11. Jaollisuudesta

Kuntalaajennosten yhteydessään käytetään usein apuna jaottomia polynomeja. Tarkastellaan seuraavaksi hieman jaollisuuskäsitettä yleensä ja todistetaan joitain kriteerejä erityisesti polynomien jaottomuudelle.

11.1. Jaollisuus kokonaisalueissa. Olkoon R kokonaisalue[16]. Jaollisuuteen liittyvät käsitteet määritellään R:ssä samalla tavoin kuin kokonaisluvuilla. 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*. Kääntyviä alkioita kutsutaan *yksiköiksi*, ja ne jakavat kaikki R:n alkiot, sillä jos a on yksikkö, niin $b = a(a^{-1}b)$. Seuraavan lemman helppo todistus jätetään harjoitustehtäväksi.

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

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

Koska jokainen alkio on jaollinen kaikilla yksiköillä sekä omilla liittoalkioillaan, niitä voidaan pitää alkion *triviaaleina tekijöinä*. Yleisessä kokonaisalueessa voi olla kahdentyyppisiä jaottomia alkioita. Koska nolla-alkio on joka tapauksessa jaollinen kaikilla alkioilla, se jätetään 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, niin a jakaa jomman kumman alkioista b ja c.

Kokonaislukujen renkaassa $\mathbb{Z}$ on vain kaksi yksikköä: 1 ja -1. Luvun $n \in \mathbb{Z}$ liittoalkioita on siis samoin kaksi: n ja $-n$. Kokonaisluku p on jaoton, jos ja vain jos se on jonkin alkuluvun liittoalkio, sillä tällöin p:llä on tekijöinä vain luvut 1, -1, p ja $-p$, jotka ovat kaikki joko yksiköitä tai p:n liittoalkioita.

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

TODISTUS. Oletetaan, että $a \in R$ on alkualkio ja $a = bc$ joillain $b, c \in R$. 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. □

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

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

[16] Monet esiteltävistä käsitteistä voidaan määritellä myös renkaissa, mutta yksinkertaisuuden vuoksi tarkastellaan tässä yhteydessä vain kokonaisalueita.

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 alkuluku.

Lukujen suurin yhteinen tekijä määritellään myös tutulla tavalla.

MÄÄRITELMÄ 11.5. Olkoot $a, b \in R$. Alkiota $d \in R$ nimitetään alkioiden 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 $d|c$.

Jos 1 on alkioiden 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 alkioiden a ja b suurin yhteinen tekijä ei yleensä ole yksikäsitteinen, mistä syystä tuttu merkintä $d = \operatorname{syt}(a,b)$ ei periaatteessa ole käyttökelpoinen. Määritelmän ehdoista kuitenkin seuraa, että kaikki kahden alkion suurimmat yhteiset tekijät ovat toistensa liittoalkioita. Merkinnän $d = \operatorname{syt}(a,b)$ voidaankin ajatella tarkoittavan, että d on eräs alkioiden a ja b suurin yhteinen tekijä, ja jokainen muu suurin yhteinen tekijä saadaan kertomalla alkiota d jollain yksiköllä. Erityisesti merkintä $\operatorname{syt}(a,b) = 1$ tarkoittaa tällöin, että jokainen suurin yhteinen tekijä on yksikkö.

Esimerkiksi renkaassa $\mathbb{Z}$ lukujen 30 ja 12 suurimpia yhteisiä tekijöitä ovat määritelmän mukaan luvut 6 ja -6. Positiivisista luvuista puhuttaessa kuitenkin yleensä määritellään, että luvun $\operatorname{syt}(m,n)$ 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 alkioiden 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.*

Tekijöihinjakorenkaat. Kokonaisaluetta, jossa jokainen nollasta poikkeava alkio voidaan hajottaa yksikäsitteisellä tavalla jaottomien alkioiden tuloksi, kutsutaan *tekijöihinjakorenkaaksi*[17] (TJR) tai *faktoriaaliseksi renkaaksi.* Jaon on oltava yksikäsitteinen sillä rajoituksella, että tekijöiden järjestyksellä ei ole väliä ja jokainen alkio voidaan korvata liittoalkiollaan. Kokonaislukujen rengas on TJR: esimerkiksi $60 = 2 \cdot 2 \cdot 3 \cdot 5$; tätä jakoa pidetään samana kuin $60 = -5 \cdot 2 \cdot 3 \cdot (-2)$. Tekijöihinjakorenkaassa jokainen jaoton alkio on alkualkio. Lisäksi kahden alkion

