PUOLIRYHMÄT Dem. III 30.3. 2017

$\boxed{1}$ Sanotaan, että kongruenssi $\rho \in \mathrm{Con}(S)$ **peittää** osajoukon $X \subseteq S$, jos X on kongruenssiluokkien unioni: $X = \bigcup_{x \in X} x\rho$. Kun $X \subseteq S$, määritellään relaatio Γ_X seuraavasti:

$$(x,y) \in \Gamma_X \text{ jos ja vain jos } \big(\forall u,v \in S^1\colon\ uxv \in X \iff uyv \in X\big). \qquad (\star)$$

Osoita, että Γ_X on suurin kongruenssi, joka peittää osajoukon X.

Ratkaisu. (1) Γ_X on ilmeisesti ekvivalenssirelaatio.

(2) Osoitetaan, että $\Gamma_X \in \mathrm{Con}(S)$. Kirjoitetaan lyhyesti $\Gamma = \Gamma_X$. Oletetaan, että $x\Gamma y$ ja olkoon $z \in S$, $u,v \in S^1$, jolloin $u(zx)v = (uz)xv$ ja $u(zy)v = (uz)yv$. Kun määrittelyä $(\star)$ sovelletaan tapaukseen $uz \in S^1$ ja $v \in S^1$, niin $u(zx)v \in X$ implikoi että $u(zy)v \in X$. Samoin $u(zy)v \in X$ implikoi että $u(zx)v \in X$, ja myös että $u(xz)v \in X$ jos ja vain jos $u(yz)v \in X$. Näin ollen $zx\Gamma zy$ ja $xz\Gamma yz$, mistä seuraa, että $\Gamma \in \mathrm{Con}(S)$.

(3) Osoitetaan, että X peittyy. Varmasti $X \subseteq \bigcup_{x\in X} x\Gamma$. Lisäksi, jos $y \in x\Gamma$, niin valitsemalla $u = 1 = v$ määrittelyssä $(\star)$, saadaan että $x \in X$ implikoi että $y \in X$. Siis $x\Gamma \subseteq X$ kaikilla $x \in X$. Siis X peittyy.

(4) Maksimaalisuutta varten oletetaan että $X = \bigcup_{x\in X} x\rho$, missä $\rho \in \mathrm{Con}(S)$. Oletetaan, että $x\rho y$ ja olkoot $u,v \in S^1$. Nyt $(uxv)\rho(uyv)$ eli $(uxv)\rho = (uyv)\rho$, mistä saadaan että $uxv \in X$ jos ja vain jos $uyv \in X$, koskapa ρ peittää joukon X. Siten $x\Gamma y$ ja $\rho \subseteq \Gamma$ kuten vaadittua.

$\boxed{2}$ Olkoon $\rho \in \mathrm{Con}(S)$.

(a) Osoita, että vain yksi kongruenssiluokka $x\rho$ voi olla puoliryhmän S ihanne.

(b) Osoita, että jos I on ihanne ja $I \subseteq x\rho$ jollain $x \in S$, niin $x\rho$ on S:n ihanne.

Ratkaisu. (a) Jos I ja J ovat ihanteita, niin samoin on $I \cap J$ ja se on epätyhjä, sillä $IJ \subseteq I \cap J$. Siten ne eivät voi olla eri kongruenssiluokkia.

(b) Olkoon $a \in I$, $y \in x\rho$ ja $z \in S$. Nyt $y\rho a$, ja siten $zy\rho za$ ja $yz\rho az$. Tässä $za \in I$ ja $az \in I$, koska I on ihanne. Siis $zy \in x\rho$ ja $yz \in x\rho$.

$\boxed{3}$ Olkoon $\delta \subseteq S \times S$ puoliryhmän S jokin relaatio. Alkioille $x,y \in S$ merkitään

$$x \xrightarrow{\delta} y\,,$$

jos on sellaiset $w_1,u,v,w_2 \in S^1$, että $x = w_1uw_2,\ y = w_1vw_2$ ja $u\delta v$. Vielä

$$x \xrightarrow{\delta}{}^{*} y\,,$$

jos $x = y$ tai on äärellinen jono alkioita $x_1, x_2, \dots, x_n$ siten, että

$$x = x_1 \xrightarrow{\delta} x_2 \xrightarrow{\delta} \dots \xrightarrow{\delta} x_n = y\,.$$

Osoita, että

$$x\delta^c y \iff x \xrightarrow{\delta^{\pm 1}}{}^{*} y,$$

missä $\delta^{\pm 1} = \delta \cup \delta^{-1}$.

Ratkaisu. (1) Määritellään ρ ehdosta

$$x\rho y \iff x \xrightarrow{\delta^{\pm 1}}{}^{*} y\,.$$

Nyt $\iota_S \subseteq \rho$ ja siten ρ on refleksiivinen. Määrittelyn mukaan $\delta^{\pm 1}$ on symmetrinen, ja samoin on siis ρ. Transitiivisuus on helposti osoitettavissa:

$$x \xrightarrow{\delta^{\pm 1}}{}^{*} y \text{ and } y \xrightarrow{\delta^{\pm 1}}{}^{*} z \implies x \xrightarrow{\delta^{\pm 1}}{}^{*} z\,.$$

Siten ρ on ekvivalenssirelaatio.

