III Kuntateoriaa

Luonnollisiin kieliin on jo hyvin varhaisessa vaiheessa sisälletytty ilmaisuja, jotka viittaavat positiivisiin kokonaislukuihin. Käytännössä ei myöskään tulla toimeen ilman murtolukuja, ja kieleen ovat muodostuneet esimerkiksi ilmaisut 'puoli' ja 'kolmannes'. Matemaattiselta kannalta katsoen tämä tarkoittaa, että kokonaislukujen rengas $(\mathbb{Z}, +, \cdot)$ on käytännön tarpeisiin riittämätön, koska ensimmäisen asteen yhtälöllä $mx = n$ ei aina ole ratkaisua, kun $m, n \in \mathbb{Z}$, vaikka pätisi $n \neq 0$.

Yleisemmin nousee esille seuraava kysymys, kun työskennellään renkaassa $\boldsymbol{R} = (R, +, \cdot)$: Koska ensimmäisen asteen yhtälöllä $ax + b = c$, missä $a, b, c \in R$, $a \neq 0$, ei välttämättä ole ratkaisua, olisiko $\boldsymbol{R}$ mahdollista laajentaa kunnaksi $\boldsymbol{K}$? Eräässä tilanteessa tämä osoittautuu mahdolliseksi, ja syntyvää minimaalista laajennusta kunnaksi nimitetään renkaan $\boldsymbol{R}$ jakokunnaksi, mitä käsitellään ensimmäisessä aliluvussa.

Kunnassa jokaisella ensimmäisen asteen yhtälöllä on ratkaisu. Voidaan ryhtyä ahneiksi ja ruveta etsimään kunnalle laajennusta, jossa kaikilla polynomiyhtälöillä on ratkaisu; tällaista kuntaa kutsutaan alkuperäisen kunnan algebralliseksi sulkeumaksi. Tässä luvussa ei kuitenkaan esitetä algebrallisen sulkeuman konstruktiota, vaan algebran tutkimus on osoittanut, että on hedelmällistä tarkastella vaatimattomampia kuntalaajennuksia, joissa on lähtökuntaan liitetään jonkin yksittäisen polynomiyhtälön ratkaisu. Näitä tarkastellaan luvun loppupuolella.

1. Jakokunta

Kunnan alirenkaat ovat aina kokonaisalueita. Tämä herättää luonnollisen kysymyksen, karakterisoiko tämä ominaisuus kokonaisalueet eli onko jokainen kokonaisalue jonkin kunnan alirengas. Vastaus on myönteinen.

1.1. Lause. *Jokaista kokonaisaluetta* $\boldsymbol{R} = (R, +, \cdot)$ *vastaa sellainen kunta* $K = (K, +, \cdot)$*, että* $\boldsymbol{R}$ *on kunnan* $\boldsymbol{K}$ *alirengas ja jokainen* $t \in K$ *voidaan esittää muodossa* $t = ab^{-1}$*, missä* $a, b \in R$*,* $b \neq 0$*.*

Todistus. Todistuksen idea on yksinkertainen: Koska halutaan konstruoida kunta $\boldsymbol{K}$, jolla on $\boldsymbol{R}$ alirenkaanaan, niin tässä kunnassa täytyy tietenkin olla alkio ab^{-1} jokaista alkioparia (a, b) kohti, missä $a, b \in R$, $b \neq 0$. Toisaalta jos $a, b, c, d \in R$, $b, d \neq 0$, niin kunnassa $\boldsymbol{K}$ täytyy olla voimassa

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

ts. normaali murtolausekkeiden yhteenlaskumenetelmä pätee. Kunnan tulee siis olla konstruoitavissa edellisten kaltaisten parien (a, b) kautta. Toisaalta, kuten lavennussäännöistä tiedetään, niin jokaisella $r \in R \setminus \{0\}$ pätee $(ra)(rb)^{-1} = ab^{-1}$, kun $a, b \in R$, $b \neq 0$. Siis samaa kunnan alkiota vastaa yleisesti ottaen moni renkaan pari (a, b). Todistus tulee olemaan siten kaksivaiheinen: Ensin konstruoidaan yo. pareista apurakenne, joka ei toteuta aivan kaikkia kunta-aksioomia. Sitten samastetaan pareja lavennussäännön mukaisesti, ja konstruktio on valmis. Suunnitelma ei ole monimutkainen, mutta tekninen toteutus sisältää lukuisia vaiheita.

Varustetaan näin ollen joukko $R \times (R \setminus \{0\})$ sopivilla yhteen- ja kertolaskuilla: kun $a, b, c, d \in R$ ja $b, d \neq 0$, niin

$$(a, b) + (c, d) = (ad + bc, bd) \quad \text{ja}$$
$$(a, b) \cdot (c, d) = (ac, bd).$$

Huomattakoon, että tulon nollasäännön nojalla $bd \neq 0$. Tarkastellaan rakennetta $(R \times (R \setminus \{0\}), +, \cdot)$ ja sen perusjoukon relaatiota

$$(a, b) \sim (c, d) \iff ad = bc.$$

Olkoot $a, b, c, d, e, f \in R$, $b, d, f \neq 0$. Laskutoimitukset ovat liitännäisiä ja vaihdannaisia renkaan $\boldsymbol{R}$ vastaavien laskulakien perusteella, sillä

$$\begin{aligned}
\big((a, b) + (c, d)\big) + (e, f) &= (ad + bc, bd) + (e, f) \\
&= ((ad + bc)f + (bd)e, (bd)f) \\
&= (a(df) + b(cf + de), b(df)) \\
&= (a, b) + (cf + de, df) \\
&= (a, b) + \big((c, d) + (e, f)\big), \\
\big((a, b) \cdot (c, d)\big) \cdot (e, f) &= (ac, bd) \cdot (e, f) = ((ac)e, (bd)f) \\
&= (a(ce), b(df)) = (a, b) \cdot (ce, df) \\
&= (a, b) \cdot \big((c, d) \cdot (e, f)\big), \\
(a, b) + (c, d) &= (ad + bc, bd) = (cb + da, db) \\
&= (c, d) + (a, b)
\end{aligned}$$

ja

$$(a, b) \cdot (c, d) = (ac, bd) = (ca, db) = (c, d) \cdot (a, b).$$

Yhteenlaskulla on neutraalialkio $(0, 1)$, sillä

$$(a, b) + (0, 1) = (a \cdot 1 + b \cdot 0, b \cdot 1) = (a, b) = (0 \cdot b + 1 \cdot a, 1 \cdot b) = (0, 1) + (a, b).$$

Kertolaskun neutraalialkio on vastaavasti $(1, 1)$, sillä

$$(a, b) \cdot (1, 1) = (a \cdot 1, b \cdot 1) = (a, b) = (1 \cdot a, 1 \cdot b) = (1, 1) \cdot (a, b).$$

Siis $(R \times (R \setminus \{0\}), +)$ ja $(R \times (R \setminus \{0\}), \cdot)$ ovat vaihdannaisia monoideja, eivät kuitenkaan välttämättä Abelin ryhmiä.

