Tässä luvussa tarkastelemme polynomien muodostamia renkaita ja polynomien jaollisuutta käsitteleviä perustuloksia. Algebrassa on tapana pitää erillään polynomin ja polynomifunktion käsitteet. Ennen näiden käsitteiden määrittelyä teemme kaksi sopimusta:

- Tässä luvussa X on muodollinen symboli, jota usein kutsutaan muuttujaksi.
- Symbolin $-\infty$ sovitaan tarkoittavan "ääretöntä negatiivista lukua", jolle pätee
  - $-\infty < a$ kaikilla kokonaisluvuilla a,
  - $-\infty + -\infty = -\infty$, ja
  - $-\infty + a = -\infty$ kaikilla kokonaisluvuilla a.

Symbolille $-\infty$ ei ole määritelty muita operaatioita, käytämme sitä ainoastaan nollapolynomin asteen merkkinä.

Määritelmä 10.1. Olkoon R kommutatiivinen rengas, jossa on vähintään kaksi alkiota. Olkoon $n \in \mathbb{N}$, ja olkoot $a_n, a_{n-1}, \ldots, a_1, a_0 \in R$. Lauseke

$$P(X) = \sum_{k=0}^{n} a_k X^k = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

on *yhden muuttujan R-kertoiminen polynomi*. Jos $a_n \neq 0$, niin polynomin $P(X)$ *aste* on $\deg(P(X)) = n$. Nollapolynomin 0 aste on $-\infty$. Kaikkien R-kertoimisten polynomien joukkoa merkitään $R[X]$.

Olkoot $P(X) = \sum_{k=1}^{n} a_k X^k$ ja $Q(X) = \sum_{k=1}^{m} b_k X^k$ R-kertoimisia polynomeja, $n \geq m$. Olkoot $b_{m+1} = b_{m+2} = \cdots = b_n = 0$, jos $n > m$. Polynomien summa ja tulo määritellään asettamalla

$$P(X) + Q(X) = \sum_{k=0}^{n} (a_k + b_k) X^k$$

ja

$$P(X)Q(X) = \sum_{k=0}^{n+m} \Big(\sum_{i+j=k} a_i b_j \Big) X^k. \tag{16}$$

Polynomien yhteen- ja kertolasku määritellään siis kuten tavallista ja on helppo nähdä, että ne ovat laskutoimituksia.

Propositio 10.2. *Olkoon R kommutatiivinen rengas, jossa on vähintään kaksi alkiota. Joukko $R[X]$ varustettuna polynomien yhteen- ja vähennyslaskulla on kommutatiivinen rengas. Kuvaus $i\colon R \to R[X]$, joka kuvaa renkaan R alkion a polynomiksi $a \in R[X]$, on injektiivinen rengashomomorfismi.*

Todistus. Selvästi polynomit 0 ja 1 ovat yhteenlaskun ja kertolaskun neutraalialkiot. Muut ominaisuudet seuraavat suoraviivaisesti siitä, että R on rengas. □

Polynomirenkaat ovat tärkeitä kommutatiivisia renkaita, havainnollistamme niiden merkitystä hieman kurssin viimeisessä luvussa, kun sovellamme niitä äärellisten kuntien konstruktiossa. Rengas R voidaan ajatella Proposition 10.2 kuvauksen i avulla polynomirenkaan $R[X]$ alirenkaaksi.

Vähemmän havainnollinen Määritelmän 10.1 kanssa ekvivalentti tapa määritellä polynomit on korvata polynomin lauseke $\sum_{k=0}^{n} a_k X^k$ kertoimien muodostamalla jonolla $(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$ ja määritellä yhteenlasku kuten jonoille on tapana ja kertolasku kaavan (16) mukaisesti. Tällöin jono $(0, 1, 0, 0, 0, \ldots)$ on symbolin X vastine.

Määritelmä 10.3. Olkoon R kommutatiivinen rengas. Polynomin

$$P(X) = \sum_{k=0}^{n} a_k X^k \in R[X]$$

määräämä *polynomifunktio* on $P\colon R \to R$, $x \mapsto \sum_{k=0}^{n} a_k x^k = P(x)$.

