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

$$\begin{aligned} & H = \langle (1234) \rangle = \{\mathrm{id}, (1234), (13)(24), (1432)\} \\ \text{ja} \quad & K = \langle (123) \rangle = \{\mathrm{id}, (123), (132)\}. \end{aligned}$$

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

$$\begin{aligned} HK = \big\{ & \mathrm{id},\ (1234),\ (13)(24),\ (1423), \\ & (123),\ (1324),\ (142),\ (34), \\ & (132),\ (14),\ (234),\ (1243) \big\}. \end{aligned}$$

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 alkiot olisivat *keskenään vaihdannaisia*, pätee edellä mainitussa tulossa

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

ja oikeanpuoleinen tulo kuuluu nyt joukkoon HK. Myös minkä tahansa alkion $hk \in HK$ käänteisalkio kuuluu 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 $e = e \times e \in HK$.

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 $HK = H \times K$ 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

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

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

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

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

Esimerkki 5.4. Tarkastellaan yhteenlaskuryhmää $\mathbb{Z}_{15} = \{[0], [1], [2], \ldots, [14]\}$, missä $[n] = [m]$ aina kun $m - n$ on jaollinen 15:llä. Tällä ryhmällä on aliryhmät $H = \langle [5] \rangle = \{[0], [5], [10]\}$ ja $K = \langle [3] \rangle = \{[0], [3], [6], [9], [12]\}$. 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 selvyyden 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 alkiolla $g \in G$ on yksikäsitteinen esitys $g = hk$, missä $h \in H$ ja $k \in K$.*

Todistus. Osoitetaan ensin, että ehto 1) pätee. Olkoot sitä varten $h' \in H$, $k' \in K$ ja $g \in G$. Osoitetaan, että konjugaatit ${}^g h'$ ja ${}^g k'$ 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 $kh' = h'k$, joten

$$gh'g^{-1} = h(kh')k^{-1}h^{-1} = h(h'k)k^{-1}h^{-1} = hh'h^{-1} \in H.$$

Toisaalta myös $h(kk'k^{-1}) = (kk'k^{-1})h$, joten

$$gk'g^{-1} = h(kk'k^{-1})h^{-1} = (kk'k^{-1})hh^{-1} = kk'k^{-1} \in K.$$

Siispä ${}^g h' \in H$ ja ${}^g k' \in K$, 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 alkiot 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. □

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

1) $h_ih_j = h_jh_i$ aina, kun $i \neq j$, $h_i \in H_i$ ja $h_j \in H_j$

2) $H_i \cap (H_{j_1}H_{j_2} \cdots H_{j_{r-1}}) = \{e\}$, missä $i \notin \{j_1, \ldots, j_{r-1}\}$.

Suoraa tuloa voidaan tällöin merkitä $H_1 \times H_2 \times \cdots \times H_n$ tai tulomerkinnällä $\prod_{i=1}^n H_i$. Määritelmä toimii myös äärettömän monen aliryhmän tapauksessa. Tällöin kuitenkin kaikilla suoran tulon $\prod_{i \in I} H_i$ alkioilla on *äärelliset* esitykset $h_{i_1}h_{i_2} \cdots h_{i_n}$,

missä $h_{i_k} \in H_{i_k}$ kaikilla k. Ääretöntä alkioiden tuloa ei nimittäin voida ryhmässä yleensä määritellä.

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

Määritelmä 5.6. Ryhmien $(G_1, \circ)$ ja $(G_2, *)$ *ulkoinen suora tulo* on ryhmä, jonka alkioina 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 $G_1 \oplus G_2$.

Ulkoisessa suorassa tulossa neutraalialkiona toimii pari (e_1, e_2), missä e_1 ja e_2 ovat ryhmien G_1 ja G_2 neutraalialkiot. Alkion $(g_1, g_2) \in G_1 \times G_2$ käänteisalkio on puolestaan (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 oheisen taulukon muotoon. (Jätetään jälleen taulukosta pois hakasulut alkioiden 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 esimerkkiin 5.4, 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 alkiota vastaa

