**Algebralliset rakenteet I**
**Helsingin yliopisto, matematiikan ja tilastotieteen laitos**
**Kevät 2017**
**Harjoitus 3 - Ratkaisuehdotuksia**

## Tehtäväsarja I

Huomautus: Kirjan aliryhmän määritelmä (3.12 kolmas painos) sanoo että jos on annettu ryhmä $(G, \cdot)$ ja osajoukko $H \subset G$, niin pari $(H, \cdot)$ on ryhmän $(G, \cdot)$ aliryhmä mikäli tietyt ehdot toteutuvat. Sillä $H$ varustettiin samalla laskutoimituksella kuin $G$, on yleinen käytäntö lyhentää sanoma "$(H, \cdot)$ on ryhmän $(G, \cdot)$ aliryhmä" sanomalla pelkästään että "$H$ on ryhmän $(G, \cdot)$ aliryhmä", sillä $H$:n laskutoimitus on kontekstista selvä (sama kuin $G$:llä, tai oikeastaan sen rajoittuma joukkoon $H$).

1. Onko $H = \{7^n \mid n \in \mathbb{Z}\}$ ryhmän $(\mathbb{Q}, +)$ aliryhmä?

   **Ratkaisuehdotus:** $H$ ei ole ryhmän $(\mathbb{Q}, +)$ aliryhmä, koska ryhmän $(\mathbb{Q}, +)$ neutraalialkiota 0 ei voi kirjoittaa muodossa $7^n$ millään $n \in \mathbb{Z}$ (koska $7^n > 0$ kaikilla $n \in \mathbb{Z}$).

   Toinen tapa saadaan siitä, että $H$ ei sisällä jokaisen (itse asiassa yhdenkään) alkionsa käänteisalkiota. Esimerkiksi $1 \in H$, mutta sen käänteisalkio yhteenlaskussa on $-1$. Edellä kuitenkin jo todettiin, että $H$ sisältää ainoastaan positiivisia lukuja, joten $-1 \notin H$.

   Kolmas tapa on huomata, että $H$ ei ole vakaa laskutoimituksen suhteen. Esimerkiksi $1 = 7^0 \in H$, mutta $1 + 1 = 2$ ei ole seitsemän potenssi. Tätä voi perustella esimerkiksi näin: Funktio $n \mapsto 7^n$ kokonaisluvuilta rationaalilukuihin on aidosti kasvava (mikä todistetaan esimerkiksi analyysin kursseilla). Koska $7^0 = 1 < 2$, niin $7^n < 2$ kaikilla $n \leq 0$. Toisaalta $7^1 = 7 > 2$, joten $7^n > 2$ kaikilla $n \geq 1$. Siis joka tapauksessa $7^n \neq 2$ kaikilla $n \in \mathbb{Z}$.

2.⋆ Onko $H = \{7^n \mid n \in \mathbb{Z}\}$ ryhmän $(\mathbb{Q} \setminus \{0\}, \cdot)$ aliryhmä?

   **Ratkaisuehdotus:** Osoitetaan, että joukko $A = \{7^n \mid n \in \mathbb{Z}\}$ on ryhmän $(\mathbb{Q}\setminus\{0\}, \cdot)$ aliryhmä.

   Ensinnäkin $A \subset \mathbb{Q} \setminus \{0\}$, koska kaikki $A$:n alkiot ovat nollasta poikkeavia rationaalilukuja.

   (H1) Oletetaan, että $a, b \in A$. Tällöin $a = 7^n$ ja $b = 7^m$ joillakin $n, m \in \mathbb{Z}$. Nähdään, että $ab = 7^m \cdot 7^n = 7^{m+n}$. Koska $n + m \in \mathbb{Z}$, kuuluu tulo $ab$ joukkoon $A$.

   (H2) Ryhmän $\mathbb{Q} \setminus \{0\}$ neutraalialkio on 1. Koska $1 = 7^0$, on neutraalialkio joukossa $A$.

   (H3) Oletetaan, että $a \in A$. Nyt $a = 7^n$ jollakin $n \in \mathbb{Z}$. Rationaaliluvun $a$ käänteisalkio on käänteisluku $a^{-1}$. Osoitetaan, että se on joukossa $A$. Potenssien laskusääntöjen mukaan $a^{-1} = (7^n)^{-1} = 7^{-n}$. Koska $-n \in \mathbb{Z}$, on $a^{-1}$ joukon $A$ alkio.

