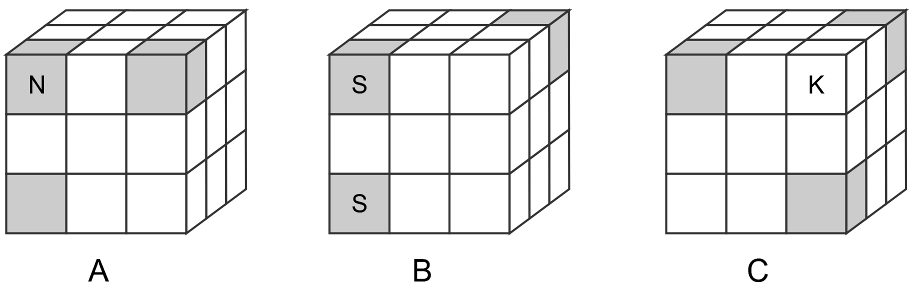
Jotta kaikki nurkkapalat saataisiin paikoilleen tunnettua 3-sykliä ja sen konjugaatteja soveltamalla, täytyisi kahden ehdon täyttyä: ensinnäkin nurkkapalojen permutaation pitäisi aina olla parillinen. Toiseksi kaikkien konjugointiin tarvittavien permutaatioiden pitäisi olla laillisia siirtoja.

Ensimmäinen ehto ei kuitenkaan päde, koska mikä tahansa perussiirto on nurkkapalojen kannalta 4-sykli, joka ei ole parillinen. Toisaalta, jos nurkkapalat ovat asennossa, joka vastaa paritonta permutaatiota, tekemällä mikä tahansa perussiirto (missä tahansa vaiheessa) saa tilanteen jälleen vastaamaan parillista permutaatiota. Tällöin se on periaatteessa mahdollista ratkaista 3-syklien avulla.

Käydään nyt läpi kaikki mahdolliset kolmen nurkkapalan kombinaatiot ja osoitetaan, että jokaista näistä kohti löytyy permutaatio σ, joka vie opittuun 3-sykliin τ osallistuvat palat noiden kolmen nurkkapalan paikalle. Tällöin voidaan mikä tahansa 3-sykli suorittaa konjugaattina ${}^{\sigma}\tau$.

Lasketaan ensin, kuinka monta erilaista kolmen nurkkapalan kombinaatiota kuutiosta yhteensä löytyy. Koska nurkkapaloja on yhteensä kahdeksan, lukumäärä on $\binom{8}{3} = 56$. Nämä kombinaatiot jakautuvat kolmeen joukkoon A, B ja C, jotka näkyvät kuvassa 14. Jokaisen joukon sisällä kombinaatiot saadaan toisistaan koko kuutiota kiertämällä.



Kuva 14: Kolmen nurkkapalan kombinaatiot

Lasketaan nyt kussakin joukossa A, B ja C olevien kombinaatioiden lukumäärä, jotta varmistutaan siitä, että nämä joukot todella sisältävät kaikki mahdolliset kombinaatiot.

A: Tämä on ainoa joukko, jossa kaikki nurkkapalat ovat samalla sivulla. Sivuvaihtoehtoja on kuusi, ja jokaisella sivulla kirjaimella N merkitty pala voi olla neljässä eri nurkassa. Näin saadaan yhteensä $6 \cdot 4 = 24$ eri kombinaatiota.

B: Kirjaimilla S merkityt palat ovat samalla särmällä. Tämä särmä voidaan valita 12 eri särmän joukosta. Kolmanneksi palaksi voidaan sitten valita jompi kumpi vastakkaisen särmän nurkkapaloista. (Nämä kombinaatiot saadaan toisistaan kiertämällä kuutio ylösalaisin.) Yhteensä saadaan siis 24 kombinaatiota.

C: Nämä kombinaatiot koostuvat kirjaimella K merkityn nurkkapalan viereisten nurkkien paloista. Nurkan K valinta määrää koko kombinaation täysin, ja se voidaan valita vapaasti kaikkien kahdeksan nurkan joukosta. Kombinaatioita on siis 8.

Yhteensä edellä laskettuja kombinaatioita on juuri $24 + 24 + 8 = 56$, joten kaikki kombinaatiot kuuluvat johonkin luetelluista joukoista.

