IV.1 Normaalit alityhmät ja tekijäryhmät

Määr.: (Maltsev.) ryhmän alityhmä $H \leq G$ on normaali alityhmä, merk. $H \trianglelefteq G$, jos

$$aH = Ha \quad \forall a \in G.$$

Jos $H \trianglelefteq G$ ja $H \neq G$, merk. $H \lhd G$.

Huom.: $aH = Ha$ ei merkitse, että $ah = ha$ $\forall h \in H$.
Esim. $aH \subset Ha \iff \forall h \in H \; \exists h_1 \in H$ s.e. $ah = h_1 a$.

Lause 1: Ol. $H \leq G$. Seur. ehdot ovat ekvivalentteja:

a) $H \trianglelefteq G$
b) $aHa^{-1} = H \quad \forall a \in G$
c) $aHa^{-1} \subset H \quad \forall a \in G$
(eli $aha^{-1} \in H$ aina, kun $a \in G$, $h \in H$).

$\rightarrow$

Tod.: a) $\Rightarrow$ c). Ol. $H \trianglelefteq G$. Olk. $a \in G$ ja $b = aha^{-1} \in aHa^{-1}$ $(h \in H)$ $\Rightarrow ah \in aH = Ha$
$\Rightarrow \exists h_1 \in H$ s.e. $ah = h_1 a \Rightarrow b = ah \cdot a^{-1} =$
$= h_1 a \cdot a^{-1} = h_1 \in H$. $\therefore aHa^{-1} \subset H$.

c) $\Rightarrow$ b). Ol. c) voimassa. Olk. $a \in G$. c) $\Rightarrow$ $aHa^{-1} \subset H$. Samoin c) $\Rightarrow$ $a^{-1}Ha = a^{-1}H(a^{-1})^{-1} \subset H$.
Nyt $h \in H \Rightarrow a^{-1}ha \in a^{-1}Ha \subset H \Rightarrow a^{-1}ha = h_1 \in H$
$\Rightarrow h = ah_1a^{-1} \in aHa^{-1}$. $\therefore H \subset aHa^{-1}$. $\therefore aHa^{-1} = H$.

b) $\Rightarrow$ a). Ol. b) voimassa. Olk. $a \in G$.
$b = ah \in aH$ $(h \in H) \Rightarrow ba^{-1} = aha^{-1} \in aHa^{-1} = H$ (c)
$\Rightarrow ba^{-1} = h_1 \in H \Rightarrow b = h_1 a \in Ha$. $\therefore aH \subset Ha$.
$b = ha \in Ha$ $(h \in H) \Rightarrow a^{-1}b = a^{-1}ha \in a^{-1}H(a^{-1})^{-1} = H$ (c)
$\Rightarrow a^{-1}b = h_1 \in H \Rightarrow b = ah_1 \in aH$. $\therefore Ha \subset aH$.
$\therefore aH = Ha$. $\square$

(Tässä $aHa^{-1} = \{aha^{-1} \mid h \in H\} = C_a(H) \leq G$.)

Esim.: a) $\{1_G\} \trianglelefteq G$, $G \trianglelefteq G$.
b) G Abelin ryhmä $\Rightarrow$ jokainen $H \leq G$ on normaali.

c) O. $H \leq G$, $|G:H| = 2$.
V. $H \trianglelefteq G$
T. $\#(G/H) = \#(H\backslash G) = 2 \Rightarrow$

$$aH = \left\{ \begin{matrix} H, \text{ kun } a \in H \\ G\setminus H, \text{ kun } a \in G\setminus H \end{matrix} \right\} = Ha \quad \forall a \in G. \quad \square$$

d) O. $f: G \to G'$ nyhmäkuvaus.
V. $\ker(f) \trianglelefteq G$.
T. Tied., että $\ker(f) \leq G$. Kun $a \in G$, $h \in \ker(f)$, niin $f(aha^{-1}) = f(a)\cdot f(h)\cdot f(a)^{-1} = f(a)\cdot 1_{G'}\cdot f(a)^{-1} =$
$= f(a)\cdot f(a)^{-1} = 1_{G'}$, joten $aha^{-1} \in \ker(f)$.
$\therefore\ a\cdot\ker(f)\cdot a^{-1} \subset \ker(f)$. $\square$

Yleisemmin pätee:

Lause 3: Jos $f: G \to G'$ on nyhmäkuvaus, niin
$H \trianglelefteq G \Rightarrow f(H) \trianglelefteq f(G)$,
$H' \trianglelefteq G' \Rightarrow f^{-1}(H') \trianglelefteq G$. (Tod. harj.tehtävä) $\square$

Esim. 2: Tark. $GL_2(\mathbb{R})$:n alinryhmiä $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) \mid \det(A) = 1\}$ ja $H = \left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R}\setminus\{0\}\right\}$.

