Tampereen yliopisto

Selina Hakala

PUOLIRYHMISTÄ

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Huhtikuu 2022

Tiivistelmä

Selina Hakala: Puoliryhmistä
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastollisen data-analyysin kandidaattiohjelma
Huhtikuu 2022

Tässä kandidaatintutkielmassa perehdytään puoliryhmiin ja joihinkin niiden ominaisuuksiin määritelmien, lauseiden ja niiden todistusten sekä esimerkkien avulla. Puoliryhmä on epätyhjän joukon ja liitännäisen laskutoimituksen muodostama pari. Pari voi olla esimerkiksi luonnolliset luvut ja kertolasku. Koska kertolasku on liitännäinen laskutoimitus, nämä muodostavat puoliryhmän. Jos puoliryhmässä on neutraalialkio, sitä kutsutaan monoidiksi. Jos taas monoidissa kaikilla alkioilla on käänteisalkio, se on ryhmä.

Puoliryhmän nolla-alkion sekä minkä tahansa muun puoliryhmän alkion tulo on nolla-alkio ja idempotenttialkion neliö on idempotenttialkio. Supistussääntö toteaa, että puoliryhmä on supistuva, jos siitä että sen kaksi alkiota kerrottuna kolmannella alkiolla ovat yhtä suuret seuraa, että myös nämä kaksi alkiota ovat yhtä suuret. Puoliryhmän alipuoliryhmä on kyseisen puoliryhmän joukon osajoukon sekä sen laskutoimituksen muodostama puoliryhmä.

Homomorfismi on kuvaus, joka käytännössä antaa toisen puoliryhmän tulon siirtämällä alkiot toiseen puoliryhmään. Jos kuvaus on homomorfismin lisäksi myös bijektio, se on isomorfismi. Lisäksi kuvaus on automorfismi, jos se on isomorfismi, jonka määrittely- ja arvojoukko ovat sama joukko.

Kaikkien kuvausten joukko joukolta itselleen on kyseisen joukon symmetrinen puoliryhmä. Tähän liittyy Cayleyn lause, jonka vastine puoliryhmille toteaa, että jokainen puoliryhmä on isomorfinen symmetrisen puoliryhmän kanssa. Suora tulo yhdistää kahden puoliryhmän laskutoimitukset siten, että syntyy uusi puoliryhmä, jolla on molempien puoliryhmien ominaisuudet.

Ekvivalenssirelaatio jakaa määrittelyjoukon ekvivalenssiluokkiin. Kongruenssin ekvivalenssiluokkaa kutsutaan kongruenssiluokaksi. Osamääräpuoliryhmä supistaa kunkin kongruenssiluokan yhdeksi elementiksi.

Avainsanat: puoliryhmä, alipuoliryhmä, homomorfismi, isomorfismi, tulopuoliryhmä, osamääräpuoliryhmä

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -ohjelmalla.

Sisällys

1 Johdanto **5**

2 Puoliryhmä **6**

2.1 Puoliryhmän määritelmä 6

2.2 Monoidi ja ryhmä 7

2.3 Nolla- ja idempotenttialkiot 8

2.4 Alipuoliryhmä 10

2.5 Homomorfismi 10

2.6 Isomorfismi ja upotus 11

2.7 Symmetrinen puoliryhmä 13

2.8 Tulo- ja osamääräpuoliryhmät 15

Lähteet **18**

1 Johdanto

Tässä tutkielmassa perehdytään puoliryhmiin ja niiden joihinkin ominaisuuksiin. Luvussa 2.2 määritellään myös monoidi ja ryhmä. Nämä ovat algebrallisia rakenteita, joiden laskutoimituksilla voi olla erilaisia ominaisuuksia. Lukijan odotetaan ymmärtävän peruslaskutoimitusten lisäksi joukko-opin perustiedot.

Ensin esitellään merkintöjä ja määritellään puoliryhmä, kerrotaan joistain sen ominaisuuksista sekä annetaan siitä muutama esimerkki. Myöhemmin tutkielmassa esitellään muun muassa monoidi ja ryhmä sekä nolla- ja idempotenttialkiot, jotka liittyvät puoliryhmän ominaisuuksiin.

Lopussa määritellään vielä puoliryhmän homomorfismi, isomorfismi, symmetrinen puoliryhmä sekä tulo- ja osamääräpuoliryhmät.

