Tekijäryhmä, tekijärengas ja kuntalaajennus

Pro Gradu-tutkielma
Juho Karekivi
Matematiikan tutkinto-ohjelma
Oulun yliopisto
Kevät 2020

Sisältö

1 Johdanto **2**

2 Ryhmän perusasioita **3**

3 Tekijäryhmä **8**

4 Renkaan perusasioita **12**

5 Tekijärengas **18**

6 Kuntien perusasioita **28**

7 Kuntalaajennus **30**

Lähdeluettelo **36**

1 Johdanto

Tutkielman ideana on luvuissa 2, 4 ja 6 esitellä ryhmän, renkaan ja kunnan perusasioita. Perusasioiden esittelyn jälkeen luvuissa 3, 5 ja 7 käydään läpi tekijäryhmän, tekijärenkaan ja kuntalaajennuksen rakenteita sekä ominaisuuksia. Lukijan tulisi omata riittävä matemaattinen perustietämys algebran peruskäsitteistä.

Tutkielma lähtee liikkeelle luvussa 2 ryhmän määritelmästä, josta edetään aliryhmän kautta sivuluokkiin. Sivuluokat ovat olennainen osa tutkielmaa, koska niiden avulla rakennetaan tekijäryhmä. Ryhmän $(\mathbb{Z}, +)$ aliryhmä $(3\mathbb{Z}, +)$ ansaitsee erityismaininnan, koska tätä aliryhmää ja varsinkin sen vasempia sivuluokkia käsitellään paljon tutkielmassa.

Luvussa 3 määritellään sivuluokkien välinen operaatio ja todistetaan operaation olevan hyvin määritelty. Operaation avulla muodostetaan tekijäryhmä, jonka todistetaan olevan ryhmärakenne. Todistetaan myös, että ryhmän ominaisuudet periytyvät tekijäryhmälle.

Luvussa 4 lähdetään liikkeelle renkaan määritelmästä, josta päästään ideaalin määritelmään. Molemmat edellä mainitut määritelmät ovat tärkeitä, koska niiden avulla muodostetaan tekijärengas.

Luvussa 5 määritellään tekijärenkaan muodostamiseen tarvittavat operaatiot, todistetaan, että ne ovat hyvin määriteltyjä ja muodostetaan tekijärengas. Lisäksi todistetaan, että tekijärengas on todella rengasrakenne ja renkaan ominaisuudet periytyvät tekijärenkaalle.

Luvussa 6 esitellään kunnan määritelmä. Lisäksi todistetaan, ettei kokonaisluvuista muodostettu rengas ole kunta.

Luvussa 7 todistetaan, että kun tekijärengas muodostetaan maksimaalisen ideaalin suhteen, niin tekijärengas on kuntarakenne. Tämä ehkä koko tutkielman merkittävin tulos todistetaan kahta eri reittiä pitkin.

Tutkielmassa esitellään useita esimerkkejä, joilla havainnollistetaan rakenteiden ominaisuuksia. Tutkielmassa esitetyt asiat pohjautuvat lähteeseen [3] J. Rotman Advanded Modern Algebra, luentomonisteisiin [1] ja [2] sekä omaan pohdintaan. Omaa kandidaadin tutkielmaa on myös hyödynnetty jollain tasolla.

2 Ryhmän perusasioita

Tässä luvussa esitellään ryhmiin liittyviä perusasioita, joita on käyty läpi Algebran perusteet -kurssilla. Todistukset sivuutetaan.

Määritelmä 2.1. Olkoot G epätyhjä joukko ja $(*)$ joukon G operaatio. Pari $(G, *)$ on *ryhmä*, mikäli seuraavat neljä ehtoa toteutuvat:

1. Operaatio $(*)$ on *binäärinen* joukossa G eli

   $$a * b \in G$$

   kaikilla $a, b \in G$ ja $a * b$ on yksikäsitteinen.

2. Operaatio $(*)$ on *assosiatiivinen* joukossa G eli

   $$(a * b) * c = a * (b * c)$$

   kaikilla $a, b, c \in G$.

3. Joukossa G on olemassa *neutraalialkio* e siten, että

   $$a * e = e * a = a$$

   kaikilla $a \in G$.

4. Jokaiselle joukon G alkiolle a on olemassa *käänteisalkio* $a^{-1} \in G$ siten, että

   $$a * a^{-1} = a^{-1} * a = e.$$

Määritelmä 2.2. Olkoon $(G,*)$ ryhmä. Ryhmää G sanotaan *kommutatiiviseksi* ryhmäksi eli *Abelin ryhmäksi*, jos operaatio $(*)$ on kommutatiivinen eli

$$a * b = b * a$$

kaikilla $a, b \in G$.

Jatkossa käytetään merkintää $a * b = ab$.

Lause 2.3. *Olkoot G ryhmä ja $a, b, c \in G$. Tällöin*

1. *Neutraalialkio e on yksikäsitteinen.*
2. *Kunkin alkion a käänteisalkio a^{-1} on yksikäsitteinen.*
3. *Jos $ab = ac$, niin $b = c$.*
4. *Jos $ba = ca$, niin $b = c$.*

Esimerkki 2.4. Pari $(\mathbb{Z}, +)$ on ryhmä. Pari $(\mathbb{Z}, \cdot)$ ei ole ryhmä.

Todistus. Olkoot $a, b, c \in \mathbb{Z}$.

1. Nyt $a + b \in \mathbb{Z}$, eli operaatio $(+)$ on binäärinen.
2. Nyt
$$\begin{aligned} & a + (b + c) \\ &= a + b + c \\ &= (a + b) + c, \end{aligned}$$
eli operaatio $(+)$ on assosiatiivinen.
3. Nyt $0 \in \mathbb{Z}$. Lisäksi
$$0 + a = a + 0 = a.$$
Näin ollen 0 on joukon $\mathbb{Z}$ neutraalialkio.
4. Nyt selvästi $-a \in \mathbb{Z}$. Lisäksi
$$a + (-a) = 0$$
ja
$$-a + a = 0.$$
Näin ollen $-a$ on alkion a käänteisalkio.

Täten pari $(\mathbb{Z}, +)$ on ryhmä.

Pari $(\mathbb{Z}, \cdot)$ ei ole ryhmä, koska jokaiselle joukon $\mathbb{Z}$ alkiolle ei ole olemassa joukkoon $\mathbb{Z}$ kuuluvaa käänteisalkiota. □

Määritelmä 2.5. Olkoon $(G, *)$ ryhmä, $H \subseteq G$ ja $H \neq \emptyset$. Jos pari $(H, *)$ täyttää ryhmän määritelmän, kutsutaan sitä *ryhmän* $(G, *)$ *aliryhmäksi*. Merkitään $H \leq G$.

Lause 2.6. *Olkoot G ryhmä, $H \subseteq G$ ja $H \neq \emptyset$. Joukko H on ryhmän G aliryhmä, jos ja vain jos seuraavat ehdot toteutuvat:*

1. *Jos $a, b \in H$, niin $ab \in H$.*
2. *Jos $a \in H$, niin $a^{-1} \in H$.*

Lause 2.7. *Olkoot G ryhmä, $H \subseteq G$ ja $H \neq \emptyset$. Joukko H on ryhmän G aliryhmä, jos ja vain jos*

$$a * b^{-1} \in H$$

kaikilla $a, b \in H$.

Esimerkki 2.8. Joukko $3\mathbb{Z} = \{3z \mid z \in \mathbb{Z}\}$. Tällöin $(3\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.

Todistus. Selvästi $3\mathbb{Z} \subseteq \mathbb{Z}$ ja $3 \in 3\mathbb{Z}$, joten $3\mathbb{Z} \neq \emptyset$. Olkoot $3k, 3l \in 3\mathbb{Z}$. Nyt

$$3k + (-3l) = 3\underbrace{(k - l)}_{\in \mathbb{Z}} \in 3\mathbb{Z},$$

Lauseen 2.7 nojalla $(3\mathbb{Z}, +) \leq (\mathbb{Z}, +)$. □

Määritelmä 2.9. Olkoon $(H, *) \leq (G, *)$ ja $a \in G$. Joukkoa

$$aH = \{a * h \mid h \in H\}$$

kutsutaan *alkion a määräämäksi aliryhmän H vasemmaksi sivuluokaksi*. Vastaavasti joukkoa $Ha = \{h * a \mid h \in H\}$ kutsutaan *alkion a määräämäksi aliryhmän H oikeaksi sivuluokaksi*.

