien alkioiden lukumäärää kutsutaan ryhmän G *kertaluvuksi* ja tätä merkitään $|G|$.

Määritelmä 2.3. Ryhmän G *aliryhmä* on joukon G epätyhjä osajoukko, joka varustettuna alkuperäisen ryhmän G laskutoimituksella, rajoitettuna joukkoon H, muodostaa ryhmän. Jos H on ryhmän G aliryhmä, niin merkitään $H \leq G$. Ryhmän G aliryhmä H on *aito* aliryhmä, jos $H \neq G$.

Lause 2.4. *Epätyhjä ryhmän G osajoukko H on ryhmän G aliryhmä, jos ja vain jos $h_1 h_2^{-1} \in H$ pätee, kun $h_1, h_2 \in H$.*

Apulause 2.5. *Olkoot H ja K ryhmän G aliryhmiä. Tällöin myös $H \cap K$ on ryhmän G aliryhmä.*

Määritelmä 2.6. Olkoon H ryhmän G aliryhmä. Tällöin H on ryhmän G *normaali aliryhmä*, merkitään $H \trianglelefteq G$, jos ja vain jos $g^{-1}hg \in H$ pätee, kun $h \in H$ ja $g \in G$.

Esimerkki 2.7. Olkoon G ryhmä. Triviaali ryhmä $\{1\}$ on ryhmän G aliryhmä, sillä neutraalialkion käänteisalkio on neutraalialkio ja kahden neutraalialkion tulo on neutraalialkio. Lisäksi $\{1\}$ on normaali, sillä $g^{-1}1g = 1 \in \{1\}$ pätee, kun $g \in G$.

Seuraava esimerkki osoittaa, että Abelin ryhmän aliryhmä on aina normaali.

Esimerkki 2.8. Olkoon H Abelin ryhmän G aliryhmä. Tällöin, koska G on Abelin ryhmä, niin $g^{-1}hg = g^{-1}gh = h \in H$ pätee, kun $g \in G$ ja $h \in H$. Täten $H \trianglelefteq G$.

Määritelmä 2.9. Olkoon G ryhmä. Tällöin G on *yksinkertainen*, jos sen ainoat normaalit aliryhmät ovat G ja triviaali aliryhmä $\{1\}$.

Apulause 2.10. *Olkoon K ryhmän G normaali aliryhmä ja $K \leq H \leq G$. Tällöin K on ryhmän H normaali aliryhmä.*

Apulause 2.11. *Olkoon H ryhmän G aliryhmä ja K ryhmän G normaali aliryhmä. Tällöin HK on ryhmän G aliryhmä.*

Apulause 2.12. *Olkoot H ja K ryhmän G aliryhmiä. Tällöin HK on ryhmän G aliryhmä, jos ja vain jos $HK = KH$.*

Apulause 2.13. *Olkoot H ja K ryhmän G normaaleja aliryhmiä. Tällöin, jos $H \cap K$ sisältää vain ryhmän G neutraalialkion 1, niin jokainen ryhmän H alkio kommutoi jokaisen ryhmän K alkion kanssa.*

Määritelmä 2.14. Olkoon H ryhmän G aliryhmä ja olkoon $g \in G$. Tällöin joukko

$$gH = \{gh \mid h \in H\}$$

on alkion g määräämä aliryhmän H *vasen sivuluokka*.

Määritelmä 2.15. Olkoon K ryhmän G normaali aliryhmä. Tällöin kaikkien ryhmän G aliryhmän K vasempien sivuluokkien joukko, merkitään G/K, varustettuna laskutoimituksella

$$(g_1K)(g_2K) = g_1g_2K,$$

kun $g_1, g_2 \in G$, muodostaa ryhmän G *tekijäryhmän*.

Lause 2.16. *Olkoon K ryhmän G normaali aliryhmä. Tällöin tekijäryhmä G/K on ryhmä.*

Esitellään tämän alaluvun lopuksi oleellisimpia kuvauksiin ja homomorfismeihin liittyviä käsitteitä ja tuloksia, joita tullaan tarvitsemaan jatkossa.

Määritelmä 2.17. Epätyhjän joukon X *Identtinen* kuvaus, merkitään I_X, on kuvaus, joka kuvaa kaikki joukon X alkiot itselleen. Jos joukko X on asiayhteydestä selvä, merkitään joukon X identtistä kuvausta symbolilla I.

Määritelmä 2.18. Olkoon $\phi\colon X \to Y$ ja olkoon joukko S joukon X osajoukko. Tällöin kuvausta $\psi\colon S \to Y$, jolle pätee ehto $s \mapsto \phi(s)$, kutsutaan kuvauksen ϕ *rajoittumaksi* joukon X osajoukkoon S. Tätä rajoittumaa ψ merkitään yleensä $\phi|S$.

Määritelmä 2.19. Olkoon epätyhjä joukko S joukon X osajoukko. Tällöin joukon X identtisen kuvauksen rajoittuma joukkoon S eli rajoittuma $I_X|S\colon S \to X$ on joukon S *inkluusio* joukolle X.

Esimerkki 2.20. Rationaalilukujen joukon inkluusio kokonaislukujen joukolle on kuvaus $I_{\mathbb{Q}}|\mathbb{Z}\colon \mathbb{Z} \to \mathbb{Q}$.

Määritelmä 2.21. Olkoot G ja H ryhmiä. Kuvaus $\phi\colon G \to H$ on *homomorfismi*, jos

$$\phi(ab) = \phi(a)\phi(b)$$

pätee, kun $a, b \in G$.

Homomorfismi, joka kuvaa kaikki alkiot neutraalialkiolle, on *triviaali homomorfismi*, homomorfismi ryhmältä G itselleen on ryhmän G *endomorfismi* ja bijektiivinen endomorfismi on *automorfismi*. Ryhmän G automorfismia merkitään $\operatorname{Aut} G$.

Esimerkki 2.22. Kaikki kuvauksen ϕ rajoittumat ovat selvästi homomorfismeja, jos ϕ on homomorfismi.

Apulause 2.23. *Olkoot kuvaukset $\phi\colon K \to H$ ja $\psi\colon G \to K$ homomorfismeja. Tällöin yhdistetty kuvaus $\phi\psi\colon G \to H$ on myös homomorfismi.*

Todistus. Olkoot $a, b \in G$. Tällöin

$$\phi\psi(ab) = \phi\big(\psi(a)\psi(b)\big),$$

sillä ψ on homomorfismi ryhmältä G ryhmälle K. Edelleen, koska ϕ on homomorfismi ryhmältä K ryhmälle G,

$$\phi\big(\psi(a)\psi(b)\big) = \phi\psi(a)\phi\psi(b).$$

Näin ollen on osoitettu, että

$$\phi\psi(ab) = \phi\psi(a)\phi\psi(b)$$

pätee, kun $a, b \in G$. □

Määritelmä 2.24. Olkoon kuvaus $\phi\colon G \to H$ homomorfismi. Tällöin kuvauksen ϕ ne alkiot, jotka kuvautuvat maaliryhmän neutraalialkiolle muodostavat kuvauksen ϕ *ytimen*. Kuvauksen ϕ ydintä merkitään $\operatorname{Ker}\phi$. Kuvauksen ϕ ne maalijoukon alkiot, jotka kuvaus voi saada arvonaan muodostavat kuvauksen ϕ *kuvajoukon*. Kuvauksen ϕ kuvajoukkoa merkitään $\operatorname{Im}\phi$.

Apulause 2.25. *Olkoon $\phi\colon G \to H$ homomorfismi. Homomorfismin ydin on ryhmän G normaali aliryhmä ja homomorfismin kuvajoukko on ryhmän H aliryhmä.*

Esitellään vielä lopuksi homomorfialause ja toinen isomorfialause, joita kumpaakin tarvitaan pääluvun 5 tuloksien todistamisessa.

Lause 2.26 (Homomorfialause)**.** *Olkoon $\phi\colon G \to H$ homomorfismi. Tällöin*

$$\operatorname{Im}\ \phi \cong G/\operatorname{Ker}\phi.$$

Lause 2.27 (Toinen isomorfialause)**.** *Olkoon H ryhmän G aliryhmä ja K ryhmän G normaali aliryhmä. Tällöin $H \cap K$ on ryhmän H normaali aliryhmä ja $H/(H \cap K) \cong HK/K$.*

2.2 Ω-ryhmät

Seuraavaksi käsitellään tämän tutkielman luvussa 5 paljon käytettyjen Ω-ryhmän ja Ω-homomorfismin käsitteet, jotka helpottavat päälauseen todistusta oleellisesti. Aloitetaan kuitenkin ensin kertaamalla konjugaatin ja konjugaation käsitteet, joita tarvitaan esimerkissä 2.32.

Lause 2.28. *Olkoon G ryhmä. Jokaiseen $g \in G$ voidaan liittää ryhmän G automorfismi τ_g, joka on määritelty seuraavasti:*

$$\tau_g \colon x \mapsto g^{-1}xg,$$

kun $x \in G$.

Määritelmä 2.29. Alkiota $\tau_g(x) = g^{-1}xg$ kutsutaan *alkion g määräämäksi alkion x konjugaatiksi*. Ryhmän G automorfismia τ_g kutsutaan *alkion g määräämäksi ryhmän G konjugaatioksi*.

