Tampereen yliopisto
Informaatiotieteiden laitos

VEHMAS, MARKO: Ryhmien perusominaisuuksista

Pro gradu -työ, 22 s.

Matematiikka

Huhtikuu 2002

TIIVISTELMÄ

Tämän työn luvussa 2 perehdytään abstraktin algebran keskeiseen käsitteeseen ryhmään ja joihinkin sen perusominaisuuksiin. Ryhmä on epätyhjän joukon sekä laskutoimituksen muodostama tietyt ehdot toteuttava algebrallinen struktuuri. Ryhmän lisäksi määritellään puoliryhmä, monoidi ja Abelin ryhmä eli kommutatiivinen ryhmä. Ryhmän ja puoliryhmän käsitteiden määrittelyn jälkeen esitetään kolme lausetta, joiden avulla voidaan todeta, onko puoliryhmä ryhmä. Työn loppupuolella määritellään ryhmän kertaluku, alkion potenssi ja alkion kertaluku. Lopuksi esitetään alkion kertalukuun liittyvä lause.

Lukijalta edellytetään käsitteen suurin yhteinen tekijä sekä jakoalgoritmin tuntemisen lisäksi perustietoja joukoista, relaatioista, kuvauksista ja laskutoimituksista (engl. binary operations). Tämän työn luvussa 1 on esitetty luettelonomaisesti ryhmää käsittelevän tarkastelun kannalta keskeisiä relaatioita, kuvauksia ja laskutoimituksia koskevia määritelmiä, lauseita ja esimerkkejä. Tarvittaessa lukija voi perehtyä edellä lueteltuihin esitietoina edellytettyihin asioihin luvussa 1 esitettyä paremmin kirjan Fundamentals of Abstract Algebra [5] sivuilta 1 – 54.

Tässä työssä seurataan pääosin kirjan Fundamentals of Abstract Algebra [5] esitystä. Kirjan esityksestä on poikettu niissä kohdin, missä sen on katsottu olevan tarkoituksenmukaista.

TAMPEREEN YLIOPISTO
Matematiikan pro gradu -työ

Marko Vehmas

Ryhmien perusominaisuuksista

Matematiikan, tilastotieteen ja filosofian laitos
Matematiikka
Huhtikuu 2002

Sisältö

Johdanto

Tämän työn luvussa 2 perehdytään abstraktin algebran keskeiseen käsitteeseen ryhmään ja joihinkin sen perusominaisuuksiin. Ryhmä on epätyhjän joukon sekä laskutoimituksen muodostama tietyt ehdot toteuttava algebrallinen struktuuri. Ryhmän lisäksi määritellään puoliryhmä, monoidi ja Abelin ryhmä eli kommutatiivinen ryhmä. Ryhmän ja puoliryhmän käsitteiden määrittelyn jälkeen esitetään kolme lausetta, joiden avulla voidaan todeta, onko puoliryhmä ryhmä. Työn loppupuolella määritellään ryhmän kertaluku, alkion potenssi ja alkion kertaluku. Lopuksi esitetään alkion kertalukuun liittyvä lause.

Lukijalta edellytetään käsitteen suurin yhteinen tekijä sekä jakoalgoritmin tuntemisen lisäksi perustietoja joukoista, relaatioista, kuvauksista ja laskutoimituksista (engl. binary operations). Tämän työn luvussa 1 on esitetty luettelonomaisesti ryhmää käsittelevän tarkastelun kannalta keskeisiä relaatioita, kuvauksia ja laskutoimituksia koskevia määritelmiä, lauseita ja esimerkkejä. Tarvittaessa lukija voi perehtyä edellä lueteltuihin esitietoina edellytettyihin asioihin luvussa 1 esitettyä paremmin kirjan Fundamentals of Abstract Algebra [5] sivuilta 1 – 54.

Ennen nykyisen määritelmän esittämistä ryhmän käsitteen kehittymiseen ovat vaikuttaneet lukuisat merkittävät matemaatikot, kuten Joseph Louis Lagrange (1736 – 1813), saksalainen Carl Friedrich Gauss (1777 – 1855), ranskalainen A. Cauchy (1789 – 1857), ranskalainen Evariste Galois (1811 – 1832), Arthur Cayley (1821 – 1895), Felix Klein (1849 – 1925) ja Sophus Lie. Nykyisen määritelmän esittivät vuonna 1882 Heinrich Weber (1842 – 1913) ja Felix Kleinin kanssa työskennellyt Walter von Dyck (1856 – 1934). Ryhmäteoriaa käytetään esimerkiksi fysiikassa ja kemiassa (kristallografia, spektroskopia, yleinen suhteellisuusteoria, molekyylivärähtelyt, molekyyliorbitaalit, kiinteän aineen fysiikka, alkeishiukkasteoria). (Ks. [1, s. 13 – 15], [2, s. 53], [5, s. 56 – 58] ja [7, s. 153 – 155])

Tässä työssä seurataan pääosin kirjan Fundamentals of Abstract Algebra

[5] esitystä. Kirjan esityksestä on poikettu niissä kohdin, missä sen on katsottu olevan tarkoituksenmukaista.

1 Relaatio, kuvaus, laskutoimitus

Tässä luvussa on esitetty luettelonomaisesti luvussa 2 tapahtuvan ryhmää käsittelevän tarkastelun kannalta keskeisiä relaatioita, kuvauksia ja laskutoimituksia koskevia määritelmiä, lauseita ja esimerkkejä.

1.1 Binäärirelaation määritelmä

Määritelmä 1.1.1 (ks. [5, s. 21]) **Binäärirelaatio** *R joukosta A joukkoon B on tulojoukon $A \times B$ osajoukko. Binäärirelaatiota R voidaan kutsua lyhyemmin* **relaatioksi** *R.*

Olkoon R relaatio joukosta A joukkoon B. Olkoon x joukon A alkio ja y joukon B alkio. Jos $(x, y) \in R$, niin voimme merkitä joko xRy tai $R(x) = y$. Tällöin sanomme relaation R liittävän alkion x alkioon y. Voimme myös sanoa alkioiden x ja y olevan keskenään relaatiossa R. Jos on ilmeistä, mistä relaatiosta kulloinkin on kysymys, voidaan relaation nimi, esimerkiksi R, jättää lausumatta. Jos $A = B$, niin sanomme relaation R olevan joukossa A määritelty relaatio. (Ks. [5, s. 21])

Määritelmä 1.1.2 (ks. [5, s. 21]) *Olkoon R relaatio joukosta A joukkoon B. Tällöin relaation R* **määrittelyjoukko** *on*

$$\{\, x \mid x \in A \text{ ja on olemassa sellainen } y \in B, \text{ että } (x, y) \in R \,\}.$$

Sitä merkitään symbolilla $\mathcal{D}(R)$. Relaation R **arvojoukko** *on*

$$\{\, y \mid y \in B \text{ ja on olemassa sellainen } x \in A, \text{ että } (x, y) \in R \,\}$$

ja sitä merkitään symbolilla $\mathcal{I}(R)$. Kyseistä arvojoukkoa voidaan kutsua myös relaation R **kuvaksi**.

