

4. Ryhmien sisäinen rakenne

Tässä luvussa tarkastellaan joitakin tapoja päästä käsiksi ryhmien sisäiseen rakenteeseen. Useimmat tuloksista ovat erityisen käyttökelpoisia äärellisten ryhmien tapauksessa.

4.1. Tuloryhmät. Olkoot A ja B ryhmän G aliryhmiä. Tutkitaan, milloin niiden *tulojoukko*

$$AB = \{ab \mid a \in A, b \in B\}$$

on aliryhmä.

Tulojoukon alkioiden $b = e \cdot b$ ja $a = a \cdot e$ tulo on ba . Jotta AB olisi aliryhmä, tämän tulon on oltava joukossa AB kaikilla $a \in A$ ja $b \in B$. Tämä tarkoittaa sitä, että jokainen tulo ba on muotoa $a'b'$ joillain $a' \in A$ ja $b' \in B$. Siispä vähimmäisehto sille, että AB on aliryhmä, on $BA = AB$. Tällöin myös kaikki käänteisalkiot ovat mukana, sillä $(ab)^{-1} = b^{-1}a^{-1} \in BA$.

Mainittu vähimmäisehto toteutuu esimerkiksi silloin, kun jokainen A :n alkio kommutoi jokaisen B :n alkion kanssa. Vähempikin kuitenkin riittää.

LEMMA 4.1. *Olkoot H ja N ryhmän G aliryhmiä. Jos $H \leq N_G(N)$, erityisesti jos N on normaali G :ssä, niin $HN \leq G$.*

TODISTUS. Käytetään aliryhmäkriteeriä. Selvästi HN on epätyhjä. Olkoot $a_1, a_2 \in H$ ja $b_1, b_2 \in N$. Ehto $H \leq N_G(N)$ tarkoittaa, että ryhmä N pysyy paikoillaan H :n alkioilla konjugoitaessa. Täten $a_2(b_1b_2^{-1})a_2^{-1} = b'$ jollain $b' \in N$. Tällöin nyt $b_1b_2^{-1}a_2^{-1} = a_2^{-1}b'$, joten

$$(a_1b_1)(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1} = a_1a_2^{-1}b' \in HN.$$

Siispä HN on aliryhmä. □

Keskitytään jatkossa siihen tapaukseen, jossa molemmat aliryhmät ovat normaaleja.

LAUSE 4.2. *Oletetaan, että H ja K ovat ryhmän G normaaleja aliryhmiä. Jos $HK = G$ ja $H \cap K = \{1\}$, niin $G \cong H \times K$.*

TODISTUS. Näytetään ensin, että H :n ja K :n alkiot ovat keskenään vaihdannaisia. Olkoot $a \in H$ ja $b \in K$. Nyt $(aba^{-1})b^{-1} \in K$, koska K on normaali. Samoin kuitenkin $a(ba^{-1}b^{-1}) \in H$, joten $aba^{-1}b^{-1} \in H \cap K = \{1\}$. Tästä seuraa, että $ba = ab$.

Harjoitustehtävänä on osoittaa, että jokaisella G :n alkiolla on yksikäsitteinen tuloesitys $g = ab$, missä $a \in H$ ja $b \in K$. Tällöin on mahdollista määritellä kuvaus $f: G \rightarrow H \times K$ kaavalla $f(ab) = (a, b)$. Kuvaus on selvästi bijektio. Olkoot $a_1, a_2 \in H$ ja $b_1, b_2 \in K$, jolloin

$$\begin{aligned} f(a_1b_1 \cdot a_2b_2) &= f(a_1a_2 \cdot b_1b_2) = (a_1a_2, b_1b_2) \\ &= (a_1, b_1) \cdot (a_2, b_2) = f(a_1a_2) \cdot f(b_1b_2). \end{aligned}$$

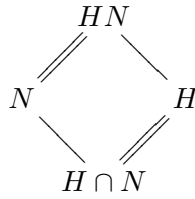
Täten f on homomorfismi. □

Jos edellisen lauseen ehdot pätevät, sanotaan, että G on aliryhmiensä H ja K *sisäinen suora tulo*. Usein merkinnöissä ei erotella sisäistä tuloa HK ja ulkoista tuloa $H \times K$, koska nämä ovat keskenään isomorfiset. Voidaan esimerkiksi kirjoittaa, että $G = H \times K$, ja merkitä G :n alkioita pareina (h, k) , vaikka ne todellisuudessa olisivat tuloja hk .

