

### 3. TEKIJÄLASKUTOIMITUS, KOKONAISLUVUT JA RATIONAALILUVUT

Tässä luvussa tutustumme kolmanteen tapaan muodostaa laskutoimitus joukkoon tunnettujen laskutoimitusten avulla. Tätä varten määrittelemme ensin tarvittavan ekvivalenssirelaation käsitteen.

**Määritelmä 3.1.** Olkoon  $A$  epätyhjä joukko. Joukon  $A \times A$  osajoukko *relaatio* joukossa  $A$ .

Jos  $R \subset A \times A$  on relaatio, usein merkitään  $a R b$ , jos  $(a, b) \in R$ .

**Määritelmä 3.2.** Joukon  $A$  relaatio  $R$  on

- (1) *refleksiivinen*, jos  $a R a$  kaikilla  $a \in A$ ,
- (2) *symmetrinen*, jos  $b R a$  kaikilla  $a, b \in A$ , joille  $a R b$ ,
- (3) *transitiivinen*, jos  $a R c$  aina kun  $a R b$  ja  $b R c$ ,
- (4) *antisymmetrinen*, jos  $b = a$  kaikilla  $a, b \in A$ , joille  $a R b$  ja  $b R a$ .

Jos relaatio on refleksiivinen, symmetrinen ja transitiivinen, se on *ekvivalenssirelaatio*. Jos  $R$  on ekvivalenssirelaatio joukossa  $A$ , sanotaan, että joukon  $A$  alkio  $a$  ja  $b$  ovat *ekvivalentteja*, jos  $a R b$ .

Ekvivalenssirelaation merkinä käytetään usein merkkiä  $\sim$ . Tällöin käytetään merkintää  $a \sim b$ , jos  $a$  ja  $b$  ovat ekvivalentteja.

**Määritelmä 3.3.** Jos  $\sim$  on ekvivalenssirelaatio joukossa  $A$ , niin jokainen joukon  $A$  alkio  $a$  määrää *ekvivalenssiluokan*

$$[a] = \{b \in A : a \sim b\}.$$

Ekvivalenssiluokkien joukko

$$A/\sim = \{[a] : a \in A\}$$

on ekvivalenssirelaatiota  $\sim$  vastaavaksi joukon  $A$  *tekijäjoukko*. Kuvaus  $E \rightarrow E/\sim$ ,  $a \mapsto [a]$ , on ekvivalenssirelaatiota  $\sim$  vastaava *tekijäkuvaus* eli *luonnollinen kuvaus*.

Ekvivalenssiluokat ovat erillisiä:

**Lemma 3.4.** *Olkoon  $\sim$  ekvivalenssirelaatio joukossa  $A$ . Pisteiden  $x, y \in A$  ekvivalenssiluokille pätee:*

- (1) *Jos  $x \sim y$ , niin  $[x] = [y]$ .*
- (2) *Jos  $[x] \cap [y] \neq \emptyset$ , niin  $[x] = [y]$ .*

*Todistus.* Harjoitustehtävä 21. □

Jos

$$(3) \quad A = \bigcup_{i \in I} A_i$$

ja kaikille  $i \neq j$  pätee  $A_i \cap A_j = \emptyset$ , sanotaan, että  $A$  on *erillinen yhdiste* joukoista  $A_i$ ,  $i \in I$ . Merkitsemme joukkojen  $A_i$ ,  $i \in I$  erillistä yhdistettä

$$A = \bigsqcup_{i \in I} A_i.$$

Tämä merkintä sisältää tiedon, että yhdistettävät joukot ovat erillisiä. Jos  $A = \bigsqcup_{i \in I} A_i$ , niin joukot  $A_i$ ,  $i \in I$  muodostavat joukon  $A$  *osituksen*.

Lemman 3.4 nojalla joukon  $X$  ekvivalenssirelaation  $\sim$  ekvivalenssiluokat muodostavat joukon  $X$  osituksen. Itse asiassa myös käänteinen väite pätee: Jos joukot  $A_i$ ,  $i \in I$  muodostavat joukon  $A$  osituksen, määritellään relaatio  $R$  asettamalla  $x R y$ , jos ja vain jos  $x, y \in A_i$  jollain  $i \in I$ . Osoittautuu, että relaatio  $R$  on ekvivalenssirelaatio.