Oletetaan, että jokin asema saadaan toisesta kiertämällä kuutiota neljänneskierros jonkin keskiakselinsa ympäri. Nurkkapalojen kannalta sama tulos saadaan, jos pidetään keskitahko paikallaan ja kierretään vain sivutahkoja. Tällöin keskipalat eivät liiku, joten kuution sivut säilyvät samassa asennossa. Jos siis ajatellaan kuvassa 14 keltaisen sivun olevan katsojaan päin ja sinisen ylöspäin, voidaan mikä tahansa kombinaatio palauttaa kuvan kaltaiseen asemaan vain sivutahkoja liikuttamalla.

Lause 4.10. *Mikä tahansa ryhmän $\mathbb{R}_p$ 3-sykli, joka liikuttaa vain nurkkapaloja, on mahdollinen siirto.*

Todistus. Merkitään luvussa 3.3 opittua nurkkapalojen 3-sykliä kirjaimella τ. Valitaan jokin kuution palojen numerointi, jossa $\tau = (123)$. Osoitetaan, että mitä tahansa kolmea nurkkapalaa a, b ja c kohti voidaan löytää siirto $\sigma \in \mathbb{R}_p$, jolle $\sigma\{1, 2, 3\} = \{a, b, c\}$. Tällöin pätee joko ${}^{\sigma}\tau = (abc)$ tai ${}^{\sigma}\tau = (acb)$. Koska joka tapauksessa $(abc)^2 = (acb)$, niin kumpikin 3-sykli voidaan muodostaa.

Olkoot siis a, b ja c jotkin kolme nurkkapalaa. Etsitään konjugoivan siirron σ sijasta sen käänteissiirto σ^{-1}. Tämän muodostaminen koostuu seuraavista vaiheista:

1. Saatetaan sivutahkoja kiertämällä kuutio johonkin kuvan 14 kolmesta asemasta, joista jokaisessa keltainen sivu osoittaa katsojaan päin ja sininen ylöspäin.

2A. Jos päädyttiin asemaan A, siirto σ^{-1} on valmis.

2B. Jos päädyttiin asemaan B, kierretään oikeaa tahkoa neljänneskierros vastapäivään siirrolla R^{-1}.

2C. Jos päädyttiin asemaan C, kierretään ensin alatahkoa vastapäivään, sitten oikeaa tahkoa vastapäivään, eli suoritetaan siirto $R^{-1}D^{-1}$.

Kaikissa tapauksissa saadaan konjugoiva siirto σ^{-1}, joka siirtää nurkat a, b ja c nurkiksi 1, 2 ja 3. Tämän käänteissiirto on etsitty σ. $\square$

Huom. Kuutiota ratkaistaessa ei tarvitse suorittaa edellisessä todistuksessa mainittua vaihetta 1 vaan riittää, että kääntää kuution ympäri ja nimeää uudelleen perussiirrot niin, että edessä olevan uuden tahkon kierto on F, ylätahkon kierto U jne. Myöskään vaiheiden 2A, 2B ja 2C konjugointeja ei tarvitse muistaa ulkoa vaan niiden sijaan voi keksiä kuhunkin tilanteeseen sopivan konjugointisiirron.

4.4 Ryhmän keskus

Usein on hyödyllistä tarkastella niiden alkioiden joukkoa, joilla konjugoiminen ei vaikuta muihin alkioihin.

Määritelmä 4.11. Olkoon G ryhmä ja olkoon $x \in G$. Alkion x *keskittäjä* on joukko
$$C_G(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}.$$
Ryhmän G *keskus* on niiden alkioiden joukko, jotka eivät konjugoitaessa liikuta mitään alkioita:
$$\zeta G = \{g \in G \mid gx = xg \text{ kaikilla } x \in G\} = \bigcap_{x \in G} C_G(x).$$
Voidaan myös sanoa, että keskus on niiden alkioiden joukko, jotka kommutoivat kaikkien alkioiden kanssa.

On helppo nähdä, että sekä keskus että jokainen keskittäjä ovat koko ryhmän aliryhmiä. Keskus on lisäksi vaihdannainen ja normaali.

