Tampereen yliopisto

Amanda Sirén

JAOLLISUUS RENKAISSA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Marraskuu 2020

Tiivistelmä

Amanda Sirén: Jaollisuus renkaissa
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Marraskuu 2020

Tässä tutkielmassa käsitellään jaollisuutta renkaissa. Lisäksi vertaillaan kokonaislukujen, polynomien ja renkaan alkioiden jaollisuutta, ja tutkitaan niiden eroja ja yhtäläisyyksiä.

Tutkielman aluksi tarkastellaan tärkeimpiä määritelmiä ja tuloksia kokonaislukuihin, polynomeihin ja renkaisiin liittyen. Tämän jälkeen käsitellään tarkemmin jaollisuutta renkaissa. Sen jälkeen vertaillaan jaollisuutta kokonaisluvuilla ja renkaan alkioilla ja lopuksi vielä polynomeilla ja renkaan alkioilla. Tätä vertailua varten tarvitaan vielä polynomirenkaan määritelmää ja siihen liittyviä tärkeitä tuloksia.

Avainsanat: jaollisuus, kokonaisluku, kommutatiivinen rengas, polynomi, polynomirengas, rengas

Sisällys

1 Johdanto

Tässä tutkielmassa käsittelemme jaollisuutta renkaissa. Sen lisäksi vertailemme jaollisuutta kokonaisluvuilla ja renkaan alkioilla sekä polynomeilla ja renkaan alkioilla.

Tutkielman luvussa 2 tarkastelemme aluksi luettelonomaisesti tärkeimpiä määritelmiä ja tuloksia kokonaislukuihin, polynomeihin ja renkaisiin liittyen. Niiden avulla pyrimme yhtenäistämään lukijan ja tutkielman käsitystä tuloksiin liityen ja esittelemään tutkielmassa käytettyjä merkintöjä. Näitä tuloksia tarvitsemme luvuissa 3 ja 4.

Luvussa 3 käsittelemme jaollisuutta renkaissa. Ensimmäiseksi esittelemme jaollisuuden määritelmän renkaissa. Sen jälkeen esitämme muita siihen liittyviä tuloksia.

Jaollisuuden vertailua käsittelemme luvussa 4. Vertailemme aluksi kokonaislukujen ja renkaan alkioiden jaollisuutta. Sen jälkeen pohdimme hieman kokonaislukujen ja polynomien jaollisuuden yhteyttä. Luvun lopuksi vertailemme myös polynomien ja renkaan alkioiden jaollisuutta. Tätä vertailua varten esittelemme myös polynomirenkaan käsitteen ja siihen liittyviä tuloksia. Polynomirengasta ja polynomien jaollisuutta käsittelemme hieman suppeammin lukijalta odotettujen pohjatietojen vuoksi.

Lukijalta edellytämme algebran perusasioiden tuntemista. Odotamme muun muassa, että lukija tuntee renkaan tarkan määritelmän sekä kommutatiivisuuden käsitteen. Lisäksi odotamme lukijalta laaja käsitystä kokonaislukujen ja polynomien jaollisuudesta. Päälähteenä käytämme Rotmanin kirjaa First Course in Abstract Algebra. Muina lähdeteoksina käytämme kahta Burtonin teosta Elementary Number Theory ja A First Course in Ringas and Ideals, Hautajärven, Ottelin ja Wallin-Jaakkolan teosta Laudatur 2: Polynomifunktiot sekä Häsän ja Rämön teosta Johdatus abstraktiin algebraan.

2 Valmistelevia tarkasteluja

Luvussa 2 esitämme lyhyesti muutamia pääaiheemme käsittelyssä tarvitsemiamme tuloksia ja lisäksi luvun 4 vertailussa tarvitsemiamme tuloksia.

2.1 Kokonaisluvuista

Tässä aliluvussa esitämme kokonaislukujen jaollisuuteen liittyviä perustuloksia, joita hyödynnämme myöhemmin luvussa 4.

Määrittelemme ensin kokonaisluvun (vrt. [5, s. 1–2]).

Määritelmä 2.1. *Kokonaisluku* on luku, joka kuuluu joukkoon $\{0, 1, -1, 2, -2, 3, \dots\}$. Kokonaislukujen joukkoa merkitään vahvennetulla kirjaimella $\mathbb{Z}$. Voidaan merkitä

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, \dots\}.$$

Seuraavaksi määrittelemme kokonaislukujen jaollisuuden (vrt. [5, s. 37]).

