Algebra I
Harjoitus 6, 9.–13.3.2009
Ratkaisut (MV)
6 sivua

1. Olkoot M ja M' multiplikatiivisia monoideja. Kuvaus $f\colon M \to M'$ on *monoidihomomorfismi*, jos

$1°$ $f(ab) = f(a)f(b)$ kaikilla $a, b \in M$;
$2°$ $f(1_M) = 1_{M'}$.

Osoita esimerkillä, että ehto $2°$ ei seuraa ehdosta $1°$.

Ratkaisu. Valitaan $M = M' = \mathbb{N}$; laskutoimituksena kertolasku. Selvästi kuvaus $f\colon M \to M'$, $n \mapsto 0$, toteuttaa ehdon $1°$, mutta ei ehtoa $2°$.

2. Olkoon G ryhmä, jonka kertaluku on korkeintaan 5. Osoita, että G on Abelin ryhmä. *Ohje.* Voit menetellä vaikkapa seuraavasti. Oleta, että on olemassa alkiot $a, b \in G$, joilla $ab \neq ba$. Osoita, että tällöin $1, a, b, ab, ba$ ovat eri alkioita ja että G:n kertaluku on siis $|G| = 5$. Johda sitten yhtälöistä $aG = Ga\,(= G)$ ja $bG = Gb\,(= G)$ kaksi eri esitystä ab:lle ja niistä lopuksi ristiriita. Tässä esimerkiksi $aG = \{ax \mid x \in G\}$ ja $Ga = \{xa \mid x \in G\}$

Ratkaisu. Tehdään vastaoletus: On olemassa alkiot $a, b \in G$ siten, että $ab \neq ba$. Osoitetaan, että joukossa $\{1, a, b, ab, ba\}$ on tällöin täsmälleen 5 alkiota.

- Osoitetaan, että $1 \neq a$, $1 \neq b$, $1 \neq ab$ ja $1 \neq ba$: $1 \neq a$, koska muuten $ab = b = ba$. Samoin $1 \neq b$. $1 \neq ab$, koska muuten $a = b^{-1}$ ja tällöin pätisi myös $ba = bb^{-1} = 1 = ab$. Samasta syystä $1 \neq ba$.
- Osoitetaan, että $a \neq b$, $a \neq ab$ ja $a \neq ba$: $a \neq b$, koska muuten $ab = a^2 = ba$. Ehdoista $a = ab$ ja $a = ba$ seuraisi kummastakin, että $b = 1$, mikä on vastoin kohtaa $1°$. Siis $a \neq ab$ ja $a \neq ba$.
- Osoitetaan, että $b \neq ab$ ja $b \neq ba$: Jos toinen yhtäsuuruuksista $b = ab$ ja $b = ba$ olisi voimassa, niin saataisiin $a = 1$ vastoin kohtaa $1°$.
- Oletuksen nojalla $ab \neq ba$.

Oletuksen nojalla $|G| = 5$ ja joukossa $\{1, a, b, ab, ba\}$ on täsmälleen 5 alkiota, joten $G = \{1, a, b, ab, ba\}$. Koska G on ryhmä, niin $aG = G = Ga$ eli

$$\{a, a^2, ab, a^2b, aba\} = \{a, a^2, ba, aba, ba^2\}.$$

Alkiot a ja a^2 esiintyvät kummassakin joukossa ja $ba \neq ab$ oletuksen nojalla, joten joko $ab = aba$, jolloin $a = 1$, tai $ab = ba^2$. Koska on osoitettu, että $a \neq 1$, niin pitää olla $ab = ba^2$. Lisäksi

$$\{b, ba, b^2, bab, b^2a\} = bG = Gb = \{b, ab, b^2, ab^2, bab\},$$

joten vastaavasti nähdään, että $ab = b^2a$. Siispä $b^2a = ba^2$, mistä seuraa, että $b = a$. Tämä on ristiriidassa oletuksen $ab \neq ba$ kanssa, kuten yllä on osoitettu. Vastaoletus on siis väärä ja ryhmän G täytyy olla Abelin ryhmä.

3. Olkoon $X \subset \mathbb{R}^2$ suljettu suorakaide kärkinään $A = (0,0)$, $B = (2,0)$, $C = (2,1)$ ja $D = (0,1)$. Määritä suorakaiteen X symmetrioiden ryhmän G alkiot ja niiden tulot. (Suorakaiteen X *symmetria* on etäisyydet säilyttävä bijektio $f\colon X \to X$, ja laskutoimituksena on kuvausten yhdistäminen.)

