

## 5 Tuloryhmät

Jotkin ryhmät voidaan jakaa toisistaan riippumattomiin osiin niin, että jokainen ryhmän alkio saadaan tulona eri osista valituista alkioista. Tällöin ryhmää voidaan käsitellä osiensa tulona eli tuloryhmänä.

### 5.1 Suorat tulot

Tarkastellaan aluksi permutaatioryhmiin liittyvää esimerkkiä.

**Esimerkki 5.1.** Symmetrisestä ryhmästä  $S_4$  löytyy muun muassa syklien virittämät aliryhmät

$$H = \langle (1234) \rangle = \{\text{id}, (1234), (13)(24), (1432)\}$$

ja

$$K = \langle (123) \rangle = \{\text{id}, (123), (132)\}.$$

Näiden aliryhmien alkioista voidaan muodostaa tulojoukko  $HK$ , johon kuuluvat kaikki muotoa  $hk$  olevat alkio, missä  $h \in H$  ja  $k \in K$ . Laskemalla kukin näistä 12 tulosta nähdään, että

$$HK = \{ \text{id}, (1234), (13)(24), (1432), \\ (123), (1324), (142), (34), \\ (132), (14), (234), (1243) \}.$$

Saatu tulojoukko ei kuitenkaan ole ryhmän  $S_4$  aliryhmä, koska esimerkiksi  $(1324) \in HK$ , mutta  $(1324)^2 = (12)(34) \notin HK$ .

Etsitään nyt jokin ehto, jolla aliryhmien tulosta  $HK$  tulisi ryhmä. Kahden tulojoukosta valitun alkion  $h_1k_1$  ja  $h_2k_2$  tulo on  $h_1k_1h_2k_2$ , joka ei välttämättä kuulu joukkoon  $HK$ . Eräs tapa korjata tilanne on vaatia, että aliryhmien  $H$  ja  $K$  alkio olisivat vaihdannaisia keskenään. Jos tämä ehto toteutuu, edellä mainitussa tulossa pätee

$$h_1 \underbrace{k_1 h_2}_{\text{vaihd.}} k_2 = h_1 h_2 k_1 k_2,$$

ja oikeanpuoleinen tulo kuuluu nyt joukkoon  $HK$ . Myös minkä tahansa tulojoukosta poimitun alkion  $hk$  käänteisalkio kuuluu tällöin joukkoon  $HK$ , sillä  $h^{-1} \in H$  ja  $k^{-1} \in K$ , ja näin ollen  $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in HK$ . Joukosta  $HK$  tulee tällöin aliryhmä, sillä myös neutraalialkiolle pätee  $e = e \cdot e \in HK$ .

**Määritelmä 5.2.** Olkoot  $H$  ja  $K$  ryhmän  $G$  aliryhmiä. Joukkoa  $HK$  kutsutaan aliryhmien  $H$  ja  $K$  *sisäiseksi suoraksi tuloksi*, jos se toteuttaa seuraavat ehdot:

- 1)  $hk = kh$  kaikilla  $h \in H$  ja  $k \in K$
- 2)  $H \cap K = \{e\}$ , missä  $e$  on ryhmän  $G$  neutraalialkio.

Sisäistä suoraa tuloa merkitään  $H \times K$  tai toisinaan (sisäisyyttä korostaen) myös  $(H \times K)_s$ . Jos ryhmässä  $G$  on laskutoimituksena yhteenlasku, tuloa kutsutaan *sisäiseksi suoraksi summaksi* ja merkitään  $H \oplus K$ .

Edellä havaittiin, että kahden aliryhmän sisäinen suora tulo  $H \times K$  on itsekin aliryhmä. Myöhemmin nähdään myös toinen tilanne, jossa kahden aliryhmän tulosta  $HK$  tulee aliryhmä.

**Esimerkki 5.3.** Tarkastellaan symmetrisen ryhmän  $S_5$  aliryhmiä

$$H = \{\text{id}, (123), (132)\} \quad \text{ja} \quad K = \{\text{id}, (45)\}.$$

Koska erilliset syklit kommutoivat keskenään, pätee  $hk = kh$  kaikille  $h \in H$  ja  $k \in K$ . Lisäksi  $H \cap K = \{\text{id}\}$ , joten joukko

$$HK = \{\text{id}, (123), (132), (45), (123)(45), (132)(45)\}$$

on aliryhmien  $H$  ja  $K$  suora tulo, eli  $HK = H \times K$ . Huomataan, että  $H \times K \leq S_5$ .

**Esimerkki 5.4.** Tarkastellaan yhteenlaskuryhmää  $\mathbb{Z}_{15} = \{[0], [1], [2], \dots, [14]\}$ , missä  $[n] = [m]$  aina, kun  $m - n$  on jaollinen luvulla 15. Tällä ryhmällä on aliryhmät

$$H = \langle [5] \rangle = \{[0], [5], [10]\} \quad \text{ja} \quad K = \langle [3] \rangle = \{[0], [3], [6], [9], [12]\}.$$

Koska ryhmä  $\mathbb{Z}_{15}$  on vaihdannainen ja  $H \cap K = \{[0]\}$ , voidaan muodostaa aliryhmien  $H$  ja  $K$  suora summa  $H \oplus K$ . Lasketaan summa-alkiot oheiseen taulukkoon. (Jätetään taulukon alkioista hakasulut selvyuden vuoksi merkitsemättä.)

$H \oplus K$	[0]	[5]	[10]
[0]	0	5	10
[3]	3	8	13
[6]	6	11	1
[9]	9	14	4
[12]	12	2	7

Taulukosta huomataan, että  $H \oplus K = \mathbb{Z}_{15}$ . Lisäksi kukin ryhmän  $\mathbb{Z}_{15}$  alkio esiintyy taulukossa täsmälleen kerran.

Todistetaan seuraavassa lemmassa kaksi hyödyllistä ehtoa, jotka pätevät kaikille ryhmille, jotka voidaan esittää aliryhmiensä suorana tulona.

**Lemma 5.5.** *Oletetaan, että  $H$  ja  $K$  ovat ryhmän  $G$  aliryhmiä ja että  $G = H \times K$ . Tällöin seuraavat ehdot pätevät:*

- 1) Ryhmät  $H$  ja  $K$  ovat  $G$ :n normaaleja aliryhmiä.
- 2) Jokaisella alkioilla  $g \in G$  on yksikäsitteinen esitys  $g = hk$ , missä  $h \in H$  ja  $k \in K$ .

*Todistus.* Osoitetaan ensin, että ehto 1) pätee. Olkoot sitä varten  $x \in H$ ,  $y \in K$  ja  $g \in G$ . Osoitetaan, että konjugaatit  ${}^g x$  ja  ${}^g y$  kuuluvat edelleen aliryhmiin  $H$  ja  $K$ . Koska  $G = H \times K$ , voidaan kirjoittaa  $g = hk$  joillain  $h \in H$  ja  $k \in K$ . Nyt pätee  $kx = xk$ , joten

$$gxg^{-1} = h(kx)k^{-1}h^{-1} = h(xk)k^{-1}h^{-1} = hxh^{-1} \in H.$$

Toisaalta myös  $h(kyk^{-1}) = (kyk^{-1})h$ , joten

$$gyg^{-1} = h(kyk^{-1})h^{-1} = (kyk^{-1})hh^{-1} = kyk^{-1} \in K.$$

Siispä  ${}^g x \in H$  ja  ${}^g y \in K$ , joten aliryhmät  $H$  ja  $K$  ovat normaaleja.

Todistetaan sitten ehto 2). Oletetaan, että alkiolla  $g \in G$  on esitykset tuloina  $h_1k_1$  ja  $h_2k_2$ , missä  $h_1, h_2 \in H$  ja  $k_1, k_2 \in K$ . Siispä  $h_1k_1 = h_2k_2$ , josta saadaan

$$h_2^{-1}h_1 = k_2k_1^{-1}.$$

Yllä olevan yhtälön vasemman puolen alkio kuuluu joukkoon  $H$  ja oikean puolen alkio joukkoon  $K$ , joten molemmat alkioit kuuluvat itse asiassa leikkausjoukkoon  $H \cap K$ . Toisaalta suoran tulon määritelmän mukaan  $H \cap K = \{e\}$ , missä  $e$  on ryhmän  $G$  neutraalialkio. Täten  $h_2^{-1}h_1 = e$  ja  $k_2k_1^{-1} = e$ , mistä nähdään, että  $h_1 = h_2$  ja  $k_1 = k_2$ . Alkion  $g$  esitys on siis yksikäsitteinen.  $\square$

*Lisätieto.* Aliryhmien sisäinen suora tulo voidaan määrittellä myös useammalle kuin kahdelle aliryhmälle. Määritelmä on aivan samanlainen kuin kahden aliryhmän tapauksessa. Jos aliryhmät ovat  $H_1, \dots, H_r$ , ehdoiksi tulee

- 1)  $h_i h_j = h_j h_i$ , kun  $i \neq j$ ,  $h_i \in H_i$  ja  $h_j \in H_j$
- 2)  $H_i \cap (H_{j_1} H_{j_2} \cdots H_{j_{r-1}}) = \{e\}$ , kun  $i \notin \{j_1, \dots, j_{r-1}\}$ .

Suoraa tuloa voidaan tällöin merkitä  $H_1 \times H_2 \times \cdots \times H_n$  tai tulomerkinällä  $\prod_{i=1}^n H_i$ . Määritelmä toimii myös äärettömän monen aliryhmän tapauksessa. Tällöin kuitenkin jokaisella suoran tulon  $\prod_{i \in I} H_i$  alkiolla on *äärellinen* esitys  $h_{i_1} h_{i_2} \cdots h_{i_n}$ , missä  $h_{i_k} \in H_{i_k}$  kaikilla  $k$ . Ääretöntä alkioiden tuloa ei nimittäin voida ryhmässä yleensä määrittellä.

Sisäinen suora tulo määritellään jonkin ryhmän  $G$  sisältämien aliryhmien välillä. Koska kuitenkin osoittautuu, että nämä aliryhmät ovat täysin riippumattomia toisistaan, ei ympäröivää ryhmää  $G$  oikeastaan tarvita mihinkään, vaan suora tulo voidaan määrittellä minkä tahansa kahden ryhmän välillä. Se, että ryhmissä on mahdollisesti täysin erilaiset alkioit ja laskutoimitukset, ei tuota estettä.