**Propositio 3.5.** *Olkoon  $X \neq \emptyset$ .*

- (1) *Joukon  $X$  ekvivalenssirelaatio määrää joukon  $X$  osituksen.*
- (2) *Joukon  $X$  ositus määrää joukon  $X$  ekvivalenssirelaation.*

*Todistus.* Kohta (1) seuraa Lemmasta 3.4.

Todistetaan kohta (2): Olkoon  $R$  osituksen  $A = \bigsqcup_{i \in I} A_i$  määräämä relaatio. Tällöin

- (1) Koska  $A = \bigcup_{i \in I} A_i$ , niin jokaiselle  $a \in A$  pätee  $a \in A_i$  jollakin  $i \in I$ . Siis  $a R a$ , joten  $R$  on refleksiivinen.
- (2) Symmetrisyys on selvä, koska relaatio  $R$  määritellään ehdolla  $a, b \in A_i$ .
- (3) Oletetaan, että  $a, b \in A_i$  ja  $b, c \in A_j$  joillain  $i, j \in I$ . Koska joukot  $A_k$ ,  $k \in I$  muodostavat joukon  $A$  osituksen, pätee joko  $A_i = A_j$  tai  $A_i \cap A_j = \emptyset$ . Oletuksen mukaan  $b \in A_i \cap A_j$ , joten  $A_i = A_j$ , ja siis  $a, c \in A_i$ , joten relaatio  $R$  on transitiiivinen.

□

**Määritelmä 3.6.** Joukon  $A$  laskutoimitus  $*$  ja ekvivalenssirelaatio  $\sim$  ovat yhteensopivat, jos  $a * b \sim a' * b'$  aina kun  $a \sim a'$  ja  $b \sim b'$ . Jos joukon  $A$  ekvivalenssirelaatio  $\sim$  ja laskutoimitus  $*$  ovat yhteensopivat, niin joukon  $A/\sim$  laskutoimitus  $*$ , joka määritellään asettamalla

$$[a] * [b] = [a * b]$$

on laskutoimituksen  $*$  määräämä tekijälaskutoimitus.

**Propositio 3.7.** *Olkoon  $\sim$  ekvivalenssirelaatio laskutoimituksella varustetussa joukossa  $(E, *)$ . Jos ekvivalenssirelaatio  $\sim$  ja laskutoimitus  $*$  ovat yhteensopivat, niin luonnollinen kuvaus on surjektiivinen homomorfismi. Jos  $e \in E$  on laskutoimituksen  $*$  neutraalialkio, niin  $[e] \in E/\sim$  on tekijälaskutoimituksen neutraalialkio.*

*Todistus.* Tämä seuraa määritelmästä: Olkoon  $\phi$  luonnollinen kuvaus. Kaikille  $a, b \in E$  pätee

$$\phi(a) * \phi(b) = [a] * [b] = [a * b] = \phi(a * b),$$

joten luonnollinen kuvaus on homomorfismi. Kuvauksen surjektiivisuus on selvää, koska jokaisella ekvivalenssiluokalla on edustaja joukossa  $E$ . Neutraalialkiota koskeva väite seuraa Propositioista 1.14. □

**Propositio 3.8.** *Jos laskutoimitus  $*$  on assosiatiivinen, sen tekijälaskutoimitus on assosiatiivinen. Jos  $*$  on kommutatiivinen, sen tekijälaskutoimitus on kommutatiivinen.*

*Todistus.* Koska luonnollinen kuvaus on Proposition 3.7 mukaan surjektiivinen homomorfismi, väite seuraa Propositioista 1.14. □

**Esimerkki 3.9.** Olkoon  $q \in \mathbb{N}$ ,  $q \geq 2$ . Olkoon relaatio  $\equiv$  kokonaislukujen joukossa  $\mathbb{Z}$  määritelty säännöllä  $a \equiv b$ , jos on  $k \in \mathbb{Z}$  siten, että  $b = a + kq$ . Tällöin  $\equiv$  on ekvivalenssirelaatio:

- (1)  $a = a + 0q$  kaikilla  $a \in \mathbb{Z}$ ,
- (2) jos  $b = a + kq$  jollain  $k \in \mathbb{Z}$ , niin  $a = b + (-kq)$ ,
- (3) jos  $b = a + kq$  ja  $c = b + nq$  joillain  $k, n \in \mathbb{Z}$ , niin  $c = a + (k + n)q$ .

