Osamääräkunta

LuK-tutkielma
Lauri Aalto
Opiskelijanumero: 2379263
Matemaattisten tieteiden laitos
Oulun yliopisto
Kevät 2016

Sisältö

Johdanto

Tässä tutkielmassa perehdytään osamääräkunnan käsitteeseen ja erityisesti sen muodostamisen eri vaiheisiin. Aluksi Luvussa 1 esitetään luettelonomaisesti kaikki tarvittavat määritelmät, lauseet ja merkinnät. Luvussa 2 perehdytään tarkasti osamääräkunnan muodostamisprosessiin. Tavoitteena on näyttää, että jokaisesta kokonaisalueesta voidaan laajentaa tai muuntaa kunta, josta löytyy vastine jokaiselle kokonaisalueen alkiolle jonkin isomorfismin kautta. Luvussa 3 käsitellään osamääräkunnan suhdetta muihin kuntiin, joilla on isomorfinen osajoukko saman kokonaisalueen kanssa kuin osamääräkunnalla.

Esitiedoiksi riittävät periaatteessa joukko-oppiin ja funktioihin liittyvät peruskäsitteet. Lukijan on kuitenkin suositeltavaa perehtyä ryhmän, renkaan ja kunnan käsitteisiin, ja niiden perusominaisuuksiin.

1 Käsitteitä ja merkintöjä

Seuraavat määritelmät ja lauseet ovat peräisin suoraan tai sisällöltään lähteistä [2] ja [3]. Niitä ei todisteta tässä tutkielmassa. Tuloksia käytetään Lukujen 2 ja 3 lauseiden todistuksissa sekä teorian apuna.

Määritelmä 1.1 (Karteesinen tulo)**.** Olkoon A epätyhjä joukko. Tällöin joukko

$$A \times A = \{(a_1, a_2) \mid a_1, a_2 \in A\}$$

on *joukon A karteesinen tulo itsensä kanssa.*

Määritelmä 1.2 (Binäärinen relaatio)**.** Joukon $A \times A$ osajoukko R on *binäärinen relaatio* joukossa A. Jos pari $(x, y) \in R$, niin alkio x on relaatiossa R alkion y kanssa. Merkitään tällöin xRy.

Määritelmä 1.3 (Ekvivalenssirelaatio, ekvivalenssiluokka)**.** Joukon A binäärinen relaatio R on *ekvivalenssirelaatio*, mikäli

1. xRx, kun $x \in A$ (refleksiivisyys),
2. $xRy \Rightarrow yRx$, kun $x, y \in A$ (symmetrisyys),
3. xRy ja $yRz \Rightarrow xRz$, kun $x, y, z \in A$ (transitiivisuus).

Jos R on ekvivalenssirelaatio ja $a \in A$, niin joukko

$$[a] = \{x \in A \mid xRa\}$$

on *alkion a määräämä ekvivalenssiluokka.*

Määritelmä 1.4 (Binäärinen operaatio)**.** Olkoon A epätyhjä joukko. Tällöin kuvaus

$$* : A \times A \to A, \quad *(a, b) = a * b$$

kaikilla $a, b \in A$ on joukon A *binäärinen operaatio.*

Määritelmä 1.5 (Monoidi, ryhmä, Abelin ryhmä)**.** Olkoot R epätyhjä joukko ja $(*)$ joukon R binäärinen operaatio. Pari $(R, *)$ on *monoidi*, mikäli seuraavat ehdot ovat voimassa:

1. Jos $a, b \in R$, niin $a * b \in R$ (binäärisyys).
2. $(a * b) * c = a * (b * c)$ kaikilla $a, b, c \in R$ (assosiatiivisuus).

3. Joukossa R on olemassa *neutraalialkio* e_R, jolle pätee $a*e_R = e_R*a = a$ kaikilla $a \in R$.

Monoidista $(R, *)$ käytetään merkintää R, jos sekaannuksen mahdollisuutta ei ole. Jos lisäksi

4. kaikilla $a \in R$ on olemassa joukossa R *käänteisalkio* a^{-1}, jolle pätee $a * a^{-1} = a^{-1} * a = e_R$,

niin monoidi $(R, *)$ on *ryhmä*. Edelleen, jos

5. $a * b = b * a$ kaikilla $a, b \in R$ (kommutatiivisuus),

niin ryhmä $(R, *)$ on *Abelin ryhmä*.

Lause 1.6. Olkoon $(R, *)$ ryhmä. Tällöin

1. $(a * b)^{-1} = b^{-1} * a^{-1}$ kaikilla $a, b \in R$.
2. $(a^{-1})^{-1} = a$ kaikilla $a \in R$.
3. Neutraalialkio e_R ja jokaisen alkion $a \in R$ käänteisalkio ovat yksikäsitteiset.

Määritelmä 1.7 (Rengas)**.** Olkoot R epätyhjä joukko ja $(+)$ sekä $(\cdot)$ joukon R binäärisiä operaatioita. Kolmikko $(R, +, \cdot)$ on *rengas*, mikäli seuraavat ehdot ovat voimassa:

1. Pari $(R, +)$ on Abelin ryhmä.
2. Pari $(R, \cdot)$ on monoidi.
3. Seuraavat osittelulait ovat voimassa:
   (a) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ kaikilla $a, b, c \in R$.
   (b) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ kaikilla $a, b, c \in R$.

Määritelmä 1.8 (Kommutatiivinen rengas)**.** Rengas $(R, +, \cdot)$ on *kommutatiivinen*, mikäli se on kommutatiivinen operaation $(\cdot)$ suhteen eli $a \cdot b = b \cdot a$ kaikilla $a, b \in R$.

Renkaan $(R, +, \cdot)$ neutraalialkiota operaation $(+)$ suhteen kutsutaan *nolla-alkioksi* ja merkitään 0_R. Alkion a käänteisalkiota operaation $(+)$ suhteen kutsutaan *vasta-alkioksi* ja merkitään $-a$. Renkaan R neutraalialkiota operaation $(\cdot)$ suhteen kutsutaan *ykkösalkioksi* ja merkitään 1_R. Renkaan R laskuoperaatiosta $(\cdot)$ käytetään seuraavaa lyhennysmerkintää: $a \cdot b = ab$, kun $a, b \in R$. Lisäksi käytetään seuraavaa laskujärjestysmerkintää: $(a \cdot b) + (c \cdot d) = a \cdot b + c \cdot d$ kaikilla $a, b, c, d \in R$.