   Siten aliryhmän ehdot täyttyvät.

3. Onko $(K_{12}, \circleddash)$ ryhmän $(\mathbb{Z}, +)$ aliryhmä?

   **Ratkaisuehdotus:** Ei ole. Molemmat ovat kyllä ryhmiä ja lisäksi $K_{12} \subset \mathbb{Z}$, mutta laskutoimitukset $\circleddash$ ja $+$ eivät ole samat. Esimerkiksi $12 \circleddash 1 = 1$, mutta $12 + 1 = 13$. Niinpä $(K_{12}, \circleddash)$ ei ole ryhmän $(\mathbb{Z}, +)$ aliryhmä.

4.⋆ Olkoon $A = \{0, 1, 2\}$ ja olkoon $\star$ joukossa $A$ määritelty laskutoimitus siten että $(A, \star)$ on ryhmä, jonka neutraalialkio on 0. Mitä on $1 \star 1$?

**Ratkaisuehdotus:** Annettujen tietojen perusteella voidaan määrittää laskutoimitustaulu. Koska 0 on neutraalialkio, aloitetaan täyttämällä sen rivit ja sarakkeet:

| $\star$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | $a$ | $b$ |
| 2 | 2 | $c$ | $d$ |

Koska $(A, \star)$ on ryhmä, lemman 3.10 (toinen painos) nojalla jokainen alkio täytyy esiintyä jokaisella rivillä ja jokaisessa sarakkeessa täsmälleen kerran, joten huomataan että $b$ on oltava 0 (samassa sarakkeessa kuin $b$ on jo alkio 2, ja samalla rivillä alkio 1). Sen avulla voidaan täydentää taulua:

| $\star$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

Nyt taulusta nähdään, että $1 \star 1 = 2$.

5. Olkoon $[0, 1] \subset \mathbb{R}$ yksikköväli. Olkoon

$$X = \{f : [0, 1] \to [0, 1] \mid f \text{ on jatkuva, aidosti kasvava surjektio}\}$$

jossa on määritelty laskutoimitus $\circ$, eli kuvausten yhdistäminen. Osoita, että $(X, \circ)$ on ryhmä.
**Ratkaisuehdotus:** Käydään läpi kaikki ryhmän määritelmän ehdot.

(G0) Oletetaan, että $f, g \in X$. Nyt $(f \circ g)(x) = f(g(x))$. Koska $g$ ja $f$ ovat aidosti kasvavia, tiedetään että kaikilla $x_1, x_2 \in [0, 1]$ pätee $x_1 < x_2 \Rightarrow g(x_1) < g(x_2)$ ja $x_1 < x_2 \Rightarrow f(x_1) < f(x_2)$, eli

$$x_1 < x_2 \Rightarrow g(x_1) < g(x_2) \Rightarrow f(g(x_1)) < f(g(x_2)).$$

Sen perusteella $f \circ g$ on aidosti kasvava, eli jos $f, g \in X$ niin $f \circ g \in X$. Laksutoimitus on siis määritelty joukossa X.

(G1) Lauseen 1.10(toinen painos) nojalla laskutoimitus $\circ$ on liitännäinen.

(G2) Neutraalialkio $e$ on funktio, jolle pätee $e \circ f = f$ ja $f \circ e = f$ kaikille $f \in X$. Oletetaan, että $f \in X$, ja arvataan, että $e(x) = x$. Nyt

$$(f \circ e)(x) = f(e(x)) = f(x)$$

ja

$$(e \circ f)(x) = e(f(x)) = f(x).$$

Neutraalialkio on siis $e(x) = x$, ja koska kuvaus $e(x) = x$ selvästi on jatkuva, aidosti kasvava surjektio, $e \in X$.

(G3) Oletetaan, että $f \in X$. Lauseen 1.13(toinen painos) nojalla $f$ on kääntyvä, jos ja vain jos se on bijektio. Tiedetään jo, että $f$ on surjektion, joten osoitetaan ensin, että se myös on injektio. Tehdään vastaoletus: oletetaan, että $f$ ei ole injektio. On siis olemassa jotkut alkiot $x_1, x_2 \in [0, 1]$, $x_1 > x_2$, niin että $f(x_1) = f(x_2)$. Mutta koska $f$ on aidosti kasvava, niin jos $x_1 < x_2$, pitää pätеä myös $f(x_1) < f(x_2)$. Päädytään siis ristiriitaan, eli $f$ on oltava injektio.