**Määritelmä 5.6.** Ryhmien  $(G_1, \circ)$  ja  $(G_2, *)$  *ulkoinen suora tulo* on ryhmä, jonka alkiot ovat parit  $(g_1, g_2)$ , missä  $g_1 \in G_1$  ja  $g_2 \in G_2$ , ja laskutoimituksena

$$(g_1, g_2) \cdot (g'_1, g'_2) = (g_1 \circ g'_1, g_2 * g'_2).$$

Ulkoista suoraa tuloa merkitään  $G_1 \times G_2$  tai toisinaan  $(G_1 \times G_2)_u$ . Jos molemmissa ryhmissä käytetään laskutoimituksena yhteenlaskua, voidaan ulkoista suoraa tuloa kutsua myös *ulkoiseksi suoraksi summaksi* ja merkitä  $G_1 \oplus G_2$ .

Se, että ulkoinen suora tulo todellakin on ryhmä, on varsin helppo tarkistaa. Erityisesti neutraalialkiona toimii pari  $(e_1, e_2)$ , missä  $e_1$  ja  $e_2$  ovat ryhmien  $G_1$  ja  $G_2$  neutraalialkiot, ja alkion  $(g_1, g_2) \in G_1 \times G_2$  käänteisalkio on  $(g_1^{-1}, g_2^{-1})$ .

**Esimerkki 5.7.** Muodostetaan ryhmien

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\} \quad \text{ja} \quad \mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$$

ulkoinen suora summa. Tulo koostuu pareista  $([m]_3, [n]_5)$ , jotka voidaan kirjoittaa oikein taulukon muotoon. (Jätetään jälleen taulukosta pois hakasulut alkoiden ympäriltä.)

$\mathbb{Z}_3 \oplus \mathbb{Z}_5$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_5$	$(0_3, 0_5)$	$(1_3, 0_5)$	$(2_3, 0_5)$
$[1]_5$	$(0_3, 1_5)$	$(1_3, 1_5)$	$(2_3, 1_5)$
$[2]_5$	$(0_3, 2_5)$	$(1_3, 2_5)$	$(2_3, 2_5)$
$[3]_5$	$(0_3, 3_5)$	$(1_3, 3_5)$	$(2_3, 3_5)$
$[4]_5$	$(0_3, 4_5)$	$(1_3, 4_5)$	$(2_3, 4_5)$

Kun verrataan saatua taulukkoa esimerkin 5.4 vastaavaan, huomataan, että aikaisemman taulukon lukua  $[k]_{15}$  vastaa tässä taulukossa aina sellainen pari  $([m]_3, [n]_5)$ , jolle pätee  $[m \cdot 5 + n \cdot 3]_{15} = [k]_{15}$ . Ryhmän  $\mathbb{Z}_{15}$  virittää alkio  $[1]_{15}$ , sillä kaikki ryhmän alkiot saadaan sen monikertoina. Taulukkoesityksestä päätellen tätä alkioita vastaa pari  $([2]_3, [2]_5)$ , ja jos lasketaan kyseisen parin monikerrat summaryhmässä  $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ , saadaan

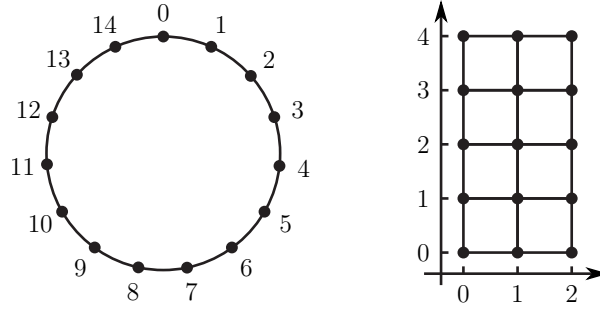
$$\begin{aligned} 2 \cdot (2_3, 2_5) &= (4_3, 4_5) = (1_3, 4_5), \\ 3 \cdot (2_3, 2_5) &= (6_3, 6_5) = (0_3, 1_5), \\ 4 \cdot (2_3, 2_5) &= (8_3, 8_5) = (2_3, 3_5), \\ 5 \cdot (2_3, 2_5) &= (10_3, 10_5) = (1_3, 0_5) \\ &\text{jne.} \end{aligned}$$

Laskemalla kaikki monikerrat huomataan, että pari  $([2]_3, [2]_5)$  virittää summaryhmän  $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ . Näin voidaan lopulta todeta, että ryhmät  $\mathbb{Z}_{15}$  ja  $\mathbb{Z}_3 \oplus \mathbb{Z}_5$  ovat isomorfiset, sillä ne ovat samankokoiset ja molemmat sykliisiä.

Kuvassa 17 on piirretty syklinen ryhmä  $\mathbb{Z}_{15}$  kahdella tavalla: yhtenä pitkänä syklinä ja kahden ryhmän tulona.

**Esimerkki 5.8.** Muodostetaan ryhmien  $A_n$  ja  $(\{1, -1\}, \cdot)$  ulkoinen suora tulo. Tulo koostuu pareista  $(\sigma, k)$ , missä  $\sigma$  on joku parillinen permutaatio ja  $k = \pm 1$ . Merkitään tällaista paria yksinkertaisesti  $\sigma$ , jos  $k = 1$ , ja  $-\sigma$ , jos  $k = -1$ . Tuloryhmän koko on  $2 \cdot |A_n| = |S_n|$ , ja houkutus olisi samastaa se symmetrisen ryhmän kanssa niin, että miinusmerkkiset alkiot vastaisivat parittomia permutaatioita. Pätehän myös tuloryhmässä

$$(-\sigma) \cdot (-\tau) = (\sigma, -1) \cdot (\tau, -1) = (\sigma \circ \tau, 1) = \sigma\tau,$$



Kuva 17: Kaksi tapaa hahmottaa 15 alkion syklinen ryhmä.

eli kahden ”negatiivisen” permutaation tulo on positiivinen. Tällainen samastus ei kuitenkaan onnistu, sillä esimerkiksi ryhmän  $S_3$  kaikki parittomat permutaatiot ovat vaihtoja, joten niiden toinen potenssi on identtinen kuvaus, mutta  $-(123)^2 = (132)$ . Yleisesti voidaan osoittaa, että ryhmät  $A_n \times (\{1, -1\}, \cdot)$  ja  $S_n$  eivät ole isomorfisia muuten kuin tapauksessa  $n = 2$ .

Jos  $H_1$  ja  $H_2$  ovat ryhmien  $G_1$  ja  $G_2$  aliryhmiä, niiden ulkoinen suora tulo on ryhmä, joka sisältyy ryhmään  $G_1 \times G_2$ . Se on siis kyseisen ryhmän aliryhmä. Osoitetaan seuraavassa lemmassa, että kahden normaalin aliryhmän tulo on myös normaali koko ryhmien tulossa.

**Lemma 5.9.** *Jos  $H_1$  ja  $H_2$  ovat ryhmien  $G_1$  ja  $G_2$  normaaleja aliryhmiä, niin ryhmä  $(H_1 \times H_2)_u$  on normaali ryhmässä  $(G_1 \times G_2)_u$ .*

*Todistus.* Olkoot  $(h_1, h_2) \in H_1 \times H_2$  ja  $(g_1, g_2) \in G_1 \times G_2$ . Tällöin pätee

$$(g_1, g_2)(h_1, h_2)(g_1, g_2)^{-1} = (g_1 h_1 g_1^{-1}, g_2 h_2 g_2^{-1}).$$

Lisäksi, koska  $H_1$  ja  $H_2$  ovat normaaleja, konjugaateille täytyy päteä  $g_1 h_1 g_1^{-1} \in H_1$  ja  $g_2 h_2 g_2^{-1} \in H_2$ . Siispä  $(g_1, g_2)(h_1, h_2) \in H_1 \times H_2$ , joten  $H_1 \times H_2$  on normaali.  $\square$

Aliryhmien sisäinen tulo poikkeaa ulkoisesta tulosta oikeastaan vain teknisiltä yksityiskohdiltaan. Seuraava lause osoittaa, että nämä käsitteet voidaan samastaa.

**Lause 5.10.** *Olkoot  $G_1$  ja  $G_2$  ryhmiä.*

- On olemassa aliryhmät  $\tilde{G}_1, \tilde{G}_2 \leq (G_1 \times G_2)_u$ , joille pätee  $\tilde{G}_1 \cong G_1$ ,  $\tilde{G}_2 \cong G_2$  ja  $(\tilde{G}_1 \times \tilde{G}_2)_s = (G_1 \times G_2)_u$ .*
- Jos  $H$  ja  $K$  ovat ryhmän  $G$  aliryhmiä, jotka muodostavat sisäisen suoran tulon, niin  $(H \times K)_s \cong (H \times K)_u$ .*

Jos ryhmä  $G$  on joidenkin aliryhmiensä  $H$  ja  $K$  sisäinen suora tulo, sitä voidaan lauseen nojalla ajatella myös ulkoisena tuloryhmänä  $H \times K$ , jonka alkiot ovat pareja  $(h, k)$ . Tällainen pari samastetaan siinä tapauksessa ryhmän  $G$  alkioon  $hk$ . Toisaalta, jos  $G_1$  ja  $G_2$  ovat eri ryhmiä, voidaan niiden ulkoisen suoran tulon alkioita  $(g_1, g_2)$  toisinaan merkitä yksinkertaisemmin  $g_1 g_2$ .

*Lauseen 5.10 todistus.* Todistetaan aluksi ensimmäinen väite. Olkoot siis  $G_1$  ja  $G_2$  jotkin kaksi ryhmää, joiden neutraalialkiot ovat  $e_1$  ja  $e_2$ . Tarkastellaan tuloryhmän  $(G_1 \times G_2)_u$  aliryhmiä  $\tilde{G}_1 = (G_1 \times \{e_2\})_u$  ja  $\tilde{G}_2 = (\{e_1\} \times G_2)_u$ . Selvästikin  $\tilde{G}_1 \cong G_1$  ja  $\tilde{G}_2 \cong G_2$ . (Isomorfismit kuvaavat  $(g_1, e_2) \mapsto g_1$  ja  $(e_1, g_2) \mapsto g_2$ .) Lisäksi  $\tilde{G}_1 \cap \tilde{G}_2 = \{(e_1, e_2)\}$  ja kaikilla  $g_1 \in G_1$  ja  $g_2 \in G_2$  pätee

$$(g_1, e_2)(e_1, g_2) = (g_1, g_2) = (e_1, g_2)(g_1, e_2).$$

Aliryhmien  $\tilde{G}_1$  ja  $\tilde{G}_2$  tulo on siis suora, ja sitä voidaan merkitä  $(\tilde{G}_1 \times \tilde{G}_2)_s$ . Edelleen nähdään, että jos  $(g_1, g_2) \in (G_1 \times G_2)_u$ , niin  $(g_1, g_2) = (g_1, e_2)(e_1, g_2)$ , missä  $(g_1, e_2) \in \tilde{G}_1$  ja  $(e_1, g_2) \in \tilde{G}_2$ . Täten  $(\tilde{G}_1 \times \tilde{G}_2)_s = (G_1 \times G_2)_u$ .