Määritelmä 1.9 (Alirengas)**.** Renkaan $(R, +, \cdot)$ epätyhjä osajoukko H on renkaan R *alirengas*, mikäli kolmikko $(H, +, \cdot)$ on rengas, joka sisältää renkaan R ykkösalkion.

Lause 1.10 (Alirengaskriteeri)**.** Renkaan $(R, +, \cdot)$ epätyhjä osajoukko H on renkaan R alirengas, jos ja vain jos seuraavat ehdot ovat voimassa:

1. Jos $a, b \in H$, niin $a + (-b) \in H$.
2. Jos $a, b \in H$, niin $ab \in H$.
3. $1_R \in H$.

Määritelmä 1.11 (Rengashomomorfismi)**.** Olkoot $(R, +, \cdot)$ ja $(R', \oplus, \odot)$ renkaita. Tällöin kuvaus $f : R \to R'$ on *rengashomomorfismi*, mikäli se täyttää seuraavat ehdot:

1. $f(a + b) = f(a) \oplus f(b)$ kaikilla $a, b \in R$.
2. $f(ab) = f(a) \odot f(b)$ kaikilla $a, b \in R$.
3. $f(1_R) = 1_{R'}$.

Määritelmä 1.12 (Rengasisomorfismi)**.** Rengashomomorfismi $f : R \to R'$ on *rengasisomorfismi*, mikäli kuvaus f on bijektio. Rengas R on *isomorfinen* renkaan R' kanssa, mikäli on olemassa jokin isomorfismi $f : R \to R'$. Tällöin merkitään $R \cong R'$.

Määritelmä 1.13 (Nollanjakaja)**.** Renkaan $(R, +, \cdot)$ nolla-alkiosta eroava alkio a on renkaan R *nollanjakaja*, mikäli on olemassa sellainen renkaan $(R, +, \cdot)$ nolla-alkiosta eroava alkio b, että $ab = 0_R$ tai $ba = 0_R$.

Määritelmä 1.14 (Kokonaisalue)**.** Kommutatiivinen rengas R on *kokonaisalue*, mikäli se ei sisällä nollanjakajia.

Lause 1.15. Olkoon $(R, +, \cdot)$ rengas. Tällöin seuraavat tulokset ovat voimassa:

1. $0_R a = a 0_R = 0_R$ kaikilla $a \in R$.
2. Jos kuvaus f on rengashomomorfismi renkaalta R jollekin renkaalle R', niin $f(0_R) = 0_{R'}$.
3. Olkoot R kokonaisalue, $a \in R \setminus \{0_R\}$ ja $b, c \in R$. Jos $ab = ac$, niin $b = c$. Vastaavasti, jos $ba = ca$, niin $b = c$.

4. Renkaan ykkösalkio on yksikäsitteinen.

5. $a(-b) = (-a)b = -(ab)$ kaikilla $a, b \in R$.

Määritelmä 1.16 (Kunta)**.** Kommutatiivinen rengas $(R, +, \cdot)$ on *kunta*, mikäli $(R \setminus \{0_R\}, \cdot)$ on Abelin ryhmä.

Määritelmä 1.17 (Alikunta)**.** Kunnan $(K, +, \cdot)$ epätyhjä osajoukko F on kunnan K *alikunta*, jos $(F, +, \cdot)$ on kunta.

Lause 1.18 (Alikuntakriteeri)**.** Kunnan $(K, +, \cdot)$ epätyhjä osajoukko F on kunnan K alikunta jos ja vain jos seuraavat ehdot ovat voimassa:

1. Joukossa F on vähintään kaksi alkiota.

2. $a + (-b) \in F$ kaikilla $a, b \in F$.

3. $ab^{-1} \in F$ kaikilla $a \in F, b \in F \setminus \{0_K\}$.

Määritelmä 1.19 (Kuntahomomofismi, kuntaisomorfismi)**.** Olkoot $(K, +, \cdot)$ ja $(K', \oplus, \odot)$ kuntia. Jos kuvaus $f : K \to K'$ on rengashomomorfismi, se on *kuntahomomorfismi*. Jos kuvaus f on rengasisomorfismi, se on *kuntaisomorfismi*. Edelleen, jos on olemassa jokin isomorfismi $f : K \to K'$, niin kunta K on *isomorfinen* kunnan K' kanssa. Tällöin merkitään $K \cong K'$.

2 Osamääräkunnan muodostaminen

Lähdetään liikkeelle kommutatiivisesta renkaasta R. Oletetaan, että rengas R ei ole kunta. Tällöin voidaan kysyä, onko olemassa mitään yksiselitteistä tapaa laajentaa rengasta R kunnaksi. Määritelmien 1.7 ja 1.16 nojalla yksi vaadittava ehto on, että joukon $R\setminus\{0_R\}$ jokaiselle alkiolle a on olemassa käänteisalkio a^{-1}, jolle pätee $aa^{-1} = a^{-1}a = 1_R$.

Oletetaan seuraavaksi, että rengas R sisältää vähintään yhden nollanjakajan. Valitaan näistä nollanjakajista yksi ja merkitään sitä kirjaimella a. Rengas R on kommutatiivinen, joten Määritelmän 1.13 nojalla on olemassa alkio $b \in R\setminus\{0_R\}$, jolle pätee $ab = ba = 0_R$. Jos alkiolla a on olemassa käänteisalkio, niin $b = 1_R b = a^{-1}ab = a^{-1}0_R = 0_R$. Tämä on ristiriita.

Näin ollen käänteisalkion olemassa olo jokaiselle joukon $R\setminus\{0_R\}$ alkiolle estää nollanjakajien esiintymisen renkaassa R. Se on itse asiassa riittävä ehto kunnan määritelmän täyttymiselle. Tällöin nimittäin binäärisyys, assosiatiivisuus, neutraalialkio ja kommutatiivisuus toteutuvat automaattisesti parille $(R\setminus\{0_R\}, \cdot)$, koska binäärinen operaatio $(\cdot)$ ei voi tuottaa nolla-alkiota.

