4. Ryhmät

Tässä luvussa tarkastelemme laskutoimituksella varustettuja joukkoja, joiden laskutoimitukselta oletamme muutamia yksinkertaisia ominaisuuksia:

Määritelmä 4.1. Laskutoimituksella varustettu joukko $(G, *)$ on *ryhmä*, jos

- laskutoimitus $*$ on assosiatiivinen,
- joukossa G on laskutoimituksen $*$ neutraalialkio, ja
- jokaisella $g \in (G, *)$ on käänteisalkio.

Ryhmä on keskeinen algebran rakenne, joka esiintyy monilla matematiikan aloilla esimerkiksi lineaarialgebrassa, geometriassa ja lukuteoriassa. Tällä kurssilla käsittelemme esimerkkejä eri aloilta yleisen teorian tarkastelun lisäksi.

Esimerkki 4.2. (a) Aikaisemmista esimerkeistämme ryhmiä ovat (ainakin)

- *kokonaislukujen (additiivinen) ryhmä* $(\mathbb{Z}, +)$,
- *rationaalilukujen (additiivinen) ryhmä* $(\mathbb{Q}, +)$,
- *reaalilukujen (additiivinen) ryhmä* $(\mathbb{R}, +)$,
- *kompleksilukujen (additiivinen) ryhmä* $(\mathbb{C}, +)$,
- *rationaalilukujen multiplikatiivinen ryhmä* $\mathbb{Q}^\times$,
- *reaalilukujen multiplikatiivinen ryhmä* $\mathbb{R}^\times$,
- *kompleksilukujen multiplikatiivinen ryhmä* $\mathbb{C}^\times$,
- *positiivisten reaalilukujen multiplikatiivinen ryhmä* $(\mathbb{R}_+, \cdot)$ ja
- *äärellinen syklinen ryhmä* $(\mathbb{Z}/q\mathbb{Z}, +)$

Se, että yllä olevan luettelon kokonais-, rationaali- ja reaaliluvuista koostuvat laskutoimituksella varustetut joukot ovat ryhmiä, seuraa näiden lukualueiden tunnetuista ominaisuuksista. Kompleksiluvuille tämä seuraa Propositiosta 2.2.

Osoitamme, että $(\mathbb{Z}/q\mathbb{Z}, +)$ on ryhmä: Kokonaislukujen yhteenlaskun indusoima laskutoimitus on assosiatiivinen Lemman 3.8 mukaan. Alkio $[0]$ on neutraalialkio Proposition 3.7 mukaan, koska luonnollinen kuvaus on surjektiivinen homomorfismi. Alkion $[k] \in \mathbb{Z}/q\mathbb{Z}$ käänteisalkio on $[-k]$:

$$[k] + [-k] = [k - k] = [0] = [-k] + [k].$$

(b) Olkoon $n \in \mathbb{N}$, $n \geq 2$ ja olkoot $\mathrm{M}_n(\mathbb{R})$, $\mathrm{M}_n(\mathbb{Q})$, $\mathrm{M}_n(\mathbb{C})$ ja $\mathrm{M}_n(\mathbb{Z})$ sellaisten $n \times n$-matriisien joukot joiden kertoimet ovat reaalilukuja, rationaalilukuja, kompleksilukuja ja kokonaislukuja. Jos nämä joukot varustetaan matriisien kertolaskulla, ne eivät muodosta ryhmiä: Jokainen näistä matriisien joukoista sisältää muunmuassa nollamatriisin, jolla ei ole käänteismatriisia.

