Polynomien suurin yhteinen tekijä ja kongruenssi

Pro gradu -tutkielma
Outi Aksela
2117470
Matemaattisten tieteiden laitos
Oulun yliopisto
Syksy 2016

Sisältö

Johdanto

Pro gradu -tutkielman aiheena on polynomien suurin yhteinen tekijä ja polynomien kongruenssi. Luvuissa 1 ja 2 on käytetty pääosin lähdeteosta [2]. Luvussa 3 on käytetty sekä lähdettä [1] että lähdettä [2]. Lähteitä [1] ja [3] on käytetty pääosin luvuissa 4 ja 5.

Tutkielman aihetta lähestytään renkaiden perusmääritelmistä ja -lauseista. Rakenteellisesti tutkielma on jaettu lukuihin, joissa määritelmät ja lauseet vaikeutuvat loppua kohden. Luvuissa $1-3$ käydään läpi niitä asioita, joita tarvitaan tutkielman varsinaisen aiheen ymmärtämisessä luvuissa 4 ja 5.

Luvussa 1 käsitellään renkaan, alirenkaan ja ideaalin määritelmiä ja tärkeimpiä lauseita. Renkaalle määritellään sen ideaalin suhteen tekijärengas, jolle määritellään kaksi laskutoimitusta, yhteen- ja kertolasku.

Kuntalaajennus esitetään luvussa 2, jota lähestytään määrittelemällä ensin kunta. Kunta muodostuu, kun kommutatiivinen rengas sisältää jokaisen nolla-alkiosta eroavan alkionsa käänteisalkiot. Kuntalaajennus saadaan, kun muodostetaan renkaan ja sen maksimaalisen ideaalin avulla tekijärengas. Tämä tekijärengas on rakenteeltaan kunta.

Luvussa 3 määritetään polynomirengas ja sille lauseita, joita tarvitaan myöhemmin tutkielmassa. Polynomeille määritellään jakoalgoritmi, jolla saadaan polynomi esitettyä muiden polynomien avulla.

Polynomien suurin yhteinen tekijä ja polynomien kongruenssi on esitetty omissa luvuissaan. Luvussa 4 määritellään polynomien suurin yhteinen tekijä ja erilaisia ominaisuuksia. Samassa luvussa esitetään Eukleideen algoritmi, jolla voi määrittää kahdelle polynomille suurimman yhteisen tekijän.

Luvussa 5 käydään läpi polynomien kongruenssia ensin määritellen ja sen jälkeen esittäen uusia ominaisuuksia. Polynomien kongruenssin avulla saadaan määriteltyä uusi rengas, jäännösluokkarengas. Jäännösluokkarengas muodostetaan polynomirenkaan ja sen jonkin polynomin avulla. Kun tämä polynomi on jaoton polynomirenkaassa, niin jäännösluokkarengas on rakenteeltaan kunta.

1 Renkaat

Tässä luvussa käydään läpi algebran käsitettä rengas ja siihen liittyviä perusmääritelmiä ja -lauseita. Rengas sisältää kaksi binääristä laskutoimitusta, yhteen- ja kertolaskun. Tuttuja esimerkkejä renkaista ovat kokonaislukujen ja reaalilukujen joukot. Renkaalle voidaan määrittää erilaisia osajoukkoja, esimerkiksi alirengas ja ideaali. Tässä luvussa viimeisenä määritetään renkaalle tekijärengas.

1.1 Rengas

Määritelmä 1.1. Kolmikko $(R, +, \cdot)$ on *rengas*, jos

1. $(R, +)$ on Abelin ryhmä:
   - $a + b \in R$ kaikilla $a, b \in R$;
   - $(a + b) + c = a + (b + c)$ kaikilla $a, b, c \in R$;
   - on olemassa nolla-alkio $\mathbf{0} \in R$, jolle
   $$a + \mathbf{0} = \mathbf{0} + a = a \quad \text{kaikilla} \quad a \in R;$$
   - jokaiselle $a \in R$ on olemassa vasta-alkio $-a \in R$, jolle
   $$a + (-a) = (-a) + a = \mathbf{0};$$
   - $a + b = b + a$ kaikilla $a, b \in R$.
2. $(R, \cdot)$ on monoidi:
   - $a \cdot b \in R$ kaikilla $a, b \in R$;
   - $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ kaikilla $a, b, c \in R$;
   - on olemassa ykkösalkio $\mathbf{1} \in R$, jolle
   $$\mathbf{1} \cdot a = a \cdot \mathbf{1} = a \quad \text{kaikilla} \quad a \in R.$$
3. Osittelulait ovat voimassa:
   - $a \cdot (b + c) = a \cdot b + a \cdot c$ kaikilla $a, b, c \in R$;
   - $(a + b) \cdot c = a \cdot c + b \cdot c$ kaikilla $a, b, c \in R$.

Määritelmä 1.2. Rengas $(R, +, \cdot)$ on *kommutatiivinen rengas*, jos $a \cdot b = b \cdot a$ kaikilla $a, b \in R$.

Jatkossa käytetään merkintää $ab = ba$.

Lause 1.3. *Jos R on rengas ja $a, b, c \in R$, niin*

1. $\mathbf{0} \cdot a = a \cdot \mathbf{0} = \mathbf{0}$;
2. $a(-b) = (-a)b = -(ab)$;
3. $(-a)(-b) = ab$;
4. $a(b-c) = ab - ac \quad ja \quad (a-b)c = ac - bc$.

Merkinnällä $b - c$ tarkoitetaan yhteenlaskua $b + (-c)$.

Todistus. 1. Kirjoittamalla

$$\mathbf{0} \cdot a = (\mathbf{0} + \mathbf{0}) \cdot a = \mathbf{0} \cdot a + \mathbf{0} \cdot a$$

ja vähentämällä puolittain alkio $\mathbf{0} \cdot a$ saadaan $\mathbf{0} = \mathbf{0} \cdot a$. Samoin saadaan

$$a \cdot \mathbf{0} = a \cdot (\mathbf{0} + \mathbf{0}) = a \cdot \mathbf{0} + a \cdot \mathbf{0}$$

ja nyt vähentämällä puolittain alkio $a \cdot \mathbf{0}$ saadaan $\mathbf{0} = a \cdot \mathbf{0}$. Siis

$$\mathbf{0} \cdot a = a \cdot \mathbf{0} = \mathbf{0}.$$

2. Koska

$$ab + a(-b) = a(b + (-b)) = a \cdot \mathbf{0} = \mathbf{0},$$

niin alkio $a(-b)$ on alkion ab vasta-alkio. Samoin saadaan, että

$$ab + (-a)b = (a + (-a))b = \mathbf{0} \cdot b = \mathbf{0},$$

joten alkio $(-a)b$ on alkion ab vasta-alkio. Vasta-alkion yksikäsitteisyyden nojalla

$$a(-b) = (-a)b = -(ab).$$

3. Edellisen kohdan avulla saadaan

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab.$$

4. Olkoon $a, b, c \in R$. Nyt

$$a(b-c) = a(b + (-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac.$$

Vastaavasti

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

□

1.2 Alirengas

Määritelmä 1.4. Olkoon $(R, +, \cdot)$ rengas ja S renkaan R epätyhjä osajoukko. Jos $(S, +, \cdot)$ on rengas, jolla on sama ykkösalkio kuin renkaalla R, niin sitä sanotaan renkaan R *alirenkaaksi.*

Lause 1.5 (Alirengaskriteeri)**.** *Olkoon R rengas ja $S \subseteq R$. Tällöin S on renkaan R alirengas, jos ja vain jos*

1. $1_R \in S$;
2. $a - b \in S \quad kaikilla \quad a, b \in S$;
3. $ab \in S \quad kaikilla \quad a, b \in S$.

Todistus. Olkoon S renkaan R alirengas. Tällöin renkaan ja alirenkaan määritelmistä seuraa suoraan vaaditut ehdot.

Oletetaan nyt, että ehdot $1 - 3$ ovat voimassa. Ehdosta 1 seuraa, että $S \neq \emptyset$. Ehdosta 2 saadaan $a - b \in S$ eli $a + (-b) \in S$, joten $(S, +)$ on ryhmän $(R, +)$ aliryhmä. Siis $(S, +)$ on ryhmä ja tarkemmin Abelin ryhmä, koska $a + b = b + a$ kaikilla $a, b \in S$.

Ehtojen 1 ja 3 nojalla voidaan sanoa, että $(S, \cdot)$ on monoidi. Koska R on rengas ja $S \subseteq R$, niin osittelulait ovat voimassa. Tällöin $(S, +, \cdot)$ on rengas ja $1_S = 1_R$ eli S on renkaan R alirengas. □

1.3 Ideaali

Määritelmä 1.6. Renkaan $(R, +, \cdot)$ epätyhjä osajoukko I on *ideaali*, mikäli

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

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

Lause 1.7. *Jos I on renkaan R ideaali ja $\mathbf{1} \in I$, niin $I = R$.*

Todistus. Olkoon alkio $r \in R$ mielivaltainen ja $\mathbf{1} \in I$. Tällöin ideaalin määritelmän kohdan 2 nojalla $r \cdot \mathbf{1} = r \in I$ kaikilla $r \in R$. Siis $R \subseteq I$ ja toisaalta $I \subseteq R$. Näin ollen $I = R$. □

Lause 1.8 (Ideaalikriteeri)**.** *Olkoon R rengas ja $I \subseteq R$. Tällöin I on renkaan R ideaali, jos ja vain jos*

1. $I \neq \emptyset$;

2. $a - b \in I \quad kaikilla \quad a, b \in I$ *;*

3. $ra \in I \quad ja \quad ar \in I \quad kaikilla \quad r \in R, \quad a \in I.$

Todistus. Seuraa suoraan ideaalin määritelmästä. □

Määritelmä 1.9. Jos $(R, +, \cdot)$ on rengas ja $a \in R$, niin suppeinta ideaalia, joka sisältää alkion a, sanotaan alkion a generoimaksi *pääideaaliksi.* Tätä ideaalia merkitään (a).

Lause 1.10. *Jos* $(R, +, \cdot)$ *on kommutatiivinen rengas ja* $a \in R$*, niin* $(a) = Ra = \{ra \,|\, r \in R\}$.

Todistus. Nyt $Ra \subseteq R$ ja $Ra \neq \emptyset$. Osoitetaan ensin, että Ra on renkaan R ideaali.

1. Osoitetaan, että $(Ra, +)$ on ryhmän $(R, +)$ aliryhmä. Olkoon $b, c \in Ra$ eli $b = r_1 a$ ja $c = r_2 a$, missä $r_1, r_2 \in R$. Nyt

$$b - c = r_1 a - r_2 a = (r_1 - r_2)a \in Ra,$$

   joten $(Ra, +) \leq (R, +)$.

2. Olkoon $x \in R$ ja $y \in Ra$ eli $y = ra$, missä $r \in R$. Nyt

$$xy = x \cdot ra = (xr)a \in Ra$$

   ja

$$yx = (ra)x = r(ax) = r(xa) = (rx)a \in Ra.$$

Siis Ra on renkaan R ideaali.

Lisäksi $a \in Ra$, koska $a = \mathbf{1} \cdot a \in Ra$.

