# Alternoivien ryhmien ominaisuuksista

Pro gradu -tutkielma

Anssi Aska

2257068

Matemaattisten tieteiden laitos

Oulun yliopisto

2017

# Sisältö

# 1 Johdanto

Tutkielma käsittelee permutaatioryhmiä, erityisesti parillisista permutaatioista koostuvia alternoivia ryhmiä. Sen päätulokset ovat alternoivien ryhmien $A_n$ yksinkertaisuus, kun aste $n$ on vähintään 5, sekä Ei-Burnsiden lemma, jonka avulla permutaatioryhmän ratojen lukumäärä voidaan laskea.

Kappaleessa 2 esitellään ryhmäteorian peruskäsitteitä ja -tuloksia, joita tarvitaan myöhemmin tutkielman aikana. Kappaleessa 3 keskitytään permutaatioihin ja niistä muodostuvaan symmetriseen ryhmään.

Kappaleessa 4 määritellään, mitä ovat parilliset ja parittomat permutaatiot. Lisäksi osoitetaan, että parilliset permutaatiot muodostavat symmetrisen ryhmän normaalin aliryhmän, alternoivan ryhmän. Symmetristen ja alternoivien ryhmien alkioiden rakenteita tarkastellaan myös hieman tarkemmin pienillä asteen $n$ arvoilla.

Kappaleessa 5 määritellään ryhmän alkioiden konjugointi sekä aliryhmien muodostama kompleksi, ja todistetaan joitakin niihin liittyviä tärkeitä tuloksia. Lisäksi määritellään aliryhmän normalisoija ja ryhmän keskus. Lopuksi osoitetaan alternoivan ryhmän $A_n$ yksinkertaisuus ensin tapaukselle $n = 5$ ja sitten yleiselle tapaukselle.

Kappaleessa 6 keskitytään permutaatioryhmien soveltamiseen käytännön ongelmiin. Ennen tätä määritellään permutaatioryhmän stabiloijat ja radat sekä todistetaan niihin liittyvä Ei-Burnsiden lemma. Sen jälkeen esimerkkien avulla havainnollistetaan, miten tulosta voidaan hyödyntää kombinatorisissa tarkasteluissa.

Lopuksi kappaleessa 7 palataan käsittelemään alternoivaa ryhmää. Tutkielman viimeisenä tuloksena osoitetaan, että jokaisessa vähintään astetta 7 olevassa alternoivassa ryhmässä on permutaatio, jonka kertaluku on suurempi kuin eräs ryhmän asteesta riippuva luku.

# 2 Peruskäsitteitä

Tässä kappaleessa esitellään myöhemmin tutkielmassa tarvittavat ryhmäteorian peruskäsitteet kuten ryhmä, aliryhmä, sivuluokka, normaali aliryhmä, tekijäryhmä ja homomorfismi. Kappale koostuu ryhmäteorian alkeellisista perustuloksista, joiden todistukset sivuutetaan. Todistukset löytyvät useimmista ryhmäteorian oppikirjoista, esimerkiksi lähteestä [4].

## 2.1 Ryhmä ja aliryhmä

**Määritelmä 2.1.** Epätyhjä joukko $G$ varustettuna binäärisellä operaatiolla $*$ on *ryhmä*, mikäli seuraavat ehdot ovat voimassa:

1) $a * b \in G$ aina, kun $a, b \in G$

2) $(a * b) * c = a * (b * c)$ aina, kun $a, b, c \in G$

3) on olemassa *neutraalialkio* $e \in G$, jolle pätee

$$e * a = a \quad \text{ja} \quad a * e = a$$

aina, kun $a \in G$

4) jokaiselle alkiolle $a \in G$ on olemassa *käänteisalkio* $a^{-1} \in G$, jolle pätee

$$a^{-1} * a = e \quad \text{ja} \quad a * a^{-1} = e.$$

Ryhmää merkitään parina $(G, *)$. Ellei operaatiota ole tarpeen korostaa, ryhmää merkitään yleensä vain joukkona $G$. Myös operaatiomerkki voidaan jättää pois ja merkitä lyhyesti $a * b = ab$.

Jos alkioille $a, b \in G$ pätee $ab = ba$, niiden sanotaan *kommutoivan* ryhmässä $G$. Jos ryhmän kaikki alkiot kommutoivat keskenään, toisin sanoen

$ab = ba$ aina, kun $a, b \in G$, ryhmää kutsutaan *kommutatiiviseksi* eli *Abelin ryhmäksi.*

Jos ryhmässä on äärellinen määrä alkioita, sitä kutsutaan *äärelliseksi.* Äärellisen ryhmän *kertaluku* on sen alkioiden lukumäärä. Ryhmän $G$ kertaluvusta käytetään merkintää $|G|$. Alkion $g$ kertaluku on pienin positiivinen kokonaisluku $n$, jolle pätee $g^n = e$. Tällöin merkitään $|g| = n$.

**Määritelmä 2.2.** Ryhmän $(G, *)$ epätyhjä osajoukko $H$ on ryhmän $G$ *aliryhmä*, mikäli $(H, *)$ on ryhmä. Tällöin merkitään $H \leq G$.

**Lause 2.3** (Aliryhmäkriteeri)**.** *Olkoon $G$ ryhmä ja $H$ sen epätyhjä osajoukko. Nyt $H \leq G$, jos ja vain jos seuraavat ehdot ovat voimassa:*

*1) $ab \in H$ aina, kun $a, b \in H$*

*2) $a^{-1} \in H$ aina, kun $a \in H$.*

**Määritelmä 2.4.** Olkoon $G$ ryhmä, $g \in G$ ja $H \leq G$. Joukkoa

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

kutsutaan alkion $g$ määräämäksi aliryhmän $H$ *vasemmaksi sivuluokaksi.* Vastaavasti joukkoa

$$Hg := \{hg \mid h \in H\}$$

kutsutaan alkion $g$ määräämäksi aliryhmän $H$ *oikeaksi sivuluokaksi.*

Aliryhmän $H$ *indeksiksi* kutsutaan sen vasempien sivuluokkien määrää ryhmässä $G$, ja merkitään $[G : H]$.

**Lause 2.5** (Lagrangen lause)**.** *Jos $G$ on äärellinen ryhmä ja $H \leq G$, niin $[G : H] = |G|/|H|$.*

## 2.2 Normaali aliryhmä ja tekijäryhmä

**Määritelmä 2.6.** Olkoon $G$ ryhmä ja $N \leq G$. Aliryhmä $N$ on *normaali*, mikäli $gN = Ng$ aina, kun $g \in G$. Tällöin merkitään $N \trianglelefteq G$.

**Lause 2.7** (Normaaliuskriteeri)**.** *Olkoon $G$ ryhmä ja $N \leq G$. Aliryhmä $N$ on normaali, jos ja vain jos $g^{-1}ng \in N$ aina, kun $g \in G$ ja $n \in N$.*

Jokaisen ryhmän $G$ *triviaalit aliryhmät* $\{e\}$ ja $G$ ovat normaaleja. Ryhmä on *yksinkertainen*, mikäli sillä ei ole triviaalien aliryhmien lisäksi muita normaaleja aliryhmiä.

**Määritelmä 2.8.** Olkoon $G$ ryhmä ja $N \trianglelefteq G$. Aliryhmän $N$ vasemmista sivuluokista koostuvaa joukkoa

$$G/N := \{gN \mid g \in G\}$$

kutsutaan ryhmän $G$ *tekijäryhmäksi* aliryhmän $N$ suhteen.

**Lause 2.9.** *Olkoon $G$ ryhmä ja $N \trianglelefteq G$. Määritellään joukkoon $G/N$ operaatio $*$ siten, että $aN * bN = (ab)N$ aina, kun $a, b \in G$. Tällöin $(G/N, *)$ on ryhmä. Jos ryhmä $G$ on äärellinen, niin $|G/N| = [G : N]$.*

## 2.3 Homomorfismi

**Määritelmä 2.10.** Olkoot $(G, *)$ ja $(F, \circ)$ ryhmiä. Kuvaus $h : G \to F$ on *homomorfismi*, mikäli pätee

$$h(a * b) = h(a) \circ h(b)$$

aina, kun $a, b \in G$.

Jos homomorfismi on bijektio, sitä kutsutaan *isomorfismiksi*. Tällöin ryhmien $G$ ja $F$ sanotaan olevan *isomorfiset* ja merkitään $G \cong F$.

**Määritelmä 2.11.** Olkoot $G$, $F$ ja $h$ kuten edellä sekä $e_F$ ryhmän $F$ neutraalialkio. Joukkoa

$$\operatorname{Ker} h := \{g \in G \mid h(g) = e_F\}$$

kutsutaan homomorfismin $h$ *ytimeksi*. Joukkoa

$$\operatorname{Im} h := \{h(g) \in F \mid g \in G\}$$

kutsutaan homomorfismin $h$ *kuvaksi*.

**Lause 2.12** (Homomorfismien peruslause)**.** *Olkoot $G$ ja $F$ ryhmiä sekä $h : G \to F$ homomorfismi. Tällöin*

*a)* $\operatorname{Ker} h \trianglelefteq G$

*b)* $\operatorname{Im} h \leq F$

*c)* $G/\operatorname{Ker} h \cong \operatorname{Im} h$.

# 3 Permutaatiot

## 3.1 Permutaatio ja symmetrinen ryhmä

Tässä kappaleessa joukon $X$ oletetaan olevan epätyhjä ja äärellinen.

**Määritelmä 3.1.** Bijektiota $\alpha : X \to X$ kutsutaan joukon $X$ *permutaatioksi*.

Koska $X$ on äärellinen joukko, se voidaan samaistaa joukon $\{1, 2, \ldots, n\}$ kanssa, kun $n$ on joukon $X$ alkioiden lukumäärä.

Permutaatiot voidaan esittää käyttämällä niin sanottua *matriisiesitystä*, jossa $2 \times n$ -matriisin ensimmäisellä rivillä ovat luvut $1, 2, \ldots, n$ ja toisella rivillä permutaation kuvat $\alpha(1), \alpha(2), \ldots, \alpha(n)$:

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}.$$

**Esimerkki 3.2.** Olkoon $X = \{1, 2, 3\}$. Tällöin joukon $X$ permutaatiot ovat

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\delta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \zeta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

**Lause 3.3.** *Joukon $X$ permutaatiot muodostavat ryhmän, kun operaationa on kuvausten yhdistäminen.*

*Todistus.* Olkoot $\alpha$, $\beta$ ja $\gamma$ joukon $X$ permutaatioita. Kuvausten yhdistäminen on suljettu operaatio, sillä yhdiste $\alpha \circ \beta$ on myös bijektio $X \to X$. Neutraalialkio on identiteettikuvaus $e$. Bijektion $\alpha$ käänteiskuvaus $\alpha^{-1} : X \to X$ on alkion $\alpha$ käänteisalkio, jolle pätee $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$. Lisäksi operaatio on assosiatiivinen, sillä

$$((\alpha\beta)\gamma)(i) = (\alpha\beta)(\gamma(i)) = \alpha(\beta(\gamma(i))) = \alpha(\beta\gamma(i)) = (\alpha(\beta\gamma))(i)$$

kaikilla $i \in X$. Näin ollen ryhmäaksioomat ovat voimassa. □

**Määritelmä 3.4.** Jos joukossa $X$ on $n$ alkiota, sen permutaatioiden muodostamaa ryhmää kutsutaan astetta $n$ olevaksi *symmetriseksi ryhmäksi*, josta käytetään merkintää $S_n$. Symmetrisen ryhmän aliryhmää kutsutaan *permutaatioryhmäksi*.

Koska $n$ alkiota voidaan järjestää $n!$ eri tavalla, on symmetrisen ryhmän $S_n$ kertaluku $n!$.

**Esimerkki 3.5.** Esimerkissä 3.2 esitellyt permutaatiot muodostavat ryhmän $S_3$, jonka kertaluku on $3! = 6$. Nähdään, että esimerkiksi $\beta \circ \gamma = \epsilon$ ja $\epsilon^{-1} = \delta$.

**Määritelmä 3.6.** Olkoon $\alpha \in S_n$ ja $i \in X$. Jos $\alpha(i) = i$, niin $\alpha$ *säilyttää* alkion $i$. Muussa tapauksessa $\alpha$ *siirtää* alkion $i$.

## 3.2 Sykli

**Määritelmä 3.7.** Olkoon $\alpha \in S_n$ ja $i_1, i_2, \ldots, i_r \in X$. Jos $\alpha(i_{s-1}) = i_s$ kaikilla $s = 1, 2, \ldots, r$, $\alpha(i_r) = i_1$ ja $\alpha$ säilyttää muut alkiot, niin $\alpha$ on *$r$-sykli*. Tällöin merkitään

$$\alpha = (i_1 \quad i_2 \quad \ldots \quad i_r).$$

Mikäli kaksi sykliä ei siirrä yhtään samaa alkiota, niitä kutsutaan *erillisiksi*. 2-sykliä kutsutaan *transpoosiksi*.

