6. Äärelliset permutaatioryhmät

Luvussa 4 tutustuimme alustavasti permutaatioryhmiin. Äärellisen n alkiosta koostuvan joukon $\{1, 2, \ldots, n\}$ symmetriaryhmälle käytetään yleisesti merkintää

$$S_n = S(\{1, 2, \ldots, n\}).$$

Harjoitustehtävän 36 nojalla minkä tahansa n alkion joukon permutaatioryhmä on isomorfinen ryhmän S_n kanssa. Kaikkia näitä permutaatioryhmiä voidaankin siksi kutsua ryhmäksi S_n vastaavalla tavalla kuin voidaan puhua abstrakteista syklisistä ryhmistä C_n ja C_∞. Äärelliset permutaatioryhmät, joita kutsutaan joskus myös symmetrisiksi ryhmiksi, ovat yllättävän tärkeitä ryhmiä matematiikan eri aloilla, esimerkiksi Galois'n teoriassa, joka käsittelee muunmuassa polynomien algebrallista ratkeavuutta, samoin ne tulevat vastaan geometriassa tarkasteltaessa esimerkiksi säännöllisten monitahokkaiden symmetriaryhmiä.

Luvun aluksi määrittelemme yleisiä käsitteitä, joita havainnollistamme ensin tutuilla ryhmillä:

Määritelmä 6.1. Ryhmän G alkioiden lukumäärä $\#G$ on ryhmän G *kertaluku*. Ryhmän G alkion g *kertaluku* $\operatorname{ord} g$ on sen virittämän syklisen aliryhmän kertaluku, $\operatorname{ord} g = \#\langle g \rangle$.

Lemma 6.2. *Olkoon G ryhmä ja olkoon e ryhmän G neutraalialkio. Tällöin*

$$\operatorname{ord} g = \min\{k \geq 1 : g^k = e\}.$$

Todistus. Harjoitustehtävä 53. □

Esimerkki 6.3. (a) Ryhmien K ja $C_2 \times C_2$ kertaluku on 4 ja niiden jokaisen neutraalialkiosta poikkeavan alkion kertaluku on 2.
(b) Ryhmän $C_4 \cong \mathbb{Z}/4\mathbb{Z}$ kertaluku on 4 ja sen alkioiden [1] ja [3] kertaluku on 4.

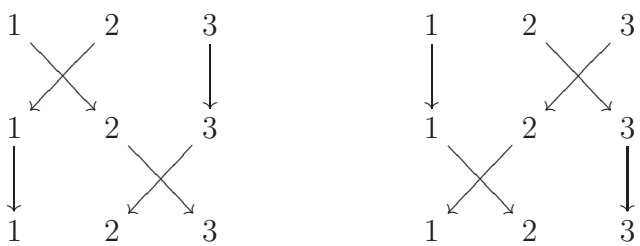
Seuraavat perusominaisuudet on helppo tarkastaa.

Propositio 6.4. *(1) Permutaatioryhmän S_n kertaluku on $n!$.*
(2) Jos $n \geq 3$, niin S_n ei ole kommutatiivinen.

Todistus. (1) Harjoitustehtävä.
(2) Tarkastellaan ensin tapaus $n = 3$. Olkoon $\sigma \in S_3$, $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 3$ ja olkoon $\tau \in S_3$, $\tau(1) = 1$, $\tau(2) = 3$, $\tau(3) = 2$. Tällöin $\tau \circ \sigma(1) = \tau(2) = 3$ ja $\sigma \circ \tau(1) = \sigma(1) = 2$, joten $\sigma \circ \tau \neq \tau \circ \sigma$.