Osoitetaan nyt, että Ra on suppein sellainen ideaali, joka sisältää alkion a. Olkoon J sellainen renkaan R ideaali, että $a \in J$. Nyt $ra \in J$ kaikilla $r \in R$ eli $Ra \subseteq J$. Näin ollen Ra on suppein ideaali, joka sisältää alkion a.

Näin ollen $Ra = (a)$.

□

Määritelmä 1.11. Jos renkaan $(R, +, \cdot)$ jokainen ideaali on pääideaali, niin rengas R on *pääideaalirengas.*

Määritelmä 1.12. Renkaan $(R, +, \cdot)$ ideaali M on *maksimaalinen*, mikäli

1. $M \neq R$;

2. jos I on renkaan R ideaali ja $M \subset I \subseteq R$, niin $I = R$.

1.4 Tekijärengas

Renkaalle $(R, +, \cdot)$ voidaan määritellä *tekijärengas* ideaalin I suhteen, jota merkitään $(R/I, +, \cdot)$. Tekijärenkaalle määritellään kaksi laskutoimitusta, yhteen- ja kertolasku.

Olkoon $(R, +, \cdot)$ rengas ja I renkaan $(R, +, \cdot)$ ideaali. Nyt ryhmä $(I, +)$ on ryhmän $(R, +)$ aliryhmä ja koska $(R, +,)$ on Abelin ryhmä, niin $(I, +) \trianglelefteq (R, +)$ eli $(I, +)$ on ryhmän $(R, +)$ normaali aliryhmä. Näin ollen tekijäryhmä $(R/I, +)$ on olemassa. Tekijäryhmän $(R/I, +)$ alkioina ovat aliryhmän $(I, +)$ vasemmat sivuluokat ryhmässä $(R, +)$ eli alkiot $r + I = \{r + i \,|\, i \in I\}$, missä $r \in R$. Sivuluokkien yhteenlasku määritellään siten, että

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

aina, kun $r_1, r_2 \in R$. Tällöin ryhmän $(R/I, +)$ nolla-alkio on $\mathbf{0} + I = I$ ja alkion $a + I \in R/I$ vasta-alkio on $(-a) + I \in R/I$. Sivuluokkien kertolasku määritellään siten, että

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

aina, kun $r_1, r_2 \in R$. Osoitetaan, että sivuluokkien kertolasku on hyvin määritelty. Jos $a_1 + I = b_1 + I$ ja $a_2 + I = b_2 + I$, niin $a_1 \in b_1 + I$ ja $a_2 \in b_2 + I$. Näin ollen $a_1 = b_1 + i_1$ ja $a_2 = b_2 + i_2$ joillakin $i_1, i_2 \in I$. Tällöin

$$\begin{aligned}
(a_1 + I) \cdot (a_2 + I) &= a_1 a_2 + I \\
&= (b_1 + i_1)(b_2 + i_2) + I \\
&= (b_1 b_2 + b_1 i_2 + i_1 b_2 + i_1 i_2) + I \\
&= (b_1 b_2 + I) + (b_1 i_2 + I) + (i_1 b_2 + I) + (i_1 i_2 + I) \\
&= (b_1 b_2 + I) + (\mathbf{0} + I) + (\mathbf{0} + I) + (\mathbf{0} + I) \\
&= (b_1 b_2 + I) \\
&= (b_1 + I) \cdot (b_2 + I),
\end{aligned}$$

sillä $b_1 i_2, i_1 b_2, i_1 i_2 \in I$, koska I on ideaali. Tulo on siis riippumaton sivuluokkien edustajista eli sivuluokkien kertolasku on hyvin määritelty.

Lause 1.13. *Olkoon I renkaan $(R, +, \cdot)$ ideaali ja $R/I = \{r + I \,|\, r \in R\}$, missä $r + I = \{r + i \,|\, i \in I\}$. Tällöin $(R/I, +, \cdot)$ on rengas, missä $(+)$ ja $(\cdot)$ ovat aikaisemmin määritellyt sivuluokkien yhteen- ja kertolasku.*

Todistus. Osoitetaan, että $(R/I, +, \cdot)$ on rengas.

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

- Olkoon $a+I, b+I \in R/I$. Tällöin

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

- Olkoon $a+I, b+I, c+I \in R/I$. Tällöin

$$\begin{aligned}(a+I)+((b+I)+(c+I)) &= (a+I)+((b+c)+I)\\ &= (a+(b+c))+I\\ &= ((a+b)+c)+I\\ &= ((a+b)+I)+(c+I)\\ &= ((a+I)+(b+I))+(c+I);\end{aligned}$$

- Nyt $\mathbf{0}+I = I \in R/I$ ja

$$\begin{aligned}(\mathbf{0}+I)+(a+I) &= (a+I)\\ &= (a+I)+(\mathbf{0}+I),\end{aligned}$$

  kaikilla $a+I \in R/I$, joten $\mathbf{0}+I = I$ on nolla-alkio joukossa R/I;
- Olkoon $a+I \in R/I$. Tällöin $(-a)+I = -a+I \in R/I$ ja

$$\begin{aligned}(a+I)+(-a+I) &= (a-a)+I\\ &= \mathbf{0}+I\\ &= (-a+I)+(a+I),\end{aligned}$$

  joten alkio $-a+I$ on alkion $a+I$ vasta-alkio joukossa R/I;
- Olkoon $a+I, b+I \in R/I$. Tällöin

$$\begin{aligned}(a+I)+(b+I) &= (a+b)+I\\ &= (b+a)+I\\ &= (b+I)+(a+I).\end{aligned}$$

Näin ollen $(R/I,+)$ on Abelin ryhmä.

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

- Olkoon $a+I, b+I \in R/I$. Tällöin

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

- Olkoon $a+I, b+I, c+I \in R/I$. Tällöin

$$\begin{aligned}(a+I)\cdot((b+I)\cdot(c+I)) &= (a+I)\cdot((bc)+I)\\ &= a(bc)+I\\ &= (ab)c+I\\ &= ((ab)+I)\cdot(c+I)\\ &= ((a+I)\cdot(b+I))\cdot(c+I);\end{aligned}$$

- Nyt $\mathbf{1}+I \in R/I$ ja

$$\begin{aligned}(\mathbf{1}+I)\cdot(a+I) &= (a+I)\\ &= (a+I)\cdot(\mathbf{1}+I)\end{aligned}$$

kaikilla $a+I \in R/I$, joten $\mathbf{1}+I$ on ykkösalkio joukossa R/I.

Näin ollen $(R/I,\cdot)$ on monoidi.

3. Osoitetaan, että osittelulait ovat voimassa. Olkoon $a+I, b+I, c+I \in R/I$. Tällöin

$$\begin{aligned}(a+I)\cdot[(b+I)+(c+I)] &= (a+I)\cdot[(b+c)+I]\\ &= a(b+c)+I\\ &= (ab+ac)+I\\ &= (ab+I)+(ac+I)\\ &= [(a+I)\cdot(b+I)]+[(a+I)\cdot(c+I)]\end{aligned}$$

ja

$$\begin{aligned}[(a+I)+(b+I)]\cdot(c+I) &= [(a+b)+I]\cdot(c+I)\\ &= (a+b)c+I\\ &= (ac+bc)+I\\ &= (ac+I)+(bc+I)\\ &= [(a+I)\cdot(c+I)]+[(b+I)\cdot(c+I)]\,.\end{aligned}$$

Kohtien $1-3$ nojalla $(R/I,+,\cdot)$ on rengas. □

2 Kunnat

Edellisen luvun käsitteestä rengas jatketaan tässä luvussa käsitteeseen kunta. Kun kommutatiivinen rengas sisältää jokaisen nolla-alkiosta eroavan alkionsa käänteisalkiot, muodostuu kunta. Tunnetuimpia kuntia ovat rationaaliluvut ja reaaliluvut.

2.1 Kunta

Määritelmä 2.1. Kommutatiivinen rengas $(K, +, \cdot)$ on *kunta*, jos $(K \setminus \{\mathbf{0}\}, \cdot)$ on Abelin ryhmä.

Kolmikko $(K, +, \cdot)$ on kunta, jos

1. $(K, +)$ on Abelin ryhmä:
   - $a + b \in K$ kaikilla $a, b \in K$;
   - $(a + b) + c = a + (b + c)$ kaikilla $a, b, c \in K$;
   - on olemassa nolla-alkio $\mathbf{0} \in K$, jolle
   $$a + \mathbf{0} = \mathbf{0} + a = a \quad \text{kaikilla} \quad a \in K;$$
   - jokaiselle $a \in K$ on olemassa vasta-alkio $-a \in K$, jolle
   $$a + (-a) = (-a) + a = \mathbf{0};$$
   - $a + b = b + a$ kaikilla $a, b \in K$.
2. Operaatiolle $(\cdot)$ pätevät seuraavat ehdot:
   - $a \cdot b \in K$ kaikilla $a, b \in K$;
   - $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ kaikilla $a, b, c \in K$;
   - on olemassa ykkösalkio $\mathbf{1} \in K$, jolle
   $$\mathbf{1} \cdot a = a \cdot \mathbf{1} = a \quad \text{kaikilla} \quad a \in K;$$
   - jokaiselle $a \in K \setminus \{\mathbf{0}\}$ on olemassa käänteisalkio $a^{-1} \in K \setminus \{\mathbf{0}\}$, jolle
   $$a \cdot a^{-1} = a^{-1} \cdot a = \mathbf{1};$$
   - $a \cdot b = b \cdot a$ kaikilla $a, b \in K$.

3. Osittelulait ovat voimassa:

   - $a \cdot (b + c) = a \cdot b + a \cdot c$ kaikilla $a, b, c \in K$;
   - $(a + b) \cdot c = a \cdot c + b \cdot c$ kaikilla $a, b, c \in K$.

Lause 2.2. *Kunnan* $(K, +, \cdot)$ *ainoat ideaalit ovat* $(\mathbf{0})$ *ja* K.

Todistus. Koska $(K, +, \cdot)$ on kunta, niin $(K, +, \cdot)$ on myös rengas. Tällöin renkaalla $(K, +, \cdot)$ on triviaali ideaali $(\mathbf{0})$.

Olkoon $I \neq \{\mathbf{0}\}$ kunnan K ideaali. Nyt on olemassa alkio $a \in I$ siten, että $a \neq \mathbf{0}$. Koska $(K, +, \cdot)$ on kunta, niin $(K \setminus \{\mathbf{0}\}, \cdot)$ on ryhmä. Siis $a \in K \setminus \{\mathbf{0}\}$. Tällöin alkiolle a on olemassa käänteisalkio $a^{-1} \in K \setminus \{\mathbf{0}\}$. Näin ollen $a \cdot a^{-1} \in I$ eli $\mathbf{1} \in I$ eli $I = K$. □

2.2 Kuntalaajennus

Lause 2.3. *Olkoon* $(R, +, \cdot)$ *kommutatiivinen rengas, jonka ainoat ideaalit ovat* $(\mathbf{0})$ *ja* R. *Tällöin* $(R, +, \cdot)$ *on kunta.*

Todistus. On osoitettava, että $(R \setminus \{\mathbf{0}\}, \cdot)$ on Abelin ryhmä. Koska $(R, \cdot)$ on monoidi, niin $(ab)c = a(bc)$ kaikilla $a, b, c \in R \setminus \{\mathbf{0}\}$ ja $\mathbf{1} \in R \setminus \{\mathbf{0}\}$. Ja koska $(R, +, \cdot)$ on kommutatiivinen rengas, niin $ab = ba$ kaikilla $a, b \in R \setminus \{\mathbf{0}\}$. Osoitetaan, että $ab \in R \setminus \{\mathbf{0}\}$ kaikilla $a, b \in R \setminus \{\mathbf{0}\}$ ja että on olemassa käänteisalkio $a^{-1} \in R \setminus \{\mathbf{0}\}$ jokaiselle $a \in R \setminus \{\mathbf{0}\}$.