Nyt $f$ on siis bijektio (koska se on sekä injektio että surjektio) eli lauseen 1.13 (toinen painos) nojalla sillä on joku käänteisfunktio $f^{-1}$.

Nyt siis pätee, että $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x$. Tarkistetaan, onko $f^{-1}$ aidosti kasvava. Tehdään vastaoletus: $f^{-1}$ ei ole aidosti kasvava. Oletetaan että $x_1, x_2 \in [0,1]$ ovat sellaiset, että $f(x_1) < f(x_2)$, ja $f^{-1}(f(x_1)) = x_1 \geq x_2 = f^{-1}(f(x_2))$. Päädytään ristitiitaan, sillä jos $x_1 \geq x_2$, niin $f(x_1) \geq f(x_2)$, koska $f$ on aidosti kasvava, mutta oletuksen mukaan $f(x_1) < f(x_2)$.

Käänteisfunktio $f^{-1}$ on siis aidosti kasvava, jos $f$ on aidosti kasvava, eli kaikille $f \in X$ myös $f^{-1} \in X$.

Kaikki ryhmän ehdot täyttyivät, joten $(X, \circ)$ on ryhmä.

### Tehtäväsarja II

6. Piirrä kuvat permutaatioista $\sigma$ ja $\tau$. Voit valita mielestäsi parhaan tavan havainnollistaa permutaatiota.

   **Ratkaisuehdotus:** Tähän voi esimerkiksi piirää kirjan kuvan 4.2 kaltaisen nuolikaavion. Tässä ratkaisuehdotuksessa ei teknisistä syistä esitetä kuvia.

7. Laske tulot $\sigma \circ \tau$, $\tau \circ \sigma$ ja $\sigma \circ \rho$.

   **Ratkaisuehdotus:** Muista, että permutaatioiden laskujärjestys on oikealta vasemmalle!

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}$$
$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$$
$$\sigma \circ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

   Huomaa, että $\sigma \circ \tau \neq \tau \circ \sigma$. Permutaatioiden tulo ei siis ole vaihdannainen laskutoimitus.

8. Määritä permutaatioiden $\sigma$ ja $\tau$ radat. Kuvista on apua.

   **Ratkaisuehdotus:** Permutaation $\sigma$ radat ovat $\{1,5,3\}$ ja $\{2,4\}$. Permutaatiosta voi myös kirjoittaa rataesityksen, jos haluaa: $\sigma = (24)(153)$. Myös kunkin radan alkioiden luetteleminen on kelvollinen ratkaisu.

   Muille permutaatioille saadaan rataesitykset $\tau = (13)(45)(2)$ ja $\rho = (135)(2)(4)$.

### Tehtäväsarja III

9. Seuraavassa on annettu permutaatioiden sykliesityksiä. Piirrä permutaatoista kuvat, joista näkyy, miten permutaatio kuvaa määrittelyjoukon alkioita.

   (a) ryhmän $S_4$ alkio (1324)
   (b) ryhmän $S_6$ alkio (1324)
   (c) ryhmän $S_5$ alkio (14)(253)

   **Ratkaisuehdotus:**

   (a) Kuvassa pitäisi näkyä neljän alkion sykli.

(b) Kuvassa pitäisi näkyä neljän alkion sykli sekä alkiot 5 ja 6, jotka pysyvät paikoillaan.
(c) Kuvassa pitäisi näkyä kahden alkion sykli ja kolmen alkion sykli.

10. Mitkä seuraavista väitteistä pitävät paikkansa?

(a) Ryhmän $S_6$ alkiot (16)(35) ja (35)(16) ovat samat.
(b) Ryhmän $S_4$ alkiot (134) ja (143) ovat samat.
(c) Ryhmän $S_6$ alkiot (236) ja (362)(4)(5) ovat samat.

**Ratkaisuehdotus:**

(a) Pitää paikkansa. Erillisten syklien järjestyksellä ei ole väliä.
(b) Ei pidä paikkaansa. Esimerkiksi alkio 1 kuvautuu ensimmäisessä permutaatiossa alkioksi 3 ja toisessa alkioksi 4, eivätkä kyseessä voi siten olla samat permutaatiot.
(c) Pitää paikkansa, sillä $(236) = (362)$ eikä yhden alkion syklejä tarvitse kirjoittaa näkyviin.