Vaikka keskittäjän määritelmä on annettu siinä muodossa, että sen alkioilla konjugoiminen ei vaikuta alkioon x, voidaan sama ajatella myös niin, että x:llä konjugoiminen ei vaikuta keskittäjän alkioihin. Jos nimittäin ${}^{g}x = x$, niin myös ${}^{g^{-1}}x = x$, ja
$${}^{x}g = (gg^{-1})(xgx^{-1}) = g \cdot {}^{g^{-1}}x \cdot x^{-1} = gxx^{-1} = g.$$
Samaten keskus voidaan määritellä niiden alkioiden joukkona, joihin mikään konjugointi ei vaikuta. Tästä seuraa tietysti suoraan keskuksen normaalisuus.

Tarkastellaan seuraavaksi hieman keskittäjäaliryhmien $C_G(x)$ sivuluokkia. Keskittäjän alkioilla konjugoitaessa x pysyy paikallaan, joten voisi olettaa, että kaikki samaan sivuluokkaan kuuluvat alkiot tuottavat konjugoitaessa x:stä saman konjugaatin. Tästä havainnosta saadaan seuraava lause.

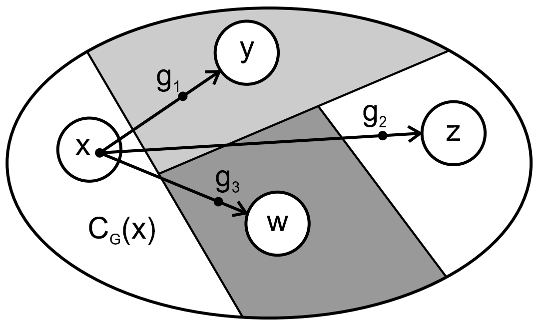
Lause 4.12. *Olkoon G äärellinen ryhmä ja olkoon $x \in G$. Keskittäjän $C_G(x)$ sivuluokkien lukumäärä $[G : C_G(x)]$ on sama kuin alkion x konjugaattiluokan koko.*

Todistus. Osoitetaan edellä mainittu seikka, eli että kaksi alkion x konjugaattia ovat samat jos ja vain jos niitä konjugoivat alkiot kuuluvat samaan keskittäjän sivuluokkaan. Tällöin konjugaatteja täytyy olla yhtä paljon kuin sivuluokkia. Olkoot siis $g_1, g_2 \in G$. Tällöin

$$\begin{aligned} {}^{g_1}x = {}^{g_1}x &\iff {}^{g_2^{-1}}({}^{g_1}x) = {}^{g_2^{-1}}({}^{g_2}x) \\ &\iff {}^{(g_2^{-1}g_1)}x = {}^{(g_2^{-1}g_2)}x = x \\ &\iff g_2^{-1}g_1 \in C_G(x). \end{aligned}$$

Saatiin siis, että kaksi konjugaattia ovat samat jos ja vain jos alkio $g_2^{-1}g_1$ kuuluu keskittäjään. Tällöin kuitenkin g_1 ja g_2 kuuluvat samaan sivuluokkaan, joten väite on todistettu. □

Oheisessa kuvassa on havainnollistettu keskittäjäaliryhmän ja konjugaattiluokan suhdetta. Alkion x konjugaattiluokka on neljän alkion joukko $\{x, y, z, w\}$. Saman alkion keskittäjällä puolestaan on neljä sivuluokkaa $C_G(x)$, $g_1 \cdot C_G(x)$, $g_2 \cdot C_G(x)$ ja $g_3 \cdot C_G(x)$. Kustakin eri sivuluokasta otettu alkio tuottaa eri konjugaatin, esimerkiksi ${}^{g_1}x = y$, toisaalta saman sivuluokan alkiot tuottavat aina saman konjugaatin. Huomaa, että konjugaatin sijaintia ryhmässä ei tunneta; ei esimerkiksi päde välttämättä $y \in g_1 \cdot C_G(x)$.



Kuva 15: Keskittäjän sivuluokat ja konjugaatit

Esimerkki 4.13. Tarkastellaan permutaation $\tau = (123)$ keskittäjää ryhmässä S_3. Koska permutaatiolla σ konjugoiminen tuottaa τ:sta syklin $(\sigma(1)\ \sigma(2)\ \sigma(3))$, täytyy tutkia, missä tapauksissa tämä tulossykli on sama permutaatio kuin τ. Permutaatio τ voidaan kirjoittaa kolmella eri tavalla: (123), (231) tai (312). Näitä vastaavat konjugoivat permutaatiot id, (123) ja (132). Muut ryhmän S_3 permutaatiot eivät pidä konjugoinnissa τ:ta paikallaan; esimerkiksi ${}^{(12)}(123) = (213) \neq (123)$.

