Aritmetiikan peruslause algebrallisten kokonaislukujen renkaissa

Pro gradu -tutkielma
Itä-Suomen yliopisto
Yliopistonkatu 2, 80101 Joensuu
Fysiikan ja matematiikan laitos
Tuomas Manninen, 243034
11. joulukuuta 2013

Sisältö

Johdanto

Aritmetiikan peruslause on ollut tunnettu jo antiikin Kreikan ajoista lähtien ja löytyy todistuksineen esimerkiksi *Eukleideen* kirjasarjan *Alkeet* seitsemännestä kirjasta. Myöhemmin *Carl Friedrich Gauss* nykyaikaisti tuloksen ja todistuksen teoksessaan *Disquisitiones Arithmeticae*, sekä yleisti tuloksen niin sanotuille *Gaussin kokonaisluvuille*

$$\mathbb{Z}(i) = \{a + bi \colon a, b \in \mathbb{Z}, i^2 = -1\}.$$

Edelleen, *Gotthold Eisenstein* osoitti aritmetiikan peruslauseen olevan voimassa *Eisensteinin kokonaisluvuille* $\mathbb{Z}(\sqrt{-3})$.

Monet matemaatikot olivat siinä käsityksessä, että aritmetiikan peruslause on voimassa kaikissa lukurenkaissa ja *Gabriel Lamé* esittikin todistuksen *Fermat'n suurelle lauseelle* jakaen summan $x^n + y^n$ kompleksilukutekijöiksi yksikköjuurten avulla. *Ernst Kummer* oli kuitenkin paria vuotta aiemmin osoittanut, että yksikäsitteinen tekijöihinjako ei toimi aina Lamén todistuksessa käyttämille kompleksiluvuille. Koko algebrallisen lukuteorian tutkimus lähtikin liikkeelle sen selvittämisestä, että milloin yksikäsitteinen tekijöihinjako on voimassa. Tässä tutkielmassa rajoitutaan tarkastelemaan tietynlaisia renkaita ja havaitaan, että yksikäsitteisen tekijöihinjaon olemassaolo riippuu renkaan ideaaleista. Yksikäsitteinen tekijöihinjako onnistuu täsmälleen silloin kun kaikki renkaan ideaalit ovat pääideaaleja, eli yhden alkion virittämiä.

Luvuissa 1 ja 2 listataan pohjatiedot, joita tutkielmassa myöhemmin käytetään. Näissä kappaleissa esitetyt asiat oletetaan tunnetuiksi ja todistuksia ei käydä läpi tässä tutkielmassa paria poikkeusta lukuunottamatta. Lukuteorian puolelta Eukleideen lemma ja perinteinen aritmetiikan peruslause esitetään todistuksineen ja varsinkin jälkimmäisen todistuksesta voi myöhemmin löytää samankaltaisuuksia yleisempien tapausten todistuksesta.

Kolmannessa luvussa keskitytään tarkastelemaan kokonaisalueita ja perehdytään hieman niiden rakenteisiin. Kolmannen luvun päätulos on yksikäsitteisen tekijöihinjaon olemassaolon osoittaminen pääideaalikokonaisalueissa. Neljännessä tutkitaan tarkemmin ideaaleja ja rakennetaan aluksi hieman toisenlainen esimerkki yksikäsitteisestä tekijöihinjaosta osoittamalla, että algebrallisten kokonaislukujen renkaiden nollasta eroavat ideaalit voidaan itse asiassa esittää yksikäsitteisesti alkuideaalien tulona. Neljännen päätulos on, että yksikäsitteinen tekijöihinjako algebrallisten koko-

naislukujen renkaassa on mahdollista täsmälleen silloin kun kaikki renkaan ideaalit ovat pääideaaleja.

1 Lukuteoriaa

1.1 Jaollisuus

Olkoot $a \in \mathbb{Z}\backslash\{0\}$ ja $b \in \mathbb{Z}$. Sanotaan, että luku a jakaa luvun b, jos löytyy luku $c \in \mathbb{Z}$ siten, että $b = a \cdot c$. Tämä merkitään usein $a|b$. Sanotaan myös, että luku a on luvun b *tekijä*.

1.2 Suurin yhteinen tekijä

Olkoot $a, b \in \mathbb{Z}$ siten, että ainakin toinen luvuista eroaa nollasta. Lukujen a ja b *suurin yhteinen tekijä* on luku $n \in \mathbb{N},\ n > 0$, joka täyttää seuraavat ehdot:

1. $n|a$ ja $n|b$
2. jos jollekin $m \in \mathbb{N}$ on myös voimassa $m|a$ ja $m|b$, niin $n \geq m$.

Suurinta yhteistä tekijää merkitään $\text{syt}(a, b) = n$.

1.3 Alkuluvut

Lukua $p \in \mathbb{N},\ p > 0$ sanotaan *alkuluvuksi*, jos luvun p ainoat tekijät ovat 1 ja p. Jos luku ei ole alkuluku, niin sitä sanotaan *yhdistetyksi luvuksi*. Alkulukujen joukkoa merkitään $\mathbb{P}$:llä, eli

$$\mathbb{P} \coloneqq \{a\colon\ a \in \mathbb{N} \text{ on alkuluku}\}.$$

Seuraava määritelmä saattaa vaikuttaa aluksi hieman kummalliselta, mutta osoittautuu myöhemmin varsin oleelliseksi.

1.4 Loppuluvut

Lukua $e \in \mathbb{N}$ sanotaan *loppuluvuksi*, mikäli ehdosta $e|ab,\ a, b \in \mathbb{N}$ seuraa $e|a$ tai $e|b$ kaikille tuloille ab, joiden tekijä e on.

1.5 Suurimman yhteisen tekijän ominaisuuksia

Suurin yhteinen tekijä voidaan ilmaista myös lineaarikombinaationa. Jos $n = \text{syt}(a, b)$, niin löytyy kokonaisluvut x ja y siten, että

$$n = a \cdot x + b \cdot y.$$

Erityisesti $\text{syt}(a, b) = 1$ jos ja vain jos löytyy luvut $x, y \in \mathbb{Z}$ siten, että

$$1 = ax + by.$$

1.6 Eukleideen lemma

Jos p on alkuluku, $a, b \in \mathbb{Z}$ ja $p|ab$, niin $p|a$ tai $p|b$.

Todistus:

Jos $p|a$, niin todistus on valmis. Oletetaan siis ettei näin ole, joten

$$\text{syt}(a, p) = 1.$$

Täten joillakin $x, y \in \mathbb{Z}$ voidaan kirjoittaa luku 1 muodossa

$$1 = ax + py.$$

Kertomalla puolittain luvulla b, saadaan

$$b = abx + pby,$$

missä p jakaa yhtälön oikean puolen, joten sen täytyy myös jakaa vasen puoli, eli $p|b$.

Induktiolla voidaan todistaa yleisempi tulos, eli ehdosta $p|\prod_i a_i$ seuraa aina, että $p|a_j$ jollakin j.

1.7 Aritmetiikan peruslause

Olkoon $a \in \mathbb{Z}, a \geq 2$. Tällöin a voidaan esittää alkulukujen tulona järjestystä vaille yksikäsitteisesti.

Todistus:

1. *Olemassaolo*:
Selvästi tulos pätee kaikille luvuille $\{2, 3, \ldots, 10\}$. Tehdään vastaoletus: on olemassa ehdot täyttävä kokonaisluku, jota ei voi kirjoittaa alkulukujen tulona. Olkoon k pienin tällainen luku. Nyt k ei voi olla alkuluku, sillä tällöin se olisi itsensä tulo, joten sen täytyy olla yhdistetty luku. Täten löytyy luvut

$$1 < l < k \text{ ja } 1 < m < k$$

siten, että $k = l \cdot m$. Koska k oli pienin luku, jolla ei ole alkutekijäesitystä, täytyy luvuilla l ja m olla sellainen. Tällöin myös luvulla k on alkutekijäesitys, joten vastaoletuksen täytyy olla väärä.

2. *Yksikäsitteisyys*:
Oletetaan sitten, että n on pienin luku, jolla on kaksi eri alkutekijäesitystä,

$$n = \prod_{i=1}^{k} s_i = \prod_{j=1}^{l} r_j.$$

Eukleideen lemman nojalla s_k jakaa r_j:n jollakin $j \in \{1, ..., l\}$. Voidaan olettaa, että $s_k | r_l$, jolloin saadaan

$$\prod_{i=1}^{k-1} s_i = \prod_{j=1}^{l-1} r_j.$$

Koska n oletettiin pienimmäksi luvuksi, jolla on kaksi eri alkutekijäesitystä, täytyy olla (tarvittaessa järjestämällä termit uudelleen)

$$s_1 = r_1, \ldots, s_{k-1} = r_{k-1}, s_k = r_k,$$

joten n:llä on vain yksi alkutekijäesitys.

1.8 Aritmetiikan peruslause polynomeille

Aritmetiikan peruslause on voimassa myös K-kertoimisille polynomeille, kun K on kompleksilukujen kunnan $\mathbb{C}$ alikunta ([1] s. 38, Theorem 3.16). Jatkossa kuitenkin keskitytään luvuista koostuvien rakenteiden tutkimiseen.

1.9 Loppuluvuista

Eukleideen lemmasta seuraa suoraan, että kaikki alkuluvut ovat loppulukuja. Muunlaisia loppulukuja ei ole, sillä jos a on loppuluku ja sillä on jokin muu tekijä l, jolle $1 < l < a$, niin $a = k \cdot l$ jollekin $1 < k < a$. Tällöin kuitenkin $a | kl$, mutta a ei jaa kumpaakaan luvuista k ja l, mikä on ristiriitaista loppulukujen määritelmän kanssa.

On siis kaksi eri määritelmää, joista molemmista tulee ulos alkulukujen joukko, eli kokonaislukujen alkuluvut voitaisiin myös määritellä loppulukujen kautta. Näin ei yleensä tehdä, koska ns. perinteinen määritelmä

on itsessään varsin selkeä ja yksinkertainen. Yleisessä tilanteessa algebrallisille luvuille joudutaan kuitenkin suorittamaan alkulukujen määrittely nimemomaan loppulukujen kautta.

