Klassiset ryhmät
Matematiikan ja tilastotieteen laitos
Harjoitus 5, ratkaisuehdotus
7 sivua

1. (a) Osoita, että kunnissa $\mathbb{F}_p$, missä p on alkuluku, ja rationaalilukujen kunnassa $\mathbb{Q}$ ei ole mahdollista määritellä konjugaatioautomorfismia $\sigma(a) = \bar{a}$.

   (b) Osoita, että kunnassa

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

   voidaan määritellä konjugaatioautomorfismi. (Tarkista ensin, että $\mathbb{Q}(\sqrt{2})$

Ratkaisu:

a) Olkoon $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ konjugaatioautomorfismi. Olkoon sitten $\alpha \in \mathbb{F}_p$, jolloin $\alpha = n \cdot 1$ jollakin luonnollisella luvulla n. Nyt

$$\sigma(\alpha) = \sigma(n \cdot 1) = n\alpha(1) = n \cdot 1 = \alpha,$$

sillä σ on kuntahomomorfismi. Siten σ on identtinen kuvaus, mikä on ristiriita.

Olkoon $\sigma : \mathbb{Q} \to \mathbb{Q}$ konjugaatioautomorfismi. Koska se on kuntahomomorfismi, niin $\sigma(n) = n$ ja $\sigma(-n) = -\sigma(n) = -n$ kaikilla $n \in \mathbb{N}$. Olkoon sitten $q = a/b \in \mathbb{Q}$, missä $a, b \in \mathbb{Z}$. Nyt

$$\sigma(q) = \sigma(a) \cdot \sigma(b)^{-1} = a \cdot b^{-1} = q.$$

Siten σ on identtinen kuvaus, mikä on ristiriita.

b) Osoitetaan aluksi, että $\mathbb{Q}(\sqrt{2})$ on kunta. Koska $\mathbb{Q}(\sqrt{2})$ on $\mathbb{R}$:n osajoukko, niin laskutoimitusten liitännäisyyttä ja osittelulakia ei tarvitse erikseen tutkia.

Koska $0 = 0 + 0 \cdot \sqrt{2}$ ja $1 = 1 + 0 \cdot \sqrt{2}$, niin $0, 1 \in \mathbb{Q}(\sqrt{2})$.
Jos $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ ja $a' + b'\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, niin

$$(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

ja

$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Lisäksi

$$-(a + b\sqrt{2}) = -a + (-b)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

ja

$$(a + b \cdot \sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Siten $Q(\sqrt{2})$ on kunta.
Määritellään kuvaus $\sigma : Q(\sqrt{2}) \to Q(\sqrt{2})$ siten, että $\sigma(a + b \cdot \sqrt{2}) = a - b \cdot \sqrt{2}$. Se on itsensä käänteiskuvaus, mistä seuraa että kyseessä on kääntyvä kuvaus, jonka kertaluku on kaksi.
Osoitetaan vielä, että σ on kuntahomomorfismi. Jos $a+b\sqrt{2} \in Q(\sqrt{2})$ ja $a' + b'\sqrt{2} \in Q(\sqrt{2})$, niin

$$\begin{aligned}
&\sigma\left((a + b\sqrt{2}) + (a' + b'\sqrt{2})\right) = \sigma\left((a + a') + (b +' b)\sqrt{2}\right) \\
&= (a + a') - (b + b')\sqrt{2} = a - b\sqrt{2} + a' - b'\sqrt{2} \\
&= \sigma(a + b\sqrt{2}) + \sigma(a' + b'\sqrt{2})
\end{aligned}$$

ja

$$\begin{aligned}
&\sigma\left((a + b\sqrt{2})(a' + b'\sqrt{2})\right) = \sigma\left((aa' + 2bb') + (ab' + a'b)\sqrt{2}\right) \\
&= (aa' + 2bb') - (ab' + a'b)\sqrt{2} = (a - b\sqrt{2})(a' - b'\sqrt{2}) \\
&= \sigma(a + b\sqrt{2})\sigma(a' + b'\sqrt{2}).
\end{aligned}$$

Siten σ on kuntahomomorfismi.
Lasketaan vielä normikuvaus. Jos $a + b\sqrt{2} \in Q(\sqrt{2})$, niin

$$\begin{aligned}
N(a + b\sqrt{2}) &= (a + b\sqrt{2})\sigma(a + b\sqrt{2}) \\
&= (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.
\end{aligned}$$

2. Osoita, että $U(V)/SU(V) \cong \operatorname{Ker} N$, missä N on normikuvaus $\lambda \mapsto \lambda\bar{\lambda}$.

   Ratkaisu:

   Olkoon $f : U(V) \to \operatorname{Ker}(N)$, $f(g) = \det(g)$. Koska jokaiselle unitaarisen ryhmän alkiolle g pätee $\det(g)\overline{\det(g)} = 1$, niin kuvauksen maalijoukko voidaan todellakin asettaa $\operatorname{Ker}(N)$. Tiedämme, että g on homomorfismi. Lisäksi $\operatorname{Ker}(f) = SU(V)$.