Tutkielmassa päälähteenä tutkielmassa käytetään Tero Harjun teosta *Lecture Notes on Semigroups*, 1996. Lisäksi lähteinä on käytetty Bernard Kolmanin, Robert C. Busbyn ja Sharon Cutler Rossin teoksen *Discrete Mathematical Structures* kolmatta versiota vuodelta 1996 sekä Thomas W. Judsonin teosta *Abstract Algebra Theory and Applications*, 2020.

2 Puoliryhmä

Tämä luku perustuu pääsääntöisesti Tero Harjun teokseen *Lecture Notes on Semigroups*, 1996 [1, s. 1–14]. Muun lähteen käyttö on merkitty erikseen.

2.1 Puoliryhmän määritelmä

Olkoon S epätyhjä joukko ja $*\colon S \times S \to S$ binäärinen kuvaus, joka kuvaa jokaisen järjestetyn parin $(x, y) \in S \times S$ joukon S alkioksi $x * y$. Paria $(S, *)$ kutsutaan groupoidiksi. Kuvausta $*$ kutsutaan parin $(S, *)$ tuloksi. Tulo ei siis välttämättä aina tarkoita kertolaskun tuloa, vaan sillä voidaan tarkoittaa minkä tahansa laskutoimituksen tuloa. Jos ei ole vaaraa sekaannukseen, paria $(S, *)$ voidaan merkitä yksinkertaisemmin S ja alkiota $x * y$ voidaan merkitä xy. Alkio xy on siis alkioiden $x \in S$ ja $y \in S$ tulo.

Määritelmä 2.1. Groupoidi S on *puoliryhmä*, jos laskutoimitus $*$ on liitännäinen: kaikilla $x, y, z \in S$,

$$x * (y * z) = (x * y) * z.$$

Käytännössä siis liitännäisen laskutoimituksen järjestyksellä ei ole väliä ja sulut voidaan poistaa myös kokonaan.

Merkitään x^n on alkion $x \in S$ tulo itsensä kanssa $n \geq 1$ kertaa. Tällöin $x^1 = x$, $x^2 = x * x$ ja $x^{n+1} = x * x^n$ kaikilla $n \geq 1$. Edelleen kaikilla kokonaisluvuilla $n, m \geq 1$, voidaan merkitä $x^n * x^m = x^{n+m}$. (Ks. [3, s. 336, Esimerkki 14.])

Puoliryhmä S on äärellinen, jos sen alkioiden määrä on äärellinen. Lisäksi S on vaihdannainen puoliryhmä, jos sen laskutoimitus $*$ on vaihdannainen: kaikilla $x, y \in S$

$$x * y = y * x.$$

Esimerkki 2.1. Olkoon $\mathbb{N} = \{0, 1, \dots\}$ ei-negatiivisten kokonaislukujen joukko. Tällöin $(\mathbb{N}, *)$ on puoliryhmä tavallisen kokonaislukujen kertolaskun suhteen. Myös $(\mathbb{N}, +)$ on puoliryhmä, kun $+$ on kokonaislukujen tavallinen summa. Määritellään $(\mathbb{N}, \star)$ siten, että

$$n \star m = \min\{n, m\}.$$

Tällöin

$$n \star (m \star k) = \min\{n, \min\{m, k\}\} = \min\{n, m, k\} = \min\{\min\{n, m\}, k\} = (n \star m) \star k,$$

joten $(\mathbb{N}, \star)$ on puoliryhmä.

Esimerkki 2.2. Edellinen tapaus yleistyy myös muilla tutuille lukujoukoille; kokonaisluvuille, rationaaliluvuille, reaaliluvuille ja kompleksiluvuille. $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{C}, \cdot)$ ja $(\mathbb{C}, +)$ ovat siis myös puoliryhmiä, kun laskutoimitukset ovat tavallisia kerto- ja yhteenlaskuja. Kertolaskun tapauksessa määrittelyjoukosta voidaan poistaa nolla-alkio 0 ja saadaan silti puoliryhmä.

