

Tehtävien 1–6 ratkaisut on muokattu Ville Puuskan tekemistä.

Tehtävä 1. Olkoon $a \in R$. Tällöin

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0,$$

joten vähentämällä molemmilta puolilta $a \cdot 0$ saadaan

$$0 = a \cdot 0.$$

Vastaavasti nähdään, että $0 \cdot a = 0$.

Tehtävä 2. Alkio $a + 126\mathbb{Z} \in \mathbb{Z}/126\mathbb{Z}$ on kääntyvä, jos ja vain jos on olemassa $b \in \mathbb{Z}$, jolle $(a + 126\mathbb{Z})(b + 126\mathbb{Z}) = 1 + 126\mathbb{Z}$ eli $ab + 126\mathbb{Z} = 1 + 126\mathbb{Z}$. Tämä pätee täsmälleen silloin, kun on olemassa sellainen $n \in \mathbb{Z}$, että $1 = ab + 126n$. Diofantoksen yhtälöistä tiedetään algebran peruskursseilta, että

$$\exists x, y \in \mathbb{Z}: cx + dy = 1 \iff \text{syt}(c, d) = 1,$$

kun $c, d \in \mathbb{Z}$. Sovelletaan tätä kertoimiin a ja 126 sekä tuntemattomiin b ja n : $a + 126\mathbb{Z}$ on kääntyvä, jos ja vain jos $\text{syt}(a, 126) = 1$. Alkutekijäesityksen $126 = 2 \cdot 3^2 \cdot 7$ avulla saadaan kääntyvien alkioiden joukoksi

$$\begin{aligned} (\mathbb{Z}/126\mathbb{Z})^* &= \{a + 126\mathbb{Z} \in \mathbb{Z}_{126} \mid \text{syt}(a, 126) = 1\} \\ &= \{a + 126\mathbb{Z} \in \mathbb{Z}_{126} \mid 2 \nmid a, 3 \nmid a, 7 \nmid a\} \\ &= \{\pm a + 126\mathbb{Z} \in \mathbb{Z}_{126} \mid a \in I\}, \end{aligned}$$

missä

$$I = \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41, 43, 47, 53, 55, 59, 61\}.$$

Tehtävä 3. a) Määritellään $A = \{(x, y) \in \mathbb{R}^2 \mid xy = 0\}$ (yleisemmin tässä sopii esimerkiksi mikä tahansa kahden origon kautta kulkevan suoran yhdiste). A on selvästi vakaa skalaarilla kertomisen suhteen, mutta ei yhteenlaskun suhteen, sillä $(1, 0), (0, 1) \in A$ ja $(1, 1) \notin A$.

b) Määritellään $B = \mathbb{Z}^2$. Selvästi B on vakaa yhteenlaskun suhteen, mutta ei skalaarilla kertomisen suhteen, sillä $(1, 0) \in B$, mutta $(\pi, 0) = \pi(1, 0) \notin B$.

Aivan toisenlaisen esimerkin saisi jälkimmäiseen kohtaan valitsemalla joukoksi jonkin tason suljetuista neljänneksistä tai yleisemmin minkä tahansa taso kulman (mukaan lukien kylkien väliin jäävä alue), missä kärki on origossa.

Tehtävä 4. *Tapa 1 á la VP:* Ryhmälle \mathbb{Z}_2 ei voida antaa \mathbb{Z}_3 -modulirakennetta. Osoitetaan tämä tekemällä vasta oletus, että $\otimes: \mathbb{Z}_3 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ on skalaarikerronta joka tekee ryhmästä \mathbb{Z}_2 \mathbb{Z}_3 -modulin. Nyt

$$\begin{aligned} 1 + 2\mathbb{Z} &= 1 + 1 + 1 + 2\mathbb{Z} \\ &= (1 + 2\mathbb{Z}) + (1 + 2\mathbb{Z}) + (1 + 2\mathbb{Z}) \\ &= (1 + 3\mathbb{Z}) \otimes (1 + 2\mathbb{Z}) + (1 + 3\mathbb{Z}) \otimes (1 + 2\mathbb{Z}) + (1 + 3\mathbb{Z}) \otimes (1 + 2\mathbb{Z}) \\ &= \left((1 + 3\mathbb{Z}) + (1 + 3\mathbb{Z}) + (1 + 3\mathbb{Z}) \right) \otimes (1 + 2\mathbb{Z}) \\ &= (1 + 1 + 1 + 3\mathbb{Z}) \otimes (1 + 2\mathbb{Z}) \\ &= (0 + 3\mathbb{Z}) \otimes (1 + 2\mathbb{Z}) \\ &= 0 + 2\mathbb{Z}, \end{aligned}$$

mikä on mahdotonta.