Määritelmä 2.30. Olkoon Ω joukko ja G ryhmä. Tällöin Ω on ryhmän G *operaattorialue* ja G on Ω-*ryhmä*, jos on olemassa kuvaus $\Omega \times G \to G$, merkitään $(\omega, g) \mapsto g^\omega$, jolle pätee

$$(g_1 g_2)^\omega = g_1^\omega g_2^\omega,$$

kun $\omega \in \Omega$ ja $g_1, g_2 \in G$.

Selvästi Ω-ryhmän ja endomorfismin määritelmistä seuraa, että mikä tahansa ryhmän G endomorfismien joukko kelpaa ryhmän G operaattorialueeksi.

Määritelmä 2.31. Olkoon G Ω-ryhmä ja H ryhmän G aliryhmä. Tällöin sanotaan, että H on Ω-*aliryhmä*, jos $h^\omega \in H$ pätee, kun $h \in H$ ja $\omega \in \Omega$.

Huomattakoon, että jos H on ryhmän G Ω-aliryhmä, niin Ω on myös ryhmän H operaattorialue.

Esimerkki 2.32. Olkoon G ryhmä. Kuvaus $G \times G \to G$ ehdolla $(\omega, g) \mapsto g^\omega$, missä $g^\omega = \omega^{-1}g\omega$, täyttää määritelmän 2.30 ehdot, sillä konjugaatiot ovat endomorfismeja. Toisin sanoen G on G-ryhmä.

Tämän G-ryhmän G-aliryhmät ovat ryhmän G normaaleja aliryhmiä, sillä kun H on G-aliryhmä, niin määritelmän 2.31 nojalla $g^{-1}hg = h^g \in H$ pätee, kun $g \in G$ ja $h \in H$.

Ylläoleva esimerkki on jatkokäsittelyä varten hyvin oleellisessa roolissa, sillä pääluvussa käsiteltävät ryhmän G Ω-ryhmät ovat lähes poikkeuksetta edellisen esimerkin mukaisia G-ryhmiä.

Määritelmä 2.33. Olkoot G ja H ryhmiä, joilla on sama operaattorialue Ω. Tällöin homomorfismia ϕ ryhmältä G ryhmälle H kutsutaan Ω-*homomorfismiksi*, jos

$$\phi(g^\omega) = (\phi(g))^\omega$$

pätee, kun $g \in G$ ja $\omega \in \Omega$.

Vastaavan ehdon toteuttavaa endomorfismia kutsutaan Ω-*endomorfismiksi.*

Apulause 2.34. *Olkoon ϕ ryhmän G Ω-homomorfismi. Tällöin* $\operatorname{Im}\phi$ *on Ω-aliryhmä.*

Todistus. Apulauseen 2.25 nojalla $\operatorname{Im}\phi \leq G$ ja

$$\Big(\phi(g)\Big)^{\omega} = \phi(g^{\omega}) \in \operatorname{Im}\phi.$$

pätee, kun $\phi(g) \in \operatorname{Im}\phi$ ja $\omega \in \Omega$. Näin ollen väite on todistettu. □

Esimerkki 2.35. Triviaalisti mielivaltaisen ryhmän G operaattorialueena voidaan ajatella olevan $\Omega = \emptyset$, jolloin G on Ω-ryhmä. Tällöin kaikki ryhmän G aliryhmät ovat myös Ω-aliryhmiä.

Apulause 2.36. *Olkoot kuvaukset $\phi\colon K \to H$ ja $\psi\colon G \to K$ Ω-homomorfismeja. Tällöin myös yhdistetty kuvaus $\phi\psi\colon G \to H$ on Ω-homomorfismi.*

Todistus. Määritelmän 2.33 nojalla kuvaukset ϕ ja ψ ovat homomorfismeja. Täten apulauseen 2.23 nojalla myös yhdistetty kuvaus $\phi\psi$ on homomorfismi. Nyt

$$\phi\psi(g^{\omega}) = \phi\big((\psi(g^{\omega})\big) = \phi\Big(\big((\psi(g)\big)^{\omega}\Big) = \big(\phi\psi(g)\big)^{\omega}$$

pätee, kun $g \in G$ ja $\omega \in \Omega$, sillä ψ on Ω-homomorfismi ryhmältä G ryhmälle H ja ϕ on Ω-homomorfismi ryhmältä K ryhmälle H. □

Apulause 2.37. *Jos ϕ on ryhmän G Ω-endomorfismi, niin kaikilla positiivisilla kokonaisluvuilla k myös ϕ^k on Ω-endomorfismi.*

Todistus. Väite seuraa apulauseesta 2.36. □

Esimerkki 2.32 osoittaa, että ryhmä G on aina myös G-ryhmä. Jatkossa viitataan lähinnä esimerkin mukaisiin G-ryhmiin, joten on luontevaa sopia, että merkinnällä g^{ω} tarkoitetaan tsätä eteenpäin yksinomaan alkion ω määräämää alkion g konjugaattia eli $g^{\omega} = \omega^{-1}g\omega$. Jatkossa puhuttaessa G-endomorfismista, viitataan aina ryhmän G G-endomorfismiin. Jos kyseessä ei ole ryhmän G G-endomorfismi, niin asia mainitaan erikseen.

3 Ryhmien suorat tulot

Tässä luvussa esitellään määritelmät ryhmien ulkoiselle ja sisäiselle suoralle tulolle, sekä esitellään muutama suoria tuloja koskeva tulos. Lukijan oletetaan tuntevan suoria tuloja koskevat perustulokset, joten näiden todistukset ohitetaan. Lähteenä on käytetty tämän tutkielman tekijän omaa kandidaatintutkielmaa *Ryhmien suorat tulot* [3], ellei toisin mainita.

Määritelmä 3.1. Olkoot $G_1, G_2, \ldots, G_n$ ryhmiä, missä n on positiivinen kokonaisluku. Tällöin ryhmien $G_1, G_2, \ldots, G_n$ *ulkoinen suora tulo*, merkitään $G_1 \times G_2 \times \cdots \times G_n$, on joukko $\{ (g_1, g_2, \ldots, g_n) \mid g_i \in G_i, i \in \{1, 2, \ldots, n\} \}$ varustettuna laskutoimituksella

$$(g_1, g_2, \ldots, g_n)(g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2 g_2', \ldots, g_n g_n').$$

Lause 3.2. *Ryhmien $G_1, G_2, \ldots, G_n$, missä n on positiivinen kokonaisluku, ulkoinen suora tulo $G_1 \times G_2 \times \cdots \times G_n$ on ryhmä.*

Apulause 3.3. *Olkoon G ryhmä. Tällöin*

$$(g_1 g_2 \cdots g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}$$

pätee, kun $g_1, g_2, \ldots, g_n \in G$.

Määritelmä 3.4. Olkoot $G_1, G_2, \ldots, G_n$, missä n on positiivinen kokonaisluku, ryhmän G normaaleja aliryhmiä. Tällöin G on ryhmien $G_1, G_2, \ldots, G_n$ *sisäinen suora tulo*, jos jokaiselle alkiolle $g \in G$ on olemassa yksikäsitteinen esitys

$$g = g_1 g_2 \cdots g_n,$$

missä $g_i \in G_i$, kun $i \in \{1, 2, \ldots, n\}$.

Lause 3.5. *Olkoot $G_1, G_2, \ldots, G_n$ ryhmän G normaaleja aliryhmiä, missä n on positiivinen kokonaisluku. Tällöin G on ryhmien $G_1, G_2, \ldots, G_n$ sisäinen suora tulo, jos ja vain jos*

$$G = G_1 G_2 \cdots G_n$$

ja

$$G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_n) = \{1\},$$

kun $i \in \{1, 2, \ldots, n\}$.

Esimerkki 3.6 (ks. [1, s. 140, harj. 1])**.** Osoitetaan, että yhteenlaskuryhmä $\mathbb{Z}_{10}$ on normaalien aliryhmiensä $H = \{\overline{0}, \overline{5}\}$ ja $K = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$ sisäinen suora tulo.

Ratkaisu. Ensinnäkin H ja K ovat selvästi ryhmän $\mathbb{Z}_{10}$ normaaleja aliryhmiä, joiden leikkaus $H \cap K$ sisältää vain ryhmän $\mathbb{Z}_{10}$ neutraalialkion $\overline{0}$. Lisäksi

$$\begin{aligned} HK &= \{\overline{0+0}, \overline{0+2}, \overline{0+4}, \overline{0+6}, \overline{0+8}, \overline{5+0}, \overline{5+2}, \overline{5+4}, \overline{5+6}, \overline{5+8}\} \\ &= \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}\} = \mathbb{Z}_{10}. \end{aligned}$$

Näin ollen lauseen 3.5 nojalla väite on tosi.

Seuraava lause osoittaa, että sisäinen suora tulo on isomorfinen ulkoisen suoran tulon kanssa.