1.2 Ekvivalenssirelaatio ja kongruenssi

Määritelmä 1.2.1 (ks. [5, s. 22]) *Olkoon R relaatio joukossa A. Relaatio R on*
(i) **refleksiivinen**, *jos xRx aina, kun $x \in A$,*
(ii) **symmetrinen**, *jos ominaisuudesta xRy seuraa ominaisuus yRx aina, kun $x, y \in A$,*
(iii) **transitiivinen**, *jos ominaisuuksista xRy ja yRz seuraa ominaisuus xRz aina, kun $x, y, z \in A$.*

Määritelmä 1.2.2 (ks. [5, s. 22]) *Relaatiota E joukossa A sanotaan* **ekvivalenssirelaatioksi** *joukossa A, jos E on refleksiivinen, symmetrinen ja transitiivinen.*

Esimerkki 1.2.3 (ks. [5, s. 22–23]) Olkoon n jokin positiivinen kokonaisluku. Määritellään joukossa $\mathbb{Z}$ relaatio $\equiv_n$ seuraavasti: jokaiselle $x, y \in \mathbb{Z}$ on voimassa $x \equiv_n y$, jos ja vain jos $n|(x-y)$. Merkintä $n|(x-y)$ tarkoittaa, että on olemassa sellainen kokonaisluku k, että $x - y = nk$. Osoitetaan, että $\equiv_n$ on ekvivalenssirelaatio joukossa $\mathbb{Z}$.

(i) Jokaiselle kokonaisluvulle x on voimassa $x - x = 0 = 0n$. Siis $x \equiv_n x$ aina, kun $x \in \mathbb{Z}$. Täten $\equiv_n$ on refleksiivinen.

(ii) Valitaan mielivaltaiset kokonaisluvut x ja y. Oletetaan, että $x \equiv_n y$. On siis olemassa sellainen kokonaisluku q, että $qn = x - y$. Tällöin $(-q)n = y - x$ eli $n|(y-x)$. Siis $y \equiv_n x$. Näin ollen $\equiv_n$ on symmetrinen.

(iii) Valitaan mielivaltaiset kokonaisluvut x, y ja z. Oletetaan, että $x \equiv_n y$ ja $y \equiv_n z$. Tällöin on olemassa sellaiset kokonaisluvut q ja r, että $qn = x - y$ ja $rn = y - z$. Siis $(q + r)n = x - z$, missä $q + r \in \mathbb{Z}$. Tämä merkitsee, että $x \equiv_n z$. Siis $\equiv_n$ on transitiivinen.

Määritelmän 1.2.2 perusteella $\equiv_n$ on ekvivalenssirelaatio joukossa $\mathbb{Z}$. Määriteltyä relaatiota $\equiv_n$ sanotaan relaatioksi **kongruenssi modulo** n.

1.3 Ekvivalenssiluokka

Määritelmä 1.3.1 (vrt. [5, s. 23]) *Olkoon E ekvivalenssirelaatio joukossa A ja olkoon x joukon A alkio. Käytetään merkintää $[x]$ joukolle*

$$[x] = \{\, y \in A \mid yEx \,\}.$$

Joukko $[x]$ on **ekvivalenssiluokka**, *jonka määräävät relaatio E ja alkio $x \in A$.*

Seuraava lause esittelee joitakin ekvivalenssiluokkien perusominaisuuksia.

Lause 1.3.2 (ks. [5, s. 23]) *Olkoon E ekvivalenssirelaatio joukossa A. Silloin*
(i) $[x] \neq \emptyset$ aina, kun $x \in A$,
(ii) jos $y \in [x]$, niin $[x] = [y]$, missä $x, y \in A$,
(iii) $[x] = [y]$ tai $[x] \cap [y] = \emptyset$ aina, kun $x, y \in A$,
(iv) $A = \cup_{x \in A}[x]$ eli kaikkien ekvivalenssiluokkien unioni on joukko A.

Todistus (ks. [5, s. 23])

1.4 Ekvivalenssirelaation ja joukon osituksen yhteys

Määritelmä 1.4.1 (ks. [5, s. 23]) *Olkoon A joukko ja olkoon $\mathcal{P}$ joukko, jonka alkioina ovat joukon A epätyhjät osajoukot. Joukkoa $\mathcal{P}$ sanotaan joukon A* **osituksesi**, *jos seuraavat ehdot toteutuvat:*
(i) $B = C$ tai $B \cap C = \emptyset$ aina, kun $B, C \in \mathcal{P}$,
(ii) $A = \cup_{B \in \mathcal{P}} B$.

Toisin sanoen, jos $\mathcal{P}$ on joukon A ositus, niin seuraavat kolme ehtoa ovat voimassa:
(i) $B \subseteq A$ aina, kun $B \in \mathcal{P}$, eli kaikki joukon $\mathcal{P}$ alkiot ovat joukon A osajoukkoja,
(ii) tarkasteltaessa kahta joukon $\mathcal{P}$ alkiota ne ovat keskenään joko samat tai erilliset,
(iii) unioni joukon $\mathcal{P}$ alkioista on joukko A. (Ks. [5, s. 24])

Lause 1.4.2 (vrt. [5, s. 24]) *Olkoon E ekvivalenssirelaatio joukossa A. Tällöin*

$$\mathcal{P} = \{\, [x] \mid x \in A \,\}$$

on joukon A ositus.

Todistus. Lause on suora seuraus lauseesta 1.3.2 ja määritelmästä 1.4.1.

Esimerkki 1.4.3 (vrt. [5, s. 24]) Tarkastellaan esimerkissä 1.2.3 määriteltyä ekvivalenssirelaatiota $\equiv_n$. Olkoon $\mathbb{Z}_n = \{\, [x] \mid x \in \mathbb{Z} \,\}$. Lauseen 1.4.2 perusteella $\mathbb{Z}_n$ on joukon $\mathbb{Z}$ ositus. Olkoon $n = 6$. Osoitetaan, että

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$$

ja

$$[i] = \{0 + i, \pm 6 + i, \pm 12 + i, \dots\} = \{\, 6q + i \mid q \in \mathbb{Z} \,\} \text{ aina, kun } i \in \mathbb{Z}.$$

Olkoon $0 \leq a < b < 6$. Tehdään oletus, että $[a] = [b]$. Nyt $a \in [b]$ eli $a \equiv_6 b$ ja siten $6|(a - b)$. Mutta tämä on ristiriita, koska $0 < a - b < 6$. Siis ekvivalenssiluokat $[0], [1], [2], [3], [4], [5]$ ovat erilliset.

Osoitetaan, ettei ole olemassa muita ekvivalenssiluokkia. Valitaan mielivaltainen kokonaisluku k. Jakoalgoritmin perusteella on olemassa sellaiset kokonaisluvut q ja $0 \leq r < 6$, että $k = 6q + r$ (ks. tarvittaessa [5, s. 10]). Siis $k - r = 6q$ ja siten $6|(k - r)$. Nyt $k \equiv_6 r$, joten $[k] = [r]$. Koska $0 \leq r < 6$, niin $[r] \in \{[0], [1], [2], [3], [4], [5]\}$. Näin ollen $[k] \in \{[0], [1], [2], [3], [4], [5]\}$, joten $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$.