Propositio 10.4. *Kuvaus, joka liittää R-kertoimiseen polynomiin $P(X)$ polynomifunktion $P\colon R \to R$, on rengashomomorfismi polynomirenkaasta $R[X]$ funktiorenkaaseen $\mathscr{F}(X, X)$.*

Todistus. Harjoitustehtävä 108. □

Esimerkki 10.5. Joillakin renkailla R kaksi polynomirenkaan $R[X]$ eri polynomia voi määrätä saman polynomifunktion: Olkoot $Q(X) = X^2, P(X) = X \in (\mathbb{Z}/2\mathbb{Z})[X]$. Tällöin $P(0) = 0 = 0^2 = Q(0)$, ja $P(1) = 1 = 1^2 = Q(1)$, joten polynomit $P(X)$ ja $Q(X)$ vastaavat samaa polynomifunktiota. Nollasta poikkeava polynomi $Q(X) - P(X) = X^2 - X$, määrää nollakuvauksen renkaalta $\mathbb{Z}/2\mathbb{Z}$ itselleen.

Esimerkki 10.6. Olkoot $P(X), Q(X) \in \mathbb{Z}[X]$,

$$P(X) = 2X^2 + 2, \quad Q(X) = 1 + 2X\ .$$

Tällöin

$$P(X)Q(X) = 4X^3 + 2X^2 + 4X + 2.$$

Nyt $\deg(P(X)) = 2$, $\deg(Q(X)) = 1$ ja $\deg(P(X)Q(X)) = 3$.

Jos polynomit $P(X), Q(X) \in (\mathbb{Z}/4\mathbb{Z})[X]$ määritellään samoilla lausekkeilla kuin edellä ja polynomin kertoimena oleva kokonaisluku a_k tulkitaan aina kongruenssiluokaksi $a_k + 4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}$, niin

$$P(X)Q(X) = 2X^2 + 2.$$

Edelleen pätee $\deg(P(X)) = 2$, $\deg(Q(X)) = 1$ mutta nyt

$$\deg(P(X)Q(X)) = 2 < 3 = 2 + 1.$$

Esimerkin 10.6 tulos yleistyy kaikille polynomirenkaille:

Lemma 10.7. *Olkoon R kommutatiivinen rengas, $R \neq \{0\}$. Tällöin*

$$\deg(P(X)Q(X)) \leq \deg P(X) + \deg Q(X)$$

kaikille $P(X), Q(X) \in R[X]$.

Todistus. Olkoot $P(X) = \sum_{k=0}^{n} a_k X^k$ ja $Q(X) = \sum_{k=0}^{m} b_k X^k$ ja oletetaan, että $a_n \neq 0$, $b_m \neq 0$. Tulopolynomin $P(X)Q(X)$ korkeimman asteen termi on $a_n b_m X^{n+m}$, jos $a_n b_m \neq 0$, muuten aste on alempi. □

Propositio 10.8. *Jos K on kokonaisalue, niin $K[X]$ on kokonaisalue. Tällöin*

$$\deg(P(X)Q(X)) = \deg(P(X)) + \deg(Q(X)).$$

Todistus. Lemman 10.7 merkinnöillä tulopolynomin korkeimman asteen termin kerroin on $a_n b_m \neq 0$, sillä K on kokonaisalue. □

Esimerkki 10.9. Polynomi $2X$ on nollan jakaja renkaassa $(\mathbb{Z}/4\mathbb{Z})[X]$:

$$(2X)(2X) = 4X^2 = 0.$$

Nyt siis

$$-\infty = \deg 0 = \deg((2X)(2X)) < 2\deg(2X) = 2.$$

Polynomirengas ei ole koskaan kunta. Jos K on kokonaisalue, niin Proposition 10.8 mukaan ainoat polynomit, joilla on käänteisalkio kertolaskun suhteen ovat vakiopolynomit u, missä $u \in K^\times$. Sen sijaan, jos kerroinrengas ei ole kokonaisalue, niin vakiopolynomeilla a, missä a on nollan jakaja renkaassa K, ei ole käänteisalkiota. Nyt kuitenkin joillakin korkeamman asteen polynomeilla on käänteisalkiot.

