Algebralliset rakenteet I
Helsingin yliopisto, matematiikan ja tilastotieteen laitos
Kevät 2017
Harjoitus 5 - Ratkaisuehdotuksia tähdettömiin tehtäviin

Tehtäväsarja I

1. (Rikkinäinen matkamittari.) Kuten aiempien harjoitusten tehtävässä tarkastellaan matkamittaria, jossa on neljä kiekkoa. Tällä kertaa matkamittari on rikki ja vaikka joku kiekko siirtyisikin yhdeksästä nollaan, se ei vaikuta seuraavaan kiekkoon mitenkään.

Tätä matkamittaria voi mallintaa seuraavasti. Olkoon M kaikkien nelikkojen (a, b, c, d) joukko, missä a, b, c ja d ovat joukon $\mathbb{Z}_{10}$ alkioita. Laskutoimitus määritellään nyt koordinaateittain, eli

$$(a_1, b_1, c_1, d_1) \oplus (a_2, b_2, c_2, d_2) = (a_1 +_{10} a_2, b_1 +_{10} b_2, c_1 +_{10} c_2, d_1 +_{10} d_2),$$

missä $+_{10}$ on ryhmän $\mathbb{Z}_{10}$ tavallinen laskutoimitus (plus-lasku jäännösluokilla). Osoita että $(M, \oplus)$ on vaihdannainen ryhmä.

Ratkaisuehdotus:

Huomataan, että joukko $M = \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_{10}$. Koska $(\mathbb{Z}_{10}, +_{10})$ on ryhmä, ja laskutoimitus joukossa M on määritelty koordinaateittain (eli komponenttain), $(M, \oplus)$ on ryhmä. Tarkastellaan vielä vaihdannaisuutta. Oletetaan, että $a, b \in M$, ja merkitään $a = (a_1, a_2, a_3, a_4)$ ja $b = (b_1, b_2, b_3, b_4)$. Tiedetään myös, että $(\mathbb{Z}_{10}, +_{10})$ on vaihdannainen, joten kaikille $x, y \in \mathbb{Z}_{10}$ pätee $x +_{10} y = y +_{10} x$. Nyt saadaan siis

$$a \oplus b = (a_1, a_2, a_3, a_4) \oplus (b_1, b_2, b_3, b_4) = (a_1 +_{10} b_1, a_2 +_{10} b_2, a_3 +_{10} b_3, a_4 +_{10} b_4) =$$

$$(b_1 +_{10} a_1, b_2 +_{10} a_2, b_3 +_{10} a_3, b_4 +_{10} a_4) = (b_1, b_2, b_3, b_4) \oplus (a_1, a_2, a_3, a_4) = b \oplus a.$$

Ryhmä $(M, \oplus)$ on siis vaihdannainen.

2. (Virheellinen allekkainlasku.) Ylermi on 10 v. ja opiskelee koulussa allekkainlaskua. Hän unohtaa aina kirjoittaa luvut muistiin. Esimerkiksi hän laskee $671 + 297$ allekkain näin:

$$\begin{array}{rr} & 671 \\ + & 297 \\ \hline & 868 \end{array}$$

Laskiessaan 7+9 hän merkitsi 6 viivan alle, mutta unohti kirjoittaa luvun 1 muistiin, joten sai vastaukseksi 868 oikean 968 sijaan. Osoita että näin määritelty laskutoimitus määrittelee kuitenkin luonnollisten lukujen joukossa $\mathbb{N} = \{0, 1, 2, \dots\}$ vaihdannaisen ryhmän.

Osoita, että $H = \{0, \dots, 9999\} \subset \mathbb{N}$ on aliryhmä, joka on isomorfinen edellisen tehtävän ryhmän kanssa. Sanallinen selitys riittää.

Ratkaisuehdotus:

Voidaan merkitä luonnollisten lukujen joukko seuraavalla tavalla

$$\{a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10^1 + a_0 \cdot 10^0 | a_0, ..., a_n \in \mathbb{Z}_{10}\}.$$

Nyt voidaan määrittää annettu laskutoimitus seuraavalla kaavalla (merkitään sitä symbolilla $+_v$):

$$(a_n \cdot 10^n + ... + a_0 \cdot 10^0) +_v (b_n \cdot 10^n + ... + b_0 \cdot 10^0) = (a_n +_{10} b_n) \cdot 10^n + ... + (a_0 +_{10} b_0) \cdot 10^0.$$

