3.5. Sisäiset symmetriat. Kuution väritysesimerkissä 3.14 tarkasteltiin yksittäisten alkioiden sijaan niiden konjugaattiluokkia ja todettiin, että konjugaattiluokkia vastaavat luonnollisella tavalla erityyppiset kiertoakselit ja eri kiertokulmat. Tarkastellaan vielä lähemmin tätä konjugointia.

Otetaan esimerkiksi kaksi eri kiertoakselia A ja B, joista kumpikin kulkee eräiden vastakkaisten nurkkien kautta. Kierto B:n ympäri saadaan kääntämällä kuutio ensin symmetrialla g niin, että B siirtyy akselin A paikalle, suorittamalla sitten kierto h akselin A ympäri, ja kääntämällä kuutio lopuksi takaisin. Nähdään, että kierto B:n ympäri on itse asiassa $g^{-1}hg$, eli A:n ympäri tapahtuvan kierron konjugaatti.

Ryhmän alkiolla $g \in G$ konjugointi tuottaa ryhmän sisäisen isomorfismin $h \mapsto {}^{g}h$, eli niin sanotun *automorfismin.* Automorfismit ovat ryhmän symmetrioita: ne ovat permutaatioita, jotka säilyttävät ryhmän laskutoimitusrakenteen. Konjugoinnista saatavia automorfismeja kutsutaan *sisäisiksi*, ja ne muodostavat ryhmän $\mathrm{Inn}(G)$.

Ryhmällä voi olla muitakin kuin sisäisiä automorfismeja. Kaikkien automorfismien ryhmää merkitään $\mathrm{Aut}(G)$. Sisäiset automorfismit ovat kuitenkin sellaisia, jotka säilyttävät myös ryhmän toiminnan ominaisuudet. Väritysesimerkissä todettiin, että esimerkiksi $\mathrm{Fix}(g) = \mathrm{Fix}(h)$, jos g ja h ovat samassa konjugaattiluokassa eli saadaan toisistaan jotain sisäistä symmetriaa käyttämällä.

On mahdollista osoittaa, että kuution symmetriaryhmän kaikki automorfismit ovat sisäisiä. Kaikille ryhmille tämä ei kuitenkaan päde. Helppo esimerkki saadaan Kleinin neliryhmästä V_4. Koska se on vaihdannainen, millä tahansa alkiolla konjugointi pitää kaikki alkiot paikallaan, joten $\mathrm{Inn}(V_4) = \{\mathrm{id}\}$. Toisaalta kaikki ryhmän V_4 neutraalialkiosta poikkeavat alkiot ovat keskenään täysin samanarvoisia, ja mikä tahansa niiden permutaatio on kyseisen ryhmän automorfismi. Täten $\mathrm{Aut}(V_4) = S_3$.

4. Ryhmien sisäinen rakenne

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

4.1. Sylowin[9] lauseet. Lagrangen lause kertoo, että äärellisen ryhmän jokaisen 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 konjugaatteja.

[9] Peter Ludwig Mejdell Sylow (1832–1918), norjalainen ryhmäteoreetikko.

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

MÄÄRITELMÄ 4.1. Olkoon p alkuluku. Äärellistä ryhmää sanotaan *p-ryhmäksi*, jos sen kertaluku on p^m jollain $m \geq 1$.

MÄÄRITELMÄ 4.2. 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 aputulos.

LEMMA 4.3. *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

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

Koska luku m ei sisällä yhtään tekijää p, riittää tutkia osoittajan termejä $p^k m - i$, missä $1 \leq i < p^k$. 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. □

LAUSE 4.4 (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 kertolaskulla: $gA = \{ga \mid a \in A\}$ kaikilla $A \in \mathcal{A}_p$. Lemman 4.3 perusteella joukon $\mathcal{A}_p$ koko ei ole jaollinen p:llä. Tämän vuoksi jollekin radalle GB pätee $p \nmid |GB|$. Toisaalta B:n kiinnittäjälle pätee $|G_B| = |G|/|GB|$, joten $|G_B|$ on jaollinen luvulla p^k. Olkoon sitten $b_0 \in B$. Jos $g \in G_B$, niin $gb_0 \in B$. Näin saadaan kuvaus $g \mapsto gb_0$ kiinnittäjältä G_B joukolle B. Tämä kuvaus on injektio, joten $|G_B| \leq p^k$. Siispä $|G_B| = p^k$, ja G_B on vaadittu Sylowin aliryhmä.