2 Algebraa

Algebran peruskäsitteet oletetaan tunnetuiksi, mutta tutkielman kannalta oleellisimmat rakenteet, kuten rengas ja kokonaisalue määritellään tässä luvussa. Lisäksi esitellään muutama hieman harvinaisempi algebrallinen rakenne, joihin ei perehdytä sen syvällisemmin. Ensimmäinen näistä on ns. *vapaa Abelin ryhmä*, jonka yhteys lineaarialgebraan on ilmeinen. Vapaat Abelin ryhmät ovat vain tukemassa tutkielmaa ja vapaiden Abelin ryhmien ominaisuuksista voi lukea lisää muualta [2].

2.1 Vapaa Abelin ryhmä

Olkoon G Abelin ryhmä ja $X = \{x_1, \ldots, x_n\}$ ryhmän G epätyhjä osajoukko. Jos jokainen $g \in G$ voidaan esittää yksikäsitteisesti muodossa

$$g = a_1x_1 + a_2x_2 + \ldots + a_nx_n,$$

missä $a_1, \ldots, a_n \in \mathbb{Z}$, niin ryhmää G sanotaan joukon X generoimaksi *vapaaksi Abelin ryhmäksi* ja joukkoa X sanotaan ryhmän G *kannaksi*.

$\mathbb{Z}$ on vapaa Abelin ryhmä, jonka kantoina ovat joukot $\{1\}$ ja $\{-1\}$, mutta $\mathbb{Z}_2$ ei ole, sillä sen ainoa mahdollinen kanta on $\{1\}$ ja

$$2 \cdot 1 + 1 \equiv 1 \pmod 2,$$

eli alkiolla 1 on useita eri esityksiä.

2.2 Vapaan Abelin ryhmän aste

Olkoon $G \neq \{0\}$ vapaa Abelin ryhmä, jonka kannassa X on äärellinen määrä alkioita. Tällöin jokainen ryhmän G kanta sisältää äärellisen määrän alkioita ja kaikissa kannoissa on täsmälleen sama määrä alkioita.

Todistus:

[3] s. 335, Theorem 38.6

Vapaan Abelin ryhmän kannan alkioiden lukumäärää kutsutaan ryhmän *asteeksi*.

2.3 Vapaan Abelin ryhmän osajoukot

Olkoon $G \neq \{0\}$ vapaa Abelin ryhmä, jonka aste on $n \in \mathbb{N}$ ja olkoon $K \neq \{0\}$ ryhmän G aliryhmä. Tällöin myös K on vapaa Abelin ryhmä asteenaan $s \leq n$. Löytyy myös kanta $\{x_1, \ldots, x_n\}$ ryhmälle G ja kokoelma kokonaislukuja $d_1, \ldots, d_s$, joille on voimassa, että luku d_i jakaa luvun d_{i+1} kaikille $i = 1, \ldots, s-1$ siten, että $\{d_1x_1, \ldots, d_sx_s\}$ on ryhmän K kanta.

Todistus:

[3] s. 337, Theorem 38.11

2.4 Rengas

Olkoon R joukko, jossa on määritelty laskutoimitukset $+$ ja $\cdot$. Kolmikkoa $(R, +, \cdot)$ sanotaan *renkaaksi*, jos

1. $(R, +)$ on Abelin ryhmä,
2. laskutoimitus $\cdot$ on liitännäinen ja
3. kaikille $a, b, c \in R$ osittelulait ovat voimassa, eli
   - $a \cdot (b + c) = a \cdot b + a \cdot c$
   - $(a + b) \cdot c = a \cdot c + b \cdot c$.

Jos renkaalla on kertolaskun suhteen neutraalialkio, sitä kutsutaan *ykkösalkioksi* ja merkitään 1_R. Rengasta $(R, +, \cdot)$ kutsutaan tällöin *ykköselliseksi renkaaksi*. Jos laskutoimitus $\cdot$ on vaihdannainen, niin $(R, +, \cdot)$ on *vaihdannainen rengas*.

2.4.1 Huomautus

Tässä tutkielmassa kaikki renkaat ovat ykkösellisiä ja vaihdannaisia, ellei erikseen mainita toisin.

2.5 Polynomirengas

Polynomit, joiden kertoimet kuuluvat renkaaseen R, muodostavat *polynomirenkaan* $R[t]$, jonka alkiot ovat siis yhden muuttujan polynomeja

$$p(t) = a_0 + a_1t + a_2t^2 + \ldots + a_nt^n,$$

missä $a_0, \ldots, a_n \in Ra_0, \ldots, a_n \in R$.

2.6 Kokonaisalue

Rengas R on *kokonaisalue*, jos $1_R \neq 0_R$ ja jos renkaassa ei ole *nollan tekijöitä*, eli ehdosta $a, b \in R\backslash\{0\}$ seuraa $ab \neq 0$. Ehto $1_R \neq 0_R$ tarkoittaa sitä, että kokonaisalueessa on aina vähintään kaksi alkiota.

2.7 Kunta

Kokonaisalue D on *kunta*, mikäli kaikilla nollasta eroavilla alkioilla on käänteisalkio kertolaskun suhteen.

2.8 Moduli

Olkoon R rengas. Abelin ryhmää $(M, +)$ ja operaatiota $R \times M \to M$, jossa kaikille $r, s \in R$ ja $m, n \in M$ pätee

1. $(r + s)m = rm + sm$,
2. $r(m + n) = rm + rn$,
3. $r(sm) = (rs)m$,
4. $1m = m$,

sanotaan R-*moduliksi*.

Ryhmän M aliryhmää N, jossa kaikilla $n \in N$ ja $r \in R$ pätee $rn \in N$, kutsutaan ryhmän M-*alimoduliksi*.

2.9 Ideaali

Renkaan R epätyhjä osajoukko I on *ideaali*, jos

1. $r - s \in I$ kaikille joukon I alkioille r ja s ja
2. $rs \in I$ aina kun $r \in I$ ja $s \in R$.

2.9.1 Huomautus

Renkaan R ideaali I on siis myös renkaan R alirengas, jos renkaalta R ei vaadita ykkösellisyyttä, tai jos renkaan R alirenkailta ei vaadita ykkösellisyyttä. Erityisesti ideaalin I voi käsittää R-*alimoduliksi*.

2.10 Tekijärengas

Jos R on rengas ja I on sen ideaali, niin sivuluokkarengasta $(R/I, +, \cdot)$ kutsutaan R:n tekijärenkaaksi ja sen alkiot ovat sivuluokat $I + r$, missä $r \in R$. Laskutoimitukset määritellään

$$(I + r) + (I + s) = I + (r + s)$$
$$(I + r) \cdot (I + s) = I + rs$$

kaikille $r, s \in R$.

2.11 Ideaalin normi

Olkoon R rengas ja I sen ideaali. Tällöin

$$N(I) = |R/I|,$$

eli tekijärenkaan R/I alkioiden lukumäärä, on ideaalin I *normi*. Esimerkiksi renkaassa $\mathbb{Z}$ ideaalin $2\mathbb{Z}$ normi

$$N(2\mathbb{Z}) = |\mathbb{Z}/2\mathbb{Z}| = |\{0_2, 1_2\}| = 2.$$

2.12 Lemma

Jos I ja J ovat renkaan R nollasta eroavia ideaaleja, niin

$$N(IJ) = N(I)N(J).$$

Todistus:

[4] Theorem 4.2.7

2.13 Pääideaali

Renkaan R alkion a virittämä joukko

$$\langle a \rangle = aR = \{ar : r \in R\}$$

muodostaa renkaan R ideaalin, ns. *pääideaalin*.

2.14 Pääideaalikokonaisalue (principal ideal domain)

Kokonaisaluetta D, jonka kaikki ideaalit ovat pääideaaleja, kutsutaan *pääideaalikokonaisalueeksi* ja lyhennetään tarpeen tullen termiksi PIKA (engl. PID)

2.15 Algebralliset luvut ja algebralliset kokonaisluvut

Lukua $a \in \mathbb{C}$ sanotaan *algebralliseksi luvuksi*, jos on olemassa jokin rationaalilukukertoiminen polynomi, jonka nollakohta a on, eli

$$p_n a^n + p_{n-1} a^{n-1} + \ldots + p_1 a + p_0 = 0,$$

missä $p_i \in \mathbb{Q}$ kaikilla $i = 0, \ldots, n-1$. Algebralliset luvut muodostavat kunnan $\mathbb{C}$ alikunnan ([5] s. 36, Theorem 2.1) ja algebrallisten lukujen joukkoa merkitään $\mathbb{A}$:lla.

Vastaavasti lukua $b \in \mathbb{C}$ sanotaan *algebralliseksi kokonaisluvuksi*, jos se toteuttaa perusmuotoisen (engl. monic, eli korkeimman asteen kerroin 1) kokonaislukukertoimisen polynomin, eli

$$b^n + q_{n-1} b^{n-1} + \ldots + q_1 b + q_0 = 0,$$

missä $q_i \in \mathbb{Z}$ kaikilla $i = 0, \ldots, n-1$. Algebralliset kokonaisluvut muodostavat algebrallisten lukujen alirenkaan ([5] s. 43, Theorem 2.9) ja algebrallisten kokonaislukujen joukkoa merkitään $\mathbb{B}$:llä.

2.16 Algebrallisten lukujen polynomit

Jos $\theta \in \mathbb{C}$ toteuttaa perusmuotoisen polynomiyhtälön, jossa polynomin kertoimet ovat algebrallisia kokonaislukuja, niin myös θ on algebrallinen kokonaisluku.

Todistus:

[5] s. 43, Theorem 2.10

2.17 Kokonaislukukanta

Olkoon K lukukunnan $\mathbb{Q}$ n-asteinen laajennos, eli $K = \mathbb{Q}(\theta)$, missä θ on algebrallinen kokonaisluku. Tällöin kunnan K $\mathbb{Q}$-kanta on se kanta, joka joukolla K on $\mathbb{Q}$-vektoriavaruutena. Kunnalla K tämä kanta on n-asteinen, sillä

$$\{1, \theta, \ldots, \theta^{n-1}\}$$

on joukon K kanta.

