

## 11. Jaollisuudesta

Edellisen luvun esimerkissä tarvittiin tietoa erään polynomin jaottomuudesta. Tämä on hyvin tavallista kuntalaaajennosten yhteydessä. Seuraavassa tarkastellaan hieman jaollisuuskäsitettä yleensä sekä todistetaan joitain kriteerejä erityisesti polynomien jaottomuudelle.

**11.1. Jaollisuus kokonaisalueissa.** Olkoon  $R$  kokonaisalue<sup>18</sup>. Jaollisuuteen liittyvät käsitteet määritellään  $R$ :ssä samalla tavoin kuin kokonaislukuilla. Alkio  $a \in R$  jakaa alkion  $b \in R$ , jos  $b = ac$  jollain  $c \in R$ . Tällöin merkitään  $a|b$ , ja sanotaan myös, että  $b$  on  $a$ :n tekijä. Jos  $a|b$  ja  $b|a$ , niin  $a$  ja  $b$  ovat toistensa *liittoalkioita*. Liittoalkioilla on samat tekijät. Kääntyviä alkioita kutsutaan *yksiköiksi*, ja ne jakavat kaikki  $R$ :n alkioit, sillä jos  $a$  on yksikkö, niin  $b = a(a^{-1}b)$ . Seuraavan lemmän helppo todistus jätetään harjoitustehtäväksi.

LEMMA 11.1. *Oletetaan, että  $a, b \in R$ .*

- Alkiot  $a$  ja  $b$  ovat liittoalkioita, jos ja vain jos  $a = bc$ , missä  $c$  on yksikkö.*
- Jos  $a, b \in R \setminus \{0\}$  ovat liittoalkioita ja  $a = bc$ , niin  $c$  on yksikkö.*
- Kaikki yksiköt ovat toistensa liittoalkioita.*

Koska jokainen alkio on jaollinen kaikilla yksiköillä sekä omilla liittoalkioillaan, näitä voidaan pitää alkion *triviaaleina tekijöinä*, joita ei huomioida jaottomuustarkasteluissa. Yleisessä kokonaisalueessa voi olla kahdentyyppisiä jaottomia alkioita. Koska nolla-alkio on joka tapauksessa jaollinen kaikilla alkioilla, se jätetään kokonaan tarkastelun ulkopuolelle.

MÄÄRITELMÄ 11.2. Oletetaan, että  $a \in R \setminus \{0\}$  ei ole yksikkö. Tällöin  $a$ :ta sanotaan *jaottomaksi*, jos sen jokainen tekijä on joko yksikkö tai  $a$ :n liittoalkio.

MÄÄRITELMÄ 11.3. Oletetaan, että  $a \in R \setminus \{0\}$  ei ole yksikkö. Alkiota  $a$  sanotaan *alkualkioksi*, jos aina kun  $a$  jakaa tulon  $bc$ , jompikumpi alkioista  $b$  ja  $c$  on jaollinen  $a$ :lla.

Kokonaislukujen renkaassa  $\mathbb{Z}$  on vain kaksi yksikköä: 1 ja  $-1$ . Luvun  $n \in \mathbb{Z}$  liittoalkioita on samoin kaksi:  $n$  ja  $-n$ . Jokainen alkuluku  $p$  on jaoton, sillä sen tekijöitä ovat vain luvut 1,  $-1$ ,  $p$  ja  $-p$ , jotka ovat kaikki yksiköitä tai  $p$ :n liittoalkioita. Alkuluvut ja niiden liittoalkiot ovat myös ainoat jaottomat kokonaisluvut.

LAUSE 11.4. *Jos  $a \in R$  on alkualkio, se on jaoton.*

TODISTUS. Oletetaan, että  $a \in R$  on alkualkio ja  $a = bc$  jollain  $b, c \in R$ . Tällöin sekä  $b$  että  $c$  jakavat  $a$ :n. Toisaalta  $a$  jakaa triviaalisti tulon  $bc$ , joten koska  $a$  on alkualkio,  $a$  jakaa  $b$ :n tai  $c$ :n. Edellisessä tapauksessa  $a$  ja  $b$  ovat liittoalkioita, jolloin  $c$  on yksikkö. Jälkimmäisessä tapauksessa  $a$  ja  $c$  ovat liittoalkioita, ja  $b$  on yksikkö. Joka tapauksessa siis  $a$  on jaollinen vain yksiköillä ja omilla liittoalkioillaan.  $\square$

---

<sup>18</sup>Monet esiteltävistä käsitteistä voidaan määritellä myös renkaissa, mutta yksinkertaisuuden vuoksi tarkastellaan tässä yhteydessä vain kokonaisalueita.