4.2. Isomorfialauseet. Seuraavat Emmy Noetherin muotoilemat tulokset selvittävät tekijäryhmien välisiä suhteita. Niiden todistukset nojaavat vahvasti homomorfialauseeseen, joka myös on yleisessä muodossaan Noetherin käsiälaa. Vastaavat tulokset pätevät myös renkailla.

LAUSE 4.3 (1. isomorfialause¹¹). *Olkoot H ja N ryhmän G aliryhmiä, ja olkoon N normaali. Tällöin $H \cap N \trianglelefteq H$, ja $H/(H \cap N) \cong HN/N$.*

Huomaa, että lemmän 4.1 nojalla HN on ryhmä. Lisäksi N on normaali ryhmässä HN , koska $HN \leq G$ ja N on normaali G :ssä. Alla oleva Hassen kaavio voi helpottaa lauseen muistamista. Kaksinkertainen viiva viittaa normaaliin aliryhmään. Yhdensuuntaiset kaksoisviivat viittaavat isomorfisiin tekijäryhmiin.



TODISTUS. Olkoon $\pi: G \rightarrow G/N$ kanoninen surjektio, ja olkoon π' sen rajoittuma ryhmään H . Kuvauksen π' arvot ovat siis sivuluokkia hN , missä $h \in H$. Tällaiset sivuluokat kuuluvat tekijäryhmään HN/N , koska jokainen sivuluokan alkio hn on ryhmässä HN .

Selvästi

$$\text{Ker } \pi' = \{h \in H \mid h \in N\} = H \cap N,$$

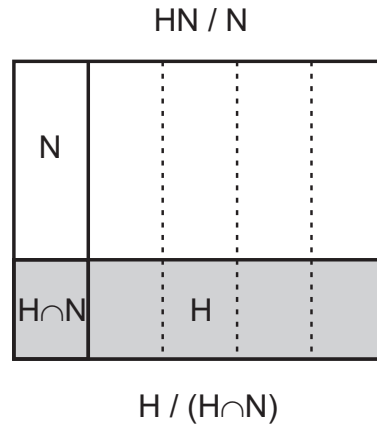
joten $H \cap N$ on normaali, ja homomorfialauseen perusteella $H/(H \cap N) \cong \text{Im } \pi'$. Toisaalta, jos $gN \in HN/N$, niin $g = hn$ joillain $h \in H$ ja $n \in N$. Nyt saadaan $\pi'(h) = hN = gN$, joten $\text{Im } \pi' = HN/N$. \square

LAUSE 4.4 (2. isomorfialause). *Olkoot H ja K ryhmän G normaaleja aliryhmiä, joille pätee $K \leq H$. Tällöin H/K on normaali ryhmässä G/K , ja*

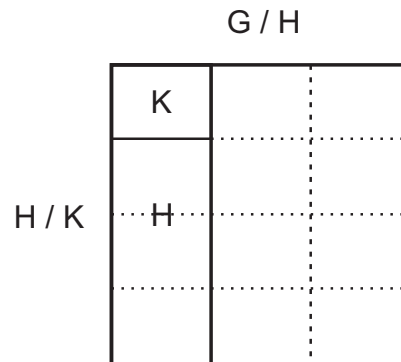
$$(G/K)/(H/K) \cong G/H.$$

TODISTUS. Olkoon $\pi: G \rightarrow G/H$ kanoninen surjektio. Koska $K \subset H$, kaikilla $k \in K$ pätee $\pi(k) = H$. Aliryhmä K siis sisältyy kuvauksen π ytimeen, joten lauseen 1.14 perusteella on olemassa homomorfismi $f: G/K \rightarrow G/H$, jolle pätee $f(gK) = \pi(g) = gH$. Tämä kuvaus ikään kuin laajentaa sivuluokkia ja on surjektiivinen, koska myös π on. Lisäksi $f(gK) = gH = H$ jos ja vain jos $g \in H$, ja tämä on yhtäpitävää sen kanssa, että $gK \in H/K$. Täten $\text{Ker } f = H/K$, ja tulos seuraa homomorfialauseesta. \square

¹¹Monissa lähteissä homomorfialauseetta nimitetään ensimmäiseksi isomorfialauseeksi. Tällöin ensimmäisestä isomorfialauseesta tuleekin toinen isomorfialause ja toisesta kolmas.