11. Määritellään

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 3 & 6 & 7 & 5 & 2 \end{pmatrix} \quad \text{ja} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 6 & 4 & 5 & 7 \end{pmatrix}.$$

Kirjoita permutaatioiden $\alpha$ ja $\beta$ sykliesitykset. Pelkkä vastaus riittää ratkaisuksi.

**Ratkaisuehdotus:** $\alpha = (146572)$, $\beta = (23)(465)$

## Tehtäväsarja IV

12. Jäännösluokkien joukossa $\mathbb{Z}_n$ voi määritellä yhteenlaskun kaavalla $[a]_n + [b]_n = [a+b]_n$. Osoita, että

(a) $[3]_5 + [6]_5 = [4]_5$
(b) $[5]_7 + [3]_7 = [1]_7$.

Mitä tuttua laskutoimitusta jäännösluokkien yhteenlasku muistuttaa?

**Ratkaisuehdotus:** a) Yhteenlaskun määritelmän mukaan $[3]_5 + [6]_5 = [3+6]_5 = [9]_5$. Jäännösluokassa $[9]_5$ ovat kaikki ne luvut, joiden jakojäännös luvulla 4 jaettaessa on sama kuin luvulla 9. Toisin sanoen jäännösluokassa $[9]_5$ ovat kaikki ne luvut, joista jää viidellä jaettaessa jakojäännökseksi 4. Samalla tavalla jäännösluokassa $[4]_5$ ovat kaikki ne luvut, joista jää viidellä jaettaessa jakojäännökseksi 4. Näin ollen $[9]_5 = [4]_5$. Siten $[3]_5 + [6]_5 = [4]_5$.

Yleisemmin voidaan todeta, että jäännösluokat $[a]_n$ ja $[b]_n$ ovat samat, jos ja vain jos luvuilla $a$ ja $b$ on sama jakojäännös luvulla $n$ jaettaessa. Toisin sanoen $[a]_n = [b]_n$, jos ja vain jos $a \equiv b \pmod{n}$.

b) Huomataan, että $[5]_7 + [3]_7 = [5+3]_7 = [8]_7$. Koska $8 \equiv 1 \pmod{7}$, pätee $[8]_7 = [1]_7$.

Jäännösluokkien yhteenlasku muistuttaa aiemmissa harjoituksissa ollutta kellotaulusummaa.

13. Päteekö $[-6]_3 + [2]_3 = [4]_3$? Perustele vastauksesi.

**Ratkaisuehdotus:** Lasketaan aluksi summa $[-6]_3 + [2]_3$.

$$[-6]_3 + [2]_3 = [-6+2]_3 = [-4]_3.$$

Pitää siis selvittää, päteekö $[-4]_3 = [4]_3$.

Samaan tapaan kuin edellisissä tehtävässä riittää vain tarkistaa, ovatko luvut $-4$ ja 4 kongruentteja modulo 3. Koska erotus jos $-4-4 = -8$ ei ole jaollinen luvulla 3, ei päde $-4 \equiv 4 \pmod{3}$. Näin ollen $[-4]_3 \neq [4]_3$. Siten väite ei päde.

14.* Jäännösluokkien joukko $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ on ryhmä jäännösluokkien yhteenlaskun suhteen (Lause 6.11 kolmas painos). Kirjoita ryhmän laskutoimitustaulu ja näytä että se on vaihdannainen.

**Ratkaisuehdotus:**

| $+$ | $[0]_4$ | $[1]_4$ | $[2]_4$ | $[3]_4$ |
|---|---|---|---|---|
| $[0]_4$ | $[0]_4$ | $[1]_4$ | $[2]_4$ | $[3]_4$ |
| $[1]_4$ | $[1]_4$ | $[2]_4$ | $[3]_4$ | $[0]_4$ |
| $[2]_4$ | $[2]_4$ | $[3]_4$ | $[0]_4$ | $[1]_4$ |
| $[3]_4$ | $[3]_4$ | $[0]_4$ | $[1]_4$ | $[2]_4$ |

Kuten ensimmäisen viikon tehtävässä 5 todettiin, nähdään että ryhmä on vaihdannainen siitä, että sen laskutoimitustaulu on symmetrinen lävistäjän suhteen. Halutaan kuitenkin näyttää että ryhmä on vaihdannainen vähän täsmällisemmin, ja koska ryhmässä on vain muutama alkio, voidaan kaikille alkioille tarkistaa, onko $[a]_4 + [b]_4 = [b]_4 + [a]_4$.