Kurssin lineaarialgebra 1 nojalla tiedämme, että matriisien kertolaskulla varustettujen joukkojen $\mathrm{M}_n(\mathbb{R})$, $\mathrm{M}_n(\mathbb{Q})$ ja $\mathrm{M}_n(\mathbb{C})$ osajoukot, jotka koostuvat matriiseista, joiden determinantti on nollasta poikkeava, muodostavat ryhmiä: Olkoon seuraavassa $\mathbb{K}$ jokin lukualueista $\mathbb{Q}$, $\mathbb{R}$ tai $\mathbb{C}$. Jos $A, B \in \mathrm{M}_n(\mathbb{K})$ ja $\det A \neq 0 \neq \det B$, niin determinantin laskusäännöistä seuraa, että $\det AB \neq 0$. Siispä joukko $\{A \in \mathrm{M}_n(\mathbb{K}) : \det A \neq 0\}$ on vakaa, ja matriisien kertolasku indusoi laskutoimituksen tähän joukkoon. Matriisien kertolasku on assosiatiivinen, identtisen matriisin $I_n = \mathrm{diag}(1, \ldots, 1)$ determinantti on 1 ja jokaisella matriisilla A, jolle pätee $\det A \neq 0$ on käänteismatriisi. Tarkastelemamme matriisit muodostavat K-*kertoimisen yleisen lineaarisen ryhmän*

$$\mathrm{GL}_n(\mathbb{K}) = \{A \in \mathrm{M}_n(\mathbb{K}) : \det A \neq 0\},$$

jonka laskutoimitus on matriisien kertolasku. Vastaavasti saadaan $\mathbb{K}$-*kertoiminen erityinen lineaarinen ryhmä*

$$\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{M}_n(R) : \det A = 1\},$$

jonka laskutoimitus on matriisien kertolasku.

On helppo nähdä, että matriisien kertolaskulla varustettu joukko $\{A \in \mathrm{M}_n(\mathbb{Z}) : \det A \neq 0\}$ ei ole ryhmä: $\det \mathrm{diag}(2,2) = 4 \neq 0$, joten sillä on käänteismatriisi $\mathrm{diag}(1/2, 1/2) \in \mathrm{GL}_2(\mathbb{Q})$. Käänteismatriisi on yksikäsitteinen, joten matriisilla $\mathrm{diag}(2,2)$ ei ole käänteismatriisia. Cramerin säännön (Kofaktorimatriisin) avulla voidaan sen sijaan osoittaa (Harjoitustehtävä 28), että

$$\mathrm{SL}_n(\mathbb{Z}) = \{A \in \mathrm{M}_n(\mathbb{Z}) : \det A = 1\}$$

on ryhmä.

Jatkossa ryhmän laskutoimitus jätetään usein mainitsematta ja puhutaan vain "ryhmästä G". Tällöin laskutoimitus on kuitenkin kiinnitetty ja usein konkreettisessa tilanteessa se on ennalta tiedossa. Esimerkiksi merkinnät $\mathbb{C}^\times$ ja $\mathrm{GL}_n(\mathbb{R})$ sisältävät tiedon käytettävästä laskutoimituksesta. Puhuttaessa abstraktisti vain ryhmästä G merkitään laskutoimitusta usein kuten kertolaskua ja neutraalialkiolle käytetään merkintää e tai joskus myös merkintää 1. Jos tarkastellaan useampia ryhmiä samalla kertaa voidaan niiden neutraalialkioille käyttää ryhmille käytettävien merkintöjen kanssa yhteensopivaa merkintää esimerkiksi niin, että ryhmän G' neutraalialkiota merkitään e'. Joskus tehdään toisenlaisiakin valintoja.

Propositio 4.3. *Olkoon G ryhmä. Tällöin*

1. *Neutraalialkio e on yksikäsitteinen.*
2. *Jokaisen alkion käänteisalkio on yksikäsitteinen.*
3. *Jos $\bar{a}a = e$, niin $\bar{a}$ on alkion a käänteisalkio.*
4. *$(a^{-1})^{-1} = a$ kaikilla $a \in G$.*
5. *$(ab)^{-1} = b^{-1}a^{-1}$.*

Todistus. (1), (2), (3): Lause 1.10.

(4): Koska $aa^{-1} = e$, niin kohdan (3) nojalla $a = (a^{-1})^{-1}$.