Käänteinen väite ei päde: jaoton alkio ei välttämättä ole alkualkio, vaikka tämä onkin totta kokonaislukujen tapauksessa (Eukleideen lemmän nojalla). Esimerkiksi kompleksilukujen alirenkaassa  $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$  pätee

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Pienellä laskulla voidaan osoittaa, että luvut 2, 3 sekä  $1 \pm i\sqrt{5}$  ovat kaikki jaottomia. Esimerkiksi 2 kuitenkin jakaa tulon  $(1 + i\sqrt{5})(1 - i\sqrt{5})$ , muttei kumpaakaan sen tekijöistä, joten se ei ole alkualkio.

Lukujen suurin yhteinen tekijä määritellään myös tutulla tavalla.

**MÄÄRITELMÄ 11.5.** Olkoot  $a, b \in R \setminus \{0\}$ . Alkiota  $d \in R$  nimitetään alkioden  $a$  ja  $b$  *suurimmaksi yhteiseksi tekijäksi*, jos seuraavat ehdot pätevät:

- i)  $d|a$  ja  $d|b$ , eli  $d$  on  $a$ :n ja  $b$ :n yhteinen tekijä.
- ii) Jos  $c|a$  ja  $c|b$ , niin  $c|d$ .

Jos 1 on alkioden  $a$  ja  $b$  suurin yhteinen tekijä, sanotaan että  $a$  ja  $b$  ovat *jaottomia toistensa suhteen*.

Kaikissa kokonaisalueissa kahdella alkiolla ei välttämättä ole suurinta yhteistä tekijää. Lisäksi alkioden  $a$  ja  $b$  suurin yhteinen tekijä ei yleensä ole yksikäsitteinen, mistä syystä tuttu merkintä  $d = \text{syt}(a, b)$  ei periaatteessa ole käyttökelpoinen. Määritelmän ehdoista kuitenkin seuraa, että kaikki kahden alkion suurimmat yhteiset tekijät ovat toistensa liittoalkioita. Merkinnän  $d = \text{syt}(a, b)$  voidaankin tulkita tarkoittavan, että  $d$  on eräs alkioden  $a$  ja  $b$  suurin yhteinen tekijä, ja jokainen muu suurin yhteinen tekijä saadaan kertomalla alkiota  $d$  jollain yksiköllä. Erityisesti merkintä  $\text{syt}(a, b) = 1$  tarkoittaa tällöin, että jokainen suurin yhteinen tekijä on yksikkö.

Esimerkiksi kokonaislukujen renkaassa lukujen 30 ja 12 suurimpia yhteisiä tekijöitä ovat määritelmän mukaan luvut 6 ja  $-6$ . Positiivisista luvuista puhuttaessa kuitenkin yleensä määritellään, että luvun  $\text{syt}(m, n)$  on myös oltava positiivinen. Tällöin sanan “suurin” voidaan ajatella tarkoittavan myös suurinta kokonaislukujen tavallisen järjestyksen suhteen.

**11.2. Erilaiset jaollisuusalueet.** Kunnassa jaollisuuskysymykset ovat triviaaleja, koska jokainen nollasta poikkeava alkio on yksikkö ja siksi jokaisen alkion tekijä. Toisaalta yleisessä kokonaisalueessa ei välttämättä voida esimerkiksi löytää kahden alkion suurinta yhteistä tekijää tai kirjoittaa alkiota jaottomien alkioden tulona. Seuraavassa esitellään muutamia kokonaisalueiden tyyppejä, joissa on toinen toistaan paremmat jaollisuusominaisuudet. Todistuksia ei käsitellä, mutta ne löytyvät monista algebran perusoppikirjoista, esimerkkinä Nathan Jacobsonin *Lectures in Abstract Algebra I. Basic Concepts*.

**Tekijöihinjakorenkoot.** Kokonaisaluetta, jossa jokainen nollasta poikkeava alkio voidaan hajottaa yksikäsitteisellä tavalla jaottomien alkioden tuloksi, kutsutaan *tekijöihinjakorenkaksi*<sup>19</sup> (TJR) tai *faktoriaaliseksi renkaaksi*. Jaon on oltava