Jonkin tietyn *lukukunnan* K (eli $K = \mathbb{Q}(\theta)$, missä $\theta \in \mathbb{B}$) *algebrallisten kokonaislukujen rengas* $\mathfrak{O}_K$ määritellään

$$\mathfrak{O}_K = K \cap \mathbb{B}.$$

Mikäli kunta K on asiayhteydestä selvä, niin lyhennetään merkintä $\mathfrak{O}$:ksi.

Lukukunnan K algebrallisten lukujen rengas $\mathfrak{O}_K$ on Abelin ryhmä yhteenlaskun suhteen ja ryhmän $(\mathfrak{O}_K, +)$ $\mathbb{Z}$-kantaa kutsutaan kunnan K *kokonaislukukannaksi*. Siis $\{\alpha_1, \ldots, \alpha_s\}$ on kokonaislukukanta jos ja vain jos jokainen luku α_i on joukossa $\mathfrak{O}$ ja jokainen ryhmän $\mathfrak{O}$ alkio voidaan kirjoittaa muodossa

$$a_1\alpha_1 + \ldots + a_s\alpha_2,$$

missä $a_1, \ldots, a_s \in \mathbb{Z}$.

2.18 Lukukunnan kokonaislukukanta

Jokaisella lukukunnalla K on olemassa kokonaislukukanta ja ryhmä $(\mathfrak{O}_K, +)$ on astetta n oleva vapaa Abelin ryhmä, missä n on sama kuin lukukunnan K aste.

Todistus:

[5] s. 46, Theorem 2.16

2.19 Kuvauksia ja normi

Olkoot $(R, +, \cdot)$ ja $(S, \oplus, \odot)$ renkaita. Kuvausta $f\colon R \to S$ sanotaan *rengashomomorfismiksi*, jos se toteuttaa ehdot

1. $f(a + b) = f(a) \oplus f(b)$ ja
2. $f(a \cdot b) = f(a) \odot f(b)$

kaikille $a, b \in R$. Mikäli kuvaus f on myös *injektio*, kutsutaan kuvausta f *rengasmonomorfismiksi*.

Algebrallisten lukujen *normi* määritellään monomorfismien avulla. Olkoot $K = \mathbb{Q}(\theta)$ lukukunta astetta n, jolloin löytyy siis n erillistä monomorfismia kunnalta K kunnalle $\mathbb{C}$ ([5] s.38, Theorem 2.4), $\sigma_1, \ldots, \sigma_n$. Nyt kaikille $\alpha \in K$ määritellään normiksi

$$N_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

2.19.1 Huomautus

Koska normi on määritelty monomorfismien avulla, niin saadaan siis ”ilmaiseksi” tulos

$$N(ab) = N(a)N(b),$$

kun a ja b ovat algebrallisia lukuja ja jos $a \neq 0$, niin myös $N(a) \neq 0$.

Eräs tärkeä ominaisuus on myös, että jos $a \in \mathbb{B}$, niin $N(a) \in \mathbb{Z}$. [5]

2.20 Esimerkki

Kunnan $\mathbb{Q}$ toisen asteen kuntalaajennuksia sanotaan *kvadraattisiksi kunniksi* (engl. quadratic fields). Tällaiset laajennukset ovat muotoa

$$K = \mathbb{Q}(\sqrt{d}),$$

missä $d \in \mathbb{Z}$ on neliövapaa (eli ei ole jaollinen millään neliöluvulla) ja toisen asteen kuntalaajennukselle löytyy kaksi monomorfismia $K \to \mathbb{C}$

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$$
$$\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}.$$

Jos nyt $K = \mathbb{Q}(\sqrt{11})$, niin

$$\sigma_1(a + b\sqrt{11}) = a + b\sqrt{11}$$
$$\sigma_2(a + b\sqrt{11}) = a - b\sqrt{11}.$$

ja

$$N(a + b\sqrt{11}) = (a + b\sqrt{11}) \cdot (a - b\sqrt{11}) = a^2 - 11b^2.$$

Myöhemmin osoittautuu hyödylliseksi tietää, millaisia kunnan $\mathbb{Q}(\sqrt{d})$, missä d on neliövapaa, algebrallisten lukujen renkaat ovat.

2.21 Kvadraattisten kuntien algebralliset luvut

Olkoon d neliövapaa kokonaisluku. Tällöin lukukunnan $\mathbb{Q}(\sqrt{d})$ algebralliset kokonaisluvut ovat:

1. $\mathbb{Z}(\sqrt{d})$, jos $d \not\equiv 1 \pmod 4$

2. $\mathbb{Z}(\frac{1}{2} + \frac{1}{2}\sqrt{d})$, jos $d \equiv 1 \pmod 4$.

Todistus:

[5] s. 62, Theorem 3.2

3 Kokonaisalueiden ominaisuuksia

Kokonaisalueet ovat jatkon kannalta tärkeitä, joten niihin on syytä paneutua hieman tarkemmin. Tässä kappaleessa R viittaa renkaisiin ja D kokonaisalueisiin, ellei toisin mainita.

3.1 Yksikkö

Alkiota $a \in R$ sanotaan *yksiköksi*, jos on olemassa $b \in R$ siten, että

$$ab = 1.$$

Tällöin tietenkin myös b on yksikkö ja jos $ac = 1$, niin

$$c = 1 \cdot c = ab \cdot c = bac = b \cdot 1 = b.$$

Yksikkö tarkoittaa siis alkiota, jolle löytyy käänteisalkio kertolaskun suhteen. Esim. renkaassa $(\mathbb{Z}, +, \cdot)$ on kaksi yksikköä, 1 ja -1 ja renkaissa $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ ja $(\mathbb{C}, +, \cdot)$ kaikki muut alkiot paitsi 0 ovat yksiköitä. Yksiköt ovat siis kaikkien renkaan alkioiden tekijöitä, sillä jos c on renkaan R alkio ja a kyseisen renkaan yksikkö, niin

$$c = 1 \cdot c = ab \cdot c.$$

3.2 Liittoalkio

Alkiota $b \in R$ sanotaan alkion $a \in R$ *liittoalkioksi*, jos $a = ub$ jollakin yksiköllä $u \in R$. Jos u on yksikkö, niin aina pätee $a = ub$, kun asetetaan $b = u^{-1}a$. Renkaassa $(\mathbb{R}, +, \cdot)$ alkiolla π esimerkiksi liittoalkiona e, sillä

$$\pi/e \cdot e = \pi$$

ja π/e on kyseisessä renkaassa yksikkö. Toisaalta alkiolla 0 on vain yksi liittoalkio, nimittäin 0 itse. Tästä voidaan havaita, että liittoalkioita, kuten myös yksiköitä, voi olla jopa ylinumeroituvasti.

3.3 Jaoton luku

Luku $p \in R \backslash \{0\}$ on *jaoton*, jos ehdosta $p = ab$ seuraa, että joko a on yksikkö tai b on yksikkö.

Kokonaislukujen renkaassa alkuluvut ovat jaottomia lukuja ja muita jaottomia ei ole. Toisaalta ja algebrallisten lukujen renkaassa ei ole jaottomia lukuja, sillä jos x ei ole nolla-alkio tai yksikkö, niin myöskään $\sqrt{x}$ ei ole nolla-alkio tai yksikkö ja $x = \sqrt{x} \cdot \sqrt{x}$.

3.4 Alkuluku

Luku $p \in R\backslash\{0\}$ on *alkuluku*, mikäli ehdosta $p|ab,\ a, b \in R$ aina seuraa, että $p|a$ tai $p|b$.

Jaoton luku on siis määritelty kuten alkuluvut johdannossa ja alkuluvut taas kuten loppuluvut. Johdannossa nähtiin, että kokonaislukujen joukossa, eli oikeastaan kokonaislukujen renkaassa, alkuluvut ja loppuluvut ovat sama asia. Alkuluvut ovat kyllä aina myös jaottomia, mutta kaikki jaottomat luvut eivät välttämättä ole alkulukuja kaikissa renkaissa.

3.5 Alkuluvut ovat jaottomia lukuja

Jos $p \in D$ on alkuluku, niin p on jaoton luku, mutta jaoton luku ei välttämättä ole alkuluku.

Todistus:

Olkoon $p \in D$ alkuluku. Tällöin jos $p = ab$ joillekin luvuille $a, b \in D$, niin alkulukujen määritelmän nojalla $p|a$ tai $p|b$. Voidaan olettaa, että $p|a$, jolloin siis $a = pc$ jollakin luvulla $c \in D$. Sijoittamalla tämä aiempaan yhtälöön, saadaan

$$p = ab = pcb,$$

joten $1 = cb$, koska kokonaisalueessa ei ole nollan tekijöitä ja oletuksen nojalla $p \neq 0$. Siten b on yksikkö, eli p on jaoton.

Väitteen toisen osan todistamiseksi riittää löytää jaoton luku, joka ei ole alkuluku. Siirretään tarkastelu renkaaseen

$$\mathbb{Z}(\sqrt{-3}) = \{a + b\sqrt{-3} \colon a, b \in \mathbb{Z}\}.$$

Nyt esimerkiksi luku 2 on jaoton, sillä jos

$$2 = (a + b\sqrt{-3}) \cdot (c + d\sqrt{-3}),$$

missä $a, b, c, d \in \mathbb{Z}$, niin saman täytyy päteä myös jos otetaan kompleksikonjugaatti molemmilta puolilta yhtälöä, eli

$$2 = (a - b\sqrt{-3}) \cdot (c - d\sqrt{-3}).$$

Kerrotaan nämä kaksi yhtälöä keskenään, jolloin saadaan

$$4 = (a^2 + 3b^2) \cdot (c^2 + 3d^2).$$

Molempien yhtälöiden oikealla puolella olevien tekijöiden pitää siis jakaa luku 4, eli $(a^2 + 3b^2)|4$. Koska luvun 4 kokonaislukutekijät ovat $1, 2$ ja 4, eikä $a^2 + 3b^2$ voi olla 2 millään kokonaisluvuilla a ja b niin toinen luvun 4 tekijöistä on 1 ja toinen on 4. Jos

$$a^2 + 3b^2 = 1,$$

niin $a = \pm 1$ ja $b = 0$, joten alkuperäisessä luvun 2 tekijöihinjaossa

$$2 = (a + b\sqrt{-3}) \cdot (c + d\sqrt{-3})$$

toinen tekijä on siis yksikkö 1, eli 2 on jaoton.