Koska $a_n +_{10} b_n \in \mathbb{Z}_{10}$ laskutoimitus on suljettu luonnollisten lukujen yli. Joukossa on myös neutraali alkio, 0, sillä kaikille alkioille pätee $(a_n \cdot 10^n + ... + a_0) +_v (0 \cdot 10^n + ... + 0) = (a_n \cdot 10^n + ... + a_0)$. Samoin löydämme kaikille alkioille käänteisalkio ($-a_n$ merkitsee täällä alkion a_n käänteisalkio ryhmässä $\mathbb{Z}_{10}$),

$$(a_n \cdot 10^n + ... + a_0) +_v ((-a_n) \cdot 10^n + ... + (-a_0)) = 0 \cdot 10^n + ... + 0 = 0.$$

Laskutoimitus on myös liitännäinen. Oletetaan, että $a, b, c \in \mathbb{N}$. Nyt

$$(a +_v b) +_v c = ((a_n +_{10} b_n) \cdot 10^n + ... + a_0 +_{10} b_0) +_v c =$$

$$((a_n +_{10} b_n +_{10} c_n) \cdot 10^n + ... + a_0 +_{10} b_0 +_{10} c_0 =$$

$$a +_v ((b_n +_{10} c_n) \cdot 10^n + ... + b_0 +_{10} c_0) = a +_v (b +_v c).$$

Tarkistetaan vielä vaihdannaisuutta. Oletetaan, että $a, b \in \mathbb{N}$ ja $a = a_b \cdot 10^n + ... + a_0$, $b = b_n \cdot 10^n + ... + b_0$. Muistetaan myös, että $(\mathbb{Z}_{10}, +_{10})$ on vaihdannainen. Nyt

$$a +_v b = (a_n +_{10} b_n) \cdot 10^n + ... + a_0 +_{10} b_0 = (b_n +_{10} a_n) \cdot 10^n + ... + b_0 +_{10} a_0 = b +_v a.$$

Ryhmä $(\mathbb{N}, +_v)$ on siis vaihdannainen.

3. Kuten tehtävässä 1, mutta tällä kertaa binäärinen matkamittari: B on kaikkien nelikkojen (a, b, c, d) joukko, missä a, b, c ja d ovat joukon $\mathbb{Z}_2$ alkioita. Laskutoimitus koordinaateittain:

$$(a_1, b_1, c_1, d_1) \oplus (a_2, b_2, c_2, d_2) = (a_1 +_2 a_2, b_1 +_2 b_2, c_1 +_2 c_2, d_1 +_2 d_2),$$

missä $+_2$ on ryhmän $\mathbb{Z}_2$ tavallinen laskutoimitus (plus-lasku jäännösluokilla). Kuten tehtävässä 1, $(B, \oplus)$ on ryhmä. Olkoon $X = \{1, 2, 3, 4\}$ ja $\mathcal{P}(X)$ sen potenssijoukko ja määritellään siinä laskutoimitukseksi symmertinen erotus $\triangle$ (Harjoitus 1, Tehtävä 16). Osoita että ryhmät $(\mathcal{P}(X), \triangle)$ ja $(B, \oplus)$ ovat isomorfisia.

Ratkaisuehdotus: Olkoon $f\colon B \to \mathcal{P}(X)$, $f(a_1, a_2, a_3, a_4) = \{n \in X \mid a_n = 1\}$. Eli jokaista alkiota joukossa X vastaa yksi komponentti alkiossa $(a_1, a_2, a_3, a_4) \in B$, ja kuvauksessa B:n alkio kertoo mitkä luvut ovat sen kuvassa. Esimerkiksi $f(0,0,1,0) = \{3\}$, $f(1,0,0,1) = \{1,4\}$ ja $f(0,0,0,0) = \emptyset$.

Huomataan, että kyseessä on bijektio, koska jokaiseen alkioon ryhmässä $P(X)$ kuvautuu täsmälleen yksi alkio ryhmästä B.

Tarkistetaan vielä, päteekö kaikille $a, b \in B$

$$f(a \oplus b) = f(a) \triangle f(b).$$

Olkoon $a = (a_1, a_2, a_3, a_4), b = (b_1, b_2, b_3, b_4) \in B$. Nyt

$$f((a_1, a_2, a_3, a_4) \oplus (b_1, b_2, b_3, b_4) = f(a_1 +_2 b_1, a_2 +_2 b_2, a_3 +_2 b_3, a_4 +_2 b_4) = \{n \in X \mid a_n +_2 b_n = 1\}.$$

Tutkitaan tulosta komponenttain. Luku n kuuluu kuvaan vain jos $a_n +_2 b_2 = 1$, ja $a_n +_2 b_2 = 1$ vain jos $a_n = 1$ tai $b_n = 1$, mutta ei molemmat. Eli $n \in f(a \oplus b)$ jos ja vain jos $n \in f(a)$ tai $n \in f(b)$, mutta $(n \notin f(a) \cap f(b)$, eli jos $n \in f(a) \triangle f(b)$. Siis $f(a \oplus b) = f(a) \triangle f(b)$.