Edellä määritellyt permutaatiot on helppo laajentaa n alkion permutaatioiksi määrittelemällä kaikille $n \geq 4$ permutaatiot $\bar{\sigma}|_{\{1,2,3\}} = \sigma$, $\bar{\tau}|_{\{1,2,3\}} = \tau$, ja $\bar{\sigma}(k) = k = \bar{\tau}(k)$. Näille pätee $\bar{\sigma} \circ \bar{\tau} \neq \bar{\tau} \circ \bar{\sigma}$ kuten tapauksessa $n = 3$. □

Permutaatioilla operointia voi havainnollistaa monilla eri tavoilla. Proposition 6.4 todistuksessa käyttämämme tapa antaa permutaatio luettelemalla kaikkien alkioiden kuvautuminen ei ole kovin kätevää. Esimerkiksi seuraavat kaaviot havainnollistavat Proposition 6.4 todistuksessa esiintyvien permutaatioiden σ ja τ yhdistettyjä kuvauksia $\tau \circ \sigma$ ja $\sigma \circ \tau$:



Yksinkertaistamista varten otamme joillekin permutaatioille käyttöön tiiviimmän merkinnän:

Määritelmä 6.5. Olkoon $\{a_1, a_2, \ldots, a_m\} \subset \{1, 2, \ldots, n\}$ m alkion osajoukko, $m \geq 2$. *Sykli* $(a_1 a_2 \cdots a_m)$ on permutaatio, joka kuvaa alkion a_i alkioksi a_{i+1} kaikilla $i \in \{1, 2, \ldots, m-1\}$, alkion a_m alkioksi a_1 ja on identtinen kuvaus osajoukon $\{a_1, a_2, \ldots, a_m\}$ komplementissa. Syklin $(a_1 a_2 \cdots a_m)$ *pituus* on m. Jos syklin pituus on m, se on *m-sykli*. Jos syklin pituus on 2, niin sitä kutsutaan *vaihdoksi* eli *transpositioksi*. Sanomme 2-sykliä $(i\ i+1)$ *alkeisvaihdoksi* eli *alkeistranspositioksi*.

Syklien yhdistettyä kuvausta merkitään ilman $\circ$-merkkiä: Jos $\sigma = (a_1 a_2 \cdots a_m)$ ja $\tau = (b_1 b_2 \cdots b_k)$, niin

$$\sigma \circ \tau = (a_1 a_2 \cdots a_m)(b_1 b_2 \cdots b_k).$$

Syklien yhdistettyä kuvausta sanotaan niiden *tuloksi*.

Syklit $(a_1 a_2 \cdots a_m)$ ja $(b_1 b_2 \cdots b_k)$ ovat *erilliset*, jos

$$\{a_1, a_2, \ldots, a_m\} \cap \{b_1, b_2, \ldots, b_k\} = \emptyset.$$

Propositiossa 6.4 osoitimme, että ryhmä S_n ei ole kommutatiivinen, kun $n \geq 3$. Vaikka ryhmä G ei olisikaan kommutatiivinen, niin joillekin alkioille $g, h \in G$ pätee $gh = hg$. Tällöin sanotaan, että g ja h kommutoivat.

Lemma 6.6. *Erilliset syklit kommutoivat.*

Todistus. Jos σ ja σ' ovat erillisiä, ne ovat kahden toisiaan leikkaamattoman osajoukon permutaatioita, joten väite pätee selvästi. □

Jos $f\colon X \to X$ on kuvaus ja $x \in X$, niin pisteen x rata (kuvauksella f) on

$$\mathscr{O}(x) = \bigcup_{n \in \mathbb{N}} \{f^n(x)\}.$$

Lemma 6.7. *Jokaisen m-syklin kertaluku on m.*

Todistus. Olkoon $\sigma = (a_1 a_2 \cdots a_m)$. Pisteen a_1 rata

$$\begin{aligned}\mathscr{O}(a_1) &= \{a_1, \sigma(a_1) = a_2, \sigma^2(a_1) = a_3, \ldots, \sigma^{m-1}(a_1) = a_m, \sigma(a_m) = a_1, \ldots\} \\ &= \{a_1, \sigma(a_1) = a_2, \sigma^2(a_1) = a_3, \ldots, \sigma^{m-1}(a_1) = a_m\}\end{aligned}$$

koostuu m pisteestä ja sama pätee kaikille muillekin pisteille $a_2, \ldots, a_m$. Väite seuraa tästä. □