Renkaassa $\mathbb{Z}(\sqrt{-3})$ luku 2 jakaa luvun

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4,$$

joten jos luku 2 olisi alkuluku, niin sen pitäisi jakaa toinen luvun 4 tekijöistä, jolloin joudutaan tilanteeseen $2|1$, mikä ei ole mahdollista. Luku 2 ei siis ole alkuluku renkaassa $\mathbb{Z}(\sqrt{-3})$.

Palataan sitten tarkastelemaan hieman yksiköiden ja liittoalkioiden perusominaisuuksia.

3.6 Yksiköistä ja liittoalkioista

Kokonaisalueessa D on voimassa:

(a) a on yksikkö täsmälleen silloin kun $a|1$
(b) mielivaltaiset kaksi yksikköä ovat keskenään liittoalkioita ja mielivaltaisen yksikön liittoalkio on aina yksikkö
(c) a ja b ovat liittoalkioita jos ja vain jos $a|b$ ja $b|a$
(d) a on jaoton aina ja vain kun kaikki luvun a jakajat ovat luvun a liittoalkioita tai yksiköitä
(e) jaottoman luvun liittoalkio on jaoton

Todistus:

(a) Oletetaan ensin, että a on yksikkö. Tällöin löytyy b siten, että $ab = 1$, eli $a|1$.

Oletetaan sitten, että $a|1$. Tällöin taas löytyy b siten, että $ab = 1$, eli a

on yksikkö.

(b) Olkoot a ja b yksiköitä, jolloin siis on olemassa yksiköt c ja d siten, että

$$ac = 1 = bd.$$

Täten siis $ac = bd$ ja kertomalla puolittain yksikön d käänteisalkiolla saadaan

$$a \cdot (c \cdot d^{-1}) = b,$$

missä cd^{-1} on kahden yksikön tulona yksikkö, sillä jos

$$ac = 1 \text{ ja } bd = 1,$$

niin $(cd) \cdot (ab) = 1$. Siten yhtälöstä

$$a \cdot (c \cdot d^{-1}) = b$$

seuraa, että b on alkion a liittoalkio.

Oletetaan sitten, että a on yksikkö ja b sen liittoalkio. Tällöin löytyy yksikkö u siten, että

$$a = ub, \text{ joten } 1 = (u \cdot a^{-1}) \cdot b,$$

eli myös b on yksikkö.

(c) Jos a ja b ovat liittoalkioita, niin $a = ub$, missä u on yksikkö, eli $b = la$, missä $l = u^{-1}$, joten $a|b$ ja $b|a$.

Jos taas $a|b$ ja $b|a$, niin $b = ka$ ja $a = lb$, joten $b = klb$. Jos $a = 0$, niin myös $b = 0$, jolloin ne ovat triviaalisti liittoalkioita. Jos taas $a \neq 0$, niin ehdosta

$$b = klb$$

seuraa $1 = kl$, eli k ja l ovat yksiköitä, joten a ja b ovat liittoalkioita.

(d) Jos d on jaoton luku ja $d = ab$ joillekin $a, b \in D$, niin jaottoman luvun määritelmän perusteella toinen luvuista a tai b on yksikkö.

Jos kaikki jakajat ovat yksiköitä, niin väite seuraa määritelmästä. Jos b on alkion a liittoalkio ja $b|a$, niin $a = ub$, missä u on yksikkö, jolloin väite seuraa taas määritelmästä.

(e) Olkoon a jaoton ja b alkion a liittoalkio, eli $a = ub$, missä u on yksikkö. Tällöin $b = u^{-1}a$, missä u^{-1} on yksikkö, eli myös b on jaoton.

3.7 Yksiköt, liittoalkiot ja ideaalit

Jos D on kokonaisalue ja $a, b \in D$, $a, b \neq 0$, niin

(a) $a|b$ jos ja vain jos $\langle a \rangle \supseteq \langle b \rangle$
(b) a ja b ovat liittoalkioita täsmälleen silloin kun $\langle a \rangle = \langle b \rangle$
(c) a on yksikkö aina ja vain kun $\langle a \rangle = D$
(d) a on jaoton silloin ja vain silloin kun $\langle a \rangle$ on kokonaisalueen D maksimaalinen aito pääideaali.

Todistus:

Olkoot $a, b \in D$.
(a) Koska $a|b$, niin b voidaan esittää muodossa $b = a \cdot s \in \langle a \rangle$, missä $s \in D$. Nyt jos $x \in \langle b \rangle = \langle a \cdot s \rangle$, niin $x \in \langle a \rangle$ ja siten $\langle b \rangle \subseteq \langle a \rangle$.

Oletetaan sitten, että $\langle b \rangle \subseteq \langle a \rangle$, jolloin kun $b \in \langle a \rangle$, niin löytyy $s \in D$ siten, että $b = a \cdot s$.

(b) Jos a ja b ovat liittoalkioita, niin kohdan 3.6 (c) nojalla $a|b$ ja $b|a$, jolloin siis $\langle a \rangle \subseteq \langle b \rangle$ ja $\langle b \rangle \subseteq \langle a \rangle$.

Jos taas $\langle a \rangle = \langle b \rangle$, niin (a)-kohdan nojalla $a|b$ ja $b|a$ ja kohdan 3.6 (c) nojalla a ja b ovat liittoalkioita.

(c) Olkoon a yksikkö, jolloin $ab = 1$ jollakin $b \in D$. Olkoon $c \in D$, jolloin $c = abc$, eli $c \in \langle a \rangle$.

Olkoon $\langle a \rangle = D$, jolloin $1 \in \langle a \rangle$, eli $1 = ab$ jollakin $b \in D$, joten a on yksikkö.

(d) Olkoon a jaoton. Jos olisi $b \in D$ siten, että

$$\langle a \rangle \subsetneq \langle b \rangle \subsetneq D,$$

niin (a)-kohdan nojalla $b|a$, mutta b ei voi olla alkion a liittoalkio, sillä tällöin olisi $\langle a \rangle = \langle b \rangle$, eikä b ole yksikkö, koska (c)-kohdan mukaan tällöin olisi $\langle b \rangle = D$. Alkion b olemassaolo siis tuottaa ristiriidan kohdan 3.6 (d) kanssa.

Olkoon sitten $\langle a \rangle$ maksimaalinen. Nyt jos $b|a$, niin $\langle a \rangle \subseteq \langle b \rangle$, eli joko b

on alkion a liittoalkio, jolloin

$$\langle a \rangle = \langle b \rangle,$$

tai b on yksikkö, jolloin

$$\langle b \rangle = D,$$

muutoin $\langle a \rangle \subsetneqq \langle b \rangle \subsetneqq D$, mikä on vastoin oletusta. Nyt kohdan 3.6 (a) nojalla a on jaoton.

3.8 Noetherilainen kokonaisalue

Jos kokonaisalueen D kaikilla ideaaleilla on äärellinen määrä virittäjiä, niin sanotaan, että D on *noetherilainen*.

3.9 Kasvavan jonon ehto (ascending chain condition)

Olkoot

$$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

kasvava jono ideaaleja. Jos tällöin löytyy $N \in \mathbb{N}$ siten, että $I_n = I_N$ kaikilla $n \geq N$, eli kasvu pysähtyy, niin sanotaan, että *kasvavan jonon ehto* täyttyy.

3.10 Maksimaalisuusehto (the maximal condition)

Jos ei-tyhjällä kokoelmalla ideaaleja on maksimaalinen alkio, joka ei sisälly mihinkään muuhun joukon ideaaliin, niin sanotaan, että *maksimaalisuusehto* täyttyy.

Huom. Maksimaalisen ideaalin ei tarvitse sisältää kaikkia muita kokoelman ideaaleja, riittää ettei joukossa ole yhtään ideaalia, joka sisältäisi maksimaalisen ideaalin.

3.11 Noetherilaisuus, kasvavan jonon ehto ja maksimaalisuusehto

Algebrallisten kokonaislukujen kokonaisalueessa D seuraavat ovat yhtäpitäviä:

(a) D on noetherilainen
(b) Kasvavan jonon ehto on voimassa kokonaisalueessa D

(c) Maksimaalisuusehto on voimassa kokonaisalueessa D.

Todistus:

Olkoon D noetherilainen ja

$$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

kasvava jono ideaaleja. Olkoon

$$I = \bigcup_{i=1}^{\infty} I_i,$$

jolloin I on sisäkkäisten ideaalien yhdisteenä ideaali ja sillä on äärellinen määrä virittäjiä. Olkoot ne

$$I = \langle x_1, \ldots, x_m \rangle.$$

Nyt jokainen x_j kuuluu johonkin ideaaliin I_i. Olkoon $N \in \mathbb{N}$ sellainen, että

$$x_j \in \bigcup_{i=1}^{N} I_i$$

kaikilla $j \in \{1, \ldots, m\}$. Nyt siis $I = I_N$ ja siten $I_n = I_N$ kaikilla $n \geq N$, eli kasvavan jonon ehto toteutuu.

Olkoon sitten D sellainen, että se toteuttaa kasvavan jonon ehdon. Olkoon $S \neq \emptyset$ joukko ideaaleja. Tehdään vastaoletus: joukossa S ei ole maksimaalista alkiota. Olkoon $I_0 \in S$. Koska I_0 ei ole maksimaalinen, voidaan valita $I_1 \in S$ siten, että $I_0 \subsetneq I_1$. Induktiolla päästään I_n:ään, joka ei myöskään ole maksimaalinen, joten voidaan valita $I_{n+1} \in S$ siten, että $I_n \subsetneq I_{n+1}$. On siis saatu kasvava jono ideaaleja, joiden kasvu ei kuitenkaan pysähdy. Tämä on vastoin oletusta.