Olkoon $a \in R$ ja $a \neq \mathbf{0}$. Koska $(R, +, \cdot)$ on kommutatiivinen rengas, niin lauseen 1.10 nojalla $(a) = Ra$. Nyt $(a) \neq (\mathbf{0})$, joten $(a) = Ra = R$.

Nyt $\mathbf{1} \in R$ eli $\mathbf{1} \in Ra$. Siis on olemassa alkio $r \in R$ siten, että $\mathbf{1} = ra$. Tällöin myös $ar = \mathbf{1}$. Näin ollen $r = a^{-1} \in R \setminus \{\mathbf{0}\}$.

Olkoon $a, b \in R \setminus \{\mathbf{0}\}$. Jos $ab = \mathbf{0}$, niin $a = (ab)b^{-1} = \mathbf{0} \cdot b^{-1} = \mathbf{0}$. Tämä ei pidä paikkaansa, joten $ab \neq \mathbf{0}$ eli $ab \in R \setminus \{\mathbf{0}\}$.

Näin ollen $(R, +, \cdot)$ on kunta. □

Lause 2.4. *Olkoon* $(R, +, \cdot)$ *kommutatiivinen rengas ja* M *renkaan* R *maksimaalinen ideaali. Tällöin tekijärengas* R/M *on kunta.*

Todistus. Koska R on kommutatiivinen rengas, niin R/M on myös kommutatiivinen rengas. Osoitetaan, että $(R/M \setminus \{\mathbf{0} + M\}, \cdot)$ on Abelin ryhmä. Riittää osoittaa, että jokaiselle tekijärenkaan nolla-alkiosta eroavalle alkiolle on olemassa käänteisalkio joukossa $R/M \setminus \{\mathbf{0} + M\}$, koska R/M on kommutatiivinen rengas.

Olkoon $a + M \in R/M$ ja $a + M \neq \mathbf{0} + M$. Tällöin $a \notin \mathbf{0} + M = M$, joten $(a) \neq M$. Renkaalla R on siis kaksi ideaalia, ideaalit M ja (a), joten ideaalien

summa $M + (a)$ on myös renkaan R ideaali ja $M \subset M + (a)$. Koska M on renkaan R maksimaalinen ideaali, niin $M + (a) = R$, ja edelleen lauseen 1.10 nojalla $(a) = Ra$.

Nyt $\mathbf{1} \in R$ eli $\mathbf{1} \in M + Ra$, joten $\mathbf{1} = m + ra$ joillakin $m \in M$ ja $r \in R$. Tällöin tekijärenkaan R/M ykkösalkio

$$\begin{aligned} \mathbf{1} + M &= (m + ra) + M \\ &= (m + M) + (ra + M) \\ &= (\mathbf{0} + M) + (ra + M) \\ &= ra + M \\ &= (r + M) \cdot (a + M). \end{aligned}$$

Koska tekijärengas R/M on kommutatiivinen rengas, niin myös

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

Näin ollen $r + M$ on alkion $a + M$ käänteisalkio ja myös $r + M \neq \mathbf{0} + M$.

Näin ollen $(R/M \backslash \{\mathbf{0}+M\}, \cdot)$ on Abelin ryhmä. Siis tekijärengas $(R/M, +, \cdot)$ on kunta. □

3 Polynomirengas

Tässä luvussa käydään läpi käsitettä polynomirengas ja siihen liittyviä tietoja, joita tarvitaan polynomien suurimman yhteisen tekijän määrittämisessä ja polynomien kongruenssissa.

3.1 Polynomirengas ja polynomin aste

Määritelmä 3.1. Olkoon $(K, +, \cdot)$ kunta. Merkitään

$$K[x] = \left\{ a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 | a_i \in K, n \in \mathbb{Z}, n \geq 0 \right\}.$$

Joukon $K[x]$ alkioita kutsutaan *K-kertoimisiksi polynomeiksi* ja joukkoa $K[x]$ varustettuna polynomien yhteen- ja kertolaskulla *polynomirenkaaksi kunnan K suhteen*, jota merkitään $(K[x], +, \cdot)$.

Lause 3.2. *Polynomirengas $(K[x], +, \cdot)$ on kommutatiivinen rengas.*

Todistus. Olkoon $(K, +, \cdot)$ kunta. Osoitetaan, että $(K[x], +, \cdot)$ on rengas. Olkoon polynomit

$$f(x) = a_n x^n + \ldots + a_1 x + a_0,$$

missä $a_n \neq \mathbf{0}$, ja

$$g(x) = b_m x^m + \ldots + b_1 x + b_0,$$

missä $b_m \neq \mathbf{0}$, sekä

$$h(x) = c_t x^t + \ldots + c_1 x + c_0,$$

missä $c_t \neq \mathbf{0}$.

1. Osoitetaan, että $(K[x], +)$ on Abelin ryhmä:

   - Olkoon $f(x), g(x) \in K[x]$. Tällöin

     $$\begin{aligned} f(x) + g(x) &= a_n x^n + \ldots + a_1 x + a_0 + b_m x^m + \ldots + b_1 x + b_0 \\ &= a_n x^n + b_m x^m + \ldots + a_0 + b_0 \in K[x]; \end{aligned}$$

   - Olkoon $f(x), g(x), h(x) \in K[x]$. Tällöin

     $$\begin{aligned} (f(x) + g(x)) + h(x) &= (a_n x^n + \ldots + a_0 + b_m x^m + \ldots + b_0) + c_t x^t + \ldots + c_0 \\ &= a_n x^n + \ldots + a_0 + b_m x^m + \ldots + b_0 + c_t x^t + \ldots + c_0 \\ &= a_n x^n + \ldots + a_0 + (b_m x^m + \ldots + b_0 + c_t x^t + \ldots + c_0) \\ &= f(x) + (g(x) + h(x)); \end{aligned}$$

- Nyt nolla-alkio on nollapolynomi $\mathbf{0} \in K[x]$, sillä

$$\mathbf{0} + f(x) = f(x) = f(x) + \mathbf{0},$$

kaikilla $f(x) \in K[x]$;

- Olkoon $f(x) \in K[x]$. Tällöin $-f(x) = -a_n x^n - \ldots - a_0 \in K[x]$ ja

$$\begin{aligned} f(x) + (-f(x)) &= a_n x^n + \ldots + a_1 x + a_0 + (-a_n x^n - \ldots - a_1 x - a_0) \\ &= a_n x^n + \ldots + a_1 x + a_0 - a_n x^n - \ldots - a_1 x - a_0 \\ &= a_n x^n - a_n x^n + \ldots + a_1 x - a_1 x + a_0 - a_0 \\ &= \mathbf{0} \\ &= -f(x) + f(x), \end{aligned}$$

joten polynomi $-f(x)$ on polynomin $f(x)$ vasta-alkio joukossa $K[x]$;

- Olkoon $f(x), g(x) \in K[x]$. Tällöin

$$\begin{aligned} f(x) + g(x) &= a_n x^n + \ldots + a_1 x + a_0 + b_m x^m + \ldots + b_1 x + b_0 \\ &= b_m x^m + \ldots + b_1 x + b_0 + a_n x^n + \ldots + a_1 x + a_0 \\ &= g(x) + f(x). \end{aligned}$$

Näin ollen $(K[x], +)$ on Abelin ryhmä.

2. Osoitetaan, että $(K[x], \cdot)$ on monoidi:

- Olkoon $f(x), g(x) \in K[x]$. Tällöin

$$\begin{aligned} f(x) \cdot g(x) &= (a_n x^n + \ldots + a_1 x + a_0) \cdot (b_m x^m + \ldots + b_1 x + b_0) \\ &= a_n b_m x^{n+m} + \ldots + a_0 b_0 \in K[x]; \end{aligned}$$

- Olkoon $f(x), g(x), h(x) \in K[x]$. Tällöin

$$\begin{aligned} [f(x) \cdot g(x)] \cdot h(x) &= [(a_n x^n + \ldots + a_0) \cdot (b_m x^m + \ldots + b_0)] \cdot (c_t x^t + \ldots + c_0) \\ &= [a_n b_m x^{n+m} + \ldots + a_0 b_0] \cdot (c_t x^t + \ldots + c_0) \\ &= a_n b_m c_t x^{n+m+t} + \ldots + a_0 b_0 c_0 \\ &= (a_n x^n + \ldots + a_0) \cdot [b_m c_t x^{m+t} + \ldots + b_0 c_0] \\ &= (a_n x^n + \ldots + a_0) \cdot [(b_m x^m + \ldots + b_0) \cdot (c_t x^t + \ldots + c_0)] \\ &= f(x) \cdot [g(x) \cdot h(x)]; \end{aligned}$$

- Nyt ykkösalkio on vakiopolynomi $\mathbf{1} \in K[x]$, sillä

$$\mathbf{1} \cdot f(x) = f(x) = f(x) \cdot \mathbf{1}$$

kaikilla $f(x) \in K[x]$.

Näin ollen $(K[x], \cdot)$ on monoidi.

3. Osoitetaan, että osittelulait ovat voimassa. Olkoon $f(x), g(x), h(x) \in K[x]$. Tällöin

$$\begin{aligned} f(x) \cdot [g(x) + h(x)] &= (a_n x^n + \ldots + a_0) \cdot [b_m x^m + \ldots + b_0 + c_t x^t + \ldots + c_0] \\ &= a_n b_m x^{n+m} + \ldots + a_0 b_0 + a_n c_t x^{n+t} + \ldots + a_0 c_0 \\ &= f(x) \cdot g(x) + f(x) \cdot h(x) \end{aligned}$$

ja

$$\begin{aligned} [f(x) + g(x)] \cdot h(x) &= [a_n x^n + \ldots + a_0 + b_m x^m + \ldots + b_0] \cdot (c_t x^t + \ldots + c_0) \\ &= a_n c_t x^{n+t} + \ldots + a_0 c_0 + b_m c_t x^{m+t} + \ldots + b_0 c_0 \\ &= f(x) \cdot h(x) + g(x) \cdot h(x). \end{aligned}$$

Kohtien $1-3$ nojalla $(K[x], +, \cdot)$ on rengas. Osoitetaan vielä, että $(K[x], +, \cdot)$ on kommutatiivinen kertolaskun suhteen. Nyt

$$\begin{aligned} f(x) \cdot g(x) &= (a_n x^n + \ldots + a_0) \cdot (b_m x^m + \ldots + b_0) \\ &= a_n b_m x^{n+m} + \ldots + a_0 b_0 \\ &= b_m a_n x^{m+n} + \ldots + b_0 a_0 \\ &= g(x) \cdot f(x). \end{aligned}$$

Näin ollen $(K[x], +, \cdot)$ on kommutatiivinen rengas. □

Määritelmä 3.3. Olkoon K kunta ja $f(x) \in K[x]$. Jos $f(x) = a_n x^n + \ldots + a_1 x + a_0$ ja $a_n \neq \mathbf{0}$, niin polynomin $f(x)$ *aste* on n, merkitään $deg f(x) = n$. Jos $a \neq \mathbf{0}$, niin vakiopolynomin $f(x) = a$ aste on nolla eli $deg\, a = \mathbf{0}$. Lisäksi $deg\, \mathbf{0} = -\infty$.

