Lukuteoria ja ryhmät

Vihjeet 6 kevät 2014

1. a) Osoita, että $\mathbb{Q}$ (rationaaliluvut) on ryhmän $(\mathbb{R}, +)$ aliryhmä.
   b) Osoita, että $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ on ryhmän $(\mathbb{R}^*, \cdot)$ aliryhmä.

   Vihje. Lausetta 4.3.2 (aliryhmäkriteeri) kannattaa käyttää molemmissa kohdissa. Ensin pitää varmistaa, että lauseen oletukset ovat voimassa.

2. a) Ovatko $H_1 = \{[0], [4]\}$ ja $H_2 = \{[0], [3], [6]\}$ ryhmän $(\mathbb{Z}_8, +)$ aliryhmiä?
   b) Määrää edellä oleville aliryhmille vasemmat sivuluokat.

   Vihje. a) Äärellisen osajoukon kyseessä ollessa kannattaa käyttää Seurausta 4.3.4 (Lauseesta 4.3.2 riittää 1. kohta). Aliryhmäksi osoittamiseen riittää, että katsoo 'ryhmätaulusta', että laskutoimituksen tulos pysyy aina osajoukossa. Jos ei ole aliryhmä, niin joko Lagrengen lauseen (Lause 4.3.8) avulla perustelu tai sitten osoittaa, että jokin laskutoimituksen tulos ei ole osajoukossa.
   b) Määritelmä 4.3.5. Ota ensin neutraalialkio ja määrää sen määräämä sivuluokka. Tähän sivuluokkaan tulevat alkiot määräävät myös tämän sivuluokan. Ota sellainen aliryhmän alkio, joka ei kuulu edelliseen sivuluokkaan ja määrää sen määräämä sivuluokka. Ota sellainen aliryhmän alkio, joka ei kuulu edellisiin sivuluokkiin ja määrää sen määräämä sivuluokka. Toista tätä, niin kauan, että jokainen aliryhmän alkio kuuluu täsmälleen yhteen sivuluokkaan.

3. Ota esille edellisessä harjoituksessa tehty ryhmän $(\mathbb{Z}_{14}^*, \cdot)$ ryhmätaulu.
   a) Onko $H_1 = \{[1], [5], [11]\}$ ryhmän $\mathbb{Z}_{14}^*$ aliryhmä?
   b) Osoita, että $H_2 = \{[1], [9], [11]\}$ on ryhmän $\mathbb{Z}_{14}^*$ aliryhmä.
   c) Määrää aliryhmän H_2 vasemmat sivuluokat.

   Vihje. a) Pysyykö laskutoimituksen tulos aina osajoukossa H_1?
   b) Aliryhmäksi soittamiseen riittää, että katsoo 'ryhmätaulusta', että laskutoimituksen tulos pysyy aina osajoukossa.
   c) Sama vihje kuin tehtävässä 2b).

4. Olkoon G ryhmä sekä H ja K ryhmän G aliryhmiä.
   a) Osoita, $H \cap K$ on ryhmän G aliryhmä.
   b) Onko $H \cap K$ ryhmien H ja K aliryhmä?
   c) Tiedetään, että $|K| = 40$ ja $|H| = 33$. Mitä voit sanoa aliryhmän $H \cap K$ kertaluvusta ja itse aliryhmästä $H \cap K$?

   Vihje. a) Voi itse valita käyttääkö Lausetta 4.3.2 vai Seurausta 4.3.3. Ensin pitää varmistaa, että lauseen/seurauksen oletukset ovat voimassa.
   b) Toteutuuko Määritelmän 4.3.1 ehdot?

c) Lagrangen lause (Lause 4.3.8) ja mieti lopuksi, mitä alkioita ryhmään $H \cap K$ kuuluu.

5. Olkoon G Abelin ryhmä. Olkoot $H \leq G$ ja $K \leq G$. Merkitään

$$HK = \{ab \mid a \in H, b \in K\}.$$

Osoita, että $HK \leq G$.

Vihje. Voi itse valita käyttääkö Lausetta 4.3.2 vai Seurausta 4.3.3. Ensin pitää varmistaa, että lauseen/seurauksen oletukset ovat voimassa.

6. a) Määrää ryhmän $(\mathbb{Z}_{18}^*, \cdot)$ alkioiden generoimat sykliset ryhmät.
b) Onko $(\mathbb{Z}_{18}^*, \cdot)$ on syklinen?
c) Mitkä ovat ryhmän $(\mathbb{Z}_{18}^*, \cdot)$ aliryhmät?
d) Määrää kertalukua 6 olevan syklisen ryhmän $G = \langle a \rangle$ kaikki aliryhmät.

Vihje. a) Määritelmä 4.4.1 eli käy ryhmän $\mathbb{Z}_{18}^*$ alkiot yksi kerrallaan läpi ja katso, mitä alkioita tulee, kun alkiolla tehdään kertolaskuja vain itsensä kanssa.
b) Generoiko joku alkio koko ryhmän $\mathbb{Z}_{18}^*$?
c) Lause 4.4.7.
d) Muodosta ryhmä G. Käy ryhmän G alkiot yksi kerrallaan läpi ja katso, mitä alkiota tulee, kun alkioita operoidaan vain itsensä kanssa.

7. a) Määrää ryhmän $(\mathbb{Z}_{15}^*, \cdot)$ alkioiden generoimat sykliset ryhmät.
b) Onko ryhmä $(\mathbb{Z}_{15}^*, \cdot)$ syklinen?
c) Määrää ryhmän $(\mathbb{Z}_{15}^*, \cdot)$ kaikki aliryhmät.

Vihje. a) Määritelmä 4.4.1 eli käy ryhmän $\mathbb{Z}_{15}^*$ alkiot yksi kerrallaan läpi ja katso, mitä alkioita tulee, kun alkiolla tehdään kertolaskuja vain itsensä kanssa.
b) Generoiko joku alkio koko ryhmän $\mathbb{Z}_{15}^*$?
c) Syklinen aliryhmä on aina pienin aliryhmä, johon sen generoija alkiot kuuluvat. Lagrangen lauseen (Lause 4.3.8) avulla voi tämän tiedon pohjalta päätellä, mitä vaihtoehtoja aliryhmiksi vielä olisi, jonka jälkeen pitää katsoa toteutuuko aliryhmän ehdot.

8. a) Osoita, että ryhmä $(\mathbb{Z}, +)$ on syklinen.
b) Osoita, että syklisen ryhmän $(\mathbb{Z}_m, +)$ generoi mikä tahansa alkio $[a]$, jolle $\text{syt}(a, m) = 1$. (Vihje: Käytä Lausetta 2.30.)

Vihje. a) Osoita, että luku 1 generoi ryhmän $(\mathbb{Z}, +)$.
b) Lähde liikkeelle yhtälöstä $ax \equiv b\ (m)$, missä $b \in \mathbb{Z}$ mielivaltainen. Käytä Lausetta 2.30 ja päättele loppu.