Matematiikan laitos
AlgebraII
Harjoitus 2
29.01.2011
Ratkaisuehdotuksia
Aleksandr Pasharin

1. Olkoon G äärellinen ryhmä, $\varphi : G \to M$ (ryhmä)homomorfismi ja $H \leq G$.
   (a) Osoita, että $\varphi(H) \leq \varphi(G) \leq M$.
   (b) Osoita, että indeksi $[\varphi(G) : \varphi(H)]$ jakaa indeksin $[G : H]$.
   (c) Osoita, että kertaluku $|\varphi(H)|$ jakaa kertaluvun $|H|$.

   Ratkaisu: a) Olkoon $\varphi|: H \to M$ kuvauksen φ rajoittuma. Tällöin se on ryhmähomomorfismi. Näin ollen riittää tarkastella tapaus $H = G$. $\varphi(G)$ on selvästi epätyhjä. Lisäksi jos $x = \varphi(a), y = \varphi(b)$, $a, b \in G$, niin $xy^{-1} = \varphi(ab^{-1}) \in \varphi(G)$, sillä φ on homomorfismi. Näin ollen $\varphi(G)$ on M:n aliryhmä.

   b) Olkoon $K = \mathrm{Ker}(\phi)$, joka on G:n normaali aliryhmä. Tällöin isomorfialauseen 1.15 nojalla $\varphi(G)$ on isomorfinen ryhmän G/K kanssa. Samalla tavalla $\varphi(H)$ on isomorfinen ryhmän $H/(K \cap H)$ kanssa, sillä $K \cap H$ on rajoittumakuvauksen $\varphi|: H \to \varphi(H)$ ydin.
   Tästä ja Langrangen lauseesta seuraa, että

$$|\varphi(G)| = [G : K] = |G|/|K|,$$

$$|\varphi(H)| = [H : H \cap K] = |H|/|H \cap K|.$$

   Tästä seuraa, että

$$[\varphi(G) : \varphi(H)] = |\varphi(G)|/|\varphi(H)| = (|G|/|H|) \cdot (|H \cap K|/|K|),$$

   josta taas saadaan

$$[G : H] = [\varphi(G) : \varphi(H)] \cdot [K : H \cap K].$$

   Väite seuraa.

   c) Tämä seuraa suoraan siitä, että $|\varphi(H)| = [H : H \cap K]$ (isomorfialauseen seuraus).

2. Olkoon $R_{m,n}$ viime viikon tehtävän 4 ekvivalenssirelaatio $\mathbb{N}$:ssä ja olkoon E kyseisen tehtävän tekijämonoidi $\mathbb{N}/R_{m,n}$. Olkoon $\varepsilon : E \to E_E$ sen kanoninen homomorfismi ($\bar{a} \mapsto [(\bar{a}, 0)]$) erotusryhmäänsä $E_E = E \times E/\sim$. Olkoot $\bar{x}, \bar{y} \in E$ lukujen $x, y \in \mathbb{N}$

luokat. Osoita, että $\varepsilon(\bar{x}) = \varepsilon(\bar{y})$, jos ja vain jos $x \equiv y \pmod{m}$.

Ratkaisu: Havaitaan, että E:ssä pätee $\bar{n} = \overline{n+m} = \bar{n} + \bar{m}$. Soveltamalla homomorfismia ε saadaan ryhmässä E_E yhtälön

$$\varepsilon(\bar{n}) = \varepsilon(\bar{n}) + \varepsilon(\bar{m}).$$

Koska E_E on ryhmä voidaan yhtälön molemmista puolista supistaa $\varepsilon(\bar{n})$ jolloin saadaan $\varepsilon(\bar{m}) = 0$ eli neutraalialkio ryhmässä E_E. Näin ollen jos $m|x-y$, niin $x = y + k \cdot m$ jollakin $k \in \mathbb{N}$ joten

$$\varepsilon(\bar{x}) = \varepsilon(\bar{y} + k\bar{m}) = \varepsilon(\bar{y}) + \varepsilon(\bar{m}) = \varepsilon(\bar{y}).$$

Kääntäisen väitteen osoittamiseksi vedotaan erotusryhmän universaaliominaisuuteen (K. Suominen, Lause 1.2.9) abelin ryhmien suhteen. Nimittäin jos G on vaihdannainen ryhmä ja $f\colon E \to G$ on monoidihomomorfismi, niin se voidaan "faktoroida "kuvauksen ε kautta, eli on olemassa (yksikäsitteinen) ryhmähomomorfismi $\bar{f}\colon E_E \to G$ jolle $f = \bar{f}\varepsilon$.

$$\begin{tikzcd}
E \arrow[rr, "f"] \arrow[dr, "\varepsilon"'] & & G \\
& E_E \arrow[ur, dotted, "\overline{f}"'] &
\end{tikzcd}$$