Lause 3.4. *Jos $f(x), g(x) \in K[x]$ ja $f(x), g(x) \neq \mathbf{0}$, niin $deg(f(x) \cdot g(x)) = deg\, f(x) + deg\, g(x)$.*

Todistus. Olkoon polynomit $f(x) = a_n x^n + \ldots + a_1 x + a_0$, missä $a_n \neq \mathbf{0}$, ja $g(x) = b_m x^m + \ldots + b_1 x + b_0$, missä $b_m \neq \mathbf{0}$, jolloin $deg\, f(x) = n$ ja $deg\, g(x) = m$. Nyt

$$f(x) \cdot g(x) = a_n b_m x^{n+m} + \ldots + a_0 b_0$$

ja $a_n b_m \neq \mathbf{0}$, koska $a_n \neq \mathbf{0}$ ja $b_m \neq \mathbf{0}$. Siis

$$deg(f(x) \cdot g(x)) = n + m = deg\, f(x) + deg\, g(x).$$

□

3.2 Jakoalgoritmi

Lause 3.5 (Jakoalgoritmi polynomeille)**.** *Jos polynomit $f(x), g(x) \in K[x]$ ja $g(x) \neq \mathbf{0}$, niin $f(x) = q(x)g(x) + r(x)$, missä $q(x), r(x) \in K[x]$ ovat yksikäsitteiset ja $deg\, r(x) < deg\, g(x)$.*

Todistus. Osoitetaan jakoalgoritmin olemassaolo. Olkoon $f(x), g(x) \in K[x]$ ja $g(x) \neq \mathbf{0}$. Tarkastellaan joukkoa

$$S = \{f(x) - s(x)g(x) \,|\, s(x) \in K[x]\}.$$

Selvästi $\emptyset \neq S \subseteq K[x]$. Olkoon $r(x) \in S$ sellainen polynomi, jonka aste on mahdollisimman pieni. Nyt $r(x) = f(x) - q(x)g(x)$ eräällä $q(x) \in K[x]$ eli

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

Osoitetaan, että $deg\, r(x) < deg\, g(x)$. Tehdään vastaoletus eli oletetaan, että $deg\, r(x) \geq deg\, g(x)$. Merkitään polynomi $r(x) = r_m x^m + \ldots + r_1 x + r_0$, missä $r_m \neq \mathbf{0}$, ja polynomi $g(x) = b_n x^n + \ldots + b_1 x + b_0$, missä $b_n \neq \mathbf{0}$. Vastaoletuksen perusteella $m \geq n$, jolloin $k(x) = r_m b_n^{-1} x^{m-n} \in K[x]$. Olkoon

$$\begin{aligned} t(x) &= r(x) - k(x)g(x) \\ &= r_m x^m + \ldots + r_1 x + r_0 - r_m b_n^{-1} x^{m-n}(b_n x^n + \ldots + b_1 x + b_0) \\ &= r_m x^m + \ldots + r_1 x + r_0 - [r_m x^m + \ldots + r_m b_0 b_n^{-1} x^{m-n}]. \end{aligned}$$

Siis $deg\, t(x) < m$ eli $deg\, t(x) < deg\, r(x)$. Toisaalta

$$\begin{aligned} t(x) &= r(x) - k(x)g(x) \\ &= f(x) - q(x)g(x) - k(x)g(x) \\ &= f(x) - [q(x) + k(x)]g(x) \in S, \end{aligned}$$

mikä on ristiriidassa polynomin $r(x)$ valinnan kanssa. Siis vastaoletus on väärin, joten $deg\, r(x) < deg\, g(x)$.

Osoitetaan polynomien $q(x)$ ja $r(x)$ yksikäsitteisyys. Olkoon polynomilla $f(x)$ seuraavat jakoalgoritmin mukaiset esitykset eli

$$f(x) = q(x)g(x) + r(x), \quad q(x), r(x) \in K[x] \quad \text{ja} \quad deg\, r(x) < deg\, g(x)$$

ja

$$f(x) = q'(x)g(x) + r'(x), \quad q'(x), r'(x) \in K[x] \quad \text{ja} \quad deg\, r'(x) < deg\, g(x).$$

Selvästi $deg(r(x) - r'(x)) < deg\, g(x)$ ja toisaalta

$$\begin{aligned} r(x) - r'(x) &= f(x) - q(x)g(x) - [f(x) - q'(x)g(x)] \\ &= q'(x)g(x) - q(x)g(x) \\ &= [q'(x) - q(x)]g(x), \end{aligned}$$

jolloin $deg(r(x) - r'(x)) = deg(q'(x) - q(x)) + deg\, g(x)$. Siis

$$deg(r(x) - r'(x)) < deg\, g(x)$$

ja

$$deg(r(x) - r'(x)) = deg(q'(x) - q(x)) + deg\, g(x),$$

mikä on mahdollista vain, kun $deg(q'(x) - q(x)) = -\infty$ eli $q'(x) - q(x) = \mathbf{0}$, josta saadaan $q'(x) = q(x)$. Tällöin myös

$$\begin{aligned} r(x) - r'(x) &= [q'(x) - q(x)]g(x) \\ &= \mathbf{0} \cdot g(x) \\ &= \mathbf{0} \end{aligned}$$

eli $r(x) - r'(x) = \mathbf{0}$, josta saadaan $r'(x) = r(x)$. Siis polynomit $r(x)$ ja $q(x)$ ovat yksikäsitteiset. □

Määritelmä 3.6. Olkoon $f(x) = a_n x^n + \ldots + a_1 x + a_0$ polynomirenkaan $K[x]$ polynomi ja $a_n \neq \mathbf{0}$. Tällöin kerroin a_n on polynomin $f(x)$ *johtava kerroin*. Polynomia $f(x)$ kutsutaan *pääpolynomiksi*, jos sen johtava kerroin on kunnan$(K, +, \cdot)$ ykkösalkio.

3.3 Polynomin nollakohdat ja jaollisuus

Määritelmä 3.7. Jos $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$ ja $\alpha \in K$ sekä

$$f(\alpha) = a_n \alpha^n + \ldots + a_1 \alpha + a_0 = \mathbf{0},$$

niin α on polynomin $f(x)$ *nollakohta*.

Lause 3.8. *Polynomirenkaan $K[x]$ 1.asteen polynomilla on aina nollakohta kunnassa K.*

Todistus. Olkoon polynomi $f(x) = ax + b$, missä $a, b \in K$ ja $a \neq \mathbf{0}$. Tällöin

$$f(x) = ax + b = \mathbf{0} \Leftrightarrow ax = -b \Leftrightarrow x = a^{-1} \cdot (-b) \in K.$$

□

Määritelmä 3.9. Jos $f(x), g(x) \in K[x]$ ja $f(x) = q(x)g(x)$ eräällä $q(x) \in K[x]$, niin sanotaan, että polynomi $g(x)$ *jakaa polynomin* $f(x)$. Merkitään $g(x) \,|\, f(x)$.

Lause 3.10. *Olkoot $f(x) \in K[x]$ ja $\alpha \in K$. Tällöin*

$$f(\alpha) = \mathbf{0} \Leftrightarrow (x - \alpha) \,|\, f(x).$$

Todistus. Jos $(x - \alpha) \,|\, f(x)$, niin $f(x) = (x - \alpha)g(x)$. Nyt

$$f(\alpha) = (\alpha - \alpha)g(x) = \mathbf{0}.$$

Olkoon $f(\alpha) = \mathbf{0}$. Jakoalgoritmia soveltaen polynomeille $f(x)$ ja $x - \alpha$ saadaan

$$f(x) = q(x)(x - \alpha) + r(x),$$

missä $deg\, r(x) < deg\,(x - \alpha)$. Nyt $deg\,(x - \alpha) = 1$ eli $deg\, r(x) = 0$ tai $deg\, r(x) = -\infty$. Siis polynomi $r(x)$ on vakiopolynomi, jolloin

$$f(x) = q(x)(x - \alpha) + c,$$

missä $c \in K$ on vakio. Nyt $f(\alpha) = \mathbf{0}$ eli $\mathbf{0} = q(\alpha)(\alpha - \alpha) + c$, josta saadaan $c = \mathbf{0}$. Näin ollen $f(x) = q(x)(x - \alpha)$ eli

$$(x - \alpha) \,|\, f(x).$$

□

Määritelmä 3.11. Polynomi $f(x) \in K[x]$ on *jaoton* polynomirenkaassa $K[x]$, jos $deg\, f(x) \geq 1$ ja polynomia $f(x)$ ei voida esittää kahden positiivista astetta olevan polynomin tulona polynomirenkaassa $K[x]$.

Lause 3.12. *Olkoon $f(x) \in K[x]$ ja $deg\, f(x) = 2$ tai $deg\, f(x) = 3$. Tällöin polynomi $f(x)$ on jaoton jos ja vain jos sillä ei ole nollakohtia kunnassa K.*

Todistus. Olkoon $f(x)$ jaoton. Jos $\alpha \in K$ on polynomin $f(x)$ nollakohta, niin lauseen 3.10 nojalla

$$x - \alpha \,|\, f(x)$$

eli polynomi $f(x)$ ei ole jaoton. Tämä on ristiriidassa oletuksen kanssa, joten polynomilla $f(x)$ ei ole nollakohtia.

Oletetaan, että polynomilla $f(x)$ ei ole nollakohtia. Jos $f(x)$ ei ole jaoton, niin

$$f(x) = h(x)g(x),$$

missä $1 \leq deg\, g(x) < deg\, f(x)$ ja $1 \leq deg\, h(x) < deg\, f(x)$. Nyt $deg\, f(x) = 2$ tai $deg\, f(x) = 3$, joten

$$deg\, g(x) = 1$$

tai

$$deg\, h(x) = 1.$$

Nyt 1. asteen polynomilla on aina nollakohta kunnassa K, joten polynomilla $f(x)$ on nollakohta. Tämä on ristiriidassa oletuksen kanssa, joten polynomi $f(x)$ on jaoton. □

Lause 3.13. *Olkoon $f(x) \in K[x]$. Jos $deg\, f(x) = n$, niin polynomilla $f(x)$ on korkeintaan n nollakohtaa kunnassa K.*

Todistus. Jos polynomilla $f(x)$ on nollakohdat $a_1, a_2, \ldots, a_r \in K$, niin polynomi $f(x)$ on jaollinen polynomilla $q(x) = (x - a_1)(x - a_2) \cdots (x - a_r)$. Nyt $deg\, q(x) = r \leq deg\, f(x) = n$, joten $r \leq n$. □

Lause 3.14. *Olkoon K kunta. Polynomirenkaan $K[x]$ jokainen ideaali on pääideaali.*

Todistus. Olkoon I polynomirenkaan $K[x]$ ideaali. Jos $I = \{\mathbf{0}\}$, niin $I = (\mathbf{0})$. Voidaan jatkossa olettaa, että $I \neq \{\mathbf{0}\}$. Näin ollen on olemassa sellainen polynomi $b(x) \in I \setminus \{\mathbf{0}\}$ siten, että polynomin $b(x)$ aste on pienin mahdollinen joukossa $I \setminus \{\mathbf{0}\}$.

