Kuntalaajennus

LuK-tutkielma
Lotta Kastell
2637714
Matematiikan tutkinto-ohjelma
Oulun yliopisto
Syksy 2021

Sisällys

Johdanto **2**

1 Renkaat ja ideaalit **3**
1.1 Johdanto 3
1.2 Renkaat ja kunta 3
1.3 Ideaalit 9
1.4 Polynomirengas 10

2 Tekijärengas **12**
2.1 Johdanto 12
2.2 Tekijäryhmä 12
2.3 Tekijärengas 13

3 Kuntalaajennus **17**
3.1 Johdanto 17
3.2 Kuntalaajennus 17

Lähdeluettelo **21**

Johdanto

Tutkielmassa on käytetty pääasiassa J. J. Rotmannin teosta *Advanced Modern Algebra* [1]. Lukijalla olisi hyvä olla taustatietona jonkinlainen käsitys algebrallisista ryhmä- ja rengasrakenteista sekä niiden operaatioista.

Ensimmäisessä luvussa käsitellään renkaiden, ideaalien, kuntien, polynomirenkaiden ja jaottomien polynomien määritelmiä sekä niihin liittyviä tärkeimpiä lauseita. Luvussa käsitellään myös pari esimerkkiä, joita hyödynnetään toisessa luvussa käsiteltävässä esimerkissä, sekä jakoalgoritmi, jota käytetään kolmannessa luvussa käsiteltävässä esimerkissä.

Toisessa luvussa määritellään tekijärengas, joka muodostetaan kommutatiivisesta renkaasta ja sen ideaalista. Lisäksi otetaan esimerkki tekijärenkaasta ja käydään läpi sen alkioiden väliset operaatiot.

Kolmannessa luvussa esitetään kuntalaajennuksen määrittelevä lause ja esimerkki, jossa laajennetaan reaalilukukunta tekijärenkaan avulla kompleksilukukunnaksi. Kuntalaajennuksen ideana on muodostaa kunnasta K polynomirengas $K[x]$, josta otetaan jaoton polynomi $p(x)$. Jaottomasta polynomista $p(x)$ muodostetaan pääideaali $(p(x))$, ja polynomirenkaasta $K[x]$ ja pääideaalista $(p(x))$ tekijärengas $K[x]/(p(x))$. Osoitetaan, että muodostettu tekijärengas $K[x]/(p(x))$ on rakenteeltaan kunta.

1 Renkaat ja ideaalit

1.1 Johdanto

Tässä luvussa on käytetty lähteenä kurssin *Algebralliset rakenteet* [3] luentomonistetta. Jotta tekijärenkaaseen ja kuntalaajennukseen liittyvät lauseet ja määritelmät voi ymmärtää, tulee lukijan tietää myös tärkeimmät määritelmät ja lauseet liittyen renkaisiin, ideaaleihin, kuntiin, polynomirenkaisiin ja jaottomiin polynomeihin. Määritellään tässä luvussa myös jakoalgoritmi, jota käytetään tutkielman varsinaiseen aiheeseen liittyvässä esimerkissä. Lisäksi otetaan esimerkki sekä kommutatiivisesta renkaasta, että ideaalista ja muodostetaan näiden esimerkkien avulla esimerkki tekijärenkaasta seuraavassa luvussa.

1.2 Renkaat ja kunta

Määritellään, mitä tarkoittaa rengas.

Määritelmä 1.1. Olkoot $R \neq \emptyset$ sekä $(+)$ ja $(\cdot)$ joukon R operaatiot. Kolmikko $(R, +, \cdot)$ on *rengas* mikäli

1. $(R, +)$ on Abelin ryhmä:

   - $(+)$ on binäärinen operaatio joukossa R eli
   $$a + b \in R$$
   ja on yksikäsitteinen kaikilla $a, b \in R$.
   - $(+)$ on assosiatiivinen operaatio eli
   $$a + (b + c) = (a + b) + c$$
   kaikilla $a, b, c \in R$.
   - Joukossa R on neutraalialkio operaation $(+)$ suhteen eli on olemassa sellainen alkio $\mathbf{0}_R \in R$, että
   $$a + \mathbf{0}_R = \mathbf{0}_R + a = a$$
   kaikilla $a \in R$.
   Tätä alkiota nimitetään renkaan R *nolla-alkioksi*.

- Jokaisella joukon R alkiolla on olemassa käänteisalkio joukossa R operaation $(+)$ suhteen eli jokaiselle $a \in R$ on olemassa sellainen alkio $-a \in R$, että

$$a + (-a) = -a + a = \mathbf{0}_R.$$

  Tätä käänteisalkiota nimitetään alkion a *vasta-alkioksi*.
- $(+)$ on kommutatiivinen operaatio eli

$$a + b = b + a$$

  kaikilla $a, b \in R$.