Määritelmä 2.2. Olkoot a ja $b \in \mathbb{Z}$. Luku b on *jaollinen* luvulla a, merkitään

$$a \mid b,$$

jos on olemassa sellainen luku $c \in \mathbb{Z}$, että $b = ac$.

Esimerkki 2.1. Olkoon $a = 3$ ja $b = -15$. Tällöin $3 \mid (-15)$, sillä $-15 = 3(-5)$. Toisaalta $3 \nmid 14$, sillä ei ole olemassa sellaista lukua $c \in \mathbb{Z}$, että $14 = 3c$.

Esittelemme seuraavaksi kokonaislukujen jaollisuudelle ominaisia tuloksia (vrt. [1, s. 20–21]).

Lause 2.1. *Olkoot $a, b, c, d, e \in \mathbb{Z}$. Tällöin ovat voimassa seuraavat tulokset:*

1. $a \mid 0, 1 \mid a, a \mid a$,
2. *Jos* $a \mid 1$, *niin* $a = \pm 1$,
3. *Jos* $a \mid b$ *ja* $c \mid d$, *niin* $ac \mid bd$,
4. *Jos* $a \mid b$ *ja* $b \mid c$, *niin* $a \mid c$,
5. *Jos* $a \mid b$ *ja* $b \mid a$, *niin* $a = \pm b$,

6. *Jos* $a \mid b$ *ja* $b \neq 0$*, niin* $|a| \leq |b|$*,*

7. *Jos* $a \mid b$ *ja* $a \mid c$*, niin* $a \mid (bx + cy)$*, kun* x *ja* y *ovat mielivaltaisia kokonaislukuja.*

Todistus. Todistamme aluksi ensimmäisen kohdan. Nyt $a \mid 0$, koska $0 = ca$, kun $c = 0$. Lisäksi $1 \mid a$, koska $a = c1$, kun $c = a$. Myös $a \mid a$, koska $a = ca$, kun $c = 1$.

Seuraavaksi todistamme toisen kohdan. Oletamme, että $a \mid 1$. Koska luku 1 on kokonaislukujoukon neutaalialkio, sen voi jakaa vain ± 1, joten $a = \pm 1$.

Seuraavaksi todistamme kohdan 3. Oletamme, että $a \mid b$ ja $c \mid d$. Nyt $b = ax$, $d = cy$, joten $bd = (ac)(xy)$. Voidaan merkitä $ac \mid bd$.

Seuraavaksi toidstamme kohdan 4. Oletamme, että $a \mid b$ ja $b \mid c$. Nyt $b = ae$ ja $c = bd$, joten $c = a(de)$, joten $a \mid c$.

Seuraavaksi todistamme kohdan 5. Oletamme, että $a \mid b$ ja $b \mid a$. Nyt $b = ca$ ja $a = db$. Nyt $a = dca$, joten $dc = 1$ (tai $a = b = 0$). Siis $d = \pm 1$ ja $c = \pm 1$. Siis $a = \pm b$.

Seuraavaksi todistamme kohdan 6. Oletamme, että $a \mid b$ ja $b \neq 0$. Nyt $b = ca$. Jos $|a| > |b|$, niin $c \notin \mathbb{Z}$. Joten täytyy olla, että $|a| \leq |b|$.

Lopuksi todistamme viimeisen kohdan. Oletamme, että $a \mid b$ ja $a \mid c$. Nyt $b = ad$, $c = ae$, joten $bx + cy = a(dx + ey)$. Näin ollen $a \mid (bx + cy)$.

Näin olemme todistaneet lauseen 2.1 kaikki kohdat. □

2.2 Polynomeista

Tässä aliluvussa esitämme polynomien jaollisuuteen liittyviä perustuloksia (vrt. [3, s. 6–24]), joita hyödynnämme myöhemmin luvussa 4.

Määrittelemme ensin polynomin (vrt. [3, s. 6–7]).

Määritelmä 2.3. *Polynomiksi* kutsutaan summalauseketta, jossa on muuttujien tuloja ja skalaarilla kertomisia, mutta muuttuja ei esiinny nimittäjässä.