Olkoon $f(x) \in I$ mielivaltainen polynomi ja jakoalgoritmin nojalla saadaan $f(x) = q(x)b(x) + r(x)$, missä $q(x), r(x) \in K[x]$ ja $deg\, r(x) < deg\, b(x)$. Nyt $f(x) \in I$ ja $q(x)b(x) \in I$, jolloin $r(x) = f(x) - q(x)b(x) \in I$. Polynomin $b(x)$ valinnasta johtuen $r(x) = \mathbf{0}$. Näin ollen

$$f(x) = q(x)b(x) \in (b(x)) \quad \text{eli} \quad I \subseteq (b(x)).$$

Toisaalta $(b(x)) = \{k(x)b(x) \,|\, k(x) \in K[x]\} \subseteq I$. Siis

$$I = (b(x)).$$

□

Lause 3.15. *Jos I on polynomirenkaan $(K[x], +, \cdot)$ ideaali, niin $I = (f(x))$, missä $f(x)$ on jokin pääpolynomi.*

Todistus. Olkoon I polynomirenkaan $(K[x], +, \cdot)$ ideaali. Lauseen 3.14 nojalla $I = (f(x))$, missä $f(x) \in K[x]$ on sellainen polynomi, jonka aste on pienin mahdollinen joukossa $I \setminus \{\mathbf{0}\}$.

Olkoon a polynomin $f(x)$ johtava kerroin. Tällöin alkion a käänteisalkio on olemassa, koska K on kunta, ja tämä käänteisalkio on myös polynomirenkaan $K[x]$ polynomi eli vakiopolynomi.

Koska I on ideaali, niin alkion a käänteisalkion ja polynomin $f(x)$ tulo on myös ideaalin I alkio ja samaa astetta kuin polynomi $f(x)$ ja siten selvästi pääpolynomi.

Tällöin lauseen 3.14 generoijapolynomiksi voidaan valita tämä tulo. □

Lause 3.16. *Jos $p(x) \in K[x]$ on jaoton polynomi, niin $(p(x))$ on renkaan $K[x]$ maksimaalinen ideaali.*

Todistus. Nyt lauseen 1.10 nojalla $(p(x)) = \{k(x)p(x) | k(x) \in K[x]\}$. Koska vakiopolynomit eivät kuulu pääideaaliin $(p(x))$, niin

$$(p(x)) \subset K[x].$$

Olkoon $I = (g(x))$ sellainen ideaali, että $(p(x)) \subset I \subseteq K[x]$. Nyt

$$p(x) \in I = (g(x)),$$

joten $p(x) = k(x)g(x)$, missä $k(x) \in K[x]$.

Koska polynomi $p(x)$ on jaoton, niin joko polynomi $k(x)$ tai $g(x)$ on vakio. Jos $k(x) = c$, niin $p(x) = c \cdot g(x)$ eli $g(x) = c^{-1} \cdot p(x) \in (p(x))$, jolloin $I \subseteq (p(x))$, mikä on ristiriidassa oletuksen kanssa. Jos $g(x) = c$, niin

$$(g(x)) = \{k(x) \cdot c \,|\, k(x) \in K[x]\} = K[x].$$

Tällöin $(p(x))$ on renkaan $K[x]$ maksimaalinen ideaali. □

Lause 3.17. *Jos K on kunta ja $p(x)$ on polynomirenkaan $K[x]$ jaoton polynomi, niin tekijärengas $K[x]/(p(x))$ on kunta.*

Todistus. Lauseen 3.16 nojalla $(p(x))$ on polynomirenkaan $K[x]$ maksimaalinen ideaali ja lauseen 2.4 nojalla $K[x]/(p(x))$ on kunta. □

Esimerkki 3.18. Olkoon polynomirengas $\mathbb{Z}_2[x]$ ja $p(x) = [1]x^2 + [1]x + [1]$ sen jaoton polynomi. Jos polynomi $p(x)$ olisi jaollinen polynomirenkaassa $\mathbb{Z}_2[x]$, niin sillä olisi nollakohta polynomirenkaassa $\mathbb{Z}_2[x]$. Nyt

$$p([0]) = [1] \cdot [0]^2 + [1] \cdot [0] + [1] = [1]$$

ja

$$p([1]) = [1] \cdot [1]^2 + [1] \cdot [1] + [1] = [1],$$

joten polynomilla $p(x)$ ei ole nollakohtia polynomirenkaassa $\mathbb{Z}_2[x]$ eli polynomi $p(x)$ on jaoton. Koska $p(x)$ on jaoton polynomi, niin $(p(x))$ on maksimaalinen ideaali ja siten tekijärengas $\mathbb{Z}_2[x]/(p(x))$ on kunta.

Nyt $[1]x^2 + [1]x + [1] + (p(x)) = [0] + (p(x))$, joten

$$\begin{aligned} [1]x^2 + (p(x)) &= -[1]x - [1] + (p(x)) \\ &= [1]x + [1] + (p(x)). \end{aligned}$$

Saadaan

$$\begin{aligned} \mathbb{Z}_2[x]/(p(x)) &= \{f(x) + (p(x)) \mid f(x) \in \mathbb{Z}_2[x]\} \\ &= \{[a_1]x + [a_0] + (p(x)) \mid [a_0], [a_1] \in \mathbb{Z}_2\}. \end{aligned}$$

Tekijärenkaan alkioiden kertoimet $[a_1]$ ja $[a_0]$ voivat saada arvon $[0]$ tai $[1]$, ja merkitään $\alpha = x + (p(x))$, jolloin $\alpha^2 = x^2 + (p(x))$, ja $0 = [0] + (p(x))$ sekä $1 = [1] + (p(x))$. Tällöin tekijärenkaaksi saadaan

$$\mathbb{Z}_2[x]/(p(x)) = \{0, 1, \alpha, \alpha + 1\}.$$

Nyt saadaan tekijärenkaan alkioille operaatiot $(+)$ ja $(\cdot)$ eli

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

ja

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

4 Polynomien suurin yhteinen tekijä

Tässä kappaleessa määritellään ensin polynomien suurin yhteinen tekijä ja myöhemmin käydään läpi Eukleideen algoritmi, joka on menetelmä suurimman yhteisen tekijän löytämiseksi.

4.1 Suurin yhteinen tekijä

Määritelmä 4.1. Olkoon $f(x), g(x) \in K[x]$ polynomeja, joista ainakin toinen on nollapolynomista eroava. Polynomien $f(x)$ ja $g(x)$ *suurin yhteinen tekijä* $syt(f(x), g(x))$ on polynomi $d(x) \in K[x]$, jolle pätee seuraavat ehdot:

1. $d(x)$ on pääpolynomi;
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 $h(x) \mid d(x)$.

Lause 4.2. *Jos $f(x), g(x) \in K[x]$, $f(x) \neq \mathbf{0}$ ja $g(x) \neq \mathbf{0}$, niin suurin yhteinen tekijä $syt(f(x), g(x)) = d(x) \in K[x]$ on olemassa ja se on yksikäsitteinen. Lisäksi on olemassa sellaiset polynomit $a(x), b(x) \in K[x]$, että $d(x) = syt(f(x), g(x)) = a(x)f(x) + b(x)g(x)$.*

Todistus. Olkoon $f(x), g(x) \in K[x]$, $f(x) \neq \mathbf{0}$, $g(x) \neq \mathbf{0}$ ja

$$I = \{r(x)f(x) + s(x)g(x) \mid r(x), s(x) \in K[x]\}.$$

Selvästi $I \subseteq K[x] \setminus \{\mathbf{0}\}$. Osoitetaan, että I on polynomirenkaan $K[x]$ ideaali.

1. Olkoon $i_1(x), i_2(x) \in I$, jolloin

   $$i_1(x) = r_1(x)f(x) + s_1(x)g(x)$$

   ja

   $$i_2(x) = r_2(x)f(x) + s_2(x)g(x)$$

   joillakin $r_1(x), r_2(x), s_1(x), s_2(x) \in K[x]$. Tälloin

   $$\begin{aligned} i_1(x) - i_2(x) &= r_1(x)f(x) + s_1(x)g(x) - [r_2(x)f(x) + s_2(x)g(x)] \\ &= [r_1(x) - r_2(x)]f(x) + [s_1(x) - s_2(x)]g(x) \in I, \end{aligned}$$

   joten $(I, +) \leq (K[x], +)$.

2. Olkoon $i(x) \in I$ ja $k(x) \in K[x]$. Nyt $i(x) = r(x)f(x)+s(x)g(x)$ joillakin $r(x), s(x) \in K[x]$, joten

$$\begin{aligned} k(x)i(x) &= k(x)[r(x)f(x) + s(x)g(x)] \\ &= k(x)r(x)f(x) + k(x)s(x)g(x) \in I. \end{aligned}$$

   Lisäksi, koska $K[x]$ on kommutatiivinen rengas, niin $i(x)k(x) = k(x)i(x) \in I$.

Kohtien 1 ja 2 nojalla I on polynomirenkaan $K[x]$ ideaali.

Lauseiden 3.14 ja 3.15 nojalla on olemassa sellainen pääpolynomi $d(x) \in K[x]$, että $I = (d(x))$. Koska

$$f(x), g(x) \in I = (d(x)) = K[x] \cdot d(x),$$

niin $d(x) \mid f(x)$ ja $d(x) \mid g(x)$. Polynomi $d(x)$ on siis polynomien $f(x)$ ja $g(x)$ yhteinen tekijä. Koska $d(x) \in I$, niin on olemassa sellaiset $a(x), b(x) \in K[x]$, että

$$d(x) = a(x)f(x) + b(x)g(x).$$

Jos $h(x) \mid f(x)$ ja $h(x) \mid g(x)$, niin $h(x) \mid a(x)f(x)$ ja $h(x) \mid b(x)g(x)$. Tällöin

$$h(x) \mid a(x)f(x) + b(x)g(x)$$

eli $h(x) \mid d(x)$. Näin ollen $d(x) = syt(f(x), g(x))$.

Osoitetaan vielä suurimman yhteisen tekijän yksikäsitteisyys. Olkoon

$$d(x) = syt(f(x), g(x))$$

ja

$$d'(x) = syt(f(x), g(x)).$$

Koska polynomi $d(x)$ on suurin yhteinen tekijä, niin määritelmän 4.1 nojalla $d'(x) \mid d(x)$. Samalla koska polynomi $d'(x)$ on suurin yhteinen tekijä, niin $d(x) \mid d'(x)$. Koska sekä $d(x)$ ja $d'(x)$ ovat pääpolynomeja, niin $d(x) = d'(x)$. □

Määritelmä 4.3. Polynomit $f(x) \in K[x]$ ja $g(x) \in K[x]$ ovat *keskenään jaottomia*, jos niiden suurin yhteinen tekijä $syt(f(x), g(x))$ on $\mathbf{1}$.