(5): Koska pätee

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e,$$

niin väite seuraa kohdasta (3). □

Supistussäännöt ovat voimassa laskutoimituksella varustetussa joukossa $(A, *)$, jos kaikilla $a, b, c \in A$ pätee

1. Jos $ab = ac$, niin $b = c$.
2. Jos $ab = cb$, niin $a = c$.

Supistussäännöt ovat voimassa monissa laskutoimituksella varustetuissa joukoissa kuten esimerkiksi luonnollisissa luvuissa ja kaikissa ryhmissä.

Propositio 4.4. *Supistussäännöt pätevät ryhmässä.*

Todistus. Harjoitustehtävä 30. □

Propositio 4.5. *Olkoon A assosiatiivisella laskutoimituksella varustettu joukko, jossa on neutraalialkio. Tällöin A on ryhmä, jos ja vain jos yhtälöillä $ax = b$ ja $ya = b$ on ratkaisu joukossa A kaikilla $a, b \in A$.*

Todistus. Harjoitustehtävä 31. □

Seuraava tulos antaa keinon muodostaa uusia ryhmiä tunnetuista ryhmistä tulolaskutoimituksen avulla.

Propositio 4.6. *Olkoot G_1 ja G_2 ryhmiä. Niiden tulo $G_1 \times G_2$ on ryhmä (varustettuna laskutoimitusten tulolla).*

Todistus. Laskutoimituksen assosiatiivisuus on selvää. Jos e_1 ja e_2 ovat ryhmien G_1 ja G_2 neutraalialkiot, niin (e_1, e_2) on neutraalialkio joukossa $G_1 \times G_2$. Alkion $(g_1, g_2) \in G_1 \times G_2$ käänteisalkio on (g_1^{-1}, g_2^{-1}). □

Esimerkki 4.7. Joukot $\mathbb{R}^n$ ja $\mathbb{Z}^n$ varustettuna vektorien komponenteittaisella yhteenlaskulla, eli yhteenlaskun n-kertaisella tulolla, ovat ryhmiä.

Olkoon X epätyhjä joukko ja olkoon

$$S(X) = \{f \colon X \to X : f \text{ on bijektio}\}.$$

Laskutoimituksella $\circ$ varustettu joukko $S(X)$ on joukon X *permutaatioryhmä*. Permutaatioryhmä on todellakin ryhmä Esimerkkien 1.6(c) ja 1.9(a) nojalla. Ryhmän $S(X)$ alkioita voidaan kutsua joukon X *permutaatioiksi*. Näin on tapana tehdä erityisesti, jos joukko X on äärellinen.

Matematiikan eri aloilla joukkoihin voidaan liittää erilaisia lisärakenteita kuten vektoriavaruusrakenne, sisätulo, metriikka ja ryhmä. Tällaisten joukkojen permutaatioryhmien osajoukot, jotka säilyttävät valitun rakenteen tai ovat sen kanssa yhteensopivia, varustettuna indusoidulla laskutoimituksella (joka siis on kuvausten yhdistäminen) ovat usein ryhmiä.

Esimerkki 4.8. Olkoon $X = \mathbb{R}^n$. Kuvaus $L \colon \mathbb{R}^n \to \mathbb{R}^n$ on *lineaarikuvaus*, jos kaikilla $x, y \in \mathbb{R}^n$ ja $a \in \mathbb{R}$ pätee

$$L(x + y) = L(x) + L(y)$$

ja

$$L(ax) = aL(x).$$

Vektoriavaruuden $\mathbb{R}^n$ lineaariset bijektioiden joukko on permutaatioryhmän vakaa osajoukko, sillä lineaarialgebrassa osoitetaan, että kahden lineaarikuvauksen yhdistetty kuvaus on lineaarikuvaus. Nämä lineaariset bijektiot muodostavat ryhmän $\mathrm{GL}(\mathbb{R}^n)$, jossa kuvausten yhdistäminen on laskutoimituksena: Laskutoimituksen assosiatiivisuutta ei tarvitse tarkastaa, koska se on ryhmän $S(\mathbb{R}^n)$ laskutoimituksen indusoima. Identtinen kuvaus on lineaarikuvaus, ja kurssilla Lineaarinen algebra ja geometria 1 osoitetaan, että lineaarisen bijektion käänteiskuvaus on lineaarinen bijektio.