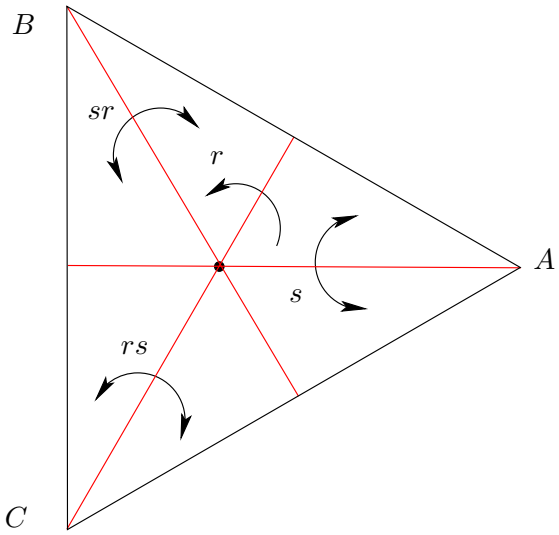
Esimerkki 6.8. (1) Kaikki Proposition 6.4 todistuksessa esintyvät kuvaukset ovat syklejä: $\sigma = (12)$, $\tau = (23)$, $\sigma \circ \tau = (23)(12) = (132)$ ja $\tau \circ \sigma = (23)(12) = (123)$. Loput permutaatioryhmän S_3 alkiot ovat vaihto (13) ja identtinen kuvaus.

(2) Kaikki syklin identtisestä kuvauksesta poikkeavat potenssit eivät välttämättä ole syklejä. Esimerkiksi $(1234)(1234) = (13)(24)$.

Esimerkki 6.9. Jos P_n on säännöllinen n-kulmio tasossa, sen symmetriaryhmä on *diedriryhmä* D_n, jonka virittävät kierto kulman $2\pi/n$ verran keskipisteen ympäri, ja heijastus valitun symmetria-akselin suhteen. Tarkastelemme kahta erikoistapausta, tasasivuista kolmiota ja neliötä.

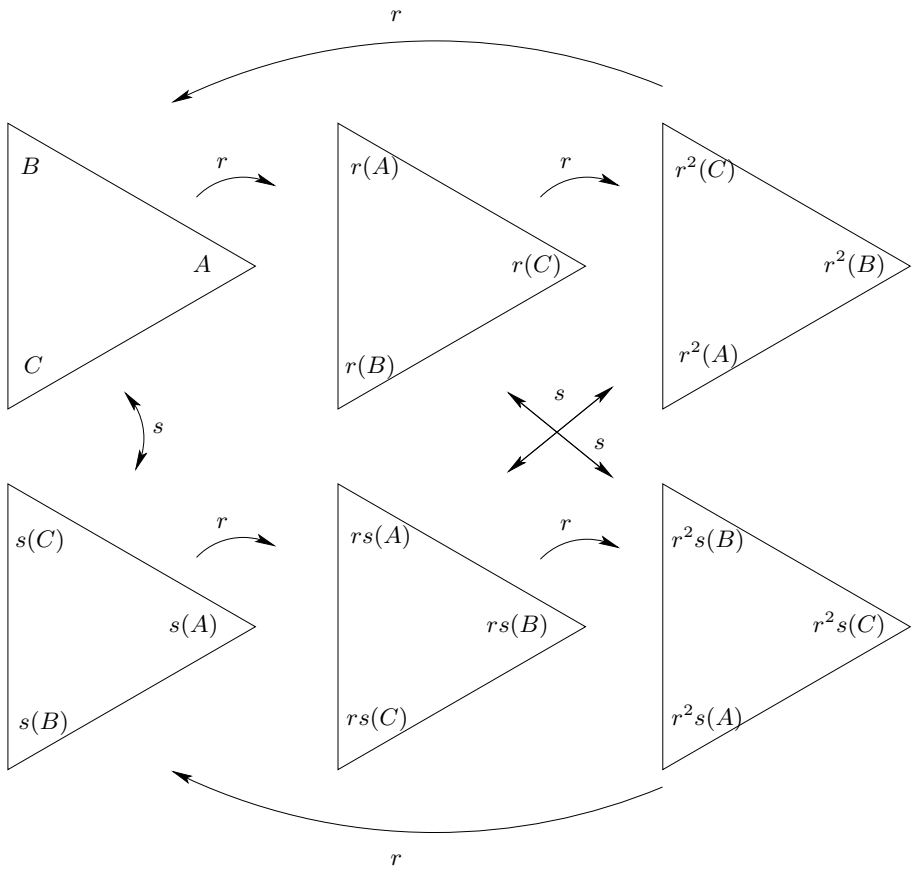
Olkoon P_3 tasasivuinen kolmio, jonka kärjet ovat A, B ja C. Kolmiolla P_3 on kuusi symmetriaa: identtinen kuvaus id, kierto r vastapäivään kulman $2\pi/3$ verran, r^2, joka on kierto kulman $4\pi/3$ verran samaan suuntaan ja peilaukset kunkin kärjen kautta kulkevien kulmanpuolittajasuorien suhteen.