(2) Jos $z \in S$ ja $x \xrightarrow{\delta^{\pm 1}} y$, niin selvästi myös $zx \xrightarrow{\delta^{\pm 1}} zy$ ja $xz \xrightarrow{\delta^{\pm 1}} yz$. Niinpä $\rho \in \mathrm{Con}(S)$.

(3) Jos $\theta \in \mathrm{Con}(S)$, jolla $\delta \subseteq \theta$, niin $x\theta y$ aina kun $x \xrightarrow{\delta^{\pm 1}} y$. Siis $\rho \subseteq \theta$ ja väite seuraa.

$\boxed{4}$ Olkoon S äärellinen puoliryhmä, jossa on nolla-alkio 0. Oletetaan, että $|S| \geq 2$. Sanotaan, että S on **nilpotentti**, jos $S^n = \{0\}$ jollain $n \geq 1$.
(Tässä $S^n = \{x_1x_2\cdots x_n \mid x_i \in S\}$.)

(a) Osoita, että S on nilpotentti jos ja vain jos on olemassa $n \geq 1$, jolle $x_1x_2\cdots x_n = y_1y_2\cdots y_n$ kaikille $x_i, y_i \in S$.

(b) Osoita, että jos S on nilpotentti, niin $S \setminus S^2$ on puoliryhmän S yksikäsitteinen pienin generaattorijoukko.

Ratkaisu. (a) Jos S on nilpotentti niin asia on selvä, sillä $x_1x_2\cdots x_n = 0$.
Jos taas ehto toteutuu, niin välttämättä $x_1x_2\cdots x_n$ on nolla-alkio.

(b) Olkoon $S^n = \{0\}$. Varmasti $S \setminus S^2$ sisältyy aina generaattorijoukkoon. Merkitään $B = S \setminus S^2$. Oletetaan, että $x \notin [B]$. Tällöin $x = x_1y_1$ tai $x = y_1x_1$, missä $x_1 \notin [B]$. Siis $x_1 \in S^2$ ja siten $x \in S^3$. Induktiivisesti saadaan $x \in S^n = \{0\}$ ja edelleen, että $x = 0$. Siis nolla-alkio on ainut alkio erotuksessa $S \setminus [B]$. Mutta $|S| > 1$, ja siten on alkio $y \in B$, jolle $y^n = 0$ ja siis $0 \in [B]$; ristiriita.

$\boxed{5}$ (*Grothendieckin ryhmä*) Olkoon S kommutatiivinen monoidi, ja $M = S \times S$ sen suora tulo (missä tulo on komponenteittain). Määritellään $\rho \subseteq M \times M$ oheisesti: $(x_1, y_1)\rho(x_2, y_2)$ jos on olemassa alkio z niin, että

$$x_1y_2z = y_1x_2z\,.$$

(Tulot ovat monoidin S operaatioita.)

(a) Osoita, että $\rho \in \mathrm{Con}(M)$.

(b) Osoita, että tekijämonoidi M/ρ on Abelin ryhmä.
(Huomioin vielä, että se on “paras” Abelin ryhmä vastaamaan monoidia S.)

Ratkaisu. (a) Transitiivisuutta varten todetaan, että jos $(x_1,y_1)\rho(x_2,y_2)$ ja $(x_2,y_2)\rho(x_3,y_3)$, niin $x_1y_2z = y_1x_2z$ ja $x_2y_3v = y_2x_3v$ joillain z ja v, ja siten

$$\begin{aligned} x_1y_3\cdot y_2zv &\overset{\text{komm}}{=} x_1y_2z\cdot y_3v = y_1x_2z\cdot y_3v \overset{\text{komm}}{=} x_2y_3v\cdot y_1z = y_2x_3v\cdot y_1z \\ &\overset{\text{komm}}{=} y_1x_3\cdot y_2zv, \end{aligned}$$

ja siten $(x_1,y_1)\rho(x_3,y_3)$.

Lisäksi jos $(x_1,y_1)\rho(x_2,y_2)$, niin on olemassa z siten, että $x_1y_2z = y_1x_2z$. Olkoon vielä $(z_1,z_2)\in M$. Tällöin $x_1y_2z\cdot z_1z_2 = y_1x_2z\cdot z_1z_2$ ja siten $(x_1z_1,y_1z_2)\rho(x_2z_1,y_2z_2)$. Koska S on kommutatiivinen, on ρ kongruenssi.

(b) Varmasti M/ρ on kommutatiivinen monoidi, koskapa S on.

Todetaan, että $(x,x)\rho(y,y)$, sillä $xy\cdot 1 = yx\cdot 1$ kaikilla $x,y\in S$. Siten kaikki diagonaalialkiot (x,x) kuuluvat samaan kongruenssiluokkaan. Olkoon se θ.
Tämä θ on ykkösalkio: $(x_1,y_1)(a,a) = (x_1a,y_1a)\sim(x_1,y_1)$, sillä $x_1ay_1\cdot 1 = y_1ax_1\cdot 1$.