Todistetaan sitten toinen väite. Olkoot  $H$  ja  $K$  ryhmän  $G$  aliryhmiä. Määritellään kuvaus  $\varphi: (H \times K)_u \rightarrow (H \times K)_s$  kaavalla  $\varphi(h, k) = hk$  ja osoitetaan, että se on isomorfismi. Ensinnäkin jokainen sisäisen suoran tulon alkio on muotoa  $hk$  joillakin  $h \in H$  ja  $k \in K$ . Nyt pätee  $\varphi(h, k) = hk$ , joten kuvaus  $\varphi$  on surjektio. Oletetaan sitten, että  $\varphi(h_1, k_1) = \varphi(h_2, k_2)$  joillain  $h_1, h_2 \in H$  ja  $k_1, k_2 \in K$ . Tällöin siis  $h_1 k_1 = h_2 k_2$  ryhmässä  $(H \times K)_s$ , ja koska lemmän 5.5 mukaan jokaisen sisäisen suoran tulon alkion esitys tällaisena tulona on yksikäsitteinen, täytyy olla  $h_1 = h_2$  ja  $k_1 = k_2$  ja edelleen  $(h_1, k_1) = (h_2, k_2)$ . Kuvaus  $\varphi$  on siis myös injektio. Homomorfisuus seuraa siitä, että yhtälökettju

$$\begin{aligned} \varphi((h_1, k_1)(h_2, k_2)) &= \varphi(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2 = h_1 k_1 h_2 k_2 \\ &= \varphi(h_1, k_1) \cdot \varphi(h_2, k_2) \end{aligned}$$

pätee kaikilla  $h_1, h_2 \in H$  ja  $k_1, k_2 \in K$ . Tässä käytettiin sisäisen suoran tulon tekijöiden vaihdannaisuutta.  $\square$

Suoran summan käsite esiintyy usein modulien ja vektoriavaruuksien yhteydessä, jotka ovat yhteenlaskun suhteen vaihdannaisia ryhmiä. Esimerkiksi taso  $\mathbf{R}^2$  on ulkoinen suora summa kahdesta ryhmästä  $(\mathbf{R}, +)$ , sillä sen alkiot ovat pareja  $(x, y)$ , ja yhteenlasku toimii komponenteittain:  $(x, y) + (z, w) = (x + z, y + w)$ . Toisaalta taso on myös  $x$ - ja  $y$ -akselin *sisäinen* suora summa, sillä jokainen tason vektori voidaan kirjoittaa eräiden muotoa  $\tilde{x} = (x, 0)$  ja  $\tilde{y} = (0, y)$  olevien vektorien summana. Molemmat esitystavat kuvaavat samaa rakennetta, ja niiden yhteys ilmenee kaavasta  $(x, y) = \tilde{x} + \tilde{y}$ .

**Esimerkki 5.11.** Osoitetaan, että jos  $n > 2$ , ryhmä  $A_n \times (\{1, -1\}, \cdot)$  ei ole isomorfinen ryhmän  $S_n$  kanssa. Jos näin nimittäin olisi, niin  $S_n$  olisi edellisen lauseen nojalla esitettävissä kahden aliryhmänsä  $B$  ja  $C$  suorana tulona. Nämä aliryhmät ovat molemmat normaaleja lemmän 5.5 perusteella, ja toinen niistä sisältää neutraalialkion lisäksi vain yhden alkion: olkoon esimerkiksi  $C = \{\text{id}, \sigma\}$ . Näytetään, että  $C$  ei voi olla normaali.

Koska  $\sigma^2 = \text{id}$ , koostuu  $\sigma$ :n sykliesitys kokonaan erillisistä vaihdoista. Olkoon yksi näistä vaihdoista  $(ab)$ . Kun  $n > 2$ , löydetään joukosta  $N_n$  jokin kolmaskin alkio  $c$ . Nyt konjugaatin  ${}^{(bc)}\sigma$  sykliesityksessä esiintyy vaihto  $(ac)$ , jota ei ollut  $\sigma$ :n sykliesityksessä. Näin ollen  $\sigma \neq {}^{(bc)}\sigma$ , joten  ${}^{(bc)}\sigma \notin C$ . Tästä seuraa, että  $C$  ei ole normaali.

Koska ryhmä  $S_n$  ei siis sisällä kaksialkioista normaalia aliryhmää, se ei voi olla isomorfinen suoran tulon  $A_n \times (\{1, -1\}, \cdot)$  kanssa.

## 5.2 Tuloryhmät Rubikin ryhmässä

Rubikin kuution rakenteesta johtuen mitkään lailliset permutaatiot eivät voi siirtää nurkkapalaa kiinnitettyä ruutua särmäpalaan tai päinvastoin. Siispä sellaiset siirrot, jotka koskevat vain nurkkaruutuja, ovat täysin riippumattomia särmäruutuja liikuttavista siirroista, jolloin on samantekevää, tekeekö pelkkiin nurkkaruutuihin vaikuttavan siirron ennen pelkkiin särmäruutuihin vaikuttavaa siirtoa vai toisinpäin. Tällaisten pelkästään yhdentyypisiin ruutuihin vaikuttavat siirtojen joukot muodostavat Rubikin ryhmässä sisäisen suoran tulon.

Tässä luvussa määritellään edellä mainittu Rubikin ryhmän sisäinen suora tulo sekä osoitetaan muutama tämän tuloryhmän ja Rubikin ryhmän väliseen suhteeseen liittyvä lause, joiden avulla voidaan myöhemmin ratkaista kaikki paikkojen ryhmän  $\mathbb{R}_p$  asemat. Tehtävän helpottamiseksi tarkastellaan myös Rubikin ryhmän ulkopuolisia ruutujen permutaatioryhmän aliryhmiä.

Merkitään kirjaimella  $N$  kaikkien nurkkapalojen ruutujen joukkoa ja kirjaimella  $S$  kaikkien särmäruutujen joukkoa. Olkoon edelleen  $S_N$  nurkkaruutujen permutaatioiden ryhmä, ja  $S_S$  vastaavasti särmäruutujen permutaatioiden ryhmä. Jos kaikki ruudut numeroidaan luvuilla  $1, \dots, 48$ , näiden permutaatioryhmien voidaan ajatella olevan ryhmän  $S_{48}$  aliryhmiä.

Edellä mainittujen ryhmien käsittelyä helpottaa, kun otetaan käyttöön *kantajan* käsite. Jos permutaatio  $\sigma$  toimii perusjoukossa  $X$ , sen kantaja on

$$\text{supp}(\sigma) = \{x \in X \mid \sigma(x) \neq x\}.$$

Permutaation kantaja on siis niiden alkioden joukko, joihin permutaatio vaikuttaa epätriviaalisti. Esimerkiksi permutaation  $(156)(28)$  kantaja ryhmässä  $S_9$  on  $\{1, 2, 5, 6, 8\}$ . Permutaation kantajalle pätee muun muassa seuraavat ominaisuudet:

- 1)  $\sigma(x) \in \text{supp}(\sigma)$ , jos ja vain jos  $x \in \text{supp}(\sigma)$
- 2)  $\text{supp}(\sigma) = \text{supp}(\sigma^{-1})$
- 3)  $\text{supp}(\sigma \circ \tau) \subset \text{supp}(\sigma) \cup \text{supp}(\tau)$ .

Näiden ominaisuuksien todistaminen on helppo harjoitustehtävä.

Nyt voidaan määritellä ryhmät  $S_N$  ja  $S_S$  kantajan käsitteen avulla seuraavasti:

$$S_N = \{\sigma \in S_{48} \mid \text{supp}(\sigma) \subset N\} \quad \text{ja} \quad S_S = \{\sigma \in S_{48} \mid \text{supp}(\sigma) \subset S\}.$$

Koska mikään ruutu ei ole kiinni sekä nurkka- että särmäpalassa, joukot  $N$  ja  $S$  ovat erillisiä. Tästä seuraa, että nurkka- ja särmäpaloja permutoivat aliryhmät  $S_N$  ja  $S_S$  muodostavat suoran tulon ryhmässä  $S_{48}$ . Tämä todistetaan seuraavassa lauseessa hieman yleisemmässä muodossa.

**Lause 5.12.** *Olko  $G$  ja  $H$  joukon  $X$  symmetrisen ryhmän  $S_X$  aliryhmiä. Oletetaan, että joillain joukoilla  $A, B \subset X$  pätee  $A \cap B = \emptyset$ ,  $\text{supp}(\sigma) \subset A$  kaikilla  $\sigma \in G$  ja  $\text{supp}(\sigma) \subset B$  kaikilla  $\sigma \in H$ . Tällöin  $G$  ja  $H$  muodostavat suoran tulon ryhmässä  $S_X$ .*

*Todistus.* Ensimmäkin huomataan, että jos  $\sigma$  kuuluu molempiin ryhmiin  $G$  ja  $H$ , täytyy päteä  $\text{supp}(\sigma) \subset A \cap B = \emptyset$ , eli  $\sigma(x) = x$  kaikilla alkioilla  $x \in X$ . Täten  $\sigma = \text{id}$ .