Olkoon $g\colon \mathbb{N} \to \mathbb{Z}_m$ kuvaus, joka on määritelty kaavalla $g(x) = \bar{x}$, joka on yhdiste inkluusiosta $\mathbb{N} \to \mathbb{Z}$ ja kanonisesta projektiosta tekijäryhmään $\mathbb{Z} \to \mathbb{Z}_m$. Kuvaus g on siis monoidihomomorfismi. Lisäksi jos $xR_{m,n}y$, niin $m|(x-y)$, joten $g(x) = g(y)$. Tästä seuraa, että g faktoroitu E:n kautta eli määrittele kuvauksen $f\colon E \to \mathbb{Z}_m$, $f(\bar{x}) = \bar{x} \in \mathbb{Z}_m$. Universaalin ominaisuuden nojalla on olemassa ryhmähomomorfismi $\overline{f}\colon E_E \to \mathbb{Z}_m$ jolle $\overline{f}\varepsilon = f$.
Olkoot $x, y \in \mathbb{N}$ joille $\varepsilon(\bar{x}) = \varepsilon(\bar{y})$. Tällöin

$$f(\bar{x}) = \overline{f}(\varepsilon(\bar{x})) = \overline{f}(\varepsilon(\bar{y})) = f(\bar{y})$$

eli $x \equiv y \pmod{m}$.

Huomautus: Huomaa, että yllä esitetty todistus ei käytä ollenkaan E_E:n konstruktiota, ainoastaan universaaliominaisuutta (ja sitä että E_E on ryhmä). Tämä on tyyppillinen tilanne matematiikassa - ei ole mitään merkitystä sillä "mitä"olio varsinaisesti on, ainoastaan mitkä ovat sen ominaisuudet. Yleensä konstruktio tarvitaan vain osoittamaan että haluttuja ominaisuuksia omaava olio on olemassa. Sitten kun olemassaolo on osoitettu riittää tuntea ainoastaan sen ominaisuudet.
Ei ole vaikeata osoittaa, että E_E on isomorfinen ryhmän $(\mathbb{Z}_m, +)$

kanssa. Kanoninen kuvaus $\varepsilon\colon E \to E_E$ vastaa tällöin kuvausta $f\colon E \to \mathbb{Z}_m$, joka on määritelty yllä.

3. Oletetaan, että ryhmä G toimii vasemmalta joukossa X. Jos $g \in G$ ja $\varphi : X \to Y$, määritellään $\varphi^g : X \to Y$ kaavalla $\varphi^g(x) = \varphi(gx)$. Osoita, että kaava $\varphi \mapsto \varphi^g$ määrittelee G:n oikeanpuoleisen toiminnan joukossa Y^X.

   Ratkaisu: Jokaisella $g \in G$ merkitään f_g:llä kuvausta $X \to X$, $g \mapsto gx$, kuten toiminnan määritelmässä. Tällöin siis $\varphi^g = \varphi \circ f_g$ jokaisella $\varphi\colon X \to Y$. Tällöin

$$\varphi e = \varphi^e = \varphi \circ f_e = \varphi \circ id_X = \varphi$$

   ja kaikilla $g, h \in G$ pätee

$$\varphi(gh)\varphi^{gh} = \varphi \circ f_{gh} = \varphi \circ (f_g \circ f_g) = (\varphi \circ f_g) \circ f_h = (\varphi^g)^h = (\varphi g)h.$$

   Näin ollen kaava $\varphi \mapsto \varphi^g$ määrittelee G:n oikeanpuoleisen toiminnan joukossa Y^X.

4. Oletetaan, että ryhmä G toimii joukossa X. Todista seuraavat väitteet:
   (a) Alkioiden radat muodostavat joukon X osituksen.
   (b) Jokainen rata on homogeeninen G-joukko.
   (c) Alkioiden kiinnittäjät ovat ryhmän G aliryhmiä, mutteivät välttämättä normaaleja.

   Ratkaisu: a) Määritellään joukossa X relaatio $\sim$ ehdolla $x \sim y$ jos ja vain jos on olemassa $g \in G$ jolle $y = gx$. Osoitetaan, että $\sim$ on kevivalenssirelaatio. Koska $ex = x$ jokaisella $x \in X$ relaatio on refleksiivinen. Jos $y = gx$, niin

$$x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y.$$

   Näin ollen $\sim$ on symmetrinen. Jos $y = gx$ ja $z = g'y$, niin

$$z = g'y = g'(gx) = (g'g)x,$$

   joten $z \sim x$. Siis $\sim$ on transitiivinen.
   Näin ollen $\sim$ on ekvivalenssirelaatio, joten radat Gx, jotka ovat relaation $\sim$ ekvivalenssiluokat mudostavat X:n osituksen.

   b) Jokainen rata Gx, $x \in X$ on selvästi vakaa G:n toiminnan suhteen, sillä jos $g' \in G$ ja $y = gx \in Gx$, niin

$$g'y = g'(gx) = (g'g)x \in Gx.$$

   Itse asiassa radat ovat minimaalisia X:n G-osajoukot ja jokainen G-osajoukko saadaan eräiden ratojen yhdisteenä.