$SL_2(\mathbb{R}) = \ker[\det: GL_2(\mathbb{R}) \to \mathbb{R}\setminus\{0\}] \trianglelefteq GL_2(\mathbb{R})$;
H ei ole normaali, sillä esim.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\cdot\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 0 & -1 \end{pmatrix} \notin H.$$

Lemma: Jos $H \trianglelefteq G$ ja $a, a', b, b' \in G$, niin

$$aH = a'H,\ bH = b'H \Rightarrow (ab)H = (a'b')H.$$

Tod.: $aH = a'H$, $bH = b'H \Rightarrow a' = ah$, $b' = bk$ eräillä $h, k \in H$. Tällöin $a'b' = ahbk$. $hb \in Hb = bH$ (H norm.!) $\Rightarrow hb = bh'$ eräällä $h' \in H$
$\Rightarrow a'b' = ahbk = abh'k \in (ab)H$ (koska $h'k \in H$)
$\Rightarrow (ab)H = (a'b')H$. $\square$

Kun $H \trianglelefteq G$, joukossa $G/H = \{aH \mid a \in G\}$ voidaan siis määritellä laskutoimitus asettamalla

$$(aH, bH) \mapsto (ab)H, \quad a, b \in G$$

($(ab)H \in G/H$ ei näin muodoin $aH, bH \in G/H$ edustajien $a, b \in G$ valinnasta, jotten saadaan kuvaus $G/H \times G/H \to G/H$.)

Lause 2: Ol. $H \trianglelefteq G$. Silloin G/H varustettuna yo. laskutoimituksella on ryhmä, G:n tekijäryhmä modulo H. Jos G on Abelin ryhmä, samoin on G/H. Kanoninen surjektio $p = p_H : G \to G/H$, $p(a) = aH$ $\forall a \in G$, on homom. ja $\ker(p_H) = H$.

Tod.: $(aH)\cdot((bH)\cdot(cH)) = (aH)\cdot(bc)H = a(bc)H = (ab)cH = (abH)\cdot(cH) = ((aH)\cdot(bH))\cdot(cH)$ $\forall a,b,c \in G$ $\Rightarrow$ G/H on liitäin.. Samoin G/H on vaihdan., jos G on. Sopiasti $1_G H \in G/H$ kelpaa G/H:n neutr. alkioksi, ja $a^{-1}H \in G/H$ kelpaa alkion $aH \in G/H$ kääntöalkioksi. G/H:n laskutoim. määr. $\Rightarrow$ p_H on homom.. Lopuksi $a \in \ker(p_H) \Leftrightarrow p_H(a) = 1_G H \Leftrightarrow aH = 1_G H \Leftrightarrow a \in H$. □

Erityisesti jokainen $H \trianglelefteq G$ on muotoa $\ker(f)$ sopivalle f.

Esim. 5: Kun $n \in \mathbb{N}_+$, niin $(\mathbb{Z}_n, +)$ on ryhmän $(\mathbb{Z}, +)$ tekijäryhmä modulo $n\mathbb{Z}$: $(\mathbb{Z}_n, +) = (\mathbb{Z}/n\mathbb{Z}, +)$.

IV. 2 Ryhmien homomorfialause

Lause 4 (homomorfialause): Ryhmähomomorfismi $f : G \to G'$ indusoi isomorfismin

$$F : G/\ker(f) \xrightarrow{\sim} \mathrm{Im}(f), \quad a\cdot\ker(f) \mapsto f(a).$$

Tod.: Merk. $K = \ker(f) \trianglelefteq G$. Jotta kaava $aK \mapsto f(a)$ määr. kuvauksen $F : G/K \to \mathrm{Im}(f)$, on todettava:

$aK = a'K \Rightarrow a^{-1}a' \in K = \ker(f) \Rightarrow f(a^{-1}a') = 1_{G'}$
$\Rightarrow f(a)^{-1}\cdot f(a') = 1_{G'} \Rightarrow f(a') = f(a)$.