Ekvivalenssirelaatiota  $\equiv$  kutsutaan *kongruenssiksi (modulo  $q$ )*. Koska ekvivalenssirelaatio riippuu luonnollisesta luvusta  $q$ , tälle ekvivalenssirelaatiolle käytetään merkintää

$$a \equiv b \pmod{q} \quad \text{tai} \quad a \equiv b \pmod{q}.$$

Kongruenssia vastaavia ekvivalenssiluokkia sanotaan *kongruenssiluokiksi (modulo  $q$ )* ja vastaavalle tekijäjoukolle käytetään merkintää

$$\mathbb{Z}/q\mathbb{Z} = \{[0], [1], [2], \dots, [q-1]\}.$$

Kokonaislukujen yhteenlasku ja kertolasku ovat yhteensopivia kongruenssin kanssa. Osoitamme tämän yhteenlaskulle: Jos  $a' = a + mq$  ja  $b' = b + nq$ , niin

$$a' + b' = a + b + (m + n)q,$$

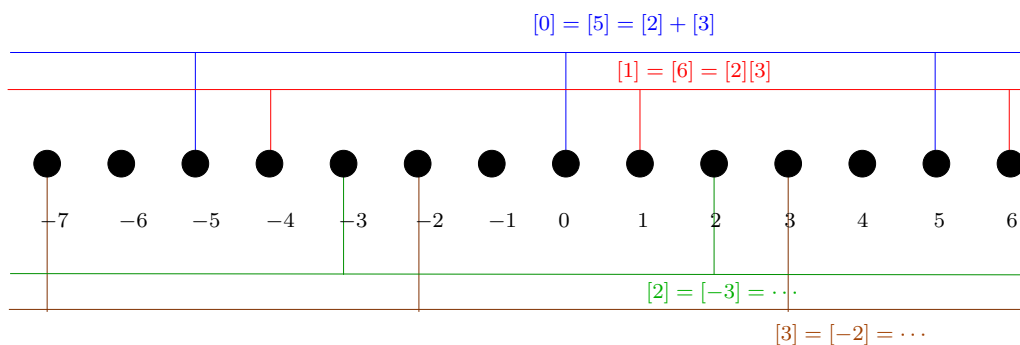
joten

$$a' + b' \equiv a + b \pmod{q}.$$

Kertolaskulle väite osoitetaan samaan tapaan harjoituksissa (Harjoitustehtävä 22). Kokonaislukujen yhteenlasku ja kertolasku määräävät siis laskutoimitukset  $q$  alkion joukolla  $\mathbb{Z}/q\mathbb{Z}$ . Lemman 3.8 nojalla molemmat laskutoimitukset ovat assosiatiivisia ja kommutatiivisia. Käytämme molemmille kongruenssiluokkien laskutoimituksille samaa merkintää kuin indusoiville laskutoimituksille:

$$[a] + [b] = [a + b] \quad \text{ja} \quad [a][b] = [ab]$$

kaikille  $[a], [b] \in \mathbb{Z}/q\mathbb{Z}$ . Proposition 3.7 mukaan  $[0]$  on kongruenssiluokkien yhteenlaskun neutraalialkio ja  $[1]$  on kongruenssiluokkien kertolaskun neutraalialkio.



KUVA 4. Kongruenssiluokat modulo 5.

Kurssilla Lukualueet tarkastellaan kokonaislukujen ja rationaalilukujen konstruktioita luonnollisista luvuista lähtien esimerkkinä tekijälaskutoimituksesta. Luonnollisten lukujen joukko ja sen laskutoimitukset yhteenlasku ja kertolasku oletetaan “intuitiivisesti tunnetuiksi”. Lukualueiden kurssin aikana konstruoidaan muut lukualueet