Tehtäväsarja II

4. Määritä ryhmän $\mathbb{Q}^* = (\mathbb{Q} \setminus \{0\}, \cdot)$ aliryhmä $\langle 17 \rangle$.

   Ratkaisuehdotus: Kirjan lauseen 6.2(toisessa painoksessa) nojalla, ryhmän alkion virittämä aliryhmä on sen kaikkien potenssien joukko, eli $\langle g \rangle = \{g^n | n \in \mathbb{Z}\}$. Sen mukaan saadaan, että $\langle 17 \rangle = \{17^n | n \in \mathbb{Z}\}$.

5. Määritä ryhmän $\mathbb{Z}$ aliryhmät $\langle 10 \rangle$, $\langle -11 \rangle$ ja $\langle 0 \rangle$.

   Ratkaisuehdotus: Kuten yllä, käytetään tulosta, jonka mukaan ryhmän alkion virittämä aliryhmä on sen kaikkien potenssien joukko. Yhteenlaskun suhteen tämä tarkoittaa monikertojen joukkoa ja niinpä nyt saadaan

   $$\langle 10 \rangle = \{10n \mid n \in \mathbb{Z}\} = 10\mathbb{Z}.$$

   Toisaalta $\langle -10 \rangle = \{-10n \mid n \in \mathbb{Z}\}$. Nyt kuitenkin $= \{-10n \mid n \in \mathbb{Z}\} = \{10n \mid n \in \mathbb{Z}\}$. (Tämä osoitetaan tarkasti näyttämällä molemmat joukot toistensa osajoukoiksi.) Siten $\langle -10 \rangle = 10\mathbb{Z}$ eli $\langle -10 \rangle = \langle 10 \rangle$.

   Lopuksi $\langle 0 \rangle = \{0n \mid n \in \mathbb{Z}\} = \{0\}$. Neutraalialkion virittämään aliryhmään kuuluu siis pelkästään neutraalialkio itse.

6. Määritä ryhmän $\mathbb{Z}_{12}$ aliryhmät $\langle 2 \rangle$, $\langle 3 \rangle$ ja $\langle 11 \rangle$.

   Ratkaisuehdotus: Kuten edellisessä tehtävässä, $\langle 2 \rangle = \{2n \mid n \in \mathbb{Z}\}$. Nyt kuitenkin $\langle 2 \rangle$ on ryhmän $\mathbb{Z}_{12}$ aliryhmä, joten huomataan, että $6 \cdot [2]_{12} = [12]_{12} = [0]_{12}$, ja siitähän seuraa että $7 \cdot [2]_{12} = 6 \cdot [2]_{12} + [2]_{12} = [0]_{12} + [2]_{12} = [2]_{12}$. Sykli pääsi siis takaisin alkuun, ja sitä korkeimmalla kertaluvuilla alkiot vaan toistuvat. Eli

   $$\langle 2 \rangle = \{[2]_{12}, 2{\cdot}[2]_{12}, 3{\cdot}[2]_{12}, 4{\cdot}[2]_{12}, 5{\cdot}[2]_{12}, 6{\cdot}[2]_{12}\} = \{[2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}, [0]_{12}\}.$$

Samalla tavalla saadaan, että

$$\langle 3\rangle = \{[3]_{12}, [6]_{12}, [9]_{12}, [0]_{12}\},$$

ja

$$\langle 11\rangle = \{[11]_{12}, [10]_{12}, [9]_{12}, [8]_{12}, [7]_{12}, [6]_{12}, [5]_{12}, [4]_{12}, [3]_{12}, [2]_{12}, [1]_{12}, [0]_{12} = \mathbb{Z}_{12}.$$

7. Olkoon $(B, \oplus)$ kuten tehtävässä 3. Määritä aliryhmät $\langle([0]_2, [1]_2, [0]_2, [0]_2)\rangle$ ja $\langle([0]_2, [1]_2, [0]_2, [1]_2)\rangle$.

   Ratkaisuehdotus: Huomataan, että

   $$2([0]_2, [1]_2, [0]_2, [0]_2) = ([0]_2, [1]_2, [0]_2, [0]_2) \oplus ([0]_2, [1]_2, [0]_2, [0]_2) = ([0]_2, [0]_2, [0]_2, [0]_2).$$

   Koska päädyimme neutraalialkioon, aliryhmässä ei ole muuta alkioita, joten

   $$\langle([0]_2, [1]_2, [0]_2, [0]_2)\rangle = \{([0]_2, [1]_2, [0]_2, [0]_2), ([0]_2, [0]_2, [0]_2, [0]_2)\}.$$

   Samalla tavalla saadaan

   $$\langle([0]_2, [1]_2, [0]_2, [1]_2)\rangle = \{([0]_2, [1]_2, [0]_2, [1]_2), ([0]_2, [0]_2, [0]_2, [0]_2)\}.$$

Tehtäväsarja III

8.* Tuloryhmällä $(\mathbb{R}, +) \times (\mathbb{R}, +)$ on aliryhmä $H = \{(a, 2a) \mid a \in \mathbb{R}\}$. Osoita, että ryhmä $(\mathbb{R}, +)$ on isomorfinen ryhmän $(H, +)$ kanssa.

