Algebra 1: Ryhmät

Harjoitus 1: Ratkaisuja

1. Varustetaan reaalilukujen joukko $\mathbb{R}$ laskutoimituksella $*$, joka määritellään asettamalla

$$a * b = \sqrt{a^2 + b^2}$$

kaikille $a, b \in \mathbb{R}$.

(a) Onko laskutoimitus $*$ assosiatiivinen?

(b) Onko laskutoimituksella $*$ neutraalialkio?

Olkoon $\psi\colon (\mathbb{R}, *) \to (\mathbb{R}, +)$ kuvaus, joka määritellään asettamalla $\psi(a) = a^2$ kaikilla $a \in \mathbb{R}$.

(c) Onko kuvaus $\psi\colon (\mathbb{R}, *) \to (\mathbb{R}, +)$ homomorfismi?

Ratkaisu. (a) Reaalilukujen yhteenlaskun assosiatiivisuuden nojalla

$$\begin{aligned} a * (b * c) &= \sqrt{a^2 + \sqrt{b^2 + c^2}^2} = \sqrt{a^2 + (b^2 + c^2)} \\ &= \sqrt{(a^2 + b^2) + c^2} = \sqrt{\sqrt{a^2 + b^2}^2 + c^2} = (a * b) * c\,. \end{aligned}$$

(b) Laskutoimituksella ei ole neutraalialkiota: $a * b \geq 0$ kaikilla $a, b \in \mathbb{R}$, joten esimerkiksi $(-1) * a > -1$ kaikilla $a \in \mathbb{R}$. Siis mikään $a \in \mathbb{R}$ ei ole neutraalialkio.

(c) $\psi(a * b) = \sqrt{a^2 + b^2}^2 = a^2 + b^2 = \psi(a) + \psi(b)$, joten ψ on homomorfismi.

2. Olkoon $(G, *)$ ryhmä. Määritellään uusi laskutoimitus $\circledast$ joukossa G asettamalla

$$a \circledast b = b * a$$

kaikille $a, b \in G$. Osoita, että $(G, \circledast)$ on ryhmä.

Ratkaisu. Osoitetaan, että ryhmän määritelmän kolme ehtoa toteutuu.

Olkoot $a, b, c \in G$. Tällöin laskutoimituksen $\circledast$ määritelmän nojalla $a \circledast (b \circledast c) = (c*b)*a$. Laskutoimitus $*$ on assosiatiivinen, joten $(c*b)*a = c*(b*a)$, ja laskutoimituksen $\circledast$ määritelmän nojalla saadaan $c*(b*a) = (a \circledast b) \circledast c$. Yhdistämällä nämä yhtälöt saadaan haluttu yhtälö $a \circledast (b \circledast c) = (a \circledast b) \circledast c$, joten $\circledast$ on assosiatiivinen.

Olkoon $e \in G$ laskutoimituksen $*$ neutraalialkio. Tällöin $e \circledast g = g * e = g$ ja $g \circledast e = e * g = g$ kaikille $g \in G$. Siis e on laskutoimituksen $\circledast$ neutraalialkio.

Olkoon $g \in G$. Koska $(G, *)$ on ryhmä, on $\underline{g} \in G$, jolle pätee $g * \underline{g} = e = \underline{g} * g$. Mutta tästä seuraa $\underline{g} \circledast g = g * \underline{g} = e = \underline{g} * g = g \circledast \underline{g}$, joten $\underline{g}$ on alkion $g \in G$ käänteisalkio laskutoimituksella varustetussa joukossa $(G, \circledast)$.

3. Osoita, että $\mathrm{SL}_n(\mathbb{Z})$ varustettuna matriisien kertolaskulla on ryhmä.

Ratkaisu. Kuten Esimerkissä 8.2 lineaarialgebran kurssilla osoitetusta determinantin laskusäännöstä $\det AB = \det A \det B$ seuraa, että joukko $\mathrm{SL}_n(\mathbb{Z})$ on laskutoimituksella varustetun joukon $(\mathrm{Mat}_n(\mathbb{K}), \cdot)$ vakaa osajoukko ja matriisien kertolasku indusoi laskutoimituksen tähän joukkoon. Lineaarialgebran kurssilla on osoitettu, että matriisien kertolasku on assosiatiivinen laskutoimitus joukossa $\mathrm{Mat}_n(\mathbb{R})$ ja identtinen matriisi I_n on tämän laskutoimituksen neutraalialkio.