Olkoot sitten  $\sigma \in G$  ja  $\tau \in H$ . Jos  $x \in \text{supp}(\sigma)$ , permutaation kantajan ominaisuuksien perusteella pätee  $\sigma(x) \in \text{supp}(\sigma)$ . Koska  $\text{supp}(\tau) \cap \text{supp}(\sigma) = \emptyset$ , nähdään että  $\tau(x) = x$  ja myöskin  $\tau\sigma(x) = \sigma(x)$ . Täten

$$\tau\sigma(x) = \sigma(x) = \sigma\tau(x).$$

Jos taas  $x \in \text{supp}(\tau)$ , niin  $\tau(x) \in \text{supp}(\tau)$ , ja samoin kuin edellä saadaan

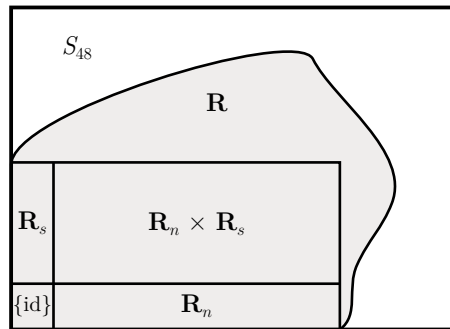
$$\sigma\tau(x) = \tau(x) = \tau\sigma(x).$$

Lopulta jos  $x \notin \text{supp}(\sigma) \cup \text{supp}(\tau)$ , niin  $\sigma(x) = \tau(x) = x$ , joten  $\sigma\tau(x) = \tau\sigma(x)$ . Näin on osoitettu, että  $\sigma\tau = \tau\sigma$ , eli aliryhmät  $G$  ja  $H$  ovat keskenään vaihdannaisia. Ne muodostavat siis suoran tulon.  $\square$

Ryhmät  $S_N$  ja  $S_S$  muodostavat suoran tulon kaikkien ruutujen permutaatioryhmässä  $S_{48}$ . Kaikki näiden ryhmien alkiot eivät kuitenkaan ole laillisia siirtoja. Määritellään siksi vielä erikseen edellä käsitellyjen ryhmien Rubikin ryhmään sisältyvät osat.

**Määritelmä 5.13.** Leikkausjoukkoa  $\mathbb{R}_n = \mathbb{R} \cap S_N$  kutsutaan Rubikin *nurkkaryhmäksi* ja leikkausjoukkoa  $\mathbb{R}_s = \mathbb{R} \cap S_S$  puolestaan Rubikin *särmäryhmäksi*.

Rubikin nurkkaryhmä sisältää sellaiset lailliset siirrot, jotka liikuttavat vain nurkka-ruutuja, ja särmäryhmä puolestaan on niiden laillisten siirtojen joukko, jotka liikuttavat vain särmäruutuja. Koska nämä joukot on määritelty kahden ryhmän leikkauksina, ne ovat itsekin ryhmiä ja siten Rubikin ryhmän aliryhmiä. Edelleen ryhmät  $\mathbb{R}_n$  ja  $\mathbb{R}_s$  muodostavat Rubikin ryhmän sisäisen suoran tulon, sillä niiden kantajat ovat erilliset (kantajat sisältyvät edelleen joukkoihin  $N$  ja  $S$ ). Tuloryhmään  $\mathbb{R}_n \times \mathbb{R}_s$  kuuluvat siirrot koostuvat nurkkiin ja särmiin vaikuttavista osista, joita voidaan käsitellä toisistaan riippumatta. Rubikin ryhmässä on kuitenkin myös sellaisia siirtoja, jotka eivät kuulu kyseiseen tuloryhmään. Kuvassa 18 on esitetty Venn-diagrammina Rubikin ryhmän ja tuloryhmän  $\mathbb{R}_n \times \mathbb{R}_s$  suhde.



Kuva 18: Tuloryhmän  $\mathbb{R}_n \times \mathbb{R}_s$  asema Rubikin ryhmässä.

Jako nurkka- ja särmäryhmiin heijastuu myös asento- ja paikkaryhmiin. Asentoryhmää koskeva tulos voidaan jälleen antaa yleisessä muodossa.



**Lause 5.14.** Jos  $H \leq G$  ja  $N \trianglelefteq G$ , niin  $H \cap N \trianglelefteq H$ .

*Todistus.* Kahden aliryhmän leikkaus on aliryhmä, joka sisältyy kumpaankin leikkaavaan aliryhmään. Se on siis erityisesti niiden molempien aliryhmä. Lisäksi, jos  $n \in H \cap N$  ja  $h \in H$ , niin  $h_n \in N$ , koska  $N$  on normaali  $G$ :ssä, ja  $h_n \in H$ , koska  $n \in H$ . Täten  $H \cap N$  on normaali aliryhmä  $H$ :ssa.  $\square$

Koska asentoryhmä  $\mathbb{R}_a$  on Rubikin ryhmän normaali aliryhmä, ovat leikkausryhmät

$$\mathbb{R}_{na} = \mathbb{R}_n \cap \mathbb{R}_a \quad \text{ja} \quad \mathbb{R}_{sa} = \mathbb{R}_s \cap \mathbb{R}_a$$

edellisen lauseen nojalla normaaleja vastaavissa ryhmissä  $\mathbb{R}_n$  ja  $\mathbb{R}_s$ . Näin ollen voidaan muodostaa tekijäryhmät

$$\mathbb{R}_{np} = \mathbb{R}_n / \mathbb{R}_{na} \quad \text{ja} \quad \mathbb{R}_{sp} = \mathbb{R}_s / \mathbb{R}_{sa}.$$

Näiden tekijäryhmien tulkinta on se, että  $\mathbb{R}_{np}$ :n alkiot vaihtavat vain *nurkkapalojen paikkoja* ja  $\mathbb{R}_{sp}$ :n alkiot vain *särmäpalojen paikkoja*, niiden asennoista välittämättä.

Näytetään vielä lopuksi, että tekijäryhmät  $\mathbb{R}_{np}$  ja  $\mathbb{R}_{sp}$  voidaan upottaa luonnollisella tavalla Rubikin paikkaryhmään, jossa ne muodostavat suoran tulon. Merkitään tässä yhteydessä eri aliryhmiin liittyviä sivuluokkia seuraavasti:

$$[\sigma]_n = \sigma \mathbb{R}_{na}, \quad [\tau]_s = \tau \mathbb{R}_{sa} \quad \text{ja} \quad [\rho] = \rho \mathbb{R}_a.$$

Tässä tietysti  $\sigma \in \mathbb{R}_n$ ,  $\tau \in \mathbb{R}_s$  ja  $\rho \in \mathbb{R}$ .

**Lause 5.15.** a) *Tekijäryhmät  $\mathbb{R}_{np}$  ja  $\mathbb{R}_{sp}$  ovat isomorfisia joidenkin Rubikin paikkaryhmän  $\mathbb{R}_p$  aliryhmien kanssa. Isomorfismeiksi voidaan lisäksi valita kuvaukset  $\varphi_1$  ja  $\varphi_2$ , joille pätee  $\varphi_1: [\sigma]_n \mapsto [\sigma]$  kaikilla  $\sigma \in \mathbb{R}_n$  ja  $\varphi_2: [\tau]_s \mapsto [\tau]$  kaikilla  $\tau \in \mathbb{R}_s$ .*

b) *Ryhmien  $\mathbb{R}_{np}$  ja  $\mathbb{R}_{sp}$  kuvat a)-kohdan isomorfismeissa muodostavat suoran tulon ryhmässä  $\mathbb{R}_p$ .*

Lauseen a)-kohdan merkitys on seuraava. Ajatellaan esimerkiksi nurkkaryhmään kuuluvia permutaatioita välittämättä palojen asennoista. Tämä on tietysti sama asia kuin jos ajateltaisiin sellaisia paikkaryhmän siirtoja, jotka vaikuttavat vain nurkkapaloihin. Kyseessä on kuitenkin eri tekijäryhmät, sillä ne on muodostettu eri normaalien aliryhmien avulla. Teknisesti ottaen aliryhmän  $\mathbb{R}_{na}$  sivuluokat ovat suppeampia kuin aliryhmän  $\mathbb{R}_a$ . Nyt todistettava lause antaa tekijäryhmien välille luonnollisen isomorfismin.

*Lauseen 5.15 todistus.* a) Tarkastellaan ryhmää  $\mathbb{R}_{np}$ . Toisen ryhmän tapauksessa todistus on aivan samanlainen. Koska ollaan määrittelemässä kuvausta tekijäryhmältä johonkin toiseen ryhmään, on aluksi tarkistettava, että kuvauksen arvot eivät riipu sivuluokan edustajan valinnasta.

Olkoon  $\sigma \in \mathbb{R}_n$ . Jos nyt  $[\sigma]_n = [\sigma']_n$  jollain  $\sigma' \in \mathbb{R}_n$ , niin  $\sigma^{-1}\sigma' \in \mathbb{R}_{na}$ . Erityisesti tällöin pätee  $\sigma^{-1}\sigma' \in \mathbb{R}_a$  eli  $[\sigma] = [\sigma']$ . Siispä jokaista sivuluokkaa  $[\sigma]_n \in \mathbb{R}_{np}$  vastaa yksikäsitteinen sivuluokka  $[\sigma] \in \mathbb{R}_p$ , joten voidaan määritellä kuvaus  $\varphi: \mathbb{R}_{np} \rightarrow \mathbb{R}_p$ , jolle

pätee  $\varphi([\sigma]_n) = [\sigma]$ . Tällainen kuvaus on lisäksi homomorfismi, sillä kaikilla  $\sigma_1, \sigma_2 \in \mathbb{R}_n$  pätee

$$\varphi([\sigma_1]_n) \cdot \varphi([\sigma_2]_n) = [\sigma_1] \cdot [\sigma_2] = [\sigma_1\sigma_2] = \varphi([\sigma_1\sigma_2]_n) = \varphi([\sigma_1]_n \cdot [\sigma_2]_n).$$

Osoitetaan, että kuvaus  $\varphi$  on injektio. Oletetaan sitä varten, että  $[\sigma_1] = [\sigma_2]$  joillain  $\sigma_1, \sigma_2 \in \mathbb{R}_n$ . Tällöin pätee  $\sigma_1^{-1}\sigma_2 \in \mathbb{R}_a$ . Toisaalta pätee myös  $\sigma_1^{-1}\sigma_2 \in \mathbb{R}_n$ , koska  $\mathbb{R}_n$  on ryhmä. Siispä  $\sigma_1^{-1}\sigma_2 \in \mathbb{R}_{na}$  eli  $[\sigma_1]_n = [\sigma_2]_n$ . Kuvaus  $\varphi$  on siis injektiivinen homomorfismi ryhmälle  $\mathbb{R}_p$ , joten lähtöryhmä  $\mathbb{R}_{np}$  on isomorfinen kuvaryhmän  $\text{Im}(\varphi) \leq \mathbb{R}_p$  kanssa.

b) Osoitetaan, että kuvaryhmät

$$H = \{[\sigma] \in \mathbb{R}_p \mid \sigma \in \mathbb{R}_n\} \quad \text{ja} \quad K = \{[\tau] \in \mathbb{R}_p \mid \tau \in \mathbb{R}_s\}$$

muodostavat suoran tulon paikkaryhmässä  $\mathbb{R}_p$ . Olkoot  $\sigma \in \mathbb{R}_n$  ja  $\tau \in \mathbb{R}_s$ . Koska  $\mathbb{R}_n$  ja  $\mathbb{R}_s$  muodostavat suoran tulon, pätee  $\sigma\tau = \tau\sigma$ . Niinpä

$$[\sigma] \cdot [\tau] = [\sigma\tau] = [\tau\sigma] = [\tau] \cdot [\sigma].$$

Kuvaryhmät  $H$  ja  $K$  ovat siis keskenään vaihdannaisia.