Lause 2.10. *Olkoot G ryhmä, $H \leq G$ ja $a, b \in G$. Tällöin*

1. $a \in bH \Leftrightarrow aH = bH$,
2. $a \in Hb \Leftrightarrow Ha = Hb$.

Määritelmä 2.11. Olkoot G ryhmä, $a \in G$ ja $k \in \mathbb{Z}_+$. Tällöin

1. a^k tarkoittaa, että alkiota a operoidaan itsensä kanssa k kertaa.
2. a^{-k} tarkoittaa alkion a^k käänteisalkiota eli $(a^k)^{-1} = a^{-k}$.
3. a^0 tarkoittaa neutraalialkiota e.

Lause 2.12. *Olkoon G ryhmä, $a \in G$ ja $H = \{a^k \mid k \in \mathbb{Z}\}$. Tällöin $H \leq G$.*

Määritelmä 2.13. Olkoon G ryhmä ja $a \in G$. Ryhmää

$$H = \{a^k \mid k \in \mathbb{Z}\}$$

kutsutaan *alkion a generoimaksi sykliseksi ryhmäksi*. Ryhmää merkitään $H = \langle a \rangle$.

Määritelmä 2.14. Olkoon $N \leq G$. Aliryhmää N kutsutaan *normaaliksi*, jos $aN = Na$ kaikilla $a \in G$. Merkitään $N \trianglelefteq G$.

Lause 2.15. *Ryhmän G aliryhmä N on normaali jos ja vain jos*

$$aNa^{-1} \subseteq N$$

kaikilla $a \in G$.

Lause 2.16. *Abelin ryhmän jokainen aliryhmä on normaali.*

Esimerkki 2.17. $(3\mathbb{Z}, +) \trianglelefteq (\mathbb{Z}, +)$.

Todistus. Esimerkin 2.8. nojalla $(3\mathbb{Z}, +) \leq (\mathbb{Z}, +)$. Olkoot $a, b \in \mathbb{Z}$. Nyt

$$a + b = b + a,$$

joten operaatio $(+)$ on kommutatiivinen joukossa $\mathbb{Z}$. Täten $(\mathbb{Z}, +)$ on Abelin ryhmä. Lauseen 2.16. nojalla $(3\mathbb{Z}, +) \trianglelefteq (\mathbb{Z}, +)$. □

Määritelmä 2.18. Olkoon G ryhmä. Ryhmän G alkioiden lukumäärää kutsutaan *ryhmän G kertaluvuksi* ja sitä merkitään $|G|$.

Lause 2.19. *Olkoot G äärellinen ryhmä, $H \leq G$ ja n aliryhmän H vasempien sivuluokkien lukumäärä ryhmän G suhteen. Tällöin*

$$|G| = n|H|,$$

toisin sanoen äärellisen ryhmän aliryhmän kertaluku jakaa ryhmän kertaluvun.

Esimerkki 2.20. Aliryhmän $(3\mathbb{Z}, +)$ vasemmat sivuluokat ryhmässä $(\mathbb{Z}, +)$ ovat

$$0 + 3\mathbb{Z} = \{0 + 3z \mid z \in \mathbb{Z}\},$$
$$1 + 3\mathbb{Z} = \{1 + 3z \mid z \in \mathbb{Z}\}$$

ja

$$2 + 3\mathbb{Z} = \{2 + 3z \mid z \in \mathbb{Z}\}.$$

Muita sivuluokkia ei ole, koska samaan sivuluokkaan kuuluvat alkiot määräävät saman sivuluokan.

3 Tekijäryhmä

Tässä luvussa perehdytään tekijäryhmän rakenteeseen ja ominaisuuksiin. Luvussa läpikäytävät asiat perustuvat teokseen [3] ja omaan pohdintaan.

Määritelmä 3.1. Olkoot $(N, *) \trianglelefteq (G, *)$. Määritellään operaatio $(*)$ sivuluokkien joukossa $\{aN \mid a \in G\}$ siten, että

$$aN * bN = (a * b)N.$$

Lause 3.2. *Operaatio $(*)$ on hyvin määritelty sivuluokkien joukossa.*

Todistus. Nyt tulee osoittaa, että operaatio $aN * bN = (a * b)N$ ei riipu sivuluokkien edustajista.Valitaan $a' \in aN$ ja $b' \in bN$, jolloin a' määrää saman sivuluokan kuin a eli $aN = a'N$ ja b' määrää saman sivuluokan kuin b eli $bN = b'N$.

On osoitettava, että $aN * bN = a'N * b'N$ eli $abN = a'b'N$.
Osoitetaan ensin, että $abN \subseteq a'b'N$.

Nyt $aN = a'N$, joten $a \in a'N$ ja edelleen on olemassa sellainen $n_1 \in N$, että $a = a'n_1$. Vastaavasti koska $b \in b'N$, on olemassa sellainen $n_2 \in N$, että $b = b'n_2$.

Olkoon $n \in N$. Koska operaatio on assosiatiivinen, niin

$$(ab)n = ((a'n_1)(b'n_2))n = a'n_1b'n_2n.$$

Nyt N on normaali aliryhmä, joten $Nb' = b'N$, ja edelleen koska $n_1 \in N$, niin on olemassa sellainen $n_3 \in N$, että $n_1b' = b'n_3$. Täten

$$(ab)n = a'n_1b'n_2n = a'b'n_3n_2n = a'b'n',$$

missä $n' = n_3n_2n \in N$. Siis $abN \subseteq a'b'N$.

Osoitetaan seuraavaksi, että $a'b'N \subseteq abN$.

Nyt $b'N = bN$, joten $b' \in bN$ ja edelleen on olemassa $n_4 \in N$ siten, että $b' = bn_4$. Samoin $a'N = aN$, joten $a' \in aN$ ja edelleen on olemassa $n_5 \in N$ siten, että $a' = an_5$.

Olkoon $n'' \in N$. Nyt

$$a'b'n'' = (an_5)(bn_4)n'' = an_5bn_4n''.$$

Edelleen N on normaali aliryhmä, joten on olemassa $n_6 \in N$ siten, että $n_5b = bn_6$. Täten

$$a'b'n'' = (an_5)(bn_4)n'' = an_5bn_4n'' = abn_6n_4n'' = abn''',$$

missä $n''' = n_6n_4n'' \in N$. Siis $a'b'N \subseteq abN$.

Nyt $abN \subseteq a'b'N$ ja $a'b'N \subseteq abN$, joten $abN = a'bN$. Täten operaatio $(*)$ on hyvin määritelty. □

Lause 3.3. *Olkoot* $(N, *) \trianglelefteq (G, *)$. *Tällöin pari* $(\{aN \mid a \in G\}, *)$ *on ryhmä.*

Todistus. Olkoot $bN, cN, dN \in \{aN \mid a \in G\}$.

1. Tällöin
$$bN * cN = \underbrace{(b * c)}_{\in G} N \in \{aN \mid a \in G\},$$
eli operaatio $(*)$ on binäärinen.

2. Nyt
$$\begin{aligned}
&(bN * cN) * dN \\
&= (b * c)N * dN \\
&= \underbrace{((b * c) * d)}_{\in G} N \\
&= (b * (c * d))N \\
&= bN * (c * d)N \\
&= bN * (cN * dN),
\end{aligned}$$
eli operaatio $(*)$ on assosiatiivinen.

3. Nyt $e \in G$, joten $eN \in \{aN \mid a \in G\}$. Tällöin

$$bN * eN = (b * e)N = bN$$

ja

$$eN * bN = (e * b)N = bN.$$

Näin ollen eN on neutraalialkio.

4. Olkoon $b \in G$, joten $b^{-1} \in G$ ja siten $b^{-1}N \in \{aN \mid a \in G\}$. Nyt

$$bN * b^{-1}N = (b * b^{-1})N = eN = N$$

ja

$$b^{-1}N * bN = (b^{-1} * b)N = eN = N.$$

Näin ollen $b^{-1}N$ on alkion bN käänteisalkio.

□

Määritelmä 3.4. Ryhmää $(\{aN \mid a \in G\}, *)$ kutsutaan *ryhmän G tekijäryhmäksi normaalin aliryhmän N suhteen.* Ryhmästä käytetään merkintää G/N.