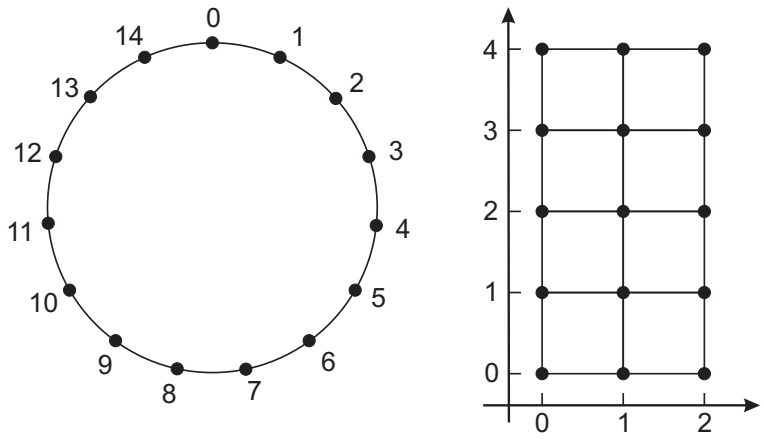
pari $([2]_3, [2]_5)$, ja jos lasketaan kyseisen parin monikerrat summaryhmässä $\mathbb{Z}_3 \oplus \mathbb{Z}_5$, saadaan

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

jne.

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 erään alkionsa virittämiä.

Kuvassa 16 on piirretty syklinen ryhmä $\mathbb{Z}_{15}$ kahdella tavalla: yhtenä pitkänä syklinä ja kahden ryhmän tulona.



Kuva 16: Kaksi tapaa hahmottaa 15 alkion syklinen ryhmä

Esimerkki 5.8. Muodostetaan ryhmien A_n ja $(\{1, -1\}, \cdot)$ ulkoinen suora tulo. Tulo koostuu pareista (σ, k), missä σ on joku parillinen permutaatio ja $k = \pm 1$. Merkitään tällaista paria yksinkertaisesti σ, 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. Päteehän myös tuloryhmässä

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

eli kahden "parittoman" permutaation tulo on jälleen parillinen. 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 voidaankin osoittaa, että ryhmät $A_n \times (\{1, -1\}, \cdot)$ ja S_n eivät ole isomorfisia paitsi tapauksessa $n = 2$.

Jos H_1 ja H_2 ovat ryhmien G_1 ja G_2 aliryhmiä, niin 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

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

ja 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. □

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. Tällöin löytyy aliryhmät $H, K \leq (G_1 \times G_2)_u$, joille pätee $(H \times K)_s = (G_1 \times G_2)_u$. Toisaalta, jos H ja K ovat mielivaltaisia ryhmän G aliryhmiä, 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 alkiota (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 $H = (G_1 \times \{e_1\})_u$ ja $K = (\{e_1\} \times G_2)_u$. Selvästikin $H \cap K = \{(e_1, e_2)\}$. Lisäksi kaikilla $g_1 \in G_1$ ja $g_2 \in G_2$ pätee

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

joten aliryhmän H alkiot kommutoivat aliryhmän K alkioiden kanssa. Aliryhmien H ja K tulo on siis suora, ja sitä voidaan merkitä $(H \times K)_s$. Lisäksi 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 $(g_1, e_2) \in H$ ja $(e_1, g_2) \in K$. Täten $(H \times K)_s = (G_1 \times G_2)_u$.

Todistetaan sitten toinen väite. Olkoot H ja K ryhmän G aliryhmiä. Määritellään kuvaus $\varphi : (H \times K)_u \to (H \times K)_s$ kaavalla $\varphi(h,k) = hk$ ja osoitetaan, että se on isomorfismi. Ensinnäkin jokainen sisäisen suoran tulon alkio on muotoa hk, missä $h \in H$ ja $k \in K$. Nyt pätee $\varphi(h,k) = hk$, joten kuvaus φ 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 $h_1k_1 = h_2k_2 \in (H \times K)_s$, ja koska lemman 5.5 mukaan jokaisen sisäisen suoran tulon alkion esitys tällaisena tulona on yksikäsitteinen, täytyy olla $(h_1,k_1) = (h_2,k_2)$. Kuvaus φ on siis myös injektio. Homomorfisuus seuraa siitä, että yhtälö

$$\begin{aligned}\varphi\Big((h_1,k_1)(h_2,k_2)\Big) &= \varphi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 \\ &= \varphi(h_1,k_1) \cdot \varphi(h_2,k_2)\end{aligned}$$

pätee kaikilla $h_1, h_2 \in H$ ja $k_1, k_2 \in K$. □

Suoran summan käsite esiintyy paljon 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, ja toinen niistä sisältää neutraalialkion lisäksi vain yhden alkion: olkoon esimerkiksi $C = \{\mathrm{id}, \sigma\}$. Näytetään, että C ei voi olla normaali.