2. $(R, \cdot)$ on monoidi:
   - $(\cdot)$ on binäärinen operaatio joukossa R eli

$$a \cdot b \in R$$

     ja on yksikäsitteinen kaikilla $a, b \in R$.
   - $(\cdot)$ on assosiatiivinen operaatio eli

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

     kaikilla $a, b, c \in R$.
   - Joukossa R on neutraalialkio operaation $(\cdot)$ suhteen eli on olemassa sellainen alkio $\mathbf{1}_R \in R$, että

$$a \cdot \mathbf{1}_R = \mathbf{1}_R \cdot a = a$$

     kaikilla $a \in R$
     Tätä alkiota nimitetään renkaan R *ykkösalkioksi*.

3. Distributiivisuus- eli osittelulait ovat voimassa:

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{ja}$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

   aina, kun $a, b, c \in R$.

Määritelmä 1.2. Rengasta $(R, +, \cdot)$ sanotaan *kommutatiiviseksi*, mikäli se on kommutatiivinen operaation $(\cdot)$ suhteen eli jos

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

aina, kun $a, b \in R$.

Esimerkki 1.3. Tutkitaan onko $(\mathbb{Z}, +, \cdot)$ rengas.
Koska esimerkiksi $1 \in \mathbb{Z}$, niin $\mathbb{Z} \neq \emptyset$.

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

   - Nyt
   $$a + b \in \mathbb{Z}$$
   ja on yksikäsitteinen kaikilla $a, b \in \mathbb{Z}$.
   Siis operaatio $(+)$ on binäärinen joukossa $\mathbb{Z}$.
   - Nyt
   $$(a + b) + c = a + (b + c)$$
   kaikilla $a, b, c \in \mathbb{Z}$.
   Siis operaatio $(+)$ on assosiatiivinen joukossa $\mathbb{Z}$.
   - Nyt $0 \in \mathbb{Z}$ ja
   $$a + 0 = a = 0 + a$$
   kaikilla $a \in \mathbb{Z}$.
   Näin ollen joukon $\mathbb{Z}$ nolla-alkio $\mathbf{0}_{\mathbb{Z}} = 0$.
   - Olkoon $a \in \mathbb{Z}$. Tällöin $-a \in \mathbb{Z}$ ja
   $$a + (-a) = 0 = -a + a$$
   eli alkion a vasta-alkio on sen vastaluku $-a$.
   - Nyt
   $$a + b = b + a$$
   kaikilla $a, b \in \mathbb{Z}$.
   Siis operaatio $(+)$ on kommutatiivinen joukossa $\mathbb{Z}$.

2. Pari $(\mathbb{Z}, \cdot)$ on monoidi:

   - Nyt
   $$a \cdot b \in \mathbb{Z}$$
   ja on yksikäsitteinen kaikilla $a, b \in \mathbb{Z}$.
   Siis operaatio $(\cdot)$ on binäärinen joukossa $\mathbb{Z}$.
   - Nyt
   $$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$
   kaikilla $a, b, c \in \mathbb{Z}$.
   Siis operaatio $(\cdot)$ on assosiatiivinen joukossa $\mathbb{Z}$.

- Nyt $1 \in \mathbb{Z}$ ja
$$a \cdot 1 = a = 1 \cdot a$$
kaikilla $a \in \mathbb{Z}$.
Siis joukon $\mathbb{Z}$ ykkösalkio $\mathbf{1}_{\mathbb{Z}} = 1$.

3. Osittelulait ovat voimassa:

- Nyt
$$a \cdot (b + c) = ab + ac$$
kaikilla $a, b, c \in \mathbb{Z}$.
- Nyt
$$(a + b) \cdot c = ac + bc$$
kaikilla $a, b, c \in \mathbb{Z}$.

Kohtien 1.-3. nojalla kolmikko $(\mathbb{Z}, +, \cdot)$ on rengas.
Tutkitaan vielä onko rengas $(\mathbb{Z}, +, \cdot)$ kommutatiivinen.
Nyt kaikilla $a, b \in \mathbb{Z}$
$$a \cdot b = b \cdot a.$$
Siis operaatio $(\cdot)$ on kommutatiivinen joukossa $\mathbb{Z}$.
Rengas $(\mathbb{Z}, +, \cdot)$ on siis kommutatiivinen rengas.

Asettamalla kertolaskuoperaatiolle lisäehtoja, saadaan kunta.

Määritelmä 1.4. Kommutatiivista rengasta $(K, +, \cdot)$ sanotaan *kunnaksi*, mikäli $(K\backslash\{\mathbf{0}_K\}, \cdot)$ on Abelin ryhmä. Ryhmä $(K\backslash\{\mathbf{0}_K\}, \cdot)$ on kunnan K *multiplikatiivinen ryhmä* ja ryhmä $(K, +)$ on kunnan *additiivinen ryhmä*.

$(K\backslash\{\mathbf{0}_K\}, \cdot)$ on Abelin ryhmä, kun operaatiolle $(\cdot)$ pätevät seuraavat ehdot:

- $(\cdot)$ on binäärinen operaatio joukossa $K\backslash\{\mathbf{0}_K\}$ eli
$$a \cdot b \in K\backslash\{\mathbf{0}_K\}$$
ja on yksikäsitteinen kaikilla $a, b \in K\backslash\{\mathbf{0}_K\}$.
- $(\cdot)$ on assosiatiivinen operaatio eli
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$
kaikilla $a, b, c \in K\backslash\{\mathbf{0}_K\}$.

