Tero Harju (2008, 2010, 2012)

Ryhmien operointi ja Sylowin lauseet

Cayleyn lauseen yleistys

Olkoon S_X joukon X **symmetriaryhmä** eli kaikkien permutaatioiden $X \to X$ muodostama ryhmä. Ryhmän S_X aliryhmät ovat **permutaatioryhmiä**.

<u>Lause</u> 1.1 (Cayley). *Jokainen ryhmä on isomorfinen jonkun permutaatioryhmän $G \leq \mathrm{S}_X$ kanssa.*

Itse asiassa, edellä $X = G$, ja isomorfismi on $g \mapsto \tau_g$, missä kaikilla $x \in G$:

$$\tau_g(x) = gx\,.$$

Seuraava tulos on Cayleyn lauseen yleistys.

<u>Lause</u> 1.2. *Olkoon $H \leq G$, jolle indeksi $[G : H] = n$ on äärellinen. Tällöin on homomorfismi $\varphi\colon G \to S_n$, jolle $\mathrm{Ker}(\varphi)$ on suurin normaali aliryhmä niin, että $\mathrm{Ker}(\varphi) \leq H$.*

Todistus. Harjoitus. □

Lauseen 1.1 todistus äärellisille ryhmille. Oletetaan, että $|G| < \infty$, ja valitaan valitaan $H = \{1\}$. Tällöin saadaan Cayleyn alkuperäinen tulos. □

<u>Seuraus</u> 1.1. *Jos G on yksinkertainen ryhmä, ja $H \leq G$ siten, että $[G : H] = n$, niin on olemassa upotus $\varphi\colon G \to S_n$.*

Todistus. Lauseen 1.2 mukaan on olemassa homomorfismi $\varphi\colon G \to S_n$, ja koskapa $\mathrm{Ker}(\varphi) = \{1\}$ normaalina aliryhmänä, on φ upotus. □

<u>Esimerkki</u> 1.1. Tiedetään, että alternoiva ryhmä $G = A_5$ on yksinkertainen. Cayleyn lauseen mukaan A_5 uppoaa symmetriseen ryhmään S_{60}, sillä nyt $|A_5| = 60$. Toisaalta $A_4 \leq G$, missä $|A_4| = 12$, joten $[A_5 : A_4] = 5$, ja niinpä seurauksen 1.1 mukaan A_5 uppoaa symmetriseen ryhmään S_5 (mikä ei ole yllätys).

Tästä saadaan heti seuraava tulos.

<u>Seuraus</u> 1.2. *Jos G on ääretön yksinkertainen ryhmä, niin ei ole aliryhmää $H \leq G$, jolle $[G : H] < \infty$.*

Permutaatioiden yleistys: Ryhmien operointi

Ryhmä G **operoi joukossa** X, jos on kuvaus $g \mapsto \alpha_g$, joka kiinnittää jokaiseen $g \in G$ funktion $\alpha_g \colon X \to X$, jolle

(i) $\alpha_g \alpha_h = \alpha_{gh}$ kaikille $g, h \in G$, ja
(ii) $\alpha_1 = id$ on identiteettifunktio.

Tällöin sanotaan myös, että X on G**-joukko**.

Jos G operoi joukossa X, kirjoitetaan mieluummin $g{\cdot}x$ merkinnän $\alpha_g(x)$ asemesta. Tällöin edeltävät ehdot saavat muodon:

$$g{\cdot}(h{\cdot}x) = (gh){\cdot}x \quad \text{ja} \quad 1{\cdot}x = x\,.$$

Operointi voidaan ilmoittaa myös kirjoittamalla $g \colon x \mapsto \alpha_g(x)$, kun $g \in G$ ja $x \in X$.

<u>Esimerkki</u> 1.2. (1) Permutaatioryhmä $G \leq \mathrm{S}_X$ operoi joukossa X luonnollisella tavalla.

(2) Cayleyn lauseen mukaan ryhmä G operoi joukossa G.

(3) Ryhmä G operoi konjugoimalla: jos $g \in G$, niin $\alpha_g(x) = gxg^{-1}$ (harjoitus). Tämä voidaan ilmaista myös seuraavasti: $g \colon x \mapsto gxg^{-1}$.

<u>Lemma</u> 1.1. *Jos ryhmä G operoi joukossa X, niin $\alpha_g \in \mathrm{S}_X$. Erityisesti*

$$g{\cdot}x = y \implies x = g^{-1}{\cdot}y$$
$$g{\cdot}x = g{\cdot}y \implies x = y$$

kaikille $g \in G$ ja $x, y \in X$.