Olkoon $A \in \mathrm{SL}_n(\mathbb{Z})$. Lineaarialgebrasta tiedämme, matriisi A on kääntyvä ryhmässä $\mathrm{SL}_n(\mathbb{R})$. Matriisin A kofaktorimatriisin $\operatorname{cof} A$ kertoimet ovat matriisin A $(n-1) \times (n-1)$ alimatriisien determinantteja, erityisesti ne ovat kokonaislukuja. Lineaarialgebrasta tiedämme, että $A^{-1} = \frac{1}{\det A} \operatorname{cof} A = \operatorname{cof} A \in \mathrm{SL}_n(\mathbb{Z})$. Alkiolla $A \in \mathrm{SL}_n(\mathbb{Z})$ on siis käänteisalkio laskutoimituksella varustetussa joukossa $\mathrm{SL}_n(\mathbb{Z})$, joten $\mathrm{SL}_n(\mathbb{Z})$ on ryhmä

4. Todista Propositio 8.6: 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 $a, b \in A$.

Ratkaisu. Oletetaan, että A on ryhmä. Olkoot $a, b \in A$. Tällöin $a(a^{-1}b) = b$ ja $ba^{-1}a = b$, joten yhtälöillä on ratkaisut.

Oletetaan, että yhtälöillä $ax = b$ ja $ya = b$ on ratkaisut joukossa A kaikilla $a, b \in A$. Olkoon $e \in A$ neutralialkio ja olkoon $a \in A$. Oletuksen mukaan yhtälöillä $ax = e$ ja $ya = e$ on ratkaisut, joten alkiolla a on vasen ja oikea käänteisalkio. Assosiatiivisuuden nojalla $y = ye = y(ax) = (ya)x = ex = x$, joten $y = x$ on alkion a käänteisalkio. Siis A on ryhmä.

5. Todista Lemma 8.7: Äärellisen ryhmän laskutaulussa jokaisella rivillä ja jokaisessa sarakkeessa esiintyvät kaikki ryhmän alkiot.

Ratkaisu. Olkoon $G = \{g_1, g_2, \ldots, g_n\}$ äärellinen ryhmä, jossa on n alkiota ja olkoon $g \in G$. Alkion g rivillä laskutaulussa on alkiot $gg_1, gg_2, \ldots, gg_n$. Jos $gg_i = g_j$ joillain $i, j \in \{1, 2, \ldots, n\}$, niin supistussäännön nojalla $g_i = g_j$. Siis rivillä on n eri alkiota, joten kaikki esiintyvät joka rivillä. Sarakkeet käsitellään samaan tapaan.

6. Monellako eri tavalla voit täydentää taulukon

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

niin, että tuloksena on ryhmän laskutaulu? Mitä voit päätellä tästä havainnosta?

Ratkaisu. On vain yksi tapa täydentää laskutaulu siten, että kaikki alkiot esiintyvät jokaisella rivillä ja jokaisella sarakkeella:

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

Jos nimittäin valitsisimme $a * a = e$, pitäisi olla $a * b = b$ ja tällöin b olisi viimeisessä sarakkeessa kahdesti. Laskutaulun mukaan e on neutraalialkio ja $ab = ba = e$, joten jokaisella alkiolla on käänteisalkio. Koska alkioita on vain kolme, on helppo tarkastaa, että saadun laskutaulun kuvaama laskutoimitus on assosiatiivinen.

Päätelmän voi tehdä loppuun toisellakin tavalla. Päättelimme juuri, että on korkeintaan yksi ryhmä, jossa on kolme alkiota e, a ja b. Toisaalta tiedämme, että $(\mathbb{Z}/3\mathbb{Z}, +)$ on ryhmä. Sen laskutaulu on

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Laskutaulussa käytetään kongruenssiluokan $k + 3\mathbb{Z}$ merkintänä edustajaa $k \in \mathbb{Z}$.