Koska $\sigma^2 = \mathrm{id}$, koostuu σ: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 σ: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 nurkkapalaan 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 yhdentyyppisiin 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 $1, \ldots, 48$, näiden permutaatioryhmien voidaan ajatella olevan ryhmän S_{48} aliryhmiä.

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

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

Permutaation kantaja on siis niiden alkioiden 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) $\sigma(x) \in \operatorname{supp}(\sigma)$ jos ja vain jos $x \in \operatorname{supp}(\sigma)$

2) $\operatorname{supp}(\sigma) = \operatorname{supp}(\sigma^{-1})$

3) $\operatorname{supp}(\sigma \circ \tau) \subset \operatorname{supp}(\sigma) \cup \operatorname{supp}(\tau)$.

Näiden ominaisuuksien todistaminen on helppo harjoitustehtävä.

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

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

Koska mikään ruutu ei ole kiinni sekä nurkka- että särmäpalassa, nähdään että $N \cap S = \emptyset$. 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. *Olkoot Σ ja T joukon X symmetrisen ryhmän S_X aliryhmiä. Oletetaan, että joillain joukoilla $A, B \subset X$ pätee $A \cap B = \emptyset$,* $\mathrm{supp}(\sigma) \subset A$ *kaikilla $\sigma \in \Sigma$ ja* $\mathrm{supp}(\tau) \subset B$ *kaikilla $\tau \in T$. Tällöin Σ ja T muodostavat suoran tulon ryhmässä S_X.*

Todistus. Ensinnäkin huomataan, että jos σ kuuluu molempiin ryhmiin Σ ja T, niin täytyy päteä $\mathrm{supp}(\sigma) \subset A \cap B = \emptyset$, eli $\sigma(x) = x$ kaikilla alkioilla $x \in X$. Täten $\sigma = \mathrm{id}$.

Olkoot sitten $\sigma \in \Sigma$ ja $\tau \in T$. Jos $x \in A$, niin permutaation kantajan ominaisuuksien perusteella pätee $\sigma(x) \in A$. Koska $\mathrm{supp}(\tau) \cap A = \emptyset$, nähdään että

$$\tau \underbrace{\sigma(x)}_{\in A} = \sigma(x) = \sigma\tau(x).$$

Jos taas $x \in B$, niin $\tau(x) \in B$, ja

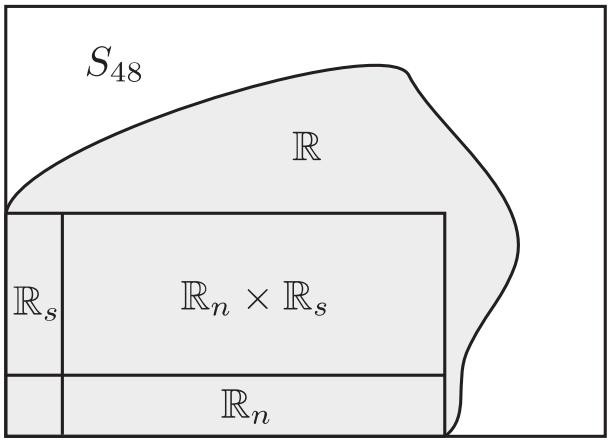
$$\sigma \underbrace{\tau(x)}_{\in B} = \tau(x) = \tau\sigma(x).$$

Lopulta, jos $x \notin A \cup B$, niin $\sigma(x) = \tau(x) = x$, joten $\sigma\tau(x) = \tau\sigma(x)$. Näin on osoitettu, että $\sigma\tau = \tau\sigma$, eli aliryhmät Σ ja T ovat keskenään vaihdannaisia. Ne muodostavat siis suoran tulon. □

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 käsiteltyjen ryhmien Rubikin ryhmään sisältyvät osat.