Lause 4.4. *Jos $f(x), g(x) \in K[x]$ ovat keskenään jaottomia polynomeja, niin $a(x)f(x) + b(x)g(x) = \mathbf{1}$ joillakin $a(x), b(x) \in K[x]$.*

Todistus. Olkoon $f(x), g(x) \in K[x]$ keskenään jaottomia polynomeja, jolloin määritelmän 4.3 ja lauseen 4.2 nojalla

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

joillakin $a(x), b(x) \in K[x]$. □

Lause 4.5. *Jos $a(x)f(x) + b(x)g(x) = \mathbf{1}$ joillakin $a(x), b(x) \in K[x]$, niin $f(x), g(x) \in K[x]$ ovat keskenään jaottomia polynomeja.*

Todistus. Olkoon $f(x), g(x) \in K[x]$ ja $a(x)f(x) + b(x)g(x) = \mathbf{1}$ joillakin $a(x), b(x) \in K[x]$. Lauseen 4.2 nojalla on olemassa polynomeille $f(x)$ ja $g(x)$ suurin yhteinen tekijä $d(x)$. Nyt $d(x)|f(x)$ ja $d(x)|g(x)$. Näin ollen

$$d(x) \,|\, a(x)f(x) + b(x)g(x)$$

eli $d(x)|\mathbf{1}$. On siis oltava $d(x) = \mathbf{1}$. Siis $syt(f(x), g(x)) = \mathbf{1}$ eli polynomit $f(x)$ ja $g(x)$ ovat keskenään jaottomia. □

Lause 4.6. *Jos polynomit $q(x) \in K[x]$ ja $f(x) \in K[x]$ ovat keskenään jaottomia ja jos $q(x) \,|\, f(x)g(x)$, missä $g(x) \in K[x]$, niin $q(x) \,|\, g(x)$.*

Todistus. Olkoon polynomit $q(x) \in K[x]$ ja $f(x) \in K[x]$ keskenään jaottomia, jolloin lauseen 4.4 nojalla $a(x)f(x) + b(x)q(x) = \mathbf{1}$ joillakin $a(x), b(x) \in K[x]$. Tällöin

$$a(x)f(x)g(x) + b(x)q(x)g(x) = g(x).$$

Oletuksen mukaan $q(x) \,|\, a(x)f(x)g(x)$ ja selvästi $q(x) \,|\, b(x)q(x)g(x)$, jolloin

$$q(x) \,|\, a(x)f(x)g(x) + b(x)q(x)g(x),$$

joten polynomi $q(x)$ jakaa myös yhtälön oikean puolen eli

$$q(x) \,|\, g(x).$$

□

4.2 Eukleideen algoritmi

Polynomien $f(x)$ ja $g(x)$ suurimman yhteisen tekijän voi määrittää menetelmällä, joka tunnetaan nimellä Eukleideen algoritmi. Tässä menetelmässä toistetaan jakoalgoritmia useaan kertaan.

Oletetaan, että $f(x) \neq \mathbf{0}$ ja $g(x) \neq \mathbf{0}$. Nyt

$$
\begin{aligned}
f(x) &= q_0(x) \cdot g(x) + r_1(x), \quad \text{missä } 0 \leq deg\, r_1(x) < deg g(x) \\
g(x) &= q_1(x) \cdot r_1(x) + r_2(x), \quad \text{missä } 0 \leq deg\, r_2(x) < deg\, r_1(x) \\
r_1(x) &= q_2(x) \cdot r_2(x) + r_3(x), \quad \text{missä } 0 \leq deg\, r_3(x) < deg\, r_2(x) \\
r_2(x) &= q_3(x) \cdot r_3(x) + r_4(x), \quad \text{missä } 0 \leq deg\, r_4(x) < deg\, r_3(x) \\
&\vdots \\
r_{k-2}(x) &= q_{k-1}(x) \cdot r_{k-1}(x) + r_k(x), \quad \text{missä } 0 \leq deg\, r_k(x) < deg\, r_{k-1}(x) \\
r_{k-1}(x) &= q_k(x) \cdot r_k(x).
\end{aligned}
$$

Tällöin viimeinen jakaja $r_k(x)$ on polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä.

Kun edellistä yhtälöryhmää käyttää takautuvasti, polynomien $f(x)$ ja $g(x)$ suurimman yhteisen tekijän voi kirjoittaa muodossa

$$d(x) = r_k(x) = a(x)f(x) + b(x)g(x).$$

Seuraavissa lauseissa perustellaan Eukleideen algoritmia.

Lause 4.7. *Jos $f(x) = q(x)g(x) + r(x)$, missä $f(x), g(x), q(x), r(x) \in K[x]$, niin $syt(f(x), g(x)) = syt(g(x), r(x))$.*

Todistus. Olkoon $syt(f(x), g(x)) = d(x)$. Koska $d(x)|f(x)$ ja $d(x)|g(x)$, niin $d(x)| - q(x)g(x)$ ja siis

$$d(x)|f(x) - q(x)g(x)$$

eli $d(x)|r(x)$. Näin ollen $d(x)$ on polynomien $g(x)$ ja $r(x)$ yhteinen tekijä.

Jos $c(x)|g(x)$ ja $c(x)|r(x)$, niin myös $c(x)|q(x)g(x) + r(x)$ eli $c(x)|f(x)$. Koska $c(x)|f(x)$, $c(x)|g(x)$ ja $syt(f(x), g(x)) = d(x)$, niin $c(x)|d(x)$. Siis $d(x)$ on polynomien $g(x)$ ja $r(x)$ suurin yhteinen tekijä.

Koska suurin yhteinen tekijä on yksikäsitteinen, niin $syt(f(x), g(x)) = syt(g(x), r(x))$. □

Lause 4.8. *Olkoon polynomit $f(x) \in K[x]$ ja $g(x) \in K[x]$ nollapolynomistaeroavia. Kun polynomeille $f(x)$ ja $g(x)$ käytetään Eukleideen algoritmia, viimeinen jakaja $r_k(x)$ on polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä.*

Todistus. Eukleideen algoritmissa muodostuville jakojäännöksille pätee

$$deg(r_1(x)) > deg(r_2(x)) > deg(r_3(x)) > \cdots,$$

joka lopulta päätyy tulokseen $deg(r_{k+1}(x)) = -\infty$ eli $r_{k+1}(x)$ on nollapolynomi. Lauseen 4.7 nojalla

$$syt(f(x), g(x)) = syt(g(x), r_1(x)) = \cdots = syt(r_{k-1}(x), r_k(x)) = r_k(x).$$

□

Esimerkki 4.9. Olkoon polynomit $f(x) = x^4 + 5x^3 - 19x^2 - 29x + 42 \in \mathbb{R}[x]$ ja $g(x) = x^3 - 2x^2 - 9 \in \mathbb{R}[x]$. Määritä polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä käyttämällä Eukleideen algoritmia.
Ratkaisu:
Jakamalla polynomi $f(x)$ polynomilla $g(x)$ saadaan

$$f(x) = (\underbrace{x+7}_{q_0(x)}) \cdot g(x) + (\underbrace{-5x^2 - 20x + 105}_{r_1(x)}).$$

Jaetaan seuraavaksi polynomi $g(x)$ polynomilla $r_1(x)$, jolloin saadaan

$$g(x) = (\underbrace{-\frac{1}{5}x + \frac{6}{5}}_{q_1(x)}) \cdot r_1(x) + (\underbrace{45x - 135}_{r_2(x)}).$$

Jatketaan jakamalla polynomi $r_1(x)$ polynomilla $r_2(x)$, jolloin saadaan

$$r_1(x) = (\underbrace{-\frac{5}{45}x - \frac{35}{45}}_{q_2(x)}) \cdot r_2(x).$$

Näin ollen polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä on polynomi $r_2(x)$ eli

$$syt(f(x), g(x)) = 45x - 135.$$

5 Polynomien kongruenssi

Tässä viimeisessä luvussa määritellään polynomien kongruenssi, jonka avulla saadaan uusi rengas $K[x]/\langle p(x)\rangle$, joka on jäännösluokkarengas.

5.1 Polynomikongruenssi

Määritelmä 5.1. Olkoon K kunta, $p(x)$ polynomirenkaan $K[x]$ polynomi ja $f(x), g(x) \in K[x]$. Polynomi $f(x)$ on *kongruentti polynomin* $g(x)$ *kanssa modulo* $p(x)$, jos $f(x) - g(x)$ on jaollinen polynomilla $p(x)$. Merkitään

$$f(x) \equiv g(x) \mod p(x).$$

Esimerkki 5.2. Olkoon polynomit $f(x) = x^2 - 4$, $g(x) = x^2 - x - 2$ ja $p(x) = x - 2$ polynomirenkaan $\mathbb{Q}[x]$ polynomeja. Nyt $f(x) \equiv g(x) \mod p(x)$, koska

$$f(x) - g(x) = x^2 - 4 - (x^2 - x - 2) = x - 2,$$

mikä on jaollinen polynomilla $p(x)$.

Lause 5.3. *Olkoon K kunta ja oletetaan, että $f(x) \equiv g(x) \mod p(x)$ polynomeille $f(x), g(x), p(x) \in K[x]$. Tällöin*

1. $f(x) \equiv f(x) \mod p(x)$;
2. *Jos* $f(x) \equiv g(x) \mod p(x)$, *niin* $g(x) \equiv f(x) \mod p(x)$;
3. *Jos* $f(x) \equiv g(x) \mod p(x)$ *ja* $g(x) \equiv h(x) \mod p(x)$, *niin* $f(x) \equiv h(x) \mod p(x)$ *kaikille* $h(x) \in K[x]$.

Relaatio $f(x) \equiv g(x) \mod p(x)$ on siten ekvivalenssirelaatio polynomirenkaassa $K[x]$.

Todistus. 1. Nyt $p(x) | \mathbf{0}$ eli $p(x) | f(x) - f(x)$ ja siten

$$f(x) \equiv f(x) \mod p(x).$$

2. Olkoon $f(x) \equiv g(x) \mod p(x)$. Nyt $p(x) | f(x) - g(x)$, josta saadaan $p(x) | g(x) - f(x)$ eli

$$g(x) \equiv f(x) \mod p(x).$$

3. Olkoon $f(x) \equiv g(x) \mod p(x)$ ja $g(x) \equiv h(x) \mod p(x)$. Nyt $p(x)|f(x)-g(x)$ ja $p(x)|g(x)-h(x)$ eli $f(x)-g(x) = m(x)p(x)$ ja $g(x)-h(x) = n(x)p(x)$, joillekin $m(x), n(x) \in K[x]$. Tällöin

$$\begin{aligned} & f(x) - g(x) + g(x) - h(x) = m(x)p(x) + n(x)p(x) \\ \Leftrightarrow\ & f(x) - h(x) = [m(x) + n(x)] \cdot p(x) \\ \Leftrightarrow\ & p(x)|f(x) - h(x), \end{aligned}$$

josta saadaan

$$f(x) \equiv h(x) \mod p(x).$$

□

Lause 5.4. *Olkoon K kunta ja oletetaan, että $f(x) \equiv g(x) \mod p(x)$ ja $a(x) \equiv b(x) \mod p(x)$ joillekin polynomeille $f(x), g(x), a(x), b(x), p(x) \in K[x]$. Tällöin*

1. $(f(x) + a(x)) \equiv (g(x) + b(x)) \mod p(x)$;
2. $f(x)a(x) \equiv g(x)b(x) \mod p(x)$;
3. *Jos $h(x) \in K[x]$, niin* $h(x)f(x) \equiv h(x)g(x) \mod p(x)$;
4. $f(x) \equiv g(x) \mod p(x)$ *jos ja vain jos polynomeilla $f(x)$ ja $g(x)$ on polynomilla $p(x)$ jakamisen jälkeen sama jakojäännös.*

Todistus. Osoitetaan kongruenssin aritmeettiset ominaisuudet.