[17] englanniksi *unique factorisation domain* eli UFD

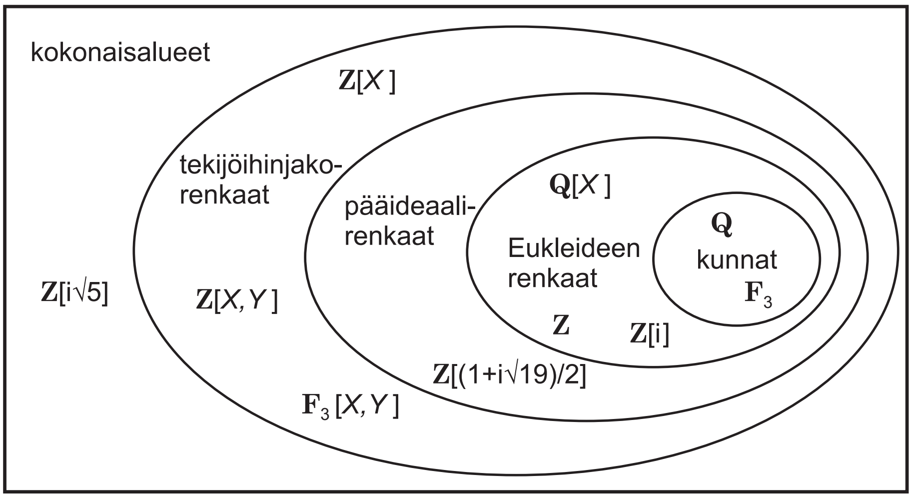
suurin yhteinen tekijä on aina mahdollista löytää vertailemalla alkioiden tekijöihinjakoja. Hieman hankalampaa on osoittaa, että jos R on TJR, niin myös polynomirengas $R[X]$ on TJR. Tästä voidaan edelleen induktiolla päätellä, että rengas $R[X_1, \dots, X_n]$ on TJR kaikilla n.

Pääideaalirenkaat. Pääideaalirenkaassa (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 pääideaalirenkaassa jokainen pääideaaleista muodostettu aidosti nouseva ketju $\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$ on äärellisen pituinen. Tämän ominaisuuden avulla voidaan osoittaa, että jokainen PIR on myös TJR. Kuitenkaan esimerkiksi polynomirengas $\mathbb{Z}[X]$ ei ole PIR vaikka onkin TJR.

Eukleideen renkaat. Eukleideen renkaaksi kutsutaan kokonaisaluetta R, jossa voidaan määritellä ns. *Eukleideen funktio* $\varepsilon : R \to \mathbb{N}$. 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 6.3 todistus). Kokonaisluvuilla voidaan määritellä Eukleideen funktio kaavalla $\varepsilon(a) = |a|$, ja jos K on kunta, niin polynomirenkaassa $K[X]$ Eukleideen funktion arvo saadaan polynomin asteesta. Tämä on myös polynomien jakoyhtälön perustana.



Kuva 22. Erilaisia jaollisuusalueita

11.3. Polynomien jaottomuus. Tarkastellaan nyt polynomien jaollisuuteen liittyviä tuloksia, jotta voidaan todistaa muutama hyödyllinen jaottomuuskriteeri. Aloitetaan kirjoittamalla virallisesti ylös polynomien jakoyhtälö, jota on jo käytetty monissa todistuksissa.

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

TODISTUS. Jakoyhtälö osoitetaan 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 $r_1 = r_2$. □

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 osoittaa, että yhden muuttujan polynomit muodostavat Eukleideen renkaan, jos kerroinrengas on kunta. Tämän avulla voidaan helposti osoittaa, että polynomirenkaassa on yksikäsitteinen tekijöihinjako. Seuraavaa lemmaa on jo käytetty muun muassa luvussa 10, kun konstruoitiin kunnan $\mathbb{F}_p$ laajennos jaottoman polynomin avulla.