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

Rubikin nurkkaryhmä sisältää sellaiset lailliset siirrot, jotka liikuttavat vain nurkkaruutuja, ja särmäryhmä puolestaan on niiden 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



Kuva 17: Tuloryhmän $\mathbb{R}_n \times \mathbb{R}_s$ asema Rubikin ryhmässä

myös sellaisia siirtoja, jotka eivät kuulu kyseiseen tuloryhmään. Kuvassa 17 on esitetty Venn-diagrammina Rubikin ryhmän ja tuloryhmän $\mathbb{R}_n \times \mathbb{R}_s$ suhde.

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

Lause 5.14. *Jos H ja K ovat ryhmän G aliryhmiä ja N on G:n normaali aliryhmä, niin $H \cap N \trianglelefteq H$ ja $K \cap N \trianglelefteq K$.*

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. Samalla tavoin voidaan todistaa, että $K \cap N$ on normaali aliryhmä K:ssa. □

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 sellaiset, että $\varphi_1 : [\sigma]_n \mapsto [\sigma]$ 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 (ks. kuva 18). Kyseessä on kuitenkin eri tekijäryhmät, sillä ne on muodostettu eri normaalien aliryhmien avulla. Nyt todistettava lause antaa tällaisten 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 (eli kuvaus on ns. hyvin määritelty).

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

$$\varphi([\sigma_1]_n) \cdot \varphi_1([\sigma_2]_n) = [\sigma_1] \cdot [\sigma_2] = [\sigma_1\sigma_2] = \varphi([\sigma_1\sigma_2]_n) = \varphi([\sigma_1]_n \cdot [\sigma_2]_n).$$

Osoitetaan, että kuvaus φ 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 $\mathbb{R}_n$ on ryhmä, joten pätee myös $\sigma_1^{-1}\sigma_2 \in \mathbb{R}_n$. Siispä $\sigma_1^{-1}\sigma_2 \in \mathbb{R}_{na}$ eli $[\sigma_1]_n = [\sigma_2]_n$. Kuvaus φ on siis injektiivinen homomorfismi ryhmälle $\mathbb{R}_p$, joten lähtöryhmä $\mathbb{R}_{np}$ on isomorfinen kuvaryhmän $\mathrm{Im}(\varphi) \leq \mathbb{R}_p$ kanssa.

b) Osoitetaan, että kuvaryhmät

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

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

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

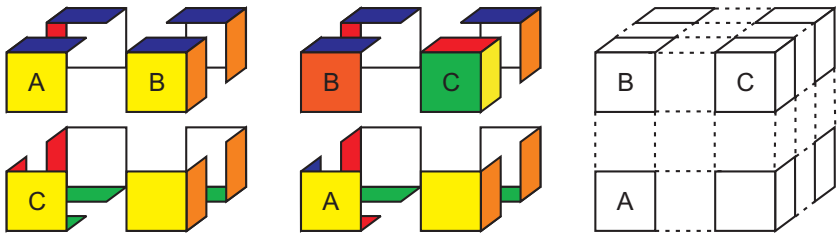
Kuvaryhmät ovat siis keskenään vaihdannaisia.

Oletetaan sitten, että $[\sigma] = [\tau]$ joillain $\sigma \in \mathbb{R}_n$ ja $\tau \in \mathbb{R}_s$, ja pyritään osoittamaan, että $[\sigma] = [\tau] = [\mathrm{id}]$. Tällöin kuvaryhmien leikkaus on triviaali.

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

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

Yhtälön vasemmalla puolella oleva permutaatio kuuluu ryhmään $\mathbb{R}_n$, joten se ei liikuta särmäpaloja paikoiltaan. Toisaalta oikealla puolella oleva permutaatio on puolestaan 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 $[\sigma] = [\tau] = [\mathrm{id}]$. □

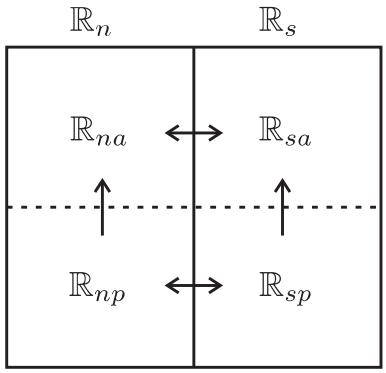


Kuva 18: Tuttu nurkkapalojen 3-sykli esitettynä nurkkaryhmässä. Kun palojen asennot jätetään huomiotta (eli siirrytään tekijäryhmään), saadaan ryhmän $\mathbb{R}_{np}$ alkio, joka voidaan samastaa paikkaryhmän $\mathbb{R}_p$ vastaavan 3-syklin kanssa.