   Osoitetaan seuraavaksi, että f on surjektio. Olkoon S avaruuden V seskvilineaarinen muoto. Lauseen 6.5. nojalla voimme olettaa, että S on diagonaalimatriisi

$$S = \begin{bmatrix} \alpha_1 & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_n \end{bmatrix}.$$

Olkoon sitten $\beta \in \mathrm{Ker}(N)$, jolloin $\beta\overline{\beta} = 1$. Olkoon g diagonaalimatriisi

$$g = \begin{bmatrix} \beta & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}.$$

Nyt

$$g^\top S \overline{q} = \begin{bmatrix} \beta\alpha_1\overline{\beta} & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_n \end{bmatrix} = \begin{bmatrix} \beta\overline{\beta}\alpha_1 & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_n \end{bmatrix} = S,$$

joten g on unitaarinen. Koska $f(g) = \beta$, niin olemme osoittaneet, että f on surjektiivinen. Ryhmien homomorfialauseen nojalla $U(V)/SU(V) \cong \mathrm{Ker}(N)$.

3. Muodosta kunta $\mathbb{F}_4$ samaan tapaan kuin esimerkissä 6.13; aloita etsimällä juureton $\mathbb{F}_2$-kertoiminen toisen asteen polynomi g. Muodosta tekijästruktuuri, jossa samastetaan ne polynomit f_1 ja f_2, joilla pätee $f_1 - f_2 = hg$ jollain polynomilla h. Kirjoita kunnan alkioiden yhteenlasku- ja kertotaulut.

   Minkälainen on konjugoiva automorfismi kunnassa $\mathbb{F}_4$? Käyttäen hermiittistä muotoa $S = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ selvitä vektoriavaruuden $\mathbb{F}_4^2$ kaikkien vektorien arvot neliömuodossa $Q(v) = S(v, v)$.

Ratkaisu:

Valitaan polynomi $x^2 + x + 1$. Koska $1^2 + 1 + 1 = 1$ ja $0^0 + 0 + 1 = 1$, niin polynomilla ei ole juuria kunnassa $\mathbb{F}_2$. Merkitään

$$\mathbb{F}_4 = \mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle.$$

Koska $x^2 + x + 1$ on jaoton kunnassa $\mathbb{F}_2$, niin $\mathbb{F}_4$ on kunta.

Tutkitaan sitten tämän kunnan alkioita. Merkitään $P = \langle x^2 + x + 1 \rangle$, jolloin $\mathbb{F}_4 = \{g + P \mid g \in \mathbb{F}[x]\} = \{P, 1 + P, x + P, (x + 1) + P\}$. Huomataan, että P ja $1 + P$ ovat yhteen- ja kertolaskun neutraalialkiot ja merkitään (kaukonäköisesti)

$$\begin{aligned} \omega &= x + P \\ \overline{\omega} &= (x + 1) + P. \end{aligned}$$

Nyt yhteenlaskutauluksi saadaan

$+$	0	1	ω	$\overline{\omega}$
0	0	1	ω	$\overline{\omega}$
1	1	0	$\overline{\omega}$	ω
ω	ω	$\overline{\omega}$	0	1
$\overline{\omega}$	$\overline{\omega}$	ω	1	0

ja kertolaskutauluksi

$\cdot$	1	ω	$\overline{\omega}$
1	1	ω	$\overline{\omega}$
ω	ω	$\overline{\omega}$	1
$\overline{\omega}$	$\overline{\omega}$	1	ω

Olkoon σ kunnan $\mathbb{F}_4$ konjugaatioautomorfismi. Koska $\sigma(0) = 0$ ja $\sigma(1) = 1$, ja σ:n kertaluku on kaksi, niin on pakko olla $\sigma(\omega) = \overline{\omega}$.