Esimerkki 10.10. Renkaassa $(\mathbb{Z}/4\mathbb{Z})[X]$ pätee

$$(2X+1)(2X+1) = 4X^2 + 4X + 1 = 1.$$

Samalla lausekkeella annettujen polynomien jaollisuus riippuu tarkasteltavasta polynomirenkaasta:

Esimerkki 10.11. (a) $(X-1) \mid (X^2-1)$ ja $(X+1) \mid (X^2-1)$ kaikissa polynomirenkaissa $R[X]$:

$$(X-1)(X+1) = X^2 + (1-1)X - 1 = X^2 - 1.$$

(b) $(X+1) \mid (X^2+1)$ renkaassa $(\mathbb{Z}/2\mathbb{Z})[X]$, sillä $1 = -1$ renkaassa $\mathbb{Z}/2\mathbb{Z}$.
(c) $(X+1) \nmid (X^2+1)$ renkaassa $\mathbb{C}[X]$: Jos $(X+1) \mid (X^2+1)$, niin on $A, B \in \mathbb{C}$, joille $(X+1)(AX+B) = X^2+1$. Tällöin toisen ja nollannen asteen kertoimia tarkastelemalla havaitaan, että pitää olla $A = 1 = B$, mutta ensimmäisen asteen termit eivät täsmää.

Olemme käyttäneet kurssilla muutamia kertoja kokonaislukujen jakoyhtälöä: Olkoot $a, b \in \mathbb{Z}$ ja $b \neq 0$. Tällöin on yksikäsitteiset $q, j \in \mathbb{Z}$, joille

$$a = qb + j \quad \text{ja} \quad 0 \leq j < |b|.$$

Todistamme seuraavaksi vastaavan tuloksen polynomeille:

Lause 10.12 (Jakoyhtälö)**.** *Olkoon R kommutatiivinen rengas, jossa on vähintään kaksi alkiota. Olkoot $A(X)$, $B(X) \in R[X]$ siten, että $B(X) \neq 0$ ja polynomin $B(X)$ korkeimman asteen termin kerroin on yksikkö. Tällöin on yksikäsitteiset $Q(X), J(X) \in R[X]$, joille*

$$A(X) = Q(X)B(X) + J(X)$$

ja $\deg J(X) < \deg B(X)$.

Todistus. Jos $B(X)$ jakaa polynomin $A(X)$, ei ole mitään todistettavaa. Muuten olkoon

$$S = \{A(X) - D(X)B(X) : D(X) \in R[X]\}.$$

Selvästi $S \neq \emptyset$. Koska $B(X) \nmid A(X)$, niin $0 \notin S$, joten

$$t = \min\{\deg P(X) : P(X) \in S\} \geq 0.$$

Olkoon $Q(X) \in R[X]$ polynomi, jolle pätee $\deg(A(X) - Q(X)B(X)) = t$. Olkoon

$$J(X) = A(X) - Q(X)B(X) = a_t X^t + \cdots + a_0.$$

Osoitamme, että $t < d = \deg B(X)$. Olkoon b_d polynomin $B[X]$ korkeimman asteen kerroin. Jos olisi $t \geq d$, niin

$$J(X) - a_t b_d^{-1} X^{t-d} B(X) = A(X) - (Q(X) + a_t b_d^{-1} X^{t-d})B(X) \in S$$

ja $\deg\big(J(X) - a_t b_d^{-1} X^{t-d} B(X)\big) < t$, mutta tämä on mahdotonta, koska polynomin $J(X)$ aste on minimaalinen.