Lause 3.5. *Olkoon ryhmä G äärellinen ja $N \trianglelefteq G$. Nyt tekijäryhmän G/N kertaluku on ryhmän G kertaluku jaettuna ryhmän N kertaluvulla, toisin sanoen*

$$|G/N| = \frac{|G|}{|N|}.$$

Todistus. Olkoot G äärellinen ryhmä ja $N \trianglelefteq G$. Nyt

$$|G/N| = |\{aN \mid a \in G\}|,$$

eli $|G/N|$ on normaalin aliryhmän N vasempien sivuluokkien lukumäärä ryhmässä G. Nyt lauseen 2.19. nojalla

$$|G| = |G/N||N|,$$

josta saadaan

$$|G/N| = \frac{|G|}{|N|}.$$

□

Lause 3.6. *Jos G on kommutatiivinen ryhmä ja $N \trianglelefteq G$, niin tekijäryhmä G/N on kommutatiivinen ryhmä.*

Todistus. Olkoon G kommutatiivinen ryhmä, $(N, *) \trianglelefteq (G, *)$ ja $a, b \in G$. Nyt

$$aN * bN = (a * b)N = (b * a)N = bN * aN,$$

sillä $a * b = b * a$ ryhmän G ollessa kommutatiivinen. □

Lause 3.7. *Jos G on syklinen ryhmä ja $N \trianglelefteq G$, niin tekijäryhmä G/N on syklinen ryhmä.*

Todistus. Olkoot $(G, *)$ syklinen ryhmä ja $(N, *) \trianglelefteq (G, *)$. Tällöin

$$G = \{g^k \mid k \in \mathbb{Z}\} = \langle g \rangle$$

jollakin alkiolla $g \in G$ ja $G/N = \{aN \mid a \in G\}$.

Olkoon $bN \in G/N$. Nyt ryhmän G alkiot ovat muotoa g^k, joten $b = g^l$ jollakin $l \in \mathbb{Z}$. Näin ollen

$$bN = g^l N = \underbrace{(g * ... * g)}_{l \text{ kpl}} N = \underbrace{gN * ... * gN}_{l \text{ kpl}} = (gN)^l.$$

Siis $G/N = \langle gN \rangle$. Eli, jos $a = g^k$, niin $aN = (gN)^k$. □

Esimerkki 3.8. Tekijäryhmän $(\mathbb{Z}/3\mathbb{Z}, +)$ alkiot ovat

$$0 + 3\mathbb{Z} = \{0 + 3z \mid z \in \mathbb{Z}\},$$

$$1 + 3\mathbb{Z} = \{1 + 3z \mid z \in \mathbb{Z}\}$$

ja

$$2 + 3\mathbb{Z} = \{2 + 3z \mid z \in \mathbb{Z}\}.$$

Tekijäryhmän $(\mathbb{Z}/3\mathbb{Z}, +)$ ryhmätaulu:

$+$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$1+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$
$2+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$

4 Renkaan perusasioita

Tässä luvussa esitellään renkaisiin liittyviä perusasioita, joita on käyty läpi Algebralliset rakenteet -kurssilla. Todistukset sivuutetaan.

Määritelmä 4.1. Kolmikko $(R, +, \cdot)$ on *rengas*, mikäli seuraavat ehdot toteutuvat:
1. Pari $(R, +)$ on Abelin ryhmä (kutsutaan *additiiviseksi ryhmäksi*, $(+)$ on *additiivinen operaatio*):

1. Operaatio $(+)$ on binäärinen joukossa R, toisin sanoen alkio $a + b$ sisältyy yksikäsitteisenä joukkoon R kaikilla joukon R alkioilla a ja b.

2. Operaatio $(+)$ on assosiatiivinen eli $a + (b + c) = (a + b) + c$ kaikilla joukon R alkioilla a, b ja c.

3. Joukossa R on olemassa neutraalialkio operaation $(+)$ suhteen eli on olemassa sellainen joukon R alkio $\mathbf{0}$, että $a + \mathbf{0} = \mathbf{0} + a = a$ kaikilla joukon R alkioilla a. Tätä neutraalialkiota kutsutaan *nolla-alkioksi*.

4. Jokaiselle joukon R alkiolle on olemassa käänteisalkio joukossa R operaation $(+)$ suhteen eli jokaiselle joukon R alkiolle a on olemassa joukon R alkio $-a$ siten, että $a + (-a) = -a + a = \mathbf{0}$. Tätä kyseessä olevaa käänteisalkiota nimitetään alkion a *vasta-alkioksi*.

5. Operaatio $(+)$ on kommutatiivinen joukossa R eli $a + b = b + a$ kaikilla joukon R alkioilla a ja b.

2. Pari $(R, \cdot)$ on monoidi ($(\cdot)$ on *multiplikatiivinen operaatio*):

1. Operaatio $(\cdot)$ on binäärinen joukossa R eli alkio $a \cdot b$ sisältyy yksikäsitteisenä joukkoon R kaikilla joukon R alkioilla a ja b.

2. Operaatio $(\cdot)$ on assosiatiivinen eli $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ kaikilla joukon R alkioilla a, b ja c.

3. Joukossa R on neutraalialkio multiplikatiivisen operaation $(\cdot)$ suhteen eli on olemassa joukon R alkio $\mathbf{1}$ siten, että $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ kaikilla joukon R alkioilla a. Kyseessä olevaa alkiota nimitetään *ykkösalkioksi*.

3. *Osittelu-* eli *distributiivisuuslait* ovat voimassa joukossa R:

   1. $a \cdot (b + c) = a \cdot b + a \cdot c$ kaikilla joukon R alkioilla a, b ja c.

   2. $(a + b) \cdot c = a \cdot c + b \cdot c$ kaikilla joukon R alkioilla a, b ja c.

Määritelmä 4.2. Olkoon $(R, +, \cdot)$ rengas. Rengasta R sanotaan *kommutatiiviseksi renkaaksi*, jos operaatio $(\cdot)$ on kommutatiivinen, eli

$$a \cdot b = b \cdot a$$

kaikilla $a, b \in R$.

Esimerkki 4.3. Kokonaisluvut varustettuna kokonaislukujen yhteenlaskulla ja kertolaskulla, $(\mathbb{Z}, +, \cdot)$, on kommutatiivinen rengas.

Todistus. Olkoot $a, b, c \in \mathbb{Z}$.

1. Osoitetaan, että $(\mathbb{Z}, +)$ on Abelin ryhmä:

   1. Nyt $a + b \in \mathbb{Z}$, eli operaatio $(+)$ on binäärinen.

   2. Nyt
   $$\begin{aligned} & a + (b + c) \\ &= a + b + c \\ &= (a + b) + c, \end{aligned}$$
   eli operaatio $(+)$ on assosiatiivinen.

3. Nyt $0 \in \mathbb{Z}$. Lisäksi
$$0 + a = a + 0 = a.$$
Näin ollen 0 on joukon $\mathbb{Z}$ nolla-alkio.

4. Nyt selvästi $-a \in \mathbb{Z}$. Lisäksi
$$a + (-a) = 0$$
ja
$$-a + a = 0.$$
Näin ollen $-a$ on alkion a vasta-alkio.

5. Nyt
$$a + b = b + a,$$
joten operaatio $(+)$ on kommutatiivinen joukossa $\mathbb{Z}$.
Näin ollen pari $(\mathbb{Z}, +)$ on Abelin ryhmä.

2. Osoitetaan, että pari $(\mathbb{Z}, \cdot)$ on monoidi:

1. Nyt $a \cdot b \in \mathbb{Z}$, eli operaatio $(\cdot)$ on binäärinen.

2. Nyt
$$\begin{aligned} & a \cdot (b \cdot c) \\ & = a \cdot b \cdot c \\ & = (a \cdot b) \cdot c, \end{aligned}$$
eli operaatio $(\cdot)$ on assosiatiivinen.

3. Nyt selvästi $1 \in \mathbb{Z}$. Lisäksi
$$a \cdot 1 = 1 \cdot a = a,$$
eli 1 on joukon $\mathbb{Z}$ ykkösalkio.

Näin ollen pari $(\mathbb{Z}, \cdot)$ on monoidi.

3. Osoitetaan, että osittelulait ovat voimassa joukossa $\mathbb{Z}$:

   1. Nyt
   $$a \cdot (b + c) = ab + ac.$$

   2. Nyt
   $$(a + b) \cdot c = ac + bc.$$

   Näin ollen osittelulait ovat voimassa joukossa $\mathbb{Z}$.