Esimerkki 2.3. Edelliset esimerkit yleistyvät myös kolmiomatriisiin

$$S = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| \, n \geq 1 \right\}.$$

Nyt S on puoliryhmä tavallisen matriisitulon suhteen, koska

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot \left(\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & m+k \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & n+(m+k) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m+k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (n+m)+k \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \left(\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \right) \cdot \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}.$$

Kaikki edellä olevien esimerkkien puoliryhmät ovat vaihdannaisia. Kaikki 2×2 matriisien puoliryhmät eivät ole vaihdannaisia kertolaskun suhteen.

Esimerkki 2.4. Olkoon $S = \{a, b, c\}$ kolmen alkion joukko ja määritellään tulo taulukolla

$*$	a	b	c
a	a	b	c
b	b	a	c
c	c	b	c

Nyt S on äärellinen puoliryhmä. Järjestyksessä tarkistamalla pitäisi käydä läpi kaikki kolmikot $x * (y * z) = (x * y) * z$. Tässä tapauksessa joukossa S on joitain helpottavia rajoituksia. Esimerkiksi, jos $z = c$, niin tulo on aina c riippumatta alkioista x ja y.

2.2 Monoidi ja ryhmä

Määritelmä 2.2. Olkoon $(S, *)$ puoliryhmä. Silloin $(S, *)$ on *monoidi*, jos sillä on neutraalialkio $x \in S$ siten, että

$$x * y = y * x = y \qquad \forall y \in S.$$

Lause 2.1. *Puoliryhmän neutraalialkio on yksikäsitteinen.*

Todistus. Tehdään vastaoletus, että $x \in S$ ja $y \in S$ ovat molemmat puoliryhmän S neutraalialkioita. Tällöin määritelmän mukaan

$$y = xy = x. \qquad \square$$

Esimerkki 2.5. Luku 0 on puoliryhmän $(\mathbb{Z}, +)$ neutraalialkio, koska

$$\forall x \in \mathbb{Z} \colon x + 0 = 0 + x = x.$$

Siis puoliryhmä $(\mathbb{Z}, +)$ on monoidi.

(Ks. [3, s. 335, Esimerkki 8.])

Määritelmä 2.3. Olkoon G monoidi, jonka neutraalialkio on x. Silloin G on *ryhmä*, jos jokaiselle $y \in G$ löytyy käänteisalkio $y^{-1} \in G$ siten, että

$$y * y^{-1} = x = y^{-1} * y.$$

Kun laskutoimitus on yhteenlaskun kaltainen, käänteisalkion sijasta puhutaan vasta-alkiosta.

Esimerkki 2.6. Edellisessä esimerkissä 2.5 todettiin, että puoliryhmä $(\mathbb{Z}, +)$ on monoidi, jonka neutraalialkio on 0. Koska lisäksi jokaiselle $x \in \mathbb{Z}$ löytyy vasta-alkio $-x \in \mathbb{Z}$ siten, että

$$x + (-x) = -x + x = 0$$

on $(\mathbb{Z}, +)$ ryhmä.

(Ks. [3, s. 349, Esimerkki 1.])

2.3 Nolla- ja idempotenttialkiot

Määritelmä 2.4. Olkoot S puoliryhmä ja $x \in S$. Nyt x on vasen nolla-alkio, jos

$$\forall y \in S \colon x * y = x.$$

Samoin x on oikea nolla-alkio, jos

$$\forall y \in S \colon y * x = x.$$

Jos x on puoliryhmän S sekä vasen että oikea nolla alkio, se on puoliryhmän S *nolla-alkio*.

Lause 2.2. *Puoliryhmän nolla-alkio yksikäsitteinen.*

Todistus. Tehdään vastaoletus, että sekä $x \in S$ että $y \in S$ ovat puoliryhmän S nolla-alkioita. Nyt

$$x * y = x = y * x = y. \qquad \square$$

Määritelmä 2.5. Olkoon S puoliryhmä. Alkio $e \in S$ on *idempotentti*, jos $e^2 = e$.

Kaikkien idempotenttialkioiden joukkoa puoliryhmässä S merkitään $E = E_s$.

Esimerkki 2.7. Määritellään äärellinen puoliryhmä S kuten esimerkissä 2.4. Alkio a on puoliryhmän S neutraalialkio, ja siten S on monoidi. Alkio c on oikea nolla-alkio ja vasenta nolla-alkiota ei ole, joten puoliryhmällä S ei ole nolla-alkiota. Kumpikin alkioista a ja c ovat idempotentteja, mutta alkio b ei ole, sillä $b^2 = a$.