Lause 3.7. *Olkoot $G_1, G_2, \ldots, G_n$ ryhmän G normaaleja aliryhmiä, missä n positiivinen kokonaisluku. Tällöin, jos G on normaalien aliryhmiensä $G_1, G_2, \ldots, G_n$ sisäinen suora tulo, niin G on isomorfinen ryhmien $G_1, G_2, \ldots, G_n$ muodostaman ulkoisen suoran tulon kanssa, eli*

$$G \cong G_1 \times G_2 \times \cdots \times G_n.$$

Tehdään seuraavaksi edellisen lauseen mahdollistama merkinnällinen sopimus, jolla yksinkertaistetaan jatkokäsittelyä. Edellisen lauseen nojalla jos G on normaalien aliryhmiensä $G_1, G_2, \ldots, G_n$, missä n on positiivinen kokonaisluku, muodostama sisäinen suora tulo, niin se on isomorfinen ullkoisen suoran tulon $G_1 \times G_2 \times \cdots \times G_n$ kanssa. Näin ollen sovitaan, että jatkossa merkinnällä $G = G_1 \times G_2 \times \cdots \times G_n$ tarkoitetaan ryhmän G olevan normaalien aliryhmiensä $G_1, G_2, \ldots, G_n$ muodostama sisäinen suora tulo, ellei toisin mainita. Jatkossa puhuttaessa suorasta tulosta viitataan sisäiseen suoraan tuloon.

Esimerkki 3.8. Olkoon G ryhmä. Koska $\{1\} \trianglelefteq G$, $G \trianglelefteq G$ ja $g = g1$ pätee, kun $g \in G$, niin määritelmän 3.4 nojalla $G = G \times \{1\}$.

Apulause 3.9. *Olkoon $G = G_1 \times G_2 \times \cdots \times G_n$. Tällöin ryhmien G_i ja G_j alkiot kommutoivat keskenään, kun $i, j \in \{1, 2, \ldots, n\}$ ja $i \neq j$.*

Todistus. Lauseesta 3.5 seuraa, että $G_i \cap G_j = \{1\}$ pätee, kun $i, j \in \{1, 2, \ldots, n\}$ ja $i \neq j$. Lisäksi, koska $G = G_1 \times G_2 \times \cdots \times G_n$, niin G_i ja G_j ovat molemmat ryhmän G normaaleja aliryhmiä. Näin ollen väite seuraa apulauseesta 2.13. □

Apulause 3.10. *Olkoon $G = H \times K$. Tällöin $H \times K = K \times H$.*

Todistus. Määritelmän 3.4 nojalla ryhmät H ja K ovat ryhmän G normaaleja aliryhmiä ja jokaiselle alkiolle $g \in G$ on olemassa yksikäsitteinen esitys $g = hk$, missä $h \in H$ ja $k \in K$. Apulauseen 3.9 nojalla $hk = kh$ pätee, kun $h \in H$ ja $k \in K$. Täten jokaiselle alkiolle $g \in G$ on olemassa yksikäsitteinen esitys $g = kh$, missä $h \in H$ ja $k \in K$. Näin ollen $G = K \times H$. □

Apulauseesta 3.10 seuraa, että suora tulo $G = G_1 \times G_2 \times \cdots \times G_n$, missä n on positiviinen kokonaisluku, on riippumaton tekijöidensä järjestyksestä. Määritellään seuraavaksi hajoava ryhmä ja esitellään tästä muutama havainnollistava esimerkki.

Määritelmä 3.11 (ks. [6, s. 67])**.** Olkoon G ryhmä. Ryhmä G on *hajoava*, jos ryhmällä G on olemassa epätriviaalit normaalit aliryhmät H ja K, joille $G = H \times K$. Hajoavan ryhmän G esitystä normaalien aliryhmiensä suorana tulona kutsutaan ryhmän G *hajotelmaksi*.

Jos ryhmä G ei ole hajoava, niin se on *hajoamaton*.

Esimerkki 3.12. Jos ryhmä G on yksinkertainen, niin yksinkertaisen ryhmän määritelmän 2.9 nojalla sen ainoat normaalit aliryhmät ovat G ja triviaali ryhmä $\{1\}$. Näin ollen kaikki yksinkertaiset ryhmät ovat hajoamattomia.

Esimerkki 3.13. Esimerkin 3.6 nojalla yhteenlaskuryhmä $\mathbb{Z}_{10}$ on hajoava ryhmä.

Esimerkki 3.14. Osoitetaan, että kokonaislukujen yhteenlaskuryhmä $\mathbb{Z}$ on hajoamaton.

Ratkaisu. Kokonaislukujen yhteenlaskuryhmä on syklinen, joten myös jokainen tämän ryhmän aliryhmä on syklinen. Täten kokonaislukujen yhteenlaskuryhmän epätriviaalit aliryhmät ovat muotoa $d\mathbb{Z} = \{dz \mid z \in \mathbb{Z}\}$, missä d on positiivinen kokonaisluku. Olkoot nyt $m\mathbb{Z}$ ja $n\mathbb{Z}$ kokonaislukujen yhteenlaskuryhmän epätriviaaleja normaaleja aliryhmiä. Jos $m = 1$ tai $n = 1$, niin selvästi $m\mathbb{Z} \cap n\mathbb{Z} \neq \{1\}$. Oletetaan nyt, että $m \neq 1$ ja $n \neq 1$. Tällöin tulo $mn > 1$ on positiivinen kokonaisluku. Koska $mn \in m\mathbb{Z}$, $nm \in n\mathbb{Z}$ ja $mn = nm$, niin $mn \in m\mathbb{Z} \cap n\mathbb{Z}$. Täten $m\mathbb{Z} \cap n\mathbb{Z} \neq \{1\}$. Näin ollen lauseen 3.5 nojalla $\mathbb{Z} \neq m\mathbb{Z} \times n\mathbb{Z}$. Täten $\mathbb{Z}$ on hajoamaton.

Apulausetta 3.16 tullaan tarvitsemaan päälauseen todistuksen apuna. Ennen tämän lauseen todistusta esitetään vielä todistuksen apuna käytettävä Dedekindin sääntö.

Apulause 3.15 (Dedekindin sääntö, ks. [4, s. 122])**.** *Olkoot J, H, K ryhmän G aliryhmiä joille $H \leq J$. Tällöin*

$$J \cap (HK) = H(J \cap K).$$

Todistus. Selvästi $H(J \cap K) \subseteq J \cap (HK)$, sillä H on ryhmän J aliryhmä. Olkoon $j \in J \cap (HK)$. Tällöin joillakin $h \in H$ ja $k \in K$ pätee $j = hk$. Tällöin, koska H on ryhmän J aliryhmä, niin $h^{-1}j = k \in J \cap K$. Täten $j \in H(J \cap K)$. Siispä $J \cap (HK) \subseteq H(J \cap K)$. Näin ollen on osoitettu, että

$$J \cap (HK) = H(J \cap K).$$

□

Apulause 3.16 (ks. [4, s. 167, harj. 402])**.** *Olkoon ryhmä G normaalien aliryhmiensä H ja K hajotelma eli $G = H \times K$, missä H ja K ovat ryhmän G epätriviaaleja normaaleja aliryhmiä. Tällöin, jos $H \leq J \leq G$, niin*

$$J = H \times (J \cap K).$$

Todistus. Ensinnäkin

$$H \cap (J \cap K) = \{1\},$$

sillä triviaalisti $1 \in J \cap K$ ja oletuksen nojalla $H \cap K = \{1\}$. Toisekseen, koska $G = HK$, niin Dedekindin säännön nojalla saadaan

$$J = J \cap G = J \cap (HK) = H(J \cap K).$$

Osoitetaan seuraavaksi, että H ja $J \cap K$ ovat ryhmän J normaaleja aliryhmiä.

Koska $H \trianglelefteq G$ ja $H \leq J \leq G$, niin apulauseen 2.10 nojalla

$$H \trianglelefteq J.$$

$J \cap K$ on ryhmän J epätyhjä osajoukko. Ryhminä J ja K ovat molemmat laskutoimituksensa suhteen suljettuja ja näin ollen myös joukko $J \cap K$ on saman laskutoimituksen suhteen suljettu. Näin ollen

$$J \cap K \leq J.$$

Osoitetaan vielä, että $J \cap K$ on ryhmän J normaali aliryhmä.

Apulauseen 3.9 nojalla kaikki ryhmien H ja K alkiot kommutoivat keskenään. Olkoon $j \in J$ ja $k \in J \cap K$. Koska $J = H(J \cap K)$, niin $j = hi$ joillakin $h \in H$ ja $i \in J \cap K$. Näin ollen saadaan

$$j^{-1}kj = (hi)^{-1}khi = i^{-1}h^{-1}khi = i^{-1}h^{-1}hki = i^{-1}ki \in J \cap K.$$

Täten

$$J \cap K \trianglelefteq J.$$

On siis osoitettu, että H ja $J \cap K$ ovat ryhmän J sellaisia normaaleja aliryhmiä, että $J = H(J \cap K)$ ja $H \cap (J \cap K) = \{1\}$. Näin ollen lauseen 3.5 nojalla

$$J = H \times (J \cap K).$$

□

4 Keskus

Tässä luvussa esitellään keskuksen ja keskittäjän määritelmät ja niitä koskevia perustuloksia. Tutkielman päälause rajoittuu tarkastelemaan tapausta, jossa ryhmän keskus on triviaali, joten keskusta koskeva oletus on keskeisessä roolissa päälauseen todistuksessa.