4. Osoitetaan, että operaatio $(\cdot)$ on kommutatiivinen:

   Nyt
   $$a \cdot b = b \cdot a,$$
   eli operaatio $(\cdot)$ on kommutatiivinen.

   Täten kolmikko $(\mathbb{Z}, +, \cdot)$ on kommutatiivinen rengas. □

Määritelmä 4.4. Renkaan $(R, +, \cdot)$ epätyhjää osajoukkoa I kutsutaan *ideaaliksi*, jos seuraavat ehdot täyttyvät:

1. $(I, +) \leq (R, +)$ eli osajoukko I on joukon R aliryhmä additiivisen operaation suhteen.
2. Alkiot ra ja ar sisältyvät osajoukkoon I kaikilla joukon I alkioilla a ja renkaan R alkioilla r.

Nyt aliryhmyys $(I, +) \leq (R, +)$ testataan lauseella 2.6. Näin ollen $(I, +) \leq (R, +)$ jos ja vain jos
$$a + (-b) \in I$$
kaikilla $a, b \in I$. Usein käytetään merkintää $a + (-b) = a - b$.

Renkaalla R on aina triviaalit ideaalit $\{\mathbf{0}\}$ ja R.

Esimerkki 4.5. Joukko $3\mathbb{Z} = \{3z \mid z \in \mathbb{Z}\}$ on renkaan $(\mathbb{Z}, +, \cdot)$ ideaali.

Todistus. Osoitetaan, että joukko $3\mathbb{Z}$ on renkaan $\mathbb{Z}$ ideaali. Selvästi $3\mathbb{Z} \subseteq \mathbb{Z}$ ja koska $3 \cdot 1 = 3 \in 3\mathbb{Z}$, niin $3\mathbb{Z} \neq \emptyset$.

Olkoot $a, b \in 3\mathbb{Z}$. Nyt $a = 3k$ ja $b = 3l$ joillakin $k, l \in \mathbb{Z}$.

1. Nyt alkion $b = 3l$ vasta-alkio on $-b = -3l = 3(-l) \in 3\mathbb{Z}$ ja

$$a + (-b) = 3k + (-3l) = 3k - 3l = 3\underbrace{(k - l)}_{\in\, \mathbb{Z}} \in 3\mathbb{Z}.$$

   Näin ollen $(3\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.

2. Olkoon $z \in \mathbb{Z}$. Nyt

$$a \cdot z = 3k \cdot z = 3\underbrace{(k \cdot z)}_{\in\, \mathbb{Z}} \in 3\mathbb{Z}$$

   ja

$$z \cdot a = z \cdot 3k = 3\underbrace{(z \cdot k)}_{\in\, \mathbb{Z}} \in 3\mathbb{Z}.$$

Täten joukko $3\mathbb{Z}$ on renkaan $\mathbb{Z}$ ideaali. □

Lause 4.6. *Olkoot R rengas ja $I \subseteq R$ ideaali. Jos renkaan R ykkösalkio $\mathbf{1} \in I$, niin $I = R$.*

Määritelmä 4.7. Olkoot $(R, +, \cdot)$ kommutatiivinen rengas ja $a \in R$. Nyt joukko

$$I = (a) = Ra = \{ra \mid r \in R\}$$

on renkaan R ideaali ja tätä ideaalia (a) kutsutaan *alkion a generoimaksi pääideaaliksi.*

Esimerkki 4.8. Nyt $3 \in (\mathbb{Z}, +, \cdot)$ ja

$$(3) = \{3r \mid r \in \mathbb{Z}\} = 3\mathbb{Z}.$$

Määritelmä 4.9. Renkaan R ideaalia M sanotaan *maksimaaliseksi ideaaliksi*, mikäli seuraavat ehdot täyttyvät:

1. $M \neq R$.
2. Jos on olemassa renkaan R ideaali J siten, että $M \subset J \subseteq R$, niin $J = R$.

Siis maksimaalinen ideaali M on renkaan R laajin mahdollinen aito ideaali.

Esimerkki 4.10. Renkaan $\mathbb{Z}$ ideaali $3\mathbb{Z}$ on maksimaalinen.

Todistus. Selvästi $3\mathbb{Z} \neq \mathbb{Z}$. Olkoon I renkaan $\mathbb{Z}$ ideaali siten, että $3\mathbb{Z} \subset I \subseteq \mathbb{Z}$. Nyt koska $3\mathbb{Z} \subset I$, niin on olemassa $a \in I$ siten, että $a \notin 3\mathbb{Z}$. Tällöin alkio a on muotoa $a = 3k + 1$ tai $a = 3l + 2$ joillakin $k, l \in \mathbb{Z}$.

1. Jos
$$a = 3k + 1,$$
niin
$$\underbrace{a}_{\in I} - \underbrace{3k}_{\in 3\mathbb{Z} \subset I} = 1 \in I.$$
2. Jos
$$a = 3l + 2,$$
niin
$$\underbrace{a}_{\in I} - \underbrace{3l}_{\in 3\mathbb{Z} \subset I} = 2 \in I.$$
Toisaalta $3 \in 3\mathbb{Z} \subset I$ ja siten
$$3 - 2 = 1 \in I.$$

Koska $1 \in I$, niin lauseen 4.6. nojalla $I = \mathbb{Z}$. Täten maksimaalisen ideaalin määritelmän nojalla osajoukko $3\mathbb{Z}$ on renkaan $\mathbb{Z}$ maksimaalinen ideaali.

□

5 Tekijärengas

Tässä luvussa perehdytään tekijärenkaan rakenteeseen ja ominaisuuksiin. Luvussa läpikäytävät asiat perustuvat luentomonisteisiin [1] ja [2], teokseen [3] sekä omaan pohdintaan.

Lause 5.1. *Olkoot* $(R, +, \cdot)$ *rengas ja* I *sen ideaali. Tällöin* $(I, +) \trianglelefteq (R, +)$.

Todistus. Olkoot $(R, +, \cdot)$ rengas, I sen ideaali, $i \in I$ ja $r \in R$.

Nyt ideaalin määritelmän nojalla $(I, +) \leq (R, +)$ ja alkion r vasta-alkio $-r \in R$, koska R on rengas. Tällöin

$$r + i + (-r) = i + r + (-r) = i + \mathbf{0} = i \in I,$$

koska r, i ja $-r$ ovat kaikki renkaan R alkioita ja operaatio $(+)$ on kommutatiivinen. Tämä pätee kaikilla $i \in I$ ja $r \in R$, joten

$$r + I + (-r) \subseteq I.$$

Täten lauseen 2.15. nojalla $(I, +) \trianglelefteq (R, +)$. □

Määritelmä 5.2. Olkoot $(R, +, \cdot)$ rengas ja I sen ideaali. Määritellään operaatio $(+)$ ryhmän $(R, +)$ sivuluokkien joukossa $\{r + I \mid r \in R\}$ siten, että

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$$

kaikilla $r_1, r_2 \in R$.

Lause 5.3. *Olkoot* $(R, +, \cdot)$ *rengas ja* I *sen ideaali. Tällöin pari* $(\{r + I \mid r \in R\}, +)$ *on ryhmä.*

Todistus. Olkoot $(R, +, \cdot)$ rengas ja I sen ideaali. Lauseen 5.1. nojalla

$$(I, +) \trianglelefteq (R, +).$$

Lauseen 3.3. nojalla $(\{r + I \mid r \in R\}, +)$ on ryhmä. □

Määritelmä 5.4. Ryhmää $(\{r + I \mid r \in R\},+)$ kutsutaan *renkaan R tekijäryhmäksi ideaalin I suhteen.* Tekijäryhmästä käytetään merkintää R/I.

Määritelmä 5.5. Olkoot $(R, +, \cdot)$ rengas ja $I \subseteq R$ ideaali. Määritellään multiplikatiivinen operaatio additiivisessa ryhmässä R/I siten, että

$$(a + I) \cdot (b + I) = a \cdot b + I.$$

Lause 5.6. *Operaatio $(\cdot)$ on hyvin määritelty.*

Todistus. Osoitetaan, ettei operaation tulo riipu sivuluokkien edustajista.

Olkoon $a + I = a' + I \in R/I$ ja $b + I = b' + I \in R/I$.