Todistus. Todetaan, että $\alpha_g \alpha_{g^{-1}}(x) = \alpha_{gg^{-1}}(x) = \alpha_1(x) = x$, joten $\alpha_{g^{-1}}$ on kuvauksen α_g käänteiskuvaus, ja siten α_g on joukon X permutaatio. □

Operoikoon G joukossa X. Alkion $x \in X$ **rata** on joukko

$$\mathrm{Orb}(x) = \{g{\cdot}x \mid g \in G\}\,.$$

Alkion x **stabiloija** on

$$G_x = \{g \in G \mid g{\cdot}x = x\}\,.$$

<u>Lemma</u> 1.2. *Jos G operoi joukossa X, niin $G_x \leq G$ kaikilla $x \in X$.*

Todistus. Harjoitus. □

<u>Esimerkki</u> 1.3. Olkoon τ_g Cayleyn lauseen operointi: $\tau_g(x) = gx$. Tällöin $\mathrm{Orb}(x) = G$, sillä jos $g \in G$, niin $g = (gx^{-1})x$, ja siten $g \in \mathrm{Orb}(x)$. Tässä tapauksessa on myös $G_x = \{1\}$, sillä jos $x = \tau_g(x) = gx$, niin toki $g = 1$.

Esimerkki 1.4. Kun G operoi konjugoimalla, merkitään $\mathrm{Orb}(x) = x^G$. Siis

$$x^G = \{axa^{-1} \mid a \in G\}\,.$$

Sanotaan että x^G on alkion x **konjugaattiluokka**.

Alkion $x \in G$ **sentralisoija** on

$$C_G(x) = \{g \in G \mid gxg^{-1} = x\}.$$

Siis $g \in C_G(x)$ jos ja vain jos g kommutoi alkion x kanssa.

Seuraavassa lauseessa **edustajisto** on osajoukko $Y \subseteq X$, johon jokaisesta radasta on valittu yksikäsitteinen alkio.

Lause 1.3. *Operoikoon ryhmä G joukossa X. Tällöin X on alkioidensa ratojen partitio. Lisäksi, jos $|X| < \infty$ ja $Y \subseteq X$ on ratojen edustajisto, niin*

$$|X| = \sum_{y \in Y} |\,\mathrm{Orb}(y)|\,.$$

Todistus. Olkoon $x \in X$. Tällöin $x = 1{\cdot}x \in \mathrm{Orb}(x)$, ja siten $X = \cup_{x \in X} \mathrm{Orb}(x)$.

Jos $\mathrm{Orb}(x) \cap \mathrm{Orb}(y) \neq \emptyset$, niin on olemassa alkiot $g, h \in G$ siten, että $g{\cdot}x = h{\cdot}y$. Tässä tapauksessa $x = g^{-1}h{\cdot}y$ ja samoin $y = h^{-1}g{\cdot}x$. Olkoon $a \in \mathrm{Orb}(x)$ eli $a = f{\cdot}x$ jollain $f \in G$. Tällöin edeltävän mukaan, $a = fg^{-1}h{\cdot}y \in \mathrm{Orb}(y)$. Näin ollen $\mathrm{Orb}(x) \subseteq \mathrm{Orb}(y)$. Symmetrisesti saadaan sisältyminen toiseen suuntaan, ja siten $\mathrm{Orb}(x) = \mathrm{Orb}(y)$. Tästä osituksesta seuraa myös väitteen viimeinen kaava. □

Lause 1.4. *Jos ryhmä G operoi joukossa X ja $x \in X$ on annettu alkio, niin*

$$|\,\mathrm{Orb}(x)| = [G : G_x]\,.$$

Todistus. Määritellään kuvaus $\gamma\colon\ \mathrm{Orb}(x) \to G/G_x$ ehdosta

$$y = g{\cdot}x \implies \gamma(y) = gG_x\,.$$

Tällöin γ on hyvin määritelty: jos $y = g{\cdot}x = h{\cdot}x$, missä $g, h \in G$, niin $h^{-1}g{\cdot}x = x$ ja siten $h^{-1}g \in G_x$, mistä seuraa että $hG_x = gG_x$.