Huom. 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 $\mathbb{R}_n \times \mathbb{R}_s$, niin 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 nurkkaettä 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 $\mathbb{R}_n \times \mathbb{R}_s$ 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 $\mathbb{R}_n \times \mathbb{R}_s$ 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 ainoastaan tuloryhmässä $\mathbb{R}_n \times \mathbb{R}_s$, joka ei sisällä kaikkia mahdollisia asemia. Luvussa 5.4 selvitetään, miten yleisestä tapauksesta voidaan aina siirtyä tuloryhmään.

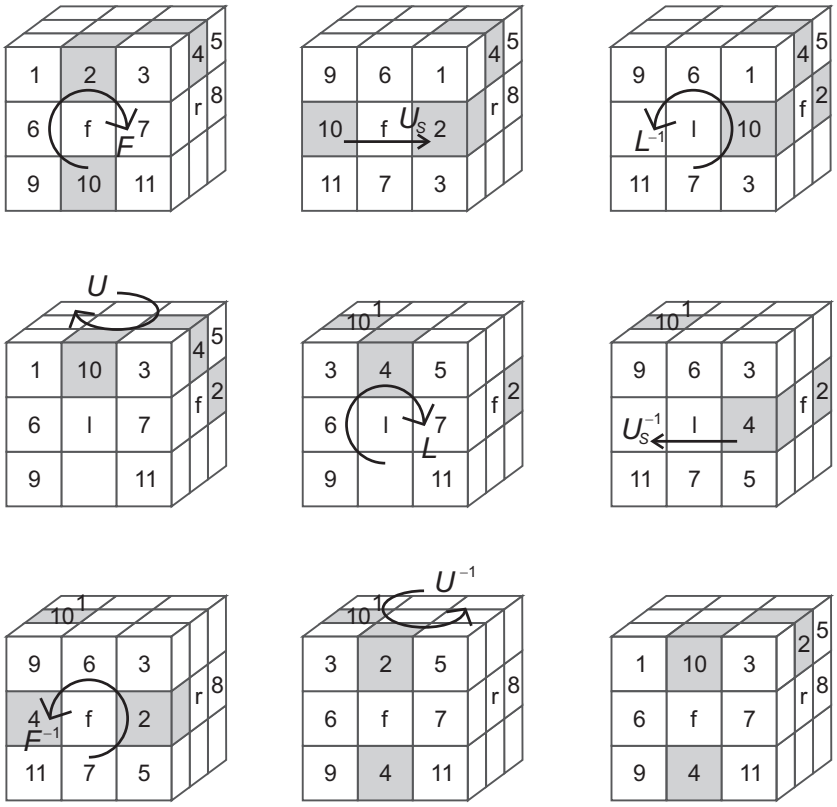
5.3 Algoritmi 2: särmäpalojen 3-sykli

Särmäpaloja kiertävä 3-sykli on samankaltainen kuin aiemmin opittu nurkkapalojen 3-sykli. Se on jälleen muotoa $\sigma\tau\sigma^{-1}\tau^{-1}$, missä σ on perussiirto U^{-1} ja τ kolmen siirron yhdistelmä $F^{-1}U_S^{-1}L$. Yhdessä näistä koostuu siis kuvassa 20 esitetty

kahdeksan siirron sarja

$$U^{-1}F^{-1}U_S^{-1}LUL^{-1}U_SF.$$

Tämä siirtosarja suoritetaan tietysti oikealta vasemmalle, aloittaen siirrosta F.