Valitaan mielivaltainen kokonaisluku i. Nyt $x \in [i]$, jos ja vain jos $6|(x - i)$. Siis $x \in [i]$, jos ja vain jos on olemassa sellainen kokonaisluku q, että $6q = x - i$, joten $x \in [i]$, jos ja vain jos on olemassa sellainen kokonaisluku q, että $x = 6q + i$. Näin ollen $[i] = \{0 + i, \pm 6 + i, \pm 12 + i, \dots\} = \{\, 6q + i \mid q \in \mathbb{Z} \,\}$

aina, kun $i \in \mathbb{Z}$. Täten $[i] = [6q + i]$, missä $i = 0, 1, \ldots, 5$ ja $q \in \mathbb{Z}$. Siis

a) kun $i = 0$, niin $[0] = [6] = [12] = \cdots = [-6] = [-12] = \ldots$;
b) kun $i = 1$, niin $[1] = [7] = [13] = \cdots = [-5] = [-11] = \ldots$;
c) kun $i = 2$, niin $[2] = [8] = [14] = \cdots = [-4] = [-10] = \ldots$;
d) kun $i = 3$, niin $[3] = [9] = [15] = \cdots = [-3] = [-9] = \ldots$;
e) kun $i = 4$, niin $[4] = [10] = [16] = \cdots = [-2] = [-8] = \ldots$;
f) kun $i = 5$, niin $[5] = [11] = [17] = \cdots = [-1] = [-7] = \ldots$

1.5 Kuvaus ja laskutoimitus

Määritelmä 1.5.1 (ks. [5, s. 40]) *Olkoot A ja B epätyhjiä joukkoja. Relaatiota f joukosta A joukkoon B sanotaan* **kuvaukseksi** *(tai* **funktioksi***)* joukolta *A joukkoon B, jos*
(i) $\mathcal{D}(f) = A$ ja
(ii) ominaisuudesta $x = x'$ seuraa ominaisuus $y = y'$ aina, kun $(x, y), (x', y') \in f$.

Kuvaukselle f joukolta A joukkoon B käytetään merkintää $f : A \to B$. Merkinnän $(x, y) \in f$ sijaan käytetään usein merkintää $f(x) = y$. Alkiota y sanotaan alkion x **kuvaksi** ja alkiota x alkion y **alkukuvaksi** (ks. [6, s. 91]). Kohta *(ii)* tarkoittaa, että jokaisen alkion $x \in A$ kuva $y \in B$ on yksikäsitteinen (ks. [7, s. 20]). (Vrt. [5, s.40])

Määritelmä 1.5.2 (vrt. [5, s. 52] ja [3]) *Olkoon S epätyhjä joukko. Kuvausta tulojoukolta $S \times S$ joukkoon S sanotaan* **laskutoimitukseksi** *(tai* **binäärioperaatioksi***) joukossa S ja sitä merkitään symbolilla $*$.*

Laskutoimitus $*$ joukossa S liittää joukon S alkioista x ja y muodostetun järjestetyn parin (x, y) täsmälleen yhteen joukon S alkioon. Tälle alkiolle käytetään merkintää $x*y$ (kuvauksen merkintöjä käyttäen olisi $*(x, y)$). (Vrt. [5, s. 52])

Määritelmä 1.5.3 (vrt. [5, s. 52] ja [3]) *Olkoon S epätyhjä joukko ja olkoon $*$ laskutoimitus joukossa S. Tällöin järjestettyä paria $(S, *)$ sanotaan (yhden laskutoimituksen)* **algebralliseksi struktuuriksi**.

Määritelmä 1.5.4 (ks. [5, s. 52] ja [3]) *Olkoon $(S, *)$ algebrallinen struktuuri. Laskutoimituksen $*$ sanotaan olevan*
(i) **liitännäinen** *(eli* **assosiatiivinen***), jos $x * (y * z) = (x * y) * z$ aina, kun $x, y, z \in S$,*
(ii) **vaihdannainen** *(eli* **kommutatiivinen***), jos $x * y = y * x$ aina, kun $x, y \in S$.*

Määritelmä 1.5.5 (ks. [5, s. 53] ja [3]) *Alkio $e \in S$ on algebrallisen struktuurin $(S, *)$* **neutraalialkio***, jos*

$$e * x = x = x * e \quad \textit{aina, kun } x \in S.$$

Esimerkki 1.5.6 (ks. [5, s. 53]) Olkoon $S = \{e, a, b\}$. Määritellään laskutoimitus $*$ joukossa S kertotaulun

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

avulla. Nyt $e * a = a = a * e$, $e * b = b = b * e$ ja $e * e = e = e * e$, joten e on algebrallisen struktuurin $(S, *)$ neutraalialkio.

2 Ryhmien perusominaisuuksia

Tässä luvussa perehdytään ryhmän käsitteeseen ja joihinkin sen perusominaisuuksiin.

2.1 Ryhmän määritelmä

Olkoon $S = \{f \mid f : A \to A\}$. Tällöin
(i) kuvausten $f, g \in S$ yhdistäminen, $\circ$, yhdistetyksi kuvaukseksi $f \circ g$ on laskutoimitus joukossa S (ks. [3]),
(ii) $f \circ (g \circ h) = (f \circ g) \circ h$ aina, kun $f, g, h \in S$,
(iii) on olemassa sellainen $i \in S$, että $f \circ i = f = i \circ f$ aina, kun $f \in S$,
(iv) jokaista alkiota $f \in S$ kohti on olemassa sellainen alkio $f^{-1} \in S$, että $f \circ f^{-1} = i = f^{-1} \circ f$.
Nämä ominaisuudet johtavat seuraavassa esitettävään ryhmän käsitteen määritelmään. (ks. [5, s. 58])

Määritelmä 2.1.1 (ks. [5, s. 58]) *Olkoon G epätyhjä joukko ja olkoon $*$ laskutoimitus kyseisessä joukossa. Järjestettyä paria $(G, *)$ nimitetään* **ryhmäksi**, *jos seuraavat ehdot toteutuvat:*
(G1) $a * (b * c) = (a * b) * c$ aina, kun $a, b, c \in G$ (liitäntälaki),
(G2) on olemassa sellainen $e \in G$, että $a * e = a = e * a$ aina, kun $a \in G$ (neutraalialkion olemassaolo),
(G3) jokaista alkiota $a \in G$ kohti on olemassa sellainen $b \in G$, että $a * b = e = b * a$ (käänteisalkion olemassaolo).

Ryhmä on aksioomat *G1* – *G3* toteuttava algebrallinen struktuuri. Seuraava lause ilmaisee kaksi ryhmää koskevaa tärkeää ominaisuutta. (Ks. [5, s. 58])

Lause 2.1.2 (ks. [5, s. 58]) *Olkoon* $(G, *)$ *ryhmä. Silloin*
(i) on olemassa sellainen yksikäsitteinen alkio $e \in G$*, että* $e * a = a = a * e$ *aina, kun* $a \in G$*,*
(ii) jokaista alkiota $a \in G$ *kohti on olemassa sellainen yksikäsitteinen* $b \in G$*, että* $a * b = e = b * a$*.*

Todistus (vrt. [5, s. 58, 54, osin virheellinen]) *(i)* Aksiooman *G2* perusteella on olemassa sellainen $e \in G$, että $e * a = a = a * e$ aina, kun $a \in G$. Osoitetaan tämän alkion olevan yksikäsitteinen. Oletetaan, että on olemassa myös toinen alkio $f \in G$, jolla on ominaisuus $f * a = a = a * f$ aina, kun $a \in G$. Koska $e * a = a$ aina, kun $a \in G$, niin myös alkiolle $f \in G$ on

$$e * f = f. \tag{1}$$

Koska $a * f = a$ aina, kun $a \in G$, niin myös alkiolle $e \in G$ on

$$e * f = e. \tag{2}$$

Yhtälöiden 1 ja 2 perusteella $e = f$, joten e on yksikäsitteinen.