Olkoon D sellainen, että maksimaalisuusehto toteutuu. Olkoon I jokin ideaali ja S joukko, joka sisältää kaikki äärellisesti viritetyt ideaalit, jotka sisältyvät ideaaliin I. Tällöin ainakin $\{0\} \in S$, joten $S \neq \emptyset$ ja sisältää siten maksimaalialkion J. Jos $J \neq I$, niin valitaan $x \in I \backslash J$, jolloin $\langle J, x \rangle$ on äärellisesti viritetty ja $J \subsetneq \langle J, x \rangle$, mikä on ristiriitaista alkion J maksimaalisuuden kanssa, joten täytyy olla $J = I$ ja I on äärellisesti viritetty.

3.12 Noetherilaisen kokonaisalueen tekijöihinjako

Jos kokonaisalue D on noetherilainen, niin kokonaisaluueessa D on mahdollista esittää luvut jaottomien lukujen tulona.

Todistus:

Vastaoletus: Löytyy jokin $a \in D\backslash\{0\}$ siten, että a ei ole yksikkö, luvulle a ei ole olemassa esitystä jaottomien lukujen tulona ja a on valittu niin, että $\langle a \rangle$ on maksimaalinen (maksimaalisuusehdon mukaan mahdollista).
Nyt a ei voi olla jaoton, sillä muuten se olisi esitettävissä "itsensä tulona", joten täytyy olla alkiot $b, c \in D$, joille $a = bc$ ja kumpikaan b tai c eivät ole yksiköitä. Kohdan 3.7 (a) nojalla tästä seuraa, että $\langle a \rangle \subseteq \langle b \rangle$, mutta jos olisi $\langle a \rangle = \langle b \rangle$, niin kohdan 3.7 (b) nojalla a ja b olisivat liittoalkioita, jolloin c olisi yksikkö. Täten siis $\langle a \rangle \subsetneqq \langle b \rangle$ ja $\langle a \rangle \subsetneqq \langle c \rangle$. Koska $\langle a \rangle$ valittiin maksimaaliseksi, täytyy olla

$$b = k_1 \cdot \ldots \cdot k_n$$
$$c = l_1 \cdot \ldots \cdot l_m,$$

missä k_i:t ja l_j:t ovat jaottomia. Nyt

$$a = b \cdot c = k_1 \cdot \ldots \cdot k_n \cdot l_1 \cdot \ldots \cdot l_m,$$

eli a on esitettävissä jaottomien lukujen tulona, mikä on vastoin vastaoletusta.

3.13 Algebrallisten kokonaislukujen joukko on noetherilainen

Lukukunnan K algebrallisten kokonaislukujen joukko $\mathfrak{O}$ on noetherilainen.

Todistus:

Osoitetaan, että jokainen ideaali $I \subset \mathfrak{O}$ on äärellisesti viritetty. Nyt $(\mathfrak{O}, +)$ on vapaa Abelin ryhmä, jonka kertaluku n on sama kuin lukukunnan K kertaluku kohdan 2.18 nojalla. Täten kohdan 2.3 nojalla $(I, +)$ on vapaa Abelin ryhmä kertalukunaan $s \leq n$. Jos $\{x_1, \ldots, x_s\}$ on ryhmän $(I, +)$ $\mathbb{Z}$-kanta, niin tällöin

$$\langle x_1, \ldots, x_s \rangle = I,$$

joten I on äärellisesti viritetty ja $\mathfrak{O}$ on noetherilainen.

Yhdistämällä kaksi edellistä lausetta, havaitaan tekijöihinjaon jaottomiin lukuihin olevan aina mahdollista renkaassa $\mathfrak{O}$.

3.14 Normin ominaisuuksia

Olkoon $\mathfrak{O}$ lukukunnan K algebrallisten kokonaislukujen rengas ja olkoot $x, y \in \mathfrak{O}$. Tällöin on voimassa:

(1) x on yksikkö täsmälleen silloin, kun $N(x) = \pm 1$ (tässä $N(x)$ on siis luvun x normi).
(2) Jos x ja y ovat liittoalkioita, niin $N(x) = \pm N(y)$.
(3) Jos $N(x) \in \mathbb{P}$, niin x on jaoton renkaassa $\mathfrak{O}$.

Todistus:

(1) Jos $xu = 1$, niin

$$N(xu) = N(x)N(u) = N(1) = 1.$$

Koska $N(x), N(u) \in \mathbb{Z}$, niin $N(x) = \pm 1$.

Jos taas $N(x) = \pm 1$, niin

$$\sigma_1(x)\sigma_2(x)\cdots\sigma_n(x) = \pm 1,$$

missä kuvaukset σ_i ovat monomorfismit lukukunnalta K lukukuntaan $\mathbb{C}$. Yksi monomorfismeista on siis identtinen kuvaus $\sigma(x) = x$ ja muut kuvaavat luvun x algebralliselle luvulle. Voidaan olettaa, että $\sigma_1(x) = x$. Asetetaan

$$u = \pm\sigma_2(x)\cdots\sigma_n(x),$$

jolloin $xu = 1$, joten $u = x^{-1} \in K$. Siten $u \in K \cap \mathbb{B} = \mathfrak{O}$ ja x on yksikkö.

(2) Jos x ja y ovat liittoalkioita, niin $x = uy$, missä u on yksikkö, joten edellisen kohdan nojalla

$$N(x) = N(uy) = N(u)N(y) = \pm N(y).$$

(3) Olkoon $x = yz$. Tällöin

$$N(y)N(z) = N(yz) = N(x) = p \in \mathbb{P},$$

joten yksi luvuista $N(y)$ ja $N(z)$ on $\pm p$ ja toinen on ± 1. Ensimmäisen kohdan nojalla toinen luvuista y ja z on yksikkö, joten x on jaoton.

3.15 Yksikäsitteinen tekijöihinjako

Tekijöihinjako kokonaisalueessa D on yksikäsitteistä, jos ehdosta

$$p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s,$$

missä jokainen p_i ja q_j on jaoton kokonaisalueessa D, seuraa

1. $r = s$

2. On olemassa permutaatio π joukossa $\{1, \ldots, r\}$ siten, että p_i ja $q_{\pi(i)}$ ovat liittoalkioita kaikille $i \in \{1, \ldots, r\}$.

Määritelmä on siis vain yleistys kokonaislukujen vastaavasta määritelmästä ja toimii myös kokonaisluvuille, sillä kokonaislukujen ainoat yksiköt ovat 1 ja -1. Toistaiseksi on tarkasteltu yksikäsitteistä tekijöihinjakoa ainoastaan kokonaislukujen renkaassa ja todettu, että yksikäsitteinen tekijöihinjako onnistuu myös polynomirenkaassa. Kuten kokonaisluvuille tehdyn todistuksen yksinkertaisuudesta voi päätellä, tulos oli tuttu jo antiikin kreikkalaisille. Muissa renkaissa asiaa ei ilmeisesti juurikaan tutkittu ennen 1800-luvun puoliväliä, jolloin *Gabriel Lamé* väitti todistaneensa Fermat'n suuren lauseen käyttäen hyväkseen yksikköjuurten (engl. roots of unity) tekijöihinjaon yksikäsitteisyyttä. *Ernst Kummer* oli kuitenkin todistanut paria vuotta aiemmin, että kokonaisalueessa $\mathbb{Z}[\alpha]$, missä

$$\alpha^{23} = 1,\ \alpha \in \mathbb{C}$$

yksikäsitteinen tekijöihinjako ei onnistu. Helpompiakin esimerkkejä onneksi löytyy.

3.16 Esimerkki

Tekijöihinjako yksikäsitteisesti ei ole mahdollista kokonaisalueen $\mathbb{Q}(\sqrt{-10})$ algebrallisten kokonaislukujen renkaassa.

Todistus:

Kokonaisalueessa $\mathbb{Q}(\sqrt{-10})$ on voimassa

$$14 = 2 \cdot 7 = (2 + \sqrt{-10}) \cdot (2 - \sqrt{-10}).$$

Osoitetaan, että $2, 7, 2 + \sqrt{10}$ ja $2 - \sqrt{-10}$ ovat jaottomia joukon $\mathbb{Q}(\sqrt{-10})$ algebrallisten lukujen renkaassa $\mathfrak{O}$. Normina on algebrallinen normi, eli

$$N(a + b\sqrt{-10}) = a^2 + 10b^2,$$

joten

$$N(2) = 4, N(7) = 49, N(2 + \sqrt{-10}) = 14 \text{ ja } N(2 - \sqrt{-10}) = 14.$$

Jos luvulle 2 löytyisi epätriviaalit tekijät, eli $2 = xy$, missä $x, y \in \mathfrak{O}$ ovat ei-yksiköitä, niin

$$4 = N(2) = N(x)N(y),$$

joten koska $N(x), N(y) \in \mathbb{Z}$, niin

$$N(x) = \pm 2 = N(y),$$

sillä vain yksikön normi voi olla ± 1.

Vastaavasti luvun 7 epätriviaalien tekijöiden normit ovat ± 7, sekä lukujen $2 + \sqrt{-10}$ ja $2 - \sqrt{-10}$ epätriviaalien tekijöiden normit ovat ± 2 ja ± 7. Koska $-10 \not\equiv 1 \pmod 4$, niin kohdan 2.21 nojalla algebralliset luvut ovat muotoa

$$a + b\sqrt{-10},\ a, b \in \mathbb{Z},$$

joten päädytään yhtälöihin

$$a^2 + 10b^2 = \pm 2 \text{ tai}$$
$$a^2 + 10b^2 = \pm 7.$$

Jos $|b| \geq 1$, niin $|a^2 + 10b^2| \geq 10$, joten täytyy olla $|b| = 0$, jolloin päädytään tilanteeseen $a^2 = \pm 2$ tai $a^2 = \pm 7$, mikä on mahdotonta joukon $\mathbb{Z}$ alkioille. Siten oletettuja jakajia ei voi olla olemassa, joten kaikki neljä lukua ovat jaottomia. Koska

$$N(2) = 4 \text{ ja } N(2 \pm \sqrt{-10}) = 14,$$

niin kohdan 3.14 (b) nojalla 2 ei ole lukujen $2 \pm \sqrt{-10}$ liittoalkio, joten tekijöihinjako ei ole yksikäsitteistä.