(ii) Olkoon P jokin Sylowin p-aliryhmä, ja Q mikä tahansa p-aliryhmä. Tarkastellaan ryhmän Q kertolaskutoimintaa P:n sivuluokkien joukossa. Näiden sivuluokkien määrä on 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 $a^{-1}Qa \subset P$. Täten 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 edelleen jokin Sylowin p-aliryhmä. Nyt P toimii konjugoimalla kaikkien Sylowin p-aliryhmien joukossa $\{P, Q_1, \dots, Q_r\}$. Kuten aikaisemmin, ratojen (eli 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 $|{}^P Q_i| = 1$, niin P sisältyy normalisoijaan $N_G(Q_i)$. Selvästi sekä P että Q_i ovat tämän normalisoijan Sylowin p-aliryhmiä. 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. Tällöin nimittäin $s_p = [G : N_G(P)]$, joten s_p jakaa ryhmän G kertaluvun $p^k m$. Koska $s_p \equiv 1 \pmod p$, niin Eukleideen lemman perusteella $s_p \mid m$. □

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 4.5. Oletetaan, 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

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

Täytyy siis päteä joko $s_5 = 1$ tai $s_5 = 6$. Ensimmäisessä tapauksessa aliryhmä olisi normaali, joten tarkastellaan jälkimmäistä. Viiden alkion aliryhmät leikkaavat toisiaan vain neutraalialkion kohdalla, joten näihin ryhmiin sisältyy neutraalialkio poisluettuna yhteensä 24 alkiota.

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 neutraalialkiosta poikkeavaa alkiota. Lisäksi mikään näistä ei voi sisältyä Sylowin 5-aliryhmään, joten yhteensä on löydetty jo $24 + 20 = 44$ alkiota. Tämä on ristiriita, joten ryhmällä on normaali aliryhmä.

Sylowin lauseet auttavat muutenkin ryhmien rakenteen selvittämisessä.

Esimerkki 4.6. 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. Tästä seuraa, että koko ryhmä on isomorfinen tuloryhmän $P \times Q \cong \mathbb{Z}_5 \times \mathbb{Z}_7$ kanssa (todistetaan myöhemmin). 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 4.7 (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.

4.2. 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 $g_1 = a_1b_1$ ja $g_2 = a_2b_2$ tulo on $g_1g_2 = a_1b_1a_2b_2$. Jos tämä tulo on joukossa AB, niin

$$b_1a_2 = a_1^{-1}\underbrace{(g_1g_2)}_{\in AB}b_2^{-1} \in AB.$$

Siispä vähimmäisvaatimus sille, että tulojoukko olisi aliryhmä, on että b_1a_2 on muotoa $a'b'$ joillain $a' \in A$ ja $b' \in B$. Koska tämän täytyy päteä kaikille alkioille, ehdoksi tulee $AB = BA$. Tämä toteutuu esimerkiksi silloin, kun jokainen A:n alkio kommutoi jokaisen B:n alkion kanssa. Vähempikin kuitenkin riittää.

LEMMA 4.8. *Olkoot H ja N ryhmän G aliryhmiä. 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 $b_1, b_2 \in N$. Koska N on normaali, niin $Na_2^{-1} = a_2^{-1}N$, joten $b_1b_2^{-1}a_2^{-1} = a_2^{-1}b'$ jollain $b' \in N$. Tällöin

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

Siispä HN on aliryhmä. □

Keskitytään jatkossa siihen tapaukseen, missä molemmat aliryhmät ovat normaaleja.