- On olemassa ykkösalkio $\mathbf{1}_K \in K\backslash\{\mathbf{0}_K\}$, jolle

$$\mathbf{1}_K \cdot a = a \cdot \mathbf{1}_K = a$$

  kaikilla $a \in K\backslash\{\mathbf{0}_K\}$.

- Jokaiselle alkiolle $a \in K\backslash\{\mathbf{0}_K\}$ on olemassa käänteisalkio $a^{-1} \in K\backslash\{\mathbf{0}_K\}$, jolle pätee

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

- $(\cdot)$ on kommutatiivinen operaatio eli

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

  kaikilla $a, b \in K\backslash\{\mathbf{0}_K\}$.

On olemassa lisäkriteeri, jolla kommutatiivisesta renkaasta saadaan kunta.

Lause 1.5. *Olkoon $(K, +, \cdot)$ kommutatiivinen rengas ja $K\backslash\{\mathbf{0}_K\} \neq \emptyset$. Mikäli tällöin jokaiselle alkiolle $a \in K\backslash\{\mathbf{0}_K\}$ on olemassa käänteisalkio $a^{-1} \in K\backslash\{\mathbf{0}_K\}$, niin kommutatiivinen rengas $(K, +, \cdot)$ on kunta.*

Todistus. Tämä lause on todistetttu kurssilla *Algebralliset rakenteet* [3]. □

Määritellään, mitä tarkoittaa rengashomomorfismi.

Määritelmä 1.6. Olkoon $(R, +, \cdot)$ ja $(R', \oplus, \odot)$ renkaita. Tällöin kuvausta $f : R \to R'$ sanotaan *rengashomomorfismiksi*, jos se täyttää seuraavat ehdot:

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

Esimerkki 1.7. Tutkitaan onko edellisen esimerkin kommutatiivinen rengas $(\mathbb{Z}, +, \cdot)$ kunta.

Täytyy selvittää, onko pari $(\mathbb{Z}\backslash\{0\}, \cdot)$ Abelin ryhmä.

Täytyy selvittää, löytyykö kaikille alkioille $a \in \mathbb{Z}\backslash\{0\}$ käänteisalkio $a^{-1} \in \mathbb{Z}\backslash\{0\}$.

Nyt

$$5 \in \mathbb{Z}\backslash\{0\},$$

mutta

$$5^{-1} = \frac{1}{5} \notin \mathbb{Z}\backslash\{0\}.$$

Koska alkiolle 5 ei löydy käänteisalkiota joukossa $\mathbb{Z}\backslash\{0\}$, niin kaikille alkioille ei löydy käänteisalkiota, joten pari $(\mathbb{Z}\backslash\{0\}, \cdot)$ ei ole Abelin ryhmä.

Tästä seuraa, että kommutatiivinen rengas $(\mathbb{Z}, +, \cdot)$ ei ole kunta.

Esimerkki 1.8. Tutkitaan onko tunnettu kommutatiivinen rengas $(\mathbb{R}, +, \cdot)$ kunta.

Täytyy selvittää, onko pari $(\mathbb{R}\backslash\{0\}, \cdot)$ Abelin ryhmä.

Selvitetään, löytyykö kaikille alkioille $a \in \mathbb{R}\backslash\{0\}$ käänteisalkio $a^{-1} \in \mathbb{R}\backslash\{0\}$.

Olkoon

$$a \in \mathbb{R}\backslash\{0\}.$$

Nyt alkion a käänteisalkio on

$$a^{-1} = \frac{1}{a} \in \mathbb{R}\backslash\{0\},$$

sillä

$$a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1 = \mathbf{1}_{\mathbb{R}}.$$

Siis alkion a käänteisalkio

$$a^{-1} = \frac{1}{a} \in \mathbb{R}\backslash\{0\}.$$

Nyt siis kommutatiivinen rengas $(\mathbb{R}, +, \cdot)$ on kunta.

1.3 Ideaalit

Määritellään, mitä tarkoitetaan renkaan ideaalilla ja pääideaalilla.

Määritelmä 1.9. Renkaan $(R, +, \cdot)$ epätyhjä osajoukko I on renkaan R *ideaali*, mikäli

1. $a - b \in I$ eli $a + (-b) \in I$ aina, kun $a, b \in I$.
   Siis $(I, +) \leq (R, +)$;
2. $ra \in I$ ja $ar \in I$ aina, kun $a \in I$ ja $r \in R$.

Määritelmä 1.10. Jos $(R, +, \cdot)$ on rengas ja $a \in R$, niin suppeinta renkaan R ideaalia, joka sisältää alkion a, sanotaan alkion a generoimaksi *pääideaaliksi* ja siitä käytetään merkintää (a).

Lause 1.11. *Jos $(R, +, \cdot)$ on kommutatiivinen rengas ja $a \in R$, niin*

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

Todistus. Lause on todistettu kurssilla *Algebralliset rakenteet* [3].

□

Määritellään normaali aliryhmä.