Määritelmä 4.1 (ks. [1, s. 73])**.** Olkoon G ryhmä. Tällöin ryhmän G *keskus*, merkitään $Z(G)$, on niiden ryhmän G alkioiden joukko, jotka kommutoivat kaikkien ryhmän G alkioiden kanssa eli

$$Z(G) = \{g \in G \mid gx = xg, \text{ kun } x \in G\}.$$

Lause 4.2. *Olkoon G ryhmä. Tällöin ryhmän G keskus $Z(G)$ on ryhmän G normaali aliryhmä.*

Todistus (vrt. [1, s. 73]). Ryhmän G neutraalialkiolle 1 pätee aina

$$1g = g = g1,$$

kun $g \in G$. Täten $1 \in Z(G)$ ja näin ollen $Z(G)$ on ryhmän G epätyhjä osajoukko. Olkoot $a, b \in Z(G)$. Tällöin

$$ab^{-1}g = ab^{-1}g1 = ab^{-1}gbb^{-1} = ab^{-1}bgb^{-1} = a1gb^{-1} = agb^{-1} = gab^{-1}$$

pätee, kun $g \in G$. Siispä $ab^{-1} \in Z(G)$. Näin ollen $Z(G)$ on lauseen 2.4 nojalla ryhmän G aliryhmä. Lisäksi

$$g^{-1}hg = g^{-1}gh = 1h = h \in Z(G)$$

pätee, kun $g \in G$ ja $h \in Z(G)$, joten $Z(G)$ on ryhmän G normaali aliryhmä. □

Esitetään vielä esimerkki, joka havainnollistaa keskuksen ja Abelin ryhmän välistä yhteyttä.

Lause 4.3 (vrt. [2, s. 48, harj. 6])**.** *Olkoon G ryhmä. Tällöin:*

1. *G on Abelin ryhmä, jos ja vain jos $Z(G) = G$.*
2. *$Z(G)$ on Abelin ryhmä.*

Todistus. Todistetaan kumpikin kohta erikseen.

1. Oletetaan, että $Z(G) = G$. Tällöin kaikilla $x, g \in G$ pätee keskuksen määritelmän nojalla

$$gx = xg.$$

Näin ollen G on Abelin ryhmä.

Oletetaan nyt, että G on Abelin ryhmä ja $x \in G$. Täten

$$gx = xg$$

pätee, kun $g \in G$. Siispä $x \in Z(G)$ ja näin ollen $G \subseteq Z(G)$. Lisäksi triviaalisti keskuksen määritelmän nojalla $Z(G) \subseteq G$. Näin ollen on oltava $Z(G) = G$.

2. Todistetaan seuraavaksi esimerkin toinen kohta. Olkoon $Z(G)$ jonkin mielivaltaisen ryhmän G keskus. Lauseen 4.2 nojalla $Z(G)$ on ryhmän G aliryhmänä itsessään ryhmä. Olkoot $x, g \in Z(G)$. Keskuksen määritelmän nojalla erityisesti $g \in G$, joten $gx = xg$ pätee. Alkiot x ja g olivat mielivaltaisesti valittuja, joten $Z(G)$ on Abelin ryhmä.

□

Määritelmä 4.4 (vrt. [4, s. 48, harj. 122])**.** Olkoon H ryhmän G aliryhmä. Tällöin aliryhmän H *keskittäjä* ryhmässä G, merkitään $C_G(H)$, on niiden ryhmän G alkioiden joukko, jotka kommutoivat kaikkien aliryhmän H alkioiden kanssa eli

$$C_G(H) = \{g \in G \mid gh = hg, \text{ kun } h \in H\}.$$

Huomattakoon, että edellä olevan määritelmän nojalla

$$C_G(G) = Z(G).$$

Lause 4.5 (vrt. [4, s. 48, harj. 122])**.** *Olkoon H ryhmän G aliryhmä. Tällöin aliryhmän H keskittäjä ryhmässä G on ryhmän G aliryhmä.*

Todistus. Koska neutraalialkio $1 \in G$ ja $H \subseteq G$, niin

$$1h = h = h1$$

pätee, kun $h \in H$. Täten $1 \in C_G(H)$. Olkoot $a, b \in C_G(H)$. Tällöin

$$ab^{-1}h = ab^{-1}h1 = ab^{-1}hbb^{-1} = ab^{-1}bhb^{-1} = a1hb^{-1} = ahb^{-1} = hab^{-1}$$

pätee, kun $h \in H$. Siispä $ab^{-1} \in C_G(H)$. Näin ollen $C_G(H)$ on ryhmän G aliryhmä.

□

Aliryhmä $C_G(H)$ ei kuitenkaan välttämättä ole ryhmän G normaali aliryhmä.

Esimerkki 4.6. Tarkastellaan symmetristä ryhmää $\Sigma_3 = \{1, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$ ja sen aliryhmiä $K = \{1, (1\,2\,3), (1\,3\,2)\}$ ja $H = \{1, (1\,2)\}$.

Nyt

$$(1\,2) \circ (1\,3) = (1\,3\,2) \neq (1\,2\,3) = (1\,3) \circ (1\,2),$$
$$(1\,2) \circ (2\,3) = (1\,2\,3) \neq (1\,3\,2) = (2\,3) \circ (1\,2),$$
$$(1\,2) \circ (1\,2\,3) = (2\,3) \neq (1\,3) = (1\,2\,3) \circ (1\,2),$$
$$(1\,2) \circ (1\,3\,2) = (1\,3) \neq (2\,3) = (1\,3\,2) \circ (1\,2),$$
$$(1\,3) \circ (1\,2\,3) = (1\,2) \neq (2\,3) = (1\,2\,3) \circ (1\,3),$$

$$(2\ 3) \circ (1\ 3\ 2) = (1\ 2) \neq (1\ 3) = (1\ 3\ 2) \circ (2\ 3)$$

ja

$$(1\ 2\ 3) \circ (1\ 3\ 2) = 1 = (1\ 3\ 2) \circ (1\ 2\ 3).$$

Lisäksi $1\sigma = \sigma = \sigma 1$, kun $\sigma \in \Sigma_3$.

Näin ollen

$$C_{\Sigma_3}(K) = \{1, (1\ 2\ 3), (1\ 3\ 2)\} = K,$$
$$C_{\Sigma_3}(H) = \{1, (1\ 2)\} = H$$

ja

$$Z(\Sigma_3) = \{1\}.$$

$C_{\Sigma_3}(K)$ on ryhmän Σ_3 normaali aliryhmä, mutta $C_{\Sigma_3}(H)$ ei ole ryhmän Σ_3 normaali aliryhmä.

Esitetään vielä luvun loppuun kaksi apulausetta, joita käytetään päälauseen todistamisen yhteydessä.

Apulause 4.7. *Olkoon H ryhmän G aliryhmä. Tällöin*

$$H \cap C_G(H) = Z(H).$$

Todistus.

$$\begin{aligned} Z(H) &= \{g \in H \mid gh = hg, \text{ kun } h \in H\} \\ &= \{g \in G \mid g \in H \text{ ja } gh = hg, \text{ kun } h \in H\} \\ &= \{g \in G \mid g \in H\} \cap \{g \in G \mid gh = hg, \text{ kun } h \in H\} \\ &= H \cap C_G(H). \end{aligned}$$

□

Apulause 4.8 (vrt. [4, s. 167, harj. 406])**.** *Olkoon $G = G_1 \times G_2 \times \cdots \times G_n$, missä n on positiivinen kokonaisluku. Tällöin $Z(G) = Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n)$.*

Todistus. Ensinnäkin $Z(G_i)$ on ryhmän $Z(G)$ normaali aliryhmä, kun $i \in \{1, 2, \ldots, n\}$, sillä $Z(G)$ on Abelin ryhmä. Oletuksen nojalla $G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_n) = \{1\}$ ja täten myös $Z(G_i) \cap \big(Z(G_1) \cdots Z(G_{i-1}) Z(G_{i+1}) \cdots Z(G_n)\big) = \{1\}$, kun $i \in \{1, 2, \ldots, n\}$. Väite seuraa lauseesta 3.5, kunhan ensin todistetaan, että $Z(G) = Z(G_1)Z(G_2) \cdots Z(G_n)$. Oletetaan koko todistuksen ajan, että $g = g_1 g_2 \cdots g_n \in G$, missä $g_i \in G_i$, kun $i \in \{1, 2, \ldots, n\}$.

Oletetaan ensin, että $z_i \in Z(G_i)$, kun $i \in \{1, 2, \ldots, n\}$. Täten

$$z_1 z_2 \cdots z_n \in Z(G_1)Z(G_2) \cdots Z(G_n).$$

Ensinnäkin kaikki ryhmien G_i ja G_j alkiot kommutoivat, kun $i, j \in \{1, 2, \ldots, n\}$ ja $i \neq j$. Lisäksi oletuksen nojalla kaikilla $i \in \{1, 2, \ldots, n\}$ pätee $z_i g_i = g_i z_i$. Täten saadaan

$$\begin{aligned} &(z_1 z_2 \cdots z_n)(g_1 g_2 \cdots g_n) \\ &= z_1 g_1 z_2 g_2 \cdots z_n g_n = g_1 z_1 g_2 z_2 \cdots g_n z_n \\ &= (g_1 g_2 \cdots g_n)(z_1 z_2 \cdots z_n). \end{aligned}$$

Siispä $z_1 z_2 \cdots z_n \in Z(G)$. Täten on osoitettu, että $Z(G_1)Z(G_2)\cdots Z(G_n) \subseteq Z(G)$.