Nollanjakajia sisältävän kommutatiivisen renkaan laajennus kunnaksi ei ole mahdollista edes minkään isomorfismin kautta, mikä nähdään käyttäen Määritelmän 1.11 kohtaa 2. Olkoot $a \in R$ nollanjakaja ja $b \in R\setminus\{0_R\}$ sellainen, että $ab = ba = 0_R$. Oletetaan, että on olemassa rengasisomorfismi f renkaalta $(R, +, \cdot)$ renkaalle $(H, \oplus, \odot)$, missä rengas $(H, \oplus, \odot)$ on erään kunnan $(K, \oplus, \odot)$ alirengas. Tällöin Lauseen 1.15 kohdan 2 nojalla $0_K = f(0_R) = f(ab) = f(a) \odot f(b)$. Nyt on oltava $f(a) = 0_K$ tai $f(b) = 0_K$, koska kunta ei voi sisältää nollanjakajia. Siis $f(0_R) = f(a)$ tai $f(0_R) = f(b)$, mikä on ristiriita, sillä $a \neq 0_R$, $b \neq 0_R$ ja kuvaus f on injektio. Siirrytään siis tarkastelemaan kokonaisalueita.

Tämän luvun määritelmät, lemmat ja lauseet on muodostettu pääosin lähteeseen [1] pohjautuen. Todistukset on tehty itsenäisesti käyttäen Luvun 1 tuloksia.

Määritelmä 2.1. Olkoon D kokonaisalue. Asetetaan karteesinen tulo

$$C(D) = D \times D \setminus \{0_D\} = \left\{(a, b) \in D^2 \;\middle|\; b \neq 0_D\right\}.$$

Joukko $C(D)$ toimii pohjana myöhemmin määriteltävälle joukolle, joka varustettuna sopivilla laskuoperaatioilla pyritään osoittamaan kunnaksi. Muodostetaan tätä varten sopiva relaatio joukon $C(D)$ alkioiden välille.

Määritelmä 2.2. Asetetaan joukon $C(D)$ binäärinen relaatio

$$R(D) = \left\{(a, b), (c, d) \in C(D) \;\middle|\; ad = bc \right\}.$$

Lemma 2.3. Binäärinen relaatio $R(D)$ on ekvivalenssirelaatio.

Todistus. Käytetään Määritelmää 1.3.

1. Olkoon $(a,b) \in C(D)$. Nyt $ab = ba$, joten $(a,b)\, R(D) (a,b)$.
2. Olkoot $(a,b),(c,d) \in C(D)$ ja $(a,b)\, R(D) (c,d)$. Nyt $ad = bc$ eli $cb = da$, joten $(c,d)\, R(D) (a,b)$.
3. Olkoot $(a,b),(c,d),(e,f) \in C(D)$ sekä $(a,b)\, R(D) (c,d)$ ja $(c,d)\, R(D)$ (e,f). Siis $ad = bc$ ja $cf = de$. Käyttäen Lauseen 1.15 kohtaa 3 ja kokonaisalueen D kommutatiivisuutta saadaan

$$ad = bc \Leftrightarrow ade = bce \Leftrightarrow acf = bce \Leftrightarrow afc = bec \Leftrightarrow af = be.$$

   Siis $(a,b)\, R(D) (e,f)$.

Kohtien 1-3 nojalla $R(D)$ on ekvivalenssirelaatio. □

Esimerkki 2.4. Verrataan joukkoa $C(\mathbb{Z})$ rationaalilukujen joukkoon $\mathbb{Q}$. Asetetaan kuvaus $f : C(\mathbb{Z}) \to \mathbb{Q}, \quad f(a,b) = \frac{a}{b}$. Olkoon $n \in \mathbb{Z} \setminus \{0,1\}$. Nyt $\frac{a}{b} = \frac{na}{nb}$. Kuitenkin $(a,b) \neq (na,nb)$. Toisaalta $anb = bna$, joten $(a,b)\, R(\mathbb{Z}) (na,nb)$.

Määritelmä 2.5. Asetetaan joukon $C(D)$ kaikkien alkioiden määräämien ekvivalenssiluokkien muodostama joukko ekvivalenssirelaation $R(D)$ suhteen

$$Q(D) = \left\{ [(a,b)] \;\middle|\; (a,b) \in C(D) \right\}.$$

Liitetään joukkoon $Q(D)$ operaatio $(\oplus)$, jonka laskusääntö on

$$[(a,b)] \oplus [(c,d)] = [(ad+bc, bd)] \quad \text{kaikilla } [(a,b)], [(c,d)] \in Q(D).$$

Lisäksi liitetään joukkoon $Q(D)$ operaatio $(\odot)$, jonka laskusääntö on

$$[(a,b)] \odot [(c,d)] = [(ac, bd)] \quad \text{kaikilla } [(a,b)], [(c,d)] \in Q(D).$$

Lemma 2.6. Joukko $Q(D)$ varustettuna operaatioilla $(\oplus)$ ja $(\odot)$ on hyvin määritelty.

Todistus. Joukko $Q(D)$ on hyvin määritelty, koska Lemman 2.3 nojalla jokaiselle joukon $C(D)$ alkiolle voidaan määrätä ekvivalenssiluokka. Todistetaan, että joukko $Q(D)$ varustettuna operaatiolla $(\oplus)$ on hyvin määritelty. Sitä varten on osoitettava, että seuraavat ehdot ovat voimassa:

1. Operoitaessa lähtöjoukon $Q(D)$ alkioita operaatiolla $(\oplus)$ maalijoukon on oltava sama kuin lähtöjoukon eli $[(a,b)] \oplus [(c,d)] \in Q(D)$ kaikilla $[(a,b)], [(c,d)] \in Q(D)$.