Oletetaan sitten, että  $[\pi] \in H \cap K$  jollain  $\mathbb{R}$ . Tällöin  $[\pi] = [\sigma]$  joillain  $\sigma \in \mathbb{R}_n$  ja  $[\pi] = [\tau]$  jollain  $\tau \in \mathbb{R}_s$ . Pyritään osoittamaan, että  $[\pi] = [\text{id}]$ . Tällöin kuvaryhmien leikkaus on triviaali.

(Huomaa, että tässä ei voida olettaa alkion  $\pi$  kuuluvan molempiin ryhmiin  $\mathbb{R}_n$  ja  $\mathbb{R}_s$ . Voisi nimittäin olla, että joukoilla  $\mathbb{R}_n \cap [\pi]$  ja  $\mathbb{R}_s \cap [\pi]$  ei olisi yhtään yhteisiä alkioita.)

Koska  $[\sigma] = [\tau]$ , nähdään että

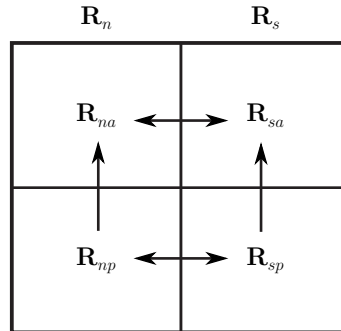
$$\sigma = \tau\rho \quad \text{jollain } \rho \in \mathbb{R}_a.$$

Tämän yhtälön vasemmalla puolella oleva permutaatio kuuluu ryhmään  $\mathbb{R}_n$ , joten se ei liikuta särmäpaloja paikoiltaan. Toisaalta oikealla puolella oleva permutaatio on tulo särmäryhmän ja asentoryhmän siirroista, joten se ei liikuta nurkkapaloja paikoiltaan. Koska vasen ja oikea puoli ovat samat, kumpikaan permutaatio ei liikuta mitään paloja paikoiltaan. Täten  $\sigma \in \mathbb{R}_a$  eli  $[\sigma] = [\pi] = [\text{id}]$ .  $\square$

Lauseen a)-kohta pätee ryhmissä yleisesti, kun ryhmät on määritelty lausetta 5.14 vastaavalla tavalla: tällöin ryhmää  $\mathbb{R}_{np}$  vastaa ryhmä  $H/(H \cap N)$  jne. Tällaiset aliryhmän tekijäryhmät voidaan siis aina upottaa laajempaan tekijäryhmään  $G/N$ . Sen sijaan b)-kohdan tulos ei päde yleisesti edes permutaatioryhmillä, vaikka aliryhmien kantajat olisivatkin erilliset. Upotetut tekijäryhmät saattavat nimittäin yleisessä tapauksessa leikata toisiaan epätriviaalisti. Rubikin kuution rakenne kuitenkin estää tämän.

Kuvassa 19 on kaavamaisesti esitetty tuloryhmän  $\mathbb{R}_n \times \mathbb{R}_s$  rakenne. Kullakin vaakarivillä vierekkäiset ryhmät muodostavat suoran tulon. Niin kuin aiemmin on mainittu, jos annettu Rubikin kuution asema sisältyy tuloryhmään  $\mathbb{R}_n \times \mathbb{R}_s$ , nurkkaruudut voidaan ratkaista särmäruuduista riippumatta. Asema on nimittäin tällöin tulo kahdesta permutaatiosta, joista toinen vaikuttaa pelkkiin nurkkaruutuihin ja toinen pelkkiin särmäruutuihin. Voidaan esimerkiksi ratkaista ensin nurkkaruudut (vasen sarake), sitten

särmäruudut (oikea sarake). Edelleen sekä nurkka- että särmäpalojen kohdalla voidaan noudattaa aikaisempaa jakoa, jossa ratkaistaan ensin palojen paikat, sitten niiden asennot. Ensin siis käytettäisiin jompaa kumpaa kuvion alarivin ryhmää (paikkaryhmä), sitten sen yläpuolella oleva ryhmää.



Kuva 19: Tuloryhmän  $R_n \times R_s$  rakenne.

Toisaalta mikä tahansa asema voidaan ratkaista myös ratkaisemalla ensin kaikkien palojen paikat, sitten niiden asennot. Lauseen 5.15 a)-kohdan perusteella paikkoja muuttavat nurkkaryhmän permutaatiot ovat sama asia kuin nurkkiin kohdistuvat paikkaryhmän permutaatiot, ja sama pätee särmäryhmälle. Lisäksi saman lauseen b)-kohdan mukaan nurkka- ja särmäpalojen paikkaryhmät muodostavat suoran tulon koko paikkaryhmässä, joten ne voidaan myös ratkaista toisistaan täysin riippumatta. Jokainen tuloryhmän  $R_n \times R_s$  asema voidaan siis ratkaista esimerkiksi siirtämällä ensin nurkkapalat paikoilleen, ratkaisemalla sitten särmien paikat ja asennot, ja asettamalla lopuksi nurkat oikeisiin asentoihin. Muutkin yhdistelmät ovat mahdollisia; ainoa rajoitus on, että ennen kutakin ylärivin ryhmää on ratkaistava sen alapuolella oleva ryhmä.

Edellä esitetyt ratkaisuvaihtoehdot toimivat kuitenkin vain tuloryhmässä  $R_n \times R_s$ , joka ei sisällä kaikkia mahdollisia asemia. Luvussa 5.4 selvitetään, miten yleisestä tapauksesta voidaan aina siirtyä tuloryhmään.

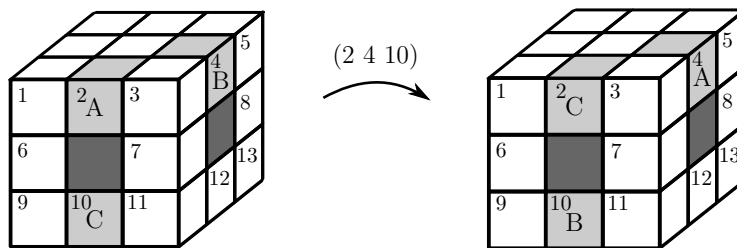
### 5.3 Algoritmi 2: särmäpalojen 3-sykli

Särmäpalojen siirtelyä varten on tunnettava jokin särmäpalojen 3-sykli. Jäljempänä tullaan näkemään, että tämä 3-sykli voidaan konjugoida mille tahansa toiselle särmäpalojen 3-syklille, ja tämä johtaa lopulta koko paikkaryhmän ratkaisuun.

Valittu 3-sykli on esitetty kuvassa 20. Kun palojen paikat numeroidaan kuvan mukaisesti, sykli on muotoa (2 4 10). Itse siirtosarja löytyy perussiirtojen avulla esitettynä liitteestä A.2.

### 5.4 Rubikin paikkaryhmän ratkaiseminen

Tässä luvussa tarkistetaan ensin, että kaikki särmäpalojen 3-syklit ovat mahdollisia siirtoja. Sen jälkeen tutkitaan Rubikin paikkaryhmän parillisuusominaisuuksia, joita hyväksikäyttäen saadaan lopulta nurkka- ja reunapalat oikeille paikoilleen.

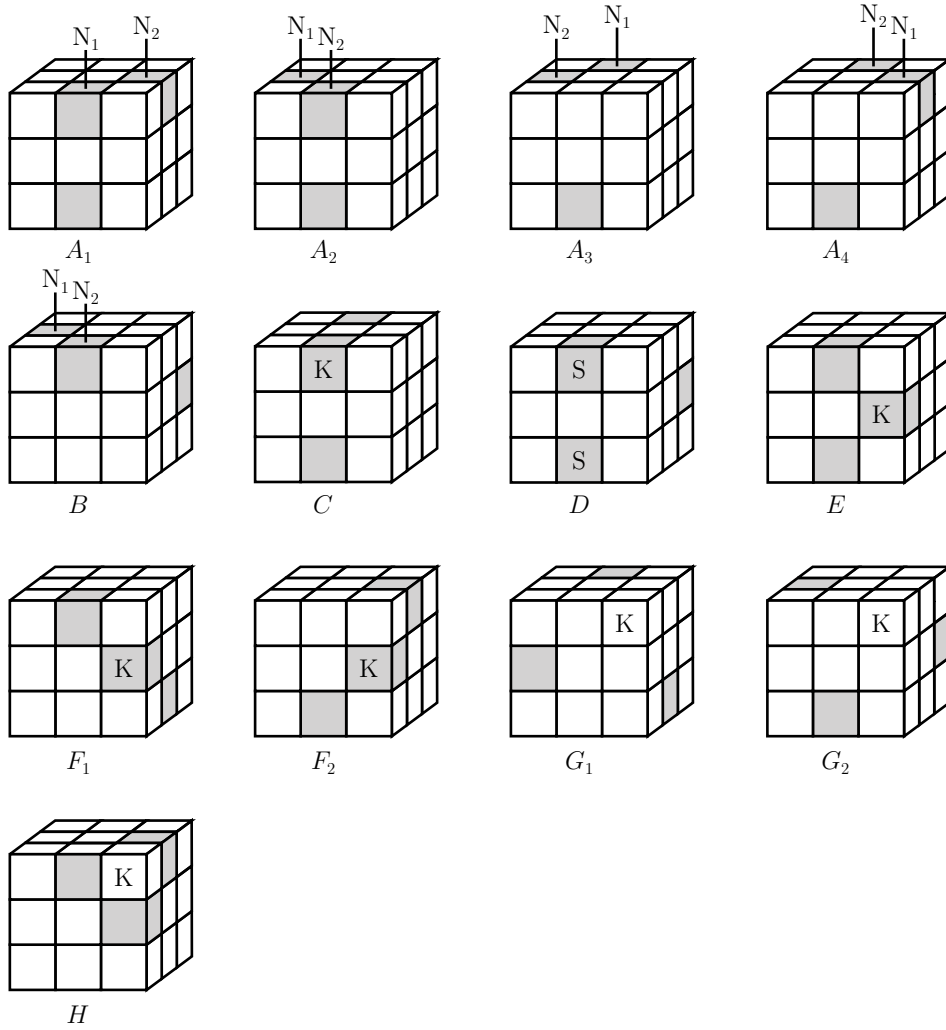


Kuva 20: Särmäpalojen 3-sykli.