**Esimerkki 3.8.** Symmetrisessä ryhmässä $S_5$ 3-syklin $\sigma = (1 \quad 3 \quad 4)$ ja transpoosin $\tau = (2 \quad 5)$ matriisiesitykset ovat

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}.$$

Syklit $\sigma$ ja $\tau$ ovat erilliset.

**Lemma 3.9.** *Erilliset syklit kommutoivat symmetrisessä ryhmässä.*

*Todistus.* [4, s. 79–80] Olkoot $\alpha, \beta \in S_n$ erilliset syklit sekä $i$ alkio, jonka $\alpha$ siirtää. Tällöin $\beta$ säilyttää alkion $i$ ja myös alkion $\alpha(i)$. Siis

$$\alpha\beta(i) = \alpha(i) = \beta\alpha(i).$$

Olkoon sitten $j$ alkio, jonka $\alpha$ säilyttää. Tällöin $\alpha$ säilyttää myös alkion $\beta(j)$, joten

$$\beta\alpha(j) = \beta(j) = \alpha\beta(j).$$

Näin ollen $\alpha\beta = \beta\alpha$. □

**Lause 3.10.** *Jokainen permutaatio voidaan esittää erillisten syklien tulona.*

*Todistus.* [4, s. 78] Olkoon $\alpha \in S_n$ ja $X = \{1, 2, \ldots, n\}$. Määritellään relaatio $\sim$ joukkoon $X$ siten, että $i \sim j$, jos ja vain jos on olemassa sellainen kokonaisluku $r$, että $\alpha^r(i) = j$. Nyt $\sim$ on ekvivalenssirelaatio, sillä

- $\alpha^0(i) = i$
- jos $\alpha^r(i) = j$, niin $\alpha^{-r}(j) = i$
- jos $\alpha^r(i) = j$ ja $\alpha^s(j) = k$, niin $\alpha^{r+s}(i) = k$.

Näin ollen $\sim$ jakaa joukon $X$ erillisiin ekvivalenssiluokkiin, ja joukko

$$\left\{\alpha^k(i) \;\middle|\; k \in \mathbf{Z}\right\}$$

koostuu kaikista saman ekvivalenssiluokan alkioista. Jos $t$ on pienin positiivinen kokonaisluku, jolla $\alpha^t(i)$ kuuluu joukkoon $\{i, \alpha(i), \alpha^2(i), \ldots, \alpha^{t-1}(i)\}$, saadaan $t$-sykli

$$\begin{pmatrix} i & \alpha(i) & \alpha^2(i) & \ldots & \alpha^{t-1}(i) \end{pmatrix},$$

joka muodostuu alkion $i$ määräämästä ekvivalenssiluokasta. Nyt eri ekvivalenssiluokista koostuvat syklit ovat erillisiä, ja $\alpha$ on niiden tulo. □

Nähdään, että $n$-syklin kertaluku on $n$, ja erillisten syklien tulon kertaluku on tulontekijöiden kertalukujen pienin yhteinen jaettava. Näin ollen Esimerkin 3.8 sykleille $\sigma$ ja $\tau$ pätee $|\sigma| = 3$, $|\tau| = 2$ ja $|\sigma\tau| = \text{pyj}(2, 3) = 6$.

**Lause 3.11.** *Jokainen permutaatio voidaan esittää transpoosien tulona.*

*Todistus.* [4, s. 81] Olkoon $\sigma = (i_1 \quad i_2 \quad \dots \quad i_k)$ sykli. Tällöin

$$\sigma = (i_1 \quad i_2 \quad \dots \quad i_k) = (i_1 \quad i_k)(i_1 \quad i_{k-1}) \dots (i_1 \quad i_2).$$

Näin ollen $\sigma$ voidaan esittää transpoosien tulona. Koska Lauseen 3.10 nojalla jokainen permutaatio voidaan esittää syklien tulona, se voidaan esittää transpoosien tulona. □

# 4 Permutaation pariteetti ja alternoiva ryhmä

## 4.1 Permutaation pariteetti

Olkoon $\sigma \in S_n$ sekä $1 \leq i < j \leq n$. Määritellään tulo

$$\begin{aligned} N &= \prod_{i<j}(j-i) \\ &= (2-1)(3-1)\dots(n-1)(3-2)(4-2)\dots(n-2)\dots(n-[n-1]). \end{aligned}$$

Kun $\sigma$ permutoi lukuja $i$ ja $j$, saadaan permutoitu tulo

$$\begin{aligned} \sigma N &= \prod_{i<j}(\sigma(j)-\sigma(i)) \\ &= (\sigma(2)-\sigma(1))\dots(\sigma(n)-\sigma(1))\dots(\sigma(n)-\sigma(n-1)). \end{aligned}$$

Olkoon esimerkiksi $\sigma = (1 \quad 3) \in S_4$. Tällöin

$$N = (2-1)(3-1)(4-1)(3-2)(4-2)(4-3) = 12$$

ja

$$\sigma N = (2-3)(1-3)(4-3)(1-2)(4-2)(4-1) = -12.$$

Huomataan, että suluissa esiintyvät tekijät ovat molemmissa tuloissa itseisarvoiltaan samat. Ne eroavat ainoastaan joidenkin tekijöiden merkkien osalta. Tällöin myös tulot ovat itseisarvoiltaan samat, ja yleisesti $\sigma N = \pm N$. Permutaatiota $\sigma$ kutsutaan *parilliseksi*, mikäli $\sigma N = N$, ja *parittomaksi*, mikäli $\sigma N = -N$.

**Lause 4.1.** *Transpoosi on pariton permutaatio.*

*Todistus.* [5, s. 5–6] Olkoon $\tau = (l \quad k) \in S_n$ transpoosi. Voidaan olettaa, että $l < k$. Nyt $\tau(l) = k$, $\tau(k) = l$, ja $\tau$ säilyttää kaikki muut alkiot. Lasketaan

tulon

$$N = \prod_{i<j} (\tau(j) - \tau(i))$$

negatiiviset tekijät.

- Kun $l < i < k$, niin $\tau(k) - \tau(i) = l - i < 0$. Näiden tekijöiden lukumäärä on $k - l - 1$.
- Kun $l < j < k$, niin $\tau(j) - \tau(l) = j - k < 0$. Näiden tekijöiden lukumäärä on $k - l - 1$.
- Lisäksi $\tau(k) - \tau(l) = l - k < 0$.

Näin ollen negatiivisten tekijöiden lukumäärä on $2(k - l - 1) + 1$, joka on pariton luku. Siis $\tau N = -N$, joten $\tau$ on pariton permutaatio. □

## 4.2 Alternoiva ryhmä

Kun $\sigma \in S_n$, niin määritellään kuvaus $F : S_n \to (\{-1, 1\}, \cdot)$ seuraavasti:

$$F(\sigma) = \begin{cases} 1, & \sigma N = N, \\ -1, & \sigma N = -N, \end{cases}$$

jolloin $\sigma N = F(\sigma)N$.

**Lause 4.2.** *Edellä määritelty kuvaus $F$ on surjektiivinen homomorfismi.*

*Todistus.* [5, s. 5–6] Olkoot $\sigma, \tau \in S_n$ ja $1 \leq i < j \leq n$. On osoitettava, että $F(\tau\sigma) = F(\tau)F(\sigma)$. Merkitään $\sigma(i) = i'$ ja $\sigma(j) = j'$. Nyt

$$(\tau\sigma)N = \prod_{i<j} (\tau\sigma(j) - \tau\sigma(i)) = \prod_{i<j} (\tau(j') - \tau(i')).$$

Korvataan jokainen tekijä $\tau(j') - \tau(i')$, missä $i' > j'$, tekijällä $-(\tau(i') - \tau(j'))$. Siis

$$\prod_{i<j}(\tau(j') - \tau(i')) = F(\sigma)\prod_{i<j}(\tau(j) - \tau(i)) = F(\sigma)F(\tau)N = F(\tau)F(\sigma)N.$$

Näin ollen $F(\tau\sigma) = F(\tau)F(\sigma)$, eli $F$ on homomorfismi. Nyt $F$ on surjektio, sillä esimerkiksi identiteettipermutaatiolle $e$ pätee $F(e) = 1$ ja mille tahansa transpoosille $\tau$ pätee $F(\tau) = -1$. □

Ryhmän $S_n$ parilliset permutaatiot muodostavat homomorfismin $F$ ytimen, joka on Lauseen 2.12 nojalla ryhmän $S_n$ normaali aliryhmä. Tätä aliryhmää kutsutaan *alternoivaksi ryhmäksi* astetta $n$, ja merkitään $A_n$.

Homomorfismien peruslauseen (Lause 2.12) nojalla $S_n/A_n \cong \{-1, 1\}$. Näin ollen $[S_n : A_n] = 2$, eli alternoivan ryhmän $A_n$ kertaluku on $n!/2$.

Koska $F(\tau\sigma) = F(\tau)F(\sigma)$, permutaatioiden tulon pariteetti määräytyy tulontekijöiden pariteetista:

- parillinen × parillinen = parillinen
- parillinen × pariton = pariton
- pariton × pariton = parillinen.

Permutaation pariteetti nähdään helposti esittämällä se transpoosien tulona. Permutaatio on pariton, jos ja vain jos sen muodostavien transpoosien määrä on pariton.

**Esimerkki 4.3.** Ryhmässä $S_5$

- permutaatio $(1 \quad 2 \quad 3 \quad 4) = (1 \quad 4)(1 \quad 3)(1 \quad 2)$ on pariton
- permutaatio $(1 \quad 2 \quad 3)(4 \quad 5) = (1 \quad 3)(1 \quad 2)(4 \quad 5)$ on pariton

- permutaatio $(1 \quad 2 \quad 3 \quad 4 \quad 5) = (1 \quad 5)(1 \quad 4)(1 \quad 3)(1 \quad 2)$ on parillinen.

Taulukoissa 4.1–4.6 on esitelty asteita 4–6 olevien symmetristen ja alternoivien ryhmien alkioiden syklirakenne ja kutakin rakennetta edustavien permutaatioiden lukumäärä ryhmässä.

Taulukko 4.1: Symmetrisen ryhmän $S_4$ alkioiden syklirakenne

| rakenne | kertaluku | pariteetti | lukumäärä |
|---|---|---|---|
| $(1)$ | 1 | parillinen | 1 |
| $(a \quad b)$ | 2 | pariton | 6 |
| $(a \quad b \quad c)$ | 3 | parillinen | 8 |
| $(a \quad b \quad c \quad d)$ | 4 | pariton | 6 |
| $(a \quad b)(c \quad d)$ | 2 | parillinen | 3 |
| yhteensä | | | 24 |

Taulukko 4.2: Alternoivan ryhmän $A_4$ alkioiden syklirakenne

| rakenne | kertaluku | lukumäärä |
|---|---|---|
| $(1)$ | 1 | 1 |
| $(a \quad b \quad c)$ | 3 | 8 |
| $(a \quad b)(c \quad d)$ | 2 | 3 |
| yhteensä | | 12 |

Taulukko 4.3: Symmetrisen ryhmän $S_5$ alkioiden syklirakenne

| rakenne | kertaluku | pariteetti | lukumäärä |
|---|---|---|---|
| $(1)$ | 1 | parillinen | 1 |
| $(a \quad b)$ | 2 | pariton | 10 |
| $(a \quad b \quad c)$ | 3 | parillinen | 20 |
| $(a \quad b \quad c \quad d)$ | 4 | pariton | 30 |
| $(a \quad b)(c \quad d)$ | 2 | parillinen | 15 |
| $(a \quad b \quad c \quad d \quad e)$ | 5 | parillinen | 24 |
| $(a \quad b \quad c)(d \quad e)$ | 6 | pariton | 20 |
| yhteensä | | | 120 |

Taulukko 4.4: Alternoivan ryhmän $A_5$ alkioiden syklirakenne

| rakenne | kertaluku | lukumäärä |
|---|---|---|
| $(1)$ | 1 | 1 |
| $(a\quad b\quad c)$ | 3 | 20 |
| $(a\quad b)(c\quad d)$ | 2 | 15 |
| $(a\quad b\quad c\quad d\quad e)$ | 5 | 24 |
| yhteensä | | 60 |

Taulukko 4.5: Symmetrisen ryhmän $S_6$ alkioiden syklirakenne

| rakenne | kertaluku | pariteetti | lukumäärä |
|---|---|---|---|
| $(1)$ | 1 | parillinen | 1 |
| $(a\quad b)$ | 2 | pariton | 15 |
| $(a\quad b\quad c)$ | 3 | parillinen | 40 |
| $(a\quad b\quad c\quad d)$ | 4 | pariton | 90 |
| $(a\quad b)(c\quad d)$ | 2 | parillinen | 45 |
| $(a\quad b\quad c\quad d\quad e)$ | 5 | parillinen | 144 |
| $(a\quad b\quad c)(d\quad e)$ | 6 | pariton | 120 |
| $(a\quad b\quad c\quad d\quad e\quad f)$ | 6 | pariton | 120 |
| $(a\quad b\quad c)(d\quad e\quad f)$ | 3 | parillinen | 40 |
| $(a\quad b\quad c\quad d)(e\quad f)$ | 4 | parillinen | 90 |
| $(a\quad b)(c\quad d)(e\quad f)$ | 2 | pariton | 15 |
| yhteensä | | | 720 |

Taulukko 4.6: Alternoivan ryhmän $A_6$ alkioiden syklirakenne

| rakenne | kertaluku | lukumäärä |
|---|---|---|
| $(1)$ | 1 | 1 |
| $(a\quad b\quad c)$ | 3 | 40 |
| $(a\quad b)(c\quad d)$ | 2 | 45 |
| $(a\quad b\quad c\quad d\quad e)$ | 5 | 144 |
| $(a\quad b\quad c)(d\quad e\quad f)$ | 3 | 40 |
| $(a\quad b\quad c\quad d)(e\quad f)$ | 4 | 90 |
| yhteensä | | 360 |

# 5 Alternoivan ryhmän yksinkertaisuus

Tässä kappaleessa osoitetaan alternoivan ryhmän $A_n$ olevan yksinkertainen, kun $n \geq 5$. Aluksi käydään läpi tarvittavat esitiedot, minkä jälkeen todistetaan yksinkertaisuus tapaukselle $n = 5$. Lopuksi todistetaan edellä mainittu kappaleen päätulos.