Osoitetaan seuraavaksi, että $\sim$ on kongruenssi molempien laskutoimitusten suhteen. Kun $a, b, c, d, e, f \in R$, $b, d, f \neq 0$, niin

1) $(a, b) \sim (a, b)$, sillä $ab = ba$,
2) Jos $(a, b) \sim (c, d)$ eli $ad = bc$, niin $cb = bc = ad = da$, joten $(c, d) \sim (a, b)$,

3) Jos $(a, b) \sim (c, d) \sim (e, f)$, niin $ad = bc$ ja $cf = de$, joten $adf = bcf = bde$, josta saadaan edelleen kertolaskun vaihdannaisuuden tähden $d(af) = d(be)$. Supistussäännön mukaan siis $af = be$ eli $(a, b) \sim (e, f)$, sillä $d \neq 0$.
Siis $\sim$ on ekvivalenssirelaatio. Kun $(a, b) \sim (a', b')$ ja $(c, d) \sim (c'd')$, niin

$$(a, b) + (c, d) = (ad + bc, bd) \text{ ja}$$
$$(a', b') + (c', d') = (a'd' + b'c', b'd')$$

sekä

$$ab' = ba' \text{ ja } cd' = dc',$$

joten

$$(ad + bc)b'd' = ab'(dd') + cd'(bb') = ba'(dd') + dc'(bb') = (a'd' + b'c')bd$$

eli

$$(a, b) + (c, d) \sim (a', b') + (c', d').$$

Lisäksi

$$(a, b) \cdot (c, d) = (ac, bd) \sim (a'c', b'd') = (a', b') \cdot (c', d'),$$

sillä

$$(ac)(b'd') = (ab')(cd') = (ba')(dc') = (a'c')(bd).$$

Siis $\sim$ on kongruenssi molempien laskutoimitusten suhteen. Voidaan siksi muodostaa tekijärakenne $(R \times (R \setminus \{0\})/\sim, +, \cdot)$, jossa laskutoimitusten liitännäisyys ja vaihdannaisuus säilyy. Yhteenlaskun neutraalialkio on $[(0, 1)]_\sim$ ja kertolaskun $[(1, 1)]_\sim$.

Merkitään yksinkertaisuuden vuoksi $[a, b] = [(a, b)]_\sim$, kun $(a, b) \in R \times (R \setminus \{0\})$. Jokaisella $[a, b]$ pätee

$$[a, b] + [-a, b] = [a \cdot b + b \cdot (-a), b \cdot b] = [0, b \cdot b] = [0, 1],$$

sillä $0 \cdot 1 = 0 = b^2 \cdot 0$. Lisäksi jos $a \neq 0$, niin $[b, a]$ on määritelty ja

$$[a, b] \cdot [b, a] = [ab, ba] = [1, 1],$$

sillä $ab \cdot 1 = ab = ba = ba \cdot 1$. Siis vasta-alkiot ja käänteisalkiot ovat olemassa.

Kun $a, b, c, d, e, f \in R$, $b, d, f \neq 0$, niin

$$\begin{aligned}(a, b) \cdot \big((c, d) + (e, f)\big) &= (a, b) \cdot (cf + de, df) \\ &= (a(cf + de), b(df)) = (acf + ade, bdf)\end{aligned}$$

ja

$$\begin{aligned}(a, b) \cdot (c, d) + (a, b) \cdot (e, f) &= (ac, bd) + (ae, bf) = \big((ac)(bf) + (bd)(ae), (bd)(bf)\big) \\ &= (b(acf + ade), b(bdf)) \\ &\sim (acf + ade, bdf),\end{aligned}$$

joten

$$[a,b]\cdot\big([c,d]+[e,f]\big) = [acf+ade,bdf] = [b(acf+ade),b(bdf)]$$
$$= [a,b]\cdot[c,d]+[a,b]\cdot[e,f].$$

Kaikkiaan on nyt näytetty, että $(R\times(R\setminus\{0\}),+,\cdot)$ on kunta. Osoitetaan, että $(R,+,\cdot)$ voidaan upottaa tähän kuntaan eli on olemassa injektiivinen homomorfismi $h\colon R\to R\times(R\setminus\{0\})/\sim$. Määritellään tämä asettamalla $h(a)=[a,1]$, kun $a\in R$. h on injektio, sillä jos $h(a)=h(b)$ eli $[a,1]=[b,1]$, niin $a=a\cdot 1=1\cdot b=b$. Kun $a,b\in R$, niin

$$h(a)+h(b)=[a,1]+[b,1]=[a\cdot 1+1\cdot b,1\cdot 1]=[a+b,1]=h(a+b)$$

ja

$$h(a)\cdot h(b)=[a,1]\cdot[b,1]=[a\cdot b,1\cdot 1]=[ab,1]=h(ab).$$

Siis h on myös homomorfismi. Koska $\boldsymbol{R}$ voidaan upottaa kuntaan, sillä on myös laajennus, joka on kunta. Kun $a,b\in R$, $b\neq 0$, niin

$$[a,b]=[a,1]\cdot[1,b]=[a,1]\cdot[b,1]^{-1}=h(a)\cdot h(b)^{-1}.$$

Siis tältä laajennukselta $\boldsymbol{K}$ voidaan myös vaatia, että jokainen alkio $t\in K$ voidaan esittää muodossa $t=ab^{-1}$, missä $a,b\in R$, $b\neq 0$. □

1.2. **Määritelmä.** Edellä konstruoitua $\boldsymbol{R}$:n laajennusta kutsutaan $\boldsymbol{R}$:n *jakokunnaksi*.

Huomautus. On varsin vaivatonta osoittaa, että lauseessa esitetyt ehdot $\boldsymbol{K}$:lle määrittävät jakokunnan isomorfiaa vaille yksikäsitteisesti.

1.3. **Esimerkki.**

a) Rationaalilukujen kunta on selvästi kokonaislukujen renkaan jakokunta.
b) Olkoon $\boldsymbol{K}=(K,+,\cdot)$ kunta. Tällöin kunnan $\boldsymbol{K}$ polynomirengas $\boldsymbol{K}[x]$ on kokonaisalue, joten sillä on lauseen mukaan jakokunta. Tätä merkitään $\boldsymbol{K}(x)=(K(x),+,\cdot)$:lla.