Käydään ensin läpi kaikki kolmen särmäpalan kombinaatiot samalla tavoin kuin luvussa 4.3 tehtiin nurkkapaloille. Tällä kertaa kombinaatioita tulee yhteensä  $\binom{12}{3} = 220$  kappaletta, ja ne voidaan jakaa 13 joukkoon kuvan 21 mukaisesti. Kunkin joukon sisällä kombinaatiot saadaan kuvan mukaiseen asentoon koko kuutiota kiertämällä.

Lasketaan kunkin edellä mainituista joukoista sisältämien kombinaatioiden lukumäärä, jotta varmistutaan siitä, että muita kombinaatioita ei ole.

- $A_1$  Kirjaimilla  $N_1$  ja  $N_2$  merkityt palat voivat sijaita millä tahansa kuution kuudesta sivusta neljässä eri nurkassa. Kolmas pala on aina palaa  $N_1$  vastapäätä. Joukossa on siis  $6 \cdot 4 = 24$  kombinaatiota.
- $A_2, A_3, A_4$  Nämä kombinaatiot saadaan joukon  $A_1$  kombinaatioista yksikäsitteisellä tavalla, nimittäin kiertämällä ylätahkoa kussakin tapauksessa tietyn verran. Kussakin joukossa on siis 24 kombinaatiota.
- $B$  Kirjaimilla  $N_1$  ja  $N_2$  merkityt palat voivat sijaita millä tahansa kuution kuudesta sivusta neljässä eri nurkassa. Kolmas pala sijaitsee vastakkaisen nurkkasärmän keskellä. Kombinaatioita on  $6 \cdot 4 = 24$  kappaletta.
- $C$  Kaikki kolme palaa sijaitsevat samalla keskitahkolla. Keskitahkoja on yhteensä kolme, ja kirjaimella  $K$  merkitty pala voi olla mikä tahansa keskitahkon neljästä reunapalasta. Vaihtoehtoja on siis yhteensä  $3 \cdot 4 = 12$  kappaletta.
- $D$  Kirjaimella  $S$  merkityt palat voivat sijaita vierekkäin millä tahansa kuution kolmesta keskitahkosta. Vaihtoehtoja niiden sijainnille saadaan yhteensä 12. Kolmas pala voidaan sen jälkeen valita vastakkaisen sivutahkon jommasta kummasta reunasta. Nämä vaihtoehdot saadaan toisistaan kääntämällä kuutio ylösalaisin. Kombinaatioita on siis 24.
- $E$  Kaikki palat sijaitsevat samalla sivutahkolla. Sivutahkoja on kuusi, ja kirjaimella  $K$  merkitty pala voidaan valita kullakin tahkolla 4 palan joukosta. Kombinaatioita on siis 24.
- $F_1, F_2$  Näissä tapauksissa kirjaimella  $K$  merkitty pala voidaan valita kunkin särmän keskeltä, ja kaikki kolme palaa määräytyvät sen mukaan. Molemmissa joukoissa on siis 12 kombinaatiota.



Kuva 21: Kolmen särmäpalan kombinaatiot.

$G_1, G_2$  Kirjaimella K merkitty pala voidaan valita vapaasti kaikkien nurkkapalojen joukosta, ja muut palat määräytyvät sen mukaisesti. Vastakkaisia nurkkia vastaa kuitenkin sama kombinaatio, joten näissä joukoissa on kummassakin  $8/2 = 4$  kombinaatiota.

$H$  Kirjaimella K merkitty pala voidaan valita kustakin nurkasta, ja palat sijaitsevat sen vierellä. Kombinaatioita on 8 kappaletta.

Yhteensä luetelluissa joukoissa on  $7 \cdot 24 + 3 \cdot 12 + 8 + 2 \cdot 4 = 220$  kombinaatiota.

**Lause 5.16.** Mikä tahansa ryhmän  $\mathbb{R}_p$  3-sykli, joka liikuttaa vain särmäpaloja, on mahdollinen siirto.

*Todistus.* Kuten luvun 4.3 vastaavassa todistuksessa, jossa tarkasteltiin nurkkapalojen 3-syklejä, tässäkin riittää todistaa, että jokaista kuvassa 21 lueteltua kombinaatioiden joukkoa kohti löytyy siirto, jolla palat saadaan kirjaimella  $A_1$  merkittyyn perusasemaan. Edelleen kunkin kombinaatiojoukon sisällä kombinaatio saadaan kuvan mukaiseen asemaan kuutiota kiertämällä, jonka jälkeen siirrot voidaan nimetä uudelleen niin, että katsojaan päin olevan tahkon kierroksi tulee  $F$ , ylätahkon kierroksi  $U$  jne.

Konjugoivan siirron käänteissiirto löytyy seuraavasti. Ensin saatetaan kuutiota kiertämällä kuutio johonkin kuvan 21 kolmestatoista asemasta, joista jokaisessa oletetaan sinisen sivun osoittavan ylöspäin ja keltaisen sivun katsojaan päin. Jos päädyttiin asemaan  $A_1$ , siirto on valmis. Muuten suoritetaan (uudelleen nimettyjä) perussiirtoja oikeisen taulukon mukaisesti riippuen siitä, mihin asemaan päädyttiin. (Siirrot suoritetaan oikealta vasemmalle.)

asema	siirto	asema	siirto
$A_2$	$U^{-1}$	$E$	$R$
$A_3$	$U^2$	$F_1$	$RD^{-1}$
$A_4$	$U$	$F_2$	$RU$
$B$	$U^{-1}D^{-1}R$	$G_1$	$UF^{-1}R^2$
$C$	$R^{-1}B^{-1}$	$G_2$	$R^{-1}U^{-1}$
$D$	$R^{-1}$	$H$	$RD^{-1}R^{-1}$

Kaikissa tapauksissa löytyy siirto, jonka käänteissiirrolla konjugoiminen tuottaa halutun 3-syklin.  $\square$

Osoitetaan seuraavaksi lemma, joka liittyy siirtojen parillisuuteen. Merkitään sitä varten kaikkien nurkkapalojen paikkojen permutaatioryhmää  $S_N^p$  ja samaten kaikkien reunalalojen paikkojen permutaatioryhmää  $S_S^p$ . Näitä ryhmiä voidaan ajatella symmetrisen ryhmän  $S_{20}$  (kaikkien palojen permutaatiot) aliryhminä. Ne muodostavat lisäksi suoran tulon ryhmässä  $S_{20}$ , sillä  $\text{supp}(\nu) \cap \text{supp}(\sigma) = \emptyset$  kaikilla  $\nu \in S_N^p$  ja  $\sigma \in S_S^p$ .

**Lemma 5.17.** *Jos  $\tau$  on Rubikin paikkaryhmän siirto, sille löytyy yksikäsitteinen esitys parina  $\tau = (\nu, \sigma)$ , missä  $\nu \in S_N^p$  ja  $\sigma \in S_S^p$ . Lisäksi pätee  $\text{sign}(\nu) = \text{sign}(\sigma)$ .*

*Todistus.* Koska  $\tau$  on paikkaryhmän siirto, se voidaan esittää paikkaryhmän perussiirtojen  $\tau_1, \dots, \tau_n$  tulona. Kaikkien palojen permutaatioiden ryhmässä  $S_{20}$  jokainen perussiirto  $\tau_i$  on puolestaan kahden erillisen 4-syklin tulo, joista toinen liikuttaa vain nurkkapaloja, toinen vain särmäpaloja. Merkitään näitä 4-syklejä  $\nu_i \in S_N^p$  ja  $\sigma_i \in S_S^p$ . Koska ryhmät  $S_N^p$  ja  $S_S^p$  muodostavat suoran tulon, voidaan kirjoittaa  $\tau_i = (\nu_i, \sigma_i)$  jokaisella  $i$ . Näin saadaan siirrolle  $\tau$  esitys

$$\tau = (\nu_1, \sigma_1) \cdots (\nu_n, \sigma_n) = (\nu_1 \nu_2 \cdots \nu_n, \sigma_1 \sigma_2 \cdots \sigma_n).$$

Merkitään nyt  $\nu = \nu_1 \cdots \nu_n$  ja  $\sigma = \sigma_1 \cdots \sigma_n$ . Koska kaikki siirrot  $\nu_i$  ja  $\sigma_i$  ovat 4-syklejä, pätee

$$\text{sign}(\nu) = (-1)^n = \text{sign}(\sigma). \quad \square$$

Jokainen Rubikin paikkaryhmän  $\mathbb{R}_p$  siirto voidaan kirjoittaa parina  $(\nu, \sigma) \in S_N^p \times S_S^p$ . Jos myös  $\nu$  ja  $\sigma$  kuuluvat ryhmään  $\mathbb{R}_p$ , niin  $(\nu, \sigma)$  on tuloryhmässä  $\tilde{\mathbb{R}}_{np} \times \tilde{\mathbb{R}}_{sp}$ , missä  $\tilde{\mathbb{R}}_{np}$  ja  $\tilde{\mathbb{R}}_{sp}$  ovat lauseen 5.15 antamat ryhmien  $\mathbb{R}_{np}$  ja  $\mathbb{R}_{sp}$  isomorfiset kuvat ryhmässä  $\mathbb{R}_p$ . Edellisen lemmän avulla saadaan nyt lause, joka mahdollistaa paikkaryhmän ratkaisemisen. Merkinnöissä samastetaan tästedes ryhmät  $\mathbb{R}_{np}$  ja  $\mathbb{R}_{ns}$  isomorfisten kuviensa kanssa.