F on homom., sillä $F(aK\cdot bK) = F((ab)K) = f(ab) = f(a)\cdot f(b) = F(aK)\cdot F(bK)$.

F on inj., sillä $F(aK) = F(bK) \Rightarrow f(a) = f(b)$
$\Rightarrow f(a^{-1}b) = f(a)^{-1}f(b) = 1_{G'} \Rightarrow a^{-1}b \in \ker(f) = K$
$\Rightarrow aK = bK$.

F on surj., sillä $y \in \mathrm{Im}(f) \Rightarrow \exists\, a \in G$ s.e. $y = f(a)$, ja tällöin $y = F(aK) \in \mathrm{Im}(F)$. $\square$

Huom.: Yo. tilanteessa kaavio

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ G/\mathrm{Ker}(f) & \xrightarrow[\sim]{F} & \mathrm{Im}(f) \end{array} \qquad \begin{pmatrix} p \text{ kan. surj.} \\ i \text{ kan. inj.} \end{pmatrix}$$

kommutoi, ts. $f = i \circ F \circ p$ (f:n "kanoninen hajotelma"), sillä $(i \circ F \circ p)(a) = i(F(p(a))) = i(F(a \cdot \mathrm{Ker}(f))) = i(f(a)) = f(a)$ $\forall a \in G$.

Esim.: a) Kuvaus $f : (\mathbb{R}\setminus\{0\}, \cdot) \to (\mathbb{R}_+^*, \cdot)$, $f(x) = |x|$, on homom., $\mathrm{Im}(f) = \mathbb{R}_+^*$ ja $\mathrm{Ker}(f) = \{1, -1\}$, joten saadaan isom.

$$F : (\mathbb{R}\setminus\{0\})/\{1,-1\} \xrightarrow{\sim} \mathbb{R}_+^* .$$

b) Kuvaus $\det : (GL_2(\mathbb{R}), \cdot) \to (\mathbb{R}\setminus\{0\}, \cdot)$ on homom., $\mathrm{Im}(\det) = \mathbb{R}\setminus\{0\}$ ja $\mathrm{Ker}(\det) = SL_2(\mathbb{R})$, joten saad. isom. $GL_2(\mathbb{R})/SL_2(\mathbb{R}) \xrightarrow{\sim} \mathbb{R}\setminus\{0\}$.

c) Olk. G_1, G_2 (mult.pl.) ryhmiä, $G_1 \times G_2$ tulоryhmä (ks. Lause II.4). Tällöin $pr_2 : G_1 \times G_2 \to G_2$ on surjektiivinen homom., ja $(a_1, a_2) \in \mathrm{Ker}(pr_2) \iff a_2 = pr_2(a_1, a_2) = 1_{G_2} \iff (a_1, a_2) \in G_1 \times \{1_{G_2}\}$, joten $\mathrm{Ker}(pr_2) = G_1 \times \{1_{G_2}\}$. Siten

$$(G_1 \times G_2)/(G_1 \times \{1_{G_2}\}) \xrightarrow{\sim} G_2 .$$

d) Olkoot $m, n \in \mathbb{N}_+$ keskenään jaottomia.
Kuvaus $f : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $f(x) = ([x]_m, [x]_n)$ $\forall x \in \mathbb{Z}$, on selvästi homomorfismi.
Kiinalainen jäännöslause $\Rightarrow$ f on surjektio.

$x \in \mathrm{Ker}(f) \iff [x]_m = [0]_m$ ja $[x]_n = [0]_n$
$\iff m \mid x$ ja $n \mid x \iff mn \mid x$ (Lemma s. 47)
$\iff x \in mn\mathbb{Z}$.

Siis $\mathrm{Ker}(f) = mn\mathbb{Z}$, ja f indusoi isomorfismin

$\varphi : \mathbb{Z}_{mn} \xrightarrow{\sim} \mathbb{Z}_m \times \mathbb{Z}_n$.

