Approbatur 3, demo 5, ratkaisut

5.1. Tehtävänä on luetella kaikki joukon S_4 alkiot eli neljän alkion permutaatiot. Tämä tarkoittaa kaikkia eri tapoja kuvata joukko $\{1,2,3,4\}$ bijektiivisesti itselleen. Käytetään lyhennysmerkintää: merkitään permutaatiota vektorilla (n_1,n_2,n_3,n_4), joka tarkoittaa, että 1 kuvautuu n_1:ksi, 2 n_2:ksi jne. Näitähän on $4! = 1\cdot 2\cdot 3\cdot 4 = 24$ kappaletta. Ja luetellaan:

$$\begin{gathered}(1,2,3,4),(1,2,4,3),(1,3,2,4),(1,3,4,2),(1,4,2,3),(1,4,3,2)\\(2,1,3,4),(2,1,4,3),(2,3,1,4),(2,3,4,1),(2,4,1,3),(2,4,3,1)\\(3,1,2,4),(3,1,4,2),(3,2,1,4),(3,2,4,1),(3,4,1,2),(3,4,2,1)\\(4,1,2,3),(4,1,3,2),(4,2,1,3),(4.2,3,1),(4,3,1,2),(4,3,2,1)\,,\end{gathered}$$

eli 24 tuli kuten pitikin.

5.2. Olkoot

$$\sigma = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} \text{ ja } \rho = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}.$$

Tehtävänä on etsiä permutaatiot $x,y,z \in S(4)$ siten, että yhtälöt

$$\sigma x = \rho, \quad y\rho = \sigma \quad \text{ja} \quad \rho z\sigma = id$$

pätevät.

Etsitään ensin x siten, että yhtälö $\sigma x = \rho$ toteutuu. Tähän on useita eri tapoja. Hoidetaan homma tarkastelemalla eri alkioiden kuvautumista. Aloitetaan siitä, että koska $x \in S(4)$, x on muotoa

$$x = \begin{pmatrix}1&2&3&4\\n_1&n_2&n_3&n_4\end{pmatrix}.$$

Muistetaan, että permutaatioryhmän laskutoimitus on kuvausten yhdistäminen ja että kuvauksia ketjutetaan oikealta vasemmalle eli kaavalla

$$(\sigma_1\sigma_2)(n) = \sigma_1(\sigma_2(n))\,,$$

missä $\sigma_1,\sigma_2 \in S(4)$ ja $n \in \{1,2,3,4\}$.

Aloitetaan alkiosta 1. Koska ρ kuvaa ykkösen kolmoselle, pitäisi vaatimuken $\rho = \sigma x$ nojalla myös σx:n kuvata. Koska σ kuvaa kakkosen kolmoselle, täytyy tällöin x:n kuvata ykkönen kakkoselle, jotta yhdistetylle kuvaukselle σx pätisi $1 \mapsto 2 \mapsto 3$. Siispä $n_1 = 2$ ja

$$x = \begin{pmatrix}1&2&3&4\\2&n_2&n_3&n_4\end{pmatrix}.$$

Seuraavaksi tarkastellaan alkion 2 kuvautumista. Koska $\rho(2) = 4$ niin on oltava $\sigma(x(2)) = 4$. Tällöin, koska $\sigma(1) = 4$, on oltava $x(2) = n_2 = 1$, ja saadaan

$$x = \begin{pmatrix}1&2&3&4\\2&1&n_3&n_4\end{pmatrix}.$$

Määritetään sitten n_3. Koska $\rho(3) = 1$ ja $\sigma(4) = 1$, on oltava $x(3) = 4$. Siispä $n_3 = 4$ ja tähän mennessä on saatu esitys

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & n_4 \end{pmatrix}. \tag{1}$$