Polynomeja merkitään usein isoilla kirjaimilla $P, Q, R \ldots$. Esimerkiksi

$$P(a) = a^2 + 2a - 1$$
$$R(x, y) = -x^2y^3 + xy^5$$

ovat polynomeja. Polynomeille voidaan laskea arvoja eri muuttujien arvoilla samoin kuin funktioille.

Esimerkki 2.2. Lausekkeet $2x^3 - 4x^2 + x - 10$ ja $\frac{a^2}{3} + 5ab - \frac{b^2}{6} + 1$ ovat polynomeja.

Seuraavaksi määrittelemme polynomien jaollisuuden.

Määritelmä 2.4. Olkoot S ja P polynomeja. Merkitään

$$P(x) = Q(x)S(x) + R(x),$$

missä $Q(x)$ on jakolaskun osamäärä ja $R(x)$ on jakojäännös. Jos jako menee tasan, voidaan sanoa, että *polynomi* $P(x)$ *on jaollinen* polynomilla $S(x)$ ja merkitään $S(x) \mid P(x)$.

Määritelmä 2.5. Joskus jakolaskua ei voi laskea siten, että vastaukseksi saisi polynomin. Jos nimittäjään jää muuttuja, sanotaan lauseketta *rationaali-* eli *murtolausekkeeksi* (vrt. [3, s. 21]).

Esimerkki 2.3. Olkoot $A(x, y) = 3xy^2$ ja $B(x, y) = 12x^2y$. Nyt

$$\frac{B(x, y)}{A(x, y)} = \frac{12x^2y}{3xy^2} = \frac{4x}{y}.$$

Tällöin vastausta kutsutaan määritelmän 2.5 nojalla rationaalilausekkeeksi.

Esimerkki 2.4. (Vrt. [3, s. 24].) Luku on jaollinen kolmella, jos sen numerojen summa on kolmella jaollinen. Esimerkiksi luvun 123 numeroiden summa 1+2+3 = 6 on kolmella jaollinen ja myös luku 123 on itse kolmella jaollinen.

Jaollisuussäännön voi johtaa osittelulain avulla. Nelinumeroinen luku $abcd$ voidaan esittää muodossa

$$abcd = 1000a + 100b + 10c + d = (999 + 1)a + (99 + 1)b + (9 + 1)c + d.$$

Oletetaan, että luku $abcd$ on jaollinen kolmella.

Merkitään

$$abcd = 1000a + 100b + 10c + d = (999 + 1)a + (99 + 1)b + (9 + 1)c + d.$$

Nyt osittelulain nojalla

$$(999 + 1)a + (99 + 1)b + (9 + 1)c + d = 999a + 1a + 99b + 1b + 9c + 1c + d.$$

Tällöin termit $999a$, $99b$ ja $9c$ ovat triviaalisti kolmella jaollisia, joten luvun $abcd$ kolmella jaollisuus riippuu nyt lukujen a, b, c ja d summasta $a + b + c + d$.

Näin olemme todistaneet, että nelinumeroinen luku $abcd$ on jaollinen kolmella, jos sen numerojen summa on jaollinen kolmella.

2.3 Renkaista

Tässä aliluvussa esitämme renkaisiin liittyviä tuloksia, joita tarvitsemme myöhemmin luvussa 3.

Ensin määrittelemme renkaan käsitteen (vrt. [2, s. 1]).

Määritelmä 2.6. *Rengas* on järjestetty kolmikko $(R, +, \cdot)$, joka sisältää epätyhjän ryhmän R ja kaksi laskutoimitusta $+$ ja $\cdot$, jotka on määritelty joukossa R siten, että

1. $(R, +)$ on kommutatiivinen ryhmä,
2. $(R, \cdot)$ on puoliryhmä,
3. laskutoimitus $\cdot$ on distributiivinen (molemmilta puolilta) laskutoimituksen $+$ suhteen.

   Toisin sanoen on voimassa aksioomat:

4. $a + b = b + a$ aina, kun $a, b \in R$,
5. $a + (b + c) = (a + b) + c$ aina, kun $a, b, c \in R$,
6. on olemassa sellainen alkio $0 \in R$, että $0 + a = a$ aina, kun $a \in R$,
7. aina, kun $a \in R$, on olemassa sellainen alkio $a' \in R$, että $a' + a = 0$,
8. $a(bc) = (ab)c$ aina, kun $a, b, c \in R$,
9. on olemassa sellainen alkio $1 \in R$, jota kutsutaan ykkösalkioksi, että $1a = a$ aina, kun $a \in R$,
10. $a(b + c) = ab + ac$ aina, kun $a, b, c \in R$, ja $(a + b)c = ac + bc$ aina, kun $a, b, c \in R$.