Tällöin a ja a' määräävät saman sivuluokan eli $a \in a' + I$. Samoin b ja b' määräävät saman sivuluokan eli $b \in b' + I$.

Nyt koska $a \in a' + I$, niin on olemassa $i_1 \in I$ siten, että $a = a' + i_1$. Samoin koska $b \in b' + I$, niin on olemassa $i_2 \in I$ siten, että $b = b' + i_2$. Nyt

$$\begin{aligned}
&(a + I)(b + I) \\
&= ab + I \\
&= (a' + i_1)(b' + i_2) + I \\
&= (a'b' + a'i_2 + i_1b' + i_1i_2) + I \\
&= (a'b' + I) + (\underbrace{a'i_2}_{\in I} + I) + (\underbrace{i_1b'}_{\in I} + I) + (\underbrace{i_1i_2}_{\in I} + I) \\
&= (a'b' + I) + (\mathbf{0} + I) + (\mathbf{0} + I) + (\mathbf{0} + I) \\
&= a'b' + I \\
&= (a' + I)(b' + I).
\end{aligned}$$

Täten operaatio $(\cdot)$ ei riipu sivuluokkien edustajista ja siten sivuluokkien kertolasku on hyvin määritelty. □

Lause 5.7. *Olkoon $(R, +, \cdot)$ rengas ja I sen ideaali. Tällöin $(R/I, +, \cdot)$ on rengas.*

Todistus. Olkoot R rengas ja $I \subseteq R$ ideaali.
Nyt $R/I = \{r + I \mid r \in R\}$. Olkoot $a + I$, $b + I$, $c + I \in R/I$.

1. Osoitetaan, että pari $(R/I, +)$ on Abelin ryhmä:

   1. Nyt
   $$(a + I) + (b + I) = \underbrace{(a + b)}_{\in R} + I \in R/I,$$
   eli operaatio $(+)$ on binäärinen.

   2. Nyt
   $$\begin{aligned}
   &(a + I) + ((b + I) + (c + I)) \\
   &= (a + I) + ((b + c) + I) \\
   &= \underbrace{(a + (b + c))}_{\in R} + I \\
   &= ((a + b) + c) + I \\
   &= ((a + b) + I) + (c + I) \\
   &= ((a + I) + (b + I)) + (c + I),
   \end{aligned}$$
   eli operaatio $(+)$ on assosiatiivinen.

   3. Nyt $\mathbf{0} + I = I \in R/I$. Lisäksi
   $$(a + I) + (\mathbf{0} + I) = (a + \mathbf{0}) + I = a + I$$
   ja
   $$(\mathbf{0} + I) + (a + I) = (\mathbf{0} + a) + I = a + I.$$
   Näin ollen $\mathbf{0} + I$ on joukon R/I nolla-alkio.

   4. Nyt $a \in R$, joten $-a \in R$ ja $-a + I \in R/I$. Lisäksi
   $$(a + I) + (-a + I) = (a + (-a)) + I = \mathbf{0} + I$$
   ja
   $$(-a + I) + (a + I) = (-a + a) + I = \mathbf{0} + I.$$
   Näin ollen $-a + I$ on alkion $a + I$ vasta-alkio.

5. Nyt

$$(a+I)+(b+I) = \underbrace{(a+b)}_{\in R}+I = (b+a)+I = (b+I)+(a+I),$$

koska $(+)$ on kommutatiivinen operaatio renkaassa R. Täten operaatio $(+)$ on kommutatiivinen joukossa R/I.

Näin ollen pari $(R/I,+)$ on Abelin ryhmä.

2. Osoitetaan, että pari $(R/I,\cdot)$ on monoidi:

1. Nyt

$$(a+I)\cdot(b+I) = \underbrace{ab}_{\in R}+I \in R/I,$$

eli operaatio $(\cdot)$ on binäärinen.

2. Nyt

$$\begin{aligned}
&(a+I)\cdot((b+I)\cdot(c+I))\\
&= (a+I)\cdot(bc+I)\\
&= \underbrace{a(bc)}_{\in R}+I\\
&= (ab)c+I\\
&= (ab+I)\cdot(c+I)\\
&= ((a+I)\cdot(b+I))\cdot(c+I),
\end{aligned}$$

eli operaatio $(\cdot)$ on assosiatiivinen.

3. Nyt $\mathbf{1}+I \in R/I$. Lisäksi

$$(a+I)\cdot(\mathbf{1}+I) = (a\cdot\mathbf{1})+I = a+I$$

ja

$$(\mathbf{1}+I)\cdot(a+I) = (\mathbf{1}\cdot a)+I = a+I.$$

Täten $\mathbf{1}+I$ on joukon R/I ykkösalkio.

Näin ollen pari $(R/I, \cdot)$ on monoidi.

3. Osoitetaan. että osittelulait ovat voimassa joukossa R/I:

   1. Nyt
   $$\begin{aligned}
   &(a+I)\cdot((b+I)+(c+I))\\
   &=(a+I)\cdot((b+c)+I)\\
   &=\underbrace{a(b+c)}_{\in R}+I\\
   &=(ab+ac)+I\\
   &=(ab+I)+(ac+I)\\
   &=(a+I)\cdot(b+I)+(a+I)\cdot(c+I).
   \end{aligned}$$

   2. Nyt
   $$\begin{aligned}
   &((a+I)+(b+I))\cdot(c+I)\\
   &=((a+b)+I)\cdot(c+I)\\
   &=\underbrace{(a+b)c}_{\in R}+I\\
   &=(ac+bc)+I\\
   &=(ac+I)+(bc+I)\\
   &=(a+I)\cdot(c+I)+(b+I)\cdot(c+I).
   \end{aligned}$$

   Näin ollen osittelulait ovat voimassa joukossa R/I.

   Täten kolmikko $(R/I, +, \cdot)$ on rengas. □

Määritelmä 5.8. Olkoot $(R, +, \cdot)$ rengas ja $I \subseteq R$ ideaali.
Rengasta $(R/I, +, \cdot) = (\{r + I \mid r \in R\}, +, \cdot)$ kutsutaan *renkaan R tekijärenkaaksi ideaalin I suhteen.*

Esimerkki 5.9. Nyt tekijäryhmä $\mathbb{Z}/3\mathbb{Z} = \{z + 3\mathbb{Z} \mid z \in \mathbb{Z}\}$ varustettuna sivuluokkien additiivisella ja multiplikatiivisella operaatiolla, $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$, on kommutatiivinen rengas.

Todistus. Olkoot $a + 3\mathbb{Z}, b + 3\mathbb{Z}, c + 3\mathbb{Z} \in \mathbb{Z}/3\mathbb{Z}$.

1. Osoitetaan, että pari $(\mathbb{Z}/3\mathbb{Z}, +)$ on Abelin ryhmä:

   1. Nyt
   $$(a + 3\mathbb{Z}) + (b + 3\mathbb{Z}) = \underbrace{(a + b)}_{\in\, \mathbb{Z}} + 3\mathbb{Z} \in \mathbb{Z}/3\mathbb{Z},$$
   eli operaatio $(+)$ on binäärinen.

   2. Nyt
   $$\begin{aligned}
   &(a + 3\mathbb{Z}) + ((b + 3\mathbb{Z}) + (c + 3\mathbb{Z})) \\
   &= (a + 3\mathbb{Z}) + ((b + c) + 3\mathbb{Z}) \\
   &= \underbrace{(a + (b + c))}_{\in\, \mathbb{Z}} + 3\mathbb{Z} \\
   &= ((a + b) + c) + 3\mathbb{Z} \\
   &= ((a + b) + 3\mathbb{Z}) + (c + 3\mathbb{Z}) \\
   &= ((a + 3\mathbb{Z}) + (b + 3\mathbb{Z})) + (c + 3\mathbb{Z}),
   \end{aligned}$$
   eli operaatio $(+)$ on assosiatiivinen.

   3. Nyt $0 \in \mathbb{Z}$ ja $0 + 3\mathbb{Z} \in \mathbb{Z}/3\mathbb{Z}$. Lisäksi
   $$(a + 3\mathbb{Z}) + (0 + 3\mathbb{Z}) = (a + 0) + 3\mathbb{Z} = a + 3\mathbb{Z}$$
   ja
   $$(0 + 3\mathbb{Z}) + (a + 3\mathbb{Z}) = (0 + a) + 3\mathbb{Z} = a + 3\mathbb{Z}.$$
   Näin ollen $0 + 3\mathbb{Z}$ on joukon $\mathbb{Z}/3\mathbb{Z}$ nolla-alkio.

