3 Tekijäryhmät

Tekijäryhmän käsitteen avulla voidaan monimutkainen ryhmä jakaa suuriin, helpommin käsiteltäviin osiin. Tämän jälkeen voidaan erikseen tarkastella, miten laskutoimitus vaikuttaa näihin osiin kokonaisuutena, ja jättää hetkeksi huomiotta se, mitä itse asiassa tapahtuu kunkin tällaisen osan sisällä.

3.1 Tekijäryhmän määritelmä

Tekijäryhmän määrittelemistä varten määritellään aluksi sivuluokat ja normaalit aliryhmät.

Määritelmä 3.1. Olkoon G jokin ryhmä, jolla on aliryhmä H. Kullakin alkiolla $g \in G$ määritellään H:n *vasen sivuluokka*

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

Vastaavasti voidaan määritellä *oikea sivuluokka* $Hg = \{hg \mid h \in H\}$.

Sivuluokista voidaan tehdä heti määritelmän perusteella muutamia havaintoja. Ensinnäkin $eH = H$, jos e on ryhmän G neutraalialkio. Aliryhmä on siis itse yksi sivuluokistaan. Toisaalta, koska $e \in H$, kaikilla $g \in G$ pätee $g = g \cdot e \in gH$. Jokainen ryhmän alkio siis kuuluu johonkin sivuluokkaan, eli sivuluokat *peittävät* koko ryhmän G. Nämä havainnot pätevät yhtä hyvin vasemmille kuin oikeillekin sivuluokille.

Esimerkki 3.2. Tarkastellaan ryhmää $(\mathbb{Z}, +)$ ja sen aliryhmää

$$4\mathbb{Z} = \{n \in Z \mid n \text{ on jaollinen 4:llä}\}.$$

Etsitään sivuluokat havainnoimalla. Ensinnäkin yksi sivuluokista on $0 + 4\mathbb{Z} = 4\mathbb{Z} = \{\dots, -4, 0, 4, 8, 12, \dots\}$. (Huomaa, että kun ryhmän laskutoimituksena on yhteenlasku, sivuluokkamerkinnässäkin on kertomerkin sijaan +-merkki.)

Muut sivuluokat saadaan lisäämällä eri lukuja aliryhmän $4\mathbb{Z}$ alkioihin:

$$\begin{aligned}
1 + 4\mathbb{Z} &= \{\dots, -3, 1, 5, 9, 13, \dots\} \\
2 + 4\mathbb{Z} &= \{\dots, -2, 2, 6, 10, 14, \dots\} \\
3 + 4\mathbb{Z} &= \{\dots, -1, 3, 7, 11, 15, \dots\} \\
4 + 4\mathbb{Z} &= \{\dots, 0, 4, 8, 12, 16, \dots\} \\
&\vdots
\end{aligned}$$

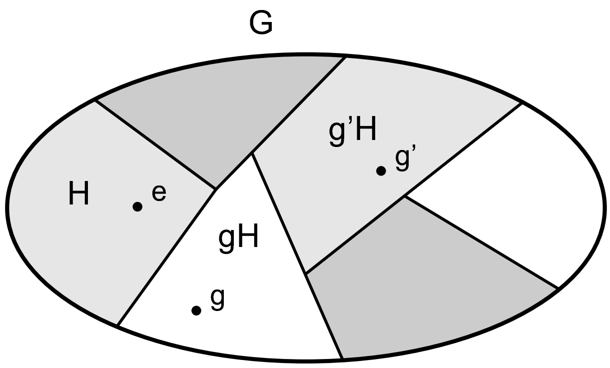
Huomataan, että $4 + 4\mathbb{Z}$ on sama joukko kuin $4\mathbb{Z}$ ja että sivuluokkia ei enää tulee lisää, vaikka kokeiltaisiin uusilla luvuilla: esimerkiksi $13 + \mathbb{Z}$ on sama joukko kuin $1 + \mathbb{Z}$. Jokainen kokonaisluku näyttää nyt kuuluvan johonkin neljästä sivuluokasta $4\mathbb{Z}$, $1 + 4\mathbb{Z}$, $2 + 4\mathbb{Z}$ ja $3 + 4\mathbb{Z}$, ja jokainen näistä sivuluokista sisältää eri lukuja kuin toiset.