2. Jos $[(a,b)],[(a',b')],[(c,d)],[(c',d')] \in Q(D)$ sekä $[(a,b)] = [(a',b')]$ ja $[(c,d)] = [(c',d')]$, niin on oltava $[(a,b)] \oplus [(c,d)] = [(a',b')] \oplus [(c',d')]$.

Käydään ehdot läpi.

1. Olkoot $[(a,b)],[(c,d)] \in Q(D)$. Nyt $ad + bc \in D$, ja koska $b, d \in D \setminus \{0_D\}$, niin $bd \in D \setminus \{0_D\}$. Näin ollen $(ad+bc, bd) \in C(D)$. Edelleen $[(ad + bc, bd)] \in Q(D)$, joten $[(a,b)] \oplus [(c,d)] \in Q(D)$.

2. Olkoot $[(a,b)],[(a',b')],[(c,d)],[(c',d')] \in Q(D)$ sekä $[(a,b)] = [(a',b')]$ ja $[(c,d)] = [(c',d')]$. Tällöin $(a',b')\, R(D)(a,b)$ ja $(c',d')\, R(D)(c,d)$. Edelleen $a'b = b'a$ ja $c'd = d'c$. Lauseen 1.15 kohdan 3 sekä kokonaisalueen D kommutatiivisuuden avulla saadaan

$$\begin{cases} a'bd'd = b'ad'd \\ c'db'b = d'cb'b \end{cases} \Leftrightarrow \begin{cases} a'd'bd = b'd'ad \\ b'c'bd = b'd'bc \end{cases} .$$

Käyttäen kokonaisalueen D operaatiota $(+)$ operoidaan yhtälöparin ensimmäisen yhtälön vasenta puolta toisen yhtälön vasemmalla puolella, ja ensimmäisen yhtälön oikeaa puolta toisen yhtälön oikealla puolella. Tällöin

$$\begin{aligned} a'd'bd + b'c'bd &= b'd'ad + b'd'bc \\ \Leftrightarrow (a'd' + b'c')bd &= b'd'(ad + bc) \\ \Leftrightarrow (a'd' + b'c', b'd')\, R(D)(ad + bc, bd) & \\ \Leftrightarrow [(a'd' + b'c', b'd')] &= [(ad + bc, bd)] \\ \Leftrightarrow [(a',b')] \oplus [(c',d')] &= [(a,b)] \oplus [(c,d)]. \end{aligned}$$

Kohtien 1-2 nojalla joukko $Q(D)$ varustettuna operaatiolla $(\oplus)$ on hyvin määritelty. Osoitetaan operaatio $(\odot)$ hyvin määritellyksi vastaavasti eli käymällä kohdat 1 ja 2 läpi operaation $(\odot)$ suhteen.

1. Olkoot $[(a,b)],[(c,d)] \in Q(D)$. Nyt $ac \in D$, ja koska $b, d \in D \setminus \{0_D\}$, niin $bd \in D \setminus \{0_D\}$. Siis $[(a,b)] \odot [(c,d)] = [(ac, bd)] \in Q(D)$.

2. Olkoot $[(a,b)],[(a',b')],[(c,d)],[(c',d')] \in Q(D)$ sekä $[(a,b)] = [(a',b')]$ ja $[(c,d)] = [(c',d')]$. On siis voimassa $ab' = ba'$ ja $cd' = dc'$. Käyttäen operaatiota $(\odot)$ operoidaan yhtälön $ab' = ba'$ vasenta puolta alkiolla

cd' ja oikeaa puolta alkiolla dc'. Saadaan

$$\begin{aligned} ab'cd' &= ba'dc' \\ \Leftrightarrow a'bc'd &= b'ad'c \\ \Leftrightarrow a'c'bd &= b'd'ac \\ \Leftrightarrow (a'c', b'd')\, R(D)(ac, bd) & \\ \Leftrightarrow [(a'c', b'd')] &= [(ac, bd)] \\ \Leftrightarrow [(a', b')] \odot [(c', d')] &= [(a, b)] \odot [(c, d)]. \end{aligned}$$

Kohtien 1-2 nojalla joukko $Q(D)$ varustettuna operaatiolla $(\odot)$ on hyvin määritelty. □

Esimerkki 2.7. Verrataan joukkoa $Q(\mathbb{Z})$ varustettuna laskuoperaatioilla $(\oplus)$ ja $(\odot)$ joukkoon $\mathbb{Q}$ varustettuna luonnollisilla laskuoperaatioilla $(+)$ ja $(\cdot)$. Asetetaan kuvaus $f : Q(\mathbb{Z}) \to \mathbb{Q}, \quad f([(a, b)]) = \frac{a}{b}$. Nyt

1.

$$\begin{aligned} f([(a, b)] \oplus [(c, d)]) = f([(ad + bc, bd)]) &= \frac{ad + bc}{bd} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{a}{b} + \frac{c}{d} \\ &= f([(a, b)]) + f([(c, d)]) \end{aligned}$$

kaikilla $a, c \in \mathbb{Z}, b, d \in \mathbb{Z} \setminus \{0\}$.

2.

$$f([(a, b)] \odot [(c, d)]) = f([(ac, bd)]) = \frac{ac}{bd} = \frac{a}{b} \cdot \frac{c}{d} = f([(a, b)]) \cdot f([(c, d)])$$

kaikilla $a, c \in \mathbb{Z}, b, d \in \mathbb{Z} \setminus \{0\}$.

3.

$$f[(a, a)] = \frac{a}{a} = \frac{1}{1}$$

kaikilla $a \in \mathbb{Z} \setminus \{0\}$.

Osoitetaan, että kuvaus f on bijektio.

4. Olkoot $[(a, b)], [(c, d)] \in Q(\mathbb{Z})$. Tällöin

$$f([(a, b)]) = f([(c, d)]) \Leftrightarrow \frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc \Leftrightarrow [(a, b)] = [(c, d)].$$

Siis kuvaus f on injektio. Toisaalta kuvaus f on myös hyvin määritelty.

5. Olkoon $\frac{a}{b} \in \mathbb{Q}$. Tällöin $a \in \mathbb{Z}, b \in \mathbb{Z}\setminus\{0\}$. Nyt

$$f([(a,b)]) = \frac{a}{b}.$$

Siis kuvaus f on surjektio.