2. Kokonaisalueet ja kunnat tekijärakenteina

Tarkastellaan, miten ideaalien ominaisuudet heijastuvat tekijärenkaiden rakenteeseen.

2.1. **Määritelmä.** Renkaan $\boldsymbol{R}=(R,+,\cdot)$ ideaali on *maksimaalinen*, jos se on maksimaalinen sisältyvyyden suhteen joukossa $\{\,J\subsetneq R\mid J \text{ on } \boldsymbol{R}\text{:n ideaali}\,\}$, ts. $\boldsymbol{R}$:n *aitojen* ideaalien joukossa.

Huomautus.

1) Toinen tapa ilmaista ideaalin I maksimaalisuus on, että jos J on $\boldsymbol{R}$:n ideaali, jolle $I\subseteq J\subseteq R$, niin joko $J=I$ tai $J=R$.
2) On tietenkin oleellista rajoittaa maksimaalisten ideaalien etsiminen aitojen ideaalien joukkoon, sillä R itse on triviaalisti suurin $\boldsymbol{R}$:n ideaaleista.

2.2. **Lause.** *Olkoon $\boldsymbol{R}$ vaihdannainen rengas ja I sen aito ideaali. Tällöin*
a) $\boldsymbol{R}/I$ on kunta, jos ja vain jos I on $\boldsymbol{R}$:n maksimaalinen ideaali.

b) $\boldsymbol{R}/\mathrm{I}$ *on kokonaisalue, jos ja vain jos* I *on alkuideaali.*

Todistus. a) *Oletetaan ensin, että* I *on maksimaalinen.* Tiedetään, että tekijärakenne $\boldsymbol{R}/\mathrm{I}$ on vaihdannainen rengas ja $1_{\boldsymbol{R}/\mathrm{I}} = 1 + \mathrm{I} \neq 0 + \mathrm{I} = 0_{\boldsymbol{R}/\mathrm{I}}$, sillä I on aito ideaali eikä sisällä ykkösalkiota. On enää osoitettava, että jokaisella nollasta poikkeavalla alkiolla on käänteisalkio. Olkoon $a \in \mathrm{R} \setminus \mathrm{I}$, jolloin $a + \mathrm{I} \neq \mathrm{I}$. Tarkastellaan ideaalia

$$\mathrm{J} = \langle \mathrm{I} \cup \{a\} \rangle.$$

Huomataan, että

$$\mathrm{J} = \{\, t + ra \mid t \in \mathrm{I},\ r \in \mathrm{R} \,\}.$$

Nimittäin jokaisella $t \in \mathrm{I}$ ja $r \in \mathrm{R}$ pätee, että $t \in \mathrm{J}$ ja $ra \in \mathrm{J}$, joten $t + ra \in \mathrm{J}$, ja toisaalta J on ideaali, sillä jos $t, t' \in \mathrm{I}$, $r, r', s \in \mathrm{R}$, niin

$$(t + ra) - (t' + r'a) = \underbrace{(t + t')}_{\in \mathrm{I}} - \underbrace{(r + r')}_{\in \mathrm{R}}\, a \in \mathrm{J}$$

ja

$$s(t + ra) = \underbrace{st}_{\in \mathrm{I}} + \underbrace{(sr)}_{\in \mathrm{R}}\, a \in \mathrm{J}.$$

J on siis $\boldsymbol{R}$:n ideaali, jolle $\mathrm{I} \subsetneq \mathrm{I} \cup \{a\} \subseteq \mathrm{J}$. Koska I on maksimaalinen, niin täytyy olla $\mathrm{J} = \mathrm{R}$ ja erityisesti $1 \in \mathrm{J}$. Ykköselle saadaan siis esitys $1 = t + ra$ joillakin $t \in \mathrm{I}$ ja $r \in \mathrm{R}$. Siis

$$(r + \mathrm{I})(a + \mathrm{I}) = ra + \mathrm{I} = ra + (t + \mathrm{I}) = (ra + t) + \mathrm{I} = 1 + \mathrm{I},$$

ts. $r + \mathrm{I} = (a + \mathrm{I})^{-1}$.

Oletetaan sitten, että I *ei ole maksimaalinen.* Tämä tarkoittaa, että on olemassa $\boldsymbol{R}$:n ideaali J, jolle $\mathrm{I} \subsetneq \mathrm{J} \subsetneq \mathrm{R} = \langle 1 \rangle$. Olkoon $a \in \mathrm{J} \setminus \mathrm{I}$, jolloin erityisesti $a + \mathrm{I} \neq \mathrm{I}$. Tällöin jokaisella $r \in \mathrm{R}$ pätee $ra \in \mathrm{J}$, joten $(r + \mathrm{I})(a + \mathrm{I}) = ra + \mathrm{I} \neq 1 + \mathrm{I}$. Siis alkiolla $a + \mathrm{I}$ ei ole käänteisalkiota.

b) *Oletetaan ensin, että* I *on* $\boldsymbol{R}$*:n alkuideaali.* Olkoot $a, b \in \mathrm{I}$ alkioita, joille $(a + \mathrm{I})(b + \mathrm{I}) = \mathrm{I}$. Tällöin $ab \in \mathrm{I}$, joten koska I on alkuideaali, niin $a \in \mathrm{I}$ tai $b \in \mathrm{I}$ eli $a + \mathrm{I} = 0 + \mathrm{I}$ tai $b + \mathrm{I} = 0 + \mathrm{I}$. Siis $\boldsymbol{R}/\mathrm{I}$ on kokonaisalue.