Ratkaisu. Olkoon $f\colon X \to X$ symmetria. Etäisyys pisteestä A pisteeseen C on $\sqrt{(2-0)^2 + (1-0)^2} = \sqrt{5}$, mikä on sama kuin pisteiden B ja D etäisyys toisistaan. Jos valitaan pisteet $P, Q \in X$ siten, että P ja Q eivät ole vastakkaisia kärkiä (eli ei päde $P = A$ ja $Q = C$ tai $P = B$ ja $Q = D$), niin $\|P - Q\| < \sqrt{5}$. Näin ollen symmetrian f pitäisi kuvata kärjet kärjille siten, että vastakkaiset kärjet päätyvät vastakkaisille kärjille.

Lisäksi havaitaan, että tehtävän suorakaide ei ole symmetrinen halkaisijoidensa suhteen eli minkä tahansa kärjen etäisyys sen viereiseen kärkeen vaihtelee sen mukaan kumpi näistä vieressä olevista kärjistä valitaan. Esimerkiksi $\|A - B\| \neq \|A - D\|$, sillä $\|A - B\| = 2$ ja $\|A - D\| = 1$. Näiden tietojen avulla nähdään, mitä $f(B)$, $f(C)$ ja $f(D)$, jos $f(A)$ tiedetään. Jos esimerkiksi $f(A) = A$, niin $f(C) = C$, koska C on A:n vastakkainen kärki, ja $f(B) = B$, koska

$$f(B) \in \{A, B, C, D\} \setminus \{f(A), f(C)\} = \{B, D\}$$

ja pitää olla $\|f(A) - f(B)\| = \|A - B\| = 2$. Käsittelemällä näin tapaukset $f(A) = A$, $f(A) = B$, $f(A) = C$ ja $f(A) = D$ päädytään siihen, että mielivaltaisen symmetrian f rajoittuma kärkien joukkoon on siis jokin seuraavista permutaatioista:

$$\begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix},$$
$$\begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}.$$

Näitä permutaatiota vastaavat ainakin seuraavat symmetriat:

$$f_0\colon (x,y) \mapsto (x,y), \quad f_1\colon (x,y) \mapsto (2-x, y),$$
$$f_2\colon (x,y) \mapsto (2-x, 1-y), \quad f_3\colon (x,y) \mapsto (x, 1-y).$$

Tässä f_0 on identtinen kuvaus, f_1 ja f_3 ovat peilaukset pysty- ja vaaka-akselien suhteen ja f_4 on peilaus sekä pysty- että vaaka-akselin suhteen.

Osoitetaan sitten, että pisteet $f(A), f(B), f(C)$ ja $f(D)$ määräävät symmetrian f täysin eli $f(P)$ tunnetaan kaikilla $P \in X$, jos $f(A), f(B), f(C)$ ja $f(D)$ tunnetaan. Oletetaan tunnetuksi, että kahden tai useamman eri ympyrän leikkaus sisältää kaksi pistettä vain, jos ympyröiden keskipisteet sijaitsevat samalla suoralla. Merkitään P-keskistä, r-säteistä ympyrää $S(P, r)$. Jos $P \in X$ ja P ei ole kärki, niin on olemassa sellaiset $r_A, r_B, r_C, r_D > 0$, että

$$P \in S(A, r_A) \cap S(B, r_B) \cap S(C, r_C) \cap S(D, r_D).$$

Koska f on symmetria, niin

$$f(P) \in S(f(A), r_A) \cap S(f(B), r_B) \cap S(f(C), r_C) \cap S(f(D), r_D).$$

Pisteet $f(A), f(B), f(C)$ ja $f(D)$ eivät ole kaikki samalla suoralla, joten $f(P)$ on täysin näiden pisteiden määräämä. Tästä seuraa, että edellä mainitut f_0, f_1, f_2 ja f_3 ovat kaikki suorakaiteen X symmetriat. Siis $G = \{f_0, f_1, f_2, f_3\}$ ja tehtävän 2 nojalla G on Abelin ryhmä ja selvästi $f_0 = \mathrm{id}$ on neutraalialkio. Kaikkien symmetrioiden tulojen sijaan tarvitsee siis listata vain tulot $f_j \circ f_i$, missä $0 < i \leq j \leq 3$. Saadaan

$$\begin{gathered}
f_1 \circ f_1 = f_0\colon (x,y) \mapsto (2-x,y) \mapsto (2-(2-x),y) = (x,y),\\
f_2 \circ f_1 = f_3\colon (x,y) \mapsto (2-x,y) \mapsto (2-(2-x),1-y) = (x,1-y)\\
f_3 \circ f_1 = f_2\colon (x,y) \mapsto (2-x,y) \mapsto (2-x,1-y)\\
f_2 \circ f_2 = f_0\colon (x,y) \mapsto (2-x,1-y) \mapsto (2-(2-x),1-(1-y)) = (x,y)\\
f_3 \circ f_2 = f_1\colon (x,y) \mapsto (2-x,1-y) \mapsto (2-x,1-(1-y)) = (2-x,y)\\
f_3 \circ f_3 = f_0\colon (x,y) \mapsto (x,1-y) \mapsto (x,1-(1-y)) = (x,y).
\end{gathered}$$