1. Olkoon $f(x) \equiv g(x) \mod p(x)$ ja $a(x) \equiv b(x) \mod p(x)$, jolloin $f(x)-g(x) = m(x)p(x)$ ja $a(x)-b(x) = n(x)p(x)$, joillakin $m(x), n(x) \in K[x]$. Nyt

$$\begin{aligned} & f(x) - g(x) + a(x) - b(x) = m(x)p(x) + n(x)p(x) \\ \Leftrightarrow\ & [f(x) + a(x)] - [g(x) + b(x)] = [m(x) + n(x)] \cdot p(x), \end{aligned}$$

josta saadaan

$$f(x) + a(x) \equiv g(x) + b(x) \mod p(x).$$

2. Olkoon $f(x) \equiv g(x) \mod p(x)$. Tällöin on olemassa polynomi $q(x) \in K[x]$, jolle $f(x) - g(x) = q(x)p(x)$ eli $f(x) = g(x) + q(x)p(x)$. Samalla tavalla saadaan polynomi $c(x) \in K[x]$, jolle $a(x) = b(x) + c(x)p(x)$. Siis

$$\begin{aligned} a(x)f(x) &= [g(x) + q(x)p(x)] \cdot [b(x) + c(x)p(x)] \\ &= g(x)b(x) + c(x)g(x)p(x) + b(x)q(x)p(x) + q(x)p(x)c(x)p(x) \\ &= g(x)b(x) + p(x)\left[c(x)g(x) + b(x)q(x) + c(x)q(x)p(x)\right]. \end{aligned}$$

Olkoon nyt polynomi $t(x) = c(x)g(x) + b(x)q(x) + c(x)q(x)p(x)$, jolloin $a(x)f(x) - g(x)b(x) = p(x)t(x)$. Siis

$$f(x)a(x) \equiv g(x)b(x) \mod p(x).$$

3. Olkoon polynomi $h(x) \in K[x]$ ja $f(x) \equiv g(x) \mod p(x)$, jolloin

$$\begin{aligned} & p(x) | f(x) - g(x) \\ & \Rightarrow p(x) | \, [f(x) - g(x)] \cdot h(x) \\ & \Rightarrow p(x) | \, f(x) \cdot h(x) - g(x) \cdot h(x). \end{aligned}$$

   Siis

$$f(x)h(x) \equiv g(x)h(x) \mod p(x).$$

4. Olkoon $f(x) = q(x)p(x) + r_f(x)$ ja $g(x) = s(x)p(x) + r_g(x)$, missä $r_f(x)$ ja $r_g(x)$ ovat jakojäännökset polynomilla $p(x)$ jakamisesta.

   Oletetaan ensiksi, että $r_f(x) = r_g(x)$, jolloin

$$f(x) - g(x) = q(x)p(x) + r_f(x) - s(x)p(x) - r_g(x) = p(x)(q(x) - s(x))$$

   eli $f(x) \equiv g(x) \mod p(x)$.

   Oletetaan nyt, että $f(x) \equiv g(x) \mod p(x)$. Siis

$$q(x)p(x) + r_f(x) \equiv s(x)p(x) + r_g(x) \mod p(x)$$

   ja siten

$$r_f(x) \equiv r_g(x) \mod p(x),$$

   joten erotus $r_f(x) - r_g(x)$ on jaollinen polynomilla $p(x)$. Koska erotuksen $r_f(x) - r_g(x)$ aste on pienempi kuin polynomin $p(x)$ aste, niin $r_f(x) - r_g(x) = \mathbf{0}$ eli $r_f(x) = r_g(x)$.

□

Lauseen 5.4 viimeisen kohdan mukaan polynomin $f(x)$ *ekvivalenssiluokan* $[f(x)] \mod p(x)$ mikä tahansa polynomi on kongruentti modulo $p(x)$ tasan yhden sellaisen polynomin kanssa, jonka aste on pienempää kuin $degp(x)$. Merkitään tätä polynomia $r_f(x)$, joka on polynomin $f(x)$ jakojäännös polynomilla $p(x)$ jakamisen jälkeen.

Jakojäännös $r_f(x)$ on polynomin $f(x)$ ekvivalenssiluokan $[f(x)]$ *pääedustaja.*

Esimerkki 5.5. Olkoon $p(x) = x^2 + 2$ polynomirenkaan $\mathbb{Q}[x]$ polynomi. Tällöin saadaan $x^2 \equiv -2 \mod p(x)$. Mille polynomille polynomi $x^4 + 3x^3 + x + 2$ on kongruentti modulo $p(x)$?

Ratkaisu:

$$\begin{aligned} x^4 + 3x^3 + x + 2 &\equiv (x^2)^2 + 3(x^2)x + x + 2 \\ &\equiv (-2)^2 + 3(-2)x + x + 2 \\ &\equiv 4 - 6x + x + 2 \\ &\equiv -5x + 6 \mod p(x). \end{aligned}$$

Nyt $deg(-5x + 6) < degp(x)$, joten ei tarvitse jatkaa. Siis polynomi $x^4 + 3x^3 + x + 2$ on kongruentti polynomin $-5x + 6$ kanssa modulo $p(x)$.

Esimerkki 5.6. Olkoon $p(x) = x^2 + x + 1$ polynomirenkaan $\mathbb{Z}_2[x]$ polynomi. Mikä on ekvivalenssiluokan $[x^4]$ modulo $p(x)$ pääedustaja polynomirenkaassa $\mathbb{Z}_2[x]$?

Ratkaisu:
Koska $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$, niin $x^2 \equiv x + 1 \mod p(x)$. Nyt

$$x^4 \equiv (x^2)^2 \equiv (x+1)^2 \equiv x^2+2x+1 \equiv x^2+1 \equiv x+1+1 \equiv x+2 \equiv x \mod p(x).$$

Näin ollen

$$x^4 \equiv x \mod p(x)$$

polynomirenkaassa $\mathbb{Z}_2[x]$ eli $[x^4] = [x] \mod p(x)$.

5.2 Jäännösluokka

Määritelmä 5.7. Ekvivalenssiluokkien joukkoa, minkä määrittää modulo $p(x)$, merkitään $K[x]/\langle p(x)\rangle$. Tämän joukon alkioina olevia ekvivalenssiluokkia kutsutaan *jäännösluokiksi modulo* $p(x)$.

Polynomin $f(x) \in K[x]$ jäännösluokkaa merkitään $[f(x)]$. Polynomin $f(x)$ jakojäännöksen aste on pienempi kuin polynomin $p(x)$ aste.

Esimerkki 5.8. Olkoon $p(x) = x^2+2x+1$ polynomirenkaan $\mathbb{Z}_3[x]$ polynomi. Nyt jäännösluokkien modulo $p(x)$ joukko

$$\mathbb{Z}_3[x]/\langle p(x)\rangle = \{[0], [1], [2], [x], [x+1], [x+2], [2x], [2x+1], [2x+2]\}.$$

Polynomista $p(x) = x^2+2x+1$ saadaan, että $x^2 \equiv -2x-1 \equiv x+2 \mod p(x)$. Nyt saadaan esimerkiksi polynomille x^4, että

$$\begin{aligned} x^4 &\equiv (x^2)^2 \equiv (x+2)^2 \equiv x^2 + 4x + 4 \\ &\equiv x^2 + x + 1 \equiv x + 2 + x + 1 \\ &\equiv 2x + 3 \equiv 2x \mod p(x). \end{aligned}$$

Näin ollen $[x^4] = [2x]$ joukossa $\mathbb{Z}_3[x]/\langle p(x)\rangle$.

Esimerkki 5.9. Olkoon polynomi $p(x) = x^2-3 \in \mathbb{Q}[x]$. Nyt jäännösluokkien joukko $K[x]/\langle p(x)\rangle = \{[ax+b] | \, a, b \in \mathbb{Q}\}$, joka on ääretön joukko, koska a ja b voivat olla mikä tahansa rationaaliluku.

Jäännösluokkien joukko $K[x]/\langle p(x)\rangle$ on rengas, kun yhteen- ja kertolasku määritellään seuraavalla tavalla. Olkoon polynomien $f(x) \in K[x]$ ja $g(x) \in K[x]$ jäännösluokat $[f(x)] \in K[x]/\langle p(x)\rangle$ ja $[g(x)] \in K[x]/\langle p(x)\rangle$. Määritellään yhteenlasku siten, että

$$[f(x)] + [g(x)] = [f(x) + g(x)],$$

ja kertolasku

$$[f(x)] \cdot [g(x)] = [f(x) \cdot g(x)].$$

Lauseen 5.4 kohtien $1-3$ mukaan jäännösluokkien operaatiot $(+)$ ja $(\cdot)$ ovat hyvin määriteltyjä.

Esimerkki 5.10. Olkoon $p(x) = x^3+2x+1$ polynomirenkaan $\mathbb{Q}[x]$ polynomi, jolloin $x^3 \equiv -2x-1 \mod p(x)$. Joukossa $\mathbb{Q}[x]/\langle p(x)\rangle$ jäännösluokkien $[x^2 + x + 1]$ ja $[2x+3]$ yhteen- ja kertolaskusta saadaan

$$[x^2 + x + 1] + [2x + 3] = [x^2 + 3x + 4]$$

ja

$$\begin{aligned} [x^2 + x + 1] \cdot [2x + 3] &= [2x^3 + 5x^2 + 5x + 3] \\ &= [2(-2x - 1) + 5x^2 + 5x + 3] \\ &= [-4x - 2 + 5x^2 + 5x + 3] \\ &= [5x^2 + x + 1]. \end{aligned}$$

5.3 Jäännösluokkarengas

Lause 5.11. *Jäännösluokkien joukko $K[x]/\langle p(x)\rangle$ on kommutatiivinen rengas.*

Todistus. Osoitetaan, että $(K[x]/\langle p(x)\rangle, +, \cdot)$ on rengas.

