Algebra I, harj. 7 16.–20.3.2009

1. $\forall k \in \mathbb{N}_+ \cup \{\infty\}\ \exists R_\varphi \in SO_2(\mathbb{R})$ s.e. $k = \mathrm{ord}(R_\varphi)$.

Tod. 1° $R_\theta R_\varphi = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$

$= \begin{pmatrix} \cos\theta\cos\varphi - \sin\theta\sin\varphi & -\cos\theta\sin\varphi - \sin\theta\cos\varphi \\ \cos\theta\sin\varphi + \sin\theta\cos\varphi & \cos\theta\cos\varphi - \sin\theta\sin\varphi \end{pmatrix} = \begin{pmatrix} \cos(\theta+\varphi) & -\sin(\theta+\varphi) \\ \sin(\theta+\varphi) & \cos(\theta+\varphi) \end{pmatrix}$

$= R_{\theta+\varphi} \implies R_\theta^2 = R_{2\theta}$ & induktiolla voi tod., että

$\underline{R_\theta^k = R_{k\theta}}$ (ol. $R_\theta^k = R_{k\theta}$ & val. yllä $\varphi = k\theta$).

2° $R_{k2\pi} = \begin{pmatrix} \cos k2\pi & -\sin k2\pi \\ \sin k2\pi & \cos k2\pi \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_{SO_2(\mathbb{R})} =: I$

kun $k \in \mathbb{Z}$.

3° Ol. $k \in \mathbb{N}_+$ & val. $\theta = \frac{2\pi}{k} \implies R_{2\pi/k}^n \overset{1°}{=} R_{2\pi n/k}$

& 2° $\implies \min\{n \in \mathbb{N}_+ \mid R_{2\pi n/k} = I\} = \min\{n \in \mathbb{N}_+ \mid \frac{n}{k} \in \mathbb{Z}\}$

$= k \implies \underline{\mathrm{ord}(R_{2\pi/k}) = k}$

4° Ol. $s \in \mathbb{R} \setminus \mathbb{Q} \implies k/s \in \mathbb{R} \setminus \mathbb{Q}\ \forall k \in \mathbb{N}_+$

$\implies k/s \notin \mathbb{Z}\ \forall k \in \mathbb{N}_+ \overset{2°}{\implies} R_{2\pi k/s} \neq I$

$\overset{1°}{\iff} R_{2\pi/s}^k \neq I\ \forall k \in \mathbb{N}_+ \implies \underline{\mathrm{ord}(R_{2\pi/s}) = \infty}$

3°–4° $\implies$ Väite. $\square$

2. $f: \mathbb{Z}_3 \to \mathbb{Z}_3$, $f = \begin{pmatrix} 0_3 & 1_3 & 2_3 \\ 0_3 & 2_3 & 1_3 \end{pmatrix}$

on homomorfismi.

Tod. $f(0_3+0_3) = f(0_3) = 0_3 = 0_3+0_3 = f(0_3)+f(0_3)$

$f(0_3+1_3) = f(1_3) = 2_3 = 0_3+2_3 = f(0_3)+f(1_3)$

$f(0_3+2_3) = f(2_3) = 1_3 = 0_3+1_3 = f(0_3)+f(2_3)$

$f(1_3+1_3) = f(2_3) = 1_3 = 2_3+2_3 = f(1_3)+f(1_3)$

$f(1_3+2_3) = f(0_3) = 0_3 = 2_3+1_3 = f(1_3)+f(2_3)$

$f(2_3+2_3) = f(1_3) = 2_3 = 1_3+1_3 = f(2_3)+f(2_3)$

Muut 3 tapausta seuraavat edellisistä koska $\mathbb{Z}_3$ on Abelin ryhmä: Esim.,

$f(2_3+1_3) = f(1_3+2_3) = f(1_3)+f(2_3) = f(2_3)+f(1_3)$

$\Rightarrow \forall a, b \in \mathbb{Z}_3 \quad f(a+b) = f(a)+f(b)$ $\square$

3. Olk. $f: G \to G'$ surj. ryhmähomom. & olk. G syklinen. Tällöin G' on syklinen.

Tod. Olk. $a \in G$ s.e. $G = \langle a \rangle$.

Olk. $a' = f(a)$. Osoitetaan, että $G' = \langle a' \rangle$:

Jos $b' \in G'$, niin $\exists\, b \in G$ s.e. $b' = f(b)$, sillä f on surj.. Nyt $\exists\, n \in \mathbb{Z}$ s.e. $b = a^n$, koska G on sykl.. Tällöin

$b' = f(b) = f(a^n) = f(a)^n = (a')^n$, sillä f on homom. $\square$

4. Olk. $A = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$

Homomorfismi $f: \mathbb{Z} \to GL_2(\mathbb{R})$ s.e. $f(1) = A$:

0° $\mathbb{Z} = \{m \cdot 1 \mid m \in \mathbb{Z}\} = \langle 1 \rangle$ l. $\mathbb{Z}$ on sykl.,

joten lause (s.73) $\Rightarrow$ $Im(f)$ on sykl. &

saman lauseen tod. $\Rightarrow$ $Im(f) = \langle f(1) \rangle$

joten etsitty f on: $f(m) = A^m$, $m \in \mathbb{Z}$

(missä $A^m = (A^{-1})^{-m}$, kun $m < 0$ & $A^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$

on yksikkömatriisi).

f on homom.: $f(m+n) = A^{m+n} = A^m A^n = f(m) f(n)$.