Edellistä ideaa voi varioida monella tavalla, saatikka sitten, että muunkinlaisia esimerkkejä on:

Tapa 2 á la OO: Osoitetaan, että reaalilukujen yhteenlaskuryhmää $(\mathbb{R}, +)$ ei voi varustaa $\mathbb{Z}/2\mathbb{Z}$ -vektoriavaruuden rakenteella. Jos tämä olisi mahdollista, saataisiin vektoriavaruuden laskulakien perusteella nimittäin

$$2\pi = \pi + \pi = 1_{\mathbb{Z}/2\mathbb{Z}} \cdot \pi + 1_{\mathbb{Z}/2\mathbb{Z}} \cdot \pi = (1_{\mathbb{Z}/2\mathbb{Z}} + 1_{\mathbb{Z}/2\mathbb{Z}})\pi = 0_{\mathbb{Z}/2\mathbb{Z}}\pi = 0,$$

mikä on mieletöntä.

Tehtävä 5. Olkoon $x, y \in G$ ja $f, g \in H$. Nyt

$$1) f \cdot (x + y) = f(x + y) = f(x) + f(y) = fx + fy,$$

$$2) (f + g)x = (f + g)(x) = f(x) + g(x) = fx + gx,$$

$$3) f \cdot (g \cdot x) = f(g(x)) = (f \circ g)(x) = (f \circ g)x,$$

$$4) 1x = \text{id}(x) = x.$$

Siispä G on H -moduli.

Tehtävä 6. Aloitetaan Abelin ryhmän aksioomista. Olkoon $A, B, C \subseteq X$.

- Todetaan ensin, että laskutoimitus on vaihdannainen: $A \Delta B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) = B \Delta A$.

- $(A \Delta B) \Delta C = ((A \setminus B) \cup (B \setminus A)) \Delta C = (((A \setminus B) \cup (B \setminus A)) \setminus C) \cup (C \setminus ((A \setminus B) \cup (B \setminus A))) = (A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \cup (C \setminus ((A \cup B) \setminus (A \cap B))) = (A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \cup (C \setminus (A \cup B)) \cup (A \cap B \cap C)$. Viimeinen joukko on selvästi aina sama joukkojen A , B ja C järjestyksestä riippumatta, joten myöskin $A \Delta (B \Delta C) = (C \Delta B) \Delta A$ on yhtäsuuri viimeisen joukon kanssa. Siis

$$(A \Delta B) \Delta C = A \Delta (B \Delta C).$$

- Triviaalisti $\emptyset \Delta A = A$, eli \emptyset on neutraalialkio.
- Selvästi myös $A \Delta A = \emptyset$, joten A on itsensä vasta-alkio.

Siis $(\mathcal{P}(X), \Delta)$ on Abelin ryhmä. Huomaa, että kahdessa viimeisessä kohdassa riittää osoittaa vain toinen aksiooman yhtäsuuruuksista, koska laskutoimituksen vaihdannaisuus antaa jäljelle jäävän yhtäsuuruuden.

Tunnetusti $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ on kunta.

Osoitetaan nyt, että ryhmä $(\mathcal{P}(X), \Delta)$ voidaan varustaa $\mathbb{Z}/2\mathbb{Z}$ -vektoriavaruuden rakenteella tehtävässä selitetyllä tavalla. Olkoot $A, B \in \mathcal{P}(X)$ ja $a, b \in \mathbb{Z}/2\mathbb{Z}$.

- 1) Jos $a = \bar{0}$, niin $a \cdot (A \Delta B) = \bar{0} \cdot (A \Delta B) = \emptyset = \emptyset \Delta \emptyset = (\bar{0} \cdot A) \Delta (\bar{0} \cdot B)$, jos taas $a = \bar{1}$, niin $a \cdot (A \Delta B) = \bar{1} \cdot (A \Delta B) = A \Delta B = (\bar{1} \cdot A) \Delta (\bar{1} \cdot B)$.

2)

$$(a + b)A = \begin{cases} \emptyset, & \text{jos } a = b = \bar{0} \text{ tai } a = b = \bar{1}, \\ A, & \text{jos } a \neq b, \end{cases}$$

ja

$$aA \Delta bA = \begin{cases} \emptyset, & \text{jos } a = b = 0 \\ A, & \text{jos } a \neq b, \\ A \Delta A, & \text{jos } a = b = 1, \end{cases} = \begin{cases} \emptyset, & a = b = 0 \text{ tai } a = b = 1 \\ A, & a \neq b, \end{cases}$$

sillä $A \Delta A = \emptyset$. Siispä $(a + b)A = aA \Delta bA$.

- 3) Jos $b = \bar{1}$, niin $bA = A$ ja $ab = a$, joten $(ab)A = aA = a(bA)$. Jos taas $b = \bar{0}$, niin $bA = \emptyset$, $ab = \bar{0}$ ja $(ab)A = \bar{0} \cdot A = \emptyset = a \cdot \emptyset = a(bA)$.

- 4) Viimeinen laskulaki pätee suoraan asetetun skalaaritulon määritelmän nojalla.

Näin ollen $(\mathcal{P}(X), \Delta)$ on $\mathbb{Z}/2\mathbb{Z}$ -vektoriavaruus.