Esimerkki 2.8. Esimerkin 2.3 matriisipuoliryhmällä ei ole idempotenttialkioita eikä neutraali- tai nolla-alkioita.

Esimerkki 2.9. Määritellään joukon S tulo siten, että

$$\forall x, y \in S\colon x * y = y.$$

Täten saadaan puoliryhmä, jonka jokainen alkio $x \in S$ on sekä vasen neutraalialkio ja oikea nolla-alkio. Lisäksi kaikki tämän puoliryhmän alkioista ovat idempotentteja eli $S = E_s$

Määritelmä 2.6. Puoliryhmä S on vasemmalta supistuva, jos

$$\forall x, y \in S\colon zx = zy \Rightarrow x = y.$$

Samoin S on oikealta supistuva, jos

$$\forall x, y \in S\colon xz = yz \Rightarrow x = y.$$

Jos S on sekä vasemmalta että oikealta supistuva, niin se on *supistuva*.

Esimerkki 2.10. Kaikki ryhmät ovat supistuvia puoliryhmiä.

Esimerkki 2.11. Tarkastellaan matriisipuoliryhmää $\mathbb{Z}^{2\times 2}$. Tällöin

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},$$

joten $\mathbb{Z}^{2\times 2}$ ei ole supistuva. Jos otetaan kuitenkin vain sellaiset matriisit A, joilla $\det(A) = 1$, niin puoliryhmä on supistuva.

2.4 Alipuoliryhmä

Määritelmä 2.7. Olkoon $(S, *)$ puoliryhmä ja olkoon A joukon S epätyhjä osajoukko. Tällöin $(A, *)$ on puoliryhmän $(S, *)$ *alipuoliryhmä*, merkitään $A \leq S$, jos A on suljettu puoliryhmän $(S, *)$ tulon suhteen:

$$\forall x, y \in A \colon x * y \in A,$$

mikä tarkoittaa, että

$$A \leq S \Leftrightarrow A^2 \subseteq A.$$

Alipuoliryhmän laskutoimitus on sama kuin sen emopuoliryhmän laskutoimitus. Siispä, jos A on puoliryhmän S alipuoliryhmä, niin varmasti sen laskutoimitus on liitännäinen, joten A on itsessään puoliryhmä. Lisäksi, jos S on puoliryhmä, se on myös itsensä alipuoliryhmä. (Ks. [3, s. 336, Esimerkki 14.])

Esimerkki 2.12. Tarkastellaan puoliryhmää $S = (\mathbb{R}, \cdot)$. Nyt $(\mathbb{N}, \cdot)$ on puoliryhmän S alipuoliryhmä, koska $\mathbb{N} \subset \mathbb{R}$ ja $\mathbb{N}$ on suljettu kertolaskun suhteen. Puoliryhmä $(\mathbb{N}, +)$ ei ole puoliryhmän S alipuoliryhmä, koska sen laskutoimitus ei ole puoliryhmän S laskutoimitus.

2.5 Homomorfismi

Määritelmä 2.8. Olkoot $(S, *)$ ja $(P, *')$ puoliryhmiä. Kuvaus $\alpha \colon S \to P$ on *homomorfismi*, jos

$$\forall x, y \in S \colon \alpha(x * y) = \alpha(x) *' \alpha(y).$$

Siis homomorfismi antaa puoliryhmän S tulon siirtämällä alkiot puoliryhmään P Homomorfismi voi samaistaa alkiot x ja y: $\alpha(x) = \alpha(y)$.

Esimerkki 2.13. Olkoot $S = (\mathbb{N}, +)$ ja $P = (\mathbb{N}, \cdot)$ ja määritellään $\alpha(n) = 2^n$ kaikilla $n \in \mathbb{N}$. Nyt

$$\alpha(n + m) = 2^{n+m} = 2^n \cdot 2^m = \alpha(n) \cdot \alpha(m),$$

joten $\alpha \colon S \to P$ on homomorfismi.

Esimerkki 2.14. Olkoon S kokonaislukujen puoliryhmä $S = (\mathbb{Z}, \cdot)$ kertolaskun suhteen, ja olkoon P kokonaislukujen puoliryhmä $P = (\mathbb{Z}, +)$ yhteenlaskun suhteen. Määritellään kuvaus $\alpha \colon S \to P$ siten, että $\alpha(n) = n$ kaikilla $n \in \mathbb{Z}$. Tällöin α ei ole homomorfismi, koska $4 = \alpha(4) = \alpha(1 \cdot 4) \neq \alpha(1) + \alpha(4) = 5$.