Kuvaus γ on bijektio: Oletetaan, että $\gamma(y) = \gamma(z)$. Tällöin on alkiot $g, h \in G$, joilla $y = g{\cdot}x$ ja $z = h{\cdot}x$ siten, että $gG_x = hG_x$. Nyt $h^{-1}g \in G_x$ ja siten $h^{-1}g{\cdot}x = x$ eli $y = g{\cdot}x = h{\cdot}x = z$. Näin ollen γ on injektiivinen. Toisaalta, jos $gG_x \in G/G_x$, niin olkoon $y = g{\cdot}x \in \mathrm{Orb}(x)$. Tällöin $\gamma(y) = gG_x$, ja siten γ on surjektiivinen.

Siis $|\,\mathrm{Orb}(x)| = |G/G_x| = [G : G_x]$, mikä oli väite. □

Esimerkki 1.5. Diedriryhmä D_4 operoi neliön kärkipisteiden v_0, v_1, v_2, v_3 joukossa permutoimalla ne. Vain permutaatio $g = (v_1\ v_3) \in \mathrm{D}_4$ ja identiteettikuvaus kiinnittävät pisteen v_0. Siis G_{v_0} on kertalukua kaksi oleva aliryhmä: $|G_{v_0}| = 2$. Voidaan laskea, että $|\,\mathrm{Orb}(v_0)| = 4$ ja $[G : G_{v_0}] = 4\ (= 8/2)$.

Lagrangen lauseen mukaan saadaan:

Seuraus 1.3. *Olkoon G äärellinen ryhmä, joka operoi joukossa X. Tällöin $|\operatorname{Orb}(x)|$ jakaa ryhmän kertaluvun $|G|$.*

Seuraus 1.4. *Olkoon G äärellinen ryhmä. Tällöin alkion $x \in G$ konjugaattien lukumäärä on*

$$|x^G| = [G : C_G(x)]\,,$$

ja siten $|x^G|$ jakaa ryhmän G kertaluvun $|G|$.

Todistus. Alkiolle $x \in G$, $\operatorname{Orb}(x) = x^G$, ja toisaalta $G_x = C_G(x)$. □

Operoikoon ryhmä G aliryhmien joukossa konjugoimalla, eli

$$g{\cdot}H = gHg^{-1}\,, \text{ kun } H \leq G\,.$$

Tällöin merkitään stabiloijaa $G_H = N_G(H)$ ja sitä kutsutaan **normalisoijaksi**. Siis

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}\,.$$

Lemman 1.2 mukaan normalisoija on ryhmän G aliryhmä.

Lemma 1.3. *Olkoon $H \leq G$. Tällöin $N_G(H)$ on suurin ryhmän G aliryhmä, jolle $H \trianglelefteq N_G(H)$.*

Todistus. Harjoitus. □

Lause 1.5. *Olkoon $H \leq G$. Tällöin aliryhmän H konjugaattien xHx^{-1} ($x \in G$) lukumäärä on sama kuin indeksi $[G : N_G(H)]$.*

Todistus. Olkoon operointi osajoukkojen joukossa konjugoimalla. Lauseen 1.4 mukaan $|\operatorname{Orb}(H)| = [G : G_H]$, missä $G_H = N_G(H) = C_G(H)$. Siten väite seuraa seurauksesta 1.4. □

Ryhmän **keskus** $Z(G)$ koostuu niistä alkioista, jotka kommutoivat kaikkien alkioiden kanssa, ja niinpä

$$Z(G) = \{x \in G \mid |x^G| = 1\}.$$

Lause 1.6 (Luokkayhtälö). *Olkoon G äärellinen ryhmä, ja olkoon A niiden konjugaattiluokkien, jotka sisältävät vähintään kaksi alkiota, edustajisto. Tällöin*

$$|G| = |Z(G)| + \sum_{x \in A} [G : C_G(x)]\,. \tag{1.1}$$

Todistus. Seuraus 1.4 antaa väitteen, koskapa konjugaattiluokat muodostavat ryhmän G partition. □

Lemma 1.4. *Olkoon G äärellinen ryhmä, joka operoi äärellisessä joukossa X. Jos $x, y \in \mathrm{Orb}(z)$ jollain z, niin $y = g{\cdot}x$ jollain $g \in G$ ja $G_y = gG_xg^{-1}$. Erityisesti,*

$$x, y \in \mathrm{Orb}(z) \implies |G_y| = |G_x|\,.$$

Todistus. Oletetaan, että $x, y \in \mathrm{Orb}(z)$ eli $x = a{\cdot}z$ ja $y = b{\cdot}z$ joillain $a, b \in G$, ja siten $y = b{\cdot}(a^{-1}{\cdot}z) = (ba^{-1}){\cdot}x \in \mathrm{Orb}(x)$, missä siis $g = ba^{-1}$.