Kiinal. jäännöslauseen tod. $\Rightarrow$ kun $am + bn = 1$, on

$$\varphi^{-1}([k]_m, [l]_n) = [lma + knb]_{mn}.$$

e) Erikoistapauksina aiemmasta on kun.

$$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3, \quad \mathbb{Z}_{18} \cong \mathbb{Z}_2 \times \mathbb{Z}_9,$$
$$\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_{15} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5.$$

IV.3 Sykliset ryhmät

Pal. mieleen: (multipl.) ryhmä G on syklinen, jos $\exists a \in G$ s.e. $G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$.

Olk. $G = \langle a \rangle$ syklinen. Silloin $f : (\mathbb{Z}, +) \to G$, $f(m) = a^m$ $\forall m \in \mathbb{Z}$, on surjekt. homom. ($a^{m+m'} = a^m \cdot a^{m'}$).
Lause III.7 $\Rightarrow$
- jos $|G| = \infty$, f on isom. $\mathbb{Z} \xrightarrow{\sim} G$;
- jos $|G| = n \in \mathbb{N}_+$, niin $G = \{1, a, \dots, a^{n-1}\}$, $a^n = 1$ ja $\ker(f) = n\mathbb{Z}$; siis f indus. isom. $\mathbb{Z}_n \xrightarrow{\sim} G$.

Lause: G syklinen, $f : G \to G'$ homom.
$\Rightarrow$ $\mathrm{Im}(f)$ on syklinen.

Tod.: $G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\} \Rightarrow \mathrm{Im}(f) = f(G) =$
$= \{f(a^m) \mid m \in \mathbb{Z}\} = \{f(a)^m \mid m \in \mathbb{Z}\} = \langle f(a) \rangle$. □

Erit. sykl. ryhmän tekijäryhmät ovat syklisiä.

Syklisen ryhmän aliryhmät: Ol. $G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$ syklinen ja $H \leq G$. Jos $H = \{1_G\}$, niin $H = \langle 1_G \rangle = \langle a^0 \rangle$. Olk. sitten $H \neq \{1_G\} \Rightarrow \exists m \in \mathbb{Z}$, $m \neq 0$, s.e. $a^m \in H \Rightarrow \exists m \in \mathbb{N}_+$ s.e. $a^m \in H$ (jos $a^m \in H$, $m < 0$, niin myös $a^{-m} = (a^m)^{-1} \in H$, $-m \in \mathbb{N}_+$).
Merk. $k = \min\{m \in \mathbb{N}_+ \mid a^m \in H\}$.

V. $H = \langle a^k \rangle \; (= \{a^{kp} \mid p \in \mathbb{Z}\})$.

T. $a^k \in H \Rightarrow a^{kp} = (a^k)^p \in H \; \forall p \in \mathbb{Z} \Rightarrow \langle a^k \rangle \subset H$.

Käänt.väen, ol. $b \in H$. $H \subset G = \langle a \rangle \Rightarrow b = a^m$ eräällä $m \in \mathbb{Z}$. Jakoyht. $\Rightarrow m = qk + r$, $0 \le r < k$.
Tällöin $a^r = a^{m-qk} = a^m \cdot a^{-qk} = b \cdot (a^k)^{-q} \in H$;
k:n minimaalisuus $\Rightarrow$ täytyy olla $r = 0$,
$b = a^m = a^{qk} = (a^k)^q \in \langle a^k \rangle$. $\therefore H \subset \langle a^k \rangle$. □

Lause 5: Äärettömän syklisen ryhmän $G = \langle a \rangle$ alіryhmät ovat $\langle a^k \rangle$, $k = 0, 1, 2, \ldots$ (kaikki eri ryhmiä). Kun $k > 0$, $\langle a^k \rangle$ on itsekin ääretön syklinen ryhmä. □

Oll. sitten $|G| = n \in \mathbb{N}_+$, $H = \langle a^k \rangle \le G$, $H \neq \{1_G\}$, $k = \min\{m \in \mathbb{N}_+ \mid a^m \in H\}$ kuten yllä.