<sup>19</sup>englanniksi *unique factorisation domain* eli UFD

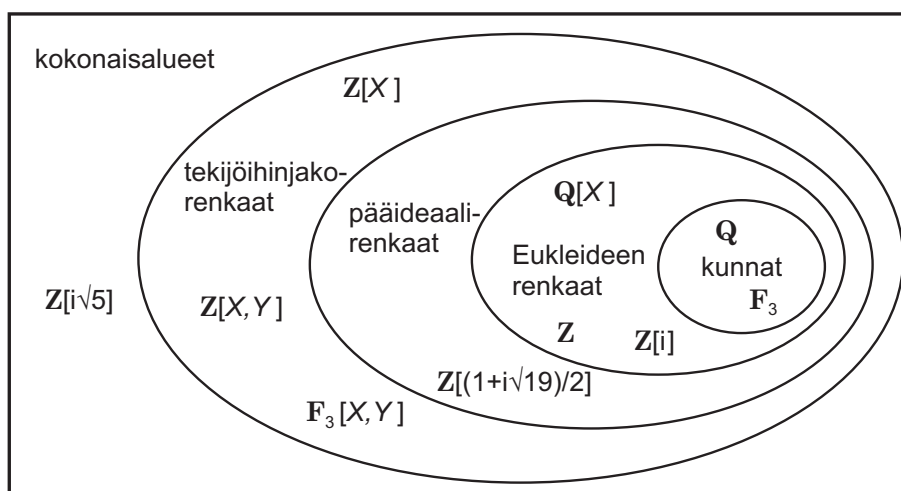
yksikäsitteinen sillä rajoituksella, että tekijöiden järjestyksellä ei ole väliä ja jokainen alkio voidaan korvata liittoalkiollaan. Kokonaislukujen rengas on TJR: esimerkiksi luvulla 60 on esitys  $2 \cdot 2 \cdot 3 \cdot 5$ , jota pidetään samana kuin jakoa  $-5 \cdot 2 \cdot 3 \cdot (-2)$ . Tekijöihinjakorengaassa jokainen jaoton alkio on alkualkio. Lisäksi kahden alkion suurin yhteinen tekijä on aina mahdollista löytää vertailemalla alkioiden tekijöihinjakoja. Hieman hankalampaa on osoittaa, että jos kokonaisalue  $R$  on TJR, niin myös polynomirengas  $R[X]$  on TJR. Tästä voidaan edelleen induktiolla päätellä, että rengas  $R[X_1, \dots, X_n]$  on TJR kaikilla  $n$ .

**Pääideaalirengaat.** Pääideaalirengaassa (PIR) jokainen ideaali on yhden alkion virittämä. Tästä seuraa, että minkä tahansa kahden alkion  $a$  ja  $b$  suurin yhteinen tekijä on olemassa ja se voidaan kirjoittaa muodossa  $xa + by$ . Lisäksi pääideaalirengaassa jokainen pääideaaleista muodostettu aidosti nouseva ketju  $\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots$  on äärellisen pituinen. Tämän ominaisuuden avulla voidaan osoittaa, että jokainen PIR on myös TJR. Kuitenkin esimerkiksi polynomirengas  $\mathbb{Z}[X]$  ei ole PIR vaikka onkin TJR.

**Eukleideen renkaat.** Eukleideen renkaaksi kutsutaan kokonaisaluetta  $R$ , jossa voidaan määritellä ns. *Eukleideen funktio*  $\varepsilon: R \rightarrow \mathbb{N}$ . Eukleideen funktion on toteutettava seuraava ehto:

Jos  $a, b \in R$  ja  $b \neq 0$ , niin löytyy sellaiset  $q, r \in R$ , että  $a = bq + r$  ja joko  $r = 0$  tai  $\varepsilon(r) < \varepsilon(b)$ .

Tämän määritelmän merkitys on siinä, että Eukleideen renkaassa on mahdollista käyttää Eukleideen algoritmia kahden alkion suurimman yhteisen tekijän löytämiseksi. Tästä seuraa, että jokainen Eukleideen rengas on PIR (vrt. lauseen 6.4 todistus). Kokonaisluvuilla voidaan määritellä Eukleideen funktio kaavalla  $\varepsilon(a) = |a|$ , ja jos  $K$  on kunta, niin polynomirengaassa  $K[X]$  Eukleideen funktion arvo saadaan polynomien asteesta. Tämä on myös polynomien jakoyhtälön perustana.



KUVA 21. Erilaisia jaollisuusalueita

**11.3. Polynomien jaottomuus.** Tarkastellaan nyt polynomien jaollisuuden liittyviä tuloksia, jotta voidaan todistaa muutama hyödyllinen jaottomuskriteeri. Kerroinrenkaan on aina oltava vähintään kokonaisalue, sillä tällöin ehto  $\deg(fg) \geq \deg(f)$  pätee kaikilla  $g \neq 0$ . Tämä ominaisuus on polynomien jaollisuusteorian perusta.

Aloitetaan todistamalla polynomien jakoyhtälö.