Edellisessä esimerkissä huomattiin, että eri sivuluokat eivät sisältäneet samoja alkioita. Tämä on itse asiassa yleinen sääntö, joka voidaan osoittaa esimerkiksi seuraavasti: oletetaan, että $x \in g_1H \cap g_2H$ eli että $x = g_1h_1$ ja $x = g_2h_2$ joillain $h_1, h_2 \in H$. Tällöin $g_1 = xh_1^{-1}$, ja kaikilla $h' \in H$ pätee

$$g_1h' = xh_1^{-1}h' = g_2\underbrace{h_2h_1^{-1}h'}_{\in H} \in g_2H,$$

joten $g_1H \subset g_2H$. Samalla tavoin nähdään myös, että $g_2H \subset g_1H$. Siispä aina pätee joko $g_1H = g_2H$ tai $g_1H \cap g_2H = \emptyset$.

Jonkin aliryhmän vasemmat tai oikeat sivuluokat muodostavat siis koko ryhmän osituksen (ks. kuva 6). Tarkoituksena olisi nyt unohtaa sivuluokkien varsinainen sisältö ja tutkia sitä, miten laskutoimitus kohtelee näitä sivuluokkina kokonaisuutena. Olisi siis tarkoitus laskea *kokonaisten sivuluokkien tuloja* $g_1H \cdot g_2H$. Tällainen tulo on joukko, joka sisältää kaikki sellaiset alkiot $g_1h_1g_2h_2$, joille pätee $h_1, h_2 \in H$. Kyseessä on sama joukko kuin $g_1 \cdot (Hg_2) \cdot H$, eli H:n *oikean* sivuluokan Hg_2 alkiot kerrottuina vasemmalta alkiolla g_1 ja oikealta kaikilla aliryhmän H alkioilla.



Kuva 6: Aliryhmän H sivuluokat

Ongelmana on nyt se, että joukko $g_1H \cdot g_2H$ ei välttämättä ole itse sivuluokka. Tällaisessa tapauksessa ei kokonaisiin sivuluokkiin rajoittumisesta olisi paljon iloa, kun sivuluokkien joukko ei olisi suljettu niiden laskutoimituksen suhteen. Ongelma kuitenkin ratkeaa, mikäli H:n vasemmat ja oikeat sivuluokat ovat samoja. Tällöin nimittäin pätee

$$g_1H \cdot g_2H = g_1 \cdot (Hg_2) \cdot H = g_1 \cdot (g_2H) \cdot H = (g_1g_2)H \cdot H = (g_1g_2)H,$$

ja näin ollen osien g_1H ja g_2H tuloksi tulee yksinkertaisesti osa $(g_1g_2)H$.

Määritelmä 3.3. Ryhmän G aliryhmää H kutsutaan *normaaliksi aliryhmäksi*, mikäli H:n vasemman- ja oikeanpuoleiset sivuluokat ovat samat eli kaikilla $g \in G$ pätee $gH = Hg$. Jos H on G:n normaali aliryhmä, merkitään $H \trianglelefteq G$.

Huom. Jos ryhmä on vaihdannainen, sen jokainen aliryhmä on normaali, sillä on aivan sama, kertooko g aliryhmän alkioita vasemmalta vai oikealta puolelta.

Seuraava lause antaa helposti tarkistettavan kriteerin sille, onko jokin aliryhmä normaali vai ei.