(ii) Olkoon a joukon G alkio. Aksiooman *G3* perusteella on olemassa sellainen $b \in G$, että $a * b = e = b * a$. Osoitetaan tämän alkion olevan yksikäsitteinen. Oletetaan, että on olemassa sellainen $c \in G$, että $a * c = e = c * a$. Nyt

$$\begin{array}{rcll} b & = & b * e & \\ & = & b * (a * c) & (e = a * c) \\ & = & (b * a) * c & (* \text{ liitännäinen}) \\ & = & e * c & (b * a = e) \\ & = & c\,. & \end{array}$$

Siis b on yksikäsitteinen. □

Aksiooman *G2* mukaista yksikäsitteistä alkiota e sanotaan ryhmän $(G, *)$ **neutraalialkioksi**. Olkoon $a \in G$. Aksiooman *G3* mukaista yksikäsitteistä alkiota b sanotaan alkion a **käänteisalkioksi** ja sitä merkitään symbolilla a^{-1}. (Ks. [5, s. 59])

Määritelmä 2.1.3 (vrt. [5, s. 59]) *Jos ryhmän* $(G, *)$ *laskutoimitus* $*$ *on vaihdannainen eli kommutatiivinen, niin ryhmää sanotaan* **Abelin ryhmäksi** *tai* **kommutatiiviseksi ryhmäksi**.

Norjalainen matemaatikko Niels Henrik Abel (1802 – 1829) on saanut nimensä kuvaamaan kommutatiivista ryhmää (ks. [2, s. 54]). Jos $(G, *)$ ei ole kommutatiivinen, sitä sanotaan ei-kommutatiiviseksi ryhmäksi (ks. [5, s. 59]).

Esimerkki 2.1.4 (vrt. [5, s. 59]) Tarkastellaan muodostaako kokonaislukujen joukko $\mathbb{Z}$ yhdessä tavanomaisen yhteenlaskun $+$ kanssa ryhmän $(\mathbb{Z}, +)$. Tiedetään, että $+$ on liitännäinen eli G1 toteutuu. Nyt 0 on kokonaisluku ja $a + 0 = 0 = 0 + a$ aina, kun $a \in \mathbb{Z}$, joten 0 on algebrallisen strukruurin $(\mathbb{Z}, +)$ neutraalialkio. Siis G2 toteutuu. Jokaista alkiota $a \in \mathbb{Z}$ kohti on olemassa alkio $-a \in \mathbb{Z}$ niin, että $a + (-a) = 0 = (-a) + a$, joten $-a$ on alkion a käänteisalkio. Myös G3 toteutuu, joten $(\mathbb{Z}, +)$ on ryhmä. Koska lisäksi $a + b = b + a$ aina, kun $a, b \in \mathbb{Z}$, niin $+$ on vaihdannainen ja $(\mathbb{Z}, +)$ on Abelin ryhmä.

Samaan tapaan voidaan osoittaa, että Abelin ryhmiä ovat $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$ ja $(\mathbb{C}\backslash\{0\}, \cdot)$, missä $+$ on tavallinen yhteenlasku ja $\cdot$ tavallinen kertolasku. Ryhmien $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot)$ ja $(\mathbb{Q} \setminus \{0\}, \cdot)$ neutraalialkio on 1.

Esimerkki 2.1.5 (ks. [5, s. 59]) Olkoon a jokin kokonaisluku. Olkoon $G = \{na \mid n \in \mathbb{Z}\}$ ja olkoon $+$ tavallinen yhteenlasku. Silloin $(G, +)$ on Abelin ryhmä.

Carl Friedrich Gaussin työ tuotti monia uusia suuntia Abelin ryhmien tutkimuksessa. Seuraava esimerkki on Gaussin työn seurausta. (Ks. [5, s. 59])

Esimerkki 2.1.6 (vrt. [5, s. 59 – 60]) Tarkastellaan esimerkeissä 1.2.3 ja 1.4.3 määriteltyä joukkoa $\mathbb{Z}_n$. Määritellään laskutoimitus $+_n$ joukossa $\mathbb{Z}_n$ säännöllä

$$[a] +_n [b] = [a + b] \text{ aina, kun } [a], [b] \in \mathbb{Z}_n.$$

Osoitetaan, että $(\mathbb{Z}_n, +_n)$ on Abelin ryhmä. Osoitetaan aluksi, että $+_n$ on laskutoimitus. Olkoot $[a], [b], [c], [d] \in \mathbb{Z}_n$. On osoitettava, että jos $([a], [b]) = ([c], [d])$, niin $[a+b] = [c+d]$. On siis osoitettava, että jos $[a] = [c]$ ja $[b] = [d]$, niin $[a + b] = [c + d]$. Oletetaan, että $[a] = [c]$ ja $[b] = [d]$. Koska $[a] = [c]$, niin $a \equiv_n c$ eli $n|(a - c)$, ja koska $[b] = [d]$, niin $b \equiv_n d$ eli $n|(b - d)$. Siis on olemassa sellaiset kokonaisluvut s ja t, että $ns = a - c$ ja $nt = b - d$. Nyt $n(s + t) = ((a + b) - (c + d))$, joten $n|((a + b) - (c + d))$. Siis $a + b \equiv_n c + d$ ja siten $[a + b] = [c + d]$. Näin ollen kuva $[a + b]$ on yksikäsitteinen, joten $+_n$ on laskutoimitus joukossa $\mathbb{Z}_n$.

Osoitetaan, että $(\mathbb{Z}_n, +_n)$ on ryhmä. Nyt

$$\begin{aligned}
([a] +_n [b]) +_n [c] &= [a + b] +_n [c] \\
&= [(a + b) + c] \\
&= [a + (b + c)] \\
&= [a] +_n [b + c] \\
&= [a] +_n ([b] +_n [c]) \text{ aina, kun } [a], [b], [c] \in \mathbb{Z}_n.
\end{aligned}$$

Siis $+_n$ on liitännäinen.

Selvästi $[0] \in \mathbb{Z}_n$ ja $[a] +_n [0] = [a + 0] = [a] = [0 + a] = [0] +_n [a]$ aina, kun $[a] \in \mathbb{Z}_n$, joten $[0]$ on neutraalialkio. Osoitetaan käänteisalkion olemassaolo. Nyt $[-a] \in \mathbb{Z}_n$ ja $[a] +_n [-a] = [a + (-a)] = [0] = [-a + a] = [-a] +_n [a]$ aina, kun $[a] \in \mathbb{Z}_n$. Siis $[-a]$ on alkion $[a]$ käänteisalkio. Aksioomat *G1* – *G3* toteutuvat, joten $(\mathbb{Z}_n, +_n)$ on ryhmä. Koska $[a] +_n [b] = [a + b] = [b + a] = [b] +_n [a]$ aina, kun $[a], [b] \in \mathbb{Z}_n$, niin $+_n$ on vaihdannainen. Täten $(\mathbb{Z}_n, +_n)$ on Abelin ryhmä.