## Tehtäväsarja V

15. Merkitään

$$A = \begin{bmatrix} 1 & 1 & -1 \\ 0 & -1 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 1 \\ -1 & -1 \\ -1 & 0 \end{bmatrix} \quad \text{ja} \quad C = \begin{bmatrix} 1 & 0 & 2 \end{bmatrix}.$$

(a) Osoita, että

$$AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$$

Voit tarvittaesa kerrata matriisikertolaskua kurssikirjan liitteestä.

(b) Tutkitaan nyt yhtälöä

$$XA = C,$$

missä $X \in \mathbb{R}^{1\times 2}$. Tarkastellaan seuraavaa päättelyketjua:

$$\begin{aligned} & XA = C \\ \Leftrightarrow\quad & XAB = CB \\ \Leftrightarrow\quad & XI = CB \\ \Leftrightarrow\quad & X = CB \\ \Leftrightarrow\quad & X = \begin{bmatrix} -1 & 1 \end{bmatrix}. \end{aligned}$$

Tarkista, että $X = [-1\ 1]$ ei ole yhtälön $XA = C$ ratkaisu. Mikä päättelyssä menee pieleen?

(c) Vaihda päättelyketjussa ekvivalenssinuolten tilalle tarpeen mukaan implikaationuolia niin, että päättelyketju on tosi.

**Ratkaisuehdotus:**

(a)

$$\begin{aligned} AB &= \begin{bmatrix} 1\cdot 1 + 1\cdot(-1) + (-1)\cdot(-1) & 1\cdot 1 + 1\cdot(-1) + (-1)\cdot 0 \\ 0\cdot 1 + (-1)\cdot(-1) + 1\cdot(-1) & 0\cdot 1 + (-1)\cdot(-1) + 1\cdot 0 \end{bmatrix} \\ &= \begin{bmatrix} 1-1+1 & 1-1+0 \\ 0+1-1 & 0+1+0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I. \end{aligned}$$

(b) Huomataan, että

$$XA = \begin{bmatrix}(-1)\cdot 1 + 1\cdot 0 & (-1)\cdot 1 + 1\cdot(-1) & (-1)\cdot(-1) + 1\cdot 1\end{bmatrix}$$
$$= \begin{bmatrix}-1+0 & -1-1 & -1+1\end{bmatrix} = \begin{bmatrix}-1 & -2 & 0\end{bmatrix} \neq C.$$

Koska saatu ratkaisuehdokas ei olekaan yhtälön ratkaisu, yhtälöllä ei ole ratkaisua.
Huomataan, että

$$BA = \begin{bmatrix} 1\cdot 1 + 1\cdot 0 & 1\cdot 1 + 1\cdot(-1) & 1\cdot(-1) + 1\cdot 1 \\ (-1)\cdot 1 + (-1)\cdot 0 & (-1)\cdot 1 + (-1)\cdot(-1) & (-1)\cdot(-1) + (-1)\cdot 1 \\ (-1)\cdot 1 + 0\cdot 0 & (-1)\cdot 1 + 0\cdot(-1) & (-1)\cdot(-1) + 0\cdot 1 \end{bmatrix}$$
$$= \begin{bmatrix} 1+0 & 1-1 & -1+1 \\ -1+0 & -1+1 & -1+1 \\ -1+0 & -1+0 & 1+0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 0 & 0 \\ -1 & -1 & 1 \end{bmatrix} \neq I.$$

Ongelma löytyy päättelyketjun ensimmäisessä askeleessa. Toisesta yhtälöstä ei seuraa ensimmäistä, koska pitäisi kertoa oikealta matriisilla $A$, mutta kuten huomattiin, $BA \neq I$, joten $CBA \neq C$.