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

TODISTUS. Harjoitustehtävä. □

LAUSE 11.8. *Jos K on kunta, polynomirengas $K[X]$ on tekijöihinjakorengas.*

TODISTUS. Tämä todistus on jälleen samanlainen kuin kokonaisluvuilla. Oletetaan, että $f \in K[X]$ ei ole jaoton. 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

$f_2 \cdots f_r = ug_2 \cdots g_s$, missä u on yksikkö. Induktion avulla voidaan päätellä, että $r = s$ ja että f_i ja g_i ovat liittoalkioita kaikilla i. □

Osoitetaan tässä välissä eräs hyödyllinen tekijöihinjakorenkaan ominaisuus.

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

TODISTUS. Oletetaan, että p on jaoton alkio, joka jakaa tulon ab. Kirjoitetaan a ja b jaottomien alkioiden tulona muodossa $a = a_1a_2 \cdots a_r$ ja $b = b_1b_2 \cdots b_s$. Koska p on tulon ab jaoton tekijä, sen täytyy olla mukana tulon ab hajotelmassa jaottomiin tekijöihin. Eräs tällainen hajotelma on $a_1 \cdots a_r b_1 \cdots b_s$. Hajotelman yksikäsitteisyydestä seuraa nyt, että p on jokin alkioista a_i tai b_i tai niiden liittoalkio. Täten $p|a$ tai $p|b$. □

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

LAUSE 11.10 (Rationaalijuuritesti). *Olkoon R tekijöihinjakorengas, jonka osamääräkunta on K. Oletetaan, että polynomilla $f = a_0 + \cdots + a_nX^n \in R[X]$ on juuri $p/q \in K$, missä* $\mathrm{syt}(p, q) = 1$. *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

$$a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_np^n = 0.$$

Ottamalla p yhteiseksi tekijäksi ja siirtelemällä termejä saadaan

$$a_0q^n = -p(a_1q^{n-1} + a_2pq^{n-2} + \cdots + a_np^{n-1}).$$

Yllä olevasta yhtälöstä nähdään, että p jakaa tulon a_0q^n. Lemman 11.9 mukaan p on alkualkio, joten p jakaa a_0:n tai q^n:n. Oletuksen mukaan p:llä ei ole yhteisiä epätriviaaleja tekijöitä alkion q^n kanssa, joten $p|a_0$. Vastaavasti yhtälöstä

$$q(a_0q^{n-1} + a_1pq^{n-2} + \cdots + a_{n-1}p^{n-1}) = -a_np^n$$

nähdään, että $q|a_n$. □

Rationaalijuuritesti soveltuu korkeintaan kolmannen asteen polynomien jaottomuustestiksi, kuten seuraava esimerkki osoittaa.

ESIMERKKI 11.11. Tarkastellaan polynomia $f = 3X^3 + 3X - 1 \in \mathbb{Z}[X]$. Jos se ei ole jaoton, se on muotoa $f = (aX + b)g$, missä $g \in \mathbb{Z}[X]$ on toisen asteen polynomi. Tällöin f:llä 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. *Olkoon R rengas, ja olkoon I renkaan R ideaali. Tällöin kuvaus $R[X] \to (R/I)[X]$, missä $\sum_i a_iX^i \mapsto \sum_i (a_i + I)X^i$ on surjektiivinen rengashomomorfismi.*

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

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

LEMMA 11.14. *Olkoon R tekijöihinjakorengas, ja olkoot $f, g \in R[X]$. 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 jaoton alkio $p \in R$, joka jakaa kaikki tulopolynomin fg kertoimet. Koska R on TJR, tiedetään, että p on alkualkio. Täten tekijärengas $R/\langle p \rangle$ on kokonaisalue, mistä seuraa, että myös $R/\langle p \rangle[X]$ on kokonaisalue.