LAUSE 4.9. *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 $f : G \to H \times K$ kaavalla $f(ab) = (a, b)$. Kuvaus on selvästi bijektio. Olkoot $a_1, a_2 \in H$ ja $b_1, b_2 \in K$, jolloin

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

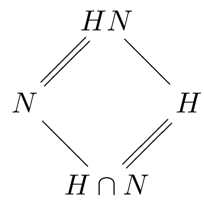
Täten f on homomorfismi. □

Jos edellisen lauseen ehdot pätevät, sanotaan, että G on aliryhmiensä H ja K *sisäinen suora tulo*. Tällöin ei yleensä erotella sisäistä tuloa HK ja ulkoista tuloa $H \times K$, koska nämä ovat keskenään isomorfiset.

4.3. Isomorfialauseet. Seuraavat Emmy Noetherin muotoilemat tulokset selvittävät tekijäryhmien välisiä suhteita. Niiden todistukset nojaavat vahvasti homomorfialauseeseen. Vastaavat tulokset pätevät myös renkaille.

Lause 4.10 (1. isomorfialause[10]). *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 lemman 4.8 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.



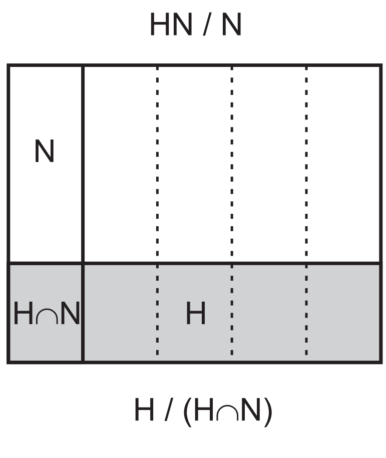
Todistus. Olkoon $\pi : G \to G/N$ kanoninen surjektio, ja olkoon π' sen rajoittuma ryhmään H. Kuvauksen π' arvot ovat siis sivuluokkia hN, missä $h \in H$. Tällaiset sivuluokat kuuluvat tekijäryhmään HN/N, koska $hn \in HN$ jokaisella $n \in N$.

Selvästi

$$\operatorname{Ker} \pi' = \{g \in H \mid g \in N\} = H \cap N,$$

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

[10] Monissa lähteissä homomorfialausetta nimitetään ensimmäiseksi isomorfialauseeksi. Tällöin ensimmäisestä isomorfialauseesta tuleekin toinen isomorfialause, ja toisesta kolmas.

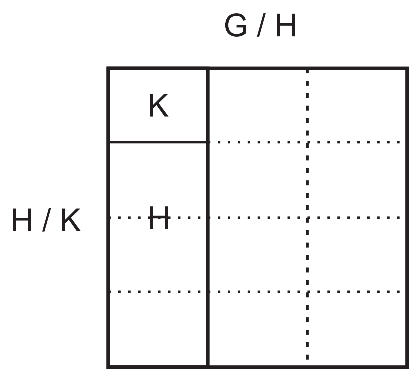


KUVA 8. Noetherin 1. isomorfialause

LAUSE 4.11 (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 $\pi : G \to G/H$ kanoninen surjektio. Koska $K \subset H$, kaikilla $k \in K$ pätee $\pi(k) = H$. Lauseen 1.14 perusteella on olemassa homomorfismi $f : G/K \to G/H$, jolle pätee $f(gK) = gH$. Tämä kuvaus ikään kuin laajentaa sivuluokkia ja on selvästi surjektio. Lisäksi $f(gK) = gH = H$ jos ja vain jos $g \in H$, ja tämä on yhtäpitävää sen kanssa, että $gK \in H/K$. Täten $\operatorname{Ker} f = H/K$, ja tulos seuraa homomorfialauseesta. $\square$



KUVA 9. Noetherin 2. isomorfialause