Lause 2.8. Kolmikko $(Q(D), \oplus, \odot)$ on kunta.

Todistus. Käyttäen Määritelmiä 1.7 ja 1.8 osoitetaan aluksi, että kolmikko $(Q(D), \oplus, \odot)$ on kommutatiivinen rengas. Tätä varten osoitetaan toteutuviksi seuraavat ehdot:

1. Pari $(Q(D), \oplus)$ on Abelin ryhmä.
2. Pari $(Q(D), \odot)$ toteuttaa Määritelmän 1.5 kohdat 1-3 (monoidi) ja 5 (kommutatiivisuus).
3. Määritelmän 1.7 mukaiset osittelulait ovat voimassa kolmikolle $(Q(D), \oplus, \odot)$.

Käydään ehdot läpi:

1. (a) Olkoot $[(a,b)], [(c,d)] \in Q(D)$. Nyt $[(a,b)] \oplus [(c,d)] \in Q(D)$ Lemman 2.6 nojalla.

   (b) Olkoot $[(a,b)], [(c,d)], [(e,f)] \in Q(D)$. Nyt

$$\begin{aligned}
&([(a,b)] \oplus [(c,d)]) \oplus [(e,f)] = [(ad+bc, bd)] \oplus [(e,f)] \\
&= [((ad+bc)f + bde, bdf)] = [(adf + bcf + bde, bdf)] \\
&= [(adf + b(cf+de), bdf)] = [(a,b)] \oplus [(cf+de, df)] \\
&= [(a,b)] \oplus ([(c,d)] \oplus [(e,f)]).
\end{aligned}$$

   (c) Olkoot $[(a,b)] \in Q(D)$ ja $c \in D\setminus\{0_D\}$. Nyt $[(0_D, c)] \in Q(D)$ ja

$$[(a,b)] \oplus [(0_D,c)] = [(ac + b0_D, bc)] = [(ac, bc)].$$

   Edelleen

$$abc = abc \Leftrightarrow abc = bac \Leftrightarrow [(a,b)] = [(ac,bc)] = [(a,b)] \oplus [(0_D,c)].$$

   Vastaavasti

$$[(0_D,c)] \oplus [(a,b)] = [(0_D b + ca, cb)] = [(ca,cb)] = [(ac,bc)] = [(a,b)].$$

   Siis alkio $[(0_D, c)]$ on nolla-alkio.

(d) Olkoon $[(a,b)] \in Q(D)$. Nyt $[(-a,b)] \in Q(D)$ ja

$$\begin{aligned}[(a,b)] \oplus [(-a,b)] &= [(ab + b(-a), bb)] = [(ba + b(-a), bb)] \\ &= [(b(a + (-a)), bb)] = [(b0_D, bb)] = [(0_D, bb)] \\ &= 0_{Q(D)}.\end{aligned}$$

Vastaavasti

$$\begin{aligned}[(-a,b)] \oplus [(a,b)] &= [(-ab + ba, bb)] = [(b(-a) + ba, bb)] \\ &= [(b(-a + a), bb)] = [(b0_D, bb)] = [(0_D, bb)] \\ &= 0_{Q(D)}.\end{aligned}$$

Siis alkio $[(-a,b)]$ on alkion $[(a,b)]$ vasta-alkio.

(e) Olkoot $[(a,b)], [(c,d)] \in Q(D)$. Tällöin

$$[(a,b)] \oplus [(c,d)] = [(ad + bc, bd)] = [(cb + da, db)] = [(c,d)] \oplus [(a,b)].$$

Kohtien (a)-(e) nojalla $(Q(D), \oplus)$ on Abelin ryhmä.

2. (a) Olkoot $[(a,b)], [(c,d)] \in Q(D)$. Tällöin $[(a,b)] \odot [(c,d)] \in Q(D)$ Lemman 2.6 nojalla.

(b) Olkoot $[(a,b)], [(c,d)], [(e,f)] \in Q(D)$. Tällöin

$$\begin{aligned}&[(a,b)] \odot ([(c,d)] \odot [(e,f)]) = [(a,b)] \odot [(ce, df)] = [(ace, bdf)] \\ &= [(ac, bd)] \odot [(e,f)] = ([(a,b)] \odot [(c,d)]) \odot [(e,f)].\end{aligned}$$

(c) Olkoot $[(a,b)] \in Q(D)$ ja $c \in D \setminus \{0_D\}$. Nyt $[(c,c)] \in Q(D) \setminus \{0_{Q(D)}\}$ ja

$$[(a,b)] \odot [(c,c)] = [(ac, bc)] = [(a,b)]$$

kohdan 1.(c) nojalla. Toisaalta $[(ac, bc)] = [(ca, cb)]$, joten $[(a,b)] \odot [(c,c)] = [(c,c)] \odot [(a,b)]$. Siis $[(c,c)]$ on ykkösalkio.

(d) Olkoot $[(a,b)], [(c,d)] \in Q(D)$. Nyt

$$[(a,b)] \odot [(c,d)] = [(ac, bd)] = [(ca, db)] = [(c,d)] \odot [(a,b)].$$

Kohtien (a)-(c) nojalla pari $(Q(D), \odot)$ on monoidi ja kohdan (d) nojalla kommutatiivinen.