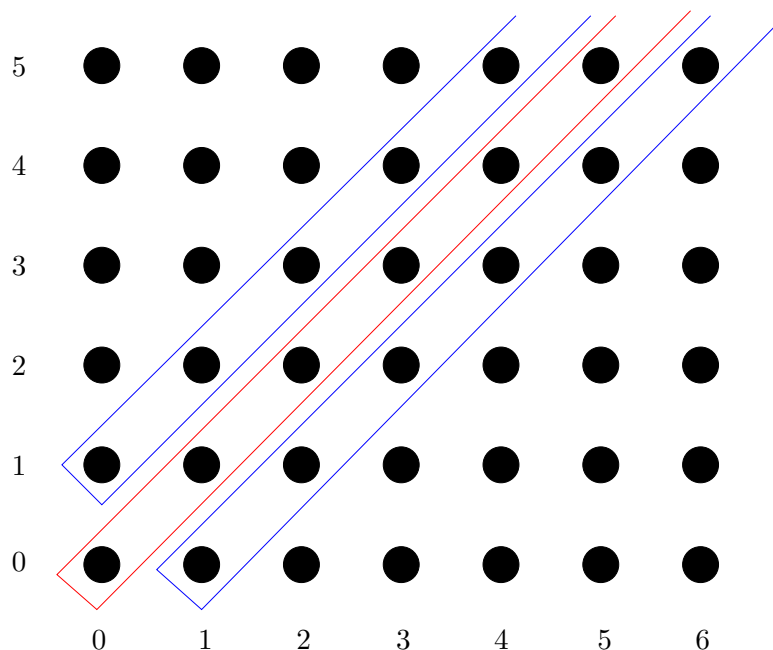
$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

laajentamalla asteittain luonnollisista luvuista lähtien. Samalla tarkastellaan, miten algebralliset ominaisuudet muuttuvat laajempaan lukualueeseen siirryttäessä. Tällä kurssilla tarkastelemme kokonaislukujen ja rationaalilukujen määrittelyä lyhyesti esimerkkinä tekijälaskutoimituksista.

**Esimerkki 3.10.** Määrittelemme kokonaisluvut “luonnollisten lukujen muodollisina erotuksina”: Jos  $m$  ja  $n$  ovat luonnollisia lukuja ja  $m \geq n$ , niin niiden erotus  $m - n$  on luonnollinen luku, se on yhtälön  $n + x = m$  ratkaisu. Toisaalta sama luonnollinen luku voidaan esittää erotuksena äärettömän monella eri tavalla, sillä kaikilla  $k \in \mathbb{N}$  pätee

$$(m + k) - (n + k) = m - n.$$

Näiden havaintojen opastamana määrittelemme joukkoon  $\mathbb{N} \times \mathbb{N}$  relaation  $\sim$  asettamalla  $(m, n) \sim (p, q)$ , jos ja vain jos  $m + q = p + n$ . Harjoitustehtävässä 23 osoitetaan, että relaatio  $\sim$  on ekvivalenssirelaatio.



KUVA 5. Kokonaislukujen määrittelyssä käytettävä ekvivalenssirelaatio joukossa  $\mathbb{N} \times \mathbb{N}$ .

Kokonaislukujen joukko on

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim .$$

Kokonaislukujen *yhteenlasku* on luonnollisten lukujen yhteenlaskun tulo

$$(4) \quad (m, n) + (p, q) = (m + p, n + q),$$

indusoima laskutoimitus, ja *kertolasku* on joukon  $\mathbb{N} \times \mathbb{N}$  laskutoimituksen

$$(5) \quad (m, n) * (p, q) = (mp + nq, mq + np)$$

indusoima laskutoimitus.

Laskutoimitusten määritelmät ovat järkeviä: Paria  $(m, n)$  tulee ajatella erotukse-  
na  $m - n$ , jolloin lausekkeet (4) ja (5) vastaavat lausekkeitä

$$(m - n) + (p - q) = (m + p) - (n + q)$$

ja

$$(m - n)(p - q) = (mp + nq) - (mq + np).$$

Kokonaislukujen laskutoimitukset ovat hyvin määriteltyjä, koska vastaavat jouk-  
koon  $\mathbb{N} \times \mathbb{N}$  määritellyt laskutoimitukset ovat yhteensopivia ekvivalenssirelaation  $\sim$   
kanssa. Todistamme tämän yhteenlaskulle: Jos  $(m, n) \sim (m', n')$  ja  $(p, q) \sim (p', q')$ ,  
niin määritelmän mukaan pätee  $m + n' = m' + n$  ja  $p + q' = p' + q$ . Siis

$$(m + p) + (n' + q') = (m' + p') + (n + q),$$

joten  $(m + p, n + q) \sim (m' + p', n' + q')$ . Kertolasku käsitellään harjoitustehtävässä  
24.