Jos kolmio P_3 ajatellaan kolmiulotteisessa avaruudessa $\mathbb{R}^3$ kaksipuolisena levynä, joka sisältyy tasoon $\mathbb{R}^2 \times \{0\}$, niin kuvaukset id, r ja r^2 kuvaavat kolmion yläpuolen

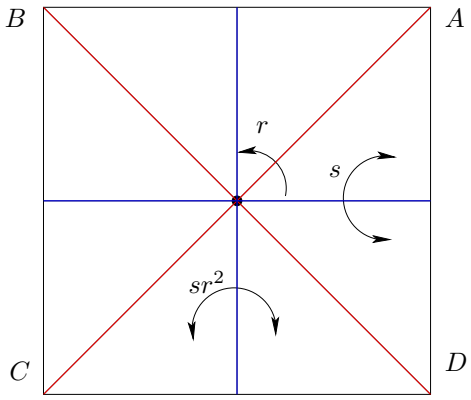


yläpuoleksi ja muut kuvaavat yläpuolen alapuoleksi. Jos s on peilaus kärjen A kautta kulkevan ja vastakkaista sivua vastaan kohtisuoran suoran suhteen, on melko helppo nähdä, että muut peilaukset ovat rs ja sr.

Ryhmä D_3 on isomorfinen permutaatioryhmän S_3 kanssa: Kun rajoitetaan symmetriakuvaukset kolmion P_3 kärkiin, r on 3-sykli (ABC), r^2 on 3-sykli $(ABC)^2 = (ACB)$, s on vaihto (BC), rs on vaihto (AB) ja sr on vaihto (AC).



Säännöllisen n-kulmion symmetriaryhmä D_n on vastaavalla tavalla isomorfinen ryhmän S_n jonkin aliryhmän kanssa. Koska ryhmän D_n kertaluku on $2n$, tämä aliryhmä on permutaatioryhmän S_4 aito aliryhmä. Esimerkiksi neliön symmetriaryhmä D_4 on isomorfinen ryhmän $\langle (1234), (14)(23) \rangle < S_4$ kanssa.



Neliön $P_4 = \{x \in \mathbb{R}^2 : |x_1| \leq 1, |x_2| \leq 1\}$ symmetriat ovat lineaarikuvauksia ja ne voidaan esittää reaalisten 2×2-matriisien avulla:

$$D_4 = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle = \langle r, s \rangle.$$

Jokaisella diedriryhmällä on vastaavanlainen esitys ryhmän $\mathrm{GL}_2(\mathbb{R})$ aliryhmänä.

Yleistämme Esimerkissä 6.9 tehdyn havainnon ja osoitamme, että kaikki ryhmät voi halutessa ajatella permutaatioryhmien aliryhminä, äärettömät ryhmät tietenkin äärettömien joukkojen permutaatioryhmien.