Viimeisen alkion eli n_4:n voi arvata, sillä koska x on bijektio, on esityksen (1) alarivillekin tultava luvut $1, 2, 3$ ja 4 – kukin täsmälleen kerran. Siispä $n_4 = 3$. Tämä voidaan myös tarkistaa. Jos $x(4) = 3$, niin

$$\sigma(x(4)) = \sigma(3) = 2$$

eli permutaatio σx kuvaa nelosen kakkoselle. Näin tekee myös ρ eli yhtälö $\sigma x = \rho$ toteutuu, niin kuin oli tarkoituskin. Lopullinen vastaus on siis

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Seuraavaksi etsitään permutaatio y siten, että yhtälö $y\rho = \sigma$ toteutuu. Tämän voi tehdä vaikkapa samalla tavalla kuin yllä tarkastelemalla eri alkioiden kuvautumsita. Tulos on

$$y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Vielä on määritettävänä permutaatio z siten, että yhtälö $\rho z \sigma = id$ toteutuu. Koska $z \in S(4)$ on joillekin $n_1, n_2, n_3, n_4 \in \{1, 2, 3, 4\}$ voimassa

$$z = \begin{pmatrix} 1 & 2 & 3 & 4 \\ n_1 & n_2 & n_3 & n_4 \end{pmatrix}.$$

Identtinen kuvaus kuvaa jokaisen alkion itselleen. Tarkastellaan taas eri alkoiden ”matkaa” näissä permutaatioissa.

Aloitetaan alkoista 1. Koska $\sigma(1) = 4$ ja $\rho(3) = 1$, on oltava $z(4) = 3$, jotta z täydentäisi – havainnollisesti ilmaistuna – sillan ykkösestä permutaatioiden σ ja ρ kautta takaisin ykköseen. Sispä $n_4 = 3$ ja täydennetään z:n esitystä

$$z = \begin{pmatrix} 1 & 2 & 3 & 4 \\ n_1 & n_2 & n_3 & 3 \end{pmatrix}.$$

Sitten alkio 2. Koska $\sigma(2) = 3$ ja $\rho(4) = 2$, on oltava $z(3) = 4$. Tämä tarkoittaa, että $n_3 = 4$, ja saadaan

$$z = \begin{pmatrix} 1 & 2 & 3 & 4 \\ n_1 & n_2 & 4 & 3 \end{pmatrix}.$$

Seuraavaksi alkio 3. Koska $\sigma(3) = 2$ ja $\rho(1) = 3$, on oltava $z(2) = n_2 = 1$ eli

$$z = \begin{pmatrix} 1 & 2 & 3 & 4 \\ n_1 & 1 & 4 & 3 \end{pmatrix}.$$

Tästä voidaan taas arvata suoraan, koska permutaatiot ovat bijektioita, että $n_1 = 2$. Voi sen tarkistaakin yhtälöön $\rho z \sigma = id$ verraten:

$$(\rho z \sigma)(4) = (\rho z)(\sigma(4)) = (\rho z)(1) = \rho(z(1)) = \rho(n_1) = \rho(2) = 4$$

eli valinta $n_1 = 2$ toimii. Lopulta siis

$$z = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

5.3. Tässä kysyttiin ensin, montako alkiota ryhmästä S_5 kuvaavat ykkösen itselleen. Ryhmässä S_5 on $5! = 120$ alkiota, joten kokeilemaan ei kannata lähteä. Edetään näin: Jos $\sigma(1) = 1$, niin kakkosella on enää 4 vaihtoehtoa, mihin kuvautua. Vastaavasti $\sigma(2)$:n kiinnityksen jälkeen kolmosella on enää kolme vaihtoehtoa, mihin kuvautua, ja niin edelleen, joten kaiken kaikkiaan erilaisia kuvauksia on

$$1 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 4! = 24\,.$$

Seuraava kysymys oli, moniko joukon S_5 alkioista kuvaa ykkösen ja kolmosen toisikseen. Tällaisille permutaatioille σ siis pätee $\sigma(1) = 3$ ja $\sigma(3) = 1$. Tämä tarkoittaa, että joukossa, josta $\sigma(2)$ valitaan, on enää kolme alkiota (alkiot 2, 4 ja 5); joukossa, josta $\sigma(4)$ valitaan, on enää 2 alkiota, ja niin edelleen. Tällaisia kuvauksia on siis kaiken kaikkiaan $3 \cdot 2 \cdot 1 = 3! = 6$ kappaletta.