## 5.1 Esitietoja

**Lemma 5.1.** *Olkoon $n \geq 3$ sekä $\tau_1, \tau_2 \in S_n$ transpooseja. Tällöin $\tau_1\tau_2$ on joko 3-sykli tai kahden 3-syklin tulo.*

*Todistus.* [3, s. 216] Jos $\tau_1 = \tau_2$, niin $\tau_1\tau_2 = \tau_1^2 = e$. Nyt $e$ on kahden 3-syklin tulo, sillä esimerkiksi $(1 \quad 2 \quad 3)(1 \quad 3 \quad 2) = e$. Olkoon siis jatkossa $\tau_1 \neq \tau_2$.

Jos $\tau_1$ ja $\tau_2$ siirtävät saman alkion, niin yleisyyden kärsimättä voidaan valita $\tau_1 = (1 \quad 2)$ ja $\tau_2 = (1 \quad 3)$. Tällöin

$$\tau_1\tau_2 = (1 \quad 2)(1 \quad 3) = (1 \quad 3 \quad 2),$$

joka on 3-sykli.

Jos $\tau_1$ ja $\tau_2$ eivät siirrä yhtään samaa alkiota, niin voidaan valita $\tau_1 = (1 \quad 2)$ ja $\tau_2 = (3 \quad 4)$. (Tämä on mahdollista vain, jos $n \geq 4$.) Tällöin

$$\tau_1\tau_2 = (1 \quad 2)(3 \quad 4) = (1 \quad 4 \quad 2)(1 \quad 4 \quad 3),$$

joka on kahden 3-syklin tulo. □

**Lemma 5.2.** *Jos $n \geq 3$ ja $\sigma \in A_n$, niin $\sigma$ voidaan esittää 3-syklien tulona.*

*Todistus.* [3, s. 216–217] Koska $\sigma \in A_n$, se on parillinen permutaatio. Näin ollen sen esityksessä transpoosien tulona on parillinen määrä transpooseja, joten se on muotoa $\sigma = \tau_1\tau_2 \ldots \tau_{2m}$ jollakin $m \in \mathbf{N}$. Lemman 5.1 nojalla jokainen tulo $\tau_{2i-1}\tau_{2i}$ on joko 3-sykli tai kahden 3-syklin tulo, kun $i = 1, 2, \ldots, m$. Näin ollen $\sigma$ on joko 3-sykli tai niiden tulo. □

## 5.2 Kompleksi ja konjugaatti

**Määritelmä 5.3.** Olkoot $A$ ja $B$ ryhmän $G$ aliryhmiä. Joukko

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

on aliryhmien $A$ ja $B$ muodostama *kompleksi*.

**Lemma 5.4.** *Nyt*

$$|AB| = \frac{|A||B|}{|A \cap B|}.$$

*Todistus.* [6, s. 6] Tulo $ab$ voidaan muodostaa $|A||B|$ eri tavalla. Näistä osa on keskenään identtisiä. Määritetään keskenään identtisten tulojen lukumäärä.

Määritellään relaatio $\sim$ joukkoon $A \times B$ siten, että $(a_1, b_1) \sim (a_2, b_2)$, jos ja vain jos $a_1 b_1 = a_2 b_2$. Nyt $\sim$ on ekvivalenssirelaatio, jonka ekvivalenssiluokkien määrä on $|AB|$. Osoitetaan, että jokaisessa ekvivalenssiluokassa on $|A \cap B|$ alkiota.

Olkoot $a \in A$, $b \in B$ ja $E$ se ekvivalenssiluokka, johon $(a, b)$ kuuluu. Osoitetaan, että $E = \left\{(ax^{-1}, xb) \mid x \in A \cap B\right\}$.

Nyt $ax^{-1} \in A$, $xb \in B$ ja $ax^{-1}xb = ab$. Näin ollen $(ax^{-1}, xb) \in E$, joten $\left\{(ax^{-1}, xb) \mid x \in A \cap B\right\} \subseteq E$.

Olkoon sitten $(c, d) \in E$, jolloin $ab = cd$. Tällöin $c^{-1}a = db^{-1} \in A \cap B$. Valitsemalla $x = c^{-1}a = db^{-1}$ saadaan $(c, d) = (ax^{-1}, xb)$, jolloin

$$(c, d) \in \left\{\left(ax^{-1}, xb\right) \mid x \in A \cap B\right\}.$$

Siis $E \subseteq \left\{(ax^{-1}, xb) \mid x \in A \cap B\right\}$, jolloin joukkojen yhtäsuuruus on todistettu. Näin ollen $|E| = |A \cap B|$, joten

$$|A \cap B||AB| = |A||B|,$$

mistä väite seuraa. □

On huomattava, että kompleksi ei ole välttämättä ryhmän $G$ aliryhmä. Sen sijaan mikäli toinen kompleksin muodostavista aliryhmistä on normaali, on kompleksi aliryhmä, kuten seuraavasta tuloksesta nähdään.

**Lemma 5.5.** *Jos $A \leq G$ ja $N \trianglelefteq G$, niin $AN = NA \leq G$.*

*Todistus.* [4, s. 61] Osoitetaan aluksi, että $AN \leq G$. Selvästi $e \in AN$, joten $AN$ on epätyhjä. Olkoot $a_1, a_2 \in A$ ja $n_1, n_2 \in N$. Nyt

$$(a_1 n_1)(a_2 n_2) = a_1 \left(a_2 a_2^{-1}\right) n_1 a_2 n_2 = a_1 a_2 \left(a_2^{-1} n_1 a_2\right) n_2.$$

Nyt $a_2^{-1} n_1 a_2 \in N$, sillä $N$ on normaali aliryhmä. Merkitään $a_2^{-1} n_1 a_2 =: n \in N$. Siis

$$(a_1 n_1)(a_2 n_2) = \underbrace{(a_1 a_2)}_{\in A} \underbrace{(n n_2)}_{\in N} \in AN.$$

Lisäksi

$$(a_1 n_1)^{-1} = n_1^{-1} a_1^{-1} = \left(a_1^{-1} a_1\right) n_1^{-1} a_1^{-1} = \underbrace{a_1^{-1}}_{\in A} \underbrace{\left(a_1 n_1^{-1} a_1^{-1}\right)}_{\in N} \in AN.$$

Näin ollen aliryhmäkriteeri (Lause 2.3) toteutuu, joten $AN \leq G$.

Osoitetaan vielä, että $AN = NA$. Olkoon nyt $g \in AN$. Koska $AN$ on aliryhmä, alkiolla $g$ on käänteisalkio $an \in AN$ joillakin $a \in A$ ja $n \in N$. Siis

$$g = (an)^{-1} = \underbrace{n^{-1}}_{\in N} \underbrace{a^{-1}}_{\in A} \in NA.$$

Näin ollen $AN \subseteq NA$. Vastaavalla päättelyllä nähdään, että myös $NA \subseteq AN$. Siis $AN = NA$. □

**Määritelmä 5.6.** Olkoot $a$ ja $b$ ryhmän $G$ alkioita. Jos on olemassa alkio $g \in G$, jolle pätee $g^{-1} a g = b$, niin $b$ *konjugoi* alkion $a$ kanssa eli on alkion $a$ *konjugaatti*. Konjugaatista käytetään myös lyhyempää merkintää $a^g := g^{-1} a g$.

Suoraan määritelmästä nähdään, että konjugaatille pätevät seuraavat lait:

1) $g^{ab} = (g^a)^b$

2) $(gh)^a = g^a h^a$

3) $(g^{-1})^a = (g^a)^{-1}$.

Jos $M$ on ryhmän $G$ epätyhjä osajoukko, niin määritellään vastaavasti joukko $M^g := \{m^g \mid m \in M\}$, joka on joukon $M$ konjugaatti ryhmässä $G$.

Konjugoimalla yhtälöä $m^g = n^g$ puolittain alkiolla $g^{-1}$ saadaan $m = n$. Kääntäen nähdään siis, että ehdosta $m \neq n$ seuraa $m^g \neq n^g$. Näin ollen konjugointi on injektiivinen operaatio, joten joukossa ja sen konjugaatissa on yhtä monta alkiota.

Jos $M \leq G$, niin myös $M^g \leq G$, sillä aliryhmäkriteeri (Lause 2.3) toteutuu: kaikille $m, n \in M$ pätee $m^g n^g = (mn)^g \in M^g$ ja $(m^g)^{-1} = (m^{-1})^g \in M^g$.

**Lemma 5.7.** *Olkoon $G$ ryhmä, $g, h \in G$ ja $M, N \leq G$. Tällöin*

*1)* $(MN)^g = M^g N^g$

*2)* $(N^g)^h = N^{gh}$.

*Todistus.* Nyt

$$\begin{aligned}(MN)^g &= \{a^g \mid a \in MN\} = \{(mn)^g \mid m \in M, n \in N\} \\ &= \{m^g n^g \mid m \in M, n \in N\} = M^g N^g\end{aligned}$$

ja

$$\begin{aligned}(N^g)^h &= \{b^h \mid b \in N^g\} = \left\{(n^g)^h \mid n \in N\right\} \\ &= \{n^{gh} \mid n \in N\} = N^{gh}.\end{aligned}$$

□

**Lemma 5.8.** *Jos $N \trianglelefteq M \trianglelefteq G$ ja $g \in G$, niin $N^g \trianglelefteq M$.*

*Todistus.* Koska $M \trianglelefteq G$, niin $M^g = M$. Osoitetaan, että $N^g \trianglelefteq M^g$. Olkoot $a \in N^g$ ja $b \in M^g$, jolloin $a = n^g$ ja $b = m^g$ joillakin $n \in N$ ja $m \in M$. Normaaliuskriteerin (Lause 2.7) mukaan riittää osoittaa, että $a^b \in N^g$. Nyt

$$\begin{aligned} a^b &= b^{-1}ab \\ &= (m^g)^{-1} n^g m^g \\ &= \left(m^{-1}\right)^g n^g m^g \\ &= \left(m^{-1}nm\right)^g \\ &= (n^m)^g . \end{aligned}$$

Koska $N \trianglelefteq M$, niin $n^m \in N$. Siis $(n^m)^g \in N^g$, joten $N^g \trianglelefteq M^g = M$. □

**Lemma 5.9.** *Jos $M, N \trianglelefteq G$, niin $MN \trianglelefteq G$.*

*Todistus.* Lemman 5.5 nojalla $MN \leq G$, joten riittää osoittaa sen normaalius. On siis osoitettava, että $a^g \in MN$ aina, kun $a \in MN$ ja $g \in G$. Nyt $a = mn$ joillakin $m \in M$, $n \in N$. Koska $M$ ja $N$ ovat normaaleja aliryhmiä, niin $m^g \in M$ ja $n^g \in N$. Siis

$$a^g = (mn)^g = m^g n^g \in MN,$$

joten $MN \trianglelefteq G$. □

## 5.3 Syklirakenne

Konjugointi on ekvivalenssirelaatio. Täten voidaan sanoa, että alkiot $a$ ja $b$ konjugoivat keskenään. Relaatio jakaa ryhmän alkiot erillisiin joukkoihin, joita kutsutaan *konjugointiluokiksi*.