Syklin τ keskittäjä on siis $C_G(\tau) = \{\mathrm{id}, (123), (132)\}$. Sen indeksi on

$$[S_3 : C_G(\tau)] = |S_3|/|C_G(\tau)| = 6/3 = 2,$$

joten sillä on itsensä lisäksi vain yksi sivuluokka. Tämä on 2-syklien muodostama joukko $(12) \circ \tau = \{(12), (23), (13)\}$.

Edellä todistetun lauseen mukaan jokaista keskittäjän $C_G(\tau)$ sivuluokkaa vastaa jokin τ:n konjugaatti. Koska symmetrisessä ryhmässä konjugaattiluokat määräytyvät syklityypin mukaan, on τ:n konjugaattiluokka kahden 3-syklin joukko $\{(123), (132)\}$. Keskittäjä vastaa itse tietysti 3-sykliä $\tau = (123)$. Toinen sivuluokka vastaa tällöin 3-sykliä (132), ja konjugoimalla permutaatiota τ tuon sivuluokan alkioilla saadaankin seuraavat tulokset:

$$\begin{aligned} &{}^{(12)}(123) = (213) = (132), \\ &{}^{(23)}(123) = (132) \\ \text{ja}\quad &{}^{(13)}(123) = (321) = (132). \end{aligned}$$

Nähdään siis, että sivuluokan alkiot tuottavat kaikki saman 3-syklin.

Todistetun lauseen seurauksena saadaan nk. *luokkayhtälö*. Numeroidaan äärellisen ryhmän G konjugaattiluokat $A_1, A_2, \ldots, A_m$ ja valitaan jokaisesta luokasta edustaja $x_i \in A_i$. Koska konjugaattiluokan A_i koko on edellisen lauseen mukaan $[G : C_G(x_i)]$ ja konjugaattiluokat muodostavat toisaalta koko ryhmän osituksen, pätee yhtälö

$$|G| = \sum_{k=1}^{m} [G : C_G(x_i)].$$

Koska $\zeta G \leq C_G(x_i)$ kaikilla i, luku $|\zeta G|$ jakaa jokaisen luvun $|C_G(x_i)|$ Lagrangen lauseen mukaisesti. Löytyy siis luvut $k_i \in \mathbb{Z}$, joille $|C_G(x_i)| = k_i \cdot |\zeta G|$ kaikilla i. Nyt kaikilla i pätee

$$[G : \zeta G] = \frac{|G|}{|\zeta G|} = \frac{k_i \cdot |G|}{|C_G(x_i)|} = k_i \cdot [G : C_G(x_i)].$$

Siispä jokainen luku $[G : C_G(x_i)]$ jakaa keskuksen indeksin $[G : \zeta G]$. Lisäksi $x_i \in \zeta G$ jos ja vain jos $G = C_G(x_i)$, jolloin $[G : C_G(x_i)] = 1$. Keskukseen kuuluvat siis täsmälleen ne alkiot, joilla indeksi $[G : C_G(x_i)]$ on 1.

Esitetään luvun lopuksi eräs luokkayhtälön sovellus.

Lemma 4.14. *Jos ryhmän G koko on p^m, missä p on alkuluku ja m nollaa suurempi kokonaisluku, niin G:llä on epätriviaali keskus.*

Todistus. Olkoon ryhmän G konjugaattiluokkien määrä r. Valitaan jokaisesta konjugaattiluokasta edustaja x_i ja merkitään $n_i = [G : C_G(x_i)]$ kaikilla i. Luokkayhtälön mukaan

$$p^m = \sum_{i=1}^{r} n_i.$$

Lagrangen lauseen perusteella jokainen indeksi n_i jakaa koko ryhmän koon p^m. Koska p on alkuluku, täytyy jokaisen luvun n_i olla muotoa p^{k_i} jollain $k_i \in \mathbb{N}$. Jos nyt keskus olisi triviaali, niin löytyisi vain yksi indeksi i, jolla $k_i = 1$. Voidaan olettaa, että kyseinen indeksi on m. Saadaan yhtälö

$$p^m = p \cdot \left(p^{k_1-1} + p^{k_2-1} + \cdots + p^{k_{r-1}-1}\right) + 1.$$