Esimerkki 2.1.7 (ks. [5, s. 61]) Olkoon

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Tällöin $(\mathbb{Q}[\sqrt{2}], +)$ ja $(\mathbb{Q}[\sqrt{2}] \setminus \{0\}, \cdot)$, missä $+$ on tavallinen yhteenlasku ja $\cdot$ tavallinen kertolasku, ovat Abelin ryhmiä. Ryhmän $(\mathbb{Q}[\sqrt{2}], +)$ neutraalialkio on $0 + 0\sqrt{2}$ eli 0 ja alkion $a + b\sqrt{2}$ käänteisalkio on $-a + (-b)\sqrt{2}$. Ryhmän $(\mathbb{Q}[\sqrt{2}] \setminus \{0\}, \cdot)$ neutraalialkio on $1 + 0\sqrt{2}$ eli 1 ja alkion $a + b\sqrt{2} \neq 0$ käänteisalkio on

$$\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

2.2 Joitakin perusominaisuuksia

Seuraavissa lauseissa esitetään joitakin ryhmän perusominaisuuksia.

Lause 2.2.1 (vrt. [5, s. 62]) *Olkoon $(G, *)$ ryhmä. Tällöin*
(i) $(a^{-1})^{-1} = a$ *aina, kun* $a \in G$,
(ii)$(a * b)^{-1} = b^{-1} * a^{-1}$ *aina, kun* $a, b \in G$,
*(iii) (***Supistussääntö** (vrt. [7, s. 53])*) jos* $a * c = b * c$ *tai* $c * a = c * b$, *niin* $a = b$ *aina, kun* $a, b, c \in G$.

Todistus (vrt. [5, s. 63]) *(i)* Olkoon a joukon G alkio. Nyt $a^{-1} * a = e = a * a^{-1}$, joten a on alkion a^{-1} käänteisalkio. Koska ryhmän käänteisalkio on yksikäsitteinen (lause 2.1.2) ja alkion a^{-1} käänteisalkiota merkitään symbolilla $(a^{-1})^{-1}$, niin $(a^{-1})^{-1} = a$.

(ii) Olkoot a ja b joukon G alkioita. Tällöin

$$\begin{aligned}(a * b) * (b^{-1} * a^{-1}) &= ((a * b) * b^{-1}) * a^{-1} \\ &= (a * (b * b^{-1})) * a^{-1} \\ &= (a * e) * a^{-1} \\ &= a * a^{-1} \\ &= e.\end{aligned}$$

Vastaavasti voidaan todeta, että $(b^{-1} * a^{-1}) * (a * b) = e$. Täten $b^{-1} * a^{-1}$ on alkion $a * b$ käänteisalkio. Koska ryhmän käänteisalkio on yksikäsitteinen, niin $(a * b)^{-1} = b^{-1} * a^{-1}$.

(iii) Olkoot a,b ja c joukon G alkioita. Oletetaan, että $a * c = b * c$. Koska laskutoimitus $*$ liittää joukon G kaksi alkiota yksikäsitteisesti kolmanteen joukon G alkioon (tarvittaessa ks. määr. 1.5.3 ja määr. 1.5.1), niin yhtälön molemmille puolille voidaan suorittaa oikealta puolelta laskutoimitus $*$ alkiolla c^{-1}. Tällöin saadaan $(a * c) * c^{-1} = (b * c) * c^{-1}$. Nyt $(a*c)*c^{-1} = a*(c*c^{-1}) = a*e = a$ ja $(b*c)*c^{-1} = b*(c*c^{-1}) = b*e = b$, joten $a = b$. Vastaavasti voidaan osoittaa ominaisuudesta $c * a = c * b$ seuraavan ominaisuuden $a = b$. □

Seuraus 2.2.2 (ks. [5, s. 63]) *Olkoon $(G, *)$ ryhmä ja olkoon a joukon G alkio. Jos $a * a = a$, niin $a = e$.*

Todistus (vrt. [5, s. 63]) Olkoon $a*a = a$. Koska $a = a*e$, niin $a*a = a*e$. Supistussäännön perusteella saadaan $a = e$. □

Lause 2.2.3 (vrt. [5, s. 62] ja [8, s.75]) *Olkoon $(G, *)$ ryhmä. Tällöin yhtälöillä $a * x = b$ ja $y * a = b$ on yksikäsitteiset ratkaisut $x, y \in G$ aina, kun $a, b \in G$. Nämä ratkaisut ovat $x = a^{-1} * b$ ja $y = b * a^{-1}$.*

Todistus (vrt. [1, s. 21]) Oletetaan, että $a * x = b$. Koska laskutoimitus $*$ on yksikäsitteinen, yhtälön molemmille puolille voidaan vasemmalta suorittaa laskutoimitus $*$ alkiolla a^{-1}, joka on alkion a yksikäsitteinen käänteisalkio. Tällöin saadaan oletuksen kanssa yhtäpitävä yhtälö $a^{-1}*(a*x) = a^{-1}*b$. Koska $a^{-1}*(a*x) = (a^{-1}*a)*x = e*x = x$, niin $x = a^{-1}*b$. Samaan tapaan osoitetaan yhtälön $y * a = b$ yksikäsitteisen ratkaisun olevan $y = b * a^{-1}$. □

Seuraus 2.2.4 (ks. [5, s. 63]) *Ryhmän $(G, *)$ alkioille muodostetussa laskutoimitustaulussa (tarvittaessa ks. esim. 1.5.6) kukin alkio esiintyy jokaisella rivillä ja jokaisessa sarakkeessa täsmälleen kerran.*

Todistus (vrt. [5, s. 64]) Olkoon b joukon G sellainen alkio, joka esiintyy kahdesti alkiolla a merkityllä rivillä. Tällöin on olemassa sellaiset joukon G ei-samat alkiot u ja v, että $a*u = b$ ja $a*v = b$. Yhtälöllä $a*x = b$ on siis kaksi eri ratkaisua u ja v. Tämä on ristiriidassa lauseen 2.2.3 kanssa, joten sama alkio voi esiintyä samalla rivillä korkeintaan kerran. Koska lisäksi rivejä ja alkioita on yhtä monta, täytyy kunkin alkion esiintyä kullakin rivillä vähintään kerran. Siis jokainen joukon G alkio esiintyy jokaisella rivillä täsmälleen kerran. Sarakkeiden kohdalla todistaminen suoritetaan samalla tavalla. □

2.3 Puoliryhmä vai ryhmä?

Jotta on voitu osoittaa tietyn joukon ja tietyn laskutoimituksen muodostavan yhdessä ryhmän, on täytynyt osoittaa määritelmän 2.1.1 aksioomien *G1* – *G3* olevan voimassa tälle algebralliselle struktuurille. Olisi kuitenkin eduksi, jos käytettävissä olisi yksinkertaisempia menetelmiä todeta, onko tietty algebrallinen struktuuri ryhmä vai ei. Osittain tästä syystä otetaan käyttöön käsitteet puoliryhmä ja monoidi. (Ks. [5, s. 65])

Määritelmä 2.3.1 (ks. [5, s. 65]) *Olkoon S epätyhjä joukko ja olkoon $*$ liitännäinen laskutoimitus joukossa S. Tällöin järjestettyä paria $(S, *)$ sanotaan* **puoliryhmäksi**.