Olkoon $h \in G_x$ eli $h{\cdot}x = x$. Nyt $y = g{\cdot}x$, ja siten

$$ghg^{-1}{\cdot}y = ghg^{-1}g{\cdot}x = gh{\cdot}x = g{\cdot}x = y\,,$$

ja siksi $gG_xg^{-1} \leq G_y$. Vastaavasti voidaan osoittaa, että $G_y \leq gG_xg^{-1}$ käyttäen yhtäsuuruutta $x = g^{-1}{\cdot}y$.

Kuvaus $\varphi_g\colon G \to G$ ehdosta $\varphi_g(h) = ghg^{-1}$ on automorfismi, jolle ylläolevan mukaan on $\varphi_g(G_x) = G_y$. Näin ollen $|G_x| = |G_y|$. □

Sylowin lauseet

Lause 1.7 (Cauchy). *Olkoon p alkuluku, joka jakaa äärellisen ryhmän G kertaluvun n. Tällöin on olemassa alkio $x \in G$, jolle $\mathrm{ord}(x) = p$.*

Lause 1.7 seuraa oheisesta yleisemmästä tuloksesta, jonka todisti J.H. McKay (1959).

Lause 1.8. *Olkoon p alkuluku, joka jakaa kertaluvun $|G|$. Tällöin yhtälöllä $x^p = 1$ on rp ratkaisua jollain $r > 0$.*

Todistus. Tarkastellaan joukkoa

$$X = \{(x_1, \ldots, x_p) \mid x_1 \cdots x_p = 1\}.$$

Tällöin $|X| = |G|^{p-1}$, sillä jokaista $(x_1, \ldots, x_{p-1})$ vastaa yksikäsitteinen x_p, jolle $x_1x_2 \ldots x_p = 1$. Siten $|X|$ on alkuluvun p monikerta. Määritellään ekvivalenssirelaatio $\sim$ joukossa X: $\alpha \sim \beta$ jos ja vain jos α ja β ovat toistensa syklisiä konjugaatteja. Siis jos $\alpha = (x_1, \ldots, x_p)$, niin $\beta = (x_i, \ldots, x_p, x_1, \ldots, x_{i-1})$ jollain i. Olkoon joukossa X tarkalleen k sellaista alkiota, joiden ekvivalenssiluokassa on vain yksi alkio, joka on siis välttämättä muotoa $(x, x, \ldots, x) \in X$, missä $x^p = 1$. Huomaa, että $(1, 1, \ldots, 1) \in X$ ja siten $k \geq 1$. Kaikissa muissa luokissa on tarkalleen p alkiota, koska p on alkuluku. Siis $|G|^{p-1} = k + p \cdot t$ jollain t. Koskapa $p||G|$, myös $p|k$, mistä väite seuraa. □

Olkoon p alkuluku. Ryhmä G, jonka kertaluku on luvun p potenssi on **p-ryhmä**. Lagrangen lauseen nojalla sen kaikkien alkioiden kertaluvut ovat luvun p potensseja.

Olkoon G äärellinen p-ryhmä, joka operoi yli joukon X. Merkitään

$$\mathrm{Fix}(G) = \{x \in X \mid \forall g \in G\colon g{\cdot}x = x\}.$$

Lemma 1.5. *Olkoon G äärellinen p-ryhmä, joka operoi yli joukon X. Tällöin*

$$|X| = |\operatorname{Fix}(G)| + \sum_{\substack{x \in I \\ x \notin \operatorname{Fix}(G)}} |\operatorname{Orb}(x)|\,, \tag{1.2}$$

missä I on ratojen edustajisto. Erityisesti,

$$|X| \equiv |\operatorname{Fix}(G)| \pmod{p}. \tag{1.3}$$

Todistus. Nyt $|X| = \sum_{x \in I} |\operatorname{Orb}(x)|$. Toisaalta, jos $x \in \operatorname{Fix}(G)$, niin $g{\cdot}x = x$ kaikilla $g \in G$ ja siten $|\operatorname{Orb}(x)| = 1$. Jälkimmäistä väitettä varten todetaan, että jos $x \notin \operatorname{Fix}(G)$, niin $|\operatorname{Orb}(x)| = p^k$ jollain $k \geq 1$, sillä $|G| = |\operatorname{Orb}(x)| \cdot |G_x|$ Lagrangen lauseen mukaan. □