Määritelmä 1.12. Olkoon G ryhmä ja $N \leq G$. Aliryhmää N sanotaan *normaaliksi*, mikäli

$$aN = Na$$

aina, kun $a \in G$. Tällöin merkitään $N \trianglelefteq G$.

Normaalille aliryhmälle on seuraava tulos:

Lause 1.13. *Jos G on abelin ryhmä ja $N \leq G$, niin aina $N \trianglelefteq G$.*

Todistus. Lause on todistettu kurssilla *Algebran perusteet* [2].

□

Seuraus 1.14. *$(I, +)$ on ryhmän $(R, +)$ normaali aliryhmä.*

Todistus. Ideaalin määritelmän nojalla $(I, +) \leq (R, +)$ ja renkaan määritelmän nojalla $(R, +)$ on Abelin ryhmä.

Nyt lauseen 1.13 nojalla $(I, +) \trianglelefteq (R, +)$ eli $(I, +)$ on ryhmän $(R, +)$ normaali aliryhmä.

□

Esimerkki 1.15. Tutkitaan onko renkaan $(\mathbb{Z}, +, \cdot)$ epätyhjä osajoukko $(3\mathbb{Z}, +, \cdot)$ sen ideaali. Nyt

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

Selvästi $3\mathbb{Z}$ on joukon $\mathbb{Z}$ osajoukko. Koska esimerkiksi $3 \in 3\mathbb{Z}$, niin $3\mathbb{Z} \neq \emptyset$. Olkoon $A, B \in 3\mathbb{Z}$, niin että $A = 3a$ ja $B = 3b$ ja $a, b, r \in \mathbb{Z}$.

1. Nyt
$$A - B = 3a - 3b = 3(a - b) \in 3\mathbb{Z},$$
sillä $a - b \in \mathbb{Z}$.

2. Nyt
$$rA = r \cdot 3a = 3 \cdot ra \in 3\mathbb{Z}$$
ja
$$Ar = 3a \cdot r = 3 \cdot ar \in 3\mathbb{Z},$$
sillä $ra, ar \in \mathbb{Z}$.

Kohtien 1. ja 2. nojalla kolmikko $(3\mathbb{Z}, +, \cdot)$ on renkaan $(\mathbb{Z}, +, \cdot)$ ideaali.

1.4 Polynomirengas

Määritellään, mitä tarkoittaa polynomirengas.

Määritelmä 1.16. Olkoon $(K, +, \cdot)$ kunta. Merkitään

$$K[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0 \mid a_i \in K, n \in \mathbb{N}\}.$$

Tämän joukon alkioita kutsutaan *K-kertoimisiksi polynomeiksi* ja koko joukkoa $K[x]$ varustettuna polynomien yhteen- ja kertolaskulla *polynomirenkaaksi kunnan K suhteen*; Merkitään $(K[x], +, \cdot)$.

Lause 1.17. *Mikäli $f(x), g(x) \in K[x]$ sekä $g(x) \neq \mathbf{0}_K$, niin on olemassa sellaiset yksikäsitteiset polynomit $q(x), r(x) \in K[x]$, että*

$$f(x) = q(x)g(x) + r(x),$$

ja deg $r(x) <$ deg $g(x)$.

Jakoalgoritmissa esiintyvä polynomi $f(x)$ on *jaettava*, $g(x)$ *jakaja*, $q(x)$ *osamäärä* ja $r(x)$ *jakojäännös*.

Todistus. Lause on todistettu kurssilla *Algebralliset rakenteet* [3].

□

Määritellään, mitä tarkoittaa polynomirenkaan jaoton polynomi ja mitä ominaisuuksia sillä on.

Määritelmä 1.18. Polynomi $f(x) \in K[x]$ on *jaoton* polynomirenkaassa $K[x]$, mikäli $\deg f(x) \geq 1$ ja polynomia $f(x)$ ei voida esittää kahden positiivista astetta olevan polynomin tulona polynomirenkaassa $K[x]$.

Lause 1.19. *Olkoon* $f(x) \in K[x]$ *ja* $\deg f(x) = 2$ *tai* $\deg f(x) = 3$. *Tällöin* $f(x)$ *on jaoton jos ja vain jos sillä ei ole nollakohtaa kunnassa* K.

Todistus. Lause on todistettu kurssilla *Algebralliset rakenteet* [3].

□

Määritelmä 1.20. Olkoon $f(x), g(x) \in K[x]$ polynomeja, joista ainakin toinen on nollapolynomista eroava. Polynomien $f(x)$ ja $g(x)$ *suurin yhteinen tekijä* $\text{syt}(f(x), g(x))$ on polynomi $d(x) \in K[x]$, joka toteuttaa seuraavat ehdot:

1. $d(x)$ on pääpolynomi eli polynomin $d(x)$ korkeimman asteen termin kerroin on kunnan K ykkösalkio $\mathbf{1}_K$.
2. $d(x) \mid f(x)$ ja $d(x) \mid g(x)$.
3. Jos $h(x) \mid f(x)$ ja $h(x) \mid g(x)$, niin $h(x) \mid d(x)$.