Määritelmä 2.3.2 (ks. [3]) *Puoliryhmää $(S, *)$, jolla on neutraalialkio, sanotaan* **monoidiksi**.

Selvästi jokainen ryhmä on sekä puoliryhmä että monoidi. Puoliryhmää ja monoidia sanotaan kommutatiiviseksi, jos $*$ on vaihdannainen eli $a*b = b*a$ aina, kun a ja b ovat joukon S alkioita. Jos puoliryhmä tai monoidi ei ole kommutatiivinen, sitä sanotaan ei-kommutatiiviseksi. (Ks. [5, s.65])

Esimerkki 2.3.3 (vrt. [5, s. 65]) Tarkastellaan positiivisten kokonaislukujen joukkoa $\mathbb{N}$. Positiivisten kokonaislukujen yhteenlasku tuottaa yksikäsitteisen

positiivisen kokonaisluvun, joten + on laskutoimitus joukossa $\mathbb{N}$. Koska + on myös liitännäinen ja vaihdannainen, niin $(\mathbb{N}, +)$ on kommutatiivinen puoliryhmä.

Esimerkki 2.3.4 (ks. [5, s. 66]) Olkoon joukossa X vähintään kaksi alkiota ja olkoon S' joukko, jonka alkioina ovat kaikki ei-injektiiviset kuvaukset $f : X \to X$. Tällöin $(S', \circ)$ on ei-kommutatiivinen puoliryhmä.

Esimerkki 2.3.5 (ks. [5, s. 66]) Olkoon X joukko ja olkoon $\mathcal{P}(X)$ joukon X potenssijoukko (tarvittaessa ks. [5, s. 8]). Tällöin $(\mathcal{P}, \cup)$ ja $(\mathcal{P}, \cap)$ ovat kommutatiivisia monoideja. Monoidin $(\mathcal{P}, \cup)$ neutraalialkio on tyhjä joukko $\emptyset$ ja monoidin $(\mathcal{P}, \cap)$ neutraalialkio on joukko X.

Seuraavat kolme lausetta ilmaisevat välttämättömät ja riittävät ehdot sille, että puoliryhmä on ryhmä.

Lause 2.3.6 (ks. [5, s. 66]) *Puoliryhmä $(S, *)$ on ryhmä, jos ja vain jos*
(i) on olemassa sellainen $e \in S$, että $e * a = a$ aina, kun $a \in S$,
(ii) jokaista alkiota $a \in S$ kohti on olemassa sellainen $b \in S$, että $b * a = e$.

Todistus (vrt. [5, s. 66]) Oletetaan, että $(S, *)$ on sellainen puoliryhmä, joka toteuttaa ehdot *i* ja *ii*. Olkoon a jokin joukon S alkio. Ehdon *ii* perusteella on olemassa sellainen alkio $b \in S$, että $b * a = e$. Samoin ehdon *ii* perusteella on olemassa sellainen alkio $c \in S$, että $c * b = e$. Nyt

$$\begin{array}{rcll} a & = & e * a & \text{(ehdon } i \text{ mukaan)} \\ & = & (c * b) * a & (c * b = e) \\ & = & c * (b * a) & (* \text{ liitännäinen}) \\ & = & c * e & (b * a = e). \end{array}$$

Edelleen

$$\begin{array}{rcll} a * b & = & (c * e) * b & (a = c * e) \\ & = & c * (e * b) & (* \text{ liitännäinen}) \\ & = & c * b & \text{(ehdon } i \text{ perusteella)} \\ & = & e. & \end{array}$$

Koska lisäksi ehdon *ii* perusteella $b * a = e$, niin $a * b = e = b * a$. Siis määritelmän 2.1.1 aksiooma *G3* toteutuu.

Osoitetaan seuraavaksi, että aksiooma *G2* toteutuu. Nyt

$$\begin{array}{rcll} a * e & = & a * (b * a) & (b * a = e) \\ & = & (a * b) * a & (* \text{ liitännäinen}) \\ & = & e * a & (a * b = e) \\ & = & a & (\text{ehdon } i \text{ mukaan}). \end{array}$$

Koska lisäksi ehdon i mukaan $e * a = a$, niin $a * e = a = e * a$, joten *G2* toteutuu. Koska puoliryhmän laskutoimitus on liitännäinen, niin aksiooma *G1* toteutuu. Siis $(S, *)$ on ryhmä.

Oletetaan sitten, että $(S, *)$ on ryhmä. Tällöin aksioomasta *G2* seuraa ehto i ja aksioomasta *G3* seuraa ehto *ii*. □

Lause 2.3.7 (ks. [5, s. 66]) *Puoliryhmä $(S, *)$ on ryhmä, jos ja vain jos yhtälöillä $a * x = b$ ja $y * a = b$ on ratkaisut $x, y \in S$ aina, kun $a, b \in S$.*

Todistus (vrt. [5, s. 66]) Oletetaan, että yhtälöillä $a * x = b$ ja $y * a = b$ on ratkaisut x ja y joukossa S. Olkoon a joukosta S mielivaltaisesti valittu alkio. Tarkastellaan yhtälöä $y * a = a$. Oletuksen perusteella yhtälöllä $y * a = a$ on ratkaisu joukossa S. Merkitään tätä ratkaisua kirjaimella u. Tällöin $u * a = a$. Olkoon b joukosta S mielivaltaisesti valittu alkio. Tarkastellaan yhtälöä $a * x = b$. Oletuksen perusteella yhtälöllä $a * x = b$ on ratkaisu joukossa S. Merkitään ratkaisua kirjaimella c. Siis $a * c = b$. Nyt

$$\begin{array}{rcll} u * b & = & u * (a * c) & (b = a * c) \\ & = & (u * a) * c & (* \text{ liitännäinen}) \\ & = & a * c & (u * a = a) \\ & = & b. & \end{array}$$

Koska b valittiin mielivaltaisesti joukon S alkioiden joukosta, niin $u * b = b$ aina, kun b on joukon S alkio. Täten $(S, *)$ toteuttaa lauseen 2.3.6 ehdon i.

Tarkastellaan yhtälöä $y * a = u$, missä a ja u ovat kuten edellä. Olkoon d yhtälön ratkaisu, jolloin $d * a = u$. Siis $(S, *)$ toteuttaa lauseen 2.3.6 ehdon *ii*. Lauseen 2.3.6 perusteella $(S, *)$ on ryhmä.

Oletetaan sitten, että $(S, *)$ on ryhmä. Lauseen 2.2.3 perusteella yhtälöillä $a * x = b$ ja $y * a = b$ on ratkaisut. □

Määritelmä 2.3.8 (vrt. [5, s. 68]). *Ryhmää, monoidia tai puoliryhmää* $(S, *)$ *sanotaan* **äärelliseksi**, *jos joukko* S *on äärellinen. Muutoin* $(S, *)$ *on* **ääretön**.