Seuraus 1.5. *Olkoon G äärellinen p-ryhmä. Tällöin $Z(G) \neq \{1\}$.*

Todistus. Tarkastellaan ryhmän G operointia konjugoimalla yli itsensä: $g\colon a \mapsto gag^{-1}$. Nyt $X = G$ ja siten $|X| = p^n$ jollain $n \geq 1$. Tällöin kongruenssin (1.3) mukaan $|\operatorname{Fix}(G)| > 1$. Mutta $\operatorname{Fix}(G) = \{x \in G \mid gxg^{-1} = x\} = Z(G)$. □

Lause 1.9 (Sylow I). *Olkoon G kertalukua $p^n m$ oleva ryhmä, missä p on alkuluku, jolle $p \nmid m$.*

(1) Tällöin ryhmällä G on kertalukua p^i oleva aliryhmä kaikille $i = 0, 1, \ldots, n$.
(2) Lisäksi, jos $H_i \leq G$ on kertalukua p^i oleva aliryhmä, niin on kertalukua p^{i+1} oleva aliryhmä $H_{i+1} \leq G$, jolle $H_i \trianglelefteq H_{i+1}$ kun $0 \leq i \leq n-1$.

Todistus. Todistetaan olemassaolo induktiolla potenssiin nähden. Cauchyn lauseen mukaan ryhmällä G on kertalukua p oleva alkio ja siten kertalukua p oleva (syklinen) aliryhmä.

Oletetaan sitten, että $H \leq G$ on kertalukua $|H| = p^i$, missä $i < n$. Tarkastellaan ryhmän H operointia yli tekijäjoukon $X = G/H$:

$$h{\cdot}(xH) = (hx)H\,.$$

Tässä

$$\begin{aligned}
xH \in \operatorname{Fix}(H) &\iff xH = hxH \text{ kaikilla } h \in H \\
&\iff x^{-1}hx \in H \text{ kaikilla } h \in H \\
&\iff x^{-1}Hx \subseteq H \\
&\iff Hx \subseteq xH \\
&\iff Hx = xH \qquad (\text{sillä } |Hx| = |H| = |xH|) \\
&\iff H = xHx^{-1} \\
&\iff x \in N_G(H)\,.
\end{aligned}$$

Siis $|\operatorname{Fix}(H)| = [N_G(H) : H]$. Koskapa $i < n$, niin

$$|\operatorname{Fix}(H)| \equiv |X| = p^{n-i}m \equiv 0 \pmod{p}\,.$$

Cauchyn lauseen mukaan ryhmällä $N_G(H)/H$ on kertalukua p oleva aliryhmä, ja tämä aliryhmä on muotoa H'/H. Näin ollen $|H'| = p^{i+1}$ ja myös $H \trianglelefteq H'$. □

<u>Seuraus</u> 1.6. *Jokainen äärellinen p-ryhmä on ratkeava.*

Todistus. Olkoon $|G| = p^n$. Tällöin on sarja aliryhmiä:

$$\{1\} = H_0 < H_1 < ... < H_n = G$$

siten, että $|H_i| = p^i$ ja $H_i \trianglelefteq H_{i+1}$. Vieläpä $H_{i+1}/H_i \cong C_p$. □

Sylowin lauseesta seuraa, että jokaisella äärellisellä ryhmällä G, jolle $|G| = p^n m$ kuten edellä, on kertalukua p^n oleva maksimaalinen p-aliryhmä. Tällaista ryhmää kutsutaan **Sylowin p-aliryhmäksi**.