Oletetaan nyt, että $z \in Z(G)$. Erityisesti $z \in G$ ja näin ollen joillakin $z_i \in G_i$, missä $i \in \{1, 2, \ldots, n\}$, pätee $z = z_1 z_2 \cdots z_n$. Koska $z \in Z(G)$, niin $zg_i = g_i z$ eli

$$(z_1 z_2 \cdots z_n)(g_i) = (g_i)(z_1 z_2 \cdots z_n)$$

pätee, kun $g \in G_i \subseteq G$, missä $i \in \{1, 2, \ldots, n\}$. Koska suoran tulon eri tekijöiden alkiot kommutoivat keskenään, niin edellisestä yhtälöstä seuraa

$$(z_i g_i) z_1 z_2 \cdots z_{i-1} z_{i+1} \cdots z_n = (g_i z_i) z_1 z_2 \cdots z_{i-1} z_{i+1} \cdots z_n.$$

Edelleen tästä seuraa

$$z_i g_i = g_i z_i.$$

Täten kaikilla $i \in \{1, 2, \ldots, n\}$ pätee $z_i \in Z(G_i)$ ja näin ollen $z = z_1 z_2 \cdots z_n \in Z(G_1)Z(G_2)\cdots Z(G_n)$. Näin on osoitettu, että $Z(G) \subseteq Z(G_1)Z(G_2)\cdots Z(G_n)$. Täten on osoitettu, että

$$Z(G_1)Z(G_2)\cdots Z(G_n) = Z(G).$$

□

Esimerkki 4.9. Tarkastellaan symmetristä ryhmää $\Sigma_3 = \{1, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$ ja sen aliryhmiä $K = \{1, (1\,2\,3), 1\,3\,2)\}$ ja $H = \{1, (1\,2)\}$. Määritetään ryhmien Σ_3, K ja H välisen suoran ulkoisen tulon keskus $Z(\Sigma_3 \times K \times H)$.

Esimerkin 4.6 nojalla $Z(\Sigma_3) = \{1\}$. Ryhmät K ja H ovat molemmat Abelin ryhmiä, joten lauseen 4.3 nojalla $Z(K) = K$ ja $Z(H) = H$. Näin ollen apulauseen 4.8 nojalla

$$Z(\Sigma_3 \times K \times H) = Z(\Sigma_3) \times Z(K) \times Z(H) = \{1\} \times K \times H = \{1\} \times \{1, (1\,2\,3), 1\,3\,2)\} \times \{1, (1\,2)\}.$$

5 Krullin, Remakin ja Schmidtin lause

Lähteinä tässä luvussa on käytetty päälähdeteoksen eli Rosen teoksen *A Course on Group Theory* [4] sivuja 175-182 ja Rotmanin teoksen *An Introduction to the Theory of Groups* [5] sivua 144.

Krullin, Remakin ja Schmidtin yleinen tapaus pätee kaikille äärellisille ryhmille ja tietyt ehdot täyttäville äärettömille ryhmille. Yleinen tapaus todistaa, että jos ryhmälle G on olemassa esitykset

$$G = H_1 \times H_2 \times \cdots \times H_n = K_1 \times K_2 \times \cdots \times K_m,$$

missä $H_1, H_2, \ldots H_n, K_1, K_2, \ldots K_m$ ovat epätriviaaleja ja hajoamattomia ryhmiä, niin tällöin $m = n$ ja tarvittaessa uudelleen luetteloimalla, $H_i \cong K_i$, kun $i \in \{1, 2, \ldots, n\}$.

Tässä tutkielmassa rajoitutaan tarkastelemaan tapausta, jossa G on epätriviaali ja äärellinen ryhmä, jonka keskus on triviaali. Tällöin ryhmälle G esitettävät hajotelmat epätriviaaleihin ja hajoamattomiin ryhmän G normaaleihin aliryhmiin ovat keskenään tekijöiden järjestystä vaille yksikäsitteiset.

Aloitetaan käymällä läpi päälauseen todistukseen tarvittavia esituloksia.

Apulause 5.1. *Olkoon G äärellinen ryhmä ja ϕ ryhmän G G-endomorfismi. Tällöin*

1. *On olemassa sellainen positiivinen kokonaisluku k, että*

$$G = \operatorname{Ker} \phi^k \times \operatorname{Im} \phi^k.$$

2. *Jos G on hajoamaton, niin tällöin joko ϕ on ryhmän G automorfismi, tai ϕ^k on ryhmän G triviaali endomorfismi jollakin positiivisella kokonaisluvulla k.*

Todistus. Todistetaan ensin ensimmäinen väite. Merkitään $K_j = \operatorname{Ker} \phi^j$, missä j on positiivinen kokonaisluku. Olkoon n positiivinen kokonaisluku ja $m \in \{1, 2, \ldots, n\}$. Oletetaan, että $x \in K_m$. Tällöin

$$\phi^{m+1}(x) = \phi(\phi^m(x)) = \phi(1) = 1.$$

Täten $x \in K_{m+1}$. Näin ollen $K_m \subseteq K_{m+1}$. Lisäksi apulauseen 2.25 nojalla $K_m, K_{m+1} \leq G$, joten näin ollen $K_m \leq K_{m+1}$. Siispä

$$K_1 \leq K_2 \leq K_3 \leq \cdots \leq G.$$

Näin ollen, koska G on äärellinen, niin on olemassa sellainen $k \in \{1, 2, \ldots, n\}$, että $K_k = K_{k+1}$.

Osoitetaan induktiolla, että $K_k = K_{k+p}$ pätee, kun $p \in \{1, 2, \ldots, n\}$. Triviaalisti tämä pätee, kun $p = 1$. Oletetaan seuraavaksi, että $p > 1$. Tehdään induktio-oletus olettamalla, että $K_k = K_{k+p-1}$ pätee. Olkoon $g \in K_{k+p}$. Tällöin

$$\phi^{k+1}(\phi^{p-1}(g)) = \phi^{(k+1)+(p-1)}(g) = \phi^{k+p}(g) = 1.$$

Siispä $\phi^{p-1}(g) \in K_{k+1} = K_k$. Näin ollen

$$\phi^{k+p-1}(g) = \phi^k(\phi^{p-1}(g)) = \phi^k(1) = 1,$$

joten $g \in K_{k+p-1}$. Täten induktio-oletuksen nojalla $g \in K_k$. On siis osoitettu, että $K_{k+p} \leq K_k$. Toisaalta myös aikaisemmin todetun nojalla $K_k \leq K_{k+p}$. Siispä oltava

$$K_k = K_{k+p},$$

kun $p \in \{1, 2, \ldots, n\}$.

Olkoon nyt $K = K_k$ ja $L = \operatorname{Im} \phi^k$. K on lauseen 2.25 nojalla ryhmän G normaali aliryhmä. Kuvaus ϕ on oletuksen nojalla G-endomorfismi, joten apulauseen 2.37 nojalla myös ϕ^k on G-endomorfismi. Täten L on ryhmän G G-aliryhmä apulauseen 2.34 nojalla ja edelleen esimerkin 2.32 nojalla ryhmän G normaali aliryhmä. Siispä apulauseen 2.11 nojalla KL on ryhmän G aliryhmä.

Olkoon $x \in K \cap L$. Tällöin

$$\phi^k(x) = 1$$

ja

$$x = \phi^k(y)$$

jollakin $y \in G$. Täten

$$\phi^{2k}(y) = \phi^k(\phi^k(y)) = \phi^k(x) = 1$$

ja näin ollen $y \in K_{2k}$. Koska aikaisemmin osoitetun nojalla $K_{2k} = K_k$, niin $y \in K_k$. Siispä

$$x = \phi^k(y) = 1.$$

Näin ollen

$$K \cap L = \{1\}.$$

Täten toisen isomorfialauseen 2.27 nojalla

$$L \cong KL/K.$$

Toisaalta homomorfialauseen 2.26 nojalla myös

$$L \cong G/K.$$

Näin ollen, koska KL on ryhmän G aliryhmä ja G on äärellinen,

$$G = KL.$$

Täten lauseen 3.5 nojalla

$$G = K \times L = \operatorname{Ker} \phi^k \times \operatorname{Im} \phi^k,$$

ja näin ollen ensimmäinen väite on todistettu.

Todistetaan seuraavaksi lauseen toinen väite. Oletetaan, että äärellinen ryhmä G on hajoamaton. Tällöin joko

$$K = G \qquad \text{ja} \qquad L = \{1\}$$

tai

$$K = \{1\} \qquad \text{ja} \qquad L = G.$$

Aikaisemmassa tapauksessa $\operatorname{Im}\phi^k = L = \{1\}$, joten ϕ^k on ryhmän G triviaali endomorfismi. Jälkimmäisessä tapauksessa $\operatorname{Im}\phi^k = L = G$. Jos endomorfismi ϕ ei olisi automorfismi, niin tällöin $\operatorname{Im}\phi \neq G$, jolloin olisi myös $\operatorname{Im}\phi^k \neq G$. Näin ollen endomorfismin ϕ on oltava ryhmän G automorfismi.

□

Määritellään seuraavaa apulauseen 5.1 tulosta laajentavaa apulausetta 5.5 varten homomorfismien summa.

Määritelmä 5.2. Olkoot ϕ ja ψ ryhmän G homomorfismeja ryhmälle H. Tällöin *homomorfismien* ϕ ja ψ *summa*

$$\phi + \psi \colon G \to H$$

on kuvaus, jolle pätee

$$\phi + \psi \colon g \mapsto \phi(g)\psi(g),$$

kun $g \in G$. Yleensä $\phi + \psi$ ei ole itsessään homomorfismi, eikä yleensä päde $\phi + \psi = \psi + \phi$.