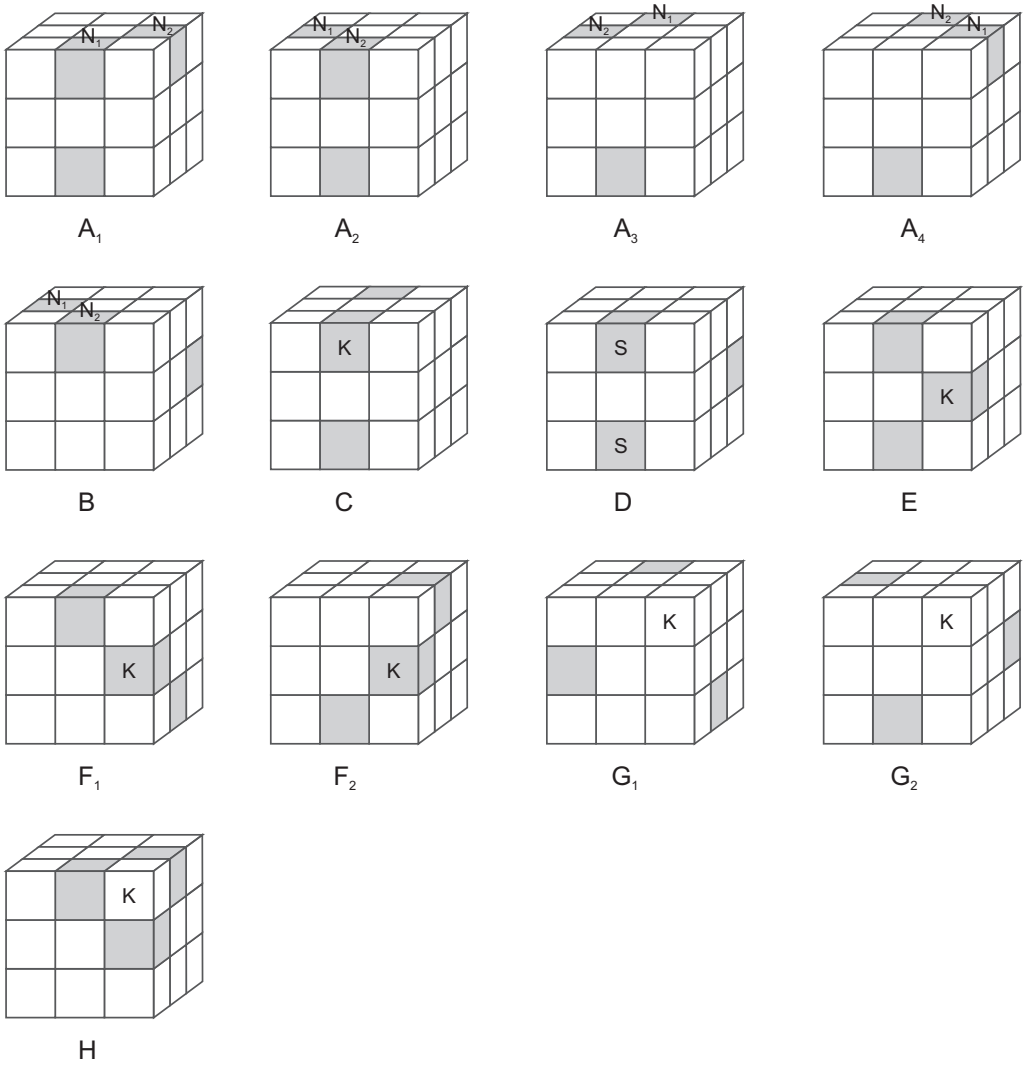
Kuva 20: Särmäpalojen 3-sykli

Algoritmi on tässä kirjoitettu siirron U_S avulla, joka on kuution keskitahkon siirto. Tämä on tehty sen takia, että siirtosarja olisi helpompi hahmottaa. Toisaalta tästä seuraa, että siirrot F ja L näyttävät nyt kuvassa molemmat pyörittävän etutahkoa, vaikka todellisuudessa kyseinen "etutahko" on kääntynyt oikealle siirron U_S vaikutuksesta siinä vaiheessa, kun ruvetaan käyttämään siirtoa L^{-1}, ja tilalle on tullut aiemmin vasemmalla sivulla ollut tahko. Kuvassa tahkoja merkitään keskipalojen kirjaimilla f, r ja l.

5.4 Rubikin paikkaryhmän ratkaiseminen

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

Käydään ensin läpi kaikki kolmen särmäpalan kombinaatiot samalla tavoin kuin aiemmin (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.



Kuva 21: Kolmen reunapalan kombinaatiot

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.