Esittelemme seuraavaksi kommutatiivisen renkaan määritelmän (vrt. [5, s. 216]).

Määritelmä 2.7. *Kommutatiivisessa renkaassa* R on on määritelty edellisten lisäksi myös seuraava ominaisuus, kun $a, b \in R$:

$$ab = ba.$$

Esimerkki 2.5. Kokonaislukujen joukko $\mathbb{Z}$ on kommutatiivinen rengas, jossa on määritelty yhteenlasku ja kertolasku (edellä olevat aksioomat ovat voimassa laskutoimitusten suhteen). (Vrt. [5, s. 216].)

Huomautus. Määritelmän 2.6 aksioomista 4 – 7 voimme huomata, että R on *Abelin ryhmä* yhteenlaskun suhteen.

Lause 2.2. *Jos R on kommutatiivinen rengas, jossa $1 = 0$, niin tällöin renkaalla R on vain yksi alkio: $R = \{0\}$. Sitä kutsutaan* nollarenkaaksi.

Todistus. Sivuutetaan. (Vrt. [5, s. 220].) □

Määritelmä 2.8. (Vrt. [5, s. 220].) Kommutatiivinen rengas (jossa $1 \neq 0$) on *kokonaisalue*, jos siellä on supistussääntö:

$$\text{Jos } ca = cb \text{ ja } c \neq 0, \text{ niin } a = b.$$

3 Jaollisuus renkaissa

Luvussa 3 käsittelemme jaollisuutta renkaissa. Esittelemme ensin jaollisuuden määritelmän ja lisäksi käsittelemme sen muita ominaisuuksia (vrt. [5, s. 224–226]).

Määritelmä 3.1. Olkoot a ja b kommutatiivisen renkaan R alkioita. Tällöin alkio a *jakaa* alkion b *renkaassa* R (eli alkio a on alkion b jakaja eli alkio b on alkion a monikerta), merkitään

$$a \mid b,$$

jos on olemassa sellainen alkio $c \in R$, että $b = ca$.

Esimerkki 3.1. Olkoot a ja b kommutatiivisen renkaan R alkioita. Jos $0 \mid a$, tällöin $a = 0 \cdot b$. Kun $0 \cdot b = 0$, täytyy olla $a = 0$. Täten $0 \mid a$, jos $a = 0$.

Huomautus. Jaollisuus $a \mid b$ ei riipu vain alkioista a ja b vaan myös kommutatiivisesta renkaasta R.

Esimerkki 3.2. Olkoon a ja b kommutatiivisen renkaan R alkioita. Olkoon $a = 5$, $b = 2$ ja $R = \mathbb{Q}$. Tällöin $a \mid b$ eli $5 \mid 2$. Eli on olemassa sellainen alkio $c \in \mathbb{Q}$, että $2 = 5 \cdot c$. Tällöin $c = \frac{2}{5}$.

Toisaalta, jos rengas $R = \mathbb{Z}$, niin jaollisuus ei päde. Ei ole olemassa sellaista alkiota $c \in R$, että $2 = 5 \cdot c$.

Määritelmä 3.2. Olkoon R kommutatiivinen rengas ja $a, b, c \in R$. Tällöin renkaan R alkioiden *lineaarikombinaatio* on $sa + tb$, missä $s, t \in R$.

Määritelmä 3.3. Olkoon $u \in R$. Jos on olemassa sellainen alkio $v \in R$, että $uv = 1$, niin alkio v on alkion u *käänteisalkio*. Merkitään u^{-1}. Jos alkiolla on käänteisalkio, se on *yksikkö*.

Olkoon $a \in R$. Kun $r \in R$, tällöin alkio a on *liitännäinen* alkion r kanssa, jos on olemassa yksikkö $u \in R$ siten, että $a = ur$.