Lause 2.3.9 (vrt. [5, s. 67]) *Äärellinen puoliryhmä* $(S, *)$ *on ryhmä, jos ja vain jos* $(S, *)$ *toteuttaa supistussäännön (eli jos* $a * c = b * c$ *tai* $c * a = c * b$*, niin* $a = b$ *aina, kun* $a, b, c \in S$*).*

Todistus (vrt. [5, s. 67] Olkoon $(S, *)$ äärellinen puoliryhmä, joka toteuttaa supistussäännön. Olkoot a ja b joukon S alkioita. Osoitetaan, että yhtälöllä $a * x = b$ on ratkaisu joukossa S. Olkoon $S = \{a_1, a_2, \ldots, a_n\}$, missä mikään alkio ei esiinny kahdesti. Koska $*$ on laskutoimitus, niin $a * a_i \in S$ aina, kun $i = 1, 2, \ldots, n$. Täten $\{a * a_1, a * a_2, \ldots, a * a_n\} \subseteq S$. Oletetaan, että $a * a_i = a * a_j$, missä $i \neq j$. Supistussäännön perusteella $a_i = a_j$, mikä on ristiriita, koska $a_i \neq a_j$. Täten joukon $\{a*a_1, a*a_2, \ldots, a*a_n\}$ alkioissa ei ole samoja alkiota. Joukoissa S ja $\{a * a_1, a * a_2, \cdots, a * a_n\}$ kummassakin on n alkiota, joten $S = \{a * a_1, a * a_2, \ldots, a * a_n\}$. Nyt $b \in S$, joten edellä esitetyn perusteella on olemassa sellainen $a_k \in S$, että $a*a_k = b$. Siis yhtälöllä $a*x = b$ on ratkaisu joukossa S. Vastaavasti osoitetaan, että yhtälöllä $y * a = b$ on ratkaisu joukossa S. Lauseen 2.3.7 perusteella $(S, *)$ on ryhmä.

Oletetaan sitten, että $(S, *)$ on ryhmä. Lauseen 2.2.1 kohdan *iii* perusteella supistussääntö toteutuu. □

2.4 Potenssi

Olkoon $(G, *)$ ryhmä ja olkoot a, b ja c joukon G alkioita. Tällöin liitäntälain perusteella $a*(b*c) = (a*b)*c$, joten voidaan määritellä $a*b*c = a*(b*c) = (a*b)*c$. Seuraavassa lauseessa tämä laajennetaan koskemaan minkä tahansa kokoista äärellistä lauseketta $a_1 * a_2 * \cdots * a_n$. (Ks. [5, s. 64])

Lause 2.4.1 (Yleistetty liitäntälaki) (vrt. [1, s. 19]) *Olkoon $(G, *)$ ryhmä ja olkoot $a_1, a_2, \ldots, a_n$ joukon G alkioita. Lausekkeen $a_1 * a_2 * \cdots * a_n$ arvo ei riipu siitä, missä järjestyksessä laskutoimitukset $*$ suoritetaan.*

Todistus (vrt. [5, s. 64]) Osoitetaan lause todeksi induktion avulla. Liitäntälain perusteella väite on tosi, kun $n = 3$. Oletetaan nyt, että väite on tosi kokonaisluvulla m, kun $3 \leq m < n$. Olkoot $a_1, a_2, \ldots, a_n$ joukon G alkioita. Olkoon $(a_1 * \cdots * a_t) * (a_{t+1} * \cdots * a_n)$ alkioista $a_1, a_2, \ldots, a_n$ (tässä järjestyksessä) muodostettu lauseke. Nyt $t < n$. Kun $t = n - 1$, niin $(a_1 * a_2 * \cdots * a_t) * a_{t+1} = a_1 * a_2 * \cdots * a_t * a_{t+1}$, koska sulut eivät muuta laskujärjestystä. Merkitään ominaisuutta symbolilla $\star$. Oletetaan, että $t < n - 1$. Tällöin

$$\begin{aligned}
(a_1 * \cdots * a_t) * (a_{t+1} * \cdots * a_n) &= (a_1 * \cdots * a_t) * ((a_{t+1} * \cdots * a_{n-1}) * a_n) \\
&= ((a_1 * \cdots * a_t) * (a_{t+1} * \cdots * a_{n-1})) * a_n \\
&= (a_1 * a_2 * \cdots * a_{n-1}) * a_n \\
&= a_1 * a_2 * \cdots * a_n.
\end{aligned}$$

Yhtäsuuruusketjussa ensimmäinen ja viimeinen yhtäsuuruus perustuu ominaisuuteen $\star$, toinen laskutoimituksen $*$ liitännäisyyteen ja kolmas induktio-oletukseen. On osoitettu, että väite on tosi kokonaisluvulle n. Induktioperiaatteen mukaan lause on tosi. □

Määritelmä 2.4.2 (vrt. [5, s. 67]) *Olkoon $(G, *)$ ryhmä. Olkoon a joukon G alkio ja olkoon n kokonaisluku. Alkion a* **potenssi** *a^n lasketaan*

$$a^n = \begin{cases} e, & jos \quad n = 0, \\ a * a^{n-1}, & jos \quad n > 0, \\ (a^{-1})^{-n}, & jos \quad n < 0. \end{cases}$$

Negatiivinen potenssi voidaan laskea myös $a^n = (a^{-n})^{-1}$, missä $n < 0$ (ks. [5, s. 67]). Kun laskutoimitus $*$ on yhteenlaskun kaltainen, käytetään potenssin sijaan nimitystä alkion a **monikerta** (ks. [3]). (Vrt. [5, s. 67])

Määritelmä 2.4.3 (vrt. [5, s. 67]) *Olkoon $(G, +)$ ryhmä, jossa $+$ on yhteenlaskun kaltainen. Olkoon a joukon G alkio ja olkoon n kokonaisluku. Alkion a monikerta na lasketaan*

$$na = \begin{cases} 0, & jos \quad n = 0, \text{ neutraalialkiota merkitään symbolilla } 0, \\ a + (n-1)a, & jos \quad n > 0, \\ (-n)(-a), & jos \quad n < 0. \end{cases}$$

Ryhmässä $(\mathbb{Z}_6, +_6)$ monikerta $2[3]$ lasketaan $2[3] = [3] +_6 [3] = [6] = [0]$. Merkintä na ei tarkoita, että alkioille n ja a suoritetaan kertolasku, koska ryhmässä $(\mathbb{Z}_6, +_6)$ ei ole kertolaskua edes määritelty. (Ks. [5, s. 67])

2.5 Ryhmän kertaluku ja alkion kertaluku

Määritelmä 2.5.1 (vrt. [5, s. 68] ja [4, s. 14]) *Äärellisen* **ryhmän** $(G, *)$ **kertaluku** *on joukon G alkioiden lukumäärä ja sitä merkitään symbolilla $|G|$. Äärettömän ryhmän kertaluku on ääretön.*