G_1, G_2 Kirjaimella K merkitty pala voidaan valita kunkin nurkkapalan joukosta, ja 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 oheisen 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	$F^{-1}D$
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. □

Osoitetaan seuraavaksi lemma, joka liittyy siirtojen parillisuuteen. Merkitään sitä varten kaikkien nurkkapalojen *paikkojen* permutaatioryhmää S_N^p ja samaten kaikkien reunapalojen 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 τ on Rubikin paikkaryhmän siirto, niin sille löytyy yksikäsitteinen esitys tulona $\tau = \nu \circ \sigma$, missä $\nu \in S_N^p$ ja $\sigma \in S_S^p$. Näille permutaatioille pätee* $\text{sign}(\nu) = \text{sign}(\sigma)$.

Todistus. Koska τ on paikkaryhmän siirto, se voidaan esittää paikkaryhmän perussiirtojen $\tau_1, \ldots, \tau_n$ tulona. Kaikkien palojen permutaatioiden ryhmässä S_{20} jokainen perussiirto τ_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 τ 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 ν_i ja σ_i ovat 4-syklejä, pätee

$$\operatorname{sign}(\nu) = (-1)^n = \operatorname{sign}(\sigma).$$

□

Jokainen Rubikin paikkaryhmän $\mathbb{R}_p$ siirto voidaan siis kirjoittaa muodossa $(\nu, \sigma) \in S_N^p \times S_S^p$. Jos myös ν ja σ kuuluvat ryhmään $\mathbb{R}_p$, niin (ν, σ) on tuloryhmässä $\mathbb{R}_{np} \times \mathbb{R}_{sp}$. Edellisen lemman avulla saadaan nyt lause, joka mahdollistaa paikkaryhmän ratkaisemisen. Merkinnöissä käytetään lauseen 5.15 antamaa upotusta.

Lause 5.18. *Oletetaan, että $\tau = (\nu, \sigma) \in \mathbb{R}_p$. Jos $\operatorname{sign}(\nu) = 1$ tai $\operatorname{sign}(\sigma) = 1$, niin ν ja σ 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 $\operatorname{sign}(\nu) = 1$ tai $\operatorname{sign}(\sigma) = 1$. Edellisen lemman perusteella pätee tällöin $\operatorname{sign}(\nu) = \operatorname{sign}(\sigma) = 1$. Aiemmin on osoitettu, että kaikki nurkkapalojen 3-syklit ovat mahdollisia siirtoja, ja lauseen 3.12 mukaan jokainen parillinen permutaatio saadaan 3-syklien yhdistelmänä. Täten $\nu \in \mathbb{R}_p$, ja sama pätee myös permutaatiolle σ.

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 $\operatorname{sign}(\nu) = -1$ tai $\operatorname{sign}(\sigma) = -1$. Tällöin täytyy kuitenkin edellisen lemman mukaan olla $\operatorname{sign}(\nu) = \operatorname{sign}(\sigma) = -1$, ja koska perussiirrolle pätee $\operatorname{sign}(\pi_1) = \operatorname{sign}(\pi_2) = -1$, saadaan

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

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 $\tau \in \pi \cdot (\mathbb{R}_{np} \times \mathbb{R}_{sp})$. Koska mikä tahansa tuloryhmään kuulumaton permutaatio kuuluu yhteen tiettyyn tuloryhmän sivuluokkaan, sivuluokkia voi olla korkeintaan kaksi. □

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-syklien 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 $n_1h_1 \cdot n_2h_2$. Jotta tämä alkio kuuluisi edelleen joukkoon NH, riittää että toinen aliryhmistä, esimerkiksi 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

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

Tarkastellaan tämän lisäksi 3-syklin virittämää aliryhmää $H = \{\mathrm{id}, (123), (132)\}$, 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. Siispä $N \rtimes H = A_4$, 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 kaavasta, joka pätee kaikissa ryhmissä:

$$n_1 h_1 \cdot n_2 h_2 = n_1 (h_1 n_2 h_1^{-1}) h_1 h_2 = n_1 {}^{h_1}n_2 \cdot h_1 h_2. \tag{5.21}$$

Olennaista tässä on, että aliryhmän N ollessa normaali konjugaatti ${}^{h_1}n_2$ kuuluu edelleen aliryhmään N. Tällöin kaavasta nähdään, että ei-normaalin ryhmän H alkiot voidaan jälleen kertoa keskenään N:n alkioista riippumatta, mutta toista normaalin aliryhmän alkiota on kerrottaessa konjugoitava ensin H:n alkiolla. Kyseessä on siis eräänlainen puolittainen riippumattomuus.