Jos nyt $v = (v_1, v_2) \in \mathbb{F}_4^2$, niin $Q(v) = v_1\overline{v_1} + v_2\overline{v_2}$. Kertotaulusta näemme, että $\alpha\overline{\alpha} = 1$ kaikilla $\alpha \in \mathbb{F}_4^*$, mistä seuraa, että

$$Q(v) = \begin{cases} 1 & \text{jos } v_1 = 0 \neq v_2 \text{ tai } v_1 \neq 0 = v_2 \\ 0 & \text{muuten.} \end{cases}$$

4. Olkoon $(u_1, v_1, \ldots, u_m, v_m)$ symplektinen kanta K-kertoimisessa avaruudessa. Järjestetään kantavektorit uudelleen, jotta saadaan kanta $S = (u_1, \ldots, u_m, v_1, \ldots, v_m)$. Osoita, että tämän kannan suhteen kirjoitettuna matriisi

$$g = \begin{bmatrix} A & 0_m \\ 0_m & (A^\top)^{-1} \end{bmatrix}$$

esittää symplektistä kuvausta kaikilla $A \in GL_m(K)$. Päättele tästä, että ryhmällä $Sp_{2m}(K)$ on aliryhmä, joka on isomorfinen ryhmän $GL_m(K)$ kanssa.

Ratkaisu:

Olkoon B avaruuden K^n symplektistä kantaa vastaavaa alternoiva muoto. Kannan $(u_1, \ldots u_m, v_1, \ldots v_m)$ suhteen kirjoitettuna muodon matriisi on

$$B = \begin{bmatrix} 0 & I_m \\ -I_m & 0 \end{bmatrix}.$$

Olkoon $A \in GL_m(K)$. Nyt

$$\begin{aligned} g^\top B g &= \begin{bmatrix} A^\top & 0 \\ 0 & A^{-1} \end{bmatrix} \begin{bmatrix} 0 & I_m \\ -I_m & 0 \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & (A^\top)^{-1} \end{bmatrix} \\ &= \begin{bmatrix} 0 & A^\top \\ -A^{-1} & 0 \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & (A^\top)^{-1} \end{bmatrix} = \begin{bmatrix} 0 & I_m \\ -I_m & 0 \end{bmatrix} = B. \end{aligned}$$

Siten g on symplektinen.

Määritellään kuvaus

$$f : GL_m(K) \to Sp_{2m}(K), \quad f(A) = \begin{bmatrix} A & 0 \\ 0 & (A^\top)^{-1} \end{bmatrix}.$$

Se on selvästikin injektio.

Kuvaus on myös homomorfismi, sillä

$$\begin{aligned} f(AB) &= \begin{bmatrix} AB & 0 \\ 0 & (AB^\top)^{-1} \end{bmatrix} = \begin{bmatrix} AB & 0 \\ 0 & (A^\top)^{-1}(B^\top)^{-1} \end{bmatrix} \\ &= \begin{bmatrix} A & 0 \\ 0 & (A^\top)^{-1} \end{bmatrix} \begin{bmatrix} B & 0 \\ 0 & (B^\top)^{-1} \end{bmatrix} = f(A)f(B). \end{aligned}$$

Siten $f(A)$ on ryhmän $Sp_{2m}(K)$ aliryhmä, joka on isomorfinen ryhmän $GL_m(K)$ kanssa.

5. Olkoon V jokin K-kertoiminen vektoriavaruus, ja olkoon $u \in V \setminus \{0\}$. Osoita, että symplektisistä transvektioista koostuva joukko

$$T_u = \{\tau_{u,a} \mid a \in K\}$$

on ryhmä, ja sellaisena isomorfinen kunnan K additiivisen ryhmän kanssa. Päättele tästä, että ryhmällä $Sp(V)$ on aliryhmänä $(K, +)$.

Ratkaisu:

Osoitetaan, että T_u on ryhmä, kun laskutoimituksena on kuvausten yhdistäminen. Koska $\tau_{u,0}(v) = v$ kaikilla $v \in V$, niin $\mathrm{id}_V = \tau_{u,0} \in T_u$. Olkoot $a, b \in K$. Nyt

$$\begin{aligned} (\tau_{u,a}\tau_{u,b})(v) &= \tau_{u,a}(\tau_{u,b}(v)) = \tau_{u,a}(v + aB(u,v)u) \\ &= v + aB(u,v)u + bB(u, v + aB(u,v)u)u \\ &= v + aB(u,v)u + bB(u,v)u + abB(u,v)\underbrace{B(u,u)}_{=0}u \\ &= v + (a+b)B(u,v)u = \tau_{u,a+b} \in T_u. \end{aligned}$$

Lisäksi

$$(\tau_{u,a}\tau_{u,-a}) = t_{u,0} = \mathrm{id}_V,$$

joten $\tau_{u,a}^{-1} = \tau_{u,-a} \in T_u$. Siten T_u on ryhmä.

Olkoon $f : (T_u, \cdot) \to (K, +)$, $f(a) = \tau_{u,a}$. Kuvaus on selvästikin surjektio. Se on myös injektio, sillä jos $f(a) = \mathrm{id}_V$, niin $\tau_{u,a}(v) = v$ kaikilla $v \in V$, ja siten $v + aB(u,v)u = v$ kaikilla $v \in V$. Tästä seuraa, että $aB(u,v)u = 0$ kaikilla $v \in V$. Koska muoto B ei voi olla surkastunut, niin on olemassa sellainen $v \in V$, jolla $B(u,v) \neq 0$. Siten on pakko olla $a = 0$, ja f on injektio.