Määritelmä 1.21. Jos polynomien $f(x)$ ja $g(x) \in K[x]$ suurin yhteinen tekijä on $\mathbf{1}_K$, niin sanotaan, että $f(x)$ ja $g(x)$ ovat *keskenään jaottomia polynomeja*.

Lause 1.22. *Jos* $f(x), g(x) \in K[x]$ *ovat keskenään jaottomia polynomeja, niin*

$$a(x)f(x) + b(x)g(x) = \mathbf{1}_K$$

joillakin $a(x), b(x) \in K[x]$.

Todistus. Lause on todistettu kurssilla *Algebralliset rakenteet* [3].

□

2 Tekijärengas

2.1 Johdanto

Tässä luvussa on käytetty lähteenä pääasiassa kirjaa *Advanced Modern Algebra* [1]. Muodostetaan tässä luvussa kommutatiivisesta renkaasta ja sen ideaalista tekijärengasrakenne, jota hyödynnetään kuntalaajennuksessa. Otetaan lisäksi esimerkki tekijärenkaasta, jotta lukijalle selkeytyy, mitä sillä tarkoitetaan.

2.2 Tekijäryhmä

Kerrataan aluksi, mitä tarkoittaa tekijäryhmä.

Määritelmä 2.1. Paria $(\{aN \mid a \in G\}, \cdot)$ kutsutaan *ryhmän* $(G, \cdot)$ *tekijäryhmäksi normaalin aliryhmän* N *suhteen.* Kyseisestä ryhmästä käytetään merkintää G/N.

Otetaan nyt kommutatiivisen renkaan R additiivisen ryhmän $(R, +)$ tekijäryhmä ideaalin I suhteen.

Nyt saadun tekijäryhmän $(R/I, +)$ alkiot ovat

$$(R/I, +) = (\{a + I \mid a \in R\}, +).$$

Osoitetaan, että $(R/I, +)$ on Abelin ryhmä.
Olkoon $a, b, c \in R$.

- $(+)$ on binäärinen operaatio, sillä

  $$(a + I) + (b + I) = (a + b) + I \in R/I$$

  ja on yksikäsitteinen kaikilla $a + I, b + I \in R/I$.

- $(+)$ on assosiatiivinen operaatio, sillä

  $(a+I)+((b+I)+(c+I)) = (a+I)+((b+c)+I) = (a+(b+c))+I$

  $= ((a+b)+c)+I = ((a+b)+I)+(c+I) = ((a+I)+(b+I))+(c+I)$

  kaikilla $a + I, b + I, c + I \in R/I$.

- Joukossa R/I on neutraalialkio operaation $(+)$ suhteen. Joukon neutraalialkio on $\mathbf{0}_R + I = \mathbf{0}_{R/I} \in R/I$, koska

  $(a+I)+(\mathbf{0}_R+I) = ((a+\mathbf{0}_R)+I) = a+I = ((\mathbf{0}_R+a)+I) = (\mathbf{0}_R+I)+(a+I)$

  kaikilla $a + I \in R/I$.

  Tätä alkiota nimitetään joukon R/I nolla-alkioksi.

- Jokaisella joukon R/I alkiolla on olemassa käänteisalkio joukossa R/I operaation $(+)$ suhteen.

  Alkion $a+I \in R/I$ käänteisalkio on $-a+I \in R/I$, sillä

  $$(a+I)+(-a+I) = (a-a)+I = \mathbf{0}_R + I = \mathbf{0}_{R/I}$$

  $$= \mathbf{0}_R + I = (-a+a)+I = (-a+I)+(a+I).$$

  Tätä alkiota nimitetään alkion $a+I$ vasta-alkioksi

- $(+)$ on kommutatiivinen operaatio, sillä

  $$(a+I)+(b+I) = (a+b)+I = (b+a)+I = (b+I)+(a+I)$$

  kaikilla $a+I, b+I \in R/I$.

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

Määritellään *Luonnollinen kuvaus* $\pi : (R,+) \to (R/I,+)$ seuraavasti:

$$\pi(a) = a+I.$$

2.3 Tekijärengas

Lause 2.2. *Jos I on kommutatiivisen renkaan R ideaali, niin additiivisesta Abelin ryhmästä $(R/I,+)$ saadaan sellainen kommutatiivinen rengas, että luonnollinen kuvaus $\pi : R \to R/I$ on surjektiivinen rengashomomorfismi.*

Todistus. Nyt $\pi(a) = a+I \in R/I$, $\pi(b) = b+I \in R/I$ ja $\pi(c) = c+I \in R/I$.

Määritellään additiiviselle Abelin ryhmälle R/I kertolaskuoperaatio:

$$(a+I)(b+I) = ab+I.$$

Osoitetaan seuraavaksi, että kertolaskuoperaatio on hyvin määritelty. Oletetaan, että

$$a+I = a'+I \qquad \text{ja} \qquad b+I = b'+I,$$

eli

$$a-a' \in I \qquad \text{ja} \qquad b-b' \in I.$$

Osoitetaan, että

$$(a' + I)(b' + I) = a'b' + I = ab + I = (a + I)(b + I),$$

eli

$$ab - a'b' \in I.$$

Nyt

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I,$$

sillä $a - a' \in I$ ja $b - b' \in I$.