**Lause 5.18.** *Oletetaan, että  $\tau = (\nu, \sigma) \in \mathbb{R}_p$ . Jos  $\text{sign}(\nu) = 1$  tai  $\text{sign}(\sigma) = 1$ , niin  $\nu$  ja  $\sigma$  kuuluvat paikkaryhmään  $\mathbb{R}_p$ . Lisäksi tuloryhmän  $\mathbb{R}_{np} \times \mathbb{R}_{sp}$  indeksille paikkaryhmän aliryhmänä pätee  $[\mathbb{R}_p : \mathbb{R}_{np} \times \mathbb{R}_{sp}] \leq 2$ .*

*Todistus.* Oletetaan, että  $\text{sign}(\nu) = 1$  tai  $\text{sign}(\sigma) = 1$ . Edellisen lemmän perusteella pätee tällöin  $\text{sign}(\nu) = \text{sign}(\sigma) = 1$ . Lauseissa 4.10 ja 5.16 on osoitettu, että kaikki nurkka- ja särmäpalojen 3-syklit ovat mahdollisia siirtoja, ja lauseen 3.12 mukaan jokainen parillinen permutaatio saadaan 3-sykliden yhdistelmänä. Täten  $\nu \in \mathbb{R}_p$ , ja sama pätee myös permutaatiolle  $\sigma$ .

Osoitetaan sitten, että  $[\mathbb{R}_p : \mathbb{R}_{np} \times \mathbb{R}_{sp}] \leq 2$ . Olkoon  $\pi = (\pi_1, \pi_2)$  jokin paikkaryhmän perussiirto. Oletetaan, että  $\tau = (\nu, \sigma) \in \mathbb{R}_p$  ei kuulu tuloryhmään  $\mathbb{R}_{np} \times \mathbb{R}_{sp}$ . Todistuksen alun perusteella joko  $\text{sign}(\nu) = -1$  tai  $\text{sign}(\sigma) = -1$ . Tällöin täytyy kuitenkin edellisen lemmän mukaan olla  $\text{sign}(\nu) = \text{sign}(\sigma) = -1$ , ja koska perussiirrolle toisaalta pätee  $\text{sign}(\pi_1) = \text{sign}(\pi_2) = -1$ , saadaan

$$\text{sign}(\pi_1^{-1}\nu) = 1 \quad \text{ja} \quad \text{sign}(\pi_2^{-1}\sigma) = 1.$$

Yllä osoitettiin, että tämän perusteella yhdistelmä  $\pi^{-1}\tau = (\pi_1^{-1}\nu, \pi_2^{-1}\sigma)$  kuuluu tuloryhmään  $\mathbb{R}_{np} \times \mathbb{R}_{sp}$ , joten  $\tau \in \pi(\mathbb{R}_{np} \times \mathbb{R}_{sp})$ . Koska mikä tahansa tuloryhmään kuuluvan permutaatio kuuluu yhteen tiettyyn tuloryhmän sivuluokkaan, sivuluokkia voi olla korkeintaan kaksi.  $\square$

Edellisen lauseen nojalla Rubikin kuution palat saadaan oikeille paikoilleen seuraavalla tavalla:

1. Selvitetään, onko ratkaistavassa asemassa nurkkapalojen (tai särmäpalojen) permutaatio parillinen. Jos ei ole, tehdään jokin perussiirto. Tämän jälkeen *sekä* nurkka- *että* särmäpalojen permutaatio on parillinen.
2. Ratkaistaan nurkat ja särmät erikseen aiemmin opittujen 3-sykliden ja niiden konjugaattien avulla.

## 5.5 Puolisuorat tulot

Kahden aliryhmän suorassa tulossa eri aliryhmien alkiot kommutoivat keskenään. Tällöin aliryhmät ovat toisistaan riippumattomia. Ehtoa voidaan kuitenkin lieventää, jos vain halutaan kahden aliryhmän tulon olevan ryhmä eikä riippumattomuudella ole niin väliä.

Tarkastellaan kahta aliryhmää  $N$  ja  $H$  jossain ryhmässä  $G$ . Tulojoukon alkiot ovat muotoa  $nh \in NH$ , ja kahden tällaisen alkion tulo on  $n_1h_1n_2h_2$ . Jotta tämä alkio kuuluisi

edelleen joukkoon  $NH$ , riittää että toinen aliryhmistä, vaikkapa  $N$ , on *normaali*. Tällöin nimittäin nähdään, että  $N$ :n vasemman sivuluokan alkio  $h_1n_2$  kuuluu myös vastaavaan oikeanpuoleiseen sivuluokkaan, joten  $h_1n_2 = n'h_1$  eräällä  $n' \in N$ . Näin ollen

$$n_1h_1 \cdot n_2h_2 = n_1n' \cdot h_1h_2 \in NH.$$

Tulojoukko on siis suljettu laskutoimituksen suhteen. Samalla tavoin nähdään myös, että käänteisalkiot ovat mukana tulojoukossa, sillä  $(nh)^{-1} = h^{-1}n^{-1} = n'h^{-1}$  eräällä  $n' \in N$ .

**Määritelmä 5.19.** Ryhmän  $G$  aliryhmät  $N$  ja  $H$  muodostavat *sisäisen puolisuoran tulon*, jos seuraavat ehdot pätevät:

- 1)  $N$  on normaali  $G$ :ssä
- 2)  $N \cap H = \{e\}$ , missä  $e$  on ryhmän  $G$  neutraalialkio.

Puolisuoraa tuloa merkitään  $NH = N \rtimes H$  tai  $HN = H \ltimes N$ .

**Esimerkki 5.20.** Alternoivalla ryhmällä  $A_4$  on normaali aliryhmä

$$N = \{\text{id}, (12)(34), (13)(24), (14)(23)\}.$$

Tarkastellaan tämän lisäksi 3-syklin virittämää aliryhmää  $H = \{\text{id}, (123), (132)\}$ , joka ei ole normaali (esim.  ${}^{(34)}(123) = (124) \notin A_4$ ). Näiden aliryhmien leikkauksessa on vain identtinen permutaatio, joten ne muodostavat puolisuoran tulon  $N \rtimes H$ . Kootaan kyseisen tulon alkiot taulukkoon.

$N \rtimes H$	id	(12)(34)	(13)(24)	(14)(23)
id	id	(12)(34)	(13)(24)	(14)(23)
(123)	(123)	(243)	(142)	(134)
(123)	(132)	(143)	(234)	(124)

Jokainen alternoivan ryhmän alkio esiintyy taulukossa täsmälleen kerran. Voidaan siis todeta, että  $N \rtimes H = A_4$  ja jokaisella  $A_4$ :n alkiolla on yksikäsitteinen esitys tulona  $n \circ h$ , missä  $n \in N$  ja  $h \in H$ .

Aivan kuten suoran tulon tapauksessa, myös puolisuorassa tulossa  $N \rtimes H$  alkioiden esitykset muodossa  $nh$  ovat yksikäsitteisiä. Tämä seuraa määritelmän kohdasta 2). Kahden alkion tulon esitys saadaan seuraavasta yhtälöstä, joka pätee kaikissa ryhmissä:

$$n_1h_1 \cdot n_2h_2 = n_1(h_1n_2h_1^{-1})h_1h_2 = n_1{}^{h_1}n_2 \cdot h_1h_2. \quad (5.1)$$

Puolisuoran tulon tapauksessa aliryhmä  $N$  on normaali, joten konjugaatti  ${}^{h_1}n_2$  kuuluu edelleen aliryhmään  $N$ .

Yllä oleva kaava kertoo, että ei-normaalien ryhmien  $H$  alkioita voidaan kertoa keskenään  $N$ :n alkioista riippumatta aivan kuten suorassa tulossa, mutta normaalien aliryhmien alkioita kerrottaessa on toista konjugoitava ensin  $H$ :n alkiolla. Kyseessä on siis eräänlainen puolittainen riippumattomuus.



Jos normaali aliryhmä on tulossa oikeanpuoleisena, kaava (5.1) tulee muotoon

$$h_1 n_1 \cdot h_2 n_2 = h_1 h_2 \cdot h_2^{-1} n_1 n_2.$$

Kaavan (5.1) avulla voidaan määrittellä myös kahden erilaisen ryhmän *ulkoinen* puolisuora tulo. Ongelmana on vain se, että alkion  $n$  konjugointi alkiolla  $h$  ei onnistu, jos  $n$  ja  $h$  ovat eri ryhmissä. Tällainen ulkoinen konjugointi voidaan kuitenkin määrittellä, kun ensin mietitään, minkälainen operaatio konjugointi itse asiassa on.

Konjugoinnissa jokaiseen ryhmän  $G$  alkioon  $g$  liitetään kuvaus  $x \mapsto {}^g x$ . Tämä kuvaus on ryhmän  $G$  sisäinen automorfismi eli bijektiivinen homomorfismi ryhmältä itselleen. Lisäksi konjugointi toteuttaa ns. *ryhmän toiminnan* ehdot: neutraaliakiota vastaa identtinen kuvaus  $x \mapsto x$ , ja alkioden tuloa vastaa yhdistetty kuvaus, nimittäin  ${}^{gh} x = {}^g ({}^h x)$ . Nämä ominaisuudet huomioiden voidaan määrittellä ryhmän konjugointi toisessa ryhmässä.

**Määritelmä 5.21.** Olkoot  $G$  ja  $H$  ryhmiä. Kuvausta  $g \mapsto \varphi_g$ , joka liittyy jokaiseen  $G$ :n alkioon  $g$  jonkin kuvauksen  $\varphi_g$  ryhmältä  $H$  itselleen, kutsutaan *konjugoivaksi toiminnaksi*, jos seuraavat ehdot täyttyvät:

- 1) kuvaus  $\varphi_g$  on isomorfismi (eli automorfismi) jokaisella  $g \in G$
- 2)  $\varphi_e$  on identtinen kuvaus, jos  $e$  on  $G$ :n neutraalialkio
- 3)  $\varphi_{g_1 g_2} = \varphi_{g_1} \circ \varphi_{g_2}$  kaikilla  $g_1, g_2 \in G$ .

Konjugoivan toiminnan käsitteen sekä kaavan (5.1) avulla voidaan määrittellä kahden mielivaltaisen ryhmän puolisuora tulo.

**Määritelmä 5.22.** Olkoot  $(N, \diamond)$  ja  $(G, *)$  ryhmiä. Oletetaan, että on määritelty jokin ryhmän  $G$  konjugoiva toiminta  $g \mapsto \varphi_g$  ryhmässä  $N$ . Ryhmien  $N$  ja  $G$  *ulkoinen puolisuora tulo*  $N \rtimes G$  muodostuu pareista  $(n, g)$ , missä  $n \in N$  ja  $g \in G$ . Laskutoimitus määritellään kaavalla

$$(n_1, g_1)(n_2, g_2) = (n_1 \diamond \varphi_{g_1}(n_2), g_1 * g_2).$$

Toisin päin merkityssä puolisuorassa tulossa  $G \rtimes N$  laskutoimitus on vastaavasti

$$(g_1, n_1)(g_2, n_2) = (g_1 * g_2, \varphi_{g_2}^{-1}(n_1) \diamond n_2).$$

Tuloa voidaan merkitä myös ulkoisuutta korostaen  $(N \rtimes G)_u$  tai  $(G \rtimes N)_u$ .