1. Osoitetaan, että $(K[x]/\langle p(x)\rangle, +)$ on Abelin ryhmä:

   - Olkoon $[f(x)], [g(x)] \in K[x]/\langle p(x)\rangle$. Tällöin
   $$[f(x)] + [g(x)] = [f(x) + g(x)] \in K[x]/\langle p(x)\rangle;$$
   - Olkoon $[f(x)], [g(x)], [h(x)] \in K[x]/\langle p(x)\rangle$. Tällöin
   $$\begin{aligned}[f(x)] + ([g(x)] + [h(x)]) &= [f(x)] + ([g(x) + h(x)]) \\ &= [f(x) + g(x) + h(x)] \\ &= [f(x) + g(x)] + [h(x)] \\ &= ([f(x)] + [g(x)]) + [h(x)];\end{aligned}$$
   - Nyt $[\mathbf{0}] \in K[x]/\langle p(x)\rangle$ ja
   $$[\mathbf{0}] + [f(x)] = [\mathbf{0} + f(x)] = [f(x)] = [f(x) + \mathbf{0}] = [f(x)] + [\mathbf{0}],$$
   kaikilla $[f(x)] \in K[x]/\langle p(x)\rangle$, joten $[\mathbf{0}]$ on nolla-alkio jäännösluokkien joukossa $K[x]/\langle p(x)\rangle$;
   - Olkoon $[f(x)] \in K[x]/\langle p(x)\rangle$. Tällöin $[-f(x)] \in K[x]/\langle p(x)\rangle$ ja
   $$[f(x)] + [-f(x)] = [f(x) - f(x)] = [\mathbf{0}] = [-f(x)] + [f(x)],$$
   joten $[-f(x)]$ on jäännösluokan $[f(x)]$ vasta-alkio jäännösluokkien joukossa $K[x]/\langle p(x)\rangle$;
   - Olkoon $[f(x)], [g(x)] \in K[x]/\langle p(x)\rangle$. Tällöin
   $$[f(x)] + [g(x)] = [f(x) + g(x)] = [g(x) + f(x)] = [g(x)] + [f(x)].$$

   Näin ollen $(K[x]/\langle p(x)\rangle, +)$ on Abelin ryhmä.

2. Osoitetaan, että $(K[x]/\langle p(x)\rangle, \cdot)$ on monoidi:

   - Olkoon $[f(x)], [g(x)] \in K[x]/\langle p(x)\rangle$. Tällöin
   $$[f(x)] \cdot [g(x)] = [f(x) \cdot g(x)] \in K[x]/\langle p(x)\rangle;$$

- Olkoon $[f(x)], [g(x)], [h(x)] \in K[x]/\langle p(x)\rangle$. Tällöin

$$\begin{aligned}[f(x)] \cdot ([g(x)] \cdot [h(x)]) &= [f(x)] \cdot ([g(x) \cdot h(x)]) \\ &= [f(x) \cdot g(x) \cdot h(x)] \\ &= [f(x) \cdot g(x)] \cdot [h(x)] \\ &= ([f(x)] \cdot [g(x)]) \cdot [h(x)];\end{aligned}$$

- Nyt $[\mathbf{1}] \in K[x]/\langle p(x)\rangle$ ja

$$[\mathbf{1}] \cdot [f(x)] = [\mathbf{1} \cdot f(x)] = [f(x)] = [f(x) \cdot \mathbf{1}] = [f(x)] \cdot [\mathbf{1}],$$

kaikilla $[f(x)] \in K[x]/\langle p(x)\rangle$, joten $[\mathbf{1}]$ on ykkösalkio jäännösluokkien joukossa $K[x]/\langle p(x)\rangle$.

Näin ollen $(K[x]/\langle p(x)\rangle, \cdot)$ on monoidi.

3. Osoitetaan, että osittelulait ovat voimassa. Olkoon $[f(x)], [g(x)], [h(x)] \in K[x]/\langle p(x)\rangle$. Tällöin

$$\begin{aligned}[f(x)] \cdot ([g(x)] + [h(x)]) &= [f(x)] \cdot [g(x) + h(x)] \\ &= [f(x) \cdot (g(x) + h(x))] \\ &= [f(x) \cdot g(x) + f(x) \cdot h(x)] \\ &= [f(x) \cdot g(x)] + [f(x) \cdot h(x)]\end{aligned}$$

ja

$$\begin{aligned}([f(x)] + [g(x)]) \cdot [h(x)] &= [f(x) + g(x)] \cdot [h(x)] \\ &= [(f(x) + g(x)) \cdot h(x)] \\ &= [f(x) \cdot h(x) + g(x) \cdot h(x)] \\ &= [f(x) \cdot h(x)] + [g(x) \cdot h(x)].\end{aligned}$$

Kohtien $1 - 3$ nojalla $(K[x]/\langle p(x)\rangle, +, \cdot)$ on rengas. Osoitetaan vielä, että $(K[x]/\langle p(x)\rangle, +, \cdot)$ on kommutatiivinen kertolaskun suhteen. Nyt

$$[f(x)] \cdot [g(x)] = [f(x) \cdot g(x)] = [g(x) \cdot f(x)] = [g(x)] \cdot [f(x)].$$

Näin ollen $(K[x]/\langle p(x)\rangle, +, \cdot)$ on kommutatiivinen rengas. □

Määritelmä 5.12. $K[x]/\langle p(x)\rangle$ on *jäännösluokkarengas modulo* $p(x)$.

Lause 5.13. *Jäännösluokkarengas* $K[x]/\langle p(x)\rangle$ *on kunta, jos ja vain jos polynomi* $p(x)$ *on jaoton polynomirenkaassa* $K[x]$.

Todistus. Jos polynomi $p(x)$ on jaollinen, niin $p(x) = f(x)g(x)$, missä polynomit $f(x), g(x) \in K[x]$ eivät ole vakiopolynomeja ja polynomien $f(x)$ ja $g(x)$ asteet ovat pienempiä kuin polynomin $p(x)$ aste. Polynomien $f(x)$ ja $g(x)$ jäännösluokat joukossa $K[x]/\langle p(x)\rangle$ ovat nollanjakajia, koska $[f(x)][g(x)] = [p(x)] = [\mathbf{0}]$. Siis $K[x]/\langle p(x)\rangle$ ei ole kunta.

Oletetaan, että polynomi $p(x)$ on jaoton. On osoitettava, että jokaisella nolla-alkiosta eroavalla alkiolla $[f(x)] \in K[x]/\langle p(x)\rangle$ on käänteisalkio.

Jos $[f(x)] \neq [\mathbf{0}]$ renkaassa $K[x]/\langle p(x)\rangle$, niin polynomi $f(x)$ ei ole jaollinen polynomilla $p(x)$ ja siksi polynomit $f(x)$ ja $p(x)$ ovat keskenään jaottomia. Lauseen 4.4 nojalla saadaan, että jos polynomit $f(x)$ ja $p(x)$ ovat keskenään jaottomia, niin

$$s(x)f(x) + t(x)p(x) = \mathbf{1},$$

joillakin $s(x), t(x) \in K[x]$. Nyt

$$s(x)f(x) \equiv \mathbf{1} \mod p(x),$$

eli $[s(x)f(x)] = [\mathbf{1}]$. Tästä saadaan $[s(x)][f(x)] = [\mathbf{1}]$ eli $[f(x)]^{-1} = [s(x)]$. Siis $[s(x)]$ on jäännösluokan $[f(x)]$ käänteisalkio renkaassa $K[x]/\langle p(x)\rangle$. Näin ollen $K[x]/\langle p(x)\rangle$ on kunta. □

Esimerkki 5.14. Olkoon polynomirengas $\mathbb{Z}_2[x]$ ja $p(x) = [1]x^2 + [1]x + [1]$ sen jaoton polynomi. Polynomista $p(x)$ saadaan, että $x^2 \equiv -x - 1 \mod p(x)$ eli

$$x^2 \equiv x + 1 \mod p(x).$$

Saadaan jäännösluokkarengas

$$\mathbb{Z}_2[x]/\langle p(x)\rangle = \{[0], [1], [x], [x+1]\}.$$

Nyt saadaan jäännösluokkarenkaan alkioille operaatiot $(+)$ ja $(\cdot)$ eli

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

ja

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Koska $p(x)$ on nyt jaoton polynomi, niin jäännösluokkarengas $\mathbb{Z}_2[x]/\langle p(x)\rangle$ on kunta.

Esimerkki 5.15. Polynomi $p(x) = x^3-2$ on jaoton polynomirenkaassa $\mathbb{Q}[x]$, joten $\mathbb{Q}[x]/\langle p(x)\rangle$ on kunta. Määritetään polynomin $f(x) = x^2 + 2x + 1$ jäännösluokalle $[f(x)]$ käänteisalkio kunnassa $\mathbb{Q}[x]/\langle p(x)\rangle$.

Eukleideen algoritmilla saadaan

$$\underbrace{x^3 - 2}_{p(x)} = (x-2)\cdot(\underbrace{x^2+2x+1}_{f(x)}) + 3x$$

ja

$$\underbrace{x^2+2x+1}_{f(x)} = (\frac{1}{3}x + \frac{2}{3})\cdot(3x) + 1.$$

Käyttämällä Eukleideen algoritmia toiseen suuntaan voidaan ratkaista yhtälöstä luku 1 eli

$$\begin{aligned}
1 &= (\underbrace{x^2+2x+1}_{f(x)}) - (\frac{1}{3}x+\frac{2}{3})\cdot(3x)\\
&= (\underbrace{x^2+2x+1}_{f(x)}) - (\frac{1}{3}x+\frac{2}{3})[((\underbrace{x^3-2}_{p(x)}) - (x-2)\cdot(\underbrace{x^2+2x+1}_{f(x)}))]\\
&= (\underbrace{x^2+2x+1}_{f(x)}) - (\frac{1}{3}x+\frac{2}{3})(\underbrace{x^3-2}_{p(x)}) + (\frac{1}{3}x+\frac{2}{3})(x-2)\cdot(\underbrace{x^2+2x+1}_{f(x)})\\
&= [1+(\frac{1}{3}x+\frac{2}{3})(x-2)](\underbrace{x^2+2x+1}_{f(x)}) - [\frac{1}{3}x+\frac{2}{3}](\underbrace{x^3-2}_{p(x)})\\
&= [\frac{1}{3}x^2-\frac{1}{3}](\underbrace{x^2+2x+1}_{f(x)}) - [\frac{1}{3}x+\frac{2}{3}](\underbrace{x^3-2}_{p(x)}).
\end{aligned}$$

Siis

$$1 \equiv [\frac{1}{3}x^2-\frac{1}{3}](\underbrace{x^2+2x+1}_{f(x)}) \mod p(x),$$

joten jäännösluokan $[f(x)]$ käänteisalkio on

$$[f(x)]^{-1} = [\frac{1}{3}x^2 - \frac{1}{3}].$$

Lähdeluettelo

[1] I. N. Herstein: *Abstract algebra Third Edition.* Prentice-Hall, New Jersey, USA, 1990.

[2] K. Myllylä: *Algebra 1 -luentomateriaali.* Oulun yliopisto, Matemaattisten tieteiden laitos, 2010.

[3] O.E. Nicodemi, M.A. Sutherland, G.W. Towsley: *An introduction to abstract algebra with notes to the future teacher.* State University of New York, USA, 2007.

[4] M. Niemenmaa: *Algebra 2 -luentomateriaali.* Oulun yliopisto, Matemaattisten tieteiden laitos, 2011.

[5] H: Paley, P.M. Weichsel : *A first course in Abstract Algebra.* University of Illinois, USA, 1963.

[6] E.M. Patterson, D.E. Ruhterford: *Elementary Abstract Algebra.* New York, USA, 1965.

[7] B.L. van der Waerden: *Algebra Volume 1.* New York, USA, 1991.