9. Tarkastellaan tason yksikköparaabelin kuvaajaa

   $$P = \{(x, y) \in \mathbb{R} \times \mathbb{R}; y = x^2\}.$$

   Keksitkö joukkoon P laskutoimituksen $*$ siten että $(\mathbb{R}, +)$ on isomorfinen ryhmän $(P, *)$ kanssa?

   Ratkaisuehdotus: Aloitetaan huomaamalla, että joukon P ehdon mukaan, sen alkiot ovat muodossa $(x, x^2), x \in \mathbb{R}$. Määritetään sitten kuvaus f. Olkoon $f\colon \mathbb{R} \to P, f(x) = (x, x^2)$. Osoitetaan että f on bijektio. Aloitetaan injektiivisyydestä. Oletetaan että $a, b \in \mathbb{R}$ ja $f(a) = f(b)$. Nyt $(a, a^2) = (b, b^2)$. Siitä seuraa, että $a = b$, eli f on injektiivinen. Osoitetaan sitten surjektiivisuus. Oletetaan, että $y \in P$. Nyt $y = (a, a^2)$ jollakin $a \in \mathbb{R}$. Nähdään, että $f(a) = (a, a^2) = y$, joten f on surjektio. Kuvaus f on siis bijektio. Jotta se olisi ryhmäisomorfismi, pitää vielä päteä kaikille $a, b \in \mathbb{R}$, että $f(a + b) = f(a) * f(b)$. Määritellään laskutoimitus $*$ siten, että

   $$(a, a^2) * (b, b^2) = f(a) * f(b) = f(a + b) = (a + b, (a + b)^2).$$

   Nyt, jos pari $(P, *)$ on ryhmä, se on isomorfinen ryhmän $(\mathbb{R}, +)$ kanssa. Osoitetaan siis vielä, että $(P, *)$ on ryhmä. Oletetaan, että $x, y \in P$, ja $x = (a, a^2), y = (b, b^2)$. Nyt $x * y = (a + b, (a + b)^2) \in P$, joten laskutoimitus on suljettu joukossa P. Oletetaan, että $(0, 0^2) \in P$ on ryhmän neutraalialkio. Olkoon $x = (a, a^2) \in P$. Nyt

   $$(0, 0) * (a, a^2) = (0 + a, (0 + a)^2) = (a, a^2) = (a + 0, (a + 0)^2) = (a, a^2) * (0, 0).$$

Eli $(0,0)$ on ryhmän $(P,*)$ neutraalialkio.

Olkoon $x=(a,a^2)\in P$. Oletetaan, että $x^{-1}=(-a,(-a)^2)\in P$. Nyt

$$x*x^{-1}=((a-a),(a-a)^2)=(0,0)=((-a+a),(-a+a)^2)=x^{-1}*x.$$

Kaikilla $x\in P$ on siis käänteisalkio.

Lopuksi tarkistetaan vielä liitännäisyys. Olkoon $x,y,z\in P$, ja $x=(a,a^2),y=(b,b^2),z=(c,c^2)$. Nyt

$$x*(y*z)=(a+(b+c),(a+(b+c))^2)=((a+b)+c,((a+b)+c)^2)=(x*y)*z.$$

Laskutoimitus on siis liitännäinen, ja siten $(P,*)$ on ryhmä, joka on isomorfinen ryhmän $(\mathbb{R},+)$ kanssa.

Tehtäväsarja IV

10. Tutkitaan matriisiryhmän $GL_2(\mathbb{R})$ (kaikkien kääntyvien 2×2 matriisien muodostama ryhmä matriisikertolaskun suhteen) alkiota $A=\left[\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right]$. Määritä aliryhmä $\langle A\rangle$. Mikä aliryhmän alkioista on A^5? Entä A^{-2}?