Määritelmä laajenee luonnollisella tavalla myös useamman homomorfismin summalle. Olkoon n positiivinen kokonaisluku ja olkoot $\phi_1, \phi_2, \ldots, \phi_n$ homomorfismeja ryhmältä G ryhmälle H. Tällöin

$$\sum_{i=1}^{n} \phi_i \colon G \to H,$$

on kuvaus, jolle pätee

$$\sum_{i=1}^{n} \phi_i \colon g \mapsto \phi_1(g)\phi_2(g)\cdots\phi_n(g),$$

kun $g \in G$.

Merkinnällä $k\phi$, missä k on positiivinen kokonaisluku, tarkoitetaan homomorfismien ϕ summaa $\phi + \phi + \cdots + \phi$, jossa summattavien homomorfismien lukumäärä on k.

Esimerkki 5.3. Olkoot ϕ ja ψ ryhmän G homomorfismeja ryhmälle H. Osoita, että jos $\phi + \psi$ on homomorfismi, niin tällöin $\phi + \psi = \psi + \phi$.

Ratkaisu Olkoon $x \in G$. Tällöin, koska ϕ ja ψ ovat homomorfismeja,

$$(\psi + \phi)(x)(\phi + \psi)(x^{-1}) = \psi(x)\phi(x)\phi(x^{-1})\psi(x^{-1})$$
$$= \psi(x)\phi(xx^{-1})\psi(x^{-1}) = \psi(x)1\psi(x^{-1}) = \psi(xx^{-1}) = 1.$$

Näin ollen $\big((\psi + \phi)(x)\big)^{-1} = (\phi + \psi)(x^{-1})$. Täten, koska $\phi + \psi$ on homomorfismi,

$$(\phi + \psi)(x)\big((\psi + \phi)(x)\big)^{-1} = (\phi + \psi)(x)(\phi + \psi)(x^{-1}) = (\phi + \psi)(xx^{-1}) = 1.$$

Tämä on yhtäpitävästi $(\phi + \psi)(x) = (\psi + \phi)(x)$. Näin ollen $\phi + \psi = \psi + \phi$.

Seuraava todistus on aputulos apulauseen 5.5 todistusta varten.

Apulause 5.4. *Olkoot ϕ ja ψ keskenään kommutoivia ryhmän G endomorfismeja ja olkoon n positiivinen kokonaisluku. Tällöin*

$$(\phi + \psi)^n = \sum_{i=0}^{n} \binom{n}{i} \phi^{n-i}\psi^i,$$

missä $\phi_1^0 = \phi_2^0 = I$.

Todistus. Todistetaan väite induktiolla luvun n suhteen. Jos $n = 1$, niin

$$(\phi + \psi)^1 = \phi I + I\psi = \binom{1}{0}\phi^1\psi^0 + \binom{1}{1}\phi^0\psi^1.$$

Oletetaan nyt, että väite pätee positiivisella kokonaisluvulla $n > 2$. Tällöin

$$(\phi + \psi)^{n+1} = (\phi + \psi)(\phi + \psi)^n = (\phi + \psi)\sum_{i=0}^{n} \binom{n}{i} \phi^{n-i}\psi^i$$
$$= \phi\left(\sum_{i=0}^{n} \binom{n}{i} \phi^{n-i}\psi^i\right) + \psi\left(\sum_{i=0}^{n} \binom{n}{i} \phi^{n-i}\psi^i\right).$$

Koska ϕ ja ψ ovat endomorfismeja ja $\phi\psi = \psi\phi$, niin edellinen lauseke saadaan muotoon

$$\sum_{i=0}^{n} \binom{n}{i} \phi\phi^{n-i}\psi^i + \sum_{i=0}^{n} \binom{n}{i} \psi\phi^{n-i}\psi^i = \sum_{i=0}^{n} \binom{n}{i} \phi^{n+1-i}\psi^i + \sum_{i=0}^{n} \binom{n}{i} \phi^{n-i}\psi^{i+1}$$
$$= \binom{n}{0}\phi^{n+1-0}\psi^0 + \sum_{i=1}^{n} \binom{n}{i} \phi^{n+1-i}\psi^i + \sum_{i=0}^{n-1} \binom{n}{i} \phi^{n-i}\psi^{i+1} + \binom{n}{n}\phi^{n-n}\psi^{n+1}$$
$$= \phi^{n+1} + \sum_{i=1}^{n} \binom{n}{i} \phi^{n+1-i}\psi^i + \sum_{i=0}^{n-1} \binom{n}{i} \phi^{n-i}\psi^{i+1} + \psi^{n+1}.$$

Muutetaan edellisen lausekkeen jälkimmäisen summan muuttuja seuraavasti:

$$\sum_{i=0}^{n-1} \binom{n}{i} \phi^{n-i}\psi^{i+1} = \sum_{i=1}^{n} \binom{n}{i-1} \phi^{n+1-i}\psi^{i}.$$

Näin ollen

$$\begin{aligned}
&\phi^{n+1} + \sum_{i=1}^{n} \binom{n}{i} \phi^{n+1-i}\psi^{i} + \sum_{i=0}^{n-1} \binom{n}{i} \phi^{n-i}\psi^{i+1} + \psi^{n+1} \\
&= \phi^{n+1} + \sum_{i=1}^{n} \binom{n}{i} \phi^{n+1-i}\psi^{i} + \sum_{i=1}^{n} \binom{n}{i-1} \phi^{n+1-i}\psi^{i} + \psi^{n+1} \\
&= \phi^{n+1} + \sum_{i=1}^{n} \left(\binom{n}{i} + \binom{n}{i-1} \right) \phi^{n+1-i}\psi^{i} + \psi^{n+1}.
\end{aligned}$$

Pascalin säännön nojalla $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$, joten edellinen lauseke saadaan muotoon

$$\begin{aligned}
&\phi^{n+1} + \sum_{i=1}^{n} \binom{n+1}{i} \phi^{n+1-i}\psi^{i} + \psi^{n+1} \\
&= \binom{n+1}{0} \phi^{n+1-0}\psi^{0} + \sum_{i=1}^{n} \binom{n+1}{i} \phi^{n+1-i}\psi^{i} + \binom{n+1}{n+1} \phi^{n+1-(n+1)}\psi^{n+1} \\
&= \sum_{i=1}^{n+1} \binom{n+1}{i} \phi^{n+1-i}\psi^{i}.
\end{aligned}$$

Näin ollen on osoitettu, että

$$(\phi + \psi)^{n+1} = \sum_{i=1}^{n+1} \binom{n+1}{i} \phi^{n+1-i}\psi^{i}.$$

Täten väite seuraa induktioperiaatteesta. □

Apulause 5.5. *Olkoon G äärellinen ryhmä, joka on epätriviaali ja hajoamaton. Oletetaan, että $\phi_1, \phi_2, \ldots, \phi_n$, missä n on positiivinen kokonaisluku, ovat sellaisia G-endomorfismeja, että $\sum_{i=1}^{j} \phi_i$ on G-endomorfismi, kun $j = 1, \ldots, n$, ja $\sum_{i=1}^{n} \phi_i$ on ryhmän G identtinen automorfismi. Tällöin ainakin yksi G-endomorfismeista $\phi_1, \phi_2, \ldots, \phi_n$ on ryhmän G automorfismi.*

Todistus. Todistetaan väite induktiolla luvun n suhteen. Jos $n = 1$, niin väite pitää oletusten nojalla triviaalisti paikkansa. Oletetaan nyt, että $n = 2$. Olkoon $x \in G$. Täten, koska ϕ_1 on endomorfismi ja $\phi_1 + \phi_2$ on identtinen automorfismi,

$$\phi_1(x) = \phi_1\big((\phi_1 + \phi_2)(x)\big) = \phi_1\big(\phi_1(x)\phi_2(x)\big) = \phi_1^2(x)\phi_1\phi_2(x).$$

Toisaalta myös

$$\phi_1(x) = (\phi_1 + \phi_2)(\phi_1(x)) = \phi_1(\phi_1(x))\phi_2(\phi_1(x)) = \phi_1^2(x)\phi_2\phi_1(x).$$

Täten

$$\phi_1^2(x)\phi_1\phi_2(x) = \phi_1^2(x)\phi_2\phi_1(x).$$

Koska G on ryhmä, niin tämä on yhtäpitävä yhtälön

$$\phi_1\phi_2(x) = \phi_2\phi_1(x)$$

kanssa. Näin ollen

$$\phi_1\phi_2 = \phi_2\phi_1.$$

Olkoon ζ ryhmän G triviaali endomorfismi. Jos kumpikaan endomorfismeista ϕ_1 tai ϕ_2 ei ole ryhmän G automorfismi, niin tällöin apulauseen 5.1 nojalla on olemassa sellaiset positiiviset kokonaisluvut k_1 ja k_2, että

$$\phi_1^{k_1} = \phi_2^{k_2} = \zeta.$$

Tällöin apulauseen 5.4 nojalla saadaan

$$(\phi_1 + \phi_2)^{k_1+k_2} = \sum_{i=0}^{k_1+k_2} \binom{k_1 + k_2}{i} \phi_1^{k_1+k_2-i}\phi_2^i,$$

missä $\phi_1^0 = \phi_2^0 = I$. Lisäksi, koska $\phi_1 + \phi_2 = I$, niin myös $(\phi_1 + \phi_2)^{k_1+k_2} = I$.