Muodostetaan saaduista tuloista vielä kertotaulu:

$\circ$	f_0	f_1	f_2	f_3
f_0	f_0	f_1	f_2	f_3
f_1	f_1	f_0	f_3	f_2
f_2	f_2	f_3	f_0	f_1
f_3	f_3	f_2	f_1	f_0

Huomautus. Jos X olisi neliö kärkinään $A = (-1,-1)$, $B = (1,-1)$, $C = (1,1)$ ja $D = (-1,1)$, niin X:n symmetrioiden ryhmä G saadaan samaan tapaan kuin yllä. Edelleen pitää vastakkaisten kärkien kuvautua vastakkaisiksi kulmapisteiksi, mutta vierekkäisten kärkien kuvautumiselle ei ole samaa rajoitusta kuin halkaisijoidensa suhteen ei-symmetrisessä suorakaiteessa. Esimerkiksi, jos f on X:n symmetria ja $f(A) = A$, niin edelleen pitää olla $f(C) = C$, mutta voi olla $f(B) = D$, sillä pisteiden A ja D keskinäinen etäisyys on sama kuin pisteiden A ja B. Sallitut kärkien permutaatiot ovat siis

$$\begin{gathered}
\begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix},\\
\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix},\\
\begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}
\end{gathered}$$

ja näitä vastaavat symmetriat ovat

$$\begin{gathered}
(x,y) \mapsto (x,y), \quad (x,y) \mapsto (y,x), \quad (x,y) \mapsto (-y,x), \quad (x,y) \mapsto (-x,y),\\
(x,y) \mapsto (-y,-x), \quad (x,y) \mapsto (-x,-y), \quad (x,y) \mapsto (y,-x), \quad (x,y) \mapsto (x,-y).
\end{gathered}$$

Sen osoittamiseksi, että nämä ovat kaikki X:n symmetriat kelpaa sama todistus kuin yllä. Ryhmää G kutsutaan tällöin tietysti neliön symmetriaryhmäksi ja sen alkiot vastaavat identtistä kuvausta, 90°, 180° ja 270° kiertoja ja peilauksia pysty- ja vaaka-akselien ja molempien halkaisijoiden suhteen.

4. Ratkaise yhtälöt $a \circ x = b$ ja $y \circ a = b$ ryhmässä S_4, kun

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

Ratkaisu. Suoraan permutaatioiden a ja b määritelmistä nähdään, että

$$a^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = b.$$

Näin ollen

$$\begin{aligned} x = (a^{-1} \circ a) \circ x = a^{-1} \circ (a \circ x) = b \circ b \quad \text{ja} \\ y = y \circ (a \circ a^{-1}) = (y \circ a) \circ a^{-1} = b \circ b. \end{aligned}$$

Koska

$$\begin{aligned} (b \circ b)(1) = b(3) = 4, \quad (b \circ b)(2) = b(2) = 2, \\ (b \circ b)(3) = b(4) = 1, \quad (b \circ b)(4) = b(1) = 3, \end{aligned}$$

niin

$$x = y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

eli $x = y = a$.

5. Onko $\{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}$ ryhmän $(\mathbb{Z}_{11}^*, \cdot)$ aliryhmä? Entä $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{8}\}$?

Ratkaisu. Jälkimmäinen osajoukoista ei ole aliryhmä, sillä se ei ole vakaa laskutoimituksen suhteen: $\overline{3} \cdot \overline{3} = \overline{9} \notin \{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{8}\}$.
Merkitään $A = \{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}$ ja todistetaan, että $A \leq \mathbb{Z}_{11}^*$. Käydään läpi monisteen vaatimukset (s. 55–56):

i) Koska $\overline{1} \cdot a = a \in A$ kaikilla $a \in A$ ja koska $\mathbb{Z}_{11}^*$ on vaihdannainen, tarvitsee tarkistaa vain, että $\overline{n} \cdot \overline{m} \in A$ kaikilla $n \leq m$. Näin ollen, koska