LAUSE 11.6 (Polynomien jakoyhtälö). *Olkoon  $K$  kunta, ja olkoot  $f, g \in K[X]$ . Oletetaan, että  $g \neq 0$ . Tällöin löytyy yksikäsitteiset polynomit  $q, r \in K[X]$ , joille pätee  $f = qg + r$  ja  $\deg(r) < \deg(g)$ .*

TODISTUS. Jakoyhtälö todistetaan samalla tavoin kuin kokonaisluvuilla. Tarkastellaan joukkoa

$$\mathcal{R} = \{f - qg \mid q \in K[X]\}.$$

Tämä joukko on selvästi epätyhjä. Olkoon  $r \in \mathcal{R}$  sellainen polynomi, jonka aste on pienin joukossa  $\mathcal{R}$ . Tällöin  $f - qg = r$  jollain  $q \in K[X]$ . Jos  $r = 0$ , väite pätee, sillä  $\deg(r) = -\infty < \deg(g)$ . Muussa tapauksessa merkitään  $r = \sum_{i=0}^n a_i X^i$  ja  $g = \sum_{i=0}^m b_i X^i$ , missä  $a_n \neq 0$  ja  $b_m \neq 0$ . Jos nyt  $\deg(r) \geq \deg(g)$ , niin määritellään  $q_1 = q + a_n b_m^{-1} X^{n-m}$ . Tällöin

$$f - q_1 g = r - a_n b_m^{-1} X^{n-m} g,$$

ja tämän polynomin aste on pienempi kuin  $n = \deg(r)$ , koska monomin  $X^n$  kerroin on 0. Toisaalta  $f - q_1 g$  on joukossa  $\mathcal{R}$ , mikä on ristiriita. Täten  $\deg(r) < \deg(g)$ .

Yksikäsitteisyyden osoittamiseksi oletetaan, että polynomit  $q_1, q_2, r_1$  ja  $r_2$  toteuttavat lauseen ehdot. Tällöin  $q_1 g + r_1 = q_2 g + r_2$ , josta edelleen saadaan  $(q_1 - q_2)g = r_1 - r_2$ . Jos  $q_1 \neq q_2$ , niin polynomin  $(q_1 - q_2)g$  aste on vähintään  $\deg(g)$ , joka on suurempi kuin  $\deg(r_1 - r_2)$ . Tämä on mahdotonta, joten  $q_1 = q_2$ , mistä seuraa, että  $r_1 = r_2$ .  $\square$

*Huom.* Todistuksessa tarvittiin vain kertoimen  $b_m$  kääntyvyyttä. Tulos pätee siksi missä tahansa kokonaisalueessa  $K$ , kunhan polynomin  $g$  korkeimman asteen kerroin on yksikkö.

Jakoyhtälön olemassaolo seuraa viime kädessä siitä, että yhden muuttujan polynomit muodostavat Eukleideen renkaan, jos kerroinrenkas on kunta. Jakoyhtälöstä seuraa, että kyseinen polynomirenkas on pääideaalirenkas, kuten aiemmin nähtiin. Tämän avulla voidaan edelleen osoittaa, että jokainen jaoton polynomi on "alkupolynomi", mistä puolestaan seuraa, että polynomirenkaassa on yksikäsitteinen tekijöihinjako.

LEMMA 11.7. *Olkoon  $K$  kunta ja  $f, g, h \in K[X]$ . Oletetaan, että  $f$  on jaoton ja  $f \mid (gh)$ . Tällöin  $f \mid g$  tai  $f \mid h$ .*

TODISTUS. Esimerkissä 6.10 on jakoyhtälön avulla näytetty, että  $\langle f \rangle$  on maksimaalinen ideaali. Tästä seuraa, että  $\langle f \rangle$  on alkuideaali. Ehto  $f \mid (gh)$  tarkoittaa, että  $gh \in \langle f \rangle$ . Tällöin joko  $g \in \langle f \rangle$  tai  $h \in \langle f \rangle$ , eli  $f \mid g$  tai  $f \mid h$ . (Myös suora todistus on mahdollinen.)  $\square$

LAUSE 11.8. *Jos  $K$  on kunta, polynomirenkas  $K[X]$  on tekijöihinjakorenkas.*

TODISTUS. Tämä todistus on jälleen samanlainen kuin kokonaisluvuilla. Oletetaan, että  $f \in K[X] \setminus \{0\}$  ei ole jaoton eikä yksikkö. Tällöin  $f = f_1 f_2$  joillain  $f_1, f_2 \in K[X]$ , joista kumpikaan ei ole yksikkö. Koska  $K$  on kunta, tästä seuraa, että  $f_1$  ja  $f_2$  eivät ole vakiopolynomeja, ja edelleen, että kummankin aste on aidosti pienempi kuin  $\deg(f)$ . Jos  $f_1$  tai  $f_2$  ei ole jaoton, jatketaan etsimällä jälleen epätriviaalit tekijät. Prosessi päättyy joskus, koska polynomin aste ei voi pienetä rajatta. Lopulta saadaan esitys  $f = f_1 f_2 \cdots f_r$ , missä jokainen  $f_i$  on jaoton.