Jos $\widetilde{Q}(X)$ ja $\widetilde{J}(X)$ ovat polynomeja, joilla on samat ominaisuudet kuin polynomeilla $Q(X)$ ja $J(X)$, niin

$$(Q(X) - \widetilde{Q}(X))B(X) = \widetilde{J}(X) - J(X).$$

Jos $\widetilde{Q}(X) \neq Q(X)$, niin vasemman puolen aste on vähintään d, kuitenkin

$$\deg(\widetilde{J}(X) - J(X)) \leq t < d.$$

Siis $\widetilde{Q}(X) = Q(X)$ ja $\widetilde{J}(X) = J(X)$. □

Seuraus 10.13 (Jakoyhtälö)**.** *Olkoon K kunta. Olkoot $A(X)$, $B(X) \in K[X]$ siten, että $B(X) \neq 0$. Tällöin on yksikäsitteiset $Q(X), J(X) \in R[X]$, joille*

$$A(X) = Q(X)B(X) + J(X)$$

ja $\deg J(X) < \deg B(X)$. □

Esimerkki 10.14. Jakoyhtälö voidaan toteuttaa algoritmisesti jakokulman avulla kuten kokonaisluvuillekin. Tällöin esimerkiksi polynomeille $A(X) = 2X^3+X^2-X-1$ ja $B(X) = X^2 - 2$ renkaassa $\mathbb{Z}[X]$ jakokulma antaa

$$\begin{array}{rr|llll} & & 2X & +1 & & \\ \cline{3-6} X^2-2 & & 2X^3 & +X^2 & -X & -1 \\ & & \mp 2X^3 & & \pm 4X & \\ \cline{3-5} & & & X^2 & +3X & -1 \\ & & & X^2 & & \pm 2 \\ \cline{4-6} & & & & 3X & +1 \end{array}.$$

Toisin sanoen

$$2X^3 + X^2 - X - 1 = (2X + 1)(X^2 - 2) + 3X + 1,$$

joten $Q(X) = 2X + 1$ ja $J(X) = 3X + 1$. Renkaassa $(\mathbb{Z}/3\mathbb{Z})[X]$ polynomeille $A(X)$ ja $B(X)$

$$2X^3 + X^2 - X - 1 = (2X + 1)(X^2 - 2) + 1 = (2X + 1)(X^2 + 1) + 1. \tag{17}$$

Toisaalta, jos $B(X) = 2X+1$, niin jakoyhtälö ei toimi renkaassa $\mathbb{Z}[X]$: jakokulmassa päädytään ongelmalliseen tilanteeseen

$$2X^3 + X^2 - X - 1 = X^2(2X + 1) - X - 1,$$

josta ei voi jatkaa. Sen sijaan renkaassa $(\mathbb{Z}/3\mathbb{Z})[X]$ voidaan jatkaa, koska $\mathbb{Z}/3\mathbb{Z}$ on kunta. Nyt

$$-X - 1 = 2X + 2 = (2X + 1) + 1$$

ja päädytään yhtälöön (17). Renkaassa $\mathbb{Q}[X]$ jakoa voi myös jatkaa, ja saadaan

$$2X^3 + X^2 - X - 1 = (X^2 - \frac{1}{2})(2X + 1) - \frac{1}{2}.$$

Polynomien jaollisuutta tutkittaessa on usein hyödyllistä tarkastella polynomien juuria (tai niitä vastaavien polynomifunktioiden nollakohtia).

Määritelmä 10.15. Olkoon R kommutatiivinen rengas, ja olkoon $P(X) \in R[X]$. Alkio $c \in R$ on polynomin $P(X)$ *juuri*, jos $P(c) = 0$.

Jakoyhtälö antaa seuraavan perustuloksen:

Propositio 10.16. *Olkoon R kommutatiivinen rengas. Olkoon $P(X) \in R[X]$, ja $c \in R$. Tällöin $P(c) = 0$, jos ja vain jos $(X - c) \mid P(X)$.*

Todistus. Oletetaa, että $P(c) = 0$. Jakoyhtälön mukaan on R-kertoimiset polynomit $Q(X)$ ja $J(X)$, joille $\deg J(X) < 1$ ja $A(X) = Q(X)(X-c)+J(X)$. Koska $\deg J < 1$, $J(X)$ on vakiopolynomi, joten on $b \in R$, jolle $J(a) = b$ kaikilla $a \in R$. Erityisesti

$$0 = P(c) = Q(c)(c - c) + J(c) = b,$$

joten $b = 0$.