Sanotaan, että ryhmän $S_n$ permutaatioilla $\alpha$ ja $\beta$ on sama *syklirakenne*, jos niiden esityksessä erillisten syklien tulona on täsmälleen sama määrä $k$-syklejä kaikilla $k = 1, 2, \ldots, n$. Esimerkiksi ryhmässä $S_5$ permutaatioilla

$(1 \quad 2)(3 \quad 4)$ ja $(1 \quad 3)(2 \quad 4)$ on sama syklirakenne, sillä kumpikin koostuu kahdesta 2-syklistä. Sen sijaan permutaation $(1 \quad 2 \quad 3)(4 \quad 5)$ syklirakenne eroaa edellä mainituista, sillä siinä esiintyy 3-sykli. Seuraavaksi osoitetaan, että ryhmän $S_n$ permutaatioilla on sama syklirakenne, jos ja vain jos ne konjugoivat ryhmässä $S_n$.

**Lemma 5.10.** *Jos* $\alpha = (a_1 \quad a_2 \quad \dots \quad a_k) \in S_n$ *ja* $\beta \in S_n$, *niin*

$$\alpha^\beta = \left(\beta^{-1}(a_1) \quad \beta^{-1}(a_2) \quad \dots \quad \beta^{-1}(a_k)\right).$$

*Todistus.* [4, s. 84] Nyt $\alpha(a_i) = a_{i+1}$, kun $1 \leq i < k$, ja $\alpha(a_k) = a_1$. Pitää osoittaa, että $\alpha^\beta$ kuvaa alkion $\beta^{-1}(a_i)$ alkioksi $\beta^{-1}(a_{i+1})$ sekä alkion $\beta^{-1}(a_k)$ alkioksi $\beta^{-1}(a_1)$ ja lisäksi säilyttää kaikki alkiot, jotka eivät ole muotoa $\beta^{-1}(a_j)$ millään $1 \leq j \leq k$.

Nyt

$$\alpha^\beta\left(\beta^{-1}(a_i)\right) = \beta^{-1}\alpha\beta\beta^{-1}(a_i) = \beta^{-1}\alpha(a_i) = \beta^{-1}(a_{i+1})$$

ja vastaavasti

$$\alpha^\beta\left(\beta^{-1}(a_k)\right) = \beta^{-1}\alpha(a_k) = \beta^{-1}(a_1).$$

Olkoon $x$ sellainen alkio, joka ei ole muotoa $\beta^{-1}(a_j)$. Nyt siis $x \neq \beta^{-1}(a_j)$, joten $\beta(x) \neq a_j$ kaikilla $1 \leq j \leq k$. Siis $\alpha$ säilyttää alkion $\beta(x)$. Nyt

$$\alpha^\beta(x) = \beta^{-1}\alpha\beta(x) = \beta^{-1}\alpha(\beta(x)) = \beta^{-1}\beta(x) = x.$$

Siis $\alpha^\beta$ säilyttää alkion $x$. Näin ollen väite pätee. □

Lemman 5.10 perusteella nähdään, että $k$-syklin konjugaatti on $k$-sykli.

**Lemma 5.11.** *Permutaatiot konjugoivat ryhmässä* $S_n$, *jos ja vain jos niillä on sama syklirakenne.*

*Todistus.* [5, s. 8]

($\Rightarrow$) Olkoot $\alpha, \beta \in S_n$. Osoitetaan, että permutaatioilla $\alpha$ ja $\alpha^\beta$ on sama syklirakenne.

Lauseen 3.10 nojalla $\alpha$ voidaan esittää erillisten syklien tulona. Olkoon siis $\alpha = \alpha_1\alpha_2 \dots \alpha_k$, missä $\alpha_i$ ja $\alpha_j$ ovat erilliset syklit aina, kun $i \neq j$. Nyt

$$\alpha^\beta = (\alpha_1\alpha_2 \dots \alpha_k)^\beta = \alpha_1^\beta\alpha_2^\beta \dots \alpha_k^\beta.$$

Lemman 5.10 perusteella syklin $\alpha_i^\beta$ pituus on sama kuin syklin $\alpha_i$ kaikilla $i$. Osoitetaan vielä, että syklit $\alpha_i^\beta$ ja $\alpha_j^\beta$ ovat erilliset aina, kun $i \neq j$.

Olkoon $x$ sellainen alkio, jonka $\alpha_i^\beta$ siirtää. Tällöin riittää osoittaa, että $\alpha_j^\beta$ säilyttää alkion $x$. Koska $\alpha_i^\beta$ siirtää alkion $x$, Lemman 5.10 nojalla $x = \beta^{-1}(a)$ jollakin alkiolla $a$, jonka $\alpha_i$ siirtää. Koska $\alpha_i$ ja $\alpha_j$ ovat erilliset, $\alpha_j$ säilyttää alkion $a$. Nyt

$$\alpha_j^\beta(x) = \beta^{-1}\alpha_j\beta(x) = \beta^{-1}\alpha_j\beta\left(\beta^{-1}(a)\right) = \beta^{-1}\alpha_j(a) = \beta^{-1}(a) = x.$$

Näin ollen $\alpha_j^\beta$ säilyttää alkion $x$, joten $\alpha_i^\beta$ ja $\alpha_j^\beta$ ovat erilliset syklit.

Edellä osoitetun perusteella $\alpha$ ja $\alpha^\beta$ muodostuvat yhtä monesta erillisestä syklistä, joiden pituudet ovat samat. Näin ollen niillä on sama syklirakenne.

($\Leftarrow$) Olkoot $\alpha, \beta \in S_n$ permutaatiot, joilla on sama syklirakenne. Olkoot niiden esitykset erillisten syklien tuloina $\alpha = \alpha_1\alpha_2 \dots \alpha_k$ ja $\beta = \beta_1\beta_2 \dots \beta_k$, missä $\alpha_i$ ja $\beta_i$ ovat samanpituiset syklit kaikilla $1 \leq i \leq k$. Käytetään syklien $\alpha_i$ ja $\beta_i$ pituudesta merkintää $s_i$, ja kirjoitetaan sykli $\alpha_i$ muodossa $\begin{pmatrix} a_i^{(1)} & a_i^{(2)} & \dots & a_i^{(s_i)} \end{pmatrix}$ sekä vastaavasti $\beta_i$ muodossa $\begin{pmatrix} b_i^{(1)} & b_i^{(2)} & \dots & b_i^{(s_i)} \end{pmatrix}$.

Määritellään kuvaus $\sigma$ siten, että se kuvaa alkion $a_i^{(j)}$ alkioksi $b_i^{(j)}$ aina, kun $1 \leq i \leq k$ ja $1 \leq j \leq s_i$. Kun permutaatioiden $\alpha$ ja $\beta$ esityksiin

erillisten syklien tuloina sisällytetään myös mahdolliset 1-syklit, jokainen joukon $\{1, 2, \ldots, n\}$ alkio esiintyy kummassakin esityksessä täsmälleen kerran. Näin ollen $\sigma$ on symmetriseen ryhmään $S_n$ kuuluva permutaatio, ja se voidaan esittää matriisimuodossa

$$\sigma = \begin{pmatrix} a_1^{(1)} & \cdots & a_1^{(s_1)} & a_2^{(1)} & \cdots & a_2^{(s_2)} & \cdots & a_k^{(1)} & \cdots & a_k^{(s_k)} \\ b_1^{(1)} & \cdots & b_1^{(s_1)} & b_2^{(1)} & \cdots & b_2^{(s_2)} & \cdots & b_k^{(1)} & \cdots & b_k^{(s_k)} \end{pmatrix}.$$

Osoitetaan, että $\alpha = \beta^\sigma$, jolloin $\alpha$ ja $\beta$ konjugoivat.

Nyt $\alpha$ kuvaa alkion $a_i^{(j)}$ alkioksi $a_i^{(j+1)}$, kun $1 \leq j < s_i$, sekä alkion $a_i^{(s_i)}$ alkioksi $a_i^{(1)}$. Vastaavasti $\beta$ kuvaa alkion $b_i^{(j)}$ alkioksi $b_i^{(j+1)}$ ja alkion $b_i^{(s_i)}$ alkioksi $b_i^{(1)}$. Kun $1 \leq j < s_i$, niin

$$\beta^\sigma \left(a_i^{(j)}\right) = \sigma^{-1}\beta\sigma \left(a_i^{(j)}\right) = \sigma^{-1}\beta \left(b_i^{(j)}\right) = \sigma^{-1} \left(\beta_i^{(j+1)}\right) = a_i^{(j+1)}.$$

Vastaavalla päättelyllä nähdään, että $\beta^\sigma \left(a_i^{(s_i)}\right) = a_i^{(1)}$. Näin ollen $\alpha = \beta^\sigma$, eli $\alpha$ ja $\beta$ konjugoivat. □

**Lemma 5.12.** *Jos $n \geq 5$, niin 3-syklit konjugoivat ryhmässä $A_n$.*

*Todistus.* [3, s. 218] Olkoot $\alpha, \beta \in S_n$ 3-syklejä. Koska niiden syklirakenne on sama, niin Lemman 5.11 nojalla ne konjugoivat ryhmässä $S_n$. Näin ollen on olemassa permutaatio $\sigma \in S_n$, jolle pätee $\beta = \alpha^\sigma$. Jos $\sigma$ on parillinen, niin $\sigma \in A_n$, jolloin lemma on todistettu. Olkoon siis $\sigma$ pariton.

Yleisyyden kärsimättä voidaan merkitä $\alpha = (1 \quad 2 \quad 3)$. Olkoon $\tau = (4 \quad 5)$. Nyt $\tau\sigma$ on parillinen, sillä Lauseen 4.1 mukaan transpoosi on pariton. Tällöin $\tau\sigma \in A_n$. Lisäksi $\alpha$ ja $\tau$ ovat erilliset syklit, joten Lemman 3.9 nojalla ne kommutoivat. Näin ollen

$$\begin{aligned} \alpha^{\tau\sigma} &= (\tau\sigma)^{-1}\alpha(\tau\sigma) = \sigma^{-1}\tau^{-1}\alpha\tau\sigma = \sigma^{-1}\tau^{-1}\tau\alpha\sigma \\ &= \sigma^{-1}\alpha\sigma = \alpha^\sigma = \beta. \end{aligned}$$

Näin ollen $\alpha$ ja $\beta$ konjugoivat ryhmässä $A_n$. □

## 5.4 Normalisoija ja keskus

**Määritelmä 5.13.** Olkoon $M$ ryhmän $G$ epätyhjä osajoukko. Tällöin joukko

$$N_G(M) := \{g \in G \mid M^g = M\}$$

on joukon $M$ *normalisoija* ryhmässä $G$.

**Lemma 5.14.** *Normalisoija $N_G(M)$ on ryhmän $G$ aliryhmä.*

*Todistus.* Selvästi $e \in N_G(M)$, joten $N_G(M)$ on epätyhjä. Olkoot $m$ ja $n$ normalisoijan alkioita, jolloin $M^m = M^n = M$. Lemman 5.7 nojalla

$$M^{mn} = (M^m)^n = M^n = M,$$

joten $mn \in N_G(M)$. Lisäksi

$$M^{m^{-1}} = (M^m)^{m^{-1}} = M^{mm^{-1}} = M,$$

joten $m^{-1} \in N_G(M)$. Näin ollen aliryhmäkriteeri (Lause 2.3) toteutuu, joten $N_G(M) \leq G$. □

Jos normalisoitava joukko on aliryhmä, sillä on seuraava ominaisuus:

**Lause 5.15.** *Olkoon $H \leq G$. Tällöin normalisoija $N_G(H)$ on suurin ryhmän $G$ aliryhmä, jonka sisällä $H$ on normaali.*

*Todistus.* Pitää osoittaa, että

1) $H$ on normalisoijan $N_G(H)$ normaali aliryhmä

2) jos $H \trianglelefteq U \leq G$, niin $U$ sisältyy normalisoijaan $N_G(H)$.

Olkoon $h \in H$ ja $n \in N_G(H)$. Selvästi $H^h = H$, joten $H \leq N_G(H)$. Lisäksi $h^n \in H^n = H$, joten $H \trianglelefteq N_G(H)$. Näin ollen ensimmäinen väite on todistettu.

Toisen väitteen todistamiseksi oletetaan, että $H \trianglelefteq U \leq G$ ja $u \in U$. Riittää osoittaa, että $H^u \subseteq H$. Jos $x \in H^u$, niin $x = h^u$ jollakin $h \in H$. Nyt $x \in H$, sillä $H \trianglelefteq U$. Näin ollen $H^u \subseteq H$. Siis $u \in N_G(H)$, joten $U \leq N_G(H)$. □

**Määritelmä 5.16.** Ryhmän $G$ *keskus* on joukko

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

Keskus koostuu siis alkioista, jotka kommutoivat kaikkien ryhmän alkioiden kanssa.