$$\begin{aligned} \overline{3} \cdot \overline{3} = \overline{9}, \quad \overline{3} \cdot \overline{4} = \overline{12} = \overline{1}, \quad \overline{3} \cdot \overline{5} = \overline{15} = \overline{4}, \quad \overline{3} \cdot \overline{9} = \overline{27} = \overline{5} \\ \overline{4} \cdot \overline{4} = \overline{16} = \overline{5}, \quad \overline{4} \cdot \overline{5} = \overline{20} = \overline{9}, \quad \overline{4} \cdot \overline{9} = \overline{36} = \overline{3} \\ \overline{5} \cdot \overline{5} = \overline{25} = \overline{3}, \quad \overline{5} \cdot \overline{9} = \overline{45} = \overline{1}, \quad \overline{9} \cdot \overline{9} = \overline{81} = \overline{4} \end{aligned}$$

ovat kaikki joukon A alkioita, A on vakaa kertolaskun suhteen.

ii) $1_{\mathbb{Z}_{11}^*} = \overline{1} \in A$

iii) Käänteisalkiot nähdään i-kohdan listasta:

$$\overline{1}^{-1} = \overline{1}, \quad \overline{3}^{-1} = \overline{4}, \quad \overline{4}^{-1} = \overline{3}, \quad \overline{5}^{-1} = \overline{9}, \quad \overline{9}^{-1} = \overline{5}.$$

A siis sisältää alkioidensa käänteisalkiot.

Määritelmän mukaan A on ryhmän $(\mathbb{Z}_{11}^*, \cdot)$ aliryhmä.

6. Kuvaus $f\colon \mathbb{R} \to \mathbb{R}$ on bi-Lipschitz, jos on olemassa sellainen luku $L \geq 1$, että

$$|x-y|/L \leq |f(x)-f(y)| \leq L|x-y| \quad \text{kaikilla } x, y \in \mathbb{R}.$$

Voidaan osoittaa, että tällöin f on aidosti monotoninen bijektio [J. Väisälä: *Topologia I*, ht. 4:10 ja ht. 9:11]. Permutaatioryhmän $S_{\mathbb{R}}$ alkioina ovat taas kaikki bijektiot $\mathbb{R} \to \mathbb{R}$ ja laskutoimituksena kuvausten yhdistäminen.

a) Osoita, että bi-Lipschitz-kuvausten $\mathbb{R} \to \mathbb{R}$ joukko BL on ryhmän $S_{\mathbb{R}}$ aliryhmä.

b) Sen tiedon avulla, että jokainen $f \in \mathrm{BL}$ on aidosti monotoninen eli siis joko aidosti kasvava ($f(x) < f(y)$, kun $x, y \in \mathbb{R}$ ja $x < y$) tai aidosti vähenevä ($f(x) > f(y)$, kun $x, y \in \mathbb{R}$ ja $x < y$), määritä ryhmän BL alkioiden kertalukujen joukko

$$\{\mathrm{ord}(f) \mid f \in \mathrm{BL}\} \subset \mathbb{N}_+ \cup \{\infty\}.$$

Tässä siis kuvaukselle $f \in \mathrm{BL}$ on $\mathrm{ord}(f) = \min\{n \in \mathbb{N}_+ \mid f^n = \mathrm{id}_{\mathbb{R}}\}$, jos on olemassa $n \in \mathbb{N}_+$, jolla $f^n = \mathrm{id}_{\mathbb{R}}$; muutoin on $\mathrm{ord}(f) = \infty$.

Ratkaisu. a) Pitää todistaa, että i) $f \circ g$ on bi-Lipschitz, jos f ja g ovat, ii) $1_{S_{\mathbb{R}}} = \mathrm{id}_{\mathbb{R}}$ on bi-Lipschitz ja iii) f^{-1} on bi-Lipschitz, kun f on.

i) Olkoot $L_1, L_2 \geq 1$ siten, että kaikilla $x, y \in \mathbb{R}$

$$\begin{gathered} |x-y|/L_1 \leq |f(x)-f(y)| \leq L_1|x-y| \quad \text{ja} \\ |x-y|/L_2 \leq |g(x)-g(y)| \leq L_2|x-y|. \end{gathered}$$

Tällöin kaikilla $x, y \in \mathbb{R}$

$$|(f \circ g)(x) - (f \circ g)(y)| \leq L_1|g(x)-g(y)| \leq L_1L_2|x-y|$$

ja

$$|(f \circ g)(x) - (f \circ g)(y)| \geq |g(x)-g(y)|/L_1 \geq |x-y|/L_1L_2.$$

Koska $L_1L_2 \geq 1$, niin $f \circ g \in \mathrm{BL}$.