Kongruenssiluokan $(x,y)\rho$ käänteisalkio on $(y,x)\rho$, sillä $(x,y)(y,x) = (xy,yx) = (xy,xy)\in\alpha$.

$\boxed{6}$ Olkoon $I\neq A^+$ sanapuoliryhmän A^+ aito ihanne, missä A on aakkosto.

(a) Osoita, että I ei ole vapaa puoliryhmä.

(b) Oletetaan, että I on äärellisesti generoitu alipuoliryhmänä. Osoita, että Reesin puoliryhmä A^+/I on äärellinen.

Ratkaisu. Ensinnäkin on olemassa kirjain $a\in A$, jolle $a\notin I$, sillä I on aito ihanne. Olkoon $x\in I$ lyhin sana ihanteessa I (yksi sellaisista).

(a) Nyt $ax, xa\in I\setminus I^2$, joten jos $I=[X]$, niin $x, ax, xa\in X$. Kuitenkin $x(ax)=(xa)x$, ja siten I ei ole vapaa.

(b) Olkoon $A^+\setminus I = \{u_1,u_2,\ldots\}$. Nyt $xu_i\in I$ kaikilla i, koska I on ihanne. Osoitetaan, että $xu_i\in I\setminus I^2$. Tehdään vastaoletus $xu_i = vw$, missä $v,w\in I$. Alkion x valinnan nojalla, x on sanan v prefiksi eli $v = xz$ jollain z, ja siten w on sanan u_i suffiksi: $u_i = zw$. Mutta koska $w\in I$, myös $u_i\in I$; ristiriita.

Näin ollen jos X generoi ihanteen I, niin $xu_i\in X$ kaikilla i. Mutta I on äärellisesti generoitu, ja siten $A^+\setminus I$ on äärellinen ja samoin on siis A^+/I.

Minimaalinen ihanne puoliryhmässä $\boldsymbol{S \leq T_n}$

Olkoon $X = \{1, 2, \ldots, n\}$ ja $S \leq T_n$ täyden transformaatiopuoliryhmän alipuoliryhmä. Merkitään

$$g(S) = \min_{\alpha \in S} g(\alpha), \text{ missä } g(\alpha) = |g(X)|\,.$$

Huomaa, että kaikille $\alpha, \beta \in S$ on

$$g(\beta\alpha) \leq \min\{g(\alpha), g(\beta)\}. \tag{1}$$

Lause. *Joukko* $I = \{\alpha \mid g(\alpha) = g(S)\}$ *on puoliryhmän* S *minimaalinen ihanne* (ja sellaisena se on yksikäsitteinen).

Todistus. Ensinnäkin I on ihanne, sillä epäyhtälön (1) mukaan jos $\alpha \in I$ ja $\beta \in S$, niin $g(\beta\alpha) = g(S) = g(\alpha\beta)$ ja siten $\beta\alpha, \alpha\beta \in I$.

Minimaalisuutta varten tehdään vastaoletus: Olkoon J ihanne, jolle $J \subset I$ aidosti, ja olkoon $\alpha \notin J$ siten, että $g(\alpha) = g(S)$. Valitaan sitten jokin alkio $\beta \in J$.

Koska I on ihanne, on $g(\gamma\alpha) = g(S)$ kaikilla $\gamma \in S$. Tässä γ on välttämättä injektiivinen, ja siten bijektiivinen, joukossa $\alpha(X)$. Näin ollen

$$\alpha(x) = \alpha(y) \iff \gamma\alpha(x) = \gamma\alpha(y) \text{ kaikilla } \gamma \in S\,. \tag{2}$$

Erityisesti $\alpha\beta\alpha$ on joukon $\alpha(X)$ permutaatio, ja siten on positiivinen kokonaisluku k, jolle $(\alpha\beta\alpha)^k$ on identiteettikuvaus joukossa $\alpha(X)$.

Väitetään, että (*) $\alpha = \alpha(\alpha\beta\alpha)^k$, mistä varsinainen väite seuraa, koska nyt $\alpha = \alpha(\alpha\beta\alpha)^{k-1} \cdot \beta \cdot \alpha \in J$ vastoin oletusta.

Kun $x \in \alpha(X)$, niin $\alpha(x) = \alpha(\alpha\beta\alpha)^k(x)$ potenssin k valinnan nojalla.

Olkoon sitten $x \notin \alpha(X)$. Koska α on permutaatio joukossa $\alpha(X)$, niin on $z \in \alpha(X)$, jolle $\alpha(z) = \alpha(x)$, ja siten (2) tuottaa $\alpha(\alpha\beta\alpha)^k(z) = \alpha(\alpha\beta\alpha)^k(x)$, mistä saadaan $\alpha(z) = \alpha(\alpha\beta\alpha)^k(x)$, koskapa $z \in \alpha(X)$. Näin ollen (*) on voimassa, sillä $\alpha(z) = \alpha(x)$.
$\square$