KUVA 8. Noetherin 1. isomorfialause



KUVA 9. Noetherin 2. isomorfialause

4.3. Sylowin¹² lauseet. Lagrangen lause kertoo, että äärellisen ryhmän jokoisen aliryhmän kertaluku jakaa ryhmän kertaluvun. Voidaanko sitten jokaista ryhmän kertaluvun tekijää p kohti löytää aliryhmä, jonka kertaluku olisi p ? Vastaus on yleisessä tapauksessa kielteinen, sillä esimerkiksi ryhmällä A_4 ei ole kuuden alkion aliryhmää, vaikka $|A_4| = 12$. Kuitenkin, jos p sattuu olemaan alkuluku, tällainen aliryhmä löytyy. Tämän tuloksen todisti Augustin Louis Cauchy vuonna 1845. Peter Sylow paransi tulosta vuonna 1872 osoittamalla, että itse asiassa jokaista sellaista p :n potenssia kohti, joka jakaa ryhmän kertaluvun, löytyy kyseistä kertalukua oleva aliryhmä, ja suurimmat niistä ovat kaikki keskenään isomorfisia, jopa toistensa konjugaatteja.

Sylowin lauseet liittyvät aliryhmiin, joiden kertaluku on jonkin alkuluvun potenssi. Tällaisilla ryhmillä on muutenkin monia kiinnostavia ominaisuuksia: esimerkiksi niillä on aina epätriviaali keskus.

MÄÄRITELMÄ 4.5. Olkoon p alkuluku. Äärellistä ryhmää sanotaan *p -ryhmäksi*, jos sen kertaluku on p^m jollain $m \geq 1$.

¹²Peter Ludwig Mejdell Sylow (1832–1918), norjalainen ryhmäteoreetikko.

MÄÄRITELMÄ 4.6. Oletetaan, että ryhmän kertaluku on $p^k m$, missä p on alkuluku, $k \geq 1$, ja m ei ole jaollinen p :llä. Sellaista aliryhmää, jonka kertaluku on p^k , kutsutaan *Sylowin p -aliryhmäksi*.

Sylow käytti lauseidensa todistamisessa yllä mainittua Cauchyn tulosta, mutta sittemmin lauseet on todistettu uudestaan monellakin eri tavalla. Tässä luvussa seurataan Helmut Wielandtin kombinatoriseen havaintoon perustuvaa esitystä, jota varten tarvitaan ensin yksinkertainen aputuloks.

LEMMA 4.7. *Oletetaan, että p on alkuluku, joka ei jaa lukua $m \in \mathbb{N}$, ja k on positiivinen kokonaisluku. Tällöin binomikerroin $\binom{p^k m}{p^k}$ ei ole jaollinen luvulla p .*

TODISTUS. Tarkasteltava binomikerroin on

$$\binom{p^k m}{p^k} = \frac{p^k m (p^k m - 1) \cdots (p^k m - i) \cdots (p^k m - p^k + 1)}{p^k (p^k - 1) \cdots (p^k - i) \cdots (p^k - p^k + 1)}.$$

Ensimmäinen tekijä sekä osoittajassa että nimittäjässä on p^k , joten ne voidaan supistaa pois. Koska luku m ei sisällä yhtään tekijää p , riittää tutkia osoittajan termejä $p^k m - i$, kun $1 \leq i < p^k$.

Olkoon $i = p^l q$, missä $l \in \mathbb{N}$ ja $p \nmid q$. Nyt

$$p^k m - i = p^l (p^{k-l} m - q),$$

ja p ei jaa lukua $p^{k-l} m - q$, koska $k-l > 0$. Siispä korkein p :n potenssi, joka jakaa termin $p^k m - i$, on p^l . Samalla päättelyllä p^l jakaa kuitenkin myös nimittäjän termin $p^k - i$. Koska osoittajassa ja nimittäjässä on yhtä monta termiä, jokainen tekijä p supistuu pois, joten binomikertoimeen ei jää yhtään tekijää p . \square

LAUSE 4.8 (Sylow). *Oletetaan, että $|G| = p^k m$, missä $k \geq 1$, ja p on alkuluku, joka ei jaa lukua m . Tällöin*

- (i) *Ryhmällä G on Sylowin p -aliryhmä.*
- (ii) *Ryhmän G Sylowin p -aliryhmät ovat keskenään konjugaatteja.*
- (iii) *Jos s_p on Sylowin p -aliryhmien lukumäärä, niin $s_p \equiv 1 \pmod{p}$, ja s_p jakaa luvun m .*