(c) Ensimmäisestä yhtälöstä seuraa toinen, mutta toisesta ei seuraa ensimmäistä, joten vaihdetaan ensimmäinen ekvivalenssi implikaatioon:

$$\begin{aligned} & XA = C \\ \Rightarrow\quad & XAB = CB \\ \Leftrightarrow\quad & XI = CB \\ \Leftrightarrow\quad & X = CB \\ \Leftrightarrow\quad & X = \begin{bmatrix}-1 & 1\end{bmatrix}. \end{aligned}$$

Nyt päättelyketju on tosi.

16. Oletetaan, että $G$ on ryhmä, jossa on alkiot $a$ ja $b$. Ratkaise ryhmässä $G$ yhtälö $x^2a^2 = xb$.

*Neuvo:* Muista edellisen tehtävän havainnot. Jos käytät yhtälönratkaisussa ekvivalenssinuolia, perustele päättelyn molemmat suunnat. Yhtälöitä on mahdollista ratkaista myös implikaatioiden avulla.

**Ratkaisuehdotus:**

Etsitään yhtälön ratkaisu muokkaamalla sitä. Saadaan

$$\begin{gathered} x^2a^2 = xb \\ \Rightarrow xxa^2 = xb \\ \Rightarrow x^{-1}xxa^2 = x^{-1}xb \\ \Rightarrow xa^2 = b \\ \Rightarrow xaa = b \\ \Rightarrow xaaa^{-1} = ba^{-1} \\ \Rightarrow xa = ba^{-1} \\ \Rightarrow xaa^{-1} = ba^{-1}a^{-1} \\ \Rightarrow x = b(a^{-1})^2 \\ \Rightarrow x = ba^{-2}. \end{gathered}$$

Nyt ollaan saatu ainoa mahdollinen ratkaisu yhtälölle: jos yhtälöllä on ratkaisu, se on $x = ba^{-2}$. Osoitetaan vielä, että tämä todella on yhtälön ratkaisu:

$$x^2a^2 = (ba^{-2})^2a^2 = ba^{-2}ba^{-2}a^2 = (ba^{-2})b.$$

Siten yhtälön ratkaisu on $x = ba^{-2}$.

17. Oletetaan, että edellisessä kohdan ryhmä on kellotauluryhmä $(K_7, \oplus)$. Oletetaan lisäksi, että $a = 4$ ja $b = 2$. Mikä tässä tapauksessa on yhtälön ratkaisu?

**Ratkaisuehdotus:**

Ryhmän $(K_7, \oplus)$ neutraalialkio on 7, joten alkion $a = 4$ käänteisalkio on $a^{-1} = 3$, sillä $4 + 3 = 7 = 3 + 4$. Nyt voidaan sijoittaa nämä alkiot edellisen tehtävän ratkaisukaavaan:

$$x = ba^{-2} = ba^{-1}a^{-1} = 2 \oplus 3 \oplus 3 = (2 \oplus 3) \oplus 3 = 5 \oplus 3 = 1.$$

18.* Tutkitaan ryhmää $G = \{a, b, c, d, e, f\}$, jolla on seuraavanlainen laskutoimitustaulu:

| $+$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |
|---|---|---|---|---|---|---|
| $a$ | $f$ | $d$ | $a$ | $e$ | $b$ | $c$ |
| $b$ | $e$ | $c$ | $b$ | $f$ | $a$ | $d$ |
| $c$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |
| $d$ | $b$ | $a$ | $d$ | $c$ | $f$ | $e$ |
| $e$ | $d$ | $f$ | $e$ | $a$ | $c$ | $b$ |
| $f$ | $c$ | $e$ | $f$ | $b$ | $d$ | $a$ |

Määritä seuraavat alkiot:

**(a)** $-d$ **(b)** $3a + 2e$ **(c)** $(-4)f$.

(Huomaa, että tämä on kolmen alkion permutaatioryhmä ja toisaalta tasasivuisen kolmion symmetriaryhmä. Tästä huomautuksesta ei ole tarkoitus olla mitään apua tehtävän ratkaisemiseen).

**Ratkaisuehdotus:**

(a) Laskutoimitustaulusta nähdään, että laskutoimituksen neutraalialkio on $c$. Laskutoimitustaulu perusteella $d + d = c$. Näin ollen $d$ on itsensä käänteisalkio, joten $-d = d$.
(b) $3a + 2e = a + a + a + e + e = f + a + e + e = c + e + e = e + e = c$
(c) Lauseen 3.8 perusteella (ks. huomio sivulla 29) pätee $(-4)f = 4(-f)$. Nyt

$$4(-f) = 4a = a + a + a + a = f + a + a = c + a = a.$$

19. Oletetaan, että $(G, +)$ on vaihdannainen ryhmä, jolla on neutraalialkio $e$. Osoita, että joukko $H = \{a \in G \mid 3a = e\}$ on ryhmän $G$ aliryhmä.