**Lause 5.17.** *Keskus $Z(G)$ on ryhmän $G$ normaali aliryhmä.*

*Todistus.* Osoitetaan aluksi, että $Z(G) \leq G$. Olkoot $a, b \in Z(G)$ ja $g \in G$. Nyt siis alkiot $a$ ja $b$ kommutoivat kaikkien ryhmän alkoiden kanssa. Aliryhmäkriteerin (Lause 2.3) nojalla riittää osoittaa, että alkiot $ab$ ja $a^{-1}$ kommutoivat alkion $g$ kanssa. Nyt

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$$

ja

$$a^{-1}g = a^{-1}\left(g^{-1}\right)^{-1} = \left(g^{-1}a\right)^{-1} = \left(ag^{-1}\right)^{-1} = \left(g^{-1}\right)^{-1}a^{-1} = ga^{-1}.$$

Näin ollen $Z(G) \leq G$.

Normaaliuskriteeri (Lause 2.7) toteutuu, sillä $g^{-1}ag = g^{-1}ga = a \in Z(G)$. Näin ollen $Z(G) \trianglelefteq G$. □

## 5.5 Ryhmän $A_5$ yksinkertaisuus

**Lemma 5.18.** *Jos $n \geq 3$, niin symmetrisen ryhmän $S_n$ keskus on triviaali, toisin sanoen $Z(S_n) = \{e\}$.*

*Todistus.* Olkoon $\alpha \in S_n \setminus \{e\}$. Tällöin $\alpha$ siirtää jonkin alkion. Yleisyyden kärsimättä voidaan valita, että $\alpha(1) = 2$. Erityisesti $\alpha(3) \neq 2$, sillä $\alpha$ on bijektio. Olkoon $\tau = (1 \quad 3) \in S_n$. Nyt

$$\tau(\alpha(1)) = \tau(2) = 2 \quad \text{ja} \quad \alpha(\tau(1)) = \alpha(3) \neq 2.$$

Siis $\tau\alpha \neq \alpha\tau$, joten $\alpha \notin Z(S_n)$. □

**Lemma 5.19.** *Jos $n \geq 5$, niin ryhmän $S_n$ ainut ei-triviaali normaali aliryhmä on $A_n$.*

*Todistus.* [3, s. 218–219] Olkoot $N \trianglelefteq S_n$ ei-triviaali ja $\sigma \in N \setminus \{e\}$. Lemman 5.18 nojalla $\sigma \notin Z(S_n)$, ja on olemassa transpoosi $\tau \in S_n$, jonka kanssa $\sigma$ ei kommutoi. Nyt $\sigma\tau \neq \tau\sigma$, joten $\tau \neq \sigma^{-1}\tau\sigma = \tau^\sigma$ ja $\tau^\sigma\tau \neq e$. Lemman 5.11 perusteella $\tau^\sigma$ on transpoosi. Koska $\sigma \in N$ ja $N$ on normaali, niin normaaliuskriteerin (Lause 2.7) nojalla $\sigma^\tau = \tau^{-1}\sigma\tau = \tau\sigma\tau \in N$. Siis

$$\tau^\sigma\tau = \underbrace{\sigma^{-1}}_{\in N}\underbrace{\tau\sigma\tau}_{\in N} \in N \setminus \{e\}.$$

Näin ollen $N$ sisältää kahden transpoosin tulon $\tau^\sigma\tau$.

Oletetaan aluksi, että $\tau^\sigma$ ja $\tau$ siirtävät saman alkion. Lemman 5.1 todistuksen perusteella $\tau^\sigma\tau$ on tällöin 3-sykli. Lemman 5.11 mukaan kaikki 3-syklit konjugoivat ryhmässä $S_n$, joten normaali aliryhmä $N$ sisältää kaikki 3-syklit. Koska Lemman 5.2 mukaan jokainen alternoivan ryhmän $A_n$ permutaatio voidaan esittää 3-syklien tulona, $A_n$ sisältyy ryhmään $N$. Nyt $A_n \leq N$, ja koska $A_n$ sisältää puolet ryhmän $S_n$ alkioista, se on Lagrangen lauseen 2.5 mukaan ryhmän $S_n$ suurin aito aliryhmä. Näin ollen on oltava $N = A_n$, jolloin lemma on todistettu.

Oletetaan sitten, että $\tau^\sigma$ ja $\tau$ eivät siirrä yhtään samaa alkiota vaan ovat erilliset. Yleisyyden kärsimättä voidaan valita $\tau^\sigma = (1 \quad 2)$ ja $\tau = (3 \quad 4)$,

jolloin $\tau^\sigma\tau = (1 \quad 2)(3 \quad 4) \in N$. Transpoosilla $(1 \quad 5)$ konjugoimalla saadaan

$$(1 \quad 5)^{-1}(1 \quad 2)(3 \quad 4)(1 \quad 5) = (2 \quad 5)(3 \quad 4) \in N.$$

Nyt

$$\underbrace{(1 \quad 2)(3 \quad 4)}_{\in N}\underbrace{(2 \quad 5)(3 \quad 4)}_{\in N} = (1 \quad 2 \quad 5) \in N.$$

Siis $N$ sisältää 3-syklin, joten vastaavalla päättelyllä kuin edellisessä kappaleessa nähdään, että $N = A_n$. □

**Lause 5.20.** *Ryhmä $A_5$ on kertalukua 60 oleva yksinkertainen ryhmä.*

*Todistus.* [3, s. 219] Tehdään vastaoletus, jonka mukaan $A_5$ ei ole yksinkertainen. Tällöin sillä on ei-triviaali normaali aliryhmä $N$, joka on kertaluvultaan pienin mahdollinen. Olkoon $T$ sen normalisoija ryhmässä $S_5$, siis

$$T := N_{S_5}(N) = \left\{\sigma \in S_n \;\middle|\; N^\sigma = N\right\}.$$

Lemman 5.14 mukaan $T \leq S_5$, ja koska $N \trianglelefteq A_5$, Lauseen 5.15 nojalla $A_5 \leq T$. On siis oltava joko $T = A_5$ tai $T = S_5$.

Jos $T = S_5$, niin olisi $N \trianglelefteq S_5$. Tällöin Lemman 5.19 mukaan olisi $N = A_5$. Tämä on ristiriita, sillä $N$ on ryhmän $A_5$ aito aliryhmä. On siis oltava $T = A_5$.

Transpoosi $\tau = (1 \quad 2) \in S_5$ on pariton permutaatio, joten $\tau \notin A_5 = T$. Näin ollen $M := N^\tau \neq N$. Nyt $N \trianglelefteq A_5 \trianglelefteq S_5$, joten Lemman 5.8 nojalla $M \trianglelefteq A_5$. Lisäksi $|M| = |N|$. Nyt $M \cap N \trianglelefteq A_5$, ja Lemman 5.9 nojalla myös $MN \trianglelefteq A_5$. Koska $N$ on ryhmän $A_5$ pienin ei-triviaali normaali aliryhmä sekä $|M| = |N|$ ja $M \neq N$, on oltava $M \cap N = \{e\}$. Nyt Lemmojen 5.7 ja 5.5 nojalla

$$(MN)^\tau = M^\tau N^\tau = (N^\tau)^\tau N^\tau = \underbrace{N^{\tau\tau}}_{=N}\underbrace{N^\tau}_{=M} = NM = MN,$$

eli $\tau \in N_{S_5}(MN)$, ja koska $MN \trianglelefteq A_5$, on oltava $MN \trianglelefteq S_5$. Näin ollen Lemman 5.19 mukaan $MN = A_5$.

Nyt siis $M$ ja $N$ ovat kumpikin alternoivan ryhmän $A_5$ ei-triviaaleja normaaleja aliryhmiä, $|M| = |N|$, $MN = A_5$ ja $M \cap N = \{e\}$. Lemman 5.4 mukaan

$$|M||N| = |MN||M \cap N|,$$

eli

$$|N|^2 = 60.$$

Tämä on ristiriita, sillä 60 ei ole minkään kokonaisluvun neliö. Näin ollen vastaoletus on väärä, ja $A_5$ on yksinkertainen ryhmä. □

**Seuraus 5.21.** *Ryhmä $A_6$ on yksinkertainen.*

*Todistus.* Tulos saadaan täysin vastaavalla päättelyllä kuin edellisessä lauseessa, sillä $|A_6| = 360$, eikä sekään ole minkään kokonaisluvun neliö. □

## 5.6 Ryhmän $A_n$ yksinkertaisuus

**Lemma 5.22.** *Jos $n \geq 4$, niin alternoivan ryhmän $A_n$ keskus on triviaali, toisin sanoen $Z(A_n) = \{e\}$.*

*Todistus.* Olkoon $\alpha \in A_n \setminus \{e\}$. Tällöin $\alpha$ siirtää jonkin alkion. Yleisyyden kärsimättä voidaan valita $\alpha(1) = 2$. Olkoon $\sigma = (2 \quad 3 \quad 4) \in A_n$. Nyt

$$\sigma(\alpha(1)) = \sigma(2) = 3 \quad \text{ja} \quad \alpha(\sigma(1)) = \alpha(1) = 2.$$

Siis $\sigma\alpha \neq \alpha\sigma$, joten $\alpha \notin Z(A_n)$. □

**Lause 5.23.** *Jos $n \geq 5$, niin ryhmä $A_n$ on yksinkertainen.*

*Todistus.* [3, s. 220] Tapaus $n = 5$ on todistettu Lauseessa 5.20, joten voidaan olettaa, että $n \geq 6$. Olkoon $N \trianglelefteq A_n$, $N \neq \{e\}$. On osoitettava, että $N = A_n$.

Olkoon $\sigma \in N \setminus \{e\}$. Lemman 5.22 mukaan ryhmän $A_n$ keskus on triviaali, ja Lemman 5.2 mukaan jokainen alternoivan ryhmän permutaatio voidaan

esittää 3-syklien tulona. Näin ollen on olemassa 3-sykli $\tau \in A_n$, jonka kanssa $\sigma$ ei kommutoi. Siis $\sigma\tau \neq \tau\sigma$, toisin sanoen $\tau^{-1}\sigma^{-1}\tau\sigma \neq e$.

Nyt $\tau^{-1}\sigma^{-1}\tau = (\sigma^{-1})^{\tau} \in N$, sillä $N \trianglelefteq A_n$. Siis

$$\underbrace{\tau^{-1}\sigma^{-1}\tau}_{\in N}\underbrace{\sigma}_{\in N} \in N.$$

Koska $\tau$ on 3-sykli, niin Lemman 5.11 nojalla $\tau^{\sigma} = \sigma^{-1}\tau\sigma$ on 3-sykli. Myös $\tau^{-1}$ on 3-sykli, joten $N$ sisältää kahden 3-syklin tulon $\tau^{-1}\sigma^{-1}\tau\sigma \neq e$. Koska kahden 3-syklin tulo siirtää korkeintaan kuusi alkiota, sen voidaan ajatella kuuluvan ryhmään $A_6$, joka on isomorfinen ryhmän $A_n$ aliryhmän kanssa.

Nyt siis $\tau^{-1}\sigma^{-1}\tau\sigma \in N \cap A_6$, joten $N \cap A_6 \neq \{e\}$ ja $N \cap A_6 \trianglelefteq A_6$. Seurauksen 5.21 mukaan $A_6$ on yksinkertainen ryhmä, joten on oltava $N \cap A_6 = A_6$. Näin ollen $N$ sisältää 3-syklin, ja koska Lemman 5.12 mukaan 3-syklit konjugoivat ryhmässä $A_n$, $N$ sisältää kaikki 3-syklit. Lemman 5.2 mukaan jokainen parillinen permutaatio voidaan esittää 3-syklien tulona, joten on oltava $N = A_n$. Näin ollen $A_n$ on yksinkertainen ryhmä. □

# 6 Permutaatioryhmien sovelluksia

## 6.1 Ryhmän operointi

**Määritelmä 6.1.** Ryhmä $G$ *operoi* joukossa $X$, mikäli on olemassa kuvaus

$$G \times X \to X : (g, x) \mapsto g \cdot x,$$

jolle pätee

1. $g \cdot (h \cdot x) = (gh) \cdot x$,
2. $e \cdot x = x$

aina, kun $g, h \in G$ ja $x \in X$. Tällöin joukon $X$ sanotaan olevan *$G$-joukko.*

**Esimerkki 6.2.** Määritellään kuvaus $S_n \times X \to X : (\sigma, x) \mapsto \sigma(x)$. Nyt Määritelmän 6.1 ehdot toteutuvat, sillä

1. $\sigma \cdot (\tau \cdot x) = \sigma \cdot (\tau(x)) = (\sigma\tau)(x)$,
2. $e \cdot x = e(x) = x$

aina, kun $\sigma, \tau \in S_n$. Näin ollen $S_n$ operoi joukossa $X$, ja $X$ on $S_n$-joukko.

**Määritelmä 6.3.** Olkoon $X$ $G$-joukko ja $x \in X$. Alkion $x$ *stabiloija* ryhmässä $G$ on joukko

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

Permutaatioryhmien tapauksessa stabiloija koostuu siis niistä permutaatioista, jotka säilyttävät alkion $x$.