Oletetaan sitten, että  $f = f_1 \cdots f_r = g_1 \cdots g_s$ , missä jokainen  $f_i$  ja  $g_i$  on jaoton. Nyt  $f_1$  jakaa tulon  $g_1 \cdots g_s$ , ja koska  $f_1$  on jaoton, seuraa edellisestä lemmasta, että  $f_1$  jakaa jonkin polynomeista  $g_i$ . Järjestystä vaihtamalla voidaan olettaa, että  $f_1 \mid g_1$ . Toisaalta  $g_1$  on jaoton, joten  $f_1$  ja  $g_1$  ovat liittoalkioita. Tästä seuraa, että  $f_2 \cdots f_r = u g_2 \cdots g_s$ , missä  $u$  on yksikkö. Induktion avulla voidaan päätellä, että  $r = s$  ja että  $f_i$  ja  $g_i$  ovat liittoalkioita kaikilla  $i$ .  $\square$

Todistuksessa käytettiin hyväksi sitä, että renkaassa  $K[X]$  jaottomat alkioit ovat myös alkualkioita. Tämä ominaisuus on jokaisella tekijöihinjakorengaalla.

LEMMA 11.9. *Tekijöihinjakorengaassa jokainen jaoton alkio on alkualkio.*

TODISTUS. Oletetaan, että  $p$  on jaoton alkio, joka jakaa tulon  $ab$ . Kirjoitetaan  $a$  ja  $b$  jaottomien alkioiden tulona muodossa  $a = a_1 a_2 \cdots a_r$  ja  $b = b_1 b_2 \cdots b_s$ . Nyt eräs tulon  $ab$  hajotelma jaottomiin tekijöihin on  $a_1 \cdots a_r b_1 \cdots b_s$ . Hajotelman yksikäsitteisyydestä seuraa, että  $p$  on jokin alkioista  $a_i$  tai  $b_i$  tai niiden liittoalkio. (Muuten on olemassa toinen hajotelma, joka koostuu  $p$ :stä ja luvun  $ab/p$  jaottomista tekijöistä.) Täten  $p \mid a$  tai  $p \mid b$ .  $\square$

Lopuksi osoitetaan joitakin käytännöllisiä jaottomuskriteerejä. Ensimmäinen on monelle tuttu lukiosta.

LAUSE 11.10 (Rationaalijuuritestit). *Olkoon  $R$  tekijöihinjakorengas, jonka osamääräkunta on  $K$ . Oletetaan, että polynomilla  $f = a_0 + \cdots + a_n X^n \in R[X]$  on juuri  $p/q \in K$ , missä  $\text{sy}(p, q) = 1$ . Tällöin  $p$  jakaa kertoimen  $a_0$ , ja  $q$  jakaa kertoimen  $a_n$ .*

TODISTUS. Kerrotaan yhtälö  $f(p/q) = 0$  puolittain luvulla  $q^n$ , jolloin saadaan

$$a_0 q^n + a_1 p q^{n-1} + a_2 p^2 q^{n-2} + \cdots + a_n p^n = 0.$$

Ottamalla  $p$  yhteiseksi tekijäksi ja siirtelemällä termejä saadaan

$$a_0 q^n = -p(a_1 q^{n-1} + a_2 p q^{n-2} + \cdots + a_n p^{n-1}).$$

Yllä olevasta yhtälöstä nähdään, että  $p$  jakaa tulon  $a_0 q^n$ . Koska  $R$  on tekijöihinjakorengas, alkio  $p$  voidaan esittää jaottomien alkioiden tulona, joista jokainen siis jakaa tulon  $a_0 q^n$ . Lemman 11.9 nojalla jokainen  $p$ :n jaoton tekijä on alkualkio, mutta oletuksen mukaan  $p$ :llä ei ole yhteisiä epätriviaaleja tekijöitä alkion  $q^n$  kanssa. Siispä jokainen  $p$ :n alkutekijä jakaa alkion  $a_0$ , mistä seuraa, että  $p \mid a_0$ .

Vastaavasti yhtälöstä

$$q(a_0 q^{n-1} + a_1 p q^{n-2} + \cdots + a_{n-1} p^{n-1}) = -a_n p^n$$

voidaan päätellä, että  $q \mid a_n$ .  $\square$

Rationaalijuuritesti soveltuu korkeintaan kolmatta astetta olevien polynomien jaottomuustestiksi, kuten seuraava esimerkki osoittaa.