Kun $0 \leq i \leq k_2$, niin $k_2 - i \geq 0$. Tällöin $\phi_1^{k_1+k_2-i} = \zeta$, sillä $\phi_1^{k_1} = \zeta$. Näin ollen $\phi_1^{k_1+k_2-i}\phi_2^i = \zeta$. Kun $k_2 < i \leq k_1 + k_2$, niin $\phi_2^i = \zeta$, sillä $\phi_2^{k_2} = \zeta$. Näin ollen $\phi_1^{k_1+k_2-i}\phi_2^i = \zeta$, sillä $\phi_1^{k_1+k_2-i}$ on ryhmän G endomorfismi. On siis osoitettu, että

$$\phi_2^i\phi_1^{k_1+k_2-i} = \zeta,$$

kun $i \leq k_1 + k_2$. Täten

$$I = (\phi_1 + \phi_2)^{k_1+k_2} = \sum_{i=0}^{k_1+k_2} \binom{k_1 + k_2}{i} \phi_1^{k_1+k_2-i}\phi_2^i = \zeta.$$

Ehdosta $I = \zeta$ seuraa, että G olisi triviaali ryhmä. Tämä on kuitenkin ristiriita, sillä oletuksen nojalla G on epätriviaali ryhmä. Näin ollen vähintään toisen endomorfismeista ϕ_1 tai ϕ_2 on oltava ryhmän G automorfismi.

Oletetaan lopuksi, että $n > 2$. Olkoon

$$\psi = \sum_{i=1}^{n-1} \phi_i.$$

Tällöin oletuksen nojalla ψ ja ϕ_n ovat ryhmän G G-endomorfismeja ja $\psi + \phi_n = I$. Täten edellä todistetun nojalla, joko ψ tai ϕ_n on ryhmän G automorfismi.

Jos $\phi_n \in \operatorname{Aut} G$, niin väite on todistettu. Oletetaan nyt, että $\psi \in \operatorname{Aut} G$. Tällöin myös $\psi^{-1} \in \operatorname{Aut} G$. Näin ollen

$$I = \psi^{-1}\psi = \psi^{-1} \sum_{i=1}^{n-1} \phi_i = \sum_{i=1}^{n-1} \psi^{-1}\phi_i.$$

Olkoot $g, \omega \in G$. Koska ψ on G-endomorfismi, niin

$$\psi(\psi^{-1}(g^\omega)) = g^\omega = (\psi(\psi^{-1}(g)))^\omega = \psi((\psi^{-1}(g))^\omega).$$

Täten $\psi^{-1}(g^\omega) = (\psi^{-1}(g))^\omega$, koska ψ on automorfismi. Näin ollen ψ^{-1} on G-endomorfismi. Apulauseen 2.36 nojalla $\psi^{-1}\phi_1, \psi^{-1}\phi_2, \ldots, \psi^{-1}\phi_n$ ja

$$\sum_{i=1}^{n-1} \psi^{-1}\phi_i = \psi^{-1}\psi$$

ovat kaikki kahden G-endomorfismin yhdistettyinä kuvauksina G-endomorfismeja.

Tällöin induktio-oletuksen nojalla $\psi^{-1}\phi_i \in \operatorname{Aut} G$, jollakin $i \in \{1, 2, \ldots, n-1\}$. Täten, koska $\psi, \psi^{-1}\phi_i \in \operatorname{Aut} G$, niin

$$\phi_i = \psi(\psi^{-1}\phi_i) \in \operatorname{Aut} G,$$

jollakin $i \in \{1, 2, \ldots, n-1\}$. Näin ollen induktioperiaatteesta seuraa väite. □

Apulause 5.6. *Olkoon ϕ ryhmän G endomorfismi. Tällöin ϕ on G-endomorfismi, jos*

$$\phi(g)g^{-1} \in C_G(\operatorname{Im} \phi),$$

kun $g \in G$.

Todistus. Olkoot $g, \omega \in G$. Oletuksen nojalla $\phi(\omega)\omega^{-1}$ kommutoi kaikkien ryhmän G kuvajoukon alkioiden kanssa. Näin ollen

$$\begin{aligned}
&\phi(g^\omega) = \phi(\omega^{-1}g\omega) = \phi(\omega^{-1})\phi(g)\phi(\omega) \\
&= \phi(\omega^{-1})\phi(g)\phi(\omega)\omega^{-1}\omega = \phi(\omega^{-1})\phi(\omega)\omega^{-1}\phi(g)\omega \\
&= \phi(\omega^{-1}\omega)\omega^{-1}\phi(g)\omega = \omega^{-1}\phi(g)\omega = \big(\phi(g)\big)^\omega.
\end{aligned}$$

Täten ϕ on G-endomorfismi. □

Huomattakoon, että vastaavan ehdon täyttävä homomorfismi ϕ joltakin ryhmältä G aliryhmälleen H olisi G-homomorfismi ryhmältä G ryhmälle H.

Määritelmä 5.7. Olkoon $G = G_1 \times G_2 \times \cdots \times G_n$, missä n on positiivinen kokonaisluku. Tällöin ryhmän G *projektio* ryhmälle G_i on kuvaus

$$\pi_i \colon G \to G_i,$$

jolle

$$\pi_i \colon g_1 g_2 \cdots g_n \mapsto g_i,$$

kun $g_n \in G_n$ ja $i \in \{1, 2, \ldots, n\}$.

Apulause 5.8. *Olkoot ryhmällä $G = G_1 \times G_2 \times \cdots \times G_n$, missä n on positiivinen kokonaisluku, projektiot $\pi_i \colon G \to G_i$, missä $i \in \{1, 2, \ldots, n\}$. Tällöin projektiot π_i ovat G-homomorfismeja ryhmältä G ryhmälle G_i.*

Todistus. Olkoon $g = g_1 g_2 \cdots g_n$, missä $g_j \in G_j$, kun $j \in \{1, 2, \ldots, n\}$. Suorien tulojen eri tekijöiden alkiot kommutoivat keskenään, joten π_i on selvästi homomorfismi ryhmältä G aliryhmälleen G_i ja

$$\begin{aligned} &\pi_i(g)g^{-1} = g_i(g_1 g_2 \cdots g_n)^{-1} = g_i g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1} \\ &= g_i g_i^{-1} g_n^{-1} g_{n-1}^{-1} \cdots g_{i+1}^{-1} g_{i-1}^{-1} \cdots g_1^{-1} \\ &= g_n^{-1} g_{n-1}^{-1} \cdots g_{i+1}^{-1} g_{i-1}^{-1} \cdots g_1^{-1} \in C_G(\operatorname{Im} \pi_i). \end{aligned}$$

Näin ollen väite seuraa apulauseesta 5.6. □

Apulause 5.9. *Olkoon ryhmällä $G = G_1 \times G_2 \times \cdots \times G_n$, missä n on positiivinen kokonaisluku, projektiot $\pi_i \colon G \to G_i$ ja inkluusiot $\phi_i \colon G_i \to G$. Tällöin kuvaus $\sum_{i=1}^{j} \phi_i \pi_i$ on G-endomorfismi, kun $j \in \{1, 2, \ldots, n\}$ ja kuvaus $\sum_{i=1}^{n} \phi_i \pi_i$ on ryhmän G identtinen automorfismi.*

Todistus. Apulauseen 5.8 nojalla kuvaus $\phi_i \pi_i$ on G-endomorfismi, kun $i \in \{1, 2, \ldots, n\}$. Täten $\sum_{i=1}^{j} \phi_i \pi_i$ on määritelty, kun $j \in \{1, 2, \ldots, n\}$. Olkoot $g = g_1 g_2 \cdots g_n$ ja $h = h_1 h_2 \cdots h_n$ ryhmän G alkioita, missä $h_i, g_i \in G_i$, kun $i \in \{1, 2, \ldots, n\}$. Ensinnäkin

$$\sum_{i=1}^{j} \phi_i \pi_i(g) = \phi_1 \pi_1(g) \phi_2 \pi_2(g) \cdots \phi_j \pi_j(g) = g_1 g_2 \cdots g_j,$$

kun $j \in \{1, 2, \ldots, n\}$. Näin ollen $\sum_{i=1}^{n} \phi_i \pi_i(g) = g$, joten $\sum_{i=1}^{n} \phi_i \pi_i = I$.

Merkitään selvyyden vuoksi $\gamma = \sum_{i=1}^{j} \phi_i \pi_i$. Nyt

$$\begin{aligned} &\gamma(gh) = \gamma(g_1 g_2 \cdots g_n h_1 h_2 \cdots h_n) \\ &= \gamma(g_1 h_1 g_2 h_2 \cdots g_n h_n) = g_1 h_1 g_2 h_2 \cdots g_j h_j \\ &= g_1 g_2 \cdots g_j h_1 h_2 \cdots h_j = \gamma(g)\gamma(h). \end{aligned}$$

Näin ollen γ on endomorfismi. Lisäksi γ on apulauseen 5.6 nojalla G-endomorfismi, sillä $\operatorname{Im} \gamma = G_1 G_2 \cdots G_j \subseteq G$ ja

$$\gamma(g)g^{-1} = g_{j+1}^{-1} g_{j+2}^{-1} \cdots g_n^{-1} \in C_G(\operatorname{Im} \gamma).$$

□

Ennen päälausetta osoitetaan vielä, että epätriviaalille äärelliselle ryhmälle ylipäätään on olemassa hajotelma epätriviaalien hajoamattomien normaalien aliryhmien suorana tulona.