Määritelmä 4.9. Ryhmä G on *kommutatiivinen* eli *Abelin ryhmä*, jos sen laskutoimitus on kommutatiivinen. Ryhmä G on *äärellinen*, jos joukko G on äärellinen.

Esimerkki 4.10. (a) Ryhmät $\mathbb{Z}$, $\mathbb{Z}/q\mathbb{Z}$, $\mathbb{Z}^n$ ovat kommutatiivisia. Erityinen lineaarinen ryhmä $\mathrm{SL}_n(\mathbb{R})$ ei ole kommutatiivinen, tämä osoitettiin harjoitustehtävässä 4 tapaukselle $n = 2$.

(b) Ryhmät $\mathbb{Z}/q\mathbb{Z}$ ja $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$, ovat äärellisiä ryhmiä kaikille $q, r \in \mathbb{N}$.

(c) Kuvaukset $\mathrm{id}, f, g, h \colon \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$, $f(x) = -x, g(x) = 1/x$, $h(x) = -1/x$, muodostavat äärellisen ryhmän $K \subset S(\mathbb{R} \setminus \{0\})$ laskutoimituksena kuvausten yhdistäminen. On helppo nähdä, että K on vakaa, joten laskutoimitus on hyvin määritelty. Joukon K alkioille f, g, h pätee

$$f \circ f = g \circ g = h \circ h = \mathrm{id},$$

joten kaikilla on käänteisalkio, ja K on siis ryhmä. Lisäksi pätee:

$$f \circ g = g \circ f = h, \quad g \circ h = h \circ g = f \text{ ja } h \circ f = f \circ h = g,$$

joten K on kommutatiivinen.

Äärellisiä (pieniä) ryhmiä voi myös tarkastella *laskutaulujen* avulla: Muodostetaan ryhmän alkioilla indeksoitu taulukko, jossa paikalla (g,h) on alkio gh. Ryhmän laskutaulussa (tai kertotaulussa, kuten sitä usein kutsutaan) jokaisella rivillä ja jokaisessa sarakkeessa esiintyvät kaikki ryhmän alkiot (Harjoitustehtävä 35).

Esimerkki 4.11. Neljän alkion ryhmien $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ ja K laskutaulut ovat

$$\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array}\ ,\quad \begin{array}{c|cccc} + & (0,0) & (0,1) & (1,0) & (1,1) \\ \hline (0,0) & (0,0) & (0,1) & (1,0) & (1,1) \\ (0,1) & (0,1) & (0,0) & (1,1) & (1,0) \\ (1,0) & (1,0) & (1,1) & (0,0) & (0,1) \\ (1,1) & (1,1) & (1,0) & (0,1) & (0,0) \end{array}\quad \text{ja}\quad \begin{array}{c|cccc} \circ & \mathrm{id} & f & g & h \\ \hline \mathrm{id} & \mathrm{id} & f & g & h \\ f & f & \mathrm{id} & h & g \\ g & g & h & \mathrm{id} & f \\ h & h & g & f & \mathrm{id} \end{array}$$

Näissä laskutauluissa käytetään kongruenssiluokan $[k]$ merkintänä edustajaa $k\in\mathbb{Z}$.

Laskutauluja vertaamalla huomaamme, että ryhmät $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ ja K ovat isomorfisia: Kuvaus $\phi\colon\ :\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\to K$,

$$\phi([0],[0])=\mathrm{id},\quad \phi([0],[1]])=f,\quad \phi([1],[0])=g,\quad \phi([1],[1])=h,$$

on isomorfismi. Kuvaus on selvästi bijektio, ja homomorfisuuden voi tarkastaa tutkimalla kaikki tapaukset, esimerkiksi

$$\phi\big(([1],[0])+([0],[1])\big)=\phi([1],[1])=h=g\circ f=\phi([0],[1])\circ\phi([1],[0])$$

Muille tapauksille pätee vastaavasti. Ryhmä K on siis “ryhmäteorian kannalta sama ryhmä kuin $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},+)$”.