Todetaan, että $\forall a, b \in \mathbb{R}$

$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$ & määritellään

1° f y.o. määritelmän sijata suoraan

$f(m) = \begin{pmatrix} 1 & 3m \\ 0 & 1 \end{pmatrix}$ $\forall m \in \mathbb{Z}$.

Nyt $f(m)f(n) = \begin{pmatrix} 1 & 3m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 3n \\ 0 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 3m+3n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3(m+n) \\ 0 & 1 \end{pmatrix} = f(m+n)$

$\forall\, m, n \in \mathbb{Z}$

$\Rightarrow$ f on homom. & $f(1) = \begin{pmatrix} 1 & 3\cdot 1 \\ 0 & 1 \end{pmatrix} = A$

2° Kun $n \in \mathbb{N}_+$, $A^n = \begin{pmatrix} 1 & 3n \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_{GL_2(\mathbb{R})}$

joten A:n kertaluku $\mathrm{ord}(A) = \infty$.

5. Olk. $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $f(m,n) = 5m - 3n$
Tällöin f on addit. ryhmien surj. homom. & $\mathrm{Ker}(f)$ on $(3,5)$:n virittämä $\mathbb{Z} \times \mathbb{Z}$:n sykl. aliryhmä.

Tod. 1° $f((m,n)+(m',n')) = f((m+m', n+n'))$

$= 5(m+m') - 3(n+n') = 5m + 5m' - 3n - 3n'$

$= 5m - 3n + 5m' - 3n' = f(m,n) + f(m',n')$

$\forall (m,n), (m',n') \in \mathbb{Z} \times \mathbb{Z} \Rightarrow$ f on homom.

2° Ol. $k \in \mathbb{Z}$. Luvuilla -3 & 5 ei ole yhteisiä tekijöitä

$\Rightarrow \exists\, m_1, n_1 \in \mathbb{Z}$ s.e. $5m_1 - 3n_1 = 1$ $\Rightarrow$ jos val. $(m,n) = (km_1, kn_1)$,

on $f(m,n) = 5km_1 - 3kn_1 = k(5m_1 - 3n_1) = k \cdot 1 = k$

$\Rightarrow$ f on surjektio.

3° Ol. $(m,n) \in \langle (3,5) \rangle \Rightarrow \exists\, k \in \mathbb{Z}$ s.e. $(m,n) = k(3,5)$

$= (3k, 5k) \Rightarrow f(m,n) = 5(3k) - 3(5k) = 0$

$\Rightarrow \langle (3,5) \rangle \leq \mathrm{Ker}(f)$. Toisaalta

$(m,n) \in \mathrm{Ker}(f) \Leftrightarrow f(m,n) = 5m - 3n = 0 \Leftrightarrow 5m = 3n$

Koska $5 \nmid 3$, $\exists\, n_1 \in \mathbb{Z}$ s.e. $n = 5n_1$. Samoin $\exists\, m_1 \in \mathbb{Z}$

s.e. $m = 3m_1 \Rightarrow 5 \cdot 3m_1 = 3 \cdot 5n_1 \Rightarrow m_1 = n_1 =: k$

$\Rightarrow (m,n) = (3k, 5k) \in \langle (3,5) \rangle$

$\Rightarrow \mathrm{Ker}(f) = \langle (3,5) \rangle$ & siis $\mathrm{Ker}(f)$ on sykl. aliryhmä. $\square$

6. Olk. G ryhmä & $c_g : G \to G$, $c_g(a) = gag^{-1}$ $\forall a \in G$. Tällöin $c_{1_G} = id_G$, $c_{g_1 g_2} = c_{g_1} \circ c_{g_2}$ $\forall g_1, g_2 \in G$ & c_g on automorfismi $\forall g \in G$.

Tod. 1° $c_{1_G}(a) = 1_G a 1_G^{-1} = 1_G a 1_G = a 1_G = a$ $\forall a \in G$

$\Rightarrow c_{1_G} = id_G$

2° $c_{g_1 g_2}(a) = (g_1 g_2) a (g_1 g_2)^{-1} = g_1 g_2 a g_2^{-1} g_1^{-1}$

$= g_1 (g_2 a g_2^{-1}) g_1^{-1} = g_1 (c_{g_2}(a)) g_1^{-1} = c_{g_1}(c_{g_2}(a))$

$= (c_{g_1} \circ c_{g_2})(a)$ $\forall a \in G \Rightarrow c_{g_1 g_2} = c_{g_1} \circ c_{g_2}$

3° i) $c_g(ab) = gabg^{-1} = ga1_G bg^{-1} = gag^{-1}gbg^{-1}$

$= c_g(a) c_g(b)$ $\forall a, b \in G \Rightarrow c_g$ on homom.

ii) Ol. $c_g(a) = 1_G \Leftrightarrow gag^{-1} = 1_G (\Leftrightarrow ga = 1_G g)$

$\Leftrightarrow a = g^{-1} 1_G g = g^{-1} g = 1_G \Rightarrow Ker(c_g) = \{1_G\}$

joten L 9. (s. 63) $\Rightarrow c_g$ on injektio.

iii) Olk. $b \in G$ (mielív.). $b = c_g(a) \Leftrightarrow b = gag^{-1}$

$\Leftrightarrow a = g^{-1} b g$ (l. $\exists a \in G$ s.e. $c_g(a) = b$)

$\Rightarrow c_g$ on surjektio

i) – iii) $\Rightarrow c_g$ on bijektiivinen homomorfismi

$G \to G$ & siis automorfismi. □