Lause 5.10. *Olkoon G jokin epätriviaali äärellinen ryhmä. Tällöin on olemassa sellaiset epätriviaalit hajoamattomat ryhmän G normaalit aliryhmät $G_1, G_2, \ldots, G_n$, että*

$$G = G_1 \times G_2 \times \cdots \times G_n,$$

missä n on positiivinen kokonaisluku.

Todistus. Todistamme väitteen induktiolla ryhmän G alkioiden lukumäärän suhteen. Jos G on hajoamaton, niin asetetaan $n = 1$ ja $G_1 = G$. Tällöin väite on todistettu. Oletetaan nyt, että G on hajoava. Tällöin on olemassa ryhmän G epätriviaalit normaalit aliryhmät H ja K siten, että $G = H \times K$. Tästä seuraa myös, että ryhmät H ja K ovat aitoja aliryhmiä, joten kummankin ryhmän alkioiden lukumäärä on pienempi kuin ryhmän G alkioiden lukumäärä. Täten induktio-oletuksen nojalla on olemassa epätriviaalit ja hajoamattomat ryhmän H normaalit aliryhmät $G_1, G_2, \ldots, G_m$ ja epätriviaalit ja hajoamattomat ryhmän K normaalit aliryhmät $G_{m+1}, G_{m+2}, \ldots, G_n$ joille

$$H = G_1 \times G_2 \times \cdots \times G_m$$

ja

$$K = G_{m+1} \times G_{m+2} \times \cdots \times G_n.$$

Täten ryhmät $G_1, G_2, \ldots, G_n$ ovat epätriviaaleja ja hajoamattomia ryhmän G normaaleja aliryhmiä ja

$$G = (G_1 \times G_2 \times \cdots \times G_m) \times (G_{m+1} \times G_{m+2} \times \cdots \times G_n) = G_1 \times G_2 \times \cdots \times G_n.$$

Näin ollen induktioperiaatteesta seuraa väite. □

Päälause 5.11 (Krullin, Remakin ja Schmidtin lause)**.** *Olkoon G epätriviaali ja äärellinen ryhmä, jonka keskus on triviaali eli $Z(G) = 1$. Oletetaan, että ryhmällä G on hajotelmat*

$$G = H_1 \times H_2 \times \cdots \times H_m = K_1 \times K_2 \times \cdots \times K_n,$$

missä luvut m ja n ovat positiivisia kokonaislukuja ja ryhmät $H_1, H_2, \ldots H_m, K_1, K_2, \ldots, K_n$ ovat ryhmän G epätriviaaleja ja hajoamattomia normaaleja aliryhmiä. Tällöin $m = n$ ja on olemassa sellainen uudelleenluettelointi, että $H_i = K_i$, kun $i \in \{1, 2, \ldots, n\}$.

Todistus. Todistetaan väite induktiolla luvun n suhteen. Jos $n = 1$, niin tällöin $m = 1$ ja $H_1 = K_1$, sillä ryhmä K_1 on hajoamaton ja ryhmät $H_1, H_2, \ldots, H_m$ ovat epätriviaaleja. Oletetaan nyt, että $n > 1$. Tällöin, koska ryhmät $K_1, K_2, \ldots, K_n$ ovat epätriviaaleja ja H_1 on hajoamaton, niin myös $m > 1$.

Osoitetaan seuraavaksi, että jollakin $i \in \{1, 2, \ldots, n\}$ ryhmien H_1 ja K_i välille on löydettävissä injektiivinen kuvaus. Olkoon π_1 projektio $G \to H_1$, ρ_i projektio $G \to K_i$ ja κ_i inkluusio $K_i \to G$ kaikilla $i \in \{1, 2, \ldots, n\}$. Olkoon

$$\pi_i^* = \pi_1 \kappa_i = \pi_1 | K_1 \colon K_i \to H_1$$

ja

$$\rho_i^* = \rho_i|H_1 : H_1 \to K_i.$$

Jokainen kuvaus $\pi_i^*\rho_i^*$ on apulauseiden 5.8 ja 2.36 nojalla ryhmän H_1 G-endomorfismi ja näin ollen myös ryhmän H_1 H_1-endomorfismi.

Apulauseen 5.9 nojalla $\sum_{i=1}^{j} \kappa_i\rho_i$ on ryhmän G G-endomorfismi, kun $j \in \{1, 2, \ldots, n\}$.

Näin ollen, apulauseen 2.36 nojalla $\pi_1(\sum_{i=1}^{j} \kappa_i\rho_i)$ on G-homomorfismi ryhmältä G ryhmälle H_1. Lisäksi, koska π_1 on G-homomorfismina homomorfismi,

$$\pi_1(\sum_{i=1}^{j} \kappa_i\rho_i) = \sum_{i=1}^{j} \pi_1\kappa_i\rho_i = \sum_{i=1}^{j} \pi_i^*\rho_i.$$

Tämän kuvauksen rajoittuma ryhmään H_1 on $\sum_{i=1}^{j} \pi_i^*\rho_i^*$, joka on näin ollen ryhmän H_1 G-endomorfismi ja täten myös ryhmän H_1 H_1-endomorfismi. Olkoon $h \in H_1$, tällöin

$$h = \pi_1(h) = \pi_1((\rho_1(h))(\rho_2(h)) \cdots (\rho_n(h)) = (\pi_1\rho_1(h))(\pi_1\rho_2(h)) \cdots (\pi_1\rho_n(h))$$
$$= (\pi_1^*\rho_1^*(h))(\pi_2^*\rho_2^*(h)) \cdots (\pi_n^*\rho_n^*(h)) = \sum_{i=1}^{n} \pi_i^*\rho_i^*(h).$$

Näin ollen $\sum_{i=1}^{n} \pi_i^*\rho_i^*$ on ryhmän H_1 identtinen automorfismi. Lisäksi H_1 on epätriviaali ja hajoamaton. Näin ollen apulauseen 5.5 ehdot täyttyvät ja täten

$$\pi_i^*\rho_i^* \in \text{Aut } H_1,$$

jollakin $i \in \{1, 2, \ldots, n\}$. Voidaan olettaa, että luettelointi on valittu siten, että $\pi_1^*\rho_1^* \in$ Aut H_1, koska suoran tulon tekijät ovat kommutatiivisia. Tästä seuraa erityisesti, että ρ_1^* on injektiivinen.

Olkoot

$$J = H_2 \times \cdots \times H_m$$

ja

$$L = K_2 \times \cdots \times K_n.$$

Tällöin oletuksen nojalla

$$H_1 \times J = K_1 \times L.$$

Koska ryhmän G keskus on triviaali, niin apulauseen 4.8 nojalla

$$Z(H_1) = Z(J) = Z(K_1) = Z(L) = \{1\}.$$

Koska H_1 ja J ovat ryhmän G normaaleja aliryhmiä ja

$$J \leq C_G(H_1) \leq G = H_1 \times J,$$

niin apulauseen 3.16 nojalla

$$C_G(H_1) = (H_1 \cap C_G(H_1)) \times J.$$

Apulauseen 4.7 nojalla $H_1 \cap C_G(H_1) = Z(H_1) = \{1\}$, joten saadaan edelleen

$$C_G(H_1) = Z(H_1) \times J = \{1\} \times J = J.$$

Täysin samoin perustein

$$C_G(J) = H_1,$$
$$C_G(K_1) = L$$

ja

$$C_G(L) = K_1.$$

Koska

$$L = \operatorname{Ker} \rho_1$$

ja ρ_1^* on aikaisemmin osoitetun nojalla injektiivinen, niin

$$\{1\} = \operatorname{Ker} \rho_1^* = H_1 \cap \operatorname{Ker} \rho_1 = H_1 \cap L.$$

Täten apulauseen 2.13 nojalla

$$hl = lh,$$

kun $h \in H_1$ ja $l \in L$. Siispä

$$H_1 \leq C_G(L).$$

Näin ollen

$$H_1 \leq K_1 \leq G = H_1 \times J,$$

ja täten apulauseen 3.16 nojalla

$$K_1 = H_1 \times (K_1 \cap J).$$

Koska oletuksen nojalla K_1 on hajoamaton ja $H_1 \neq \{1\}$, niin on oltava

$$K_1 = H_1.$$

Siispä

$$J = C_G(H_1) = C_G(K_1) = L.$$

Täten

$$J = H_2 \times \cdots \times H_m = K_2 \times \cdots \times K_n.$$

Koska

$$Z(J) = \{1\},$$

niin induktio-oletuksen nojalla $m = n$ ja, oikealla luetteloinnilla,

$$H_i = K_i,$$

kun $i \in \{2, \ldots, m\}$. Näin ollen induktioperiaatteesta seuraa väite. □

Lähteet

[1] Bhattacharya, P. B. & Jain, S. K. & Nagpaul, S. R., *Basic Abstract Algebra.* 2. painos, Cambridge University Press, 1994.

[2] Eie, Minking & Chang Shou-Te, *A Course on Abstract Algebra.* 1. painos, World Scientific, 2010.

[3] Nieminen, Veli-Matti, *Ryhmien suorat tulot.* Tampereen yliopisto, Informaatiotieteiden yksikkö, Kandidaatin tutkielma, 2013.

[4] Rose, John S., *A Course on Group Theory.* 1. painos, Dover, 2012.

[5] Rotman, Joseph J., *An Introduction to the Theory of Groups.* 4. painos, Springer Verlag, 1995.

[6] Scott, W.E., *Group Theory.* 1. painos, Dover, 1964.