V. $k \mid n$.

T. Jakoyht. $\Rightarrow n = kl + s$, $0 \le s < k$.
$1_G = a^n = a^{kl+s} = (a^k)^l \cdot a^s \Rightarrow a^s = (a^k)^{-l} \in H$.
k:n minimaalisuus $\Rightarrow s = 0$, $n = kl$. □

Siis $n = kl$, $l \in \mathbb{N}_+$, ja $H = \{1_G, a^k, a^{2k}, \ldots, a^{(l-1)k}\}$, $|H| = l$.

Lause 6: Äärellisen syklisen ryhmän $G = \langle a \rangle$, $|G| = n \in \mathbb{N}_+$, alіryhmät ovat

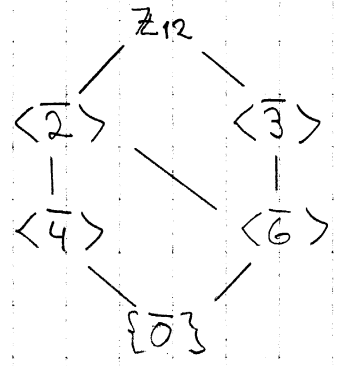
$$\langle a^k \rangle = \{1_G, a^k, a^{2k}, \ldots, a^{(m-1)k}\}, \quad m \in \mathbb{N}_+, \; m \mid n, \; k = \tfrac{n}{m}.$$

Tässä siis $|\langle a^k \rangle| = m$. Jos $m \mid n$ ja $m' \mid n$, $k = \frac{n}{m}$ ja $k' = \frac{n}{m'}$, niin $\langle a^k \rangle \subset \langle a^{k'} \rangle \Leftrightarrow m \mid m'$.

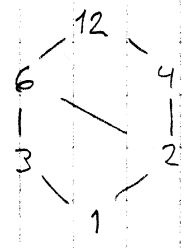
Tod.: Väitt. väite: $\Leftarrow$ on selvä.
$\Rightarrow$ $\langle a^k \rangle \subset \langle a^{k'} \rangle \Rightarrow \langle a^k \rangle \le \langle a^{k'} \rangle \Rightarrow |\langle a^{k'} \rangle| = m'$ on jaoll. alіryhmän kertaluvulla $|\langle a^k \rangle| = m$. □

Esim.: a) Ryhmän $(\mathbb{Z}, +)$ alіryhmät ovat
$k\mathbb{Z}$, $k = 0, 1, 2, \ldots$.

b) Ryhmän $(\mathbb{Z}_{12}, +)$ alіryhmät ja niiden väliset sisältymisrelaatiot:



Kertaluvut:



Lause 7: G (multipl.) ryhmä, $a \in G$, $\operatorname{ord}(a) = n \in \mathbb{N}_+$

$$\Rightarrow \quad \operatorname{ord}(a^m) = \frac{n}{\operatorname{syt}(m,n)} .$$

Tod.: Merk. $d = \operatorname{syt}(m,n)$; $n = n_1 d$, $m = m_1 d$, missä $\operatorname{syt}(m_1, n_1) = 1$. Nyt

$(a^m)^r = 1_G \iff a^{mr} = 1_G \iff \operatorname{ord}(a) \mid (mr)$

$\iff n \mid (mr) \iff n_1 \mid (m_1 r) \iff n_1 \mid r$

(koska $\operatorname{syt}(m_1, n_1) = 1$).

$\therefore \operatorname{ord}(a^m) = n_1 = n/d$. □

Ol. $G = \langle a \rangle$ syklinen, $|G| = n \in \mathbb{N}_+$. Tällöin a^m kelpaa G:n viittäjäksi $\iff G = \langle a^m \rangle$

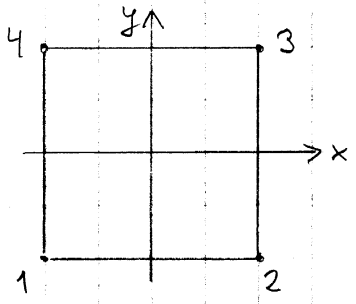
$\iff \operatorname{ord}(a^m) = n \iff \operatorname{syt}(m,n) = 1$ (Lause 7).