Propositio 6.10. *Ryhmä G on isomorfinen ryhmän $S(G)$ jonkin aliryhmän kanssa.*

Todistus. Olkoon $g \in G$. Kuvaus $\ell_g \colon G \to G$ on surjektio koska $\ell_g(g^{-1}z) = z$ kaikilla $z \in G$ ja supistussäännön nojalla se on injektio. Siis voidaan määritellä kuvaus $\rho \colon G \to S(G)$, $\rho(g) = \ell_g$. Kuvaus ρ on homomorfismi sillä kaikille $x \in G$ pätee

$$\rho(gh)(x) = \ell_{gh}(x) = (gh)x = g(hx) = \ell_g \circ \ell_h(x) = \rho(g) \circ \rho(h)(x).$$

Supistussäännöstä seuraa myös, että Φ on injektio, joten $\Phi \colon G \to \Phi(G) < S(G)$ on isomorfismi. □

Propositio 6.11. *Olkoon G äärellinen ryhmä, jonka kertaluku on n. Permutaatioryhmällä S_n on aliryhmä, joka on isomorfinen ryhmän G kanssa.*

Todistus. Ryhmät S_n ja $S(G)$ ovat isomorfisia, joten voimme käsitellä ryhmää $S(G)$ ja väite seuraa Propositiosta 6.10 □

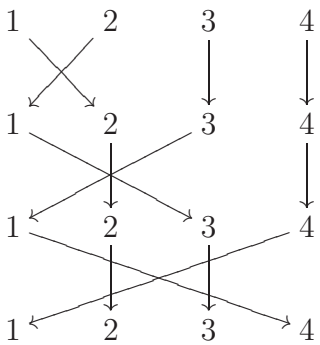
Tarkastelemme seuraavaksi äärellisten permutaatioryhmien rakennetta.

Propositio 6.12. *Jokainen sykli on vaihtojen tulo.*

Todistus. Induktiolla on helppo osoittaa, että

$$(a_1 a_2 \cdots a_m) = (a_1 a_m)(a_1 a_{m-1}) \ldots (a_1 a_2).$$

Todistuksen idea sisältyy seuraavaan kaavioon:



Yksityiskohdat harjoitustehtävässä 59. □

Propositio 6.13. *Jokainen vaihto on alkeisvaihtojen pariton tulo.*

Todistus. Koska harjoitustehtävässä 58 osoitetaan, että $(km) = (1k)(1m)(1k)$ kaikilla $k, m \in \{1, 2, \ldots, n\}$, $k \neq m$, riittää osoittaa, että $(1k)$ on alkeisvaihtojen pariton tulo kaikilla $k \in \{2, 3, \ldots, n\}$. Vaihto (12) on alkeellinen. Oletetaan, että $(1\ k-1)$ on alkeisvaihtojen tulo. Koska $(1k) = (1\ k-1)(k-1\ k)(1\ k-1)$, väite seuraa. □

Propositio 6.14. *Jokainen identtisestä kuvauksesta poikkeava permutaatio voidaan esittää erillisten syklien tulona.*

Todistus. Jos permutaatio τ kiinnittää pisteet $a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n\}$, riittää todistaa väite permutaation τ rajoittumalle joukkoon $\{1, 2, \ldots, n\} \setminus \{a_1, a_2, \ldots, a_k\}$. Riittää siis tarkastella permutaatioita, jotka eivät kiinnitä yhtään pistettä.

Selvästi väite pätee, kun $n = 2$. Oletetaan, että se pätee kaikilla S_k, kun $k \leq n-1$. Olkoon $\tau \in S_n$. Jos τ on sykli ei ole mitään todistettavaa, joten voimme olettaa, että τ ei ole sykli. Pisteen 1 rata on

$$\mathcal{O}(1) = \{1, \tau(1), \tau^2(1), \ldots, \tau^k(1), \ldots\}.$$

Koska $\{1, \ldots, n\}$ on äärellinen joukko täytyy olla $\tau^q(1) = \tau^r(1)$ joillain luonnollisilla luvuilla $q < r$. Valitaan luvut q ja r siten, että q on minimaalinen. Koska τ on bijektio, täytyy olla $q = 0$, $\tau^r(1) = 1$. Tästä nähdään, että

$$\tau|_{\mathcal{O}(1)} = (1\ \tau(1)\ \tau^2(1) \cdots \tau^{r-1}(1)).$$

Induktio-oletuksesta seuraa, että permutaation τ rajoittuma pienempään joukkoon $\{1, 2, \ldots, n\} \setminus \mathcal{O}(1)$ on syklien tulo, joten väite on todistettu. □

Propositioista 6.12, 6.13 ja 6.14 saadaan

Lause 6.15. *(Alkeis)vaihdot virittävät permutaatioryhmän.* □

Jokaiseen permutaatioon liittyvä tärkeä invariantti on permutaation merkki:

Määritelmä 6.16. Permutaatio $\sigma \in S_n$ on *parillinen*, jos se on tulo parillisesta määrästä vaihtoja ja *pariton*, jos se on tulo parittomasta määrästä vaihtoja. Permutaation σ *merkki* on

$$\epsilon(\sigma) = \begin{cases} -1, & \text{jos } \sigma \text{ on pariton} \\ 1, & \text{jos } \sigma \text{ on parillinen.} \end{cases}$$

Seuraavassa tuloksessa osoitetaan muunmuassa, että permutaation merkki on hyvin määritelty kuvaus. Apuna käytetään antisymmetrisiä kuvauksia: Olkoon X epätyhjä joukko ja olkoon $(V, +)$ additiivinen ryhmä. Kuvaus $f\colon X^n \to V$ on *antisymmetrinen*, jos kaikille alkeistranspositioille $\tau \in S_n$ pätee

$$f(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) = -f(x).$$

Propositio 6.17. *Olkoon $f\colon X^n \to V$ antisymmetrinen kuvaus. Tällöin*

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = (-1)^r f(x),$$

jos σ on r alkeistranspositon tulo.

Todistus. Väite pätee selvästi, kun $r = 1$. Oletetaan, että se pätee, kun σ on $r-1$ alkeispermutaation tulo. Olkoon $\sigma = \tau \circ \omega$ permutaatio, joka on r alkeistranspositon tulo siten, että ω on $r-1$ alkeistranspositon tulo ja τ on alkeistranspositio.

Nyt soveltamalla antisymmetrisyyden määritelmää alkeistranspositiolla τ ja pisteellä $(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$ saadaan

$$\begin{aligned} f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) &= f(x_{\tau(\omega(1)}, x_{\tau(\omega(2))}, \ldots, x_{\tau(\omega(n))}) \\ &= -f(x_{\omega(1)}, x_{\omega(2)}, \ldots, x_{\omega(n)}) = (-1)^r f(x) \,. \end{aligned}$$ □

Proposition 6.13 avulla saadaan välittömästi

Seuraus 6.18. *Jos f on antisymmetrinen, niin kaikille transpositioille $\tau \in S_n$ pätee*

$$f(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) = -f(x) \,.$$ □

Propositio 6.19. *Permutaation merkki on hyvin määritelty.*

Todistus. Kuvaus $f\colon \mathbb{Z}^n \to \mathbb{Z}$,

$$f(x) = \prod_{1 \le i < j \le n} (x_i - x_j)$$

on antisymmetrinen (Harjoitustehtävä 61). Lisäksi, kun muuttujan x komponentit ovat eri kokonaislukuja, $f(x) \neq 0$. Jos permutaatio σ voidaan esittää r ja s permutaation tulona, saadaan Proposition 6.17 nojalla $(-1)^r = (-1)^s$, joten $r \equiv s \mod 2$. □

Lause 6.20. *Permutaation merkki $\epsilon\colon S_n \to \{-1, 1\}$ on ainoa homomorfismi permutaatioryhmästä S_n multiplikatiiviseen ryhmään $\{-1, 1\}$, joka saa transpositioilla arvon -1.*

Todistus. Harjoitustehtävässä 62 osoitetaan, että ϵ on homomorfismi. Proposition 6.17 nojalla $\epsilon(\tau) = -1$ kaikille vaihdoille, joten merkki on halutunlainen homomorfismi. Toisaalta alkeisvaihdot virittävät koko permutaatioryhmän, joten, jos homomorfismin arvot tunnetaan kaikille alkeisvaihdoille, sen arvot kiinnittyvät kaikille permutaatioille. Siis ϵ on ainoa homomorfismi, jolla on haluttu ominaisuus. □

Permutaatioiden merkkihomomorfismin $\epsilon\colon S_n \to \{-1, 1\}$ ydin on *alternoiva ryhmä* A_n, joka koostuu parillisista permutaatioista.