Jos G ja G' ovat ryhmiä, niin homomorfismia $\phi\colon G\to G'$ kutsutaan joskus *ryhmähomomorfismiksi*. Huomaa, että isomorfismin, eli bijektiivisen homomorfismin, käänteiskuvaus on myös isomorfismi. Jos G ja G' ovat isomorfisia ryhmiä, voidaan käyttää merkintää $G\cong G'$.

Propositio 4.12. *Ryhmähomomorfismi $\phi\colon G\to G'$ kuvaa ryhmän G neutraalialkion ryhmän G' neutraalialkioksi, ja jokaiselle $g\in G$ pätee $\phi(g^{-1})=\phi(g)^{-1}$.*

Todistus. Neutraalialkiota koskeva väite todistetaan harjoitustehtävässä 29.

Todistetaan käänteisalkiota koskeva väite: Olkoon e ryhmän G neutraalialkio. Olkoon $g\in G$. Tällöin

$$\phi(g^{-1})\phi(g)=\phi(g^{-1}g)=\phi(e).$$

Ensimmäisen väitteen mukaan tämä on ryhmän G neutraalialkio. Väite seuraa Proposition 4.3 kohdasta (3). $\square$

Esimerkki 4.13. (a) Esimerkissä 1.13(a) osoitettiin, että $\exp\colon(\mathbb{R},+)\to(\mathbb{R}_+,\cdot)$ on ryhmäisomorfismi.

(b) Vektoriavaruuden $\mathbb{R}^n$ lineaaristen bijektioiden ryhmä $\mathrm{GL}(\mathbb{R}^n)$ (katso Esimerkki 4.8) on isomorfinen yleisen lineaarisen ryhmän $\mathrm{GL}_n(\mathbb{R})$ kanssa: Olkoon $K=\{v_1,v_2,\dots,v_n\}$ vektoriavaruuden $\mathbb{R}^n$ kanta, ja olkoon $(Lv_i)_K\in\mathbb{R}^n$ vektorin Lv_i koordinaattivektori sarakevektorina kannassa K. Lineaarialgebrassa on osoitettu, että kuvaus $\mathrm{Mat}\colon\mathrm{GL}(\mathbb{R}^n)\to\mathrm{GL}_n(\mathbb{R})$,

$$\mathrm{Mat}(L)=\big((Lv_1)_K,(Lv_2)_K,\dots,(Lv_n)_K\big),$$

on isomorfismi: kaikille lineaarisille bijektioille $L_1,L_2\colon\mathbb{R}^n\to\mathbb{R}^n$ pätee

$$\mathrm{Mat}(L_2\,L_1)=\mathrm{Mat}(L_2)\,\mathrm{Mat}(L_1)\,.$$

Harjoitustehtäviä.

Tehtävä 27. Osoita, että joukon X potenssijoukko $\mathscr{P}(X)$ varustettuna laskutoimituksella $\triangle$ (symmetrinen erotus), joka määritellään asettamalla kaikille $A, B \in \mathscr{P}(X)$

$$A \triangle B = (A \setminus B) \cup (B \setminus A),$$

on ryhmä.

Tehtävä 28. Osoita, että $\mathrm{SL}_n(\mathbb{Z})$ varustettuina matriisien kertolaskulla on ryhmä.

Tehtävä 29. Olkoot G ja G' ryhmiä. Olkoon $h : G \to G'$ homomorfismi. Osoita, että h kuvaa ryhmän G neutraalialkion ryhmän G' neutraalialkioksi.

Tehtävä 30. Olkoon G ryhmä. Osoita, että kaikilla $a, b, c \in G$ pätee supistussääntö:

(1) Jos $ab = ac$, niin $b = c$.
(2) Jos $ab = cb$, niin $a = c$.