5.4. Kysyttiin esimerkkiä ryhmän S_4 permutaatioista σ ja ρ siten, että $\rho\sigma \neq \sigma\rho$. Muistetaan, että kuvaukset ovat samat täsmälleen silloin, kun ne kuvaavat jokaisen määrittelyjoukkonsa (tässä $\{1, 2, 3, 4\}$) pisteen samoin. Riittää siis löytää $\sigma, \rho \in S_4$ ja jokin luku $n \in \{1, 2, 3, 4\}$ siten, että

$$\sigma\rho(n) \neq \rho\sigma(n)\,.$$

Huomataan, että tämän ehdon toteuttavat (esimerkiksi) muuttujan arvolla $n = 1$ permutaatiot

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \text{ ja } \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

sillä näille pätee

$$\sigma\rho(1) = 3 \neq 4 = \rho\sigma(1)\,.$$

Sitten kysyttin, onko olemassa permutaatioita $\sigma, \rho \in S_4$ siten, että $\sigma, \rho \neq id$ ja $\sigma\rho = \rho\sigma$. Vastaus on, että kyllä näitä löytyy. Esimerkiksi tehtävän 5.2 permutaatiot σ ja ρ kelpaavat, sillä kumpikaan ei selvästi ole identtinen kuvaus, ja toisaalta

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

ja

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

eli samat permutaatiot saadaan.

5.5. Määritellään, kuten tehtävänasettelussa, kaikille $[k] \in \mathbb{Z}_{24}$ $f([k]) = [4k+3]$ ja $g([k]) = [7k]$. Näissä siis hakasulut viittaavat luokkiin joukossa $\mathbb{Z}_{24}$. Kysymys kuului, ovatko f ja g joukon $\mathbb{Z}_{24}$ permutaatioita. Permutaation määritelmän mukaisesti kysymyksen voi muotoilla seuraavasti: ovatko f ja g bijektioita joukolta $\mathbb{Z}_{24}$ itselleen?

Ainakaan f ei ole bijektio, koska se ei ole injektio. Nimittäin esimerkiksi

$$f([6]) = [4 \cdot 6 + 3] = [24 + 3] = [0 + 3] = [0]$$

ja toisaalta myös

$$f([12]) = [4 \cdot 12 + 3] = [2 \cdot 24 + 3] = [0 + 3] = 0\,.$$

Toisaalta $[6] \neq [12]$, kuten helposti nähdään. Siispä kaksi eri luokkaa kuvautuvat samaksi luokaksi eli injektiiviisyys ei toteudu. Vastaus tehtävän kysymykseen on näin ollen kielteinen funktion f tapauksessa.

Funktiolle g tilanne on toinen: kyseessä on bijektio. Todistetaan tämä. Osoitetaan ensin, että g on injektio. Olkoot tätä varten $k, l \in \mathbb{Z}$ ja $[k], [l] \in \mathbb{Z}_{24}$ siten, että

$$g([k]) = g([l])\,. \tag{1}$$

On osoitettava,

$$[k] = [l]\,. \tag{2}$$

Jos $k = l$, on asia selvä. Voidaan siis olettaa, että $k \neq l$. Oletus (1) tarkoittaa kuvauksen g määritelmän nojalla, että

$$[7k] = [7l]$$

eli että on olemassa kokonaisluku m siten, että

$$7k - 7l = 24m$$

eli

$$7(k - l) = 24m\,. \tag{3}$$

Koska $syt(7, 24) = 1$, voi ehto (3) toteutua vain, jos $(k - l)|24$. On siis olemassa $n \in \mathbb{Z}$ siten, että