    Ratkaisuehdotus: Lasketaan matriisin A potensseja kunnes saadaan neutraalilkio. Nyt

$$\begin{aligned}A^2&=\begin{bmatrix}0&1\\-1&0\end{bmatrix}\begin{bmatrix}0&1\\-1&0\end{bmatrix}=\begin{bmatrix}-1&0\\0&-1\end{bmatrix}\\A^3=A^2A&=\begin{bmatrix}-1&0\\0&-1\end{bmatrix}\begin{bmatrix}0&1\\-1&0\end{bmatrix}=\begin{bmatrix}0&-1\\1&0\end{bmatrix}\\A^4=A^3A&=\begin{bmatrix}0&-1\\1&0\end{bmatrix}\begin{bmatrix}0&1\\-1&0\end{bmatrix}=\begin{bmatrix}1&0\\0&1\end{bmatrix}.\end{aligned}$$

    Näin ollen $A^4=I$, joka on ryhmän $GL_2(\mathbb{R})$ neutraalialkio. Käytetään jälleen lemmaa 6.6, jonka mukaan ryhmä $\langle A\rangle$ on nyt muotoa

$$\langle A\rangle=\{I,A,A^2,A^3\}.$$

    Ryhmä $\langle A\rangle$ on siis

$$\langle A\rangle=\left\{\begin{bmatrix}1&0\\0&1\end{bmatrix},\begin{bmatrix}0&1\\-1&0\end{bmatrix},\begin{bmatrix}-1&0\\0&-1\end{bmatrix},\begin{bmatrix}0&-1\\1&0\end{bmatrix}\right\}.$$

    Lasketaan vielä ryhmän alkiot A^5 ja A^{-2}.

    Huomataan, että $A^5=A^4A$. Edellisten laskujen perusteella $A^4=I$, joten $A^5=IA=A$.

    Määritetään sitten potenssi A^{-2}. Aloitetaan määrittämällä käänteisalkio (eli käänteismatriisi) A^{-1}. Koska $A^4=I$, niin $A^3A=I$ ja $AA^3=I$. Siten $A^{-1}=A$.

(Käänteismatriisin voi toki määrittää myös lineaarialgebran tietojen perusteella.) Näin ollen

$$A^{-2} = (A^{-1})^2 = A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Edellinen antaa viitteitä siitä, että ryhmästä $\langle A \rangle$ löytyvät kaikki A:n potenssit, vaikka alkioita onkin vain neljä. Eri potenssit vain sattuvat olemaan keskenään samoja.

Tehtäväsarja V

11. Määritä seuraavien ryhmän S_6 alkioiden kertaluvut:

$$(14), \quad (253), \quad (14)(253).$$

Ratkaisuehdotus: Määritelmän mukaan alkion kertaluku on sen virittämän aliryhmän kertaluku; lauseen 6.8 nojalla äärellisen ryhmän tapauksessa tämä on pienin niistä positiivisista luvuista, joiden suhteen alkion potenssi on ryhmän neutraalialkio. Toisin sanoen ryhmän alkion g kertaluku $o(g)$ on pienin sellainen $n \in \mathbb{N}$, jolla $g^n = e$ ja toisaalta $\langle g \rangle = \{g, \ldots, g^n\}$.

Ratkaistaan sitten itse tehtävä. Huomataan, että $(14)^2 = (1)$, joten $o((14)) = 2$.

Nähdään, että $(253)^2 = (235)$ ja $(253)^3 = (253)(253)^2 = (253)(235) = (1)$, joten $o((253)) = 3$.

Määritetään sitten alkion $(14)(253)$ kertaluku. Syklit (14) ja (253) ovat erilliset, joten niiden kertomisjärjestyksen saa vaihtaa. Näin ollen potensseja on helppo laskea käyttäen edellisiä tietoja:

$$\begin{aligned} ((14)(253))^2 &= (235) \\ ((14)(253))^3 &= (14) \\ ((14)(253))^4 &= (253) \\ ((14)(253))^5 &= (14)(235) \\ ((14)(253))^6 &= (1). \end{aligned}$$

Nyt tiedämme, että $o((14)(253)) = 6$.

Jo tässä vaiheessa kannattaa huomata, että $o((14)(253)) = o((14)) \cdot o((253))$. Mieti, osaisitko selittää tämän!

12. Tutkitaan korttipakkaa, jossa on kymmenen korttia. Sekoitetaan kortteja niin, että otetaan pakan päältä neljän kortin pino ja laitetaan se pakan alle. Kuinka monen sekoituskerran jälkeen ollaan takaisin lähtötilanteessa?

Vihje: Edellisen tehtävän havainnoista on hyötyä.