Tehtävä 31. Olkoon A assosiatiivisella laskutoimituksella varustettu joukko, jossa on neutraalialkio. Osoita, että A on ryhmä, jos ja vain jos yhtälöillä $ax = b$ ja $ya = b$ on ratkaisu joukossa A kaikilla $a, b \in A$.

Tehtävä 32. Olkoon $T\colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z})$, $T(B) = {}^tB$, kuvaus, joka liittää matriisiin B sen transpoosin. Olkoon $\mathrm{inv}\colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z})$ kuvaus $\mathrm{inv}(B) = B^{-1}$. Mitkä kuvauksista T, inv, $T \circ \mathrm{inv}$ ja $\mathrm{inv} \circ T$ ovat ryhmän $\mathrm{SL}_2(\mathbb{Z})$ automorfismeja?

Tehtävä 33. Olkoon G ryhmä, ja olkoon $\operatorname{Aut} G$ sen automorfismien joukko. Osoita, että $\operatorname{Aut} G$ on ryhmä, kun laskutoimituksena on kuvausten yhdistäminen.

Tehtävä 34. Kuvaus $f\colon \mathbb{R} \to \mathbb{R}$ on *kasvava*, jos kaikille $x, y \in \mathbb{R}$ pätee $f(x) \geq f(y)$, kun $x \geq y$. Kuvaus $f\colon \mathbb{R} \to \mathbb{R}$ on *vähenevä*, jos kaikille $x, y \in \mathbb{R}$ pätee $f(x) \leq f(y)$, kun $x \geq y$. Kuvaus on *monotoninen*, jos se on kasvava tai vähenevä. Kasvavien, vähenevien ja monotonisten bijektioiden joukot ovat permutaatioryhmän $S(\mathbb{R})$ osajoukkoja. Indusoiko kuvausten yhdistäminen laskutoimituksen näihin joukkoihin? Muodostavatko kasvavat bijektiot ryhmän? Entä vähenevät bijektiot? Entä monotoniset bijektiot?

Tehtävä 35. Osoita, että kaikki ryhmän alkiot esiintyvät sen laskutaulun jokaisella rivillä ja sarakkeella.

Tehtävä 36. Olkoot X ja Y epätyhjiä joukkoja, ja olkoon $f\colon X \to Y$ bijektio. Osoita, että permutaatioryhmät $S(X)$ ja $S(Y)$ ovat isomorfisia.

Tehtävä 37. Olkoon

$$H_3 = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{R} \right\}.$$

Osoita, että H_3 varustettuna matriisien kertolaskulla on ryhmä.

Tehtävä 38. Osoita, että tehtävässä 37 määritelty ryhmä H_3 ei ole isomorfinen ryhmän $(\mathbb{R}^3, +)$ kanssa.

---

[29]Vihje: Supistussääntö.
[37]Vihje: Propositio 1.14(1)

Tehtävä 39. Määritellään reaalilukujen joukossa $\mathbb{R}$ laskutoimitus $*$ asettamalla

$$x * y = \sqrt[3]{x^3 + y^3}\,.$$

(a) Osoita, että $(\mathbb{R}, *)$ on ryhmä.

(b) Osoita, että ryhmät $(\mathbb{R}, *)$ ja $(\mathbb{R}, +)$ ovat isomorfiset.

Tehtävä 40. Olkoon G ryhmä. Olkoon R ryhmän G relaatio, joka määritellään säännöllä

$$a\mathrm{R}b \iff a = gbg^{-1} \text{ jollakin } g \in G.$$

Onko R ekvivalenssirelaatio?

[39]Vihje: Jos x on reaaliluku, sen kolmas juuri $\sqrt[3]{x}$ on reaaliluku, jolle pätee $(\sqrt[3]{x})^3 = x$. Jokaisella reaaliluvulla on yksikäsitteinen reaalinen kolmas juuri.