4. Nyt $a \in \mathbb{Z}$, joten $-a \in \mathbb{Z}$ ja $-a + 3\mathbb{Z} \in \mathbb{Z}/3\mathbb{Z}$. Lisäksi

$$(a + 3\mathbb{Z}) + (-a + 3\mathbb{Z}) = (a + (-a)) + 3\mathbb{Z} = 0 + 3\mathbb{Z}$$

ja

$$(-a + 3\mathbb{Z}) + (a + 3\mathbb{Z}) = (-a + a) + 3\mathbb{Z} = 0 + 3\mathbb{Z}.$$

Näin ollen $-a + 3\mathbb{Z}$ on alkion $a + 3\mathbb{Z}$ vasta-alkio.

5. Nyt

$$(a+3\mathbb{Z})+(b+3\mathbb{Z}) = \underbrace{(a+b)}_{\in\,\mathbb{Z}}+3\mathbb{Z} = (b+a)+3\mathbb{Z} = (b+3\mathbb{Z})+(a+3\mathbb{Z}).$$

Täten operaatio $(+)$ on kommutatiivinen joukossa $\mathbb{Z}/3\mathbb{Z}$.

Näin ollen pari $(\mathbb{Z}/3\mathbb{Z}, +)$ on Abelin ryhmä.

2. Osoitetaan, että pari $(\mathbb{Z}/3\mathbb{Z}, \cdot)$ on monoidi:

1. Nyt

$$(a + 3\mathbb{Z}) \cdot (b + 3\mathbb{Z}) = \underbrace{ab}_{\in\,\mathbb{Z}} + 3\mathbb{Z} \in \mathbb{Z}/3\mathbb{Z},$$

eli operaatio $(\cdot)$ on binäärinen.

2. Nyt

$$\begin{aligned}
&(a + 3\mathbb{Z}) \cdot ((b + 3\mathbb{Z}) \cdot (c + 3\mathbb{Z})) \\
&= (a + 3\mathbb{Z}) \cdot (bc + 3\mathbb{Z}) \\
&= \underbrace{a(bc)}_{\in\,\mathbb{Z}} + 3\mathbb{Z} \\
&= (ab)c + 3\mathbb{Z} \\
&= (ab + 3\mathbb{Z}) \cdot (c + 3\mathbb{Z}) \\
&= ((a + 3\mathbb{Z}) \cdot (b + 3\mathbb{Z})) \cdot (c + 3\mathbb{Z}),
\end{aligned}$$

eli operaatio $(\cdot)$ on assosiatiivinen.

3. Nyt $1 + I \in \mathbb{Z}/3\mathbb{Z}$. Lisäksi

$$(a + 3\mathbb{Z}) \cdot (1 + 3\mathbb{Z}) = (a \cdot 1) + 3\mathbb{Z} = a + 3\mathbb{Z}$$

ja

$$(1 + 3\mathbb{Z}) \cdot (a + 3\mathbb{Z}) = (1 \cdot a) + 3\mathbb{Z} = a + 3\mathbb{Z}.$$

Täten $1 + 3\mathbb{Z}$ on joukon $\mathbb{Z}/3\mathbb{Z}$ ykkösalkio.
Näin ollen pari $(\mathbb{Z}/3\mathbb{Z}, \cdot)$ on monoidi.

3. Osoitetaan, että osittelulait ovat voimassa joukossa $\mathbb{Z}/3\mathbb{Z}$:

1. Nyt

$$\begin{aligned}
&(a + 3\mathbb{Z}) \cdot ((b + 3\mathbb{Z}) + (c + 3\mathbb{Z})) \\
&= (a + 3\mathbb{Z}) \cdot ((b + c) + 3\mathbb{Z}) \\
&= \underbrace{a(b + c)}_{\in\, \mathbb{Z}} + 3\mathbb{Z} \\
&= (ab + ac) + 3\mathbb{Z} \\
&= (ab + 3\mathbb{Z}) + (ac + 3\mathbb{Z}) \\
&= (a + 3\mathbb{Z}) \cdot (b + 3\mathbb{Z}) + (a + 3\mathbb{Z}) \cdot (c + 3\mathbb{Z}).
\end{aligned}$$

2. Nyt

$$\begin{aligned}
&((a + 3\mathbb{Z}) + (b + 3\mathbb{Z})) \cdot (c + 3\mathbb{Z}) \\
&= ((a + b) + 3\mathbb{Z}) \cdot (c + 3\mathbb{Z}) \\
&= \underbrace{(a + b)c}_{\in\, \mathbb{Z}} + 3\mathbb{Z} \\
&= (ac + bc) + 3\mathbb{Z} \\
&= (ac + 3\mathbb{Z}) + (bc + 3\mathbb{Z}) \\
&= (a + 3\mathbb{Z}) \cdot (c + 3\mathbb{Z}) + (b + 3\mathbb{Z}) \cdot (c + 3\mathbb{Z}).
\end{aligned}$$

Näin ollen osittelulait ovat voimassa joukossa $\mathbb{Z}/3\mathbb{Z}$.

4. Osoitetaan, että operaatio $(\cdot)$ on kommutatiivinen:

Nyt

$$(a+3\mathbb{Z})\cdot(b+3\mathbb{Z}) = \underbrace{ab}_{\in\,\mathbb{Z}} + 3\mathbb{Z} = ba + 3\mathbb{Z} = (b+3\mathbb{Z})\cdot(a+3\mathbb{Z}),$$

eli operaatio $(\cdot)$ on kommutatiivinen.

Täten kolmikko $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ on kommutatiivinen rengas.

Laskutaulu operaation $(+)$ suhteen:

$+$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$1+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$
$2+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$

Laskutaulu operaation $(\cdot)$ suhteen:

$\cdot$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$0+3\mathbb{Z}$
$1+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$2+3\mathbb{Z}$	$0+3\mathbb{Z}$	$2+3\mathbb{Z}$	$1+3\mathbb{Z}$

□

Toisaalta, koska $(\mathbb{Z}, +, \cdot)$ on rengas ja $3\mathbb{Z}$ sen ideaali, niin lause 5.7 kertoo suoraan, että $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ on rengas. Lisäksi seuraava lause kertoo kommutatiivisuuden.

Lause 5.10. *Jos $(R, +, \cdot)$ on kommutatiivinen rengas ja $I \subseteq R$ ideaali, niin tekijärengas $(R/I, +, \cdot)$ on kommutatiivinen rengas.*

Todistus. Olkoot $(R, +, \cdot)$ kommutatiivinen rengas, $I \subseteq R$ ideaali ja $a+I$, $b+I \in R/I$. Nyt

$$(a+I)\cdot(b+I) = (a\cdot b) + I = (b\cdot a) + I = (b+I)\cdot(a+I),$$

sillä $a \cdot b = b \cdot a$ renkaan R ollessa kommutatiivinen. □

Lause 5.11. *Jos* $(R, +, \cdot)$ *on äärellinen rengas ja* $I \subseteq R$ *ideaali, niin*

$$|(R/I, +, \cdot)| = \frac{|R|}{|I|}.$$

Todistus. Olkoot $(R, +, \cdot)$ äärellinen rengas ja $I \subseteq R$ ideaali. Nyt koska R on rengas, I on renkaan R ideaali ja edelleen $(I, +) \trianglelefteq (R, +)$, niin lauseen 3.5. nojalla

$$|R/I| = \frac{|R|}{|I|}.$$

□

6 Kuntien perusasioita

Tässä luvussa esitellään kuntiin liittyviä perusasioita, joita on käyty läpi Algebralliset rakenteet -kurssilla. Todistukset sivuutetaan.

Määritelmä 6.1. Olkoon $(K, +, \cdot)$ kommutatiivinen rengas. Nyt $(K, +, \cdot)$ on *kunta*, jos pari $(K \backslash \{\mathbf{0}\}, \cdot)$ on Abelin ryhmä.

Toisaalta kunta voidaan myös määritellä seuraavasti.

Määritelmä 6.2. Kolmikko $(K, +, \cdot)$ on *kunta*, mikäli seuraavat ehdot toteutuvat:
1. Pari $(K, +)$ on Abelin ryhmä:

1. Operaatio $(+)$ on binäärinen joukossa K, toisin sanoen alkio $a + b$ sisältyy yksikäsitteisenä joukkoon K kaikilla joukon K alkioilla a ja b.