**Lemma 6.4.** *Stabiloija $G_x$ on ryhmän $G$ aliryhmä.*

*Todistus.* [4, s. 90] Nyt $G_x$ on epätyhjä, sillä Määritelmän 6.1 mukaan $e \in G_x$. Olkoot $g, h \in G_x$. Nyt

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$$

ja

$$\left(g^{-1}\right) \cdot x = g^{-1} \cdot (g \cdot x) = \left(g^{-1}g\right) \cdot x = e \cdot x = x.$$

Siis $gh, g^{-1} \in G_x$, joten aliryhmäkriteerin (Lause 2.3) nojalla $G_x \leq G$. □

**Määritelmä 6.5.** Olkoon $X$ $G$-joukko ja $x \in X$. Alkion $x$ *rata* on joukko

$$\operatorname{Orb} x := \{g \cdot x \in X \mid g \in G\}.$$

**Lemma 6.6.** *Olkoot $X$ $G$-joukko ja $x, y \in X$. Relaatio $xRy \iff x \in \operatorname{Orb} y$ on ekvivalenssirelaatio.*

*Todistus.* [4, s. 91] Nyt $e \cdot x = x$, joten $x \in \operatorname{Orb} x$. Siis $xRx$, joten relaatio on refleksiivinen.

Jos $xRy$, niin $x \in \operatorname{Orb} y$, joten $y = g \cdot x$ jollakin $g \in G$. Tällöin

$$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = \left(g^{-1}g\right) \cdot x = e \cdot x = x.$$

Siis $y \in \operatorname{Orb} x$, joten $yRx$, eli relaatio on symmetrinen.

Jos $xRy$ ja $yRz$, niin $x \in \operatorname{Orb} y$ ja $y \in \operatorname{Orb} z$. Siis $y = g \cdot x$ ja $z = h \cdot y$ joillakin $g, h \in G$. Tällöin

$$z = h \cdot (g \cdot x) = (hg) \cdot x,$$

joten $x \in \operatorname{Orb} z$. Siis $xRz$, joten relaatio on transitiivinen. Näin ollen $R$ on ekvivalenssirelaatio. □

Lemman 6.6 nojalla radat jakavat joukon $X$ erillisiin ekvivalenssiluokkiin.

## 6.2 Rata–stabiloijalause ja Ei-Burnsiden lemma

**Lause 6.7** (Rata–stabiloijalause)**.** *Olkoon $G$ äärellinen ryhmä ja $X$ $G$-joukko. Tällöin*

$$|\operatorname{Orb} x| = [G : G_x].$$

*Todistus.* [4, s. 92] Määritellään kuvaus $\theta$ seuraavasti:

$$\theta : \operatorname{Orb} x \to \{gG_x \mid g \in G\}, \quad \theta(g \cdot x) = gG_x.$$

Nyt $\theta$ siis kuvaa alkion $x$ radalla olevat alkiot sen määräämän stabiloijaaliryhmän vasemmiksi sivuluokiksi. Kuvaus on hyvin määritelty, sillä jos $g \cdot x = h \cdot x$, niin $(h^{-1}g) \cdot x = x$, eli $h^{-1}g \in G_x$. Näin ollen $gG_x = hG_x$.

Osoitetaan, että $\theta$ on bijektio. Nyt $\theta$ on surjektio, sillä $gG_x = \theta(g \cdot x)$ aina, kun $g \in G$. Riittää siis osoittaa injektiivisyys.

Olkoot $g_1$ ja $g_2$ sellaiset, että $\theta(g_1 \cdot x) = \theta(g_2 \cdot x)$. Tällöin $g_1G_x = g_2G_x$, joten $g_2^{-1}g_1 \in G_x$, siis $x = \left(g_2^{-1}g_1\right) \cdot x$. Operoimalla puolittain alkiolla $g_2$ saadaan

$$g_2 \cdot x = g_2 \cdot \left(\left(g_2^{-1}g_1\right) \cdot x\right) = \left(g_2g_2^{-1}g_1\right) \cdot x = g_1 \cdot x.$$

Siis $\theta$ on injektio ja siten bijektio. Näin ollen jokaista radan $\operatorname{Orb} x$ alkiota vastaa täsmälleen yksi stabiloijan $G_x$ vasen sivuluokka, joten

$$|\operatorname{Orb} x| = [G : G_x]. \qquad \square$$

**Määritelmä 6.8.** Olkoot $G$ ryhmä, $X$ $G$-joukko ja $g \in G$. Määritellään joukko

$$\operatorname{Fix}_X(g) := \{x \in X \mid g \cdot x = x\}.$$

Permutaatioryhmän tapauksessa $\operatorname{Fix}_X(g)$ koostuu siis niistä alkioista, jotka permutaatio $g$ säilyttää.

**Lause 6.9** (Ei-Burnsiden lemma)**.** *Olkoon $G$ äärellinen ryhmä ja $X$ äärellinen $G$-joukko. Tällöin ryhmän $G$ ratojen lukumäärä joukossa $X$ on*

$$\frac{1}{|G|}\sum_{g\in G}|\operatorname{Fix}_X(g)|.$$

*Todistus.* [2, s. 489] Lemman 6.6 nojalla ryhmä $G$ jakaa joukon $X$ erillisiin ratoihin $T_1, T_2, \ldots, T_r$. Määritellään joukko

$$S_j = \{(x,g) \in T_j \times G \;\big|\; g\cdot x = x\}.$$

Nyt $S_j$ koostuu kaikista pareista $(x,g)$, missä $g \in G$ ja $x \in \operatorname{Fix}_{T_j}(g)$. Toisaalta se koostuu kaikista pareista $(x,g)$, missä $x \in T_j$ ja $g \in G_x$. Näin ollen

$$|S_j| = \sum_{g\in G}|\operatorname{Fix}_{T_j}(g)| = \sum_{x\in T_j}|G_x|.$$

Nyt Lauseen 6.7 mukaan $|T_j| = |G|/|G_x|$, eli $|G_x| = |G|/|T_j|$, joten

$$|S_j| = \sum_{x\in T_j}|G_x| = \sum_{x\in T_j}\frac{|G|}{|T_j|} = |G|.$$

Siis

$$\begin{aligned}\sum_{g\in G}|\operatorname{Fix}_X(g)| &= \sum_{g\in G}\left(\sum_{j=1}^{r}|\operatorname{Fix}_{T_j}(g)|\right)\\ &= \sum_{j=1}^{r}\left(\sum_{g\in G}|\operatorname{Fix}_{T_j}(g)|\right)\\ &= \sum_{j=1}^{r}|G| = r|G|.\end{aligned}$$

Näin ollen ratojen lukumäärä $r$ on

$$r = \frac{1}{|G|}\sum_{g\in G}|\operatorname{Fix}_X(g)|. \qquad \square$$

## 6.3 Ei-Burnsiden lemman sovelluksia

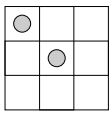
Permutaatioryhmien hyödyllisyys perustuu siihen, että niiden avulla voidaan kuvata erilaisten matemaattisten objektien sisältämiä symmetrioita. Ei-Burnsiden lemma vastaa kysymykseen ”Kuinka monta oleellisesti erilaista ilmentymää tietyllä matemaattisella objektilla on?” Kun muodostetaan joukko objektin kaikista mahdollisista ilmentymistä, niin oleellisesti samanlaiset (*ekvivalentit*) ilmentymät ovat permutaatioryhmän samalla radalla. Ei-Burnsiden lemma kertoo näiden ratojen lukumäärän ja siten myös oleellisesti erilaisten ilmentymien lukumäärän. Tämän kappaleen esimerkkien tarkoituksena on valottaa, miten symmetrioiden lukumäärä voidaan laskea.

### Neliön muotoinen reikäkortti

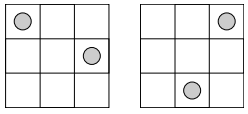
Ajatellaan neliön muotoinen $3 \times 3$ -ruudukko, ja numeroidaan reiät seuraavalla tavalla:

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |

Tehdään reikä kahteen ruutuun. Kun reiät ovat ruuduissa $i$ ja $j$, kutsutaan sitä $(i, j)$-*rei'itykseksi*. Esimerkiksi $(1, 5)$-rei'itys on seuraavanlainen:

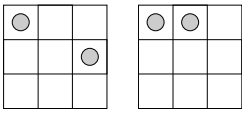


Kahta rei'itystä pidetään samana, jos toisesta päädytään toiseen kiertämällä ruudukkoa. Esimerkiksi rei'itykset $(1, 6)$ ja $(3, 8)$ ovat samat:



Rei'ityksestä $(1, 6)$ saadaan $(3, 8)$ kiertämällä myötäpäivään $90°$.

Sen sijaan rei'itykset $(1, 6)$ ja $(1, 2)$ eivät ole samat:



Tehtävänä on laskea, kuinka monta oleellisesti erilaista rei'itystä on olemassa.

Olkoon $X$ kaikkien rei'itysten joukko. Kaikkiaan mahdollisia rei'ityksiä on olemassa $\binom{9}{2} = 36$ kappaletta, joten $|X| = 36$. Nyt 90°:n kiertoa myötäpäivään

| | | |
|---|---|---|
| 7 | 4 | 1 |
| 8 | 5 | 2 |
| 9 | 6 | 3 |

vastaa permutaatio $\alpha = (1 \quad 3 \quad 9 \quad 7)(2 \quad 6 \quad 8 \quad 4)(5)$. Koska $|\alpha| = 4$, niin kaikki kierrot muodostavat neljän alkion syklisen ryhmän

$$C_4 = \{e, \alpha, \alpha^2, \alpha^3\}.$$

Nyt $C_4$ on permutaatioryhmä joukon $X$ suhteen, ja samanlaiset rei'itykset sijaitsevat samalla ryhmän $C_4$ radalla joukossa $X$. Lasketaan joukkojen $\mathrm{Fix}_X(g)$ alkioiden lukumäärät, kun $g$ käy läpi ryhmän $C_4$ alkiot.

Nyt permutaatio säilyttää rei'ityksen, jos ja vain jos se pitää paikoillaan molemmat rei'itetyt ruudut tai vaihtaa niiden paikat päittäin. Toisin sanoen sen syklirakenteessa on oltava transpoosi tai kaksi 1-sykliä. Esimerkiksi $\alpha$ koostuu kahdesta 4-syklistä ja yhdestä 1-syklistä, joten se ei säilytä mitään rei'itystä. Sen sijaan $\alpha^2 = (1 \quad 9)(2 \quad 8)(3 \quad 7)(4 \quad 6)(5)$ sisältää neljä transpoosia, joten se säilyttää ne neljä rei'itystä, joissa reiät ovat saman transpoosin ruuduissa. Säilyvät rei'itykset ovat siis $(1, 9)$, $(2, 8)$, $(3, 7)$ ja $(4, 6)$.

Ryhmän $C_4$ alkiot syklirakenteineen sekä niiden säilyttämät rei'itykset on eritelty Taulukossa 6.1.

Taulukon 6.1 perusteella joukoissa $\mathrm{Fix}_X(g)$ on yhteensä 40 alkiota, joten

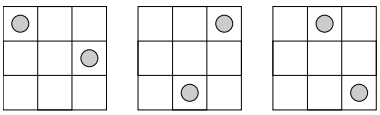
Taulukko 6.1: Ryhmän $C_4$ alkiot ja niiden säilyttämät rei'itykset

| $g$ | Syklirakenne | Säilyvät rei'itykset | $\lvert \mathrm{Fix}_X(g) \rvert$ |
|---|---|---|---|
| $e$ | $(1)(2)\ldots(9)$ | Säilyttää kaikki rei'itykset | 36 |
| $\alpha$ | $(1\ 3\ 9\ 7)(2\ 6\ 8\ 4)(5)$ | Ei sisällä transpooseja eikä kahta 1-sykliä, joten säilyviä rei'ityksiä ei ole | 0 |
| $\alpha^2$ | $(1\ 9)(2\ 8)(3\ 7)(4\ 6)(5)$ | Säilyttää ne rei'itykset, joissa reiät ovat saman transpoosin ruuduissa | 4 |
| $\alpha^3$ | $(1\ 7\ 9\ 3)(2\ 4\ 8\ 6)(5)$ | Kuten $\alpha$ | 0 |
| yhteensä | | | 40 |

Ei-Burnsiden lemman nojalla oleellisesti erilaisten rei'itysten lukumäärä on

$$r = \frac{1}{|C_4|} \sum_{g \in C_4} |\,\mathrm{Fix}_X(g)| = \frac{1}{4} \cdot 40 = 10.$$

Entä, jos kiertämisen lisäksi reikäkortti voidaan myös kääntää ympäri (eli peilata jonkin symmetria-akselin suhteen), ja myös näin toisistaan saatuja rei'ityksiä pidetään samoina? Tällöin esimerkiksi rei'itykset $(1, 6)$, $(3, 8)$ ja $(2, 9)$ ovat samat:



Kuten edellä, rei'ityksestä $(1, 6)$ saadaan $(3, 8)$ kiertämällä myötäpäivään $90°$, ja tästä päästään edelleen rei'itykseen $(2, 9)$ peilaamalla kortti vaaka-akselin suhteen.