Esimerkin 2.1.6 perusteella jokaista positiivista kokonaislukua n kohti on olemassa äärellinen Abelin ryhmä, jonka kertaluku on n. Äärettömiä ryhmiä alettiin tarkastella paljolti sen johdosta, että Felix Klein ja Sophus Lie käyttivät ryhmän käsitettä geometrian parissa. Esimerkkien 2.1.4, 2.1.5 ja 2.1.7 ryhmät ovat äärettömiä, joten niiden kertaluvut ovat äärettömiä. (Ks. [5, s. 68])

Olkoon $(G, *)$ äärellinen ryhmä ja olkoon a joukon G alkio. Tällöin $a^2 = a * a$ on joukon G alkio. Induktioperiaatteen avulla voidaan osoittaa, että $a^m \in G$ aina, kun $m \geq 1$. Näin ollen $\{a, a^2, \ldots, a^m, \ldots\} \subseteq G$. Koska G on äärellinen, joukon $\{a, a^2, \ldots, a^m, \ldots\}$ alkioista joidenkin täytyy olla samoja. Siis on olemassa sellaiset kokonaisluvut k ja l, että $a^k = a^l$ ja $k > l$. Tällöin on oltava $a^{k-l} = e$. Merkitään $n = k-l$. Täten on olemassa sellainen positiivinen kokonaisluku n, että $a^n = e$. Myös äärettömän ryhmän alkiolle a voi olla olemassa sellainen kokonaisluku n, että $a^n = e$. (Ks. [5, s. 68])

Määritelmä 2.5.2 (vrt. [5, s. 68] ja [4, s. 14]) *Olkoon $(G, *)$ ryhmä ja olkoon a joukon G alkio.* **Alkion a kertaluku** *on pienin sellainen positiivinen kokonaisluku n, että $a^n = e$. Jos sellaista kokonaislukua ei ole, alkion a kertaluku on ääretön. Alkion a kertalukua merkitään symbolilla $\circ(a)$.*

Alkion kertaluku on hyvin tärkeä ryhmäteoriassa. Alkion kertalukuun liittyvä tieto kertoo siitä, millaisesta ryhmästä kulloinkin on kyse. (Ks. [5, s. 68])

Esimerkki 2.5.3 (vrt. [5, s. 68]) Tarkastellaan ryhmää $(\mathbb{Z}_6, +_6)$. Ryhmän kertaluku $|\mathbb{Z}_6| = 6$. Alkioiden $[0], [1], [2], [3], [4], [5]$ kertaluvut ovat $1, 6, 3, 2, 3, 6$. Esimerkiksi $3[2] = [2] +_6 [2] +_6 [2] = [6] = [0]$. Alkion $[2]$ kertaluku on 3, koska se on pienin sellainen positiivinen kokonaisluku n, jolla $n[3] = [0]$.

Olkoon $(G, *)$ ryhmä ja olkoon a joukon G alkio. Jos $\circ(a)$ on ääretön, niin alkion kertaluvun määritelmän perusteella myös $\circ(a^k)$ on ääretön aina, kun $k \geq 1$. Toisin sanoen jos $\circ(a)$ on ääretön, niin alkion a positiivisen potenssin kertaluku on ääretön. Jos $\circ(a)$ on äärellinen, niin alkion a potenssin a^k kertaluku voidaan laskea seuraavan lauseen mukaisesti. Lauseessa käytetään symbolia $\text{syt}(t, n)$ (engl. $\gcd(t, n)$), jolla merkitään kokonaislukujen t ja n suurinta yhteistä tekijää (tarvittaessa ks. [5, s. 11]). (Vrt. [5, s. 68])

Lause 2.5.4 (ks. [5, s. 68 – 69]) *Olkoon $(G, *)$ ryhmä ja olkoon a joukon G sellainen alkio, että $\circ(a) = n$. Tällöin:*

(i) jos on olemassa sellainen positiivinen kokonaisluku m, että $a^m = e$, niin n on luvun m tekijä,
(ii) $\circ(a^t) = \dfrac{n}{\mathrm{syt}(t,n)}$ *aina, kun t on positiivinen kokonaisluku.*

Todistus (Vrt. [5, s. 69]) *(i)* Jakoalgoritmin perusteella on olemassa sellaiset kokonaisluvut q ja r, että $m = nq + r$, missä $0 \leq r < n$. Tällöin $a^r = a^{m-nq} = a^m * a^{-nq} = a^m * (a^n)^{-q} = e * (e)^{-q} = e$. Koska lisäksi n on pienin sellainen positiivinen kokonaisluku, että $a^n = e$, ja $r < n$, niin $r = 0$. Täten $m = nq$ eli n on luvun m tekijä.

(ii) Olkoon $\circ(a^t) = k$. Tällöin $a^{kt} = e$. Kohdan i perusteella n on luvun kt tekijä. Näin ollen on olemassa sellainen kokonaisluku r, että $kt = nr$. Olkoon $\mathrm{syt}(t, n) = d$. Tällöin on olemassa sellaiset kokonaisluvut u ja v, että $t = du$ ja $n = dv$ sekä $\mathrm{syt}(u, v) = 1$. Täten yhtälö $kt = nr$ saadaan muotoon $kdu = dvr$ ja edelleen muotoon $ku = rv$. Näin ollen v on luvun ku tekijä. Koska $\mathrm{syt}(u, v) = 1$, niin v on luvun k tekijä. Näin ollen $\frac{n}{d}$ on luvun k tekijä. Nyt

$$(a^t)^{\frac{n}{d}} = a^{\frac{ndu}{d}} = a^{nu} = (a^n)^u = e^u = e.$$

Koska $\circ(a^t) = k$, niin k on luvun $\frac{n}{d}$ tekijä. Nyt $\frac{n}{d}$ on luvun k tekijä ja k on luvun $\frac{n}{d}$ tekijä, joten $k = \frac{n}{d}$. Näin ollen

$$\circ(a^t) = k = \frac{n}{d} = \frac{n}{\mathrm{syt}(t,n)}.$$

□

Viitteet

[1] David S. Dummit, Richard M Foote, *Abstract Algebra*, Prentice-Hall International, New Jersey, 1991.

[2] John B. Fraleigh, *A first course in abstract algebra*, 6th ed., Addison-Wesley, 1999.

[3] Pentti Haukkanen, *Algebraa*, luentomonisteen luonnos, 1997.

[4] Mika Kurki, Ryhmistä, Pro gradu -tutkielma, Tampereen yliopisto, Matematiikan, tilastotieteen ja filosofian laitos, 1999.

[5] D. S. Malik, John N. Mordeson, M. K. Sen, *Fundamentals of Abstract Algebra*, WCB/McGraw-Hill, 1997.

[6] Jorma Merikoski, Ari Virtanen, Pertti Koivisto, *Diskreetti matematiikka I*, Tampereen yliopisto, Matemaattisten tieteiden laitos, B42, Tampere, 1994.

[7] Tauno Metsänkylä, Marjatta Näätänen, *Algebra*, Jyväskylän yliopisto, Matematiikan laitos, Luentomoniste 44, Jyväskylä, 1999.

[8] Thomas A. Whitelaw, *Introduction to Abstract Algebra*, 3th ed., Chapman & Hall/CRC, 1998.