Lause 3.4. *Olkoon G ryhmä ja H sen aliryhmä. Aliryhmä H on normaali täsmälleen silloin, kun kaikilla $g \in G$ pätee $gHg^{-1} \subset H$ eli*

$$ghg^{-1} \in H \quad \textit{jokaisella } h \in H.$$

Todistus. Ryhmä on normaali, jos kaikilla $g \in G$ pätee $gH = Hg$. Kun yhtälön molemmilla puolilla olevien joukkojen alkiot kerrotaan oikealta g:n käänteisalkiolla, saadaan joukkoyhtälö $H = gHg^{-1}$. Tämä yhtälö pätee siis kaikilla $g \in G$ täsmälleen silloin, kun H on normaali. Tästä nähdään heti, että jos H on normaali, niin myös $gHg^{-1} \subset H$ pätee kaikilla $g \in G$.

Oletetaan sitten, että $g^{-1}Hg \subset H$ pätee kaikilla $g \in G$. Olkoot $h \in H$ ja $g \in G$. Nyt myös $g^{-1} \in G$, joten oletuksen mukaan $g^{-1}h(g^{-1})^{-1} = g^{-1}hg \in H$. Edelleen

$$h = g\underbrace{g^{-1}hg}_{\in H}g^{-1} \in gHg^{-1},$$

mistä seuraa, että $H \subset gHg^{-1}$. Näin ollen $H = gHg^{-1}$ kaikilla $g \in G$, ja H on normaali. □

Esimerkki 3.5. Ryhmä S_3 koostuu kuudesta alkiosta: (12), (23), (13), (123), (132) ja id. Tarkistetaan, onko aliryhmä $H = \langle(123)\rangle = \{\mathrm{id}, (123), (132)\}$ normaali. Lasketaan sitä varten muotoa ghg^{-1} olevat tulot, missä $h \in H$. Niissä tapauksissa, joissa $g \in H$ tai $h = \mathrm{id}$, tulo kuuluu selvästi aliryhmään H. Toisaalta silloin, kun $g \notin H$, alkio g on vaihto, joten $g^{-1} = g$. Laskettavat tulot ovat siis itse asiassa muotoa ghg. Saadaan

$$\begin{aligned} &(12)(123)(12) = (132), \qquad && (12)(132)(12) = (123) \\ &(23)(123)(23) = (132), && (23)(132)(23) = (123) \\ &(13)(123)(13) = (132), && (13)(132)(13) = (123). \end{aligned}$$

Koska jokainen tulo ghg^{-1} kuuluu aliryhmään H, kyseinen aliryhmä on normaali.

Olkoon nyt $H' = \langle (12) \rangle = \{\mathrm{id}, (12)\}$. Tämä aliryhmä ei ole normaali, sillä esimerkiksi

$$(123)(12)(123)^{-1} = (123)(12)(321) = (23) \notin H'.$$

Määritelmä 3.6. Olkoon $H \trianglelefteq G$. Ryhmää, jonka alkioita ovat sivuluokat gH, missä $g \in G$, kutsutaan *tekijäryhmäksi.* Tekijäryhmää merkitään G/H, ja sen laskutoimitus noudattaa sääntöä $g_1H \cdot g_2H = (g_1g_2)H$. Tekijäryhmän alkioita voidaan merkitä myös $gH = [g]$, jolloin laskusäännöksi tulee $[g_1][g_2] = [g_1g_2]$.

Esimerkki 3.7. Koska ryhmä $(\mathbb{Z}, +)$ on vaihdannainen, sen kaikki aliryhmät ovat normaaleja. Tutkitaan tekijäryhmää $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$. Tämän tekijäryhmän alkiot ovat aiemmassa esimerkissä määritetyt neljä sivuluokkaa $\mathbb{Z} = [0]$, $1 + \mathbb{Z} = [1]$, $2 + \mathbb{Z} = [2]$ ja $3 + \mathbb{Z} = [3]$. Kyseessä on siis äärellinen 4 alkion ryhmä. Tekijäryhmän laskutoimituksen määritelmän mukaan esimerkiksi $[1] + [2] = [1 + 2] = [3]$ ja $[3] + [4] = [7] = [3]$, missä viimeinen yhtäsuuruus tulee siitä, että sivuluokat $7 + \mathbb{Z}$ ja $3 + \mathbb{Z}$ ovat sama joukko. Laskemalla kaikki mahdolliset summat voidaan muodostaa tekijäryhmän *laskutoimitustaulu*:

$$\begin{array}{c|cccc} + & [0] & [1] & [2] & [3] \\ \hline [0] & [0] & [1] & [2] & [3] \\ [1] & [1] & [2] & [3] & [0] \\ [2] & [2] & [3] & [0] & [1] \\ [3] & [3] & [0] & [1] & [2] \end{array}.$$