ESIMERKKI 11.11. Tarkastellaan polynomia  $f = 3X^3 + 3X - 1 \in \mathbb{Z}[X]$ . Kyseinen polynomi ei ole jaollinen millään kokonaisluvulla, joten jos se ei ole jaoton, se on muotoa  $f = (aX + b)g$ , missä  $g \in \mathbb{Z}[X]$  on toisen asteen polynomi. Tällöin sillä on rationaalijuuri  $-b/a$ . Rationaalijuuritestin perusteella  $f$ :n rationaalijuuret ovat joukossa  $\{\pm 1, \pm 1/3\}$ . Mikään näistä luvuista ei kuitenkaan ole  $f$ :n juuri, joten  $f$  on jaoton.

Muita kriteerejä varten tarvitaan hieman aputuloksia. Seuraava yksinkertainen havainto on usein käyttökelpoinen, ja siksi se mainitaan tässä erikseen. Helppo todistus sivuutetaan.

LEMMA 11.12. *Olkkoon  $R$  rengas, ja olkkoon  $I$  renkaan  $R$  ideaali. Tällöin kuvaus  $R[X] \rightarrow (R/I)[X]$ , missä  $\sum_i a_i X^i \mapsto \sum_i (a_i + I)X^i$  on surjektiivinen rengashomomorfismi.*

Jatkossa merkitään polynomin  $f \in R[X]$  kuvaa yllä olevan lemman kuvauksessa  $\bar{f}$ . Polynomi  $\bar{f} \in (R/I)[X]$  saadaan siis korvaamalla  $f$ :n kertoimet sivuluokillaan. Tyypillisesti ideaali  $I$  valitaan alkuideaaliksi, jotta syntyvästä tekijärenkaasta tulisi kokonaisalue.

MÄÄRITELMÄ 11.13. *Olkkoon  $R$  tekijöihinjakorengas, ja olkkoon  $f \in R[X]$ . Jos polynomin  $f$  kertoimilla on suurimpana yhteisenä tekijänä 1, sanotaan että  $f$  on primitiivinen.*

Primitiivisyyden käsitettä tarvitaan erottelemaan sellaiset jaolliset polynomit, jotka ovat jaollisia jollain yksiköstä poikkeavalla vakiolla. Esimerkiksi ei-primitiivinen polynomi  $2X + 2$  jakautuu epätriviaaleihin tekijöihin renkaassa  $\mathbb{Z}[X]$ , mutta on jaoton renkaassa  $\mathbb{Q}[X]$ , koska jälkimmäisessä tekijä 2 on yksikkö.

LEMMA 11.14. *Olkkoon  $R$  tekijöihinjakorengas, ja olkkoot  $f, g \in R[X]$ . Jos  $f$  ja  $g$  ovat primitiivisiä, niin  $fg$  on primitiivinen.*

TODISTUS. Oletetaan vastoin väitettä, että  $f$  ja  $g$  ovat primitiivisiä mutta  $fg$  ei ole. Tällöin löytyy jokin alkio  $p \in R$ , joka jakaa kaikki tulopolynomin  $fg$  kertoimet eikä ole yksikkö. Koska  $R$  on TJR, voidaan olettaa, että  $p$  on alkualkio. Nyt tekijärenkas  $R/\langle p \rangle$  on kokonaisalue, mistä seuraa, että myös  $R/\langle p \rangle[X]$  on kokonaisalue.

Olkkoot  $\bar{f}, \bar{g} \in R/\langle p \rangle[X]$  ne polynomit, jotka saadaan polynomeista  $f$  ja  $g$  vaihtamalla kertoimet sivuluokkiinsa ideaalin  $\langle p \rangle$  suhteen (vrt. lemma 11.12). Koska  $f$  ja  $g$  ovat primitiivisiä, alkio  $p$  ei jaa kummankaan kaikkia kertoimia. Tästä nähdään, että  $\bar{f} \neq 0$  ja  $\bar{g} \neq 0$ . Koska  $R/\langle p \rangle[X]$  on kokonaisalue, niin  $\overline{fg} = \bar{f} \cdot \bar{g} \neq 0$ . Tämä taas tarkoittaa sitä, että  $p$  ei jaa kaikkia tulon  $fg$  kertoimia, mikä on ristiriita. Siispä  $fg$  on primitiivinen.  $\square$

LAUSE 11.15 (Gaussin lemma<sup>20</sup>). *Olkkoon  $R$  tekijöihinjakorengas, jonka osamääräkunta on  $K$ . Tällöin  $f \in R[X]$  on jaoton, jos ja vain jos  $f$  on primitiivinen ja jaoton renkaassa  $K[X]$ .*

<sup>20</sup>Myös lemmaa 11.14 nimitetään toisinaan Gaussin lemmäksi.