3. Osoitetaan, että osittelulait ovat voimassa.

(a) Olkoot $[(a,b)],[(c,d)],[(e,f)] \in Q(D)$. Nyt

$$\begin{aligned}
&[(a,b)] \odot ([(c,d)] \oplus [(e,f)]) = [(a,b)] \odot [(cf+de,df)] \\
&= [(a(cf+de),bdf)] = [(acf+ade,bdf)] \\
&= 1_{Q(D)} \odot [(acf+ade,bdf)] = [(b,b)] \odot [(acf+ade,bdf)] \\
&= [(b(acf+ade),bbdf)] = [(bacf+bade,bbdf)] \\
&= [(acbf+bdae,bdbf)] = [(ac,bd)] \oplus [(ae,bf)] \\
&= ([(a,b)] \odot [(c,d)]) \oplus ([(a,b)] \odot [(e,f)]).
\end{aligned}$$

(b) Olkoot $[(a,b)],[(c,d)],[(e,f)] \in Q(D)$. Nyt

$$\begin{aligned}
&([(a,b)] \oplus [(c,d)]) \odot [(e,f)] = [(ad+bc,bd)] \odot [(e,f)] \\
&= [((ad+bc)e,bdf)] = [(ade+bce,bdf)] \\
&= 1_{Q(D)} \odot [(ade+bce,bdf)] = [(f,f)] \odot [(ade+bce,bdf)] \\
&= [(f(ade+bce),fbdf)] = [(fade+fbce,fbdf)] \\
&= [(aedf+bfce,bfdf)] = [(ae,bf)] \oplus [(ce,df)] \\
&= ([(a,b)] \odot [(e,f)]) \oplus ([(c,d)] \odot [(e,f)]).
\end{aligned}$$

Kohtien (a)-(b) nojalla osittelulait ovat voimassa.

Kohtien 1-3 nojalla kolmikko $(Q(D),\oplus,\odot)$ on kommutatiivinen rengas. Luvun alussa havaittiin, että kommutatiivinen rengas R on kunta, mikäli jokaiselle joukon $R\setminus\{0_R\}$ alkiolle löytyy käänteisalkio samasta joukosta. Kolmikon $(Q(D),\oplus,\odot)$ ollessa kommutatiivinen rengas kunnan määritelmä täyttyy, jos pari $(Q(D)\setminus\{0_{Q(D)}\},\odot)$ toteuttaa Määritelmän 1.5 kohdan 4 (käänteisalkio). Olkoon $[(a,b)] \in Q(D)\setminus\{0_{Q(D)}\}$. Nyt $[(b,a)] \in Q(D)\setminus\{0_{Q(D)}\}$ ja

$$\begin{aligned}
[(a,b)] \odot [(b,a)] &= [(ab,ba)] = [(ab,ab)] \\
&= 1_{Q(D)} \\
&= [(ba,ba)] = [(ba,ab)] = [(b,a)] \odot [(a,b)].
\end{aligned}$$

Siis $[(b,a)]$ on alkion $[(a,b)]$ käänteisalkio. Näin ollen kommutatiivinen rengas $(Q(D),\oplus,\odot)$ on kunta. □

Määritelmä 2.9. Kuntaa $Q(D)$ tai sen kanssa isomorfista kuntaa kutsutaan *kokonaisalueen D osamääräkunnaksi* tai lyhyesti *osamääräkunnaksi.*

Esimerkki 2.10. Kunta $\mathbb{Q}$ on kokonaisalueen $\mathbb{Z}$ osamääräkunta. Tämä seuraa siitä, että Esimerkin 2.7 ja Määritelmien 1.11, 1.12 ja 1.19 nojalla on olemassa isomorfismi $f : Q(\mathbb{Z}) \to \mathbb{Q}$.

Tähän mennessä on osoitettu, että jokaisesta kokonaisalueesta saadaan johdettua kunta. Jotta osamääräkunnan määritelmä olisi mielekäs, on vielä todistettava, että osamääräkunnasta löytyy vastine jokaiselle kokonaisalueen alkiolle.

Lause 2.11. Olkoon $Q(D)$ kokonaisalueen D osamääräkunta. Tällöin on olemassa sellainen osamääräkunnan $Q(D)$ osajoukko H, että $D \cong H$. Erityisesti $H = \big\{[(\mathrm{a}, 1_D)] \;\big|\; \mathrm{a} \in D\big\}$ on tällainen joukko.

Todistus. Valitaan $H = \big\{[(a, 1_D)] \;\big|\; a \in D\big\}$. Osoitetaan ensin, että joukko H on renkaan $Q(D)$ alirengas käyttäen Lausetta 1.10. Tämän jälkeen osoitetaan käyttäen Määritelmiä 1.11, 1.12 ja 1.19, että $D \cong H$.

1. Nyt $\emptyset \neq H \subseteq Q(D)$. Osoitetaan, että kolmikko $(H, \oplus, \odot)$ on renkaan $Q(D)$ alirengas.

   (a) Olkoot $[(a, 1_D)], [(b, 1_D)] \in H$. Alkion $[(b, 1_D)]$ vasta-alkio on $[(-b, 1_D)]$. Nyt

   $$\begin{aligned}[(a, 1_D)] \oplus [(-b, 1_D)] &= [(a1_D + 1_D(-b), 1_D1_D)] \\ &= [(a + (-b), 1_D)] \in H.\end{aligned}$$

   (b) Olkoot $[(a, 1_D)], [(b, 1_D)] \in H$. Nyt

   $$[(a, 1_D)] \odot [(b, 1_D)] = [(ab, 1_D1_D)] = [(ab, 1_D)] \in H.$$

   (c) Nyt $1_{Q(D)} = [(a, a)] = [(1_D, 1_D)] \in H$ kaikilla $a \in D$ Lauseen 2.8 todistuksen kohdan 1.(c) nojalla.

   Kohtien (a)-(c) nojalla kolmikko $(H, \oplus, \odot)$ on renkaan $(Q(D), \oplus, \odot)$ alirengas.

2. Asetetaan kuvaus

   $$f : (D, +, \cdot) \to (H, \oplus, \odot), \quad f(a) = [(a, 1_D)].$$

   Osoitetaan, että kuvaus f on rengasisomorfismi.

   (a) Osoitetaan, että kuvaus f on rengashomomorfismi.

      i. Olkoot $a, b \in D$. Nyt

      $$\begin{aligned}f(a + b) &= [(a + b, 1_D)] \\ &= [(a1_D + 1_Db, 1_D1_D)] \\ &= [(a, 1_D)] \oplus [(b, 1_D)] \\ &= f(a) \oplus f(b).\end{aligned}$$

ii. Olkoot $a, b \in D$. Nyt

$$\begin{aligned} f(ab) &= [(ab, 1_D)] \\ &= [(ab, 1_D 1_D)] \\ &= [(a, 1_D)] \odot [(b, 1_D)] \\ &= f(a) \odot f(b). \end{aligned}$$

iii. Nyt

$$\begin{aligned} f(1_D) &= [(1_D, 1_D)] \\ &= 1_{Q(D)}. \end{aligned}$$

Kohtien i-iii nojalla kuvaus f on rengashomomorfismi.