G:n viittäjien lkm on siis $= \#\{a^m \mid \operatorname{syt}(m,n) = 1\} =$

$= \#\{m \mid 0 \le m \le n-1, \operatorname{syt}(m,n) = 1\} = \varphi(n)$.

IV.6 Nelion symmetriaryhmä eli diedriryhmä D_4

Tark. tason $\mathbb{R}^2$ neliötä A:



Kärjet: $1 \leftrightarrow (-1,-1) \in \mathbb{R}^2$

$2 \leftrightarrow (1,-1) \in \mathbb{R}^2$

$3 \leftrightarrow (1,1) \in \mathbb{R}^2$

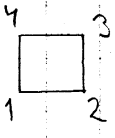
$4 \leftrightarrow (-1,1) \in \mathbb{R}^2$.

Merk. $R = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \in S_4$, $S = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \in S_4$

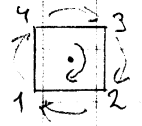
ja $D_4 = \langle R, S \rangle \le S_4$.

Ryhmässä D_4 on (ainakin) seur. 8 alkiota:

$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \leftrightarrow I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2$

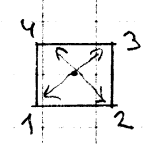


$R = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \longleftrightarrow R_{270} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$



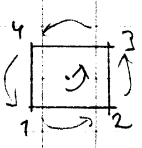
kierto origon ymp. 90° myötäpäivään

$R^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \longleftrightarrow R_{180} = -I_2 \in GL_2(\mathbb{R})$



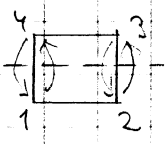
kierto origon ymp. 180°

$R^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \longleftrightarrow R_{90} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$



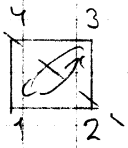
kierto origon ymp. 90° vastapäivään

$S = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \longleftrightarrow H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in GL_2(\mathbb{R})$



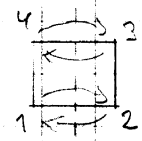
peilaus x-akselin suhteen

$RS = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \longleftrightarrow D' = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$



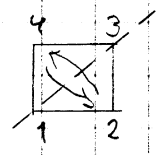
peilaus suoran $y = -x$ suhteen

$R^2S = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \longleftrightarrow V = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$



peilaus y-akselin suhteen

$R^3S = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \longleftrightarrow D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$



peilaus suoran $y = x$ suhteen.

Seuraavat "relaatiot" ovat voimassa: $R^4 = id = S^2$,

$SR = R^3S \quad \left(= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \right)$.

V. $D_4 = \{ R^i S^j \mid i = 0,1,2,3 ;\ j = 0,1 \}$.

T. $\supseteq$ selvää.

Tm. Riittää os., että yo. 8 alkiota muod. S_4:n aliryhmän. Käytetään aliryhmäkriteeriä ja sovell. yo. relaatioita:

$i,k \in \{0,1,2,3\}$; $j,l \in \{0,1\}$ $\Longrightarrow$

$(R^i S^j) \circ (R^k S^l)^{-1} = R^i S^{j-l} R^{-k}$

$= \begin{cases} R^{i-k} = R^p, \text{ kun } j-l \equiv 0 \pmod 2,\ i-k \equiv p \pmod 4 \\ R^i S R^{4-k} = R^i R^{3(4-k)} S \\ \quad = R^q S, \text{ kun } j-l \equiv 1 \pmod 2,\ i+3(4-k) \equiv q \pmod 4. \end{cases}$

□

Siis $|D_4| = 8$. Myös $D_4 \cong \langle R_{270}, H \rangle \leq GL_2(\mathbb{R})$.

Jatkan todistusta, että D_4:n alkioina ovat kaikki neliön $A \subset \mathbb{R}^2$ "symmetriat", so. isometriat $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$, joilla $\varphi(A) = A$.