Lause 2.3. *Jos $\alpha\colon S \to P$ ja $\beta\colon P \to T$ ovat homomorfismeja, niin myös $\beta\alpha\colon S \to T$ on homomorfismi.*

Todistus. Kaikilla $x, y \in S$

$$\beta\alpha(x*y) = \beta(\alpha(x*y)) = \beta(\alpha(x)*\alpha(y)) = \beta(\alpha(x))*\beta(\alpha(y)) = \beta\alpha(x)*\beta\alpha(y). \quad \square$$

Lause 2.4. *Jos $(S, *)$ on vaihdannainen puoliryhmä, $(P, *')$ on puoliryhmä ja kuvaus $\alpha\colon S \to P$ on homomorfismi, myös $(P, *')$ on vaihdannainen.*

Todistus. (Ks. [3, s. 340, Lause 5.])

Olkoot $x_1, x_2 \in S$ ja $y_1, y_2 \in P$ siten, että

$$y_1 = \alpha(x_1) \qquad \text{ja} \qquad y_2 = \alpha(x_2).$$

Edelleen

$$y_1 *' y_2 = \alpha(x_1) *' \alpha(x_2) = \alpha(x_1 * x_2) = \alpha(x_2 * x_1) = \alpha(x_2) *' \alpha(x_1) = y_2 *' y_1. \quad \square$$

2.6 Isomorfismi ja upotus

Homomorfismi $\alpha\colon S \to P$ on

- **upotus**, jos se on injektiivinen eli jos $\alpha(x) = \alpha(y)$ implikoi $x = y$, merkitään $\alpha\colon S \hookrightarrow P$,
- **epimorfismi**, jos se on surjektiivinen eli jos kaikille $y \in P$ on olemassa sellainen $x \in S$, että $\alpha(x) = y$, merkitään $\alpha\colon S \twoheadrightarrow P$,
- **isomorfismi**, jos se on sekä upotus että epimorfismi eli se on bijektio, merkitään $\alpha\colon S \rightarrowtail P$,
- **endomorfismi**, jos $P = S$,
- **automorfismi**, jos se on sekä isomorfismi että endomorfismi.

Lause 2.5. *Jos $\alpha\colon S \to P$ on isomorfismi, niin myös käänteiskuvaus $\alpha^{-1}\colon P \to S$ on isomorfismi.*

Todistus. Ensinnäkin käänteiskuvaus α^{-1} on olemassa, koska α on bijektio. Lisäksi $\alpha\alpha^{-1} = e$, ja siten koska α on homomorfismi, niin

$$\alpha(\alpha^{-1}(x) * \alpha^{-1}(y)) = \alpha(\alpha^{-1}(x)) *' \alpha(\alpha^{-1}(y)) = x *' y, \qquad \forall x, y \in P$$

ja edelleen

$$\alpha^{-1}(x) * \alpha^{-1}(y) = \alpha^{-1}(x *' y),$$

joten α^{-1} on homomorfismi. Koska se on myös bijektio, väite on tosi. □

Kahdella isomorfisella puoliryhmällä on samat algebralliset ominaisuudet (mutta niiden kombinatoriset ominaisuudet saattavat erota).

Esimerkki 2.15. Olkoon S ääretön puoliryhmä siten, että $S = \{x, x^2, x^3, \dots\}$. Määritellään $\alpha\colon S \to (\mathbb{N}_+, +)$ niin, että $\alpha(x^n) = n$. Nyt α on homomorfismi, koska $\alpha(x^n * x^m) = \alpha(x^{n+m}) = n + m = \alpha(x^n) + \alpha(x^m)$. Lisäksi α on bijektio ja edelleen isomorfismi.

Osoittaakseen, että puoliryhmät $(S, *)$ ja $(P, *')$ ovat isomorfisia, täytyy tehdä seuraavat asiat:

1. Määritellään kuvaus $\alpha\colon S \to P$ siten, että sen määrittelyjoukko on S.
2. Osoitetaan, että α on injektio.
3. Osoitetaan, että α on surjektio.
4. Osoitetaan, että $\alpha(x * y) = \alpha(x) *' \alpha(y)$.