Nyt peilausta vaaka-akselin suhteen

| | | |
|---|---|---|
| 7 | 8 | 9 |
| 4 | 5 | 6 |
| 1 | 2 | 3 |

vastaa permutaatio $\beta = (1 \quad 7)(2 \quad 8)(3 \quad 9)(4)(5)(6)$.

Permutaatioilla $\alpha$ ja $\beta$ saadaan aikaan kahdeksan alkion permutaatioryhmä, neliön symmetrioista koostuva *dihedraaliryhmä* $D_4$:

$$D_4 = \{e, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3\}.$$

Nyt $D_4$ on permutaatioryhmä joukon $X$ suhteen, ja samanlaiset rei'itykset sijaitsevat samalla ryhmän $D_4$ radalla joukossa $X$. Kuten aiemmin, riittää laskea joukkojen $\mathrm{Fix}_X(g)$ alkioiden lukumäärät, kun $g$ käy läpi ryhmän $D_4$ alkiot.

Nyt $\beta$ koostuu kolmesta transpoosista ja yhdestä 1-syklistä. Se siis säilyttää yhteensä kuusi rei'itystä: rei'itykset $(1, 7)$, $(2, 8)$ ja $(3, 9)$ vaihtamalla reikien paikat päittäin sekä rei'itykset $(4, 5)$, $(4, 6)$ ja $(5, 6)$ pitämällä molemmat reiät paikoillaan.

Ryhmän $D_4$ alkiot syklirakenteineen sekä niiden säilyttämät rei'itykset on eritelty Taulukossa 6.2.

Taulukon 6.2 perusteella joukoissa $\mathrm{Fix}_X(g)$ on yhteensä 64 alkiota, joten Ei-Burnsiden lemman nojalla oleellisesti erilaisten rei'itysten lukumäärä on

$$r = \frac{1}{|D_4|} \sum_{g \in D_4} |\,\mathrm{Fix}_X(g)| = \frac{1}{8} \cdot 64 = 8.$$

### Helminauha

Ajatellaan päistä avoin nauha, jossa on kuusi helmeä. Jokainen helmi on joko musta tai valkoinen. Kahta nauhaa pidetään ekvivalentteina, jos toinen saadaan toisesta kääntämällä nauha ympäri eli peilaamalla nauhan keskikohdan

Taulukko 6.2: Ryhmän $D_4$ alkiot ja niiden säilyttämät rei'itykset

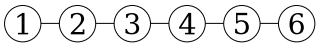
| $g$ | Syklirakenne | Säilyvät rei'itykset | $\lvert \mathrm{Fix}_X(g) \rvert$ |
|---|---|---|---|
| $e$ | $(1)(2)\dots(9)$ | Säilyttää kaikki rei'itykset | 36 |
| $\alpha$ | $(1\ 3\ 9\ 7)(2\ 6\ 8\ 4)(5)$ | Ei sisällä transpooseja eikä kahta 1-sykliä, joten säilyviä rei'ityksiä ei ole | 0 |
| $\alpha^2$ | $(1\ 9)(2\ 8)(3\ 7)(4\ 6)(5)$ | Säilyttää ne rei'itykset, joissa reiät ovat saman transpoosin ruuduissa | 4 |
| $\alpha^3$ | $(1\ 7\ 9\ 3)(2\ 4\ 8\ 6)(5)$ | Kuten $\alpha$ | 0 |
| $\beta$ | $(1\ 7)(2\ 8)(3\ 9)(4)(5)(6)$ | Säilyttää rei'itykset, joissa reiät ovat saman transpoosin ruuduissa (3 kpl) sekä rei'itykset, joissa molemmat reiät pysyvät paikoillaan ($\binom{3}{2} = 3$ kpl) | 6 |
| $\beta\alpha$ | $(1\ 9)(2\ 6)(4\ 8)(3)(5)(7)$ | Kuten $\beta$ | 6 |
| $\beta\alpha^2$ | $(1\ 3)(4\ 6)(7\ 9)(2)(5)(8)$ | Kuten $\beta$ | 6 |
| $\beta\alpha^3$ | $(2\ 4)(3\ 7)(6\ 8)(1)(5)(9)$ | Kuten $\beta$ | 6 |
| yhteensä | | | 64 |

suhteen. Esimerkiksi seuraavat nauhat ovat ekvivalentit:

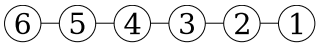
Seuraava nauha taas ei ole ekvivalentti edellisten kanssa:

Kuinka monta oleellisesti erilaista nauhaa on olemassa?

Olkoon $X$ kaikkien mahdollisten nauhojen joukko. Nyt $|X| = 2^6 = 64$. Numeroidaan helmet seuraavasti:




Nauhan kääntämistä

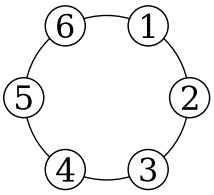



vastaa permutaatio $\alpha = (1 \quad 6)(2 \quad 5)(3 \quad 4)$. Nyt $|\alpha| = 2$, joten joukkoa $X$ permutoiva permutaatioryhmä on $G = \{e, \alpha\}$, ja ekvivalentit nauhat sijaitsevat sen samalla radalla. Permutaatio $e$ säilyttää kaikki nauhat, joten $\mathrm{Fix}_X(e) = 64$. Permutaatio $\alpha$ säilyttää ne nauhat, joissa saman transpoosin muodostavat helmet ovat samanväriset. Koska värejä on 2 ja transpooseja 3, on säilyviä nauhoja $2^3 = 8$ kappaletta. Siis $\mathrm{Fix}_X(\alpha) = 8$. Näin ollen ei-Burnsiden lemman nojalla ratojen lukumäärä eli oleellisesti erilaisten nauhojen lukumäärä on

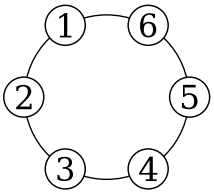
$$r = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}_X(g)| = \frac{1}{2}(64 + 8) = 36.$$

Entä, jos nauha yhdistetään päistään? Nyt nauhaa voidaan kääntämisen lisäksi kiertää, ja myös kiertämällä toisistaan saatuja nauhoja pidetään keskenään ekvivalentteina. Kuinka monta oleellisesti erilaista nauhaa on nyt olemassa?

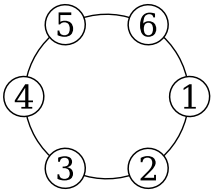
Numeroidaan helmet nyt seuraavasti:




Nauhan kääntämistä ympäri




vastaa edelleen permutaatio $\alpha = (1 \quad 6)(2 \quad 5)(3 \quad 4)$. Nyt nauhan kiertämistä $60°$ myötäpäivään




vastaa permutaatio $\beta = (1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6)$. Permutaatioilla $\alpha$ ja $\beta$ saadaan aikaan säännöllisen kuusikulmion symmetrioista koostuva kahdentoista alkion permutaatioryhmä, dihedraaliryhmä $D_6$:

$$D_6 = \{e, \alpha, \beta, \beta\alpha, \beta^2, \beta^2\alpha, \beta^3, \beta^3\alpha, \beta^4, \beta^4\alpha, \beta^5, \beta^5\alpha\}.$$

Nyt $D_6$ on permutaatioryhmä joukon $X$ suhteen, ja ekvivalentit nauhat sijaitsevat samalla ryhmän $D_6$ radalla joukossa $X$.

Permutaatio säilyttää nauhan täsmälleen silloin, kun jokainen erillinen sykli koostuu keskenään samanvärisistä helmistä. Koska värivaihtoehtoja on kaksi, permutaation säilyttämien nauhojen lukumäärä on $2^n$, missä $n$ on erillisten syklien lukumäärä. Näin ollen joukkojen $\mathrm{Fix}_X(g)$ alkioiden lukumäärät nähdään suoraan permutaatioiden syklirakenteista.

Taulukko 6.3: Ryhmän $D_6$ alkiot ja niiden säilyttämät nauhat

| $g$ | Syklirakenne | Erillisiä syklejä ($n$) | $\lvert \mathrm{Fix}_X(g) \rvert$ ($2^n$) |
|---|---|---|---|
| $e$ | $(1)(2)\ldots(6)$ | 6 | 64 |
| $\alpha$ | $(1\quad 6)(2\quad 5)(3\quad 4)$ | 3 | 8 |
| $\beta$ | $(1\quad 2\quad 3\quad 4\quad 5\quad 6)$ | 1 | 2 |
| $\beta\alpha$ | $(1)(2\quad 6)(3\quad 5)(4)$ | 4 | 16 |
| $\beta^2$ | $(1\quad 3\quad 5)(2\quad 4\quad 6)$ | 2 | 4 |
| $\beta^2\alpha$ | $(1\quad 2)(3\quad 6)(4\quad 5)$ | 3 | 8 |
| $\beta^3$ | $(1\quad 4)(2\quad 5)(3\quad 6)$ | 3 | 8 |
| $\beta^3\alpha$ | $(1\quad 3)(2)(4\quad 6)(5)$ | 4 | 16 |
| $\beta^4$ | $(1\quad 5\quad 3)(2\quad 6\quad 4)$ | 2 | 4 |
| $\beta^4\alpha$ | $(1\quad 4)(2\quad 3)(5\quad 6)$ | 3 | 8 |
| $\beta^5$ | $(1\quad 6\quad 5\quad 4\quad 3\quad 2)$ | 1 | 2 |
| $\beta^5\alpha$ | $(1\quad 5)(2\quad 4)(3)(6)$ | 4 | 16 |
| yhteensä | | | 156 |

Ryhmän $D_6$ alkiot syklirakenteineen sekä niiden säilyttämät nauhat on eritelty Taulukossa 6.3.

Ei-Burnsiden lemman nojalla oleellisesti erilaisten nauhojen lukumäärä on nyt

$$r = \frac{1}{|D_6|} \sum_{g \in D_6} |\,\mathrm{Fix}_X(g)| = \frac{1}{12} \cdot 156 = 13.$$

# 7 Alaraja alternoivan ryhmän suurimman alkion kertaluvulle

Tutkielman lopuksi osoitetaan vielä yksi tulos permutaatioryhmiin liittyen. Tuloksessa annetaan eräs alaraja alternoivan ryhmän permutaation suurimmalle kertaluvulle riippuen ryhmän asteesta. Ennen tulokseen päätymistä esitetään todistuksessa tarvittavia esitietoja.

**Lemma 7.1.** *Olkoot $n$ positiivinen kokonaisluku ja $p$ alkuluku. Tällöin suurin luvun $p$ potenssi, joka jakaa luvun $n!$, on $p^{\nu(n)}$, missä*

$$\nu(n) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

*Todistus.* Joukossa $\{1, 2, \ldots, n\}$ on luvun $p$ monikertoja yhteensä $\lfloor n/p \rfloor$ kappaletta. Vastaavasti luvun $p^2$ monikertoja on $\lfloor n/p^2 \rfloor$ kappaletta ja yleisesti luvun $p^i$ monikertoja $\lfloor n/p^i \rfloor$ kappaletta. Näin ollen luvussa $n!$ esiintyvien monikertojen määrä on

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \nu(n).$$

Summattavia on äärellinen määrä, sillä $\lfloor n/p^i \rfloor = 0$, kun $p^i > n$. Näin ollen $p^{\nu(n)}$ on suurin luvun $p$ potenssi, joka jakaa luvun $n!$. □

**Lemma 7.2.** *Määritellään funktio*

$$\theta^*(z) := \sum_{2<p\leq z} \log p$$

*kaikilla $z \in \mathbf{R}_+$, kun* log *on luonnollinen logaritmi ja $p$ käy läpi parittomat alkuluvut. Tällöin $\theta^*(z) > z/2$ aina, kun $z \geq 11$.*

*Todistus.* [1, s. 143–144] Nyt $\theta^*(11) \geq 7 > 11/2$, joten väite pätee arvolla 11. Lisäksi tästä nähdään suoraan väitteen pätevän myös arvolla 13, sillä $\theta^*$

Taulukko 7.1: Tiettyjä alkulukuja $p$ vastaavat funktion $\theta^*$ alarajat. Alkuluvut on valittu siten, että $p_{i+1}$ on suurin alkuluku, jolle pätee $p_{i+1} < 2\theta^*(p_i)$.

| $p_i$ | $=$ | 11 | 13 | 19 | 29 | 43 | 71 | 113 | 211 | 383 | 709 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\theta^*(p_i)$ | $\geq$ | 7,0 | 9,6 | 15,3 | 21,8 | 36,4 | 60,8 | 106,3 | 193,2 | 358,0 | 678,8 |

on kasvava ja $7 > 13/2$. Yleisesti voidaan päätellä väitteen pätevän kaikilla $p < 2\theta^*(p_0)$, mikäli se pätee arvolla $p_0$. Näin ollen Taulukosta 7.1 nähdään, että väite pätee, kun $z < 1270$, joten voidaan olettaa, että $z \geq 1270$.