<u>Lause</u> 1.10 (Sylow II). *Olkoon $|G| = p^n m$, missä alkuluku p ei jaa lukua m. Olkoot P ryhmän G Sylowin p-aliryhmä ja H ryhmän G jokin p-aliryhmä. Tällöin on olemassa $x \in G$ niin, että $xHx^{-1} \leq P$.*

Todistus. Merkitään $X = G/P$, ja operoikoon H yli joukon X kuten edellä: $h{\cdot}(xP) = hxP$, jolloin lemman 1.5 mukaan $|\operatorname{Fix}(H)| \equiv |X| = m \pmod{p}$. Eritoten on $\operatorname{Fix}(H) \neq \emptyset$, ja

$$xP \in \operatorname{Fix}(H) \iff \forall h \in H\colon hxP = xP \iff x^{-1}Hx \leq P\,.$$

Väite seuraa tästä. □

<u>Seuraus</u> 1.7. *Olkoon $|G| = p^n m$, missä alkuluku p ei jaa lukua m. Tällöin kaikki ryhmän G Sylowin p-aliryhmät ovat toistensa konjugaatteja: jos P ja H ovat Sylowin p-aliryhmiä, niin $P = x^{-1}Hx$ jollain $x \in G$.*

<u>Lause</u> 1.11 (Sylow III). *Olkoon $|G| = p^n m$, missä alkuluku p ei jaa lukua m, ja olkoon k_p ryhmän G Sylowin p-aliryhmien lukumäärä. Tällöin $k_p | m$ ja $k_p \equiv 1 \pmod{p}$.*

Todistus. Olkoon P jokin Sylowin p-aliryhmä, ja olkoon $\mathcal{X} = \{xPx^{-1} \mid x \in G\}$ aliryhmän P konjugaattiluokka. Seurauksen 1.7 mukaan $\mathcal{X}$ koostuu kaikista Sylowin p-aliryhmistä, ja näin ollen lauseen 1.5 mukaan $k_p = |\mathcal{X}| = [G : N_G(P)]$.

Tarkastellaan ryhmän G operointia konjugoimalla yli joukon $\mathcal{X}$ eli $g\colon H \mapsto gHg^{-1}$ ($g \in G$, $H \in \mathcal{X}$). Lauseen 1.10 mukaan tämä operointi on transitiivista: jos $H, K \in \mathcal{X}$, niin on olemassa $g \in G$, jolla $K = gHg^{-1}$ ja siten $\operatorname{Orb}(H) = \mathcal{X}$ kullakin $H \in \mathcal{X}$. Näin ollen $k_p = |\mathcal{X}|$ jakaa kertaluvun $|G| = p^n m$, sillä $|G| = |G_H| \cdot |\operatorname{Orb}(H)|$.

Tarkastellaan nyt ryhmän P vastaavaa operointia: $g\colon H \to gHg^{-1}$ ($g \in P$, $H \in \mathcal{X}$). Olkoon $H \in \mathcal{X}$. Tällöin

$$H \in \mathrm{Fix}(P) \iff \forall g \in P\colon gHg^{-1} = H \iff P \leq N_G(H)\,.$$

Tässä tapauksessa sekä P että H ovat ryhmän $N_G(H)$ Sylowin p-aliryhmiä ja siten ne ovat konjugaatteja ryhmässä $N_G(H)$. Lemman 1.3 mukaan $H \trianglelefteq N_G(H)$ ja siten ryhmällä H ei ole muita konjugaatteja ryhmässä $N_G(H)$ kuin se itse, joten $P = H$, ja eritoten $\mathrm{Fix}(P) = \{P\}$. Lemman 1.5 mukaan $k_p = |\mathfrak{X}| \equiv 1 \pmod p$. Tällöin myös $p \not| k_p$, ja niinpä $k_p | m$. □

Esimerkkejä

<u>Esimerkki</u> 1.6. Osoitetaan, että kertalukua 200 oleva ryhmä ei ole yksinkertainen. Tätä varten olkoon $|G| = 200 = 2^3 \cdot 5^2$. Tällöin $k_5 = 1$, sillä $k_5 \equiv 1 \pmod 5$ ja $k_5 | 2^3$. Siten jos P on Sylowin 5-aliryhmä, myös gPg^{-1} on Sylowin p-aliryhmä, ja näin ollen $gPg^{-1} = P$ kaikilla $g \in G$, mikä tietää, että $P \trianglelefteq G$. Johtopäätöksenä todetaan, että G ei ole yksinkertainen ryhmä.

<u>Esimerkki</u> 1.7. Olkoon p alkuluku. Osoitetaan, että kertalukua $2p$ oleva ryhmä on joko syklinen tai diedraaliryhmä. Myös tapauksessa $p = 1$ ainoa ryhmä on syklinen: $\mathbb{Z}_2$. Oletetaan sitten, että $p > 2$.