3.17 Ehto tekijöihinjaon yksikäsitteisyydelle

Jos kokonaisalueessa tekijöihinjako jaottomiin lukuihin on mahdollista kaikille alkioille, niin tekijöihinjako on yksikäsitteinen täsmälleen silloin kun kaikki jaottomat luvut ovat alkulukuja.

Todistus:

Olkoon D ko. kokonaisalue. Ilmaistaan alkio $a \in D$ jaottomien lukujen tulona

$$a = up_1 \cdot \ldots \cdot p_r,$$

missä u on yksikkö ja luvut $p_1, \ldots, p_r$ jaottomia (up_1 on siis jaoton tapauksessa $r \geq 1$).

Olkoon nyt $p \in D$ jaoton. Jos $p|ab$, niin on olemassa $c \in D$ siten, että $pc = ab$ (jaollisuuden määritelmä). Voidaan olettaa, että $a \neq 0 \neq b$, jolloin myös $c \neq 0$ (kokonaisalue). Ilmaistaan a, b ja c jaottomien tulona

$$a = u_1 p_1 \cdots p_n$$
$$b = u_2 q_1 \cdots q_m$$
$$c = u_3 r_1 \cdots r_s,$$

missä luvut u_i ovat yksiköitä ja luvut p_i, q_i ja r_i jaottomia, joten

$$p \cdot (u_3 r_1 \cdots r_s) = (u_1 p_1 \cdots p_n) \cdot (u_2 q_1 \cdots q_m)$$

Koska tekijöihinjako on yksikäsitteistä, niin p on liittoalkio jonkun luvun p_i tai q_i kanssa, eli p jakaa jonkin luvuista p_i tai q_i ja siten $p|a$ tai $p|b$, eli p on alkuluku.

Olkoot nyt kaikki jaottomat luvut alkulukuja. Osoitetaan, että jos

$$u_1 p_1 \cdots p_m = u_2 q_a \cdots q_n,$$

missä u_1 ja u_2 ovat yksiköitä ja luvut p_i ja q_i jaottomia, niin $m = n$ ja on olemassa permutaatio π luvuista $\{1, \ldots, m\}$ siten, että p_i ja $q_{\pi(i)}$ ovat liittoalkioita ($1 \leq i \leq m$).

Jos $m = 0$, niin ei ole mitään todistettavaa.

Jos $m \geq 1$, niin $p_m | u_2 q_1 \cdots q_n$. Koska oletuksen nojalla p_m on alkuluku, niin $p_m | u_2$ tai $p_m | q_j$ jollakin j. Jos $p_m | u_2$, niin $p_m | 1$, eli p_m on kohdan 3.6 (a) mukaan yksikkö, joten täytyy olla $p_m | q_j$. Järjestetään indeksit uudelleen siten, että $j = n$, jolloin $p_m | q_n$ ja $q_n = up_m$, missä u on yksikkö. Täten siis

$$u_1 p_1 \cdots p_m = u_2 q_1 \cdots q_{n-1} u p_m,$$

joka voidaan jakaa puolittain luvulla p_m:

$$u_1 p_1 \cdots p_{m-1} = (uu_2) q_1 \cdots q_{n-1}.$$

Induktiolla $n - 1 = m - 1$ ja löytyy permutaatio joukosta $\{1, \ldots, m\}$ siten, että p_i ja $q_{\pi(i)}$ ovat liittoalkioita ($1 \leq i \leq m - 1$). Laajennetaan permutaatio koskemaan joukkoa $\{1, \ldots, m\}$ asettamalla $\pi(m) = m$.

3.18 Yksikäsitteinen tekijöihinjako pääideaalikokonaisalueessa

Jokainen pääideaalikokonaisalue on yksikäsitteisen tekijöihinjaon kokonaisalue, eli yksikäsitteinen tekijöihinjako on mahdollista kaikissa pääideaalikokonaisalueissa.

Todistus:

Olkoon D PIKA. Pääideaalit ovat yhden alkion virittämiä, eli hyvinkin äärellisesti viritettyjä, joten D on siis noetherilainen ja täten kohdan 3.12 perusteella tekijöihinjako jaottomiin lukuihin on mahdollista. Riittää siis osoittaa, että kaikki jaottomat luvut ovat alkulukuja (ts. kohdan 3.17 ehto).

Olkoon p jaoton. Tällöin kohdan 3.7 (d) nojalla $\langle p \rangle$ on maksimaalinen joukon D pääideaalien joukossa. Koska joukon D kaikki ideaalit ovat pääideaaleja, on $\langle p \rangle$ siis maksimaalinen kaikkien joukon D ideaalien joukossa.

Oletetaan, että $p|ab$, mutta $p \nmid a$. Nyt

$$\langle p, a \rangle \supsetneq \langle p \rangle$$

ja siten maksimaalisuuden nojalla $\langle p, a \rangle = D$. Erityisesti $1 \in \langle p, a \rangle$, joten löytyy alkiot $c, d \in D$ siten, että

$$1 = cp + da$$

ja kertomalla puolittain luvulla b

$$b \cdot 1 = b \cdot cp + b \cdot da.$$

Oletuksen nojalla $p|ab$, joten

$$p|(bcp + bda),$$

eli $p|b$, joten p on alkuluku.

Aiemmin löydettiin esimerkki kokonaisalueesta, jossa yksikäsitteinen tekijöihinjako ei onnistunut. Nyt riittäisi siis löytää kokonaisalue, jonka kaikki ideaalit ovat pääideaaleja, jolloin tiedetään yksikäsitteisen tekijöihinjaon toimivan siellä. Tämä saattaa kuitenkin olla hivenen haastavaa ja tähän löytyykin hieman helpompia tapoja.

Jos peruutetaan takaisin aritmetiikan peruslauseeseen kokonaisluvuissa, niin havaitaan, että yksikäsitteisyyden todistamisessa Eukleideen lemma oli varsin tärkeässä asemassa. Kokonaisalueessa alkuluvut onkin määritelty Eukleideen lemman antaman tuloksen mukaan, joten kyseistä ominaisuutta ei ole tarvinnut "todistaa" missään vaiheessa. Kokonaislukujen joukossa taas todistukseen käytettiin erästä varsin kätevää ominaisuutta, nimittäin jakoyhtälöä. Jakoyhtälön yleistys osoittautuukin käytännölliseksi tavaksi löytää esimerkki kokonaisalueesta, jossa yksikäsitteinen tekijöihinjako on voimassa.

3.19 Euklidinen kuvaus

Olkoon D kokonaisalue. *Euklidinen kuvaus* (tai *Euklidinen funktio*) kokonaisalueelle D on kuvaus $\phi\colon D\backslash\{0\} \to \mathbb{N}$ siten, että

1. Jos $a, b \in D\backslash\{0\}$ ja $a|b$, niin $\phi(a) \leq \phi(b)$

2. Jos $a, b \in D\backslash\{0\}$, niin on olemassa luvut $q, r \in D$ siten, että $a = bq+r$, missä joko $r = 0$ tai $\phi(r) < \phi(b)$.

Kokonaislukujen joukossa kuvaus $\phi(n) = |n|$ ja polymeille renkaassa $K[t]$ kuvaus $\phi(p) = \partial p$, missä siis ∂p on polynomin p aste, ovat Euklidisia kuvauksia.

3.20 Euklidinen kokonaisalue

Jos kokonaisalueessa D on Euklidinen kuvaus, niin sanotaan, että D on *Euklidinen kokonaisalue*.

3.21 Euklidinen kokonaisalue on PIKA

Jokainen Euklidinen kokonaisalue on pääideaalikokonaisalue.

Todistus:

Olkoon D Euklidinen kokonaisalue ja $I \subset D$ ideaali. Jos $I = 0$, niin se on pääideaali, joten voidaan olettaa, että on olemassa $x \in I, x \neq 0$. Valitaan x niin, että $\phi(x)$ on mahdollisimman pieni. Jos $y \in I$, niin Euklidisen funktion toisen ominaisuuden nojalla

$$y = qx + r, \text{ missä joko } r = 0 \text{ tai } \phi(r) < \phi(x).$$

Nyt koska $r \in I$ ($y \in I$ ja $qx \in I$ kaikilla $q \in D$), niin ei voi olla $\phi(r) < \phi(x)$, sillä x valittiin niin, että $\phi(x)$ on mahdollisimman pieni. Siten täytyy olla $r = 0$, joten y on luvun x moninkerta ja siten $I = \langle x \rangle$ on pääideaali.

Yksikäsitteistä tekijöihinjakoa varten riitää siis löytää kokonaisalue, jossa on Euklidinen funktio. Koska kokonaislukujen tapauksessa itseisarvo, eli kokonaislukujen normi, on sopiva Euklidinen kuvaus, niin hyvänä kandidaattina jollekin vähän alkioiden mielessä suuremmalle kokonaisalueelle voisi olla algebrallinen normi.

3.22 Esimerkki

Lukukunnan $\mathbb{Q}(\sqrt{-2})$ algebrallisten lukujen rengas $\mathfrak{O}$ on Euklidinen kokonaisalue ja Euklidinen funktio on algebrallinen normi, eli $\phi(\alpha) = |N(\alpha)|$. Käydään läpi normin vaatimukset. Havaitaan ensin, että renkaan $\mathfrak{O}$ alkiot ovat muotoa

$$a = x + y\sqrt{-2},\ x, y \in \mathbb{Z},$$

joten alkiolle $a \neq 0$

$$|N(a)| = |x^2 + 2y^2| \geq 1.$$

(1) Jos $a, b \in \mathfrak{O}$ ja $a|b$, niin $b = la$ jollakin $l \in \mathfrak{O}$. Tällöin

$$|N(a)| \leq |N(l)N(a)| = |N(la)| = |N(b)|,$$

joten ainakin ensimmäinen ehto on voimassa.