TODISTUS. (i) Olkoon $\mathcal{A}_p = \{A \subset G : |A| = p^k\}$. Määritellään G :n toiminta tässä joukossa *siirtona*: $gA = \{ga \mid a \in A\}$ kaikilla $A \in \mathcal{A}_p$. Lemman 4.7 perusteella joukon \mathcal{A}_p koko ei ole jaollinen p :llä. Radat muodostavat osituksen, joten jollekin radalle GB (missä siis $B \in \mathcal{A}_p$) pätee näin ollen $p \nmid |GB|$. Toisaalta B :n kiinnittäjälle pätee $|G_B| = |G|/|GB|$ (lause 2.7), joten $|G_B|$ on jaollinen luvulla p^k . Olkoon sitten $b_0 \in B$. Jos $g \in G_B$, niin $gB = B$, joten $gb_0 \in B$. Näin saadaan kuvaus $g \mapsto gb_0$ kiinnittäjältä G_B joukolle B . Tämä kuvaus on injektio, joten $|G_B| \leq p^k$. Koska yllä nähtiin että p^k jakaa luvun $|G_B|$, täytyy päteä $|G_B| = p^k$, jolloin G_B on vaadittu Sylowin aliryhmä.

(ii) Olkoon P jokin Sylowin p -aliryhmä, ja Q mikä tahansa p -aliryhmä. Tarkastellaan ryhmän Q siirtotoimintaa tällä kertaa P :n sivuluokkien joukossa. (Harjoitustehtäväksi jää tarkistaa, että tällainen toiminta voidaan määritellä.) Näiden sivuluokkien määrä on $[G : P] = m$, joka ei ole jaollinen p :llä. Koska jokaisen radan koko kuitenkin jakaa ryhmän Q kertaluvun (jälleen lause 2.7) eli on p :n

potenssi, täytyy ratojen joukossa olla jokin yksiö $\{aP\}$. Tällöin $QaP = aP$, joten $a^{-1}Qa \subset P$. On päätelty, että jokaisella p -aliryhmällä on konjugaatti, joka sisältyy annettuun Sylowin p -aliryhmään. Jos Q on itse Sylowin aliryhmä eli $|Q| = |P|$, täytyy olla $a^{-1}Qa = P$.

(iii) Olkoon P yhä jokin Sylowin p -aliryhmä. Nyt P toimii *konjugoimalla* kaikkien Sylowin p -aliryhmien joukossa $\{P, Q_1, \dots, Q_r\}$. Kuten aikaisemmin, ratojen (eli tässä konjugaattiluokkien) koot jakavat toimivat ryhmän kertaluvun $|P| = p^k$. Koska ${}^P P = P$, ryhmän P rata on yksiö. Osoitetaan, että jokaisen muun radan ${}^P Q_i$ koko on jaollinen p :llä. Tällöin nimittäin

$$s_p = 1 + \sum_i p^{k_i},$$

missä i käy läpi kaikki radat ja $k_i \geq 1$ kaikilla i . Tästä seuraa ensimmäinen väite.

Jos ${}^P Q_i = Q_i$, niin P sisältyy normalisoijaan $N_G(Q_i)$. Selvästi sekä P että Q_i ovat tämän normalisoijan Sylowin p -aliryhmiä – yksinkertaisesti siitä syystä, että $N_G(Q_i) \leq G$. Toisaalta $Q_i \trianglelefteq N_G(Q_i)$, joten Q_i ja P eivät ole konjugaatteja ryhmässä $N_G(Q_i)$. Tämä on ristiriidassa kohdan (ii) kanssa, joten $|{}^P \{Q_i\}| > 1$, mikä oli todistettava.