Oletetaan sitten, että I *ei ole* $\boldsymbol{R}$*:n alkuideaali,* ts. joillakin $a, b \in \mathrm{R} \setminus \mathrm{I}$ pätee $ab \in \mathrm{I}$. Tällöin

$$(a + \mathrm{I})(b + \mathrm{I}) = ab + \mathrm{I} = \mathrm{I},$$

vaikka $a + \mathrm{I} \neq \mathrm{I}$ ja $b + \mathrm{I} \neq \mathrm{I}$, ts. tulon nollasääntö ei ole voimassa. □

2.3. Esimerkki.

a) $(\mathbb{Z}, +, \cdot)$:n ideaalit ovat muotoa $m\mathbb{Z}$, missä $m \in \mathbb{Z}$. Parametrista m voidaan olettaa, että $m \geqslant 0$, sillä $m\mathbb{Z} = (-m)\mathbb{Z}$. Tällä oletuksella pätee

$$\begin{aligned} & m \text{ on alkuluku} \\ \iff\ & m \text{ on alkualkio } (\mathbb{Z}, +, \cdot)\text{:ssa} \\ \iff\ & m\mathbb{Z} \text{ on alkuideaali } (\mathbb{Z}, +, \cdot)\text{:ssa} \\ \iff\ & (\mathbb{Z}/m\mathbb{Z}, +, \cdot) \text{ on äärellinen kokonaisalue.} \end{aligned}$$

Toisaalta $m\mathbb{Z} \subseteq n\mathbb{Z} \iff m \in n\mathbb{Z} \iff n \mid m$, joten $m\mathbb{Z}$ on maksimaalinen, jos ja vain jos m on alkuluku. Siis $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ on kunta, jos ja vain jos se on äärellinen kokonaisalue, kun $m \in \mathbb{Z}$.

b) Varustetaan $\mathbb{Z} \times \mathbb{Z}$ pisteittäisesti määritellyillä laskutoimituksilla. Selvästi

$$\{0\} \times \mathbb{Z} \text{ ja } \mathbb{Z} \times \{0\}$$

ovat tämän renkaan alkuideaaleja. Kuitenkaan

$$(\mathbb{Z} \times \mathbb{Z}/\{0\} \times \mathbb{Z}, +, \cdot) \cong (\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \{0\}, +, \cdot) \cong (\mathbb{Z}, +, \cdot)$$

ei ole kunta, joten nämä ideaalit eivät ole maksimaalisia.

3. Polynomit ja kuntalaajennukset

3.1. Merkintä. Olkoon $\boldsymbol{R} = (R, +, \cdot)$ pseudorenkaan $\boldsymbol{S} = (S, +, \cdot)$ alipseudorengas ja $A \subseteq S$. Merkitään tällöin joukon $R \cup A$ virittämän alirenkaan perusjoukkoa $R[A]$:lla. Vastaavaa alipseudorengasta merkitään $\boldsymbol{R}[A]$:lla. Jos $A = \{a_0, \ldots, a_{n-1}\}$ on äärellinen ($n \in \mathbb{N}$), niin merkitään yksinkertaisesti $R[a_0, \ldots, a_{n-1}] = R[\{a_0, \ldots, a_{n-1}\}]$ (ja vastaavasti alirenkaille).

3.2. Määritelmä. Olkoon $(R, +, \cdot)$ vaihdannainen rengas ja $n \in \mathbb{Z}_+$. Renkaan $\boldsymbol{R} = (R, +, \cdot)$ n muuttujan polynomirengas $\boldsymbol{R}[x_0, \ldots, x_{n-1}] = (R[x_0, \ldots, x_{n-1}], +, \cdot)$ määritellään induktiivisesti niin, että kaikilla $m \in \mathbb{N}$, $m < n$, $\boldsymbol{R}[x_0, \ldots, x_{m-1}, x_m]$ on renkaan $\boldsymbol{R}[x_0, \ldots, x_{m-1}]$ (yhden muuttujan) polynomirengas,
ts. $\boldsymbol{R}[x_0, \ldots, x_m] = \boldsymbol{R}[x_0, \ldots, x_{m-1}][x_m]$ (ja $\boldsymbol{R}[] = \boldsymbol{R}$).

Huomautus. Merkinnät ovat keskenään konsistentteja, sillä n muuttujan polynomirengas on joukon $R \cup \{x_0, \ldots, x_{n-1}\}$ virittämä. Huomattakoon myös, että muuttujille joudutaan tietenkin käyttämään eri nimiä, joten sekaannuksen välttämiseksi on jossakin tilanteessa hyvä korostaa, mitkä ovat muuttujia.

3.3. Lemma. *Olkoon h homomorfismi vaihdannaisesta renkaasta $\boldsymbol{R} = (R, +, \cdot)$ vaihdannaiseen renkaaseen $\boldsymbol{S} = (S, +, \cdot)$. Tällöin*

$$g\colon R[x] \to S[x],\ g\Big(\sum_{i=0}^{n} a_i x^i\Big) = \sum_{i=0}^{n} h(a_i) x^i$$

on homomorfismi polynomirenkaasta $\boldsymbol{R}[x]$ polynomirenkaaseen $\boldsymbol{S}[x]$.

Todistus. Olkoot $p, q \in R[x]$. Esitetään nämä polynomit kertoimien avulla: $p = \sum_{i=0}^{n} a_i x^i$, $q = \sum_{i=0}^{n} b_i x^i$, missä $n \in \mathbb{N}$ ja $a_0, \ldots, a_n, b_0, \ldots, b_n \in R$. Merkitään myös $a_i = b_i = 0$, kun $i \in \mathbb{N}$, $i > n$. Tällöin

$$\begin{aligned} g(p+q) &= g\left(\sum_{i=0}^{n} (a_i + b_i) x^i\right) = \sum_{i=0}^{n} h(a_i + b_i) x^i \\ &= \sum_{i=0}^{n} (h(a_i) + h(b_i)) x^i = \sum_{i=0}^{n} h(a_i) x^i + \sum_{i=0}^{n} h(b_i) x^i = g(p) + g(q) \end{aligned}$$

ja

$$g(pq) = g\left(\sum_{k=0}^{2n}\left(\sum_{i=0}^{n} a_i b_{k-i}\right)x^k\right) = \sum_{k=0}^{2n}\left(h\left(\sum_{i=0}^{n} a_i b_{k-i}\right)x^k\right)$$
$$= \sum_{k=0}^{2n}\left(\sum_{i=0}^{n} h(a_i)h(b_{k-i})\right)x^k = \left(\sum_{i=0}^{n} h(a_i)x^i\right)\left(\sum_{j=0}^{n} h(b_j)x^i\right)$$
$$= g(p)g(q). \quad \square$$

3.4. Lause. *Olkoon $\boldsymbol{R} = (R, +, \cdot)$ vaihdannainen rengas ja olkoot $a_0, \ldots, a_{n-1} \in R$ ($n \in \mathbb{Z}_+$). Tällöin on olemassa homomorfismi e n muuttujan renkaasta $\boldsymbol{R}[x_0, \ldots, x_{n-1}]$ renkaaseen $\boldsymbol{R}$, jolle $e{\restriction}R = \mathrm{id}_R$ ja $e(x_i) = a_i$, kun $i \in \{0, \ldots, n-1\}$.*

Todistus. Todistetaan väite induktiolla luvun $n \in \mathbb{Z}_+$ suhteen.