Ratkaisuehdotus: Aloitetaan selvittämällä sekoitusta vastaavan permutaation sykliesitys. Numeroidaan korttipakan alkiot pohjalta lukien luvuilla $1, \ldots, 10$. Kun

päällimmäinen kortti asetetaan pohjimmaiseksi, myös kaikkien muiden korttien paikat muuttuvat, ja tämä yksinkertainen sekoitus on kymmenen alkion permutaatio

$$\tau = (10, 1, 2, 3, 4, 5, 6, 7, 8, 9).$$

Neljän päällimmäisen kortin asettaminen pakan pohjalle voitaisiin yhtä hyvin tehdä kortti kerrallaan, ja niinpä tätä sekoitusta vastaa permutaatio

$$\rho = \tau^4 = (10, 4, 8, 2, 6)(9, 3, 7, 1, 5).$$

Permutaation kertaluku kertoo, kuinka monen kerran jälkeen ollaan lähtötilanteessa. Voidaan esimerkiksi havaita ρ:n olevan kahden erillisen 5-syklin tulo, joten sen itsensäkin kertaluku on 5. Voidaan myös laskea ρ:n potensseja ja huomata, että

$$\begin{aligned} \rho^2 &\neq (1), \\ \rho^3 &\neq (1), \\ \rho^4 &\neq (1), \end{aligned}$$

mutta

$$\rho^5 = ((10, 4, 8, 2, 6)(9, 3, 7, 1, 5))^5 = (10, 4, 8, 2, 6)^5(9, 3, 7, 1, 5)^5 = (1)(1) = (1).$$

Siis $o(\rho) = 5$. (Huomaa, että erillisten syklien kertomisjärjestyksellä ei ole merkitystä!)

Siten lähtötilanteessa ollaan viiden sekoituskerran jälkeen.

13. Täydessä korttipakassa on 52 korttia joten sen kaikki mahdolliset permutaatiot (järjestykset/sekoitukset) voidaan mallintaa ryhmällä S_{52}. Merkitään luvun x jakojäännöstä luvulla y jaettaessa $x\%y$. Esimerkiksi $2\%3 = 2$ ja $4\%3 = 1$. Korttipakan nosto on permutaatio muotoa

$$\begin{pmatrix} 1 & 2 & \cdots & 52 \\ (1+k)\%52 & (2+k)\%52 & \cdots & (52+k)\%52 \end{pmatrix},$$

missä k on joku luku joukossa $\{0, \ldots, 51\}$. Merkitään tätä permutaatiota σ_k. Osoita, että $\sigma_1^2 = \sigma_2$. Osoita edelleen että $\sigma_k\sigma_1 = \sigma_{k+1}$, kun $k < 51$. Huomataan että σ_1 on sykli $(1, 2, 3, 4, \ldots, 52)$. Joten kaikkien nostojen joukko on itse asiassa tämän syklin virittämä aliryhmä: $\langle(1, 2, 3, 4, \ldots, 52)\rangle$.

Selitä miten tästä seuraa se, että jos pakan nostaa monta kertaa peräkkäin, sen saa alkuperäiseen järjestykseen nostamalla se vain kerran (oikeasta paikasta); eli yksi nosto riittää kumoamaan monta nostoa.

Ratkaisuehdotus: (Huomautus: tässä tehtävässä, sanotaan että $52\%52 = 52$, niin että kaavamme toimii.)

Permutaatio σ_1 on siis

$$\begin{pmatrix} 1 & 2 & \cdots & 51 & 52 \\ 2 & 3 & \cdots & 52 & 1 \end{pmatrix},$$

eli permutaation $(1, 2, ..., 52)$. Nyt

$$\sigma_1^2 = (1, 2, ..., 52)(1, 2, ..., 52) = (1, 3, 5, ..., 51)(2, 4, ..., 52) =$$

$$\begin{pmatrix} 1 & 2 & \cdots & 52 \\ 3 & 4 & \cdots & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & 52 \\ (1+2)\%52 & (2+2)\%52 & \cdots & (52+2)\%52 \end{pmatrix} = \sigma_2.$$

Tarkistetaan sitten, onko $\sigma_k\sigma_1 = \sigma_{k+1}$.

$$\sigma_k\sigma_1 = \begin{pmatrix} 1 & 2 & \cdots & 52 \\ (1+k)\%52 & (2+k)\%52 & \cdots & (52+k)\%52 \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & 52 \\ 2 & 3 & \cdots & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 2 & \cdots & 52 \\ (2+k)\%52 & (3+k)\%52 & \cdots & (1+k)\%52 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 2 & \cdots & 52 \\ (1+(k+1))\%52 & (2+(k+1))\%52 & \cdots & (52+(k+1))\%52 \end{pmatrix} = \sigma_{k+1}.$$

Jokainen nosto on siis permutaatio aliryhmässä $\langle(1, 2, 3, 4, \ldots, 52)\rangle$. Koska kyseessä on aliryhmä, useamman noston kombinaatio on myös permutaatio samassa joukossa, joten sitä vastaa jokin tietty nosto. Aliryhmän perusteella kaikilla permutaatioilla on jokin käänteisalkio, joten voidaan aina löytää pakan järjestystä vastaavan permutaation käänteisalkio. Jos sitten tehdään se nosto, joka vastaa juuri sitä käänteisalkiota, pääsemme takaisin alkuperäiseen järjestykseen.