Kyseisen yhtälön vasen puoli on jaollinen p:llä mutta oikea puoli ei. Keskus ei siis voi olla triviaali. $\square$

Lause 4.15. *Jos G on ryhmä ja $|G| = p^2$, missä p on alkuluku, G on vaihdannainen.*

Todistus. Olkoon p alkuluku ja olkoon $|G| = p^2$. Koska G:n keskus on G:n aliryhmä, niin Lagrangen lauseen mukaan $|\zeta G| \in \{1, p, p^2\}$. Edellisen lemman mukaan $|\zeta G| \neq 1$. Täten keskuksen indeksi eli tekijäryhmän $G/\zeta G$ koko on joko 1 tai p. Kummassakin tapauksessa tekijäryhmä on syklinen. Tästä seuraa (todistus harjoitustehtävänä), että G on vaihdannainen. $\square$

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

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

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. Jos kuitenkin vaaditaan, 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 $h^{-1} \in H$, $k^{-1} \in K$ 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.

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 $HK = H \times K$. Lisäksi $H \times K \leq S_5$.

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

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

1) 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. Näin ollen $h_2^{-1}h_1 = e$ ja $k_2k_1^{-1} = e$, mistä nähdään, että $h_1 = h_2$ ja $k_1 = k_2$. Nähtiin, että alkion g esitys on yksikäsitteinen. □

Huomautus 5.6. Aliryhmien sisäinen suora tulo voidaan määritellä myös usemmalle kuin kahdelle aliryhmälle. Määritelmä on aivan samanlainen kuin kahden aliryhmän tapauksessa, ja ehdoiksi tulee

1) $h_ih_j = h_jh_i$ aina, kun $i \neq i$ ja alkiot h_i ja h_j kuuluvat aliryhmiin H_i ja H_j

2) $H_i \cap H_j = \{e\}$ kaikilla aliryhmillä H_i ja H_j, kun $i \neq j$.

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 $\prod_{i=1}^{\infty} H_i$ 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 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 5.7. 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 $G_1 \times G_2$ ja 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 5.8. 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 aikaisempaan 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

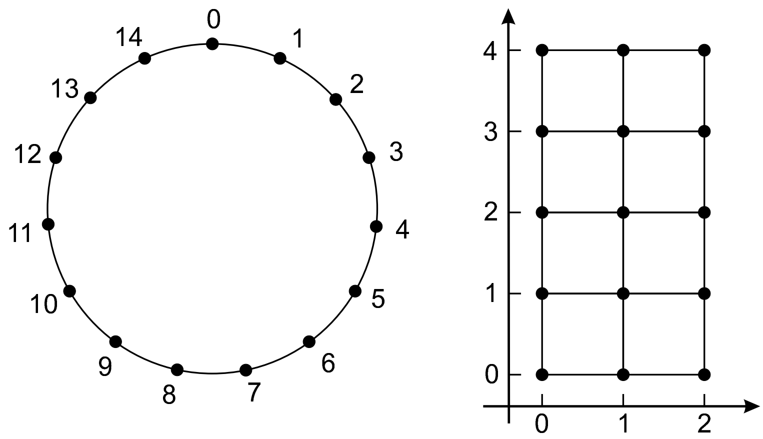
$$\begin{aligned}
2 \cdot (2_3, 2_5) &= (4_3, 4_5) = (1_3, 4_5), \\
3 \cdot (2_3, 2_5) &= (6_3, 6_5) = (0_3, 1_5), \\
4 \cdot (2_3, 2_5) &= (8_3, 8_5) = (2_3, 3_5), \\
5 \cdot (2_3, 2_5) &= (10_3, 10_5) = (1_3, 0_5) \\
&\text{jne.}
\end{aligned}$$

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 erään alkionsa virittämiä.

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

Esimerkki 5.9. 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 tuloryhmässä myös

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



Kuva 16: Kaksi tapaa hahmottaa 15 alkion syklinen ryhmä

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 $n = 2$.