$$k - l = 24l\,.$$

Mutta tämähän on yhtäpitävää väitteen (2) kanssa, joten funktion g injektiivisyys on todistettu. Väitteen (eli g:n bijektiivisyyden) todistamiseksi on vielä osoitettava, että g on surjektio. Yksi tapa olisi huomata, että kyseessä on injektio äärelliseltä joukolta itselleen, mistä surjektiivisuus seuraa välittömästi. Esimerkin vuoksi tehdään todistus kuitenkin suoraan surjektiivisuuden määritelmän kautta. Olkoon tätä varten $[l] \in \mathbb{Z}_{24}$ kiinteä. Riittää löytää $k \in \mathbb{Z}$ siten, että

$$g([k]) = [l]$$

eli että

$$[7k] = [l]\,. \tag{4}$$

Valitaan luokalle $[l]$ edustaja, olkoon se $l \in \mathbb{Z}$. Väitteen (4) todistamiseksi riittää nyt löytää $k \in \mathbb{Z}$ ja $m \in Z$ siten, että

$$7k - l = 24m\,. \tag{5}$$

Koska $syt(7, 24) = 1$, on olemassa $a, b \in \mathbb{Z}$ siten, että

$$7a + 24b = 1\,; \tag{6}$$

helposti nähdään, että $a = 7$ ja $b = -2$, mutta se ei ole tässä oleellista. Kertomalla yhtälö (6) puolittain kokonaisluvulla l saadaan

$$7la + 24lb = l$$

eli

$$7la - l = 24lb\,.$$

Tämä tarkoittaa, että ehdossa (5) voidaan valita $k = la$ ja $m = lb$. Tällaisten k:n ja m:n löytyminen, kuten edellä selitetty, riittää todistamaan g:n surjektiivisuuden. Väite on siis loppuun todistettu.

5.6. Kysyttiin ensinnäkin, miksi englannin kielen salaamiseen ei kannata käyttää salausfunktiota $f(k) \equiv 13k + 5$. Ongelma on siinä, että salaus olisi aika ei-injektiivinen. Nimittäin, kun eletään renkaassa $\mathbb{Z}_{26}$, pätee $[2 \cdot 13] = [26] = [0]$, joten mille tahansa salattavalle kirjaimelle, jonka koodi k olisi parillinen ($k = 2m$ jollekin $m \in \mathbb{Z}$), olisi voimassa

$$[f(k)] = [13k + 5] = [13 \cdot 2m + 5] = [0 + 5] = [5]\,,$$

joten kaikki tällaiset viestit kuvautuisivat vitoselle eli kirjaimelle E.

Suomen kielessä, kun salattavia merkkejä on 29 ja eletään siis renkaassa $\mathbb{Z}_{29}$, ei tuota ongelmaa ole. Nimittäin $syt(13, 29) = 1$, ja siten salaaminen – ja kääntäminen – onnistuu yksikäsitteisesti.

5.7. Eletään suomalaisittain modulossa 29. Tarkastellaan salausfunktiota $[f(k)] = [5k+11]$. Puretaan tehtävänasettulossa annetut viestit. Tehdään tähän ensin toimintasuunnitelma. Olkoon siis $m \in \{0, \ldots, 28\}$ salattu kirjain. On löydettävä $k \in \{0, \ldots, 28\}$ siten, että

$$5[k] + [11] = [m]$$

eli

$$5[k] = [m - 11]\,. \tag{1}$$

Ensinnäkin huomataan, että koska $syt(5, 29) = 1$, ratkeaa yhtälö (1) yksikäsitteisesti renkaassa $\mathbb{Z}_{29}$. Ratkaisu on

$$[k] = [m - 11] \cdot [5]^{-1}\,. \tag{2}$$

Luokan $[5]$ käänteisalkio löytyy helposti: koska $5 \cdot 6 = 30 = 29 + 1$, pätee

$$[5]^{-1} = [6]\,.$$

Tästä seuraa ehdon (2) kanssa, että

$$[k] = [m - 11] \cdot [6] = [6m - 66]\,. \tag{3}$$

a) Kun $m = 5$, saadaan ehdosta (3), että

$$[k] = [6 \cdot 5 - 66] = [-33] = [22]$$

eli salattu kirjain on (kun tulkitaan A ykköseksi ja niin edelleen) V. Vastaavasti voidaan avata loppukoodi, tuloksena sana VAPPUNA. Muut näistä hoituvat vastaavasti, alla tulokset:

b) OTAN
c) IISISTI
d) KIPPIS!