Toisaalta, jos $P(X) = (X - c)Q(X)$ jollain polynomilla $Q(X) \in R[X]$, niin

$$P(c) = (c - c)Q(c) = 0. \qquad \square$$

Propositio 10.17. *Olkoon K kokonaisalue. Olkoon $P(X) \in K[X]$ polynomi, ja olkoot $c_1, c_2, \ldots, c_k \in K$ polynomin $P(X)$ k eri juurta. Tällöin on $Q(X) \in K[X]$, jolle*

$$P(X) = (X - c_1)(X - c_2) \cdots (X - c_k)Q(X).$$

Todistus. Harjoitustehtävä 111. $\square$

Lause 10.18. *Olkoon K kokonaisalue, ja olkoon $n \geq 1$. Jos $P(X) \in K[X]$ ja $\deg P(X) = n$, niin polynomilla $P(X)$ on korkeintaan n juurta.*

Todistus. Propositioiden 10.17 ja 10.8 mukaan, jos polynomilla $P(X)$ on k juurta, niin $\deg(P(X)) \geq k$. $\square$

Erityisesti siis Propositio 2.9 antaa kaikki toisen asteen kompleksikertoimisen polynomiyhtälön ratkaisut.

Seuraus 10.19. *Olkoot $a_0, a_1 \in \mathbb{C}$. Yhtälön*

$$z^2 + a_1 z + a_0 = 0$$

ratkaisut ovat

$$z_1 = -\frac{a_1}{2} + \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0} \quad ja \quad z_2 = -\frac{a_1}{2} - \sqrt{\left(\frac{a_1}{2}\right)^2 - a_0}\,.$$

Propositio 10.20. *Olkoon K ääretön kokonaisalue. Tällöin jokaista kokonaisalueen K polynomifunktiota vastaa yksikäsitteinen polynomi renkaassa $K[X]$.*

Todistus. Olkoot $P(X), Q(X) \in K[X]$ siten, että $P(c) = Q(c)$ kaikilla $c \in K$. Tällöin polynomilla $P(X) - Q(X)$ on äärettömän monta juurta. Ainoa tällainen polynomi on 0. $\square$

Seuraus 10.21. *Olkoon K jokin kokonaisalueista $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ tai $\mathbb{C}$. Kuvaus, joka liittää jokaiseen polynomiin $P(X) \in K[X]$ vastaavan polynomifunktion $P\colon K \to K$, on injektio.*

Määritelmä 10.22. Kunta K on *algebrallisesti suljettu*, jos jokaisella vakiosta poikkeavalla polynomilla $P(X) \in K[X]$ on juuri.

Seuraus 10.23. *Jos K algebrallisesti suljettu kunta, niin jokainen vakiosta poikkeava polynomi $P(X) \in K[X]$ on ensimmäisen asteen polynomien tulo.* $\square$

Polynomin $P(X) \in R[X]$ sanotaan olevan *jaoton* jos ei ole polynomeja $S(X) \in R[X]$ ja $T(X) \in R[X]$, joille $P(X) = S(X)T(X)$ ja $\deg S(X), \deg T(X) < \deg P(X)$. Seurauksen 10.23 mukaan, jos K on algebrallisesti suljettu kunta, niin mikään vähintään toisen asteen polynomi ei ole jaoton. Toisaalta kaikki ensimmäisen asteen polynomit ovat jaottomia Proposition 10.8 nojalla.

Jos $(X - c)^k$ jakaa polynomin $P(X)$ renkaassa $R[X]$, niin c on polynomin $P(X)$ *k-kertainen juuri*. Yleensä, kun lasketaan polynomin juuria, k-kertaiset juuret huomioidaan laskussa k kertaa. Esimerkiksi 0 on polynomin X^2 kaksinkertainen juuri, ja kertaluku huomioiden polynomilla X^2 on siis kaksi juurta.

