Lukuteoria ja ryhmät

Vihjeet 8 kevät 2014

1. Olkoot G Abelin ryhmä ja $f\colon G \to G$, $f(a) = (a^{-1})^2$.
   a) Osoita, että f on ryhmähomomorfismi.
   b) Olkoon $G = \mathbb{Z}_{14}^*$. Määrää $\mathrm{Im}(f)$ ja $\mathrm{Ker}(f)$. (Voit käyttää apuna harjoituksen 5 tehtävää 6c).)
   c) Muodosta tekijäryhmä $G/\mathrm{Ker}(f)$ ja esitä sen ryhmätaulu.

   Vihje. a) Määritelmä 4.7.1.
   b) Määritelmä 4.7.7.
   c) Tavallista tekijäryhmän ja ryhmätaulun muodostamista.

2. Osoita, että ryhmähomomorfismi $f\colon G \to G'$ on injektio jos ja vain jos $\mathrm{Ker}(f) = \{e_G\}$.

   Vihje. Oleta ensin, että f on injektio. Osoita sen ja Lauseen 4.7.2 avulla, että $\mathrm{Ker}(f) = \{e_G\}$.
   Oleta $\mathrm{Ker}(f) = \{e_G\}$. Mitä tämä tarkoittaa Määritelmän 4.7.7 nojalla? Osoita, kun $x, y \in G$ ja $f(x) = f(y)$, että $f(xy^{-1}) = e_{G'}$. Tähän osoitukseen tarvitsee Määritelmää 4.7.1 ja Lausetta 4.7.2. Käytä tämän jälkeen oletusta $\mathrm{Ker}(f) = \{e_G\}$ sen osoittamiseen, että $x = y$.

3. Olkoon G kertalukua m oleva syklinen ryhmä. Osoita, että G on isomorfinen ryhmän $(\mathbb{Z}_m,+)$ kanssa.

   Vihje. Muodosta kuvaus $f\colon G \to \mathbb{Z}_m$. Kannattaa lähteä siitä liikkeelle, että neutraalialkio kuvautuisi neutraalialkioksi aina neutraalialkion ollessa kysymyksessä (eri alkion a potenssit). Mieti tämän jälkeen, miksi alkion a^k pitäisi kuvautua, että kuvaus olisi hyvin määritelty ja voitaisiin saada bijektio aikaiseksi. Kun saat kuvauksen keksittyä, osoita, että se on hyvin määritelty, homomorfismi, injektio ja surjektio.

4. Onko ryhmä $(\mathbb{Z}_4, +)$ isomorfinen ryhmän $(\mathbb{Z}_m^*, \cdot)$ kanssa, kun
   a) $m = 9$, b) $m = 5$, c) $m = 8$?

   Vihje. Määritelmän 4.7.9 jälkeinen huomautus, Lause 4.7.11 (tehtävä kolme ja Määritelmän 4.7.9 jälkeinen toinen huomautus). Lisäksi Määritelmästä 4.7.9 seuraa (luennot), että sellaiset ryhmät eivät voi olla isomorfiset, joista vain toinen on syklinen.

5. Olkoot $f\colon G \to G'$ ja $g\colon G' \to G''$ ryhmähomomorfismeja.
   a) Osoita, että $g \circ f\colon G \to G''$ on homomorfismi.
   b) Olkoot f ja g isomorfismeja. Osoita, että $g \circ f$ on isomorfismi.

   Vihje. a) Määritelmä 4.7.1.
   b) Bijektiivisyys osoitettu Johdatus matemaattiseen päättelyyn -kurssilla (ei tarvitse todistaa, kun vain kertoo, mikä tulos on voimassa).

6. Olkoon $f\colon G \to G'$ ryhmäisomorfismi. Osoita, että $f^{-1}\colon G' \to G$ on isomorfismi.

   Vihje. Bijektiivisyys osoitettu Johdatus matemaattiseen päättelyyn -kurssilla (ei tarvitse todistaa, kun vain kertoo, mikä tulos on voimassa). Homorfismin saa osoitettua surjektion avulla.

7. Osoita, että ryhmien välinen isomorfia on ekvivalenssirelaatio missä tahansa ryhmistä muodostuvassa joukossa. (Käytä apuna kahden edellisen tehtävän tuloksia.)

   Vihje. Määritelmä 1.3. Refleksiivisyyden saat, kun osoitat kuvauksen $i\colon G \to G$, $i(a) = a$, ryhmäisomorfismiksi. Miksi symmetrisyys ja transitiivisuus seuraavat tehtävistä 5 ja 6?

8. Kuvaus $f\colon (\mathbb{Z}_{32}^*) \to (\mathbb{Z}_{32}^*)$, $f(a) = a^2$, on ryhmähomomorfismi. Osoita, että $(\mathbb{Z}_{32}^*/\mathrm{Ker}(f), \cdot) \cong (\mathbb{Z}_4, +)$.

   Vihje. Määrää ryhmä $\mathbb{Z}_{32}^*$. Ilmoita loppuosan alkiot vielä niin, että ne on ilmoitettu pienimmän negatiivisen edustajan avulla. Määrää $\mathrm{Im}(f)$ tai $\mathrm{Ker}(f)$. Voit käyttää Homomorfismien peruslausetta (Lause 4.7.10) tapauksessa $\mathrm{Im}(f)$, mutta kuitenkin molemmissa tapauksissa $\mathrm{Im}(f)$ ja $\mathrm{Ker}(f)$ tehtävästä 3 on hyötyä.

9. Olkoot $M = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \text{ ja } \det A \neq 0\}$
   ja $N = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \text{ ja } \det A = 1\}$.
   Harjoituksen 5 perusteella tiedetään, että $(M, \cdot)$ ja $(\mathbb{R}^* = \mathbb{R} \setminus \{0\}, \cdot)$ ovat ryhmiä. Osoita, että $(N, \cdot) \trianglelefteq (M, \cdot)$ ja $(M/N, \cdot) \cong (\mathbb{R}^*, \cdot)$. (Vihje: Etsi sellainen homomorfismi $f\colon M \to \mathbb{R}^*$, jolle $\mathrm{Ker}(f) = N$ ja $\mathrm{Im}(f) = \mathbb{R}^*$.)

   Vihje. Homomorfismien peruslauseen (Lause 4.7.10) nojalla riittää etsiä sellainen kuvaus $f\colon M \to \mathbb{R}^*$, joka on homomorfismi ja jolle $\mathrm{Ker}(f) = N$ ja $\mathrm{Im}(f) = \mathbb{R}^*$. Osoita, että kuvaus $f\colon M \to \mathbb{R}^*$, $f(A) = \det A$ on tälläinen.