1) Kun $n = 1$, niin laskuharjoitustehtävän mukaan sijoitushomomorfismi

$$e_{a_0}\colon R[x_0] \to R,\ e_{a_0}\left(\sum_{i=0}^{m} r_i x^i\right) = \sum_{i=0}^{m} r_i {a_0}^i$$

on todella homomorfismi. Selvästi $e_{a_0}(r) = r$, kun $r \in R$, ja $e_{a_0}(x_0) = e_{a_0}(1 \cdot {x_0}^1) = 1 \cdot a_0 = a_0$.

2) Oletetaan, että väite pätee arvolla $n \in \mathbb{Z}_+$. Olkoot $a_0, \ldots a_n \in R$. Induktio-oletuksen mukaan on olemassa homomorfismi $e_{(a_0,\ldots,a_{n-1})}$ renkaasta $\boldsymbol{R}[x_0, \ldots, x_{n-1}]$ renkaaseen $\boldsymbol{R}$, jolle $e_{(a_0,\ldots,a_{n-1})}{\restriction}R = \mathrm{id}_R$ ja $e_{(a_0,\ldots,a_{n-1})}(x_i) = a_i$, kun $i \in \{0, \ldots, n-1\}$. Lemman nojalla

$$h\colon R[x_0, \ldots, x_{n-1}][x_n] \to R[x_n],\ h\left(\sum_{i=0}^{m} p_i {x_n}^i\right) = \sum_{i=0}^{m} e_{(a_0,\ldots,a_{n-1})}(p_i){x_n}^i$$

on homomorfismi renkaasta $\boldsymbol{R}[x_0, \ldots, x_n]$ renkaaseen $\boldsymbol{R}[x_n]$. Siis yhdistetty kuvaus $e_{(a_0,\ldots,a_n)} = e_{a_n} \circ h\colon R[x_0, \ldots, x_n] \to R$ on homomorfismi, missä $e_{a_n}\colon R[x_n] \to R$ on sijoitushomomorfismi, jolle $e_{a_n}(x_n) = a_n$. Kun $r \in R$, niin

$$e_{(a_0,\ldots,a_n)}(r) = e_{a_n}(h(r)) = e_{a_n}(e_{(a_0,\ldots,a_{n-1})}(r)) = e_{a_n}(r) = r.$$

Lisäksi jokaisella $i \in \{0, \ldots n-1\}$ pätee

$$e_{(a_0,\ldots,a_n)}(x_i) = e_{a_n}(h(x_i)) = e_{a_n}(e_{(a_0,\ldots,a_{n-1})}(x_i)) = e_{a_n}(a_i) = a_i$$

sekä

$$e_{(a_0,\ldots,a_n)}(x_n) = e_{a_n}(h(x_n)) = e_{a_n}(x_n) = a_n. \quad \square$$

Huomautus. Tässä todistuksessa määriteltyä homomorfismia $e_{(a_0,\ldots,a_n)}$ kutsutaan myös *sijoitushomomorfismiksi.*

3.5. Seuraus. *Olkoon $\boldsymbol{R} = (R, +, \cdot)$ vaihdannaisen renkaan $\boldsymbol{S} = (S, +, \cdot)$ alirengas ja $a_0, \ldots, a_{n-1} \in S$, $n \in \mathbb{N}$. Tällöin on olemassa yksikäsitteinen homomorfismi $h\colon R[x_0, \ldots, x_{n-1}] \to S$, jolle $h{\restriction}R = \mathrm{id}_R$ ja $h(x_i) = a_i$, kun $i \in \{0, \ldots, n-1\}$.*

Todistus. Lauseen perusteella tiedetään, että $e_{(a_0,\ldots,a_{n-1})}\colon S[x_0,\ldots,x_{n-1}] \to S$ on homomorfismi, joka toteuttaa lisäehdot (erityisesti $e_{(a_0,\ldots,a_{n-1})}{\restriction}R = (e_{(a_0,\ldots,a_{n-1})}{\restriction}S){\restriction}R = \mathrm{id}_S{\restriction}R = \mathrm{id}_R$), mutta jonka lähtöjoukko on väärä. Sen sijaan $h = e_{(a_0,\ldots,a_{n-1})}{\restriction}R$ on halutunlainen.

Yksikäsitteisyys: Tapauksessa $n = 1$ on kyse siitä, että jokainen polynomi $p \in R[x_0]$ voidaan kirjoittaa muodossa $p = \sum_{i=0}^{n} r_i {x_0}^i$, jolloin väitteen ehdoista seuraa

$$h(p) = h\Big(\sum_{i=0}^{n} r_i {x_0}^i\Big) = \sum_{i=0}^{n} h\Big(r_i {x_0}^i\Big) = \sum_{i=0}^{n} h(r_i)h(x_0)^i = \sum_{i=0}^{n} r_i {a_0}^i = e_{a_0}(p).$$

Yleinen yksikäsitteisyys seuraa induktiolla tästä. □

3.6. Määritelmä. Rengasta $\boldsymbol{S}$ kutsutaan renkaan $\boldsymbol{R}$ *laajennukseksi*, jos $\boldsymbol{R}$ on $\boldsymbol{S}$:n alirengas. Jos molemmat ovat kuntia, käytetään nimitystä *kuntalaajennus*.

3.7. Seuraus. *Jos vaihdannainen rengas $\boldsymbol{S}$ on $\boldsymbol{R}$:n laajennus ja $\boldsymbol{S} = \boldsymbol{R}[a_0,\ldots,a_{n-1}]$ joillakin $a_0,\ldots,a_{n-1} \in S$, niin $\boldsymbol{S} \cong \boldsymbol{R}[x_0,\ldots,x_{n-1}]/I$, missä I on polynomirenkaan $\boldsymbol{R}[x_0,\ldots,x_{n-1}]$ ideaali.*

Todistus. Kun h on edellisen seurauksen homomorfismi ja valitaan $I = \mathrm{Ker}\, h$, niin renkaiden homomorfialauseesta seuraa

$$\boldsymbol{R}[x_0,\ldots,x_{n-1}]/I \cong (\mathrm{Im}\, h, +, \cdot) = \boldsymbol{S}. \quad \square$$

Tarkastellaan nyt tilannetta, jossa $\boldsymbol{L}$ on $\boldsymbol{K}$:n aito kuntalaajennus ja $\boldsymbol{L} = \boldsymbol{K}[a]$. Tällöin $a \notin K$ ja edellisen seurauksen mukaan $\boldsymbol{L} \cong \boldsymbol{K}[x]/I$ jollakin polynomirenkaan $\boldsymbol{K}[x]$ ideaalilla I. Koska $\boldsymbol{K}[x]$ on pääideaalialue, niin puolestaan $I = \langle p\rangle$ jollakin polynomilla $p \in K[x]$. Koska $\boldsymbol{L} \cong \boldsymbol{K}[x]/I$ on kunta, niin ideaalin I on oltava maksimaalinen. Koska $\boldsymbol{K}[x]$ on jopa faktoriaalinen, niin $I = \langle p\rangle$ on alkuideaali, jos ja vain jos p on alkualkio, jos ja vain jos p on jaoton, jos ja vain jos $I = \langle p\rangle$ on maksimaalinen. Tällaisten kuntalaajennusten analysoiminen palautuu siis jaottomien polynomien tutkimiseen.