Seuraus 10.24. *Jos K algebrallisesti suljettu kunta, niin jokaisella nollasta poikkeavalla polynomilla $P(X) \in K[X]$ on juurten kertaluku huomioiden $\deg P(X)$ juurta.* $\square$

Lukualueiden ja kompleksianalyysin kursseilla todistetaan seuraava tärkeä tulos:

Lause 10.25 (Algebran peruslause)**.** *Kompleksilukujen kunta on algebrallisesti suljettu.* □

Seuraus 10.26. *Jokainen vakiosta poikkeava polynomi $P(X) \in \mathbb{C}[X]$ on ensimmäisen asteen polynomien tulo. Nollasta poikkeavalla polynomilla $P(X) \in \mathbb{C}[X]$ on juurten kertaluku huomioiden* $\deg P(X)$ *juurta.* □

Esimerkki 10.27. (a) Usein polynomeilla on vähemmän juuria kuin niiden asteesta tuleva maksimimäärä. Esimerkiksi polynomilla $X^3 + X \in \mathbb{R}[X]$ on täsmälleen yksi juuri ja polynomilla $X^2 + 1 \in \mathbb{R}[X]$ ei ole juuria lainkaan.

(b) Polynomi X^2+1 on jaoton renkaissa $\mathbb{Z}[X]$ ja $\mathbb{R}[X]$ mutta kompleksikertoimisten polynomien renkaassa $\mathbb{C}[X]$ pätee $X^2 + 1 = (X + i)(X - i)$.

(c) Polynomi $X^2 + X + 1$ on jaoton $\mathbb{Z}/2\mathbb{Z}$-kertoimisten polynomien renkaassa koska sillä ei ole yhtään juurta kahden alkion kunnassa $\mathbb{Z}/2\mathbb{Z}$. Sen sijaan mikään muu toisen asteen polynomit ei ole jaoton tässä renkaassa: X^2 on selvä tapaus, samoin $X^2 + X = X(X + 1)$. Lisäksi $X^2 + 1 = (X + 1)^2$.

Harjoitustehtäviä.

Tehtävä 108. Osoita, että kuvaus, joka liittää polynomiin $P(X) \in R[X]$ vastaavan polynomifunktion $P \in \mathscr{F}(X, X)$, on rengashomomorfismi.

Tehtävä 109. Osoita, että $F(X) = 1 - 2X$ on yksikkö renkaassa $(\mathbb{Z}/16\mathbb{Z})[X]$.

Tehtävä 110. Olkoon p alkuluku. Montako juurta polynomilla $X^p - X \in (\mathbb{Z}/p\mathbb{Z})[X]$ on?

Tehtävä 111. Olkoon K kokonaisalue. Olkoon $P(X) \in K[X]$ polynomi, ja olkoot $c_1, c_2, \ldots, c_k \in K$ polynomin $P(X)$ juuria. Osoita, että on $Q(X) \in K[X]$, jolle

$$P(X) = (X - c_1)(X - c_2) \cdots (X - c_k)Q(X).$$

Tehtävä 112. Olkoot $P(X), Q(X) \in (\mathbb{Z}/8\mathbb{Z})[X]$,

$$P(X) = 3 + 2X + 4X^2 + 2X^3$$

ja

$$Q(X) = 4 + 4X + 4X^2 + 4X^3 + 4X^4.$$

(1) Kerro $Q(X)$ polynomilla $P(X)$.

(2) Jaa $Q(X)$ polynomilla $P(X)$.

Tehtävä 113. Olkoon K kunta. Osoita, että toisen tai kolmannen asteen polynomi $P(X) \in K[X]$ on jaoton, jos ja vain jos sillä ei ole juurta kokonaisalueessa K. Anna esimerkki, joka osoittaa, että väite ei päde neljännen asteen polynomeille.

Tehtävä 114. (a) Onko polynomi $X^2 - 2 \in (\mathbb{Z}/5\mathbb{Z})[X]$ jaoton?

(b) Onko polynomi $X^2 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$ jaoton?

Tehtävä 115. Jaa polynomi

$$P(X) = X^3 + 2X^2 + 3X + 2$$

polynomilla

$$Q(X) = 2X^2 + 3X + 1$$

(1) polynomirenkaassa $\mathbb{Q}[X]$ ja

(2) polynomirenkaassa $(\mathbb{Z}/7\mathbb{Z})[X]$.

[109] Vihje: Kerroinrengas $\mathbb{Z}/16\mathbb{Z}$ ei ole kokonaisalue.

[110] Vihje: Käytä ryhmäteoriaa!