Gx on homogeeninen, sillä jos $y = gx \in Gx$ ja $z = g'x \in Gx$, niin

$$z = g'x = (g'g^{-1})y.$$

c) Ensiksi todetaan, että $e \in G_x$ jokaisella $x \in X$, sillä

$$ex = x.$$

Toiseksi huomataan, että jos $g, h \in G_x$, niin $gx = x$ ja $hx = x$. Toisesta ehdosta saadaan kertomalla molemmat puoleet h^{-1} ehto $x = h^{-1}x$, joten

$$(gh^{-1})x = g(h^{-1}x) = gx = x.$$

Näin ollen $gh^{-1} \in G_x$.

G_x ei ole vältämättä normaali. Itse asiassa mielivaltaisen ryhmän G mielivaltainen aliryhmä H voidaan helposti realisoida jonkun G:n toimintaan liittyvänä kiinnittäjä-aliryhmänä. Nimittäin otetaan G:n kanoninen toiminta joukossa G/H, joka on määritelty kaavalla

$$g(g'H) = (gg')H.$$

Tällöin alkion $eH = H$ kiinnittäjä on H.

5. Todista *Cayleyn lause*: Jokainen ryhmä on isomorfinen jonkin permutaatioryhmän eli symmetrisen ryhmän aliryhmän kanssa. (Tarkastele translaatiota ryhmässä.) Mikä olisi vastaava tulos monoideilla?

Ratkaisu: Olkoon G ryhmä. Jokaisella $g \in G$ tarkastellaan translaatiokuvaus $f_g \colon G \to G$, joka on määritelty kaavalla

$$f_g(x) = gx.$$

Tällöin neutraalialkiolle $e \in G$ pätee $f_e = \mathrm{id}_G$. Lisäksi jos $g, h \in G$ niin $f_g \circ f_h = f_{gh}$. Tästä seuraa, että

$$f_g \circ f_{g^{-1}} = f_e = f_{g^{-1}} \circ f_g,$$

joten jokainen f_g on itse asiassa bijektio, käänteiskuvauksena $f_{g^{-1}}$. Voidaan siis määritellä kuvaus $F \colon G \to \mathrm{Sym}(G)$,

$$F(g) = f_g.$$

Yllä todistettu kaava $f_{gh} = f_g \circ f_h$ osoittaa, että F on ryhmähomomorfismi. Osoitetaan, että se on injektiivinen. Riittää osoittaa, että ydin on triviaali. Olkoon siis $g \in G$ jolla $f_g = \mathrm{id}_G$. Tällöin erityisesti

$$g = f_g(e) = id_G(e) = e.$$

Siis F on injektiivinen. Näin ollen G on isomorfinen ryhmän $\Im(F)$ kanssa, joka on permutaatioryhmä.

Jos G on vain monoidi voidaan määritellä $f_g \colon G \to G$ jokaisella $g \in G$ kuten yllä. Pätee edelleen, että $f_e = \mathrm{id}_G$ ja $f_{gh} = f_g \circ f_h$. Nyt kuitenkin f_g ei ole vältämättä bijektio joten saadaan monoidihomomorfismi

$$F \colon G \to G^G, F(g) = f_g.$$

F on edellenkin injektiivinen, mutta vetoaminen ytimeen ei enää toimi. Sen sijaan huomataan vain että yhtälö $f_g = f_h$ implikoi, että

$$g = f_g(e) = f_h(e) = h.$$

Saadaan siis seuraava tulos: Jokainen monoidi on isomorfinen jonkun monoidin X^X alimonoidin kanssa.

6. Olkoon G ryhmä ja $f_x(y) = xyx^{-1}$ kaikilla $x, y \in G$. Osoita, että f_x on G:n automofismi, ns. *sisäinen automorfismi*, kaikilla $x \in G$, ja että $x \mapsto f_x$ on G:n toiminta G:ssä, ns. *konjugointi*.

Ratkaisu: Olkoot $y, z \in G$. Tällöin

$$f_x(yz) = x(yz)x^{-1} = (xy)(x^{-1}x)zx^{-1} = (xyx^{-1})(xzx^{-1}) = f_x(y)f_x(z).$$

Näin ollen G on homomorfismi.
Seuraavaksi osoitetaan, että kuvaus $x \mapsto f_x$ on monoidihomomorfismi $G \to G^G$. Selvästi $f_e = \mathrm{id}_G$. Jos $x, x' \in G$, niin

$$f_{xx'}(y) = xx'y(xx')^{-1} = x(x'yx'^{-1})x^{-1} = f_x(x'yx'^{-1}) = f_x(f_{x'}(y)),$$

joten $f_{xx'} = f_x \circ f_{x'}$.
Siis $x \mapsto f_x$ on G:n toiminta G:ssä.

Periaattessa pitää vielä näyttää, että jokainen f_x on bijektio. Mutta tämä seuraa siitä, että $x \mapsto f_x$ on G:n toiminta G:ssä suoraan toimintojen yleisistä ominaisuuksista. Vaihtoehtoisesti voidaan näyttää suoraan, että $f_{x^{-1}}$ on f_x:n käänteiskuvaus.