Huom. Jos normaali aliryhmä on tulossa oikeanpuoleisena, yllä oleva kaava tulee muotoon $h_1 n_1 \cdot h_2 n_2 = h_1 h_2 \cdot {}^{h_2^{-1}}n_1 n_2$.

Kaavan (5.21) avulla voidaan määritellä 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 määritellä, 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: neutraalialkiota vastaa identtinen kuvaus $x \mapsto x$, ja alkioiden tuloa vastaa yhdistetty kuvaus, nimittäin ${}^{gh}x = {}^g\big({}^h x\big)$. Nämä ominaisuudet huomioiden voidaan määritellä ryhmän konjugointi toisessa ryhmässä.

Määritelmä 5.22. Olkoot G ja H ryhmiä. Kuvausta $g \mapsto \varphi_g$, joka liittää jokaiseen G:n alkioon g jonkin kuvauksen φ_g ryhmältä H itselleen, kutsutaan *konjugoivaksi toiminnaksi*, jos seuraavat ehdot täyttyvät:

1) kuvaus φ_g on isomorfismi (eli automorfismi) jokaisella $g \in G$

2) φ_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 (5.21) avulla voidaan määritellä kahden mielivaltaisen ryhmän puolisuora tulo.

Määritelmä 5.23. 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

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

Toisinpäin merkityssä puolisuorassa tulossa $G \ltimes N$ laskutoimitus on vastaavasti

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

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

Huom. Ulkoisen suoran tulon rakenne riippuu valitusta konjugoivasta toiminnasta. Toiminnaksi voidaan aina valita $\varphi_g = \mathrm{id}$ kaikilla g, jolloin puolisuorasta tulosta tulee suora tulo. Eri valinnat tuottavat kuitenkin erilaisen tulon.

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

Lause 5.24. *Ryhmien $(N, \diamond)$ ja $(H, *)$ puolisuora tulo on ryhmä.*

Todistus. Puolisuora tulo on suljettu 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

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

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 on N:n neutraalialkio ja e_G on G:n. 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 $\varphi_{e_N} = \mathrm{id}$ ja $\varphi_g(e_N) = e_N$ (homomorfismi).

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

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

ja

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

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

Esimerkki 5.25. Tarkastellaan neliön symmetriaryhmän aliryhmää

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

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

$\circ$	id	π	ρ^2	$\pi \circ \rho^2$
id	id	π	ρ^2	$\pi \circ \rho^2$
π	π	id	$\pi \circ \rho^2$	ρ^2
ρ^2	ρ^2	$\pi \circ \rho^2$	id	π
$\pi \circ \rho^2$	$\pi \circ \rho^2$	ρ^2	π	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 olla $\varphi_0 = \mathrm{id}$, ja $\varphi_2 = \varphi_{1+1} = \varphi_1 \circ \varphi_1$. Tarvitsee siis valita vain alkiota $[1] \in \mathbb{Z}_3$ vastaava homomorfismi φ_1. Määritellään se seuraavan taulukon mukaisesti:

σ	id	π	ρ^2	$\pi \circ \rho^2$
$\varphi_1(\sigma)$	id	ρ^2	$\pi \circ \rho^2$	π

Taulukosta nähdään suoraan, että φ_1 on bijektio. Homomorfisuuden tarkistamiseksi pitäisi tarkistaa kaikki tulot $\varphi_1(\sigma) \circ \varphi_1(\tau)$, joissa σ ja τ ovat N:n identtisestä poikkeavia permutaatioita. Tyydytään tässä tarkistamaan vain yksi:

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

Koska φ_1 on isomorfismi, myös φ_2 on. Lisäksi voidaan helposti varmistua myös siitä, että

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

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

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

sillä kaikkien N:n alkioiden kertaluku on 2. Muotoa $(\sigma, 0)$ olevien alkioiden kertaluku on siis kaksi (paitsi neutraalialkion $(\mathrm{id}, 0)$).

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 nollasta 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 $\sigma = \mathrm{id}$, niin tulo $\sigma \circ \varphi_k(\sigma) \circ \varphi_{2k}(\sigma)$ on kolmen identtisen permutaation tulo. Jos taas $\sigma \neq \mathrm{id}$, 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 (σ, k) kertaluku on kolme.

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