Osoitetaan lopuksi, että f on ryhmähomomorfismi. Jos $a, b \in K$, niin tehtävän alkuosan laskuista seuraa, että

$$f(a+b) = \tau_{u,a+b} = \tau_{u,a}\tau_{u,b} = f(a)f(b).$$

Siten f on ryhmähomomorfismi.

6. (a) Olkoon K kunta. Osoita, että $Sp_2(K) = SL_2(K)$.

(b) Tarkastellaan ryhmää $U(n) = U_n(\mathbb{C})$, muotona hermiittinen pistetulo. Osoita, että on olemassa bilineaariset muodot A ja B, joille pätee $U(n) \cong O_{2n}^{(A)}(\mathbb{R}) \cap Sp_{2n}^{(B)}(\mathbb{R})$.

Ratkaisu:

(a) Olkoon B avaruuden V alternoiva bilineaarinen muoto, ja valitaan kanta niin, että muodon matriisi on

$$B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Olkoon

$$L = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Nyt

$$\begin{aligned} L^\top BL = \begin{bmatrix} a & c \\ d & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \begin{bmatrix} 0 & -bc + ad \\ -ad + bc & 0 \end{bmatrix} \\ &= \begin{bmatrix} 0 & \det(L) \\ -\det(L) & 0 \end{bmatrix}. \end{aligned}$$

Siten $L \in Sp_2(K)$ jos ja vain jos $L \in SL_2(K)$.

(b) Olkoon S avaruuden $\mathbb{C}^n$ hermiittinen pistetulo. Samastetaan avaruudet $\mathbb{C}^n$ ja $\mathbb{R}^{2n}$ kuvauksella ι samaan tapaan kuin luentomateriaalin luvussa 7.4, ja merkitään $\iota(x) = x'$ kaikilla $x \in \mathbb{C}^n$.

Oletetaan sitten, että $L \in U_n(\mathbb{C})$. Määritellään kuvaus $L' : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ siten, että $L'(x') = L(x)'$. Huomataan, että L' on $\mathbb{R}$-kertoimisen vektoriavaruuden $\mathbb{R}^{2n}$ lineaarikuvaus. Jos nimittäin $\alpha \in \mathbb{R}$ ja $x', y' \in \mathbb{R}^{2n}$, niin

$$\begin{aligned} L'(x' + y') =& L'((x + y)') = L(x + y)' = (L(x) + L(y))' \\ =& L(x)' + L(y)' = L'(x') + L'(y') \end{aligned}$$

ja

$$\begin{aligned} L'(\alpha x') =& L'((\alpha x)') = L(\alpha x)' = (\alpha L(x))' \\ =& \alpha(L(x))' = \alpha L'(x'). \end{aligned}$$

Siten L' on $\mathbb{R}$-kertoimisen vektoriavaruuden $\mathbb{R}^{2n}$ lineaarikuvaus.

Edelleen luvun 7.4 nojalla on olemassa symmetrinen muoto A ja alternoiva muoto B, joille pätee $S(x, y) = A(x', y') + B(x', y')i$ kaikilla

$x, y \in \mathbb{C}^n$. Olkoot $x, y \in \mathbb{C}^n$. Nyt

$$\begin{aligned}
&L \in U_n(\mathbb{C}) \\
&\iff S(L(x), L(y)) = S(x, y) \\
&\iff A(L(x)', L(y)') + B(L(x)', L(y)')i = A(x', y') + B(x', y')i \\
&\iff A(L'(x'), L'(y')) + B(L'(x'), L'(y'))i = A(x', y') + B(x', y')i \\
&\iff A(L'(x'), L'(y')) = A(x', y') \text{ ja } B(L'(x'), L'(y')) = B(x', y') \\
&\iff L' \in O_{2n}^{(A)}(\mathbb{R}) \cap Sp_{2n}^{(B)}(\mathbb{R}).
\end{aligned}$$

Siten kuvaus $f : U_n(\mathbb{C}) \to O_{2n}^{(A)}(\mathbb{R}) \cap Sp_{2n}^{(B)}(\mathbb{R})$, $f(L) = L'$ on bijektio. Nähdään helposti, että f on myös ryhmähomomorfismi. Siten

$$U_n(\mathbb{C}) \cong O_{2n}^{(A)}(\mathbb{R}) \cap Sp_{2n}^{(B)}(\mathbb{R}).$$