(b) Osoitetaan, että kuvaus f on bijektio.

i. Olkoon $a, b \in D$. Nyt

$$f(a) = f(b) \Leftrightarrow [(a, 1_D)] = [(b, 1_D)] \Leftrightarrow a1_D = 1_D b \Leftrightarrow a = b.$$

Siis kuvaus f on injektio ja myös hyvin määritelty.

ii. Olkoon $[(a, 1_D)] \in H$. Tällöin $a \in D$ ja

$$f(a) = [(a, 1_D)].$$

Näin ollen kuvaus f on surjektio.

Kohtien i-ii nojalla kuvaus f on bijektio.

Kohtien (a)-(b) nojalla kuvaus f on rengasisomorfismi.

Kohtien 1-2 nojalla $D \cong H$. □

3 Osamääräkunnan isomorfismit

Tarkastellaan kokonaisalueen D osamääräkunnan $Q(D)$ suhdetta kuntaan K, jolla on kokonaisalueen D kanssa isomorfinen osajoukko. Tämän osajoukon tulee olla myös kokonaisalue. Esitetään aluksi erikoistapaus, jossa kunta K on osamääräkunta. Laajennetaan lopuksi tulos koskemaan mitä tahansa kuntaa, joka täyttää ehdon. Seuraavan lemman, lauseen ja seurauksen muodostamisen apuna on käytetty lähdettä [1]. Todistukset on tehty itsenäisesti.

Lemma 3.1. Olkoot D ja H kokonaisalueita. Jos $D \cong H$, niin $Q(D) \cong Q(H)$.

Todistus. Olkoot D ja H sellaisia kokonaisalueita, että $D \cong H$. Todistetaan väite käyttäen Määritelmiä 1.11, 1.12 ja 1.19. Koska kokonaisalueet D ja H ovat isomorfiset, niin on olemassa isomorfismi

$$g : D \to H, \quad g(a) = a_g$$

ja kuvaus

$$f : Q(D) \to Q(H), \quad f([(a, b)]) = [(a_g, b_g)],$$

missä kokonaisalueen D alkiot a ja b kuvautuvat alkioiksi a_g ja b_g kuvauksen g mukaisesti. Lauseen 1.15 kohdasta 2 ja isomorfismin g injektiivisyydestä seuraa, että $g(a) \neq 0_H$, kun $a \neq 0_D$. Kuvaus f tuottaa siis aina joukon $Q(H)$ alkion. Osoitetaan, että kuvaus f on hyvin määritelty. Olkoot $[(a, b)], [(c, d)] \in Q(D)$. Käyttäen Määritelmän 1.11 kohtaa 2 ja kuvauksen g bijektiivisyyttä saadaan

$$\begin{aligned}[(a, b)] = [(c, d)] &\Leftrightarrow ad = bc \Leftrightarrow (ad)_g = (bc)_g \Leftrightarrow a_g d_g = b_g c_g \\ &\Leftrightarrow [(a_g, b_g)] = [(c_g, d_g)] \Leftrightarrow f([(a, b)]) = f([(c, d)]).\end{aligned}$$

Osoitetaan että kuvaus f on isomorfismi.

1. Osoitetaan, että kuvaus f on homomorfismi.

   (a) Olkoot $[(a, b)], [(c, d)] \in Q(D)$. Tällöin

$$\begin{aligned}f([(a, b)] \oplus [(c, d)]) &= f([(ad + bc, bd)]) \\ &= [((ad + bc)_g, (bd)_g)] \\ &= [(a_g d_g + b_g c_g, b_g d_g)] \\ &= [(a_g, b_g)] \oplus [(c_g, d_g)] \\ &= f([(a, b)]) \oplus f([(c, d)]).\end{aligned}$$

(b) Olkoot $[(a,b)], [(c,d)] \in Q(D)$. Tällöin

$$\begin{aligned} f([(a,b)] \odot [(c,d)]) &= f([(ac,bd)]) \\ &= [((ac)_g, (bd)_g)] \\ &= [(a_g c_g, b_g d_g)] \\ &= [(a_g, b_g)] \odot [(c_g, d_g)] \\ &= f([(a,b)]) \odot f([(c,d)]). \end{aligned}$$

(c) Nyt

$$f(1_{Q(D)}) = f([(a,a)]) = [(a_g, a_g)] = 1_{Q(H)}$$

kaikilla $a \in D$.

Kohtien (a)-(c) nojalla kuvaus f on homomorfismi.

2. Osoitetaan, että kuvaus f on bijektio.

(a) Todistuksen alussa osoitettiin, että kuvaus f on hyvin määritelty. Samalla tultiin osoittaneeksi, että kuvaus f on injektio.

(b) Koska kuvaus g on isomorfismi, niin jokainen kokonaisalueen H alkio on muotoa a_g kuvauksen g mukaisesti. Näin ollen jokainen osamääräkunnan $Q(H)$ alkio on muotoa $[(a_g, b_g)]$. Lisäksi $b \neq 0_D$, kun $b_g \neq 0_H$, joten $[(a,b)] \in Q(D)$ ja

$$f([(a,b)]) = [(a_g, b_g)],$$

kun $[(a_g, b_g)] \in Q(H)$. Siis kuvaus f on surjektio.

Kohtien (a)-(b) nojalla kuvaus f on bijektio.

Kohtien 1-2 nojalla kuvaus f on isomorfismi. □

Lause 3.2. Olkoot D kokonaisalue, $Q(D)$ kokonaisalueen D osamääräkunta ja K kunta. Olkoon H sellainen kunnan K alirengas, että H on kokonaisalue. Jos $D \cong H$, niin on olemassa sellainen kunnan K alikunta L, että $Q(D) \cong L$.