**Esimerkki 3.11.** Rationaaliluvut muodostetaan vastaavalla tavalla kuin kokonais-  
luvut edellä kokonaislukujen muodollisten osamäärien avulla: Määrittelemme ekvi-  
valenssirelaation  $\sim$  joukossa  $\mathbb{Z} \times \mathbb{Z}^*$  (missä  $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ ) asettamalla  $(a, b) \sim (c, d)$ ,  
jos ja vain jos  $ad = bc$ .

Rationaalilukujen joukko on

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^* / \sim .$$

Käytämme rationaaliluvuista tavanomaista merkintää  $p/q = [(p, q)]$ . Rationaalilukujen *yhteenlasku* on laskutoimituksen

$$(a, b) \oplus (c, d) = (ad + bc, bd)$$

indusoima tekijälaskutoimitus

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

ja rationaalilukujen *kertolasku* on kokonaislukujen kertolaskun tulon

$$(a, b) \otimes (c, d) = (ac, bd)$$

indusoima laskutoimitus. Harjoitustehtävässä 25 osoitetaan, että laskutoimitukset  $\oplus$  ja  $\otimes$  ovat ekvivalenssirelaation  $\sim$  kanssa yhteensopivia.

### Harjoitustehtäviä.

**Tehtävä 19.** Olkoon  $R$  relaatio joukossa  $\mathbb{R}^2$  siten, että  $(x, y) R (z, w)$ , jos ja vain jos  $x^2 + y^2 = z^2 + w^2$ . Osoita, että  $R$  on ekvivalenssirelaatio. Millaisia joukkoja relaation  $R$  ekvivalenssiluokat ovat?

**Tehtävä 20.** Mitkä seuraavista ovat joukon  $\mathbb{C}$  ekvivalenssirelaatioita?

- $z R w$ , jos ja vain jos  $\operatorname{Re} z = \operatorname{Re} w$ .
- $z R w$ , jos ja vain jos  $|z| \leq |w|$ .
- $z R w$ , jos ja vain jos  $\operatorname{Re} z = \operatorname{Im} w$ .

**Tehtävä 21.** Olkoon  $\sim$  ekvivalenssirelaatio joukossa  $A$ . Olkoot  $x, y \in A$ . Osoita, että ekvivalenssiluokille pätee:

- (1) Jos  $x \sim y$ , niin  $[x] = [y]$ .
- (2) Jos  $[x] \cap [y] \neq \emptyset$ , niin  $[x] = [y]$ .

**Tehtävä 22.** Osoita, että kokonaislukujen kertolasku on yhteensopiva kongruenssin kanssa.

**Tehtävä 23.** Määritellään relaatio  $\sim$  joukossa  $\mathbb{N} \times \mathbb{N}$  asettamalla  $(m, n) \sim (p, q)$ , jos ja vain jos  $m + q = n + p$ . Osoita, että  $\sim$  on ekvivalenssirelaatio.

**Tehtävä 24.** Määritellään laskutoimitus  $*$  joukossa  $\mathbb{N} \times \mathbb{N}$  asettamalla

$$(m, n) * (p, q) = (mp + nq, mq + np)$$

Osoita, että  $*$  on yhteensopiva tehtävän 23 ekvivalenssirelaation kanssa.

**Tehtävä 25.** Osoita, että joukon  $\mathbb{Z} \times \mathbb{Z}^*$  ekvivalenssirelaatio, joka määritellään asettamalla  $(a, b) \sim (c, d)$ , jos ja vain jos  $ad = bc$ , on yhteensopiva laskutoimitusten

$$(a, b) \oplus (c, d) = (ad + bc, bd)$$

ja

$$(a, b) \otimes (c, d) = (ac, bd)$$

kanssa.

**Tehtävä 26.** Määritellään relaatio  $\sim$  reaalilukujen joukossa  $\mathbb{R}$  asettamalla  $x \sim y$ , jos ja vain jos  $x = qy$  jollain  $q \in \mathbb{Q}^\times$ . Osoita, että  $\sim$  on ekvivalenssirelaatio. Osoita, että tekijäjoukko  $\mathbb{R}/\sim$  on ylinumeroituva.

<sup>24</sup>Vihje: Todistuksessa voi käyttää vain luonnollisia lukuja!

<sup>26</sup>Vihje: Euklidiset avaruudet.