Ensimmäinen havainto polynomien jaottomuudesta on, että ensimmäisen asteen polynomit ovat ainoita jaottomia polynomeja, joilla on juuria. Toisaalta ne ovat nimittäin selvästi jaottomia kuntakertoimisessa tapauksessa. Toisaalta jos $a \in K$ on polynomin p juuri, niin $x - a \mid p$, joten p ei ole jaoton, jos $\deg(p) > 1$. Juurettomuudesta ei kääntäen seuraa yleisesti jaottomuutta, mutta seuraava tulos voidaan alhaisasteisille polynomeille todistaa.

3.8. Lause. *Tarkastellaan kunnan $\boldsymbol{K} = (K, +, \cdot)$ polynomirengasta $\boldsymbol{K}[x]$ ja sen polynomia $p \in K[x]$, jolle $\deg(p) = 2$ tai $\deg(p) = 3$. Tällöin p on jaoton, jos ja vain jos sillä ei ole juuria.*

Todistus. Edellä on jo todettu, että p ei voi olla jaoton, jos sillä on juuria. Oletetaan kääntäen, että p olisi jaollinen, ts. $p = qr$, missä kumpikaan polynomeista p ja q ei ole vakiopolynomi (eli tässä tapauksessa yksikkö). Koska $\deg(p) = \deg(q) + \deg(r) \in \{2, 3\}$, niin $\deg(q) = 1$ tai $\deg(r) = 1$. Voidaan olettaa, että $\deg(q) = 1$, jolloin $q = cx + d$ joillakin $c, d \in K$ ja $-d/c$ on q:n ja siten myös p:n juuri. □

3.9. Esimerkki. Etsitään kunnan $\mathbb{Z}_2 = (\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ polynomirenkaan jaottomat polynomit, joiden aste on korkeintaan 3.

p	$p(0)$	$p(1)$	juurten joukko	jaottomuus
x	0	1	$\{0\}$	jaoton
$x+1$	1	0	$\{1\}$	jaoton
x^2	0	1	$\{0\}$	
x^2+1	1	0	$\{1\}$	
x^2+x	0	0	$\{0,1\}$	
x^2+x+1	1	1	$\emptyset$	jaoton
x^3	0	1	$\{0\}$	
x^3+1	1	0	$\{1\}$	
x^3+x	0	0	$\{0,1\}$	
x^3+x+1	1	1	$\emptyset$	jaoton
x^3+x^2	0	0	$\{0,1\}$	
x^3+x^2+1	1	1	$\emptyset$	jaoton
x^3+x^2+x	0	1	$\{0\}$	
x^3+x^2+x+1	1	0	$\{1\}$	

Etsityt jaottomat polynomit ovat siis x, $x+1$, x^2+x+1, x^3+x+1 ja x^3+x^2+1.

Jatketaan esimerkkiä tarkastelemalla erityisesti jaotonta polynomia x^3+x+1. Jaottomuudesta seuraa siis, että $\langle x^3+x+1\rangle$ on maksimaalinen ideaali ja $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ on kunta. Jokaisella $p \in (\mathbb{Z}/2\mathbb{Z})[x]$ on jakoyhtälön nojalla olemassa sellaiset $q, r \in (\mathbb{Z}/2\mathbb{Z})[x]$, että

$$p = (x^3+x+1)\cdot q + r,$$

missä $\deg(r) < \deg(x^3+x+1) = 3$, jolloin

$$p + \langle x^3+x+1\rangle = r + \langle x^3+x+1\rangle.$$

Koska polynomeja $r \in (\mathbb{Z}/2\mathbb{Z})[x]$, joille $\deg(r) \leqslant 2$, on $2^3 = 8$ kappaletta, niin kunnassa $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ on korkeintaan 8 alkiota. Toisaalta jakoyhtälön jaon yksikäsitteisyydestä seuraa, että $r + \langle x^3+x+1\rangle \neq r' + \langle x^3+x+1\rangle$, kun $r \neq r'$, $\deg(r) \leqslant 2$ ja $\deg(r') \leqslant 2$.

Merkitään $I = \langle x^3+x+1\rangle$. Konkreettisissa laskuissa on käytännöllistä merkitä $p \equiv q \pmod{I}$, kun $p, q \in (\mathbb{Z}/2\mathbb{Z})[x]$. Yhteen- ja kertolaskutauluissa esiintyy alkioiden sijasta ekvivalenssiluokkien edustajia eli polynomeja.

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Esimerkiksi

$$x \cdot x^2 = x^3 \equiv x^3 + (x^3 + x + 1) = x + 1 \pmod{I},$$

$$\begin{aligned}(x+1)(x^2+x) &= x^3 + x^2 + x^2 + x = x^3 + x \\ &\equiv x^3 + x + (x^3 + x + 1) = 1 \pmod{I}\end{aligned}$$

ja

$$x^2 \cdot x^2 = x^4 \equiv x^4 + x \cdot (x^3 + x + 1) = x^4 + x^4 + x^2 + x = x^2 + x \pmod{I}.$$

4. Rationaalikertoimisten polynomien jaollisuusoppia

4.1. Määritelmä. Kokonaisalueen $\boldsymbol{R} = (R, +, \cdot)$ polynomirenkaan alkiota $p \in R[x]$ kutsutaan *pääpolynomiksi*, jos sen korkeimman asteen termin kerroin on 1, ts. $p = x^n + q$, missä $q \in R[x]$ ja $n = \deg(p) > \deg(q)$. Polynomi $p = \sum_{i=0}^{n} a_i x^i$ on *primitiivinen*, jos sen kertoimien suurin yhteinen tekijä on 1.