Riittää osoittaa, että $\theta^*(2n) \geq n + 1$ kaikilla kokonaisluvuilla $n \geq 635$, sillä tällöin

$$\theta^*(z) \geq \theta^*\left(2\left\lfloor\frac{z}{2}\right\rfloor\right) \geq \left\lfloor\frac{z}{2}\right\rfloor + 1 > \frac{z}{2}.$$

Todistetaan väite induktiolla luvun $n$ suhteen, kun $n \geq 635$. Oletetaan siis, että väite pätee kaikilla kokonaisluvuilla $k$, joille $11 \leq k < n$.

Olkoon nyt $m = \binom{2n}{n}$. Tällöin $m$ on suurin binomikertoimista

$$\binom{2n}{0}, \binom{2n}{1}, \ldots, \binom{2n}{2n},$$

ja lisäksi

$$2^{2n} = (1+1)^{2n} = \underbrace{\overbrace{\binom{2n}{0}}^{=1<m} + \binom{2n}{1} + \ldots + \binom{2n}{2n-1} + \overbrace{\binom{2n}{2n}}^{=1<m}}_{2n+1 \text{ kpl}} < 2n \cdot m.$$

Siis $m > 2^{2n}/2n$.

Nyt $m = (2n)!/(n!)^2$. Lemman 7.1 nojalla

$$(2n)! = \prod_{p \leq 2n} p^{s_p}, \quad \text{missä } s_p = \sum_{i=1}^{\infty} \left\lfloor \frac{2n}{p^i} \right\rfloor,$$

ja

$$n! = \prod_{p \le 2n} p^{t_p}, \quad \text{missä } t_p = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor .$$

(Jälkimmäisessä esityksessä $p$ voi käydä läpi alkuluvut aina lukuun $2n$ saakka, sillä eksponentit $t_p$ ovat nollia, kun $p > n$.) Näin ollen

$$\begin{aligned} \log m &= \log \frac{(2n)!}{(n!)^2} = \log[(2n)!] - 2\log(n!) \\ &= \sum_{p \le 2n} s_p \log p - 2 \sum_{p \le 2n} t_p \log p = \sum_{p \le 2n} (s_p - 2t_p) \log p = \sum_{p \le 2n} \delta(p) \log p, \end{aligned}$$

missä

$$\delta(p) = s_p - 2t_p = \sum_{i=1}^{\infty} \left( \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right).$$

Koska $\lfloor 2\xi \rfloor = 2\lfloor \xi \rfloor$ tai $2\lfloor \xi \rfloor + 1$ kaikilla $\xi \in \mathbf{R}$, jokainen luvun $\delta(p)$ summattava on joko 0 tai 1. Lisäksi kaikki termit ovat nollia, kun $p^i > 2n$. Näin ollen summattavien lukumäärälle ja siten myös luvulle $\delta(p)$ saadaan yläraja

$$\delta(p) \le \left\lfloor \frac{\log 2n}{\log p} \right\rfloor .$$

Jos $\sqrt{2n} < p \le 2n$, niin $\delta(p) \le 1$, sillä tällöin

$$\frac{\log 2n}{\log p} < \frac{\log 2n}{\log \sqrt{2n}} = 2.$$

Jos taas $p \le \sqrt{2n}$, niin

$$\delta(p) \log p \le \left\lfloor \frac{\log 2n}{\log p} \right\rfloor \log p \le \frac{\log 2n}{\log p} \log p = \log 2n.$$

Siis

$$\begin{aligned} \log m &= \sum_{p \le 2n} \delta(p) \log p = \sum_{p \le \sqrt{2n}} \underbrace{\delta(p) \log p}_{\le \log 2n} + \sum_{\sqrt{2n} < p \le 2n} \underbrace{\delta(p)}_{\le 1} \log p \\ &\le \underbrace{\sum_{p \le \sqrt{2n}} \log 2n}_{\le \sqrt{2n} \log 2n} + \underbrace{\sum_{\sqrt{2n} < p \le 2n} \log p}_{= \theta^*(2n) - \theta^*\left(\sqrt{2n}\right)} . \end{aligned}$$

Koska $m > 2^{2n}/2n$, niin $\log m > 2n \log 2 - \log 2n$. Näin ollen

$$2n \log 2 - \log 2n < \log m \leq \sqrt{2n} \log 2n + \theta^*(2n) - \theta^* \left( \sqrt{2n} \right).$$

Nyt siis

$$\begin{aligned} \theta^*(2n) &> 2n \log 2 - \log 2n - \sqrt{2n} \log 2n + \theta^* \left( \sqrt{2n} \right) \\ &= 2n \log 2 - \left( 1 + \sqrt{2n} \right) \log 2n + \theta^* \left( \sqrt{2n} \right). \end{aligned}$$

Vähentämällä epäyhtälön molemmilta puolilta $n + 1$ se saadaan muotoon

$$\theta^*(2n) - n - 1 > (2 \log 2 - 1)n - \left( 1 + \sqrt{2n} \right) \log 2n + \theta^* \left( \sqrt{2n} \right) - 1. \quad (7.1)$$

Induktio-oletuksen nojalla $\theta^*(2k) \geq k + 1$ kaikilla kokonaisluvuilla $k$, kun $11 \leq k < n$. Nyt

$$2 \left\lfloor \frac{\sqrt{2n}}{2} \right\rfloor \geq 2 \left\lfloor \frac{\sqrt{2 \cdot 635}}{2} \right\rfloor = 34,$$

joten

$$\theta^* \left( \sqrt{2n} \right) \geq \theta^* \left( 2 \left\lfloor \frac{\sqrt{2n}}{2} \right\rfloor \right) \geq \left\lfloor \frac{\sqrt{2n}}{2} \right\rfloor + 1 > \frac{\sqrt{2n}}{2}.$$

Näin ollen epäyhtälöstä (7.1) saadaan

$$\theta^*(2n) - n - 1 > (2 \log 2 - 1)n - \left( 1 + \sqrt{2n} \right) \log 2n + \frac{\sqrt{2n}}{2} - 1. \quad (7.2)$$

Merkitään epäyhtälön (7.2) oikeaa puolta funktiona $f(n)$. Nyt $f(635) > 0$, ja lisäksi

$$f'(n) = 2 \log 2 - 1 + \frac{1}{2\sqrt{2n}} - \left( \frac{\log 2n}{\sqrt{2n}} + \frac{1 + \sqrt{2n}}{n} \right).$$

Kun $n \geq 635$, suluissa olevat termit ovat väheneviä, sekä niille pätevät arviot

$$\frac{\log 2n}{\sqrt{2n}} < \frac{1}{4} \quad \text{ja} \quad \frac{1 + \sqrt{2n}}{n} < \frac{1}{17}.$$

Lisäksi termi $1/\left(2\sqrt{2n}\right)$ on positiivinen, joten

$$f'(n) > 2 \log 2 - 1 - \frac{1}{4} - \frac{1}{17} > 0.$$

Näin ollen epäyhtälön (7.2) oikea puoli on positiivinen, joten

$$\theta^*(2n) > n + 1.$$

Induktioväite on todistettu, joten lemma pätee. □

**Lause 7.3.** *Jos $n \geq 7$, niin alternoiva ryhmä $A_n$ sisältää permutaation, jonka kertaluku on suurempi kuin*

$$\mathrm{e}^{\sqrt{\frac{1}{4}n \log n}}.$$

*Todistus.* [1, s. 145] Olkoot $p_1, p_2, \ldots, p_r$ erisuuret parittomat alkuluvut, joille $p_1 + p_2 + \ldots + p_r \leq n$. Tällöin voidaan valita erilliset syklit $\alpha_1, \alpha_2, \ldots, \alpha_r$ siten, että $|\alpha_i| = p_i$ kaikilla $i$. Edellä mainitun epäyhtälön nojalla nämä syklit siirtävät korkeintaan $n$ alkiota. Koska niiden pituudet ovat parittomia, ne ovat parillisia permutaatioita. Näin ollen ne kuuluvat alternoivaan ryhmään $A_n$, samoin kuin niiden tulo $\alpha = \alpha_1\alpha_2 \ldots \alpha_r$. Koska syklien pituudet ovat keskenään jaottomia, on $|\alpha| = p_1p_2 \ldots p_r$. Nyt

$$\log |\alpha| = \log \prod_{i=1}^{r} p_i = \sum_{i=1}^{r} \log p_i,$$

joten väitteen todistamiseksi riittää osoittaa, että on olemassa luku $z \in \mathbf{R}_+$, jolle pätee

$$\text{(a)} \quad \sum_{2<p\leq z} p \leq n \quad \text{ja} \quad \text{(b)} \quad \theta^*(z)^2 > \frac{1}{4} n \log n.$$

Ennen tätä osoitetaan kuitenkin, että väite pätee, kun $7 \leq n \leq 26$.

- Kun $n = 7$, $A_n$ sisältää alkion kertalukua 7.
- Kun $8 \leq n \leq 11$, $A_n$ sisältää alkion kertalukua $3 \cdot 5 = 15$.
- Kun $12 \leq n \leq 17$, $A_n$ sisältää alkion kertalukua $5 \cdot 7 = 35$.
- Kun $18 \leq n \leq 26$, $A_n$ sisältää alkion kertalukua $3 \cdot 5 \cdot 7 = 105$.

Taulukko 7.2: Tiettyjä luvun $n$ arvoja vastaavat funktion $\mathrm{e}^{\sqrt{\frac{1}{4}n\log n}}$ ylärajat.

| $n$ | $=$ | 7 | 11 | 17 | 26 |
|---|---|---|---|---|---|
| $\mathrm{e}^{\sqrt{\frac{1}{4}n\log n}}$ | $\leq$ | 6,4 | 13,1 | 32,2 | 99,7 |

Vertaamalla näitä kertalukuja Taulukon 7.2 arvoihin nähdään, että väite pätee, kun $7 \leq n \leq 26$. Oletetaan jatkossa, että $n \geq 22$.

Määritellään kuvaus

$$F(z) := \frac{z}{\log z}.$$

Nyt

$$F'(z) = \frac{\log z - 1}{\log^2 z} > 0, \quad \text{kun } z > \mathrm{e}.$$

Siis $F(z)$ on aidosti kasvava, kun $z > \mathrm{e}$, joten

$$\begin{aligned}
\sum_{2<p\leq z} p &= \sum_{2<p\leq z} \left(\frac{p}{\log p}\log p\right) \\
&= \sum_{2<p\leq z} \underbrace{F(p)}_{\leq F(z)} \log p \\
&\leq F(z) \sum_{2<p\leq z} \log p \\
&= F(z)\theta^*(z).
\end{aligned}$$

Valitaan $z$ siten, että $F(z)\theta^*(z) = n$. Jos $z < 11$, niin

$$F(z)\theta^*(z) < F(11)\theta^*(11) = \frac{11}{\log 11}\log(3\cdot 5\cdot 7) < 22.$$

Tällöin ehto (a) ei toteudu, joten on oltava $z \geq 11$. Lemman 7.2 nojalla

$z < 2\theta^*(z)$, joten

$$n = F(z)\theta^*(z) < F\left(2\theta^*(z)\right)\theta^*(z) = \frac{2\theta^*(z)}{\log 2\theta^*(z)}\theta^*(z) = \frac{2\theta^*(z)^2}{\log 2\theta^*(z)}$$
$$= \frac{4\theta^*(z)^2}{2\log 2\theta^*(z)} = \frac{4\theta^*(z)^2}{\log\left[(2\theta^*(z))^2\right]} = \frac{4\theta^*(z)^2}{\log\left[4\theta^*(z)^2\right]} = F\left(4\theta^*(z)^2\right).$$

Toisaalta

$$F(n\log n) = \frac{n\log n}{\log(n\log n)} = n\frac{\log n}{\log n + \underbrace{\log\log n}_{>0,\ \text{kun } n > \mathrm{e}}} < n\frac{\log n}{\log n} = n.$$

Siis $F(n\log n) < n < F\left(4\theta^*(z)^2\right)$. Koska $F$ on kasvava, saadaan

$$n\log n < 4\theta^*(z)^2,$$

jolloin ehto (b) on voimassa. Näin ollen väite on todistettu. □

# Viitteet

[1] Dixon, J. D. & Mortimer, B.: *Permutation Groups*. New York: Springer-Verlag, 1996.

[2] Gallian, J. A.: *Contemporary Abstract Algebra* (7. painos). Belmont, CA: Brooks/Cole, 2010.

[3] Herstein, I. N.: *Abstract Algebra* (3. painos). Upper Saddle River, NJ: Prentice-Hall, 1996.

[4] Humphreys, J. F.: *A Course in Group Theory*. New York: Oxford University Press, 1996.

[5] Niemenmaa, M.: *Algebra II* (luentomoniste). Oulun yliopisto, 2008.

[6] Niemenmaa, M.: *Ryhmäteoria* (luentomoniste). Oulun yliopisto, 2009.