**Ratkaisuehdotus:** Selvästi $H \subset G$, joten yhteenlaskulla varustettuna kyseinen joukko todella saattaa olla $G$:n aliryhmä.

Ainakin $H$ sisältää $G$:n neutraalialkion $e$, koska tälle pätee $3e = e + e + e = e + e = e$. Jos sitten $a, b \in H$ ovat mielivaltaiset, pätee ryhmän vaihdannaisuuden nojalla niiden summalle

$$3(a + b) = (a + b) + (a + b) + (a + b) = a + a + a + b + b = 3a + 3b = e + e = e,$$

joten myös $a + b \in H$. Siis $H$ on vakaa yhteenlaskun suhteen. Jos vielä $a \in H$, niin sillä on $G$:ssä vasta-alkio $-a$; lauseen 3.8 nojalla

$$3(-a) = -(3a) = -e = e,$$

joten $-a \in H$.

Näin ollen kaikki aliryhmän ehdot täyttyvät ja $H$ todella on $G$:n aliryhmä.

**Ylimääräiset tehtävät**

20. Lauseessa 3.17 on osoitettu, että kahden aliryhmän leikkaus on aina aliryhmä. Anna esimerkki tilanteesta missä kahden aliryhmän yhdiste ei ole aliryhmä.

    **Ratkaisuehdotus:**

    Valitaan ryhmä $(\mathbb{Z}, +)$, eli kokonaisluvut varustettu tavallisella yhteenlaskulla. Valitaan myös aliryhmät $2\mathbb{Z} = \{n \mid n = 2k, k \in \mathbb{Z}\}$ ja $3\mathbb{Z} = \{n \mid n = 3k, k \in \mathbb{Z}\}$. Aliryhmien yhdiste on nyt $2\mathbb{Z} \cup 3\mathbb{Z} = \{n \mid n = 2k \text{ tai } n = 3k, k \in \mathbb{Z}\}$. Nyt selvästi $2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ ja $3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, mutta $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$, koska 5 ei ole jaollinen kahdella eikä kolmella.

    Aliryhmien yhdiste ei siis ole vakaa yhteenlaskun suhteen, joten se ei ole aliryhmä.

21. Anna riittävä ja välttämätön ehto sille milloin kahden aliryhmän yhdiste on aliryhmä.

    **Ratkaisuehdotus:** Osoitetaan, että kahden aliryhmän yhdiste on aliryhmä täsmälleen silloin, kun toinen aliryhmistä sisältyy toiseen.

    Olkoot $A$ ja $B$ ryhmän $G$ aliryhmiä.

    Oletetaan ensin, että $A \subset B$ tai $B \subset A$. Jos $A \subset B$, niin $A \cup B = B$. Siis yhdiste on aliryhmä. Jos taas $B \subset A$, niin $A \cup B = A$ ja yhdiste on aliryhmä. Siten molemmissa tapauksissa $A \cup B$ on ryhmän $G$ aliryhmä.

    Oletetaan sitten, että $A \cup B$ on ryhmän $G$ aliryhmä. Osoitetaan, että $A \subset B$ tai $B \subset A$. Oletetaan vastoin väitettä, että $A$ ei ole $B$:n osajoukko ja $B$ ei ole $A$:n osajoukko.

    Oletetaan, että $x \in A \setminus B$ ja $y \in B \setminus A$. Näin voidaan tehdä, sillä vastaoletuksen mukaan joukot $A \setminus B$ ja $B \setminus A$ ovat epätyhjiä. Koska $x, y \in A \cup B$ ja yhdiste $A \cup B$ on aliryhmä, pätee $xy \in A \cup B$. Jos nyt $xy \in A$, niin $y = x^{-1}(xy) \in A$. Tämä on kuitenkin ristiriita. Jos taas $xy \in B$, niin $x = (xy)y^{-1} \in B$, mikä on myöskin ristiriita. Koska joka tapauksessa päädytään ristiriitaan, väite on todistettu.