Huom.: Ryhmän D_4 "kertotaulu" on helppo muodostaa relaatioiden $R^4 = id = S^2$, $SoR = R^3 oS$ avulla:

$$R^i o (R^k o S^l) = R^{i+k} o S^l = R^p o S^l, \quad i+k \equiv p \pmod 4;$$
$$(R^i o S) o (R^k o S^l) = R^i o (SoR^k) o S^l$$
$$= R^i o (R^{3k} o S) o S^l = R^{i+3k} o S^{l+1}$$
$$= R^p o S^q, \quad i+3k \equiv p \pmod 4, \quad l+1 \equiv q \pmod 2.$$

D_4:n alityhmät:

1) Kierrot muod. alityhmän $\langle R \rangle = \{id, R, R^2, R^3\} \cong \mathbb{Z}_4$. $|D_4 : \langle R \rangle| = 2 \Rightarrow \langle R \rangle \triangleleft D_4$ (normaalius seuraa myös siitä, että $SoRoS^{-1} = (R^3 oS) oS^{-1} = R^3$). Tässä $D_4 / \langle R \rangle \cong \mathbb{Z}_2$, virittäjänä S:n sivuluokka.

2) D_4:ssä on 2-alkioiset alityhmät $\langle R^2 \rangle = \{id, R^2\}$, $\langle S \rangle = \{id, S\}$, $\langle RoS \rangle = \{id, RoS\}$, $\langle R^2 oS \rangle = \{id, R^2 oS\}$ ja $\langle R^3 oS \rangle = \{id, R^3 oS\}$.

3) Muut D_4:n aidot alityhmät ovat $\{id\}$ sekä $\langle R^2, S \rangle = \{id, R^2, S, R^2 oS\}$ ja $\langle R^2, RoS \rangle = \{id, R^2, RoS, R^3 oS\}$.
(jos $H \leq D_4$ sisältää joukon peilauksen ja joko R:n tai R^3:n, niin $R, S \in H$, jolloin $H = D_4$.)

Julkisen avaimen salakirjoitus

Esittelemme hieman RSA - salakirjoitusmenetelmää (Rivest - Shamir - Adelman, 1977)

Idea: Koodin laatija haluaa, että hänelle lähetettävät viestit koodataan tietoturvasyistä. Hän julkistaa avaimesta viestien koodaamiseen tarvittavan osan. Koodattujen viestien purkamiseen tarvitaan koko avain, jotten tämä onnistuu (kohtuullisella vaivalla) vain koodin laatijalta.

I. Avaimen muodostaminen

Valitaan kaksi (suurta) alkulukua p, q $(p \neq q)$.

Olk. $n = pq$ ja $m = pyj(p-1, q-1)$.
Val. jokin k, $1 < k < m$, s.e. $syt(m,k) = 1$.

Julkinen avain on pari n, k.

Näiden avulla on hyvin työlästä löytää p, q (kun p ja q ovat suuria).

II. Viestin koodaus

Viestiyksiköt ovat lukuja $M \in \mathbb{N}_+$ (esim. A = 1, B = 2, ... ; käytännössä yksiköt ovat paljon pitempiä). M koodattuna on $r \in \{0, 1, \ldots, n-1\}$, $r \equiv M^k \pmod n$.

III. Koodatun viestin purku

Etsitään (esim. Eukleideen algoritmilla) j s.e.
$jk \equiv 1 \pmod m$. Em. koodattu viesti r saadaan purettua operaatiolla r^j:

V. $r^j \equiv M \pmod n$.
T. $r \equiv M^k \pmod n \Rightarrow r^j \equiv M^{jk} \pmod n$.
$jk \equiv 1 \pmod m \Rightarrow jk = 1 + sm$ jollakin $s \in \mathbb{Z}$.
$m = pyj(p-1, q-1) \Rightarrow m = (p-1)m' = (q-1)m''$ eräillä $m', m'' \in \mathbb{N}_+$.

$$M^{jk} = M^{1+sm} = M \cdot (M^m)^s.$$

$$M^m = (M^{p-1})^{m'} \equiv 1^{m'} \pmod p \quad \text{(Fermat)}$$
$$\equiv 1 \pmod p,$$

ja samoin $M^m \equiv 1 \pmod q$.
Esimerkin d) s. 72 isom. $\mathbb{Z}_n \xrightarrow{\sim} \mathbb{Z}_p \times \mathbb{Z}_q \Rightarrow$
$M^m \equiv 1 \pmod n$
$\Rightarrow M^{jk} = M \cdot (M^m)^s \equiv M \pmod n$. □