3.2 Rubikin ryhmä jako paikkojen ja asentojen mukaan

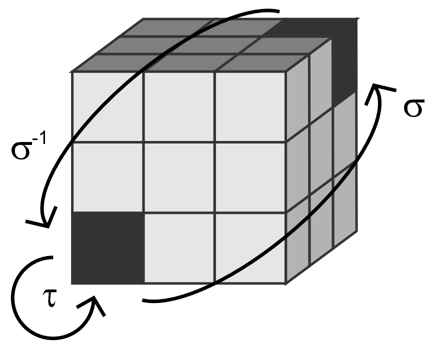
Tarkastellaan sellaista Rubikin ryhmän osajoukkoa $\mathbb{R}_a$, jonka permutaatiot pitävät kuution jokaisen palan paikallaan, vaikka voivatkin muuttaa niiden asentoa.

Lause 3.8. *Osajoukko $\mathbb{R}_a$ on Rubikin ryhmän normaali aliryhmä.*

Todistus. Helposti nähdään, että $\mathbb{R}_a$ on Rubikin ryhmän aliryhmä. Jos nimittäin permutaatiot σ ja τ pitävät kaikki kuution palat paikoillaan, myös niiden yhdistelmä $\sigma\tau$ pitää palat paikoillaan. Toisaalta identtinen permutaatio pitää palat paikoillaan, ja jos σ ei liikuta paloja, ei myöskään käänteiskuvaus σ^{-1} liikuta niitä.

Osoitetaan sitten, että aliryhmä $\mathbb{R}_a$ on normaali käyttämällä aiemmin todistettua kriteeriä 3.4. Olkoot $\tau \in \mathbb{R}_a$ ja $\sigma \in \mathbb{R}$. Tarkastellaan yhdistelmää $\sigma\tau\sigma^{-1}$ siltä kannalta, liikuttaako se paloja vai ei.

Jos σ siirtää jonkin palan paikasta A paikkaan B, niin σ^{-1} siirtää kyseisen palan takaisin paikasta B paikkaan A. Koska τ puolestaan pitää tuon palan paikallaan kohdassa A, ei yhdistelmä liikuta lainkaan kyseistä palaa (ks. oheinen kuva). Sama päättely voidaan tehdä jokaisen palan kohdalla, joten yhdistelmä ei liikuta paloja. Näin ollen $\sigma\tau\sigma^{-1} \in \mathbb{R}_a$, ja $\mathbb{R}_a$ on normaali. $\square$



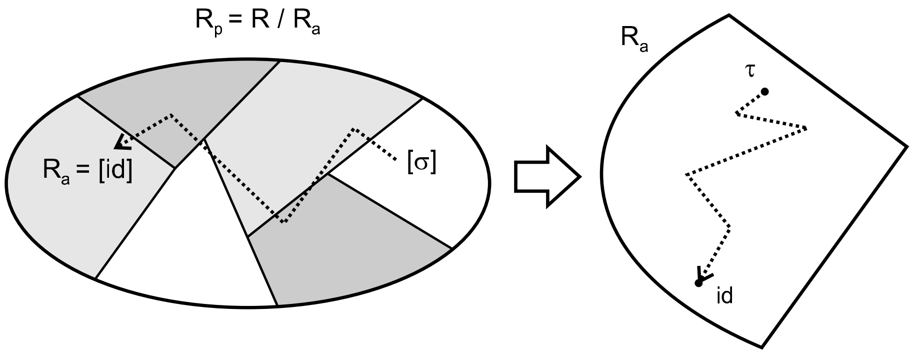
Kuva 7: Yhdistelmä $\sigma\tau\sigma^{-1}$ ei siirrä paloja