5.8. Tässä pitää esittää tehtävänasettelun permutaatio σ erillisten kiertojen tulona. Tämä hoituu kuten kurssikirjan esimerkissä 4.2.2 etsimällä ja kirjaamalla jokainen permutaatiosta σ löytyvä sykli. Tuloksena on

$$\sigma = (1\ 5\ 15\ 8\ 9\ 4\ )(2\ 11\ 14\ 7\ )(3\ 6\ 13\ 12\ )(10\ 16)\,.$$

Kuten luennoilla lienee todettu, tässä esityksessä kiertojen järjestys ei ole yksikäsitteinen eli kierrot voi laittaa mihin järjestykseen tahansa.

5.9. Olkoon $k \in \{1, \ldots, n\}$. Olkoot lisäksi $\tau_1 \in S_n$ ja $\tau_2 \in S_n$ eri vaihtoja siten, että $\tau_1(k) \neq k$.

Väite: On olemassa vaihdot $\sigma_1, \sigma_2 \in S_n$ siten, että

$$\sigma_1(k) = k\,, \tag{1}$$
$$\sigma_2(k) \neq k \quad \text{ja} \tag{2}$$
$$\tau_2\tau_1 = \sigma_2\sigma_1\,. \tag{3}$$

Todistus: Koska $\tau_1(k) \neq k$, on olemassa $l \in \{1, \ldots, n\}$ siten, että $l \neq k$ ja $\tau_1(k) = l$. Koska τ_1 on oletuksen mukaisesti vaihto, on siis voimassa

$$\tau_1 = (kl)\,.$$

Permutaatiosta τ_2 ei ole oletettu mitään muuta kuin, että se on eri permutaatio kuin τ_1. Jakaudutaan kahteen vaihtoehtoon: pätee joko

$$\tau_2(k) = k \quad \text{tai} \tag{4}$$
$$\tau_2(k) \neq k\,. \tag{5}$$

Oletetaan ensin, että ehto (4) on voimassa. Tällöin τ_2 on muotoa $\tau_2 = (mr)$ joillekin $m, r \in \{1, \ldots, n\}$, $m, r \neq k$, $m \neq r$. Taas jakaudutaan kahteen vaihtoehtoon: pätee joko

$$r \neq l \quad \text{tai} \tag{6}$$
$$r = l\,. \tag{7}$$

Tapauksessa (6) tehtyjen oletusten nojalla kierrot τ_1 ja τ_2 ovat erillisiä. Tällöin valinnat $\sigma_2 = \tau_1$ ja $\sigma_1 = \tau_2$ toteuttavat ehdot (1)–(3), sillä

$$\sigma_1(k) = \tau_2(k) \overset{a)}{=} k\,,$$
$$\sigma_2(k) = \tau_1(k) = l \overset{b)}{\neq} l \text{ ja}$$
$$\tau_2\tau_1 = \sigma_1\sigma_2 \overset{a)}{=} \sigma_2\sigma_1\,.$$

Tässä yhtälössä a) on käytetty oletusta (4) ja huomiossa b) aivan todistuksen alussa tehtyä valintaa $k \neq l$. Yhtälö c) seuraa siitä, että erillisten kiertojen kertomisjärjestyksen saa vaihtaa. Väite on siis tosi tapauksessa (6).