Todistus. Olkoot D, $Q(D)$, K ja H lauseen oletuksen mukaiset. Olkoon $D \cong H$. Asetetaan kokonaisalueen H osamääräkunta $Q(H)$. Lemman 3.1 nojalla $Q(D) \cong Q(H)$. Riittää siis osoittaa, että on olemassa sellainen kunnan K alikunta L, että $Q(H) \cong L$. Asetetaan

$$L = \left\{ ab^{-1} \;\middle|\; a, b \in H, b \neq 0_K \right\} \subseteq K.$$

Osoitetaan, että L on kunnan K alikunta Lauseen 1.18 avulla.

1. Koska H on kunnan K alirengas, niin $0_K, 1_K \in H$. Renkaan ykkösalkion yksikäsitteisyyden nojalla $0_K \neq 1_K$. Nyt $1_K = 1_K 1_K = 1_K 1_K^{-1} \in L$ ja $0_K = 0_K 1_K = 0_K 1_K^{-1} \in L$ eli joukossa L on vähintään kaksi alkiota.

2. Olkoot $ab^{-1}, cd^{-1} \in L$, jolloin $a, c, \in H$ ja $b, d \in H \setminus \{0_K\}$. Käyttäen Lauseen 1.15 kohtia 3 ja 5, Lauseen 1.6 kohtaa 1 ja kunnan K kommutatiivisuutta saadaan

$$\begin{aligned} ab^{-1} + (-(cd^{-1})) &= ab^{-1} + (-c)d^{-1} = a1_K b^{-1} + (-c)d^{-1}1_K \\ &= add^{-1}b^{-1} + (-c)d^{-1}bb^{-1} = (add^{-1} + (-c)d^{-1}b)b^{-1} \\ &= (add^{-1} + (-c)bd^{-1})b^{-1} = (ad + (-c)b)d^{-1}b^{-1} \\ &= (ad + (-c)b)(bd)^{-1} \in L. \end{aligned}$$

3. Olkoot $ab^{-1}, cd^{-1} \in L$ ja $cd^{-1} \neq 0_K$. Tällöin $a \in H$ ja $b, c, d \in H \setminus \{0_K\}$. Käyttäen Lauseen 1.6 kohtaa 2 saadaan

$$\begin{aligned} (ab^{-1})(cd^{-1})^{-1} &= ab^{-1}(d^{-1})^{-1}c^{-1} = ab^{-1}dc^{-1} = adb^{-1}c^{-1} \\ &= (ad)(cb)^{-1} \in L. \end{aligned}$$

Kohtien 1-3 nojalla L on kunnan K alikunta. Asetetaan seuraavaksi kuvaus

$$f : Q(H) \to L, \quad f([(a, b)]) = ab^{-1}$$

ja osoitetaan, että se on isomorfismi. Perustellaan aluksi, että kuvaus f on hyvin määritelty. Olkoot $[(a, b)], [(c, d)] \in Q(H)$. Nyt

$$\begin{aligned} [(a, b)] = [(c, d)] &\Leftrightarrow ad = bc \Leftrightarrow ad(b^{-1}d^{-1}) = bc(b^{-1}d^{-1}) \Leftrightarrow ab^{-1} = cd^{-1} \\ &\Leftrightarrow f([(a, b)]) = f([(c, d)]). \end{aligned}$$

Osoitetaan, että kuvaus f on isomorfismi.

4. Osoitetaan, että kuvaus f on homomorfismi.

   (a) Olkoot $[(a, b)], [(c, d)] \in Q(H)$. Nyt

$$\begin{aligned} f([(a, b)] \oplus [(c, d)]) &= f([(ad + bc, bd)]) \\ &= (ad + bc)(bd)^{-1} \\ &= (ad + bc)(d^{-1}b^{-1}) \\ &= add^{-1}b^{-1} + bcd^{-1}b^{-1} \\ &= ab^{-1} + cd^{-1} \\ &= f([(a, b)]) + f([(c, d)]). \end{aligned}$$

(b) Olkoot $[(a,b)], [(c,d)] \in Q(H)$. Nyt

$$\begin{aligned} f([(a,b)] \odot [(c,d)]) &= f([(ac,bd)]) \\ &= ac(bd)^{-1} \\ &= acd^{-1}b^{-1} \\ &= (ab^{-1})(cd^{-1}) \\ &= f([(a,b)])f([(c,d)]). \end{aligned}$$

(c) Nyt

$$\begin{aligned} f(1_{Q(H)}) &= f([(a,a)]) \\ &= aa^{-1} \\ &= 1_K = 1_L \end{aligned}$$

kaikilla $a \in H$.

5. Osoitetaan, että kuvaus f on bijektio.

   (a) Todistuksen alun kohdan, jossa osoitettiin kuvaus f hyvin määritellyksi, nojalla kuvaus f on injektio.

   (b) Olkoon $ab^{-1} \in L$. Tällöin $a \in H$ ja $b \in H \setminus \{0_K\}$, joten $[(a,b)] \in Q(H)$ ja

   $$f([(a,b)]) = ab^{-1}.$$

   Näin ollen kuvaus f on surjektio.

   Kohtien (a)-(b) nojalla kuvaus f on bijektio.

Kohtien 4-5 nojalla kuvaus f on isomorfismi. Siis $Q(H) \cong L$. Koska $Q(D) \cong Q(H)$, niin $Q(D) \cong L$. □

Seuraus 3.3. Kokonaisalueen D osamääräkunta $Q(D)$ on suppein kunta, jolla on kokonaisalueen D kanssa isomorfinen osajoukko.

Todistus. Seuraa suoraan Lauseesta 3.2. □

Lähdeluettelo

[1] John B. Fraleigh. A First Course in Abstract Algebra. Sixth Edition. Addison-Wesley. s. 277-283.

[2] Markku Niemenmaa, Kari Myllylä, Juha-Matti Tirilä, Antti Torvikoski, Topi Törmä. 802354A Lukuteoria ja ryhmät. Luentorunko. Kevät 2015. s. 3, 19-38.

[3] Markku Niemenmaa, Kari Myllylä, Juha-Matti Tirilä, Antti Torvikoski, Topi Törmä. 802355A Renkaat, kunnat ja polynomit. Luentorunko. Syksy 2014.