Lause 3.1. *(Vrt. [2, s. 91].) Olkoon R kommutatiivinen rengas ja $a, b, c \in R$.*

1. $a \mid 0$, $1 \mid a$, $a \mid a$,
2. *Jos* $a \mid 1$, *niin a on yksikkö,*
3. *jos* $a \mid b$ *ja* $c \mid d$, *niin* $ac \mid bd$,

4. *jos* $a \mid b$ *ja* $b \mid c$*, niin* $a \mid c$*,*

5. *jos* $a \mid b$ *ja* $a \mid c$*, niin* a *jakaa kaikki* $bx + cy$*, kun* $x, y \in R$*.*

Todistus. Aloitetaan todistamalla ensimmäinen kohta. Nyt $a \mid 0$, koska $0 = ca$, kun $c = 0$. Lisäksi $1 \mid a$, koska $a = c1$, kun $c = a$. Edellisen nojalla $a \mid a$, koska $a = ca$, kun $c = 1$.

Seuraavaksi todistamme kohdan 2. Oletamme, että $a \mid 1$. Merkitään $1 = ca$. Nyt määritelmän 3.3 nojalla $c = a^{-1}$ eli alkio a on kääntyvä.

Seuraavaksi todistamme kolmannen kohdan. Oletamme, että $a \mid b$ ja $c \mid d$. Nyt $b = ax$ ja $d = cy$, joten $bd = (ac)(xy)$. Voidaan merkitä $ac \mid bd$.

Seuraavaksi todistamme kohdan 4. Oletamme, että $a \mid b$ ja $b \mid c$. Nyt $b = ae$ ja $c = bd$, joten $c = a(de)$, joten $a \mid c$

Lopuksi todistamme viidennen kohdan. Oletamme, että $a \mid b$ ja $a \mid c$. Nyt $b = ad$ ja $c = ae$, joten $bx + cy = a(dx + ey)$. Näin ollen $a \mid (bx + cy)$.

Näin olemme todistaneet kaikki kohdat. □

Lause 3.2. *(Vrt. [2, s. 92].) Olkoot* a *ja* b *kokonaisalueen* R *nollasta poikkeavia alkioita. Tällöin seuraavat kohdat ovat yhtäpitäviä:*

1. a *ja* b *ovat liitännäisiä,*

2. $a \mid b$ *ja* $b \mid a$*,*

3. $(a) = (b)$*, missä* $(a) = \{ra | r \in R\}$ *alkion* a *generoima pääihanne [vastaavasti* (b)*].*

Todistus. Oletetaan, että $a = bu$, kun u on kääntyvä. Tällöin $b = au^{-1}$, joten $a \mid b$ ja $b \mid a$. Jos $a \mid b$, voidaan merkitä $b = ax$, kun $x \in R$. Jos $b \mid a$, voidaan merkitä $a = by$, kun $y \in R$. Edelleen $b = (by)x = b(yx)$. Kun $b \neq 0$, supistussäännön nojalla $1 = yx$. Näin ollen alkiolla y on käänteisalkio renkaassa R. Nyt $a = by$, joten a ja b ovat liitännäisiä.

Nyt olemme todistaneet, että kohdat 1. ja 2. ovat yhtäpitäviä.

Kun $a \mid b$, voidaan merkitä $b = ac$, kun $c \in R$. Nyt siis $b \in (a)$, eli $(b) \subseteq (a)$. Kun $b \mid a$, voidaan merkitä $a = bd$, kun $d \in R$. Nyt siis $a \in (b)$, eli $(a) \subseteq (b)$. Edellisistä voidaan päätellä, että $(a) = (b)$.

Nyt olemme todistaneet, että kohdasta 2. seuraa kohta 3..

Jos $(a) = (b)$, niin edellisestä voidaan todeta, että $a = by$, kun $y \in R$, ja $b = ax$, kun $x \in R$. Tästä seuraa edelleen samoin kuin edellä jo todistettiin, että $a \mid b$ ja $b \mid a$.

Nyt olemme todistaneet, että kohdasta 3. seuraa kohta 2..

Näin ollen olemme todistaneet koko lauseen. □

Lause 3.3. *Olkoon R kokonaisalue ja $a, b \in R$. Nyt $a \mid b$ ja $b \mid a$, jos ja vain jos on olemassa yksikkö $u \in R$ siten, että $b = ua$.*

Todistus. Jos $a \mid b$ ja $b \mid a$, on olemassa sellaiset alkiot $u, v \in R$, että $b = ua$ ja $a = vb$. Eli $b = ua = uvb$. Kun $b = 1b$ ja $b \neq 0$, supistussäännön nojalla kokonaisalueessa R pätee, $1 = uv$, joten alkio u on yksikkö.