Olkoon $H \leq G$ niin, että $|H| = p$, sanokaamme $H = \langle x \rangle$. Sylowin lauseen mukaan $k_p = 1$ ja siten $H \trianglelefteq G$. Samoin on aliryhmä $U \leq G$ siten, että $|U| = 2$, sanokaamme $U = \langle y \rangle$. Koska H on normaali, $yxy^{-1} = x^k$ jollain k. Nyt

$$x = y^2xy^{-2} = yx^ky^{-1} = x^{k^2}$$

ja näin ollen $k^2 \equiv 1 \pmod p$. Siis $k \equiv 1 \pmod p$ tai $k \equiv -1 \pmod p$.

(1) Oletetaan, että $k \equiv 1 \pmod p$. Tällöin $xy = yx$, ja siten G on Abelin ryhmä. Kiinalaisen jäännösluokkalauseen nojalla G on syklinen.

(2) Oletetaan sitten, että $k \equiv -1 \pmod p$. Tällöin $xy = yx^{-1}$. Tämä ryhmä on kertalukua $2p$ oleva diedraaliryhmä.

Wielandtin todistus Sylowin aliryhmän olemassaololle

<u>Lemma</u> 1.6. *Osoita, että alkuluku p ei jaa lukua $\binom{p^nm}{p^n}$, missä $p \not| m$ ja $n \geq 1$.*

Todistus. Itse asiassa $\binom{p^nm}{p^n} \equiv m \pmod p$.

Tarkastellaan polynomia $f(x) = x + 1$. Koskapa $p \in \mathbb{P}$, niin $f(x)^p = \sum_{i=0}^{n} \binom{p}{i} x^i \equiv x^p + 1 \pmod p$. (Tarkastele binomikertoimia $\binom{p}{i}$.) Toistetaan tämä induktiivisesti, jolloin saadaan

$$f(x)^{p^n} \equiv x^{p^n} + 1 \pmod p\,, \text{ ja siis } (x+1)^{p^nm} \equiv (x^{p^n} + 1)^m \pmod p\,.$$

Oikeanpuolen tekijän x^{p^n} kerroin on m, ja samoin täytyy olla vasemmanpuolen saman tekijän kerroin $\binom{p^nm}{p^n}$ modulo p. Tästä väite seuraa. □

Lause 1.12. *Olkoon G kertalukua $p^n m$ oleva ryhmä, missä alkuluku p ei jaa lukua m. Tällöin ryhmällä G on Sylowin p-aliryhmä.*

Todistus. Olkoon $\mathcal{A} = \{A \subset G \mid |A| = p^n\}$. Tällöin G operoi joukossa $\mathcal{A}$ luonnolliseen tapaan: $gA = \{g(a) \mid a \in A\}$.

Osoitetaan, että on olemassa rata $\mathrm{Orb}(A)$, $A \in \mathcal{A}$, jonka kokoa p ei jaa.

Operointi osittaa perheen $\mathcal{A}$ ratoihin, joten $|\mathcal{A}|$ on ratojen kokojen summa. Niinpä

$$|\mathcal{A}| \equiv \binom{p^n m}{p^n} \pmod{p},$$

missä p ei jaa binomikerrointa Lemman 1.6 nojalla. Siis on olemassa ainakin yksi rata, jolle $p \not| |\mathrm{Orb}(A)|$.

Olkoon $H = G_A$ joukon A stabiloija, jolloin $|G| = |\mathrm{Orb}(A)| \cdot |H|$. Koska p ei jaa radan kokoa, mutta p^n jakaa ryhmän G kertaluvun, jakaa p^n ryhmän H kertaluvun, ja siten $p^n \leq |H|$. Nyt H stabiloi alkion $A \in \mathcal{A}$, joten jos $a \in A$, niin $Ha \subseteq A$. Saadaan, että $|H| = |Ha| \leq |A| = p^n$. Yhdistämällä saadaan, että $|H| = p^n$, joten H on ryhmän G Sylowin aliryhmä. □

Abelin ryhmät

Seuraavassa tuloksessa G ei ole välttämättä Abelin ryhmä.

Lause 1.13. *Olkoon G kertalukua $p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ oleva ryhmä, missä $p_1, \ldots, p_r$ ovat eri alkulukuja, ja olkoon P_i ryhmän G Sylowin p_i-aliryhmä. Tällöin $G \cong P_1 \times P_2 \times \cdots \times P_r$ jos ja vain jos jokainen Sylowin aliryhmä P_i on normaali.*

Todistus. (1) Jos $G \cong P_1 \times P_2 \times \cdots \times P_r$, niin jokainen P_i on normaali.