Esimerkki 6.21. (a) $A_3 = \langle (123) \rangle < S_3$, $A_3 \cong C_3$.
(b) $A_4 = \langle (123), (124), (134), (234), (12)(34), (13)(24), (14)(23) \rangle < S_4$.
(c) Permutaatiot esiintyvät lineaarialgebrassa determinanttien yhteydessä: Neliömatriisin $A = (a_{ij})_{i=1}^n$ determinantti on

$$\det A = \sum_{\sigma \in S_n} \epsilon(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n} \,.$$

Jos neliömatriisien vektoriavaruus M_n samastetaan avaruudeksi $(\mathbb{R}^n)^n$ esittämällä matriisi $A \in M_n$ sarakkeidensa tai riviensä avulla muodossa

$$A = \begin{pmatrix} v_1 \cdots v_n \end{pmatrix} = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix},$$

niin determinantti on antisymmetrinen kuvaus $\det\colon (\mathbb{R}^n)^n \to \mathbb{R}$:

$$\det(v_{\sigma(1)}\ v_{\sigma(2)} \cdots v_{\sigma(n)}) = \det \begin{pmatrix} w_{\sigma(1)} \\ w_{\sigma(2)} \\ \vdots \\ w_{\sigma(n)} \end{pmatrix} = \epsilon(\sigma) \det A.$$

Harjoitustehtäviä.

Tehtävä 52. Osoita, että permutaatioryhmän S_n kertaluku on $n!$.

Tehtävä 53. Olkoon G ryhmä ja olkoon e ryhmän G neutraalialkio. Osoita, että

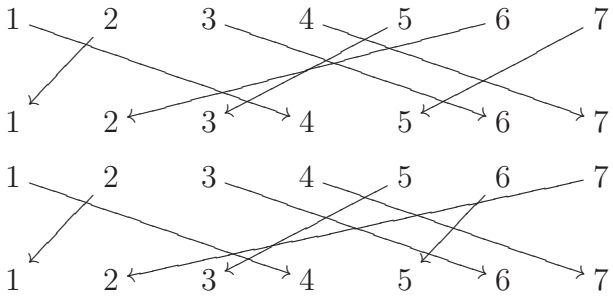
$$\operatorname{ord} g = \min\{k \geq 1 : g^k = e\}.$$

Tehtävä 54. Määritä matriisien $A, B, C \in \mathrm{SL}_2(\mathbb{Z})$ kertaluvut, kun

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ ja } C = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Tehtävä 55. Kirjoita permutaatio $(123)(24)$ syklinä.

Tehtävä 56. Kirjoita kaavioita



vastaavat permutaatiot erillisten syklien tuloina.

Tehtävä 57. Kirjoita permutaatio $(1234)(235)$ erillisten syklien tulona.

Tehtävä 58. Osoita, että $(km) = (1k)(1m)(1k)$.

Tehtävä 59. Täydennä Proposition 6.12 todistus induktiotodistukseksi.

Tehtävä 60. Osoita, että $S_3 = \langle (12), (23) \rangle$

Tehtävä 61. Osoita, että kuvaus $f\colon \mathbb{Z}^n \to \mathbb{Z}$,

$$f(x) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

on antisymmetrinen.

Tehtävä 62. Osoita, että permutaation merkki $\epsilon\colon S_n \to \{-1, 1\}$ on homomorfismi.

———

Olkoon seuraavissa tehtävissä

$$B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \right\}.$$

Tehtävä 63. Osoita, että joukko B varustettuna matriisien kertolaskulla on ryhmän $\mathrm{GL}_2(\mathbb{Q})$ aliryhmä. Onko B ryhmän $\mathrm{SL}_2(\mathbb{Z})$ aliryhmä?

Tehtävä 64. Onko ryhmä B kommutatiivinen? Onko se syklinen? Luettele kaikki ryhmän B aliryhmät.

Tehtävä 65. Osoita, että ryhmä B on isomorfinen permutaatioryhmän S_3 kanssa.

[65] Vihje: Homomorfismi $\phi\colon S_3 \to B$ määräytyy arvoista $\phi((12))$ ja $\phi((23))$. Koska $(12)(12) = (23)(23) = \mathrm{id}$, täytyy olla $\phi((12))^2 = \phi((23))^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.