Tehtäväsarja VI

14. Ryhmällä $\mathbb{Z}_{16}$ on aliryhmä $H = \{[0]_{16}, [4]_{16}, [8]_{16}, [12]_{16}\}$. Onko olemassa alkiota, joka virittää aliryhmän H? Toisin sanoen, onko H syklinen?

    Ratkaisuehdotus: Osoitetaan, että H on alkion $[4]_{16}$ virittämä aliryhmä. Ensinnäkin $[4]_{16} \in H$. Lisäksi huomataan, että

    $$\begin{aligned} 1 \cdot [4]_{16} &= [4]_{16} \neq [0]_{16} \\ 2 \cdot [4]_{16} &= [4]_{16} + [4]_{16} = [2 \cdot 4]_{16} = [8]_{16} \neq [0]_{16} \\ 3 \cdot [4]_{16} &= [3 \cdot 4]_{16} = [12]_{16} \neq [0]_{16} \\ 4 \cdot [4]_{16} &= [4 \cdot 4]_{16} = [16]_{16} = [0]_{16}. \end{aligned}$$

    Koska saatiin tulokseksi neutraalialkio $[0]_{16}$, on löydetty kaikki ryhmän $\langle[4]_{16}\rangle$ kaikki alkiot. Näin ollen $\langle[4]_{16}\rangle = \{[0]_{16}, [4]_{16}, [8]_{16}, [12]_{16}\} = H$. Siis H on syklinen.

15. Onko ryhmän S_5 aliryhmä $\{(1), (25), (34), (25)(34)\}$ syklinen?

    Ratkaisuehdotus: Aliryhmä sisältää vain kertalukua 1 ja 2 olevia alkioita: $(25)^2 = (1)$, $(34)^2 = (1)$ $((25)(34))^2 = (1)$. Siksi sen jokainen alkio virittää korkeintaan kahden alkion aliryhmän, eikä siten voi olla tarkasteltavan aliryhmän virittäjä. Niinpä syklisyys ei tule kysymykseen.

Tehtäväsarja VII

16. Määritellään kokonaislukujen joukossa relaatio $\sim$ ehdolla

$$a \sim b, \quad \text{jos} \quad -a+b \in 7\mathbb{Z}.$$

Osoita, että $\sim$ on ekvivalenssirelaatio. Mikä tuttu relaatio on itse asiassa kyseessä?

Ratkaisuehdotus: Oletetaan, että $a, b, c \in \mathbb{Z}$. Nyt

$$-a+a = 0 = 7 \cdot 0 \in 7\mathbb{Z}.$$

Näin ollen $a \sim a$, joten refleksiivisyys toteutuu.

Oletetaan seuraavaksi, että $a \sim b$. Tällöin $-a+b \in 7\mathbb{Z}$, eli

$$-a+b = 7k, \text{ jollain } k \in \mathbb{Z}.$$

Kerrotaan yhtälö puolittain -1:llä ja saadaan

$$-(-a+b) = -7k,$$

ja edelleen

$$-b+a = 7(-k).$$

Tästä seuraa, että $-b+a \in 7\mathbb{Z}$, eli että $b \sim a$. Näin ollen $\sim$ on symmetrinen relaatio.

Oletetaan, että $a \sim b$ ja $b \sim c$. Nyt

$$-a+b \in 7\mathbb{Z} \quad \text{ja} \quad -b+c \in 7\mathbb{Z}.$$

Tällöin

$$-a+b = 7k \quad \text{ja} \quad -b+c = 7l, \text{ joillakin } k, l \in \mathbb{Z}.$$

Ensimmäisestä yhtälöstä saadaan $b = a+7k$, jollain $k \in \mathbb{Z}$. Sijoitetaan tämä toiseen yhtälöön ja saadaan

$$-(a+7k)+c = 7l$$

eli

$$-a+c = 7l-7k = 7(l-k).$$

Koska $l-k \in \mathbb{Z}$, niin $-a+c \in 7\mathbb{Z}$, joten $a \sim c$ ja transitiivisuus toteutuu. On siis osoitettu, että $\sim$ on ekvivalenssirelaatio.

Huomataan, että kyseessä on kongruenssirelaatio: kokonaisluvuilla a ja b pätee $a \sim b$, jos ja vain jos $a \equiv b \pmod 7$.

17. Jatkoa edelliseen tehtävään. Määritä luvun 11 ekvivalenssiluokka. Missä yhteydessä olet aiemmin törmännyt tähän joukkoon?