Jotta R/I olisi kommutatiivinen rengas, täytyy osoittaa, että se on assosiatiivinen ja kommutatiivinen kertolaskuoperaation suhteen. Binäärisyys seuraa suoraan kertolaskuoperaation määritelmästä. Lisäksi täytyy osoittaa, että osittelulait ovat voimassa ja että ykkösalkio on $\mathbf{1}_R + I$. Nämä ominaisuudet periytyvät renkaasta R.

Nyt kertolaskuoperaatio on on assosiatiivinen joukossa R/I, sillä

$$(a + I) \cdot ((b + I)(c + I)) = (a + I) \cdot (bc + I) = a(bc) + I$$

$$= (ab)c + I = (ab + I) \cdot (c + I) = ((a + I)(b + I)) \cdot (c + I)$$

aina, kun $a + I,\ b + I,\ c + I \in R/I$.

Kertolaskuoperaatio on kommutatiivinen joukossa R/I, koska

$$(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I)$$

aina, kun $a + I,\ b + I \in R/I$.

Distributiivisuus- eli osittelulait ovat voimassa, sillä

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

$$= (ab + ac) + I = (ab + I) + (ac + I) = (a + I)(b + I) + (a + I)(c + I)$$

ja

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

$$= (ac + bc) + I = (ac + I) + (bc + I) = (a + I)(c + I) + (b + I)(c + I).$$

Joukon ykkösalkio on $\mathbf{1}_R + I = \mathbf{1}_{R/I} \in R/I$, sillä

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

kaikilla $a + I \in R/I$.

Kirjoittamalla yhtälö

$$(a+I)(b+I) = ab + I$$

uudelleen kuvauksen π avulla, koska $\pi(a) = a + I$ ja $\pi(b) = b + I$, saadaan

$$\pi(a)\pi(b) = \pi(ab).$$

Nyt siis saadaan

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

$$\pi(ab) = ab + I = (a+I)(b+I) = \pi(a)\pi(b) \qquad \text{ja}$$

$$\pi(\mathbf{1}_R) = (\mathbf{1}_R + I) = \mathbf{1}_{R/I}.$$

Näin ollen kuvaus π on rengashomomorfismi ja koska

$$a + I = \pi(a),$$

niin kuvaus π on myös surjektiivinen.

□

Määritelmä 2.3. Edellisessä lauseessa rakennettua kommutatiivista rengasta $(R/I, +, \cdot)$ sanotaan renkaan R *tekijärenkaaksi* ideaalin I suhteen.

Esimerkki 2.4. Muodostetaan esimerkin 1.3 renkaasta $(\mathbb{Z}, +, \cdot)$ ja esimerkin 1.15 ideaalista $(3\mathbb{Z}, +, \cdot)$ tekijärengas $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$. Nyt

$$(\mathbb{Z}/3\mathbb{Z}, +, \cdot) = (\{a + 3\mathbb{Z} \mid a \in \mathbb{Z}\}, +, \cdot),$$

joten tekijärenkaaseen kuuluvat alkiot

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

Tekijärenkaan alkioiden välillä on voimassa seuraavat yhteenlaskuoperaatiot:

$$\begin{aligned}
&(0 + 3\mathbb{Z}) + (0 + 3\mathbb{Z}) = (0 + 0) + 3\mathbb{Z} = 3\mathbb{Z},\\
&(0 + 3\mathbb{Z}) + (1 + 3\mathbb{Z}) = (0 + 1) + 3\mathbb{Z} = 1 + 3\mathbb{Z},\\
&(0 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) = (0 + 2) + 3\mathbb{Z} = 2 + 3\mathbb{Z},\\
&(1 + 3\mathbb{Z}) + (1 + 3\mathbb{Z}) = (1 + 1) + 3\mathbb{Z} = 2 + 3\mathbb{Z},\\
&(1 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) = (1 + 2) + 3\mathbb{Z} = 3 + 3\mathbb{Z} = 3\mathbb{Z},\\
&(2 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) = (2 + 2) + 3\mathbb{Z} = 4 + 3\mathbb{Z} = 1 + 3\mathbb{Z}.
\end{aligned}$$

Tekijärenkaan alkioiden välillä on seuraavat kertolaskuoperaatiot:

$$\begin{aligned}
&(0 + 3\mathbb{Z}) \cdot (0 + 3\mathbb{Z}) = (0 \cdot 0) + 3\mathbb{Z} = 3\mathbb{Z},\\
&(0 + 3\mathbb{Z}) \cdot (1 + 3\mathbb{Z}) = (0 \cdot 1) + 3\mathbb{Z} = 3\mathbb{Z},\\
&(0 + 3\mathbb{Z}) \cdot (2 + 3\mathbb{Z}) = (0 \cdot 2) + 3\mathbb{Z} = 3\mathbb{Z},\\
&(1 + 3\mathbb{Z}) \cdot (1 + 3\mathbb{Z}) = (1 \cdot 1) + 3\mathbb{Z} = 1 + 3\mathbb{Z},\\
&(1 + 3\mathbb{Z}) \cdot (2 + 3\mathbb{Z}) = (1 \cdot 2) + 3\mathbb{Z} = 2 + 3\mathbb{Z},\\
&(2 + 3\mathbb{Z}) \cdot (2 + 3\mathbb{Z}) = (2 \cdot 2) + 3\mathbb{Z} = 4 + 3\mathbb{Z} = 1 + 3\mathbb{Z}.
\end{aligned}$$