TODISTUS. Oletetaan ensin, että  $f$  on primitiivinen ja jaoton renkaassa  $K[X]$ . Jos  $f$  ei ole jaoton renkaassa  $R[X]$ , niin  $f = gh$  joillain  $g, h \in R[X]$ , missä  $g$  ja  $h$  eivät kumpikaan ole yksiköitä renkaassa  $R[X]$ . Kuitenkin, koska  $f$  on jaoton renkaassa  $K[X]$ , joko  $g$  tai  $h$  on vakio. Tämä vakio jakaa kaikki polynomin  $gh = f$  kertoimet, mikä on mahdotonta, koska  $f$  on primitiivinen. Täten  $f$  on jaoton renkaassa  $R[X]$ .

Oletetaan sitten, että  $f$  on jaoton renkaassa  $R[X]$ . Se voidaan kuitenkin kirjoittaa muodossa  $f = cf_1$ , missä  $c$  on  $f$ :n kertoimien suurin yhteinen tekijä ja  $f_1$  on primitiivinen. Jaottomuudesta seuraa nyt, että  $c$  on yksikkö  $R[X]$ :ssä, joten myös  $f$  on primitiivinen.

Tehdään vastaoletus, että  $f$  ei ole jaoton renkaassa  $K[X]$ . Tällöin  $f = gh$  joillain  $g, h \in K[X]$ , missä  $g$  ja  $h$  eivät kumpikaan ole vakioita. Laventamalla tulo  $gh$  kertoimet samannimisiksi, kyseinen tulo voidaan kirjoittaa muodossa  $gh = a/b \cdot g_1h_1$ , missä  $g_1, h_1 \in R[X]$  ovat primitiivisiä ja  $a, b \in R$  ovat jaottomia toistensa suhteen. Tällöin  $bf = ag_1h_1$ . Edellisen lemmän perusteella tulo  $g_1h_1$  on primitiivinen. Nyt  $b$  on polynomin  $bf$  kertoimien suurin yhteinen tekijä (koska  $f$  on primitiivinen), ja  $a$  on polynomin  $ag_1h_1$  kertoimien suurin yhteinen tekijä, joten  $b$  ja  $a$  ovat liittoalkioita. Koska  $\text{sy}(a, b) = 1$ , tämä on mahdotonta, elleivät  $a$  ja  $b$  ole  $R$ :n yksiköitä. Viimeksi mainitussa tapauksessa voidaan kuitenkin kirjoittaa  $f = (ag_1)(b^{-1}h_1)$ , jolloin  $f$  ei olekaan jaoton renkaassa  $R[X]$ . Tämä on ristiriita, joten  $f$  on jaoton renkaassa  $K[X]$ .  $\square$

LAUSE 11.16 (Eisensteinin kriteeri). *Olkoon  $R$  tekijöihinjakorengas, jonka osamääräkunta on  $K$ , ja olkoon  $f = a_0 + \dots + a_nX^n \in R[X]$ . Polynomi  $f$  on jaoton renkaassa  $K[X]$ , jos jompikumpi seuraavista ehdoista on voimassa:*

- a) *Jokin alkualkio  $p \in R$  jakaa kertoimet  $a_0, \dots, a_{n-1}$  mutta ei kerrointa  $a_n$ , ja  $p^2$  ei jaa kerrointa  $a_0$ .*
- b) *Jokin alkualkio  $p \in R$  jakaa kertoimet  $a_1, \dots, a_n$  mutta ei kerrointa  $a_0$ , ja  $p^2$  ei jaa kerrointa  $a_n$ .*

TODISTUS. Oletetaan, että ehto a) pätee. Voidaan olettaa, että  $f$  on primitiivinen. (Muuten jaetaan  $f$  kertoimiensa suurimmalla yhteisellä tekijällä, mikä ei vaikuta jaottomuuteen kunnan  $K$  suhteen.) Olkoon  $\bar{f}$  se renkaan  $R/\langle p \rangle[X]$  polynomi, joka saadaan  $f$ :stä muuttamalla kertoimet sivuluokikseen ideaalin  $\langle p \rangle$  suhteen (ks. lemma 11.12). Ehdon a) perusteella pätee  $\bar{f} = \bar{a}_nX^n$ . Oletetaan, että  $f$  ei ole jaoton renkaassa  $K[X]$ . Gaussin lemmän perusteella  $f = gh$ , missä  $g, h \in R[X]$ . Koska  $f$  on primitiivinen, kumpikaan  $g$ :stä ja  $h$ :sta ei ole vakio. Nyt  $\bar{g} \cdot \bar{h} = \bar{f} = \bar{a}_nX^n$ , mistä seuraa, että sekä  $\bar{g}$  että  $\bar{h}$  ovat muotoa  $cX^i$ . Jos kumpikaan polynomeista  $\bar{g}$  ja  $\bar{h}$  ei ole vakio, niin  $p$  jakaa polynomien  $g$  ja  $h$  vakiotermit. Tällöin kuitenkin  $p^2$  jakaa  $a_0$ :n, mikä on vastoin oletusta. Siispä voidaan olettaa, että esimerkiksi  $\bar{g}$  on vakio. Kuitenkaan  $g$  ei ole vakio, joten  $p$  jakaa  $g$ :n korkeimman asteen kertoimen. Tällöin  $p$  jakaa myös kertoimen  $a_n$ , mikä on jälleen vastoin oletusta. Polynomi  $f$  on siis jaoton renkaassa  $K[X]$ . Ehdon b) tapaus todistetaan samalla tavalla.  $\square$