4.2. Lemma. *Primitiivisten kokonaiskertoimisten polynomien tulo on primitiivinen.*

Todistus. Oletetaan vastoin väitettä, että on olemassa primitiiviset $f, g \in \mathbb{Z}[x]$, joille fg ei ole primitiivinen. On siis olemassa alkuluku p, joka jakaa kaikki polynomin fg kertoimet. Tarkastellaan kanonista homomorfismia $h\colon \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ ja siihen luonnollisella tavalla liittyvää polynomirenkaiden välistä homomorfismia $\tilde{h}\colon \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$,

$$\tilde{h}\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} h(a_i) x^i.$$

Tiedetään, että

$$0 = \tilde{h}(fg) = \tilde{h}(f)\tilde{h}(g).$$

Koska $\mathbb{Z}_p$ on kunta, niin $\mathbb{Z}_p[x]$ on kokonaisalue, joten $\tilde{h}(f) = 0$ tai $\tilde{h}(g) = 0$. Edellisessä tapauksessa p jakaa kaikki polynomin f kertoimet, jälkimmäisessä tapauksessa g:n. Siis f tai g ei ole primitiivinen. □

4.3. Lemma. *Olkoon* $f \in \mathbb{Q}[x]$, $f \neq 0$. *Tällöin on olemassa yksikäsitteiset primitiivinen* $f^* \in \mathbb{Z}[x]$ *ja kerroin* $c(f) \in \mathbb{Q}_+ = \{ q \in \mathbb{Q} \mid q > 0 \}$, *joille* $f = c(f)f^*$. *Jos* $f \in \mathbb{Z}[x]$, *niin* $c(f) \in \mathbb{Z}$.

Todistus. Kirjoitetaan

$$f = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i,$$

missä $a_i, b_i \in \mathbb{Z}$, $b_i \neq 0$, kun $i \in \{0, \ldots, n\}$. Tällöin

$$\tilde{f} = \left(\prod_{i=0}^{n} b_i \right) \cdot f \in \mathbb{Z}[x].$$

Olkoon D polynomin $\tilde{f}$ kertoimien positiivinen tai negatiivinen suurin yhteinen tekijä sen mukaan, kumpi on samanmerkkisen tulon $\prod_{i=0}^{n} b_i$ kanssa. Tällöin $f^* = \tilde{f} \cdot D^{-1} \in \mathbb{Z}[x]$ on primitiivinen ja $c(f) = D / \prod_{i=0}^{n} b_i > 0$. Selvästi $f = c(f) \cdot f^*$ ja jos $f \in \mathbb{Z}[x]$, niin $c(f) = D \in \mathbb{Z}$.

Todistetaan esityksen yksikäsitteisyys: Olkoot $e \in \mathbb{Q}_+$ ja primitiivinen $h \in \mathbb{Z}[x]$ sellaiset, että $f = eh$. Tällöin on olemassa $u, v \in \mathbb{Z}$, joille $\mathrm{syt}(u, v) = 1$ ja $uf^* = vh$. Kirjoitetaan

$$h = \sum_{i=0}^{n} s_i x^i,$$

missä $s_i \in \mathbb{Z}$, kun $i \in \{0, \ldots, n\}$. Koska $uf^* = vh$, niin $u \mid vs_i$ jokaisella $i \in \{0, \ldots, n\}$. Koska $\mathrm{syt}(u, v) = s_i$, tästä seuraa $u \mid s_i$. Mutta h on primitiivinen, josta seuraa $u = \pm 1$. Samoin $v = \pm 1$. Merkkiehdosta seuraa $u = v$, joten $f^* = h$ ja $c(f) = e$. □

4.4. Määritelmä. Lemman vakiota $c(f)$ kutsutaan polynomin $f \in \mathbb{Q}[x]$ *sisällöksi.*

4.5. Lemma. *Kun* $f, g \in \mathbb{Q}[x] \setminus \{0\}$, *niin*

$$c(fg) = c(f)c(g).$$

Todistus. Koska polynomeille f ja g saadaan esitykset $f = c(f)f^*$ ja $g = c(g)c^*$, missä f^* ja g^* ovat primitiivisiä, niin

$$fg = c(f)c(g)f^*g^*.$$

Koska f^* ja g^* ovat primitiivisiä, niin lemman 4.2 nojalla f^*g^* on primitiivinen. Lisäksi $c(f)c(g) > 0$, joten edellä on haluttu esitys, jossa $c(fg) = c(f)c(g)$. Tulos seuraa siis esityksen yksikäsitteisyydestä. □

4.6. Gaussin lause. *Olkoon* $f \in \mathbb{Z}[x]$. *Jos on olemassa sellaiset polynomit* $g_0, h_0 \in \mathbb{Q}[x]$, *joille*

$$f = g_0 h_0,$$

niin on olemassa myös sellaiset $g, h \in \mathbb{Z}[x]$, *joille*

$$f = gh, \deg(g) = \deg(g_0) \textit{ ja } = \deg(h) = \deg(h_0).$$

Erityisesti: Jos f ei ole vakiopolynomi eikä jakaudu alempiasteisiin tekijöihin polynomirenkaassa $(\mathbb{Z}[x], +, \cdot)$, niin f on jaoton renkaassa $(\mathbb{Q}[x], +, \cdot)$.

Todistus. Tämän alaluvun lemmojen mukaan $g_0 = c(g_0)g_0^*$ ja $h_0 = c(g)h_0^*$, missä $g_0^*, h_0^* \in \mathbb{Z}[x]$ ovat primitiivisiä. Edelleen tiedetään, että

$$c(g_0)c(h_0) = c(g_0h_0) = c(f) \in \mathbb{Z}.$$

Siis $g = c(g_0)c(h_0)g_0^* \in \mathbb{Z}[x]$ ja $h = h_0^* \in \mathbb{Z}[x]$ ovat polynomeja, joille $gh = c(g_0)c(h_0)g_0^*h_0^* = g_0h_0 = f$, $\deg(g) = \deg(g_0)$ ja $\deg(h) = \deg(h_0)$.