(Ks. [3, s. 337])

Esimerkki 2.16. Olkoon P kaikkien parillisten kokonaislukujen joukko. Osoitetaan edellisien kohtien avulla, että puoliryhmät $(\mathbb{Z}, +)$ ja $(P, +)$ ovat isomorfisia.

1. Määritellään kuvaus $\alpha\colon \mathbb{Z} \to P$ siten, että $\alpha(x) = 2x$.
2. Oletetaan, että $\alpha(x_1) = \alpha(x_2)$. Nyt $2x_1 = 2x_2$, joten $x_1 = x_2$ ja siten α on injektio.
3. Oletetaan nyt, että y on mikä tahansa parillinen kokonaisluku. Nyt $x = y/2 \in \mathbb{Z}$ ja
$$\alpha(x) = \alpha(y/2) = 2(y/2) = y,$$
joten α on surjektio.
4. Saadaan
$$\alpha(x + y) = 2(x + y) = 2x + 2y = \alpha(x) + \alpha(y).$$

Siispä $(\mathbb{Z}, +)$ ja $(P, +)$ ovat isomorfisia puoliryhmiä.

(Ks. [3, s. 337–338, Esimerkki 17.])

2.7 Symmetrinen puoliryhmä

Määritelmä 2.9. Olkoon X joukko, ja merkitään kaikkien kuvausten $\alpha\colon X \to X$ joukkoa T_X. Nyt T_X on joukon X *symmetrinen puoliryhmä*.

Esimerkki 2.17. Olkoon $X = \{1, 2, 3\}$. Nyt joukossa T_X on yhteensä $3^3 = 27$ kuvausta. Määritellään kuvaus $\alpha\colon X \to X$ siten, että $\alpha(1) = 2$, $\alpha(2) = 2$, $\alpha(3) = 1$. Tämä voidaan esittää seuraavasti:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 1 \end{pmatrix}$$

Olkoon sitten

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 3 \end{pmatrix},$$

ja puoliryhmän T_X kuvausten α ja β generoima alipuoliryhmä $S = [\alpha, \beta]_{T_X}$. Nyt saadaan

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 2 \end{pmatrix}, \qquad \beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \end{pmatrix}, \qquad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \end{pmatrix},$$

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 3 \end{pmatrix}, \qquad \beta^2\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix} = \alpha^2\beta.$$

Voitaisiin vielä tarkistaa, ettei puoliryhmässä S ole muita alkioita näiden seitsemän alkion lisäksi ja siten $S = \{\alpha, \beta, \alpha^2, \beta^2, \alpha\beta, \beta\alpha, \beta^2\alpha\}$.

Määritelmä 2.10. Homomorfismi $\rho\colon S \to T_X$ on puoliryhmän S *esitys*. Jos ρ on upotus, $\rho\colon S \hookrightarrow T_X$, se on puoliryhmän S *injektiivinen esitys*.

Lause 2.6. *Jokaisella puoliryhmällä S on injektiivinen esitys.*

Toisin sanoen edellinen lause 2.6 toteaa, että puoliryhmän S voidaan ajatella olevan joukon X symmetrisen puoliryhmän T_X alipuoliryhmä P siten, että $S \cong P \subseteq T_X$.

Todistus. Olkoon $X = S^1$, joka on puoliryhmä S, johon on lisätty identiteettialkio 1, jos se ei ole monoidi. Merkitään symmetristä puoliryhmää $T = T_{S^1}$. Määritellään jokaisella $x \in S$ kuvaus

$$\rho\colon S^1 \to S^1, \qquad \rho_x(y) = xy \qquad (y \in S^1).$$

Siis $\rho \in T$ ja kaikilla $x, y \in S$ ja $z \in S^1$ saadaan

$$\rho_{xy}(z) = (xy)z = x(yz) = \rho_x(yz) = \rho_x(\rho_y(z)) = \rho_x\rho_y(z),$$

joten $\rho_{xy} = \rho_x\rho_y$. Siis kuvaus

$$\rho\colon S \to T, \qquad \rho(x) = \rho_x$$

on homomorfismi. Lisäksi ρ on injektiivinen, sillä

$$\rho(x) = \rho(y) \Rightarrow \rho_x = \rho_y \Rightarrow \rho_x(1) = \rho_y(1) \Rightarrow x = y, \qquad \square$$