(2) Olkoot $a, b \in \mathfrak{O}$ ja $b \neq 0$. Pitää siis löytää luvut $r, q \in \mathfrak{O}$ siten, että

$$a = bq + r,\ \text{missä joko } r = 0 \text{ tai } |N(r)| < |N(b)|.$$

Olkoon

$$a/b = ab^{-1} = c + d\sqrt{-2},$$

missä siis $c, d \in \mathbb{Q}$. Olkoot nyt $m, n \in \mathbb{Z}$ sellaisia, että m on mahdollisimman lähellä lukua c ja n mahdollisimman lähellä lukua d, eli

$$|m - c| \leq \frac{1}{2} \text{ ja } |n - d| \leq \frac{1}{2}.$$

Olkoot

$$q = m + n\sqrt{-2} \text{ ja } r = a - bq.$$

Jos $r = 0$, niin Euklidisen funktion ehto täyttyy. Jos taas $r \neq 0$, niin

$$\begin{aligned} |N(a/b - q)| &= |N((c + d\sqrt{-2}) - (m + n\sqrt{-2}))| \\ &= |N((c - m) + (d - n)\sqrt{-2})| \\ &\leq \left| \left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2 \right| = \frac{1}{4} + \frac{2}{4} = \frac{3}{4}. \end{aligned}$$

Siten

$$|N(r)| = |N(a - bq)| = \left|N\left(b\left(\frac{a}{b} - q\right)\right)\right| = \left|N(b)N\left(\frac{a}{b} - q\right)\right| \leq \left|N(b)\frac{3}{4}\right|,$$

joten $|N(r)| < |N(b)|$ ja $\mathfrak{O}$ on Euklidinen kokonaisalue.

Jos katsoo todistusta hieman tarkemmin läpi, niin huomaa, että esimerkki toimii sellaisenaan myös *Gaussin kokonaisluvuille*, eli renkaalle $\mathbb{Z}(\sqrt{-1})$, joten löydettiin itse asiassa ainakin kaksi rengasta, joissa yksikäsitteinen tekijöihinjako onnistuu.

Aiemmin todistettiin, että jos D on PIKA, niin D on myös yksikäsitteisen tekijöihinjaon kokonaisalue. Osoittautuu, että tulos pätee myös toiseen suuntaan ja kaikki yksikäsitteisen tekijöihinjaon kokonaisalueet ovat pääideaalikokonaisalueita. Tämän todistamista varten pitää kuitenkin perehtyä hieman tarkemmin ideaaliteoriaan.

4 Ideaaleista

Ernst Kummer käytti ensimmäisenä ilmaisua ”ideaalinen kompleksiluku” vuonna 1847 kuvaamaan lukuja, jotka säilyttävät yksikäsitteisen tekijöihinjaon ominaisuuden tietyissä algebrallisten lukujen renkaissa. Kummer halusi jakaa luvut tietynlaisiin alkutekijöihin, jotka olivat muotoa

$$a_0 + a_1\alpha + \ldots + a_{p-1}\alpha^{p-1},$$

missä luvut $a_i \in \mathbb{Z}$, p on alkuluku ja α on kompleksinen yhtälön $x^p = 1$ juuri. Kummer oli havainnut, että perinteinen alkulukujen määrittely jaottomina lukuina ei toiminut odotetusti, sillä kahden tällaisen alkuluvun tulo saattoi olla jaollinen jollain kolmannella jaottomalla luvulla. Kohdassa 3.16 todettiinkin, että yksikäsitteinen tekijöihinjako ei ole voimassa kokonaisalueen $\mathbb{Q}(\sqrt{-10})$ algebrallisten lukujen renkaissa ja annettiin esimerkkinä

$$14 = 2 \cdot 7 = (2 + \sqrt{-10}) \cdot (2 - \sqrt{-10}),$$

jolloin kumpikaan luvuista 2 tai 7 ei jaa lukuja $2 \pm \sqrt{-10}$ kyseisessä renkaassa. Niinpä Kummerin ideana oli laajentaa rengasta niin, että yksikäsitteinen tekijöihinjako onnistuisi. Laajennuksessa lisättyjä alkioita Kummer kutsui ”ideaalisiksi luvuiksi”. *Richard Dedekind* tutki samoja asioita kuin Kummer toisesta näkökulmasta ja toi termin ”ideaali” rengasteoriaan seuraten Kummerin ajatuksia. Termi jäi elämään ja myöhemmin erityisesti *Emmy Noether* kehitti ideaalien teoriaa.

Dedekind myös osoitti, että vaikka yksikäsitteinen tekijöihinjako ei välttämättä onnistu luvuilla, niin vastaava tulos voidaan osoittaa todeksi ideaaleilla. Tämän kappaleen alkupuolella esitellään tarpeelliset käsitteet, jotta voidaan todistaa ideaalien yksikäsitteinen tekijöihinjako.

4.1 Ideaalien kertolasku

Kokonaislukurenkaan $\mathfrak{O}$ ideaalien $\mathfrak{a}$ ja $\mathfrak{b}$ kertolasku määritellään

$$\mathfrak{ab} = \sum_{i=1}^{n} a_i b_i, a_i \in \mathfrak{a}, b_i \in \mathfrak{b}, n \in \mathbb{N}.$$

4.2 Alkuideaali

$\mathfrak{a}$ on *alkuideaali*, jos aina kun $\mathfrak{b}$ ja $\mathfrak{c}$ ovat renkaan R ideaaleja ja $\mathfrak{bc} \subseteq \mathfrak{a}$, niin joko $\mathfrak{b} \subseteq \mathfrak{a}$ tai $\mathfrak{c} \subseteq \mathfrak{a}$.

4.3 Ideaalien ja tekijärenkaiden ominaisuuksia

Olkoon R rengas ja $\mathfrak{a}$ renkaan R ideaali. Tällöin
(a) $\mathfrak{a} = R$ jos ja vain jos $1_R \in \mathfrak{a}$,
(b) $R/\mathfrak{a}$ on ykkösellinen ja vaihdannainen,
(c) $R/\mathfrak{a}$ on kunta täsmälleen silloin kun $\mathfrak{a}$ on maksimaalinen,
(d) $R/\mathfrak{a}$ on kokonaisalue aina ja vain kun $\mathfrak{a}$ on alkuideaali.

Todistus:

(a) Jos $\mathfrak{a} = R$, niin väite on selvä.

Jos taas $1_R \in \mathfrak{a}$, niin ideaalin määritelmän nojalla

$$1_R \cdot r \in \mathfrak{a} \text{ kaikilla } r \in R,$$

eli $\mathfrak{a} = R$.

(b) Olkoot $r, s \in R$. Nyt

$$(r + \mathfrak{a})(s + \mathfrak{a}) = rs + \mathfrak{a} = sr + \mathfrak{a} = (s + \mathfrak{a})(r + \mathfrak{a})$$

ja

$$(1_R + \mathfrak{a})(r + \mathfrak{a}) = r + \mathfrak{a} = (r + \mathfrak{a})(1_R + \mathfrak{a}),$$

joten $R/\mathfrak{a}$ on vaihdannainen ja ykkösellinen, ykkösalkionaan $1_R + \mathfrak{a}$.

(c) Olkoon $R/\mathfrak{a}$ kunta. Olkoon $\mathfrak{b}$ ideaali, jolle pätee $\mathfrak{a} \subsetneq \mathfrak{b} \subseteq R$. Koska $\mathfrak{a} \subsetneq \mathfrak{b}$, niin on olemassa alkio $r \in \mathfrak{b}$ siten, että $r \notin \mathfrak{a}$. Täten $r + \mathfrak{a} \neq \mathfrak{a}$, eli alkiolla $r + \mathfrak{a}$ on olemassa käänteisalkio $s + \mathfrak{a}$ siten, että

$$rs + \mathfrak{a} = (r + \mathfrak{a})(s + \mathfrak{a}) = 1 + \mathfrak{a}.$$

Koska $0 \in \mathfrak{a}$, niin löytyy alkio $q \in \mathfrak{a}$, jolle pätee

$$rs + q = 1.$$

Nyt $r \in \mathfrak{b}$ ja $s \in R$, joten $rs \in \mathfrak{b}$. Toisaalta $q \in \mathfrak{a} \subsetneq \mathfrak{b}$, joten

$$rs + q \in \mathfrak{b},$$

eli $1 \in \mathfrak{b}$ ja (a)-kohdan nojalla $\mathfrak{b} = R$.

Olkoon sitten $\mathfrak{a}$ maksimaalinen. Riittää siis löytää alkion $r + \mathfrak{a}, r \notin \mathfrak{a}$ käänteisalkio kertolaskun suhteen. Koska $\mathfrak{a}$ on maksimaalinen ja $r \in Rr + \mathfrak{a}$,

niin täytyy olla $Rr + \mathfrak{a} = R$. Tällöin myös $1 \in Rr + \mathfrak{a}$, joten on olemassa alkiot $s \in R$ ja $q \in \mathfrak{a}$ siten, että

$$1 = sr + q,$$

jolloin

$$(s + \mathfrak{a})(r + \mathfrak{a}) = sr + \mathfrak{a} = (1 - q) + \mathfrak{a} = 1 + \mathfrak{a}, \text{ koska } q \in \mathfrak{a}.$$

Täten $s + \mathfrak{a}$ on alkion $r + \mathfrak{a}$ käänteisalkio kertolaskun suhteen.

(d) Olkoon $R/\mathfrak{a}$ kokonaisalue ja olkoon $rs \in \mathfrak{a}$. Tällöin

$$rs + \mathfrak{a} = (r + \mathfrak{a})(s + \mathfrak{a}) = \mathfrak{a}.$$

Koska $R/\mathfrak{a}$ on kokonaisalue, niin $r + \mathfrak{a} = \mathfrak{a}$ tai $s + \mathfrak{a} = \mathfrak{a}$, eli $r \in \mathfrak{a}$ tai $s \in \mathfrak{a}$.

Olkoon $\mathfrak{a}$ sitten alkuideaali. Tehdään vastaoletus: $R/\mathfrak{a}$ ei ole kokonaisalue. Tällöin löytyy nollasivuluokasta eroavat sivuluokat $r + \mathfrak{a}$ ja $s + \mathfrak{a}$, joille $rs + \mathfrak{a} = \mathfrak{a}$. Koska $\mathfrak{a}$ on alkuideaali, niin tällöin $r \in \mathfrak{a}$ tai $s \in \mathfrak{a}$, joten vastaoletus tuottaa ristiriidan alkuperäisen oletuksen kanssa.