3 Kuntalaajennus

3.1 Johdanto

Tässä luvussa on käytetty lähteenä kirjaa *Advanced Modern Algebra* [1]. Kuntalaajennuksen ideana on muodostaa kunnasta K polynomirengas $K[x]$, josta otetaan jaoton polynomi $p(x)$. Jaottomasta polynomista $p(x)$ muodostetaan pääideaali $(p(x))$, ja polynomirenkaasta $K[x]$ ja pääideaalista $(p(x))$ tekijärengas $K[x]/(p(x))$. Osoitetaan, että muodostettu tekijärengas $K[x]/(p(x))$ on rakenteeltaan kunta.

3.2 Kuntalaajennus

Otetaan lemma, jota tarvitaan seuraavan lauseen todistamisessa.

Lemma 3.1. *Olkoon K kunta, $p(x), f(x) \in K[x]$ ja $d(x) = syt(p(x), f(x))$. Jos $p(x)$ on jaoton polynomi, niin*

$$d(x) = \begin{cases} \mathbf{1}_K & jos\ p(x) \nmid f(x) \\ p(x) & jos\ p(x) \mid f(x) \end{cases}.$$

Todistus. Koska $d(x) \mid p(x)$ ja $p(x)$ on jaoton polynomi, niin $d(x) = \mathbf{1}_K$ tai $d(x) = p(x)$.

□

Lause 3.2. *Jos K on kunta ja $I = (p(x))$, missä $p(x) \neq \mathbf{0}_K$ on polynomirenkaan $K[x]$ polynomi, niin tekijärengas $K[x]/I$ on kunta jos ja vain jos $p(x)$ on jaoton polynomi.*

Todistus. " $\Leftarrow$ " : Olkoon $p(x)$ jaoton polynomi. Nyt $I = (p(x))$ on pääideaali, joten tekijärenkaan $K[x]/I$ ykkösalkio $\mathbf{1}_K + I$ ei ole nolla-alkio, sillä jos näin olisi, niin ykkösalkiolla kertomisesta tulisi aina nolla-alkio ja näin ei voi olla.

Jos $\mathbf{0}_{K[x]/I} \neq f(x) + I \in K[x]/I$, niin $f(x) \notin I$.

Lauseen 1.11 mukaan ideaalin I alkiot ovat muotoa

$$I = (p(x)) = \{r(x)p(x) \mid r(x) \in K[x]\}$$

ja $f(x) \notin I$, niin $f(x)$ ei ole polynomin $p(x)$ monikerta eli $p(x) \nmid f(x)$.

Lemman 3.1 nojalla $p(x)$ ja $f(x)$ ovat keskenään jaottomia polynomeja ja lauseen 1.22 nojalla on olemassa sellaiset polynomit $s(x)$ ja $t(x)$, että $s(x)f(x) + t(x)p(x) = \mathbf{1}_K$.

Nyt

$$s(x)f(x) + t(x)p(x) = \mathbf{1}_K \Rightarrow s(x)f(x) - \mathbf{1}_K = -t(x)p(x)$$

eli $s(x)f(x) - \mathbf{1}_K$ on polynomin $p(x)$ monikerta, jolloin $s(x)f(x) - \mathbf{1}_K \in I$, joten $\mathbf{1}_K + I = s(x)f(x) + I = (s(x) + I)(f(x) + I)$.

Tällöin jokaisella tekijärenkaan $K[x]/I$ nolla-alkiosta eroavalla alkiolla on olemassa käänteisalkio, jolloin $K[x]/I$ on kunta.

" $\Rightarrow$ " : Olkoon $K[x]/I$ kunta. Tehdään vastaoletus, että $p(x)$ ei ole jaoton polynomi. Jos $p(x)$ ei ole jaoton polynomi polynomirenkaassa $K[x]$, niin se voidaan jakaa tekijöihin $p(x) = g(x)h(x)$ polynomirenkaassa $K[x]$, niin että deg $g(x) <$ deg $p(x)$ ja deg $h(x) <$ deg $p(x)$.

Kumpikaan alkioista $g(x) + I$ ja $h(x) + I$ ei voi olla nolla-alkio tekijärenkaassa $K[x]/I$, koska tekijärenkaan $K[x]/I$ nolla-alkio on $\mathbf{0}_K + I = I$. Tällöin $g(x) + I = I$, jos $g(x) \in I = (p(x))$. Vastaavasti $h(x) + I = I$, jos $h(x) \in I = (p(x))$. Mutta jos näin olisi, niin $p(x) \mid g(x)$ ja $p(x) \mid h(x)$, jolloin syntyy ristiriita deg $p(x) \leq$ deg $g(x)$ ja deg $p(x) \leq$ deg $h(x)$.