Lauseen lisäväite seuraa suoraan jo todistetusta. □

4.7. Lause. *Olkoon $f \in \mathbb{Z}[x]$ pääpolynomi ja p alkuluku. Olkoon $h\colon \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ kanoninen homomorfismi ja $\tilde{h}\colon \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ siihen liittyvä polynomirenkaiden välinen homomorfismi. Tällöin jos $\tilde{h}(f)$ on jaoton $\mathbb{Z}_p[x]$:ssä, niin f on jaoton $(\mathbb{Q}[x], +, \cdot)$:ssä.*

Todistus. Oletetaan, että $\tilde{h}(f)$ on jaoton $\mathbb{Z}_p[x]$:ssä. Koska f on pääpolynomi, $\deg(\tilde{h}(f)) = \deg(f)$. Koska $\tilde{h}(f)$ on jaoton, se ei voi olla vakiopolynomi. Oletetaan vastoin väitettä, että f olisi jaollinen $(\mathbb{Q}[x], +, \cdot)$:ssä. Edellisen lauseen mukaan f jakautuisi tällöin alempiasteisiin tekijöihin jo $(\mathbb{Z}[x], +, \cdot)$:ssä, ts. pätisi $f = qr$, missä $q, r \in \mathbb{Z}[x]$, $\deg(q) < \deg(f)$, $\deg(r) < \deg(f)$. Koska $(\mathbb{Z}[x], +, \cdot)$ on kokonaisalue, q:n ja r:n korkeimpien asteiden termien tulo on f:n korkeimman asteen termi, ts. 1. Voidaan siis olettaa, että q ja r ovat pääpolynomeja. Saadaan

$$\tilde{h}(f) = \tilde{h}(qr) = \tilde{h}(q)\tilde{h}(r),$$

missä $\deg(\tilde{h}(q)) = \deg(q) < \deg(f) = \deg(\tilde{h}(f))$ ja $\deg(\tilde{h}(r)) < \deg(\tilde{h}(f))$, mikä on ristiriidassa $\tilde{h}(f)$:n jaottomuuden kanssa. □

4.8. Esimerkki. Onko $x^3 + 20x^2 + 11x + 2013$ jaoton $(\mathbb{Q}[x], +, \cdot)$:ssä? Muodostetaan homomorfismi $\tilde{h}\colon \mathbb{Z}[x] \to (\mathbb{Z}/2\mathbb{Z})[x]$ kuten lauseessa, jolloin $\tilde{h}(x^3 + 20x^2 + 11x + 2013) = x^3 + x + 1$, joka on jaoton $\mathbb{Z}_2[x]$:ssä, sillä se on kolmatta astetta, mutta sillä ei ole juuria:

$$0^3 + 0 + 1 = 1 \neq 0 \text{ ja } 1^3 + 1 + 1 = 1 \neq 0.$$

Siis alkuperäinen polynomi $x^3 + 20x^2 + 11x + 2013$ on jaoton.

4.9. Eisensteinin kriteerio *Olkoon $a = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, missä $n = \deg(a) > 0$, ja olkoon p alkuluku. Oletetaan, että $p \mid a_i$ jokaisella $i \in \{0, \ldots, n-1\}$, mutta $p \nmid a_n$, $p^2 \nmid a_0$. Tällöin a on jaoton $(\mathbb{Q}[x], +, \cdot)$:ssä.*

Todistus. Tarkastellaan jälleen kanonista homomorfismia $h\colon \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ ja siihen liittyvää polynomirenkaiden homomorfismia $\tilde{h}\colon \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$. Siis

$$\tilde{h}(a) = \sum_{i=0}^{n} h(a_i)x^i = \bar{a}_n x^n,$$

missä $\bar{a}_n = a_n + p\mathbb{Z}$. Oletetaan vastoin väitettä, että a olisikin jaollinen, ts. $a = bc$, missä $\deg(b) < \deg(a)$ ja $\deg(c) < \deg(a)$. Tästä seuraa

$$\bar{a}_n x^n = \tilde{h}(a) = \tilde{h}(b)\tilde{h}(c).$$

Koska $\mathbb{Z}_p$ on kunta, niin polynomirengas $\mathbb{Z}_p[x]$ on faktoriaalinen. Tästä seuraa, että

$$\tilde{h}(b) = ux^m \text{ ja } \tilde{h}(c) = vx^k,$$

missä $u, v \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ ja $m, k \in \mathbb{Z}_+$. Siis $p \mid b_0$ ja $p \mid c_0$, missä b_0 on b:n ja c_0 c:n vakiotermi. Tästä saadaan $p^2 \mid b_0c_0 = a_0$, mikä on vastoin oletusta. □

Käsitellään Eisensteinin kriteerion esimerkkisovelluksena syklotomisia polynomeja.

4.10. Määritelmä. Kun p on alkuluku, *p:s syklotominen polynomi* on

$$\Phi_p = \sum_{i=0}^{p-1} x^i \in \mathbb{Z}[x].$$

Selvästi

$$x^p - 1 = (x-1)\sum_{i=0}^{p-1} x^i = (x-1)\Phi_p.$$

4.11. Lemma. *Kun p on alkuluku, niin jokaisella $k \in \{1, 2, \ldots, p-1\}$ pätee*

$$p \mid \binom{p}{k}.$$

Todistus. Tiedetään, että $\binom{p}{k} = (p)_k/k!$, missä *kertomapotenssi* $(p)_k$ määritellään induktiivisesti: $(p)_0 = 1$, $(p)_{i+1} = (p)_i \cdot (p-i)$. Selvästi

$$p \mid (p)_k = \binom{p}{k} \cdot k!,$$

kun $k \in \{1, 2, \ldots, p-1\}$, joten

$$p \mid \binom{p}{k} \text{ tai } p \mid k!.$$

Kuitenkaan $p \nmid k!$, koska $p \nmid j$ millään $j \in \{1, \ldots, k\}$. Siis $p \mid \binom{p}{k}$. □

4.12. Lemma. *Olkoon $\boldsymbol{R} = (R, +, \cdot)$ vaihdannainen rengas ja $t \in R$. Tällöin*

$$f\colon R[x] \to R[x],\ f\Big(\sum_{i=0}^{n} a_i x^i\Big) = \sum_{i=0}^{n} a_i (x+t)^i$$

on polynomirenkaan $\boldsymbol{R}[x]$ automorfismi. □

4.13. Lause. *Kun* p *on alkuluku,* p*:s syklotominen polynomi* Φ_p *on jaoton* $(\mathbb{Q}[x], +, \cdot)$*:ssa.*

Todistus. Edellisen lemman mukaan Φ_p on jaoton, jos ja vain jos $\Phi_p(x+1)$ on jaoton. Koska

$$x^p - 1 = (x-1)\Phi_p,$$

niin

$$(x+1)^p - 1 = x\Phi_p(x+1),$$

mistä saadaan $\Phi_p(x+1) = \sum_{j=0}^{p-1} \binom{p}{j+1} x^j$. Kertoimista havaitaan, että

$$\binom{p}{(p-1)+1} = \binom{p}{p} = 1$$

ja kun $j \in \{0, \ldots, p-2\}$, niin $j+1 \in \{1, 2, \ldots, p-1\}$ ja

$$p \mid \binom{p}{j+1}$$

sekä

$$p^2 \nmid \binom{p}{0+1} = \binom{p}{1} = p.$$

Siis Eisensteinin kriteerion mukaan $\Phi_p(x+1)$ on jaoton. Siis myös Φ_p on jaoton. □