Määritellään kuvaus $f\colon \mathbb{Z}/3\mathbb{Z} \to \{e, a, b\}$ asettamalla $f(0 + 3\mathbb{Z}) = e$, $f(1 + 3\mathbb{Z}) = a$ ja $f(2 + 3\mathbb{Z}) = b$. Laskutauluja vertaamalla. näemme, että $f\colon (\mathbb{Z}/3\mathbb{Z}, +) \to (\{e, a, b\}, *)$ on isomorfismi, joten $(\{e, a, b\}, *)$ on ryhmä.

7. 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 homomorfismeja?

Ratkaisu. Lineaarialgebran tietojen nojalla

$$T(AB) = {}^t(AB) = {}^tB^tA = T(B)T(A)$$

kaikille $A, B \in \mathrm{SL}_2(\mathbb{Z})$. Samoin pätee

$$\mathrm{inv}(AB) = (AB)^{-1} = B^{-1}A^{-1} = \mathrm{inv}(B)\,\mathrm{inv}(A)$$

kaikille $A, B \in \mathrm{SL}_2(\mathbb{Z})$. Koska $\mathrm{SL}_2(\mathbb{Z})$ ei ole kommutatiivinen (katso Esimerkki 1.9(c)), kuvaukset T ja inv eivät ole homomorfismeja. Toisaalta edellisten laskujen nojalla

$$T \circ \mathrm{inv}(AB) = T(\mathrm{inv}(B)\,\mathrm{inv}(A) = T \circ \mathrm{inv}(A) T \circ \mathrm{inv}(A)$$

ja

$$\mathrm{inv} \circ T(AB) = \mathrm{inv}(T(B)T(A) = \mathrm{inv} \circ T(A)\,\mathrm{inv} \circ T(A)$$

kaikille $A, B \in \mathrm{SL}_2(\mathbb{Z})$, joten $T \circ \mathrm{inv}$ ja $\mathrm{inv} \circ T$ ovat homomorfismeja.

8. Minkä kurssilla käsitellyn ryhmän kanssa ryhmä $(\mathbb{Z}/12\mathbb{Z})^\times$ on isomorfinen?

Ratkaisu. Proposition 8.22 nojalla $(\mathbb{Z}/12\mathbb{Z})^\times = \{1 + 12\mathbb{Z}, 5 + 12\mathbb{Z}, 7 + 12\mathbb{Z}, 11 + 12\mathbb{Z}\}$. Ryhmän $(\mathbb{Z}/12\mathbb{Z})^\times$ laskutaulu on

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

kun merkitsemme kongruenssiluokkaa $k + 12\mathbb{Z}$ edustajallaan $k \in \mathbb{Z}$. Vertaamalla ryhmän $(\mathbb{Z}/8\mathbb{Z})^\times$ laskutauluun

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

jossa merkitsemme kongruenssiluokkaa $k + 8\mathbb{Z}$ edustajallaan $k \in \mathbb{Z}$, huomaamme, että kuvaus

$$\begin{aligned} 1 + 8\mathbb{Z} &\mapsto 1 + 8\mathbb{Z}\,, \\ 3 + 8\mathbb{Z} &\mapsto 5 + 8\mathbb{Z}\,, \\ 5 + 8\mathbb{Z} &\mapsto 7 + 8\mathbb{Z}, \\ 7 + 8\mathbb{Z} &\mapsto 11 + 8\mathbb{Z} \end{aligned}$$

on ryhmäisomorfismi ryhmien $(\mathbb{Z}/8\mathbb{Z})^\times$ ja $(\mathbb{Z}/12\mathbb{Z})^\times$ välillä. Siis $(\mathbb{Z}/12\mathbb{Z})^\times$ ja $(\mathbb{Z}/8\mathbb{Z})^\times$ ovat isomorfisia ja Esimerkin 8.26 nojalla ne ovat isomorfisia Kleinin neliryhmän kanssa.