Tulos

$$(g(x) + I)(h(x) + I) = p(x) + I = I$$

on tekijärenkaan nolla-alkio ja tämä aiheuttaa ristiriidan sen kanssa, että $K[x]/I$ on kunta. Tällöin polynomin $p(x)$ täytyy olla jaoton polynomi.

□

Esimerkki 3.3. Olkoon $K = (\mathbb{R}, +, \cdot)$ kunta ja $K[x] = \mathbb{R}[x]$. Olkoon polynomirenkaassa polynomi $p(x) = x^2 + 1 \in \mathbb{R}[x]$. Nyt

$$\begin{aligned} x^2 + 1 &= 0 \\ x^2 &= -1 \end{aligned}$$

eli polynomilla $x^2 + 1$ ei ole reaalisia nollakohtia. Näin ollen lauseen 1.19 nojalla polynomi $x^2 + 1$ on jaoton polynomirenkaassa $\mathbb{R}[x]$.
Nyt siis lauseen 3.2 nojalla

$$\mathbb{R}[x]/(x^2 + 1) \text{ on kunta.}$$

Nyt tekijärenkaan määritelmän mukaan

$$\mathbb{R}[x]/(p(x)) = \{f(x) + (p(x)) \mid f(x) \in \mathbb{R}[x]\},$$

josta saadaan jakamalla polynomi $f(x)$ polynomilla $p(x)$ jakoalgoritmin mukaisesti

$$\mathbb{R}[x]/(p(x)) = \{q(x)p(x) + r(x) + (p(x)) \mid \deg r(x) < \deg p(x) = 2\}.$$

Nyt tekijärenkaan alkioiden yhteenlaskun nojalla ja koska $\deg p(x) = 2$, niin

$$\mathbb{R}[x]/(p(x)) = \{q(x)p(x) + (p(x)) + r(x) + (p(x)) \mid \deg r(x) < 2\},$$

missä $q(x)p(x) \in (p(x)) = \mathbb{R}[x] \cdot p(x)$. Nyt $q(x)p(x) + (p(x)) = 0 + (p(x))$, joten tekijärenkaan alkioiden yhteenlaskun nojalla saadaan

$$\mathbb{R}[x]/(p(x)) = \{r(x) + (p(x)) \mid \deg r(x) < 2\}.$$

Nyt koska $\deg r(x) < 2$, niin voidaan merkitä $r(x) = ax + b$, jolloin

$$\begin{aligned}\mathbb{R}[x]/(p(x)) &= \{ax + b + (p(x)) \mid a, b \in \mathbb{R}\} \\ &= \{ax + b + (x^2 + 1) \mid a, b \in \mathbb{R}\}.\end{aligned}$$

Merkitään nyt

$$\begin{aligned}0 + (x^2 + 1) &= \mathbf{0} \\ 1 + (x^2 + 1) &= \mathbf{1} \\ b + (x^2 + 1) &= \mathbf{b} \\ x + (x^2 + 1) &= \alpha \\ a + (x^2 + 1) &= \mathbf{a}\end{aligned}$$

ja huomataan, että

$$ax + b + (x^2 + 1) = (ax + (x^2 + 1)) + (b + (x^2 + 1))$$

$$= (a + (x^2 + 1)) \cdot (x + (x^2 + 1)) + (b + (x^2 + 1)) = \mathbf{a} \cdot \alpha + \mathbf{b} = \mathbf{a}\alpha + \mathbf{b}.$$

Tällöin

$$\mathbb{R}[x]/(x^2 + 1) = \{\mathbf{a}\alpha + \mathbf{b} \mid \mathbf{a}, \mathbf{b} \in \mathbb{R}\} \text{ on kunta.}$$

Nyt

$$\alpha = x + (p(x)) = x + (x^2 + 1)$$

ja

$$\alpha^2 + \mathbf{1} = \alpha \cdot \alpha + \mathbf{1} = (x + (x^2 + 1)) \cdot (x + (x^2 + 1)) + (1 + (x^2 + 1))$$

$= (x \cdot x + (x^2 + 1)) + (1 + (x^2 + 1)) = x^2 + 1 + (x^2 + 1) = 0 + (x^2 + 1) = \mathbf{0}$,
kun $x^2 + 1 \in (x^2 + 1)$.

Siis

$$\mathbb{R}[x]/(x^2 + 1) = \{\mathbf{a}\alpha + \mathbf{b} \mid \mathbf{a}, \mathbf{b} \in \mathbb{R}\}$$

on kunta ja

$$\alpha^2 + \mathbf{1} = \mathbf{0}$$

eli

$$\alpha^2 = \mathbf{-1}.$$

Näin ollen

$$\mathbb{R}[x]/(x^2 + 1) \cong (\mathbb{C}, +, \cdot).$$

Lähdeluettelo

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

[2] Myllylä, K. *Algebran perusteet*, Oulun yliopisto. 2021.

[3] Myllylä, K. *Algebralliset rakenteet*, Oulun yliopisto. 2021.