2. Operaatio $(+)$ on assosiatiivinen eli $a + (b + c) = (a + b) + c$ kaikilla joukon K alkioilla a, b ja c.

3. Joukossa K on olemassa *nolla-alkio* eli on olemassa sellainen joukon K alkio $\mathbf{0}$, että $a + \mathbf{0} = \mathbf{0} + a = a$ kaikilla joukon K alkioilla a.

4. Jokaiselle joukon K alkiolle on olemassa *vasta-alkio* joukossa K eli jokaiselle joukon K alkiolle a on olemassa joukon K alkio $-a$ siten, että $a + (-a) = -a + a = \mathbf{0}$.

5. Operaatio $(+)$ on kommutatiivinen joukossa K eli $a + b = b + a$ kaikilla joukon K alkioilla a ja b.

2. Operaatiolle $(\cdot)$ on voimassa:

1. Operaatio $(\cdot)$ on binäärinen joukossa K eli alkio $a \cdot b$ sisältyy yksikäsitteisenä joukkoon K kaikilla joukon K alkioilla a ja b.

2. Operaatio $(\cdot)$ on assosiatiivinen eli $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ kaikilla joukon K alkioilla a, b ja c.

3. Joukossa K on *ykkösalkio* eli on olemassa joukon K alkio $\mathbf{1}$ siten, että $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ kaikilla joukon K alkioilla a.

4. Jokaiselle joukon $K\backslash\{\mathbf{0}\}$ alkiolle on olemassa *käänteisalkio* joukossa $K\backslash\{\mathbf{0}\}$, eli jokaiselle joukon $K\backslash\{\mathbf{0}\}$ alkiolle a on olemassa joukon $K\backslash\{\mathbf{0}\}$ alkio a^{-1} siten, että $a \cdot a^{-1} = a^{-1} \cdot a = \mathbf{1}$.

5. Operaatio $(\cdot)$ on kommutatiivinen joukossa K eli $a \cdot b = b \cdot a$ kaikilla joukon K alkioilla a ja b.

3. Osittelu- eli distributiivisuuslait ovat voimassa joukossa K:

1. $a \cdot (b + c) = a \cdot b + a \cdot c$ kaikilla joukon K alkioilla a, b ja c.

2. $(a + b) \cdot c = a \cdot c + b \cdot c$ kaikilla joukon K alkioilla a, b ja c.

Esimerkki 6.3. Kommutatiivinen rengas $(\mathbb{Z}, +, \cdot)$ ei ole kunta.

Todistus. Todistetaan väite vastaesimerkin avulla. Nyt $5 \in \mathbb{Z}$. Olkoon $a \in \mathbb{Z}$. Tällöin

$$\begin{aligned} & 5 \cdot a = 1 \\ \Leftrightarrow\ & a = \frac{1}{5}, \end{aligned}$$

eli alkion 5 käänteisalkio olisi $\frac{1}{5}$, mutta $\frac{1}{5} \notin \mathbb{Z}$, joten $(\mathbb{Z}, +, \cdot)$ ei ole kunta. □

7 Kuntalaajennus

Tässä luvussa perehdytään kuntalaajennuksen rakenteeseen ja ominaisuuksiin. Luvussa läpikäytävät asiat perustuvat omaan pohdintaan, luentomonisteeseen [1] ja teokseen [3].

Lause 7.1. *Kommutatiivinen rengas R on kunta jos ja vain jos $\{\mathbf{0}\}$ on renkaan R maksimaalinen ideaali.*

Todistus. Nyt tiedetään, että $\{\mathbf{0}\}$ on renkaan R ideaali ja $\{\mathbf{0}\} \subseteq I$ kaikilla renkaan R ideaaleilla I. Todistetaan ensiksi, että jos rengas R on kunta, niin $\{\mathbf{0}\}$ on maksimaalinen ideaali.

Olkoot R kunta, $I \subseteq R$ ideaali ja $\mathbf{0} \neq i \in I$. Nyt koska R on kunta, niin on olemassa alkion i käänteisalkio $i^{-1} \in R$ siten, että

$$i \cdot i^{-1} = \mathbf{1}.$$

Nyt koska I on ideaali, niin ideaalin alkion ja renkaan alkion välinen operaatio $(\cdot)$ tuottaa ideaalin alkion, eli

$$\underbrace{i}_{\in I} \cdot \underbrace{i^{-1}}_{\in R} = \mathbf{1} \in I.$$

Lauseen 4.6. nojalla $I = R$, koska $\mathbf{1} \in I$. Siis jos ideaali I sisältää nollaalkiosta eroavan alkion, niin $I = R$ ja tällöin ideaali I ei ole aito ideaali.

Täten $\{\mathbf{0}\}$ on kunnan R maksimaalinen ideaali.

Todistetaan seuraavaksi, että jos $\{\mathbf{0}\}$ on kommutatiivisen renkaan R maksimaalinen ideaali, niin rengas R on kunta.

Olkoon R kommutatiivinen rengas ja $\{\mathbf{0}\}$ sen maksimaalinen ideaali. Tällöin renkaan R ainoat ideaalit ovat triviaalit ideaalit $\{\mathbf{0}\}$ ja R, koska $\{\mathbf{0}\} \subseteq I$ kaikilla ideaaleilla $I \subseteq R$. Olkoon $\mathbf{0} \neq a \in R$. Nyt pääideaali $(a) = R$, joten ykkösalkio $\mathbf{1} \in (a)$.

Nyt Määritelmän 4.7. nojalla $(a) = Ra$. Koska $\mathbf{1} \in (a) = Ra$, niin on olemassa $r \in R$ siten, että

$$\mathbf{1} = r \cdot a,$$

eli jokaiselle kommutatiivisen renkaan R alkiolle $a \in R\backslash\{\mathbf{0}\}$ on olemassa käänteisalkio $a^{-1} \in R\backslash\{\mathbf{0}\}$ siten, että

$$a^{-1} \cdot a = a \cdot a^{-1} = \mathbf{1}.$$

Täten R on kunta.

□

Toisin sanoen, jos kommutatiivisella renkaalla R ei ole muita ideaaleja kuin $\{\mathbf{0}\}$ ja rengas R itse, niin rengas R on kunta.

Lause 7.2. *Olkoot R rengas ja $I \subseteq R$ ideaali. Jos ideaali I on maksimaalinen, niin tekijärenkaan $(R/I, +, \cdot)$ ainoat ideaalit ovat R/I ja $\{\mathbf{0} + I\}$.*

Todistus. Olkoot R rengas ja I renkaan R maksimaalinen ideaali. Tällöin $(R/I, +, \cdot)$ on rengas. Todistetaan lause vastaoletuksen kautta. Oletetaan, että renkaalla R/I on olemassa ideaali J, joka ei ole R/I tai $\{\mathbf{0} + I\}$.

Olkoon J sellainen renkaan R/I ideaali, että $J \neq \{\mathbf{0} + I\}$ ja $J \neq R/I$. Nyt ideaali J sisältää nolla-alkiosta eroavia alkioita, eli

$$J = \{\mathbf{0} + I, r_1 + I, r_2 + I, \ldots\},$$

joillakin $r_i \in R$ ja $r_i \notin I$. Muodostetaan renkaan R osajoukko T siten, että tekijärenkaan R/I ideaalin J alkioiden $r_i + I$ määrääjäalkiot r_i muodostavat joukon T, eli

$$T = \{\mathbf{0}, r_1, r_2, \ldots\}.$$

Muistetaan myös, että samaan sivuluokkaan kuuluvat alkiot määräävät saman sivuluokan. Selvästi $I \subseteq T$, koska $i_j + I = \mathbf{0} + I \in J$ kaikilla $i_j \in I$. Lisäksi $I \subset T$, koska $J \neq \{\mathbf{0} + I\}$.

Osoitetaan nyt, että joukko T on renkaan R ideaali.

1. Olkoot $t_1, t_2 \in T$, eli $t_1 + I, t_2 + I \in J$. Koska J on renkaan R/I ideaali, niin
$$(t_1 + I) - (t_2 + I) \in J$$
eli
$$(t_1 - t_2) + I \in J.$$
Näin ollen
$$t_1 - t_2 \in T,$$
eli $(T, +) \leq (R, +)$.