Päinvastoin, oletetaan, että $b = ua$, missä $u \in R$ ja alkio u on yksikkö. Selvästi, $a \mid b$. Olkoon $uv = 1$. Tällöin $vb = vua = a$, ja täten $b \mid a$. □

4 Jaollisuuden vertailua

Luvussa 4 tarkastelemme jaollisuuden eroja kokonaisluvuilla, polynomeilla ja renkaan alkioilla. Aliluvuissa 2.1 ja 2.2 ja luvussa 3 käsittelimme jaollisuuden määritelmiä kokonaislukujen, polynomien ja renkaiden osalta. Aliluvussa 4.1 käsittelemme kokonaislukujen ja renkaan alkioiden jaollisuutta. Aliluvussa 4.2 käsittelemme polynomien ja renkaan alkioiden jaollisuutta.

4.1 Kokonaisluvut ja renkaat

Kuten aliluvun 2.3 esimerkissä 2.5 totesimme, kokonaislukujen joukko $\mathbb{Z}$ on kommutatiivinen rengas. Siitä voimme edelleen todeta, että kokonaislukujen joukon $\mathbb{Z}$ jaollisuus on osa renkaiden jaollisuutta. Siinä pätee siis samat säännöt kuin renkaiden jaollisuuden yhteydessä on esitetty. (Vrt. luku 3.)

Kuten luvun 3 huomautuksessa totesimme, jaollisuus renkaissa riippuu alkioiden lisäksi myös renkaasta. Sama siis pätee kokonaislukujen joukossa ja tämän huomasimme aliluvun 2.1 esimerkistä 2.1.

Seuraavaksi esitämme havainnollistavan esimerkin kokonaislukujen tapauksesta.

Esimerkki 4.1. Olkoot $a, b \in \mathbb{Z}$. Nyt $a \mid b$, jos on olemassa alkio $c \in \mathbb{Z}$ siten, että $a = bc$.

Kun puhutaan kokonaislukujen jaollisuudesta, on tiedossa tietty joukko, jossa luvut ovat määritelty. Nyt tässä tapauksessa $a, b, c \in \mathbb{Z}$. Jaollisuus riippuu siis myös joukosta $\mathbb{Z}$. Kun taas puhutaan joukosta $\mathbb{Z}$ renkaana, niin puhutaan myös alkioiden a ja b jaollisuudesta renkaassa, silloin kyseessä on rengas $\mathbb{Z}$. Se jää kuitenkin kokonaislukujen jaollisuudessa usein sanomatta, että $\mathbb{Z}$ on rengas. Usein puhutaan vain kokonaislukujen joukosta.

Kokonaislukujen jaollisuus on siis sama asia kuin jaollisuus renkaassa $\mathbb{Z}$, joten voidaan todeta, että kokonaislukujen jaollisuus menee samalla tavalla kuin renkaiden jaollisuus.

4.2 Polynomit ja renkaat

Polynomien jakolaskun vastauksen voi esittää kaikilla samoilla tavoilla kuin kokonaislukujen jakolaskun vastauksen (vrt. [3, s. 23]). Jakolaskun $\frac{P(x)}{Q(x)}$ vastaus voidaan

kirjoittaa mutoon $\frac{P(x)}{Q(x)} = S(x)$ jää $R(x)$ tai muotoon $\frac{P(x)}{Q(x)} = S(x) + \frac{R(x)}{Q(x)}$. Jakoyhtälönä vastaus on muotoa $P(x) = Q(x) \cdot S(x) + R(x)$.

Vertailua helpottamaan käsittelemme polynomirenkaan käsitettä. Polynomirenkaaseen liittyvät tulokset pohjautuvat Häsän ja Rämön teokseen [4, s. 260-276]. Polynomirenkaaseen liittyviä tuloksia käsittelemme melko suppeasti, koska laajempi käsittely vaatisi lukijalta enemmän algerballisia pohjatietoja muun muassa kunnan käsitteen osalta.

Ensin määrittelemme polynomirenkaan.

Määritelmä 4.1. Olkoon R vaihdannainen rengas. Yhden muuttujan R-kertoimista polynomia voidaan merkitä äärellisenä summana,

$$\sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + \cdots + a_n x^n,$$

missä $n \in \mathbb{Z}_+$ ja $a_k \in R$ kaikilla k. Alkioita $a_0, a_1, \ldots, a_n$ sanotaan polynomin *kertoimiksi* ja rengasta R *kerroinrenkaaksi*. Kaikkien R-kertoimisten polynomien muodostamaa joukkoa merkitään $R[x]$.