Kutsutaan aliryhmää $\mathbb{R}_a$ *Rubikin asentoryhmäksi*. Koska asentoryhmä on normaali, voidaan määritellä tekijäryhmä $\mathbb{R}_p = \mathbb{R}/\mathbb{R}_a$. Tätä tekijäryhmää kutsutaan puolestaan *Rubikin paikkaryhmäksi*. Tekijäryhmän alkiot ovat sivuluokkia $[\sigma]$. Aina kun $[\sigma_1] = [\sigma_2]$, täytyy päteä $\sigma_1 = \sigma_2 \circ \tau$ jollain $\tau \in \mathbb{R}_a$. Tämä tarkoittaa sitä, että saman sivuluokan alkiot eroavat toisistaan vain jonkin sellaisen siirron verran, joka ei muuta palojen paikkoja. Tekijäryhmä voidaan nähdä permutaatioryhmänä, jonka alkiot permutoivat kuution *paloja* niiden asennoista välittämättä.

Yllä kuvatun jaon merkitys on siinä, että sen avulla voidaan hetkeksi unohtaa, missä asennoissa kuution palat ovat, ja keskittyä palojen liikuttamiseen. Kuution ratkaisemiseksi olisi annetusta asemasta σ lähtien löydettävä perussiirtojen ketju, joka palauttaisi kuution perusasemaan id. Edetään ratkaisussa nyt niin, että yritetään ensin palauttaa *paikkaryhmässä* asema $[\sigma]$ asemaksi $[\mathrm{id}]$. Koska $[\mathrm{id}] = \mathbb{R}_a$, niin tässä asemassa kaikki palat ovat jo oikeilla paikoillaan, mutta ne voivat olla vielä väärissä asennoissa. Tämän jälkeen katsotaan tarkemmin, mihin asemaan τ aliryhmässä $\mathbb{R}_a$ ollaan päädytty, ja yritetään palauttaa tämä asema vielä perusasemaksi id. Nämä vaiheet näkyvät kuvassa 8.

3.3 Algoritmi 1: nurkkapalojen 3-sykli

Kuten yllä todettiin, paikkaryhmää $\mathbb{R}_p$ voidaan ajatella kuution palojen permutaatioryhmänä. Kukin sivuluokka $[\sigma]$ vastaa sitä palojen permutaatiota, jonka σ aiheuttaa. Jos kaksi permutaatiota siirtävät paloja samalla tavalla, ne kuuluvat samaan sivuluokkaan.



Kuva 8: Ratkaisun vaiheet

Seuraavaksi kuvattava algoritmi tuottaa 3-syklin palojen paikkoja permutoivassa ryhmässä $\mathbb{R}_p$. Jos kuutio asetetaan siten, että keltainen sivu on katsojaan päin ja sininen sivu ylöspäin, ja keltaisen sivun palat numeroidaan vasemmalta oikealle ja ylhäältä alas keskipalaa lukuunottamatta numeroilla $\{1, \ldots, 8\}$, niin saatava 3-sykli on (316). Se koostuu kahdenlaisista siirroista: ensimmäinen on perussiirto $\sigma = U$ ja toinen kolmen perussiirron yhdistelmä $\tau = RD^{-1}R^{-1}$. Näistä kootaan lopuksi yhdistelmä $\sigma\tau\sigma^{-1}\tau^{-1}$. Kokonaisuudessa siirtosarja on siis seuraavanlainen:

$$(316) = URD^{-1}R^{-1}U^{-1}RDR^{-1}.$$

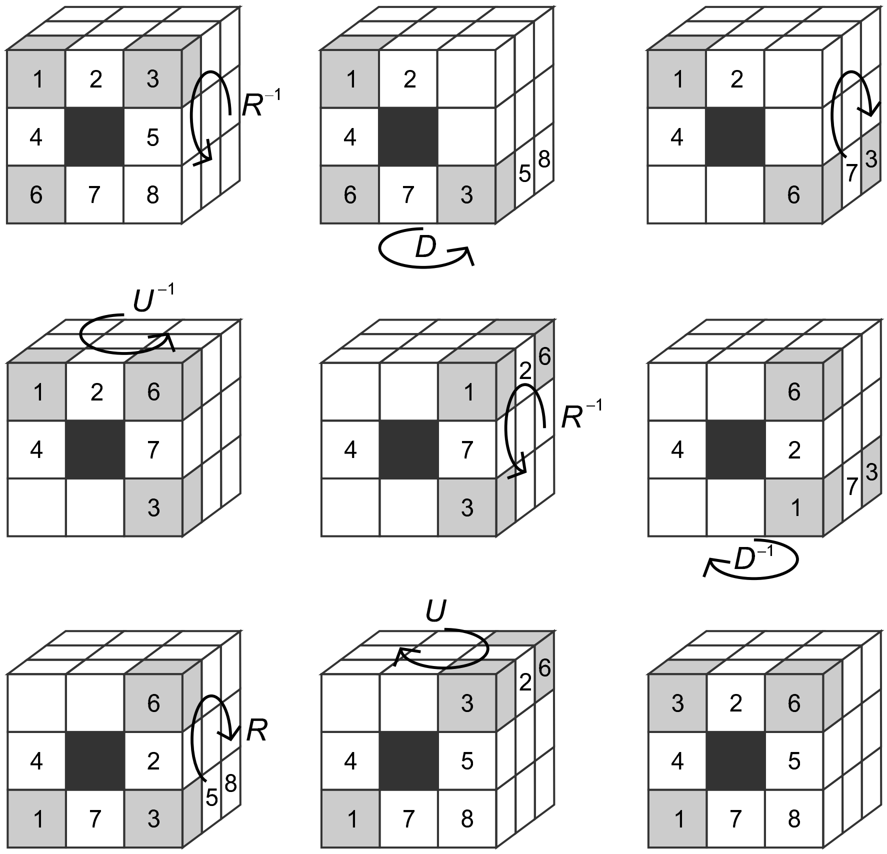
Tämä siirtosarja, kuten kaikki permutaatioiden yhdistelmät, suoritetaan oikealta vasemmalle.

Kuvassa 9 esitetään koko siirtosarja vaihe kerrallaan. Huomaa erityisesti, miten yhdistelmät $\sigma\tau$ ja $\sigma^{-1}\tau^{-1}$ käsittelevät 3-sykliin kuulumattomia paloja. Nämä palat siirtyvät ensin permutaatiossa $\sigma^{-1}\tau^{-1}$ jonnekin, mistä ne sitten palaavat takaisin permutaatiossa $\sigma\tau$. Näiden palojen osalta siis näyttäisi siltä, että kyseiset permutaatiot olisivat toistensa käänteissiirtoja, vaikka tosiasiassa $\sigma^{-1}\tau^{-1} = (\tau\sigma)^{-1} \neq (\sigma\tau)^{-1}$. Permutaatioiden $\tau\sigma$ ja $\sigma\tau$ (tai niiden käänteisalkioiden) ero tulee näkyviin vain 3-sykliin osallistuvissa paloissa. Tästä puhutaan lisää myöhemmin.

Huomaa myös, että permutaatio τ eroaa permutaatiosta τ^{-1} vain siinä, että jälkimmäisessä on perussiirto D, edellisessä D^{-1}. Samaten koko 3-syklin käänteisalkio on

$$(\sigma\tau\sigma^{-1}\tau^{-1})^{-1} = (\tau^{-1})^{-1}(\sigma^{-1})^{-1}\tau^{-1}\sigma^{-1} = \tau\sigma\tau^{-1}\sigma^{-1}.$$

Käänteisalkiossa tehdään siis edelleen ensin käänteispermutaatiot; eroa alkuperäiseen 3-sykliin on siis vain siinä, että σ-permutaatiot tehdään ennen τ-permutaatioita.



Kuva 9: Nurkkapalojen 3-sykli