Olkoot $\overline{f}, \overline{g} \in R/\langle p \rangle[X]$ 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 niiden kaikkia kertoimia. Tästä nähdään, että $\overline{f} \neq 0$ ja $\overline{g} \neq 0$. Koska $R/\langle p \rangle[X]$ on kokonaisalue, niin $\overline{fg} = \overline{f} \cdot \overline{g} \neq 0$. 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[18]). *Olkoon R tekijöihinjakorengas, jonka osamääräkunta on K. Tällöin $f \in R[X]$ on jaoton, jos ja vain jos f on primitiivinen ja jaoton renkaassa $K[X]$.*

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. Koska f on jaoton $K[X]$:ssä, niin joko g tai h on vakio. Tämä vakio kuitenkin 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 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 tulon gh kertoimet samannimisiksi, kyseinen tulo voidaan kirjoittaa muodossa $gh = a/b \cdot g_1 h_1$, missä $g_1, h_1 \in R[X]$ ovat primitiivisiä ja $a, b \in R$ ovat jaottomia toistensa suhteen. Tällöin $bf = ag_1 h_1$. Edellisen lemman perusteella tulo $g_1 h_1$ on primitiivinen. Nyt b on polynomin bf kertoimien suurin yhteinen tekijä, ja a on polynomin $ag_1 h_1$ kertoimien suurin yhteinen tekijä, joten b ja a ovat liittoalkioita. Koska $\operatorname{syt}(a, b) = 1$, tämä on mahdotonta, elleivät a ja b ole R:n yksiköitä. Viimeksi mainitussa tapauksessa voidaan kirjoittaa $f = (ag_1)(b^{-1} h_1)$, jolloin f ei olekaan jaoton renkaassa $R[X]$. Tämä on ristiriita, joten f on jaoton renkaassa $K[X]$. $\square$

[18]Myös lemmaa 11.14 nimitetään toisinaan Gaussin lemmaksi.

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

a) *Jokin alkualkio $p \in R$ jakaa kertoimet $a_0, \ldots, a_{n-1}$ mutta ei kerrointa a_n, ja p^2 ei jaa kerrointa a_0.*
b) *Jokin alkualkio $p \in R$ jakaa kertoimet $a_1, \ldots, a_n$ 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 $\overline{f}$ 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 $\overline{f} = \overline{a}_n X^n \neq 0$. Oletetaan, että f ei ole jaoton renkaassa $K[X]$. Gaussin lemman perusteella $f = gh$, missä $g, h \in R[X]$. Koska f on primitiivinen, kumpikaan g:stä ja h:sta ei ole vakio. Nyt $\overline{g} \cdot \overline{h} = \overline{f} = \overline{a}_n X^n$, mistä seuraa, että sekä $\overline{g}$ että $\overline{h}$ ovat muotoa cX^i. Jos kumpikaan polynomeista $\overline{g}$ ja $\overline{h}$ 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 $\overline{g}$ 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. □

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 $f \in R[X]$ primitiivinen polynomi. Oletetaan, että $p \in R$ on alkualkio, joka ei jaa f:n korkeimman asteen termin kerrointa. Jos $\overline{f}$ on jaoton renkaassa $R/\langle p\rangle[X]$, niin f on jaoton renkaassa $K[X]$.*

Todistus. Jos f ei ole jaoton renkaassa $K[X]$, niin Gaussin lemman mukaan se jakautuu tekijöihin myös renkaassa $R[X]$. Jos $f = gh$, missä $g, h \in R[X]$, niin $\overline{f} = \overline{g} \cdot \overline{h}$ lemman 11.12 perusteella. Lisäksi kumpikaan g:stä ja h:sta ei ole vakio, koska f on primitiivinen. Jos $\overline{f}$ on jaoton, niin $\overline{g}$ tai $\overline{h}$ 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 $K[X]$. □

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 $f = 3 + 2X - X^3 + 7X^4 \in \mathbb{Z}[X]$. Kirjoittamalla kertoimet modulo 2, saadaan polynomi $\overline{f} = 1 + X^3 + X^4 \in \mathbb{F}_2[X]$. Oletetaan, että $f = (X^2 + aX + b)(X^2 + cX + d)$ joillain $a, b, c, d \in \mathbb{F}_2$. Kertomalla 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 $\overline{f}$ 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.