2. Olkoot $t \in T$ ja $r \in R$, eli $t + I \in J$ ja $r + I \in R/I$. Koska J on renkaan R/I ideaali, niin
$$(t + I) \cdot (r + I) \in J$$
eli
$$tr + I \in J,$$
jolloin $tr \in T$. Vastaavasti
$$(r + I) \cdot (t + I) \in J$$
eli
$$rt + I \in J,$$
jolloin $rt \in T$.

Täten joukko T on renkaan R ideaali ja $T \subset R$, koska $J \subset R/I$.

Nyt $I \subset T \subset R$, mikä on ristiriita, koska I on maksimaalinen ideaali. Täten vastaoletus on väärä ja alkuperäinen väite, "renkaan $(R/I, +, \cdot)$ ainoat ideaalit ovat R/I ja $\{\mathbf{0} + I\}$", pätee. □

Lause 7.3. *Olkoot R kommutatiivinen rengas ja I renkaan R ideaali. Jos ideaali I on maksimaalinen, niin tekijärengas $(R/I, +, \cdot)$ on kunta.*

Todistus. Olkoot R kommutatiivinen rengas ja I renkaan R maksimaalinen ideaali. Tällöin Lauseen 7.2. nojalla tekijärenkaan $(R/I, +, \cdot)$ ainoat ideaalit ovat R/I ja $\{\mathbf{0} + I\}$.

Lisäksi Lauseen 5.10. nojalla tekijärengas $(R/I, +, \cdot)$ on kommutatiivinen rengas, koska rengas R on kommutatiivinen.

Nyt koska kommutatiivisen renkaan R/I ainoat ideaalit ovat rengas R/I itse ja renkaan nolla-alkion muodostama joukko $\{\mathbf{0} + I\}$, niin Lauseen 7.1. nojalla rengas R/I on kunta.

□

Osoitetaan kuntalaajennustulos myös toisella tavalla. Tätä varten tarvitsemme muutaman lisätuloksen.

Lause 7.4. *Olkoon R rengas ja $I, J \subseteq R$ ideaaleja. Tällöin myös ideaalien I ja J summajoukko*

$$I + J = \{i + j \mid i \in I, j \in J\}$$

on renkaan R ideaali.

Todistus. Osoitetaan, että joukko $I + J$ on renkaan R ideaali. Olkoot $i_1 + j_1, i_2 + j_2 \in I + J$.

1. Nyt koska $-i_2 \in I$ ja $-j_2 \in J$, niin $-i_2 + (-j_2) = -(i_2 + j_2) \in I + J$. Tällöin

   $$(i_1 + j_1) - (i_2 + j_2) = \underbrace{(i_1 - i_2)}_{\in I} + \underbrace{(j_1 - j_2)}_{\in J} \in I + J.$$

   Siis $(I + J, +) \leq (R, +)$.

2. Olkoon $r \in R$. Nyt koska I ja J ovat renkaan R ideaaleja, niin

   $$(i_1 + j_1)r = \underbrace{i_1 r}_{\in I} + \underbrace{j_1 r}_{\in J} \in I + J$$

ja

$$r(i_1 + j_1) = \underbrace{ri_1}_{\in I} + \underbrace{rj_1}_{\in J} \in I + J.$$

Täten summajoukko $I + J$ on renkaan R ideaali. □

Lause 7.5. *Olkoot R kommutatiivinen rengas ja I sen ideaali. Ideaalin I ollessa maksimaalinen tekijärengas $(R/I, +, \cdot)$ on kunta.*

Todistus. Olkoot R kommutatiivinen rengas ja $I \subseteq R$ maksimaalinen ideaali. Tällöin tekijärengas $(R/I, +, \cdot)$ on kommutatiivinen rengas.

Osoitetaan, että tekijärengas $(R/I, +, \cdot)$ toteuttaa kunnan määritelmän eli osoitetaan, että $(R/I \backslash \{\mathbf{0} + I\}, \cdot)$ on Abelin ryhmä. Koska R/I on kommutatiivinen rengas, niin riittää löytää jokaiselle nolla-alkiosta eroavalle alkiolle käänteisalkio joukosta $R/I \backslash \{\mathbf{0} + I\}$.

Olkoot $a \in R$ sellainen, että $a + I \neq \mathbf{0} + I$. Tällöin $a \notin \mathbf{0} + I = I$, joten renkaan alkion a generoima pääideaali $(a) \neq I$, koska $a \in (a) = Ra$.

Lauseen 7.4. nojalla ideaalien (a) ja I summajoukko $(a) + I$ on renkaan R ideaali. Nyt koska $I \subset (a) + I$ ja I on maksimaalinen ideaali, niin maksimaalisen ideaalin määritelmän nojalla $(a) + I = R$ ja edelleen Määritelmän 4.7. nojalla $R = I + Ra$.

Nyt $\mathbf{1} \in R$, joten $\mathbf{1} \in I + Ra$. Tällöin on olemassa $i \in I$ ja $r \in R$ siten, että $\mathbf{1} = i + ra$. Siten tekijärenkaan R/I ykkösalkio

$$\begin{aligned} &\mathbf{1} + I \\ &= (i + ra) + I \\ &= (\underbrace{i}_{\in I} + I) + (ra + I) \\ &= (\mathbf{0} + I) + (ra + I) \\ &= ra + I \end{aligned}$$

$$= (r + I) \cdot (a + I).$$

Rengas R on kommutatiivinen, joten Lauseen 5.10. nojalla myös tekijärengas R/I on kommutatiivinen, joten myös

$$(a + I) \cdot (i + I) = \mathbf{1} + I.$$

Siis alkio $r + I$ on alkion $a + I$ käänteisalkio ja $r + I \neq \mathbf{0} + I$. Eli jokaiselle tekijärenkaan alkiolle $a+I \neq \mathbf{0}+I$ on olemassa käänteisalkio $r+I \in R/I$.

Täten tekijärengas $(R/I, +, \cdot)$ on kunta. □

Esimerkki 7.6. Tekijärengas $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ on kunta.

Todistus. Osoitetaan, että tekijärengas $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ toteuttaa kunnan määritelmän eli osoitetaan, että pari $(\mathbb{Z}/3\mathbb{Z}\backslash\{0+3\mathbb{Z}\}, \cdot)$ on Abelin ryhmä. Koska $\mathbb{Z}/3\mathbb{Z}$ on kommutatiivinen rengas, niin riittää löytää jokaiselle nolla-alkiosta eroavalle alkiolle käänteisalkio joukosta

$$\mathbb{Z}/3\mathbb{Z}\backslash\{0 + 3\mathbb{Z}\} = \{1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}.$$

Nyt

$$(1 + 3\mathbb{Z}) \cdot (1 + 3\mathbb{Z}) = (1 \cdot 1) + 3\mathbb{Z} = 1 + 3\mathbb{Z}$$

ja

$$(2+3\mathbb{Z})\cdot(2+3\mathbb{Z}) = 4+3\mathbb{Z} = (1+3)+3\mathbb{Z} = (1+3\mathbb{Z})+(\underbrace{3}_{\in\, 3\mathbb{Z}}+3\mathbb{Z}) = (1+3\mathbb{Z})+(0+3\mathbb{Z}) = 1+3\mathbb{Z}.$$

Näin ollen jokaiselle joukon $\mathbb{Z}/3\mathbb{Z}\backslash\{0 + 3\mathbb{Z}\}$ alkiolle on olemassa käänteisalkio joukossa $\mathbb{Z}/3\mathbb{Z}\backslash\{0 + 3\mathbb{Z}\}$.

Täten tekijärengas $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ on kunta. □

Toisaalta, koska $3\mathbb{Z}$ on renkaan $(\mathbb{Z}, +, \cdot)$ maksimaalinen ideaali, niin tekijärengas $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ on kunta Lauseen 7.3. tai Lauseen 7.5. perusteella.

Lähdeluettelo

[1] Niemenmaa M., Myllylä K., Törmä T., Leinonen M.: *802355A Algebralliset rakenteet Luentorunko Syksy 2015*. Oulun yliopisto, 2015.

[2] Niemenmaa M., Myllylä K., Törmä T.: *802354A Algebran perusteet Luentorunko Kevät 2020*. Oulun yliopisto, 2020.

[3] Rotman J.: *Advanced Modern Algebra*. Prentice Hall, 2002.