ii) Jos valitaan $L = 1$, niin tietysti

$$|x-y|/L \leq |\,\mathrm{id}_{\mathbb{R}}(x) - \mathrm{id}_{\mathbb{R}}(y) \leq L|x-y| \quad \text{kaikilla } x, y \in \mathbb{R},$$

joten $\mathrm{id}_{\mathbb{R}} \in \mathrm{BL}$.

iii) Olkoon $L \geq 1$ siten, että

$$|x-y|/L \leq |f(x)-f(y)| \leq L|x-y| \quad \text{kaikilla } x, y \in \mathbb{R}.$$

Tällöin kaikilla $x, y \in \mathbb{R}$

$$|f^{-1}(x) - f^{-1}(y)|/L \leq |f(f^{-1}(x)) - f(f^{-1}(x))| = |x-y|$$

ja

$$L|f^{-1}(x) - f^{-1}(x)| \geq |f(f^{-1}(x)) - f(f^{-1}(x))| = |x - y|,$$

joten

$$|x - y|/L \leq |f^{-1}(x) - f^{-1}(x)| \leq L|x - y|.$$

Siispä $f^{-1} \in \mathrm{BL}$.

On osoitettu, että $\mathrm{BL} \leq S_{\mathbb{R}}$.

b) Jos $f = \mathrm{id}_{\mathbb{R}}$, niin tietysti $\mathrm{ord}(f) = 1$, ja jos $f = -\mathrm{id}_{\mathbb{R}}$ eli $f(x) = -x$ kaikilla $x \in \mathbb{R}$, niin $\mathrm{ord}(f) = 2$. Osoitetaan, että jos $\mathrm{ord}(f) \neq 1$ ja $\mathrm{ord}(f) \neq 2$, niin $\mathrm{ord}(f) = \infty$ eli $f^n \neq \mathrm{id}_{\mathbb{R}}$ kaikilla $n \in \mathbb{N}_+$. Koska on olemassa bi-Lipschitz-kuvauksia $\mathbb{R} \to \mathbb{R}$, joiden kertaluku ei ole 1 eikä 2 (esim. $x \mapsto 2x$), tästä seuraa, että $\{\mathrm{ord}(f) \mid f \in \mathrm{BL}\} = \{1, 2, \infty\}$.
Joko f on aidosti kasvava tai aidosti vähenevä. Oletetaan aluksi, että f on aidosti kasvava. Koska $f \neq \mathrm{id}_{\mathbb{R}}$, on olemassa $x \in \mathbb{R}$ siten, että $f(x) \neq x$. Jos $f(x) > x$, niin kuvauksen f aidosta kasvavuudesta seuraa induktion avulla, että $f^n(x) > f^{n-1}(x)$ ja $f^n(x) > x$ kaikilla $n \in \mathbb{N}_+$; erityisesti siis $f^n(x) > x$ kaikilla $n \in \mathbb{N}_+$. Tällöin $\mathrm{ord}(f) = \infty$. Jos taas $f(x) < x$, niin samaan tapaan voidaan todistaa induktiolla, että $f^n(x) < f^{n-1}(x)$ ja $f^n(x) < x$ kaikilla $n \in \mathbb{N}_+$, joten jälleen $\mathrm{ord}(f) = \infty$.
Olkoon sitten f aidosti vähenevä. Koska $\mathrm{ord}(f) \neq 2$, niin $f^2 \neq \mathrm{id}_{\mathbb{R}}$. Koska f on aidosti vähenevä, niin kaikilla $x < y$ pätee $f(x) > f(y)$, joten $f^2(x) < f^2(y)$. Siis f^2 on aidosti kasvava ja edellä nähdyn nojalla $f^{2n} = (f^2)^n \neq \mathrm{id}_{\mathbb{R}}$ kaikilla $n \in \mathbb{N}_+$. Jos jollakin $n \in \mathbb{N}_+$ pätisi $f^{2n-1} = \mathrm{id}_{\mathbb{R}}$, niin silloin pätisi myös $f^{2(2n-1)} = \mathrm{id}_{\mathbb{R}}$, mikä olisi edellä nähdyn nojalla mahdotonta, sillä $2n - 1 \in \mathbb{N}_+$. Siten myös $f^{2n-1} \neq \mathrm{id}_{\mathbb{R}}$ kaikilla $n \in \mathbb{N}_+$, joten $f^n \neq \mathrm{id}_{\mathbb{R}}$ kaikilla $n \in \mathbb{N}_+$. Siis $\mathrm{ord}(f) = \infty$.