Ulkoisen suoran tulon rakenne riippuu valitusta konjugoivasta toiminnasta ja eri valinnat tuottavat erilaisen tulon. Toiminnaksi voidaan myös valita  $\varphi_g = \text{id}$  kaikilla  $g$ , jolloin puolisuorasta tulosta tulee suora tulo.

Toisin kuin suoran tulon tapauksessa, ulkoisesta puolisuorasta tulosta on vaikea äkkiseltään nähdä, että se todella on ryhmä. Todistetaan tämä seuraavaksi.

**Lause 5.23.** *Ryhmien  $(N, \diamond)$  ja  $(H, *)$  puolisuora tulo on ryhmä.*

*Todistus.* Puolisuora tulo on suljettu määritellyn laskutoimituksen suhteen, koska konjugaatti  $\varphi_{g_1}(n_2)$  on ryhmän  $N$  alkio ja siten tulo  $n_1 \diamond \varphi_{g_1}(n_2)$  kuuluu ryhmään  $N$ . Tarkistetaan ryhmän aksioomat.

1) Laskutoimitus on liitännäinen, sillä kaikilla  $n_1, n_2, n_3 \in N$  ja  $g_1, g_2, g_3 \in G$  pätee

$$\begin{aligned} ((n_1, g_1)(n_2, g_2))(n_3, g_3) &= (n_1 \diamond \varphi_{g_1}(n_2), g_1 * g_2)(n_3, g_3) \\ &= (n_1 \diamond \varphi_{g_1}(n_2) \diamond \varphi_{g_1 * g_2}(n_3), g_1 * g_2 * g_3) \\ &= (n_1 \diamond \varphi_{g_1}(n_2) \diamond \varphi_{g_1}(\varphi_{g_2}(n_3)), g_1 * g_2 * g_3) \\ &= (n_1 \diamond \varphi_{g_1}(n_2 \diamond \varphi_{g_2}(n_3)), g_1 * g_2 * g_3) \\ &= (n_1, g_1)(n_2 \diamond \varphi_{g_2}(n_3), g_2 * g_3) \\ &= (n_1, g_1)((n_2, g_2)(n_3, g_3)). \end{aligned}$$

Tässä käytettiin hyväksi muun muassa niitä tietoja, että  $\varphi_g(n_1 n_2) = \varphi_g(n_1) \varphi_g(n_2)$  ja  $\varphi_{g_1 g_2}(n) = \varphi_{g_1}(\varphi_{g_2}(n))$ .

2) Puolisuoran tulon neutraalialkio on pari  $(e_N, e_G)$ , missä  $e_N$  ja  $e_G$  ovat ryhmien  $N$  ja  $G$  neutraalialkiot. Kaikilla  $n \in N$  ja  $g \in G$  nimittäin pätee

$$(e_N, e_G)(n, g) = (e_N \diamond \varphi_{e_N}(n), e_G * g) = (e_N \diamond n, g) = (n, g)$$

ja

$$(n, g)(e_N, e_G) = (n \diamond \varphi_g(e_N), g * e_G) = (n \diamond e_N, g) = (n, g).$$

Yllä käytettiin tietoja  $\varphi_{e_N} = \text{id}$  ja  $\varphi_g(e_N) = e_N$  (homomorfismin ominaisuus).

3) Alkion  $(n, g)$  käänteisalkio puolisuorassa tulossa on  $(\varphi_{g^{-1}}(n^{-1}), g^{-1})$ , sillä

$$\begin{aligned} (\varphi_{g^{-1}}(n^{-1}), g^{-1})(n, g) &= (\varphi_{g^{-1}}(n^{-1}) \diamond \varphi_{g^{-1}}(n), g^{-1} * g) \\ &= (\varphi_{g^{-1}}(n^{-1} \diamond n), e_G) = (\varphi_{g^{-1}}(e_N), e_G) \\ &= (e_N, e_G) \end{aligned}$$

ja

$$\begin{aligned} (n, g)(\varphi_{g^{-1}}(n^{-1}), g^{-1}) &= (n \diamond \varphi_g(\varphi_{g^{-1}}(n^{-1})), g * g^{-1}) \\ &= (n \diamond \varphi_{g * g^{-1}}(n^{-1}), e_G) = (n \diamond \varphi_{e_G}(n^{-1}), e_G) \\ &= (n \diamond n^{-1}, e_G) = (e_N, e_G). \end{aligned}$$

Nyt on osoitettu, että puolisuora tulo  $N \rtimes G$  on ryhmä. Tapaus  $G \rtimes N$  voidaan käsitellä samalla tavalla. Tuossa tapauksessa käänteisalkioksi tulee  $(g^{-1}, \varphi_g(n^{-1}))$ .  $\square$

**Esimerkki 5.24.** Tarkastellaan neliön symmetriaryhmän aliryhmää

$$N = \{\text{id}, \pi, \rho^2, \pi\rho^2\},$$

missä  $\pi$  on peilaus pystyakselin suhteen,  $\rho^2$  kierto puolirympyrän verran, ja  $\pi\rho^2$  peilaus vaak-akselin suhteen (vrt. esimerkkiin 4.9). Tämä ryhmä on vaihdannainen, ja sen kertotaulu näyttää seuraavalta:

$\circ$	id	$\pi$	$\rho^2$	$\pi\rho^2$
id	id	$\pi$	$\rho^2$	$\pi\rho^2$
$\pi$	$\pi$	id	$\pi\rho^2$	$\rho^2$
$\rho^2$	$\rho^2$	$\pi\rho^2$	id	$\pi$
$\pi\rho^2$	$\pi\rho^2$	$\rho^2$	$\pi$	id

Muodostetaan nyt ryhmän  $N$  puolisuora tulo ryhmän  $\mathbb{Z}_3 = \{[0], [1], [2]\}$  kanssa. Sitä varten on ensin määriteltävä ryhmän  $\mathbb{Z}_3$  konjugoiva toiminta ryhmässä  $N$ .

Konjugoivan toiminnan määritelmän mukaan täytyy päteä  $\varphi_0 = \text{id}$  ja toisaalta myös  $\varphi_2 = \varphi_{1+1} = \varphi_1 \circ \varphi_1$ . Toiminta riippuu siis vain alkioita  $[1] \in \mathbb{Z}_3$  vastaavasta isomorfisista  $\varphi_1$ . Määritellään se seuraavan taulukon mukaisesti:

$\sigma :$	id	$\pi$	$\rho^2$	$\pi\rho^2$
$\varphi_1(\sigma) :$	id	$\rho^2$	$\pi\rho^2$	$\pi$

Taulukosta nähdään suoraan, että  $\varphi_1$  on bijektio. Homomorfisuuden tarkistamiseksi pitäisi tarkistaa kaikki tulot  $\varphi_1(\sigma) \circ \varphi_1(\tau)$ , joissa  $\sigma$  ja  $\tau$  ovat  $N$ :n identtisestä poikkeavia permutaatioita. Tyydytään tässä tarkistamaan vain yksi:

$$\varphi_1(\pi)\varphi_1(\rho^2) = \rho^2 \cdot \pi\rho^2 = \pi = \varphi_1(\pi\rho^2).$$

Koska  $\varphi_1$  on isomorfismi, myös  $\varphi_2$  on. Lisäksi voidaan helposti varmistua myös siitä, että

$$\varphi_0(\sigma) = \varphi_{1+1+1}(\sigma) = \varphi(\varphi(\varphi(\sigma))) = \text{id}(\sigma)$$

kaikilla  $\sigma \in N$ . Konjugoiva toiminta voidaan siis määritellä edellä kuvatulla tavalla, ja niinpä voidaan määritellä myös tätä toimintaa vastaava puolisuora tulo  $N \rtimes \mathbb{Z}_3$ .

Lasketaan lopuksi esimerkin vuoksi alkioiden kertaluvut ryhmässä  $N \rtimes \mathbb{Z}_3$ . Kaikilla  $\sigma \in N$  pätee

$$(\sigma, 0)(\sigma, 0) = (\sigma \circ \varphi_0(\sigma), 0 + 0) = (\sigma \circ \sigma, 0) = (\text{id}, 0),$$

sillä kaikkien ryhmän  $N$  alkioiden kertaluku on 2. Muotoa  $(\sigma, 0)$  olevien alkioiden kertaluku on siis kaksi, lukuunottamatta neutraalialkiota  $(\text{id}, 0)$ .

Olkoot sitten  $\sigma \in N$  ja  $k \neq 0$ . Tällöin

$$(\sigma, k)(\sigma, k) = (\sigma \circ \varphi_k(\sigma), k + k) = (\sigma \circ \varphi_k(\sigma), 2k).$$

Saatu alkio ei ole neutraalialkio, koska  $2k$  on nolasta poikkeava kaikilla  $k \in \mathbb{Z}_3$ . Toisaalta

$$\begin{aligned} (\sigma, k)^3 &= (\sigma \circ \varphi_k(\sigma), 2k)(\sigma, k) = (\sigma \circ \varphi_k(\sigma) \circ \varphi_{2k}(\sigma), 2k + k) \\ &= (\sigma \circ \varphi_k(\sigma) \circ \varphi_{2k}(\sigma), 0). \end{aligned}$$

Jos viimeisessä lausekkeessa  $\sigma = \text{id}$ , niin tulo  $\sigma \circ \varphi_k(\sigma) \circ \varphi_{2k}(\sigma)$  on kolmen identtisen permutaation tulo. Jos taas  $\sigma \neq \text{id}$ , niin kyseisessä tulossa on kolme eri identtisestä

poikkeavaa permutaatiota. Molemmissa tapauksissa tulo on identtinen kuvaus, joten  $(\sigma, k)^3$  on neutraalialkio. Siis jos  $k \neq 0$ , niin alkion  $(\sigma, k)$  kertaluku on kolme.

Tarkempi tutkimus osoittaisi, että puolisuora tulo  $N \rtimes \mathbb{Z}_3$  on itse asiassa isomorfinen ryhmän  $A_4$  kanssa.