Ratkaisuehdotus: Luvun 11 ekvivalenssiluokkaan kuuluvat kaikki luvut a, joille pätee

$$-11+a \in 7\mathbb{Z}$$

eli

$$-11 + a = 7k, \text{ jollain } k \in \mathbb{Z}.$$

Luokka $[11]_\sim$ saadaan siis muotoon

$$\begin{aligned}[11]_\sim &= \{a \in \mathbb{Z} \mid -11 + a = 7k \text{ jollakin } k \in \mathbb{Z}\} = \{a \in \mathbb{Z} \mid a = 11 + 7k \text{ jollakin } k \in \mathbb{Z}\} \\ &= \{11 + 7k \mid k \in \mathbb{Z}\} = \{\dots, -3, 4, 11, 18, 25, \dots\}.\end{aligned}$$

Luvun 11 ekvivalenssiluokka on siis sama kuin jäännösluokka $[11]_7$.

Tehtäväsarja VIII

18.* Olkoon $f\colon G \to H$ ryhmäisomorfismi. Osoita, että jos G on vaihdannainen ryhmä, myös H on vaihdannainen ryhmä.

19. Onko jäännösluokkaryhmä $\mathbb{Z}_6$ isomorfinen symmetrisen ryhmän S_3 kanssa?

Ratkaisuehdotus: Olkoot $x, y \in \mathbb{Z}_n$, jolloin $x = [a]_n$ ja $y = [b]_n$ joillain $a, b \in \mathbb{Z}$. Nyt kokonaislukujen yhteenlaskun vaihdannaisuudesta seuraa, että

$$x + y = [a]_n + [b]_n = [a + b]_n = [b + a]_n = [b]_n + [a]_n = y + x,$$

joten $\mathbb{Z}_n$ on vaihdannainen.

Edellisessä tehtävässä osoitettiin, että vaihdannaisen ryhmän kanssa isomorfinen ryhmä on vaihdannainen. Siis jos pätisi $\mathbb{Z}_6 \cong S_3$, niin S_3 olisi vaihdannainen. Mutta tunnetusti S_3 *ei* ole vaihdannainen, joten $\mathbb{Z}_6 \ncong S_3$.

Ylimääräinen tehtävä

20. Ovatko ryhmät $(\mathbb{R}^*, \cdot)$ ja $(\mathbb{C}^*, \cdot)$ isomorfiset?

Ratkaisuehdotus: Tehdään vastaoletus ja valitaan jokin isomorfismi $f : \mathbb{R}^* \to \mathbb{C}^*$.

Tapa 0: $\mathbb{C}^*$:llä on neljän alkion kokoinen aliryhmä $\{-1, 1, i, -i\}$, mutta $\mathbb{R}^*$:llä ei; sen ainoat äärelliset aliryhmät ovat $\{1\}$ ja $\{-1, 1\}$.

Tapa 1: Jos $a \in \mathbb{C}$, yhtälöllä $x^2 = a$ on aina ratkaisu kompleksilukujen joukossa. Erityisesti löytyy sellainen $x \in \mathbb{C}^*$, jolla $x^2 = f(-1)$. Koska f on bijektio, sillä on olemassa käänteiskuvaus $f^{-1} : \mathbb{C}^* \to \mathbb{R}^*$. Sen avulla edellisestä yhtälöstä saadaan $f^{-1}(x^2) = -1$. Kirjassa on osoitettu, että isomorfismin käänteiskuvaus on sekin isomorfismi, joten nyt $-1 = (f^{-1}(x))^2$. Tämä on kuitenkin mahdotonta, sillä $f^{-1}(x) \in \mathbb{R}$. Siis vastaoletus johti ristiriitaan, eivätkä ryhmät voi olla isomorfisia.

Tapa 2: Koska f on bijektio, on olemassa jokin reaaliluku a, jolla $f(a) = i$, missä i on imaginaariyksikkö. Mutta koska $i^5 = i$, täytyy olla $f(a)^5 = f(a)$. Kuvaus f on isomorfismi, joten edellisestä saadaan $f(a^5) = f(a)$ ja edelleen $a^5 = a$. Tämä on mahdollista vain, jos $a = 0$ tai $a = \pm 1$. Joka tapauksessa $a = a^3$, mutta

$$f(a) = i \neq i^3 = f(a)^3 = f(a^3),$$

mikä on ristiriita. Niinpä vastaoletuksen mukaista kuvausta ei voi olla olemassa, eivätkä ryhmät siksi ole isomorfiset.

Lisätieto: ryhmät $(\mathbb{R}^2, +)$ ja $(\mathbb{R}, +)$ *ovat* isomorfiset. Tämän todistaminen menee kuitenkin tämän kurssin ulkopuolelle ja siihen tarvitaan valinta-aksioomaa.