(2) Oletetaan, että $P_i \trianglelefteq G$, $i = 1, 2, \ldots, r$. Selvästi $P_i \cap P_j = \{1\}$ kun $i \neq j$. Olkoot $g_i \in P_i$, kun $i = 1, 2, \ldots, r$. Normaaliudesta seuraa, että $[g_i, g_j] = g_i g_j g_i^{-1} g_j^{-1} = 1$, sillä $g_i g_j g_i^{-1} \in P_j$ ja $g_j g_i^{-1} g_j^{-1} \in P_i$. Siten alkiot g_i ja g_j kommutoivat.

Oletetaan, että $g_1 g_2 \cdots g_r = 1$, missä $g_i \in P_i$ on kertalukua $m_i = p_i^{s_i}$. Olkoon $1 \leq j \leq r$ ja merkitään $m = m_1 m_2 \cdots m_{j-1} m_{j+1} \ldots m_r$. Tällöin kommutoinnin avulla saadaan $1 = (g_1 g_2 \cdots g_r)^m = g_1^m g_2^m \cdots g_r^m = g_j^m$. Koska $g_j^{m_j} = 1$ ja $\mathrm{syt}(m, m_j) = 1$, niin välttämättä $g_j = 1$. Kaiken kaikkiaan siis $1 = g_1 = g_2 = \ldots = g_r$.

Oletetaan sitten, että

$$x = g_1 g_2 \ldots g_r \quad \text{missä } g_i \in P_i\,. \tag{1.4}$$

Jos myös $x = h_1 h_2 \ldots h_r$, missä $h_i \in P_i$, niin jälleen kommutointiin vedoten saadaan

$$1 = (g_1 g_2 \cdots g_r)(h_1 h_2 \cdots h_r)^{-1} = (g_1 h_1^{-1}) \cdots (g_2 h_2^{-1}) \cdots (g_r h_r^{-1}) \text{ missä } g_i h_i^{-1} \in P_i\,,$$

ja siten $g_i h_i^{-1} = 1$, jolloinka $g_i = h_i$ kaikilla i. Siis jokaisella alkiolla $x \in P_1 P_2 \cdots P_r$ on yksikäsitteinen esitys (1.4). Tästä seuraa, että $P_1 \times P_2 \times \cdots \times P_r \cong P_1 P_2 \ldots P_r \subseteq G$. Lisäksi $|P_1 \times P_2 \times \cdots \times P_r| = |G|$ ja näin ollen $G \cong P_1 \times P_2 \times \cdots \times P_r$. □

Lause 1.14. *Olkoon G kertalukua $p^n m$ oleva Abelin ryhmä, missä alkuluku p ei jaa lukua m. Merkitään*

$$G(p) = \{g \in G \mid \textit{alkion } g \textit{ kertaluku on alkuluvun } p \textit{ potenssi}\}.$$

Tällöin $G(p)$ on yksikäsitteinen ryhmän G Sylowin p-aliryhmä.

Todistus. Selvästi $G(p) \leq G$. Olkoon P Sylowin p-ryhmä, jolloin $|P| = p^n$. Sylowin lauseen nojalla P on yksikäsitteinen, sillä G on Abelin ryhmä. Jokaisen alkion $a \in P$ kertaluku on alkuluvun p potenssi, ja siten $a \in G(p)$, eli $P \subseteq G(p)$. Mutta $G(p)$ on ryhmän G p-aliryhmä, ja siten se sisältyy konjugaattiryhmään: $G(p) \subseteq aPa^{-1} = P$ (Abelin ryhmä). Näin $G(p) = P$. □

Lause 1.15. *Olkoon G kertalukua $p_1^{n_1} p_2^{n_2} \dots p_n^{n_r}$ oleva Abelin ryhmä. Tällöin*

(1) $G = G(p_1) \oplus G(p_2) \oplus \cdots \oplus G(p_r)$.
(2) $|G(p_i)| = p_i^{n_i}$ *kaikilla* $i = 1, 2, \dots, r$.

Todistus. Olkoon $|G| = p_i^{n_i} m_i$, missä alkuluku p_i ei jaa lukua m_i. Edeltävän nojalla $G(p_i)$ on yksikäsitteinen Sylowin p_i-aliryhmä, ja näin ollen väite (2) seuraa. Lisäksi, $G(p_i) \trianglelefteq G$ kaikilla i, joten myös väite (1) on voimassa. □