Viimeinen väite seuraa siitä, että ryhmän G konjugointitoiminta kaikkien Sylowin p -aliryhmien joukossa on transitiivista, mikä puolestaan on kohdan (ii) sisältö. Tämä tarkoittaa, että koko ryhmä G on yksi rata eli Sylowin p -aliryhmien konjugaattiluokka. Lauseesta 2.11 saadaan nyt $s_p = [G : N_G(P)]$, joten s_p jakaa ryhmän G kertaluvun $p^k m$. Koska $s_p \equiv 1 \pmod{p}$, niin Eukleideen lemmän perusteella $s_p \mid m$. \square

Kaikki Sylowin p -aliryhmät ovat keskenään konjugaatteja, mistä seuraa, että ne ovat myös keskenään isomorfisia. Toisaalta jokainen Sylowin p -aliryhmän konjugaatti on itse Sylowin p -aliryhmä. Jos tällaisia löytyy vain yksi, kyseinen aliryhmä on silloin väistämättä normaali. Sylowin lauseet auttavat tällä tavoin ns. *yksinkertaisten* ryhmien löytämisessä. Ryhmää sanotaan yksinkertaiseksi, jos sillä ei ole aitoja epätriviaaleja normaaleja aliryhmiä.

ESIMERKKI 4.9. Osoitetaan, että ryhmä, jonka kertaluku on 30, ei voi olla yksinkertainen. Kertaluvun alkutekijähajotelma on $2 \cdot 3 \cdot 5$. Tarkastellaan ensin Sylowin 5-aliryhmiä. Niitä löytyy Sylowin lauseen mukaan s_5 kappaletta, missä

$$s_5 \equiv 1 \pmod{5} \quad \text{ja} \quad s_5 \mid 6.$$

Täytyy siis päteä joko $s_5 = 1$ tai $s_5 = 6$. Ensimmäisessä tapauksessa aliryhmä olisi normaali, joten tarkastellaan jälkimmäistä. Kahden 5-aliryhmän leikkaus on aliryhmä, jonka kertaluku on luvun 5 tekijä. Koska viisi on alkuluku, leikkauksen on oltava triviaali. Ainoa yhteinen alkio kaikissa 5-aliryhmissä on siis neutraalialkio, joten se poisluetettuna ryhmiin sisältyy yhteensä 24 alkioita.

Tarkastellaan sitten Sylowin 3-aliryhmiä. Niitä on s_3 kappaletta, missä $s_3 \equiv 1 \pmod{3}$ ja $s_3 \mid 10$. Näin ollen $s_3 = 1$ tai $s_3 = 10$. Keskitytään jälleen jälkimmäiseen tapaukseen, jolloin näistä kolmen alkion aliryhmistä saadaan yhteensä 20 neutraalialkiota poikkeavaa alkioita. Lisäksi mikään Sylowin 3-aliryhmistä ei voi

kertalukunsa puolesta leikata yhtäkään 5-aliryhmää epätriviaalisti, joten yhteensä on löydetty jo $24 + 20 = 44$ erillistä alkioita. Tämä on ristiriita ryhmän koon kanssa, joten ryhmällä on normaali aliryhmä.

Sylowin lauseet auttavat muutenkin ryhmien rakenteen selvittämisessä.

ESIMERKKI 4.10. Tarkastellaan ryhmiä, joiden kertaluku on $35 = 5 \cdot 7$. Niiden Sylowin 5-aliryhmien lukumäärälle pätee $s_5 \equiv 1 \pmod{5}$ ja $s_5 \mid 7$, joten näitä ryhmiä on vain yksi. Merkitään sitä kirjaimella P . Samalla tavoin Sylowin 7-aliryhmiä on vain yksi; olkoon se Q . Sekä P että Q ovat normaaleja aliryhmiä, ja niiden leikkaus on triviaali. Lauseesta 4.2 seuraa, että koko ryhmä on isomorfinen tuloryhmän $P \times Q \cong \mathbb{Z}_5 \times \mathbb{Z}_7$ kanssa. Lisäksi $\mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{35}$, joten ryhmä on itse asiassa syklinen.

Sylowin lauseesta saadaan seurauksena Cauchyn lause.

LAUSE 4.11 (Cauchy). *Olkoon p jokin ryhmän G kertaluvun alkutekijä. Tällöin G :ssä on alkio, jonka kertaluku on p .*

TODISTUS. Harjoitustehtävä. □

Ääretön p -ryhmä määritellään niin, että sen jokaisen alkion kertaluku on jaollinen p :llä. Äärellisessä tapauksessa tämä määritelmä on yhtäpitävä aiemman kanssa. Lagrangen lauseesta nimittäin seuraa, että p -ryhmän jokaisen alkion kertaluku on jaollinen p :llä. Toisaalta, jos ryhmän kertaluvulla on alkutekijä $q \neq p$, niin Cauchyn lauseen perusteella se sisältää alkion, jonka kertaluku on q .