Seuraavaksi esitämme kommutatiivisuuden renkaassa R polynomien rakenteen.

Määritelmä 4.2. Olkoon rengas R kommutatiivinen ja polynomit $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ ja $Q(x) = b_0 + b_1 x + \cdots + b_m x^m \in R[x]$, missä $n, m \in \mathbb{Z}$ ja $n, m \geq 0$.

Tällöin polynomeille on määritelty seuraavat laskutoimitukset:

1. $P(x) + Q(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_m x^m$,
2. $P(x)Q(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + a_n b_m x^{n+m}$.

Huomautus. Joukko $R[x]$ on kommutatiivinen rengas laskutoimitusten $+$ ja $\cdot$ suhteen.

Seuraavaksi esittelemme polynomin asteen määritelmän.

Määritelmä 4.3. (Vrt. [4, s. 265].) Olkoon $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ jonkin vaihdannaisen renkaan R polynomi. Oletetaan, että $a_n \neq 0$. Lukua n kutsutaan polynomin *asteeksi* ja sitä merkitään $\deg(P)$.

Seuraavaksi määrittelemme polynomien jaollisuuden polynomirenkaassa.

Määritelmä 4.4. (Vrt. [4, s. 270].) Olkoon rengas R kommutatiivinen rengassa ja P ja $Q \in R[x]$. *Polynomi P on jaollinen polynomilla Q*, jos on olemassa polynomi $S \in R[x]$ siten, että $P = QS$. Tällöin merkitään $Q \mid P$.

Seuraavaksi määrittelemme polynomien jaottomuuden.

Määritelmä 4.5. (Vrt. [4, s. 270].) Polynomi $P \in R(x)$ on *jaoton*, jos se ei ole vakiopolynomi eikä kahden positiivista astetta olevan polynomin tulo.

Esimerkki 4.2. (Vrt. [4, s. 270].) Oletetaan, että $\deg(P) = 1$. Tällöin P ei ole vakiopolynomi. Jos $P = QR$, kun $\deg(Q) \geq 1$ ja $\deg(R) \geq 1$, niin tällöin $\deg(P) = \deg(Q) + \deg(R) \geq 2$. Tämä on ristiriita, joten polynomi P on jaoton.

Tulon asteesta tarkemmin ([4, s. 265]).

Jo edellä esitettyjen tulosten pohjalta voimme todeta, että polynomien jaollisuus mukailee samoja sääntöjä ja tapoja kuin renkaiden ja kokonaislukujen tapauksessa erityisesti, kun tarkastelussamme on yhden muuttujan polynomit. Polynomien jaollisuuden tarkastelu on nyt hieman suppeampi kuin lähdekirjallisuudessa, sillä sen tarkempi läpikäyminen vaatisi lukijalta enemmän valmiuksia algebrallisten ominaisuuksien tuntemiseen. Tämän vuoksi esittelimme vain olennaisimmat tulokset hyvin suppeasti. Niin kuin kokonaislukujenkin tapauksessa myös polynomeilla on sellaisia alkioita, jotka eivät ole jaollisia.

Kokonaislukujen jaollisuus on tiukemmin sidoksissa renkaaseen, koska kokonaislukujen joukko itsessään on rengas. Sen sijaan satunnainen polynomi voi olla jaollinen muuten, kuin tietyssä polynomirenkaassa. Esimerkiksi kahden muuttujan polynomi voi olla jaollinen jollain satunnaisella polynomilla, mutta kun polynomi asetetaan tiettyyn polynomirenkaaseen, saattaa jaollisuus kumoutua.

Lähteet

[1] Burton, *Elementary Number Theory*. New York: McGraw-Hill, 2007.

[2] Burton, *A First Course in Rings and Ideals*. Massachusetts: Addison-Wesley Publishing Company, Inc, 1970.

[3] Hautajärvi, Ottelin, Wallin-Jaakkola, *Laudatur 2: Polynomifunktiot*. Helsinki: Otava, 2005.

[4] Häsä, Rämö, *Johdatus abstraktiin algebraan*. Helsinki: Gaudeamus, 2015.

[5] Rotman, *First Course in Abstract Algebra*. New Jersey: Prentice Hall, 2006.