ESIMERKKI 11.17. Polynomi  $X^5 - 12X^3 + 2X + 2$  nähdään jaottomaksi renkaassa  $\mathbb{Q}[x]$ , kun valitaan Eisensteinin kriteerissä  $p = 2$ . Aikaisemman esimerkin

polynomi  $3X^3 + 3X - 1$  on myös jaoton, mikä huomataan valitsemalla  $p = 3$ . Sen sijaan esimerkiksi polynomista  $X^4 + 2X + 4$  Eisensteinin kriteeri ei sano mitään.

LAUSE 11.18. *Olkoon  $R$  tekijöihinjakorengas, jonka osamääräkunta on  $K$ , ja olkoon  $f \in R[X]$ . Oletetaan, että  $p \in R$  on alkuaikio, joka ei jaa  $f$ :n korkeimman asteen termin kerrointa. Jos  $\bar{f}$  on jaoton renkaassa  $R/\langle p \rangle[X]$ , niin  $f$  on jaoton renkaassa  $K[X]$ .*

TODISTUS. Voidaan jälleen olettaa, että  $f$  on primitiivinen. Jos  $f$  ei ole jaoton renkaassa  $K[X]$ , niin Gaussin lemmän mukaan se jakautuu tekijöihin myös renkaassa  $R[X]$ . Jos  $f = gh$ , missä  $g, h \in R[X]$ , niin  $\bar{f} = \bar{g} \cdot \bar{h}$  lemmän 11.12 perusteella. Lisäksi kumpikaan  $g$ :stä ja  $h$ :sta ei ole vakio, koska  $f$  on primitiivinen. Jos  $\bar{f}$  on jaoton, niin  $\bar{g}$  tai  $\bar{h}$  on yksikkö kokonaisalueessa  $R/\langle p \rangle[X]$ . Polynomirenkaan yksiköt ovat vakioita, joten koska  $g$  ja  $h$  eivät ole vakioita,  $p$  jakaa joko  $g$ :n tai  $h$ :n korkeimman asteen kertoimen. Tämä on mahdotonta, koska  $f$ :n korkeimman asteen kerroin ei ole jaollinen  $p$ :llä. Näin ollen  $f$  on jaoton renkaassa  $K[X]$ .  $\square$

Yllä oleva lause ei päde käänteisessä muodossa: esimerkiksi  $X^3 + X + 1 \in \mathbb{Z}[X]$  on jaoton, mutta renkaassa  $\mathbb{F}_3[X]$  se jakautuu tuloksi  $(X - 1)(X^2 + X - 1)$ .

ESIMERKKI 11.19. Tarkastellaan polynomia  $f = 7X^4 - X^3 + 2X + 3 \in \mathbb{Z}[X]$ . Kirjoittamalla kertoimet modulo 2, saadaan polynomi  $\bar{f} = X^4 + X^3 + 1 \in \mathbb{F}_2[X]$ . Koska polynomilla  $\bar{f}$  ei ole juuria, sillä ei ole myöskään ensimmäisen asteen tekijöitä.

Oletetaan, että  $f = (X^2 + aX + b)(X^2 + cX + d)$  joillain  $a, b, c, d \in \mathbb{F}_2$ . Kerromalla tulo auki ja vertailemalla kertoimia nähdään, että

$$a + c = 1, \quad ac + b + d = 0, \quad ad + bc = 0 \quad \text{ja} \quad bd = 1.$$

Ensimmäisestä ehdosta seuraa, että täsmälleen yksi luvuista  $a$  ja  $c$  on nolla. Viimeisestä ehdosta nähdään, että  $b = d = 1$ . Tällöin kuitenkin  $ad + bc = 1$ , mikä on ristiriita. Siispä  $\bar{f}$  on jaoton, joten myös  $f$  on jaoton kunnan  $\mathbb{Q}$  suhteen. Samalla vaivalla on myös osoitettu, että mikä hyvänsä neljännen asteen polynomi  $\sum_{i=0}^4 a_i X^i$  on jaoton  $\mathbb{Q}$ :n suhteen, kunhan kertoimista  $a_0, a_3$  ja  $a_4$  ovat parittomia ja muut parillisia.