Lause 2.7 (Cayley)**.** *Jokainen ryhmä voidaan esittää bijektioiden $\alpha\colon X \to X$ ryhmänä.*

Todistus. (Ks. [2, s. 117, Lauseen 9.12 todistus])

Olkoon G ryhmä. Määritellään kaikilla $g \in G$ sellainen kuvaus $\rho_g\colon G \to G$, että $\rho_g(x) = gx$. Osoitetaan, että ρ_g on ryhmän G permutaatio. Oletetaan, että $\rho_g(x) = \rho_g(y)$. Tällöin

$$gx = \rho_g(x) = \rho_g(y) = gy.$$

Siis $x = y$ ja kuvaus ρ_g on injektiivinen. Olkoon sitten $y = g^{-1}(x)$, jolloin on olemassa sellainen y, että $\rho_g(y) = x$, jokaisella $x \in G$. Tästä seuraa, että ρ_g on myös surjektiivinen.

Määritellään nyt ryhmä $\overline{G}$ siten, että

$$\overline{G} = \{\rho_g | g \in G\}.$$

Saadaan kuvausten suljettu laskutoimitus:

$$(\rho_g \circ \rho_h)(x) = \rho_g(hx) = ghx = \rho_{gh}(x).$$

Nyt myös

$$\rho_e(x) = ex = x$$

ja

$$(\rho_{g^{-1}} \circ \rho_g)(x) = \rho_{g^{-1}}(gx) = g^{-1}gx = x = \rho_e(x).$$

Määritellään isomorfismi ryhmältä G ryhmälle $\overline{G}$ siten, että $\phi\colon g \rightarrowtail \rho_g$. Ryhmän laskutoimitus on homomorfismi, sillä:

$$\phi(gh) = \rho_{gh} = \rho_g\rho_h = \phi(g)\phi(h).$$

Se on injektiivinen, koska jos $\phi(g)(x) = \phi(h)(x)$, niin

$$gx = \rho_g(x) = \rho_h(x) = hx.$$

Tällöin siis $g = h$. Koska $\phi(g) = \rho_g$ kaikilla $\rho_g \in \overline{G}$, niin ϕ on myös surjektiivinen ja isomorfisuus on todistettu. □

Huomautus. Cayleyn lauseen vastine puoliryhmälle toteaa, että jokainen puoliryhmä on isomorfinen symmetrisen puoliryhmän kanssa. Tämän todistus on vastaavan lainen kuin edellä oleva Cayleyn lauseen todistus.

2.8 Tulo- ja osamääräpuoliryhmät

Määritelmä 2.11. Olkoot S ja T puoliryhmiä. Nyt *suora tulo* $S \times T$ määritellään

$$(x_1, y_1) * (x_2, y_2) = (x_1x_2, y_1y_2) \qquad (x_i \in S, y_i \in T).$$

Tulon liitännäisyys voidaan todeta helposti pareille $(x, y) \in S \times T$:

$$(x_1, y_1) * ((x_2, y_2) * (x_3, y_3)) = (x_1, y_1) * (x_2x_3, y_2y_3) = (x_1(x_2x_3), y_1(y_2y_3))$$
$$= ((x_1x_2)x_3, (y_1y_2)y_3) = (x_1x_2, y_1y_2) * (x_3, y_3) = ((x_1, y_1) * (x_2, y_2)) * (x_3, y_3).$$

Tästä seuraa, että suora tulo on puoliryhmä.

Suora tulo yhdistää kätevästi kahden puoliryhmän laskutoimitukset. Syntyneellä puoliryhmällä $S \times T$ on molempien puoliryhmien S ja T ominaisuudet.

Esimerkki 2.18. Olkoot $S = (\mathbb{R}, +)$ ja $T = (\mathbb{R}, \cdot)$. Nyt suora tulo $S \times T$ on

$$(n, r) \cdot (m, s) = (n + m, rs).$$

Vaikka yleisesti $S \times T \neq T \times S$, kuten edellisestä esimerkistä 2.18 näkee, suora tulo on kuitenkin puoliryhmillä liitännäinen laskutoimitus ja $S \times (T \times U) = (S \times T) \times U$. Edelleen voidaan määritellä, että $S_1 \times S_2 \times \cdots \times S_n$ on puoliryhmien S_i suora tulo.