Oletetaan sitten, että tapaus (7) on kyseessä, jolloin siis $\tau_2 = ml$, $l \neq m$, $m \neq k$, missä l on siis **sama alkio** kuin permutaatiossa $\tau_1 = (kl)$. Tällöin väitteessä haetut permutaatiot σ_1 ja σ_2 voidaan yksinkertaisesti konstruoida. Tätä varten huomataan, että tehdyillä valinnoilla

$$\tau_2\tau_1(k) = \tau_2(\tau_1(k)) = \tau_2(l) = m\,, \tag{7}$$
$$\tau_2\tau_1(l) = \tau_2(\tau_1(l)) = \tau_2(k) = k \quad \text{ja} \tag{8}$$
$$\tau_2\tau_1(m) = \tau_2(\tau_1(m)) = \tau_2(m) = l\,. \tag{9}$$

Valitaan $\sigma_1(k) = k$, $\sigma_1(m) = l$ ja $\sigma_1(l) = m$ eli $\sigma_1 = (ml)$. Osoitetaan, että tämän valinnan avulla voidaan konstruoida σ_2. Selvästi valinta toteuttaa ehdon (1). Toisaalta, jotta väite (3) täyttyisi, on pädettävä

$$\sigma_2(\sigma_1(k)) = \tau_2\tau_1(k)\,,$$

mistä saadaan ehdon (7) avulla, koska $\sigma_2(\sigma_1(k)) = \sigma_2(k)$,

$$\sigma_2(k) = m\,. \tag{10}$$

Vastaavasti ehdon (8) avulla nähdään, että on oltava

$$\sigma_2(\sigma_1(l)) = k$$

eli, koska $\sigma_1(l) = m$,

$$\sigma_2(m) = k\,. \tag{11}$$

Ja lopuksi ehdon (9) avulla huomataan, että täytyy päteä

$$\sigma_2(\sigma_1(m)) = l$$

eli, koska $\sigma_1(l) = m$,

$$\sigma_2(l) = l\,. \tag{12}$$

Yhdistämällä vaatimukset (10)–(12) huomataan, että $\sigma_2 = (km)$. Se, että tällainen valinta voidaan tehdä (tai "löytyy"), osoittaa, että väite pätee myös tapauksessa (7). Todistuksen ensimmäinen haara eli ehto (4) on siis loppuun käsitelty.

Täytyy vielä todistaa väite tapauksessa (5). Tällöin siis $\tau_2 = (km)$ jollekin $m \neq k$ ja, kuten muistetaan aivan todistuksen alusta, $\tau_1 = (kl)$, $l \neq k$. Koska on oletettu, että τ_1 ja τ_2 ovat eri vaihtoja, on oltava $m \neq l$.

Nyt voi suoraan huomata (tai edetä samankaltaisilla vaiheittaisilla argumenteilla kuin edellä), että valinnat $\sigma_1 = (ml)$ ja $\sigma_1 = (kl)$ toimivat eli toteuttavat ehdot (1)–(3). Väite on siis kokonaisuudessaan todistettu. □

5.10. Tässä taas eletään modulossa 29. Tiedetään, että salauskielelle muunnetun viestin

$$12\ 0\ 26\ 3\ 3\ 26\ 5\ 20\ 20\ 25\ 5 \tag{1}$$

viimeinen kirjain on A ja, että salausfunktio on $f(p) = [p + k]$ jollekin $k \in \{0, \ldots, 28\}$. Selvitetään k. Koska viestin viimeinen kirjain on A vastaten numeroa 1, niin on voimassa

$$[k + 1] = [5] .$$

Tällöin $k = 4$ eli salausfunktio on $f(p) = [p+4]$. Tämän avulla voidaan viesti avata seuraavalla reseptillä: jos viestin kirjain p on salattu luvuksi m, niin

$$[p + 4] = [p] + [4] = [m]$$

eli

$$[p] = [m - 4] ,$$

ja sitten valitaan edustaja joukosta $\{0, \ldots, 28\}$. Tällöin esimerkiksi, kun $m = 12$, saadaan

$$[p] = [12 - 4] = [8] ,$$

jolloin viestin (1) ensimmäinen kirjain on H. Loput löydetään vastaavasti, ja koko viesti (1) purettuna on

HYVÄÄVAPPUA.