Määritelmä 2.12. Olkoot $\pi_1 \colon S \times T \to S$ ja $\pi_2 \colon S \times T \to T$ sellaisia kuvauksia, että $\pi_1(x, y) = x$ ja $\pi_2(x, y) = y$. Nyt kuvauksia π_1 ja π_2 kutsutaan suoran tulon $S \times T$ *projektioiksi* .

Määritelmä 2.13. Ekvivalenssirelaatio ρ puoliryhmässä S on vasen kongruenssi, jos

$$\forall x, y, z \in S \colon x\rho y \Rightarrow (zx)\rho(zy).$$

Samoin, ρ on oikea kongruenssi, jos

$$\forall x, y, z \in S\colon x\rho y \Rightarrow (xz)\rho(yz).$$

Jos ρ on sekä vasen että oikea kongruenssi, se on *kongruenssi*.

Ekvivalenssirelaatio ρ jakaa siis määrittelyjoukon S ekvivalenssiluokkiin $x\rho(x \in S)$. Kongruenssin ekvivalenssiluokkaa kutsutaan kongruenssiluokaksi.

Lause 2.8. *Ekvivalenssirelaatio ρ puoliryhmässä S on kongruenssi, jos ja vain jos kaikilla $x_1, x_2, y_1, y_2 \in S$ pätee*

$$\left.\begin{matrix} x_1\rho y_1 \\ x_2\rho y_2 \end{matrix}\right\} \Rightarrow (x_1x_2)\rho(y_1y_2).$$

Todistus. Oletetaan ensin, että ρ on kongruenssi. Jos $x_1\rho y_1$ ja $x_2\rho y_2$, niin määritelmän 2.13 mukaan $(x_1x_2)\rho(x_1y_2)$ ja $(x_1y_2)\rho(y_1y_2)$ ja edelleen transitiivisuuden nojalla $(x_1x_2)\rho(y_1y_2)$. Toiseen suuntaan todistus seuraa suoraan määritelmästä 2.13. □

Esimerkki 2.19. Tarkastellaan puoliryhmää $(\mathbb{Z}, +)$ ja määritellään ekvivalenssirelaatio R kokonaisluvuille $\mathbb{Z}$ seuraavasti:

$$xRy, \qquad \text{jos ja vain jos} \qquad x \equiv y \pmod 3.$$

Jos $x \equiv y \pmod 3$ ja jos $u \equiv v \pmod 3$, niin $x - y$ ja $u - v$ ovat jaollisia luvulla 3, joten $x - y = 3m$ ja $u - v = 3n$, kun $m, n \in \mathbb{Z}$. Lisäksi saadaan

$$(x - y) + (u - v) = 3m + 3n$$

tai

$$(x + u) - (y + v) = 3(m + n),$$

joten $x + y \equiv u + v \pmod 3$ ja relaatio R on kongruenssi.

(Vrt. [3, s. 342, Esimerkki 1.])

Määritelmä 2.14. Olkoot ρ kongruenssi puoliryhmässä S ja

$$S/\rho = \{x\rho | x \in S\}$$

kaikkien kongruenssin ρ luokkien joukko. Nyt *osamääräpuoliryhmä* määrittelyjoukossa S/ρ määritellään

$$x\rho * y\rho = (xy)\rho.$$

Samoin kuin tulon, osamäärän liitännäisyys on myös helppo tarkistaa:

$$x\rho * (y\rho * z\rho) = x\rho * (yz)\rho = (x(yz))\rho = ((xy)z)\rho = (xy)\rho * z\rho = (x\rho * y\rho) * z\rho.$$

Esimerkki 2.20. Esimerkin 2.19 ekvivalenssirelaatio tuottaa jäännösluokat modulo 3.

Lähteet

[1] Tero Harju. *Lecture Notes on Semigroups*. Turun Yliopisto 1996

[2] Thomas W. Judson *Abstract Algebra Theory and Applications*. Stephen F. Austin State University 2020

[3] Bernard Kolman, Robert C. Busby, Sharon Cutler Ross *Discrete Mathematical Structures*, 3rd ed. Prentice Hall 1996. ISBN 0-13-320912-1.