4.4 Seuraus

Jokainen maksimaalinen ideaali on alkuideaali.

4.5 Algebrallisten lukujen renkaan ominaisuuksia

Lukukunnan K algebrallisten lukujen renkaalla $\mathfrak{O}$ on seuraavat ominaisuudet:
(a) $\mathfrak{O}$ on noetherilainen,
(b) Jos $\alpha \in K$ toteuttaa perusmuotoisen (monic) polynomiyhtälön, jonka tekijät ovat renkaassa $\mathfrak{O}$, niin myös $\alpha \in \mathfrak{O}$,
(c) Jokainen joukon $\mathfrak{O}\backslash\{0\}$ alkuideaali on maksimaalinen.

Todistus:

(a) Kohdan 2.18 mukaan $(\mathfrak{O}, +)$ on vapaa Abelin ryhmä kertalukua n ja jos $\mathfrak{a}$ on renkaan $\mathfrak{O}$ ideaali, niin kohdan 2.3 nojalla $(\mathfrak{a}, +)$ on vapaa Abelin ryhmä kertalukua $s \leq n$. Tällöin mikä tahansa ryhmän $(\mathfrak{a}, +)$ $\mathbb{Z}$-kanta generoi ideaalin $\mathfrak{a}$, joten jokainen renkaan $\mathfrak{O}$:n ideaali on äärellisesti viritetty.

(b) Seuraus kohdasta 2.16

(c) Olkoon $\mathfrak{p}$ alkuideaali renkaassa $\mathfrak{O}$ ja olkoon $0 \neq \alpha \in \mathfrak{p}$. Tällöin

$$\mathcal{N} = N(\alpha) = \alpha_1 \cdot \ldots \cdot \alpha_n \in \mathfrak{p},$$

sillä jollain i pätee $\alpha_i = \alpha$, koska identtinen kuvaus kuuluu monomorfismien joukkoon. Voidaan olettaa, että $\alpha_1 = \alpha$. Näin ollen $\langle \mathcal{N} \rangle \subseteq \mathfrak{p}$ ja siten $\mathfrak{O}/\mathfrak{p}$ on renkaan $\mathfrak{O}/\mathcal{N}\mathfrak{O}$ tekijärengas. Nyt $\mathfrak{O}/\mathcal{N}\mathfrak{O}$ on äärellisesti viritetty Abelin ryhmä ja sen virittäjät ovat myös äärellisiä, joten koko ryhmä on äärellinen. Koska $\mathfrak{O}/\mathfrak{p}$ on äärellinen ja kohdan 4.3 (d) nojalla kokonaisalue, on se äärellisenä kokonaisalueena kunta. Täten kohdan 4.3 (c) mukaan $\mathfrak{p}$ on maksimaalinen ideaali.

Ideaalien kertolasku on siis selvästi vaihdannainen ja liitännäinen ja löytyy jopa neutraalialkio, nimittäin $\mathfrak{O}$ itse. Käänteisalkio ei kuitenkaan aina välttämättä ole olemassa, joten ideaaleista ei saada aikaiseksi ryhmää. Käänteisalkio voidaan kuitenkin aina löytää, jos laajennetaan hieman ideaalin käsitettä.

Esimerkiksi renkaassa $\mathbb{Z}$ ideaalilla $2\mathbb{Z}$ ei ole käänteisideaalia, mutta joukolla $\frac{1}{2}\mathbb{Z}$ kerrottaessa saadaan

$$2\mathbb{Z}\frac{1}{2}\mathbb{Z} = \langle 2 \rangle \langle \frac{1}{2} \rangle = \langle 1 \rangle = \mathbb{Z}.$$

Nyt vain joukko $\frac{1}{2}\mathbb{Z}$ ei ole renkaan $\mathbb{Z}$ ideaali, vaikka siitä saisi ideaalin kertomalla sitä luvulla 2. Aiemmin havaittiinkin, että ideaalit ovat itse asiassa $\mathfrak{O}$-alimoduleita renkaassa $\mathfrak{O}$. Koska kunnista löytyy aina käänteisalkio myös kertolaskulle, siirrytään tarkastelemaan lukukunnan K $\mathfrak{O}$-alimoduleita. Määritellään ryhmärakenteen saamiseksi uusi käsite:

4.6 Murtoideaali

Lukukunnan K $\mathfrak{O}$-alimoduli $\mathfrak{a}$ on algebrallisten lukujen renkaan $\mathfrak{O}$ *murtoideaali*, jos on olemassa jokin $0 \neq c \in \mathfrak{O}$ siten, että $c\mathfrak{a} \subseteq \mathfrak{O}$.

Toisin sanoen, joukko $\mathfrak{b} = c\mathfrak{a}$ on renkaan $\mathfrak{O}$ ideaali ja $\mathfrak{a} = c^{-1}\mathfrak{b}$. Renkaan $\mathfrak{O}$ murtoideaalit ovat siis kunnan K osajoukkoja ja muotoa $c^{-1}\mathfrak{b}$, missä c on jokin nollasta eroava renkaan $\mathfrak{O}$ alkio ja $\mathfrak{b}$ on renkaan $\mathfrak{O}$ ideaali. Tavalliset ideaalit ovat tietenkin myös murtoideaaleja ja murtoideaalit ovat ideaaleja, jos (ja vain jos) ne sisältyvät renkaaseen $\mathfrak{O}$. Kuten nimestä ja määritelmästä voi päätellä, yhteys *murtolukuihin* on ilmeinen.

4.7 Murtoideaalien ominaisuuksia

Jos $\mathfrak{a}_1$ ja $\mathfrak{a}_2$ ovat murtoideaaleja, eli

$$\mathfrak{a}_1 = c_1^{-1}\mathfrak{b}_1$$
$$\mathfrak{a}_2 = c_2^{-1}\mathfrak{b}_2$$

ideaaleille $\mathfrak{b}_1, \mathfrak{b}_2 \subseteq \mathfrak{O}$ ja nollasta eroaville $c_1, c_2 \in \mathfrak{O}$, niin

$$\mathfrak{a}_1\mathfrak{a}_2 = (c_1c_2)^{-1}\mathfrak{b}_1\mathfrak{b}_2,$$

joten kahden murtoideaalin tulo on myös murtoideaali. Kuten tavallisille ideaaleilla, kertolasku on myös vaihdannainen ja liitännäinen ja $\mathfrak{O}$ toimii edelleen neutraalialkiona. Tarkastellaan hieman sopivaa käänteisalkiokandidaattia ja osoitetaan sitten, että se todella on käänteisalkio kertolaskun suhteen.

4.8 Käänteisideaali

Olkoon $\mathfrak{a}$ renkaan $\mathfrak{O}$ ideaali. Tällöin joukkoa

$$\mathfrak{a}^{-1} \coloneqq \{x \in K \colon x\mathfrak{a} \subseteq \mathfrak{O}\}$$

sanotaan ideaalin $\mathfrak{a}$ *käänteisideaaliksi*. Näin määriteltynä $\mathfrak{a}^{-1}$ on selvästi $\mathfrak{O}$-alimoduli: Jos $\mathfrak{a} \neq 0$, niin kaikilla $0 \neq c \in \mathfrak{a}$ pätee $c\mathfrak{a}^{-1} \subseteq \mathfrak{O}$, joten $\mathfrak{a}^{-1}$ on $\mathfrak{O}$-alimoduli. Selvästi $\mathfrak{O} \subseteq \mathfrak{a}^{-1}$, joten

$$\mathfrak{a} = \mathfrak{a}\mathfrak{O} \subseteq \mathfrak{a}\mathfrak{a}^{-1}.$$

Määritelmästä myös nähdään, että

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathfrak{O},$$

eli murtoideaali $\mathfrak{a}\mathfrak{a}^{-1}$ on itse asiassa ideaali. Huomataan myös, että kun $\mathfrak{a} \subseteq \mathfrak{p}$, niin $\mathfrak{O} \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$: Jos $x \in \mathfrak{p}^{-1}$, niin $xp \in \mathfrak{O}$ kaikilla $p \in \mathfrak{p}$, eli erityisesti $x\mathfrak{a} \in \mathfrak{O}$ kaikilla $a \in \mathfrak{a} \subseteq \mathfrak{p}$, joten $x \in \mathfrak{a}^{-1}$.

4.9 Lemma

Olkoon $\mathfrak{a} \neq 0$ renkaan $\mathfrak{O}$ ideaali. Tällöin on olemassa alkuideaalit $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ siten, että

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}.$$

Todistus:

Tehdään vastaoletus: väitteen mukaisia alkuideaaleja ei ole olemassa. Kohdan 4.5 (a) nojalla $\mathfrak{O}$ on noetherilainen, joten voidaan valita mahdollisimman suuri $\mathfrak{a}$, jolle alkuideaaleja ei löydy. Tällöin $\mathfrak{a}$ ei voi olla itse alkuideaali ja löytyy siis renkaan $\mathfrak{O}$ ideaalit $\mathfrak{b}$ ja $\mathfrak{c}$, joille

$$\mathfrak{bc} \subseteq \mathfrak{a}, \mathfrak{b} \nsubseteq \mathfrak{a}, \mathfrak{c} \nsubseteq \mathfrak{a}.$$

Asetetaan

$$\mathfrak{a}_1 = \mathfrak{a} + \mathfrak{b}$$
$$\mathfrak{a}_2 = \mathfrak{a} + \mathfrak{c}.$$

Tällöin $\mathfrak{a}_1, \mathfrak{a}_2 \subseteq \mathfrak{a}$, $\mathfrak{a} \subsetneqq \mathfrak{a}_1$ ja $\mathfrak{a} \subsetneqq \mathfrak{a}_2$. Koska $\mathfrak{a}$ oli suurin mahdollinen, on olemassa alkuideaalit $\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{p}_{s+1}, \ldots, \mathfrak{p}_r$ siten, että

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq \mathfrak{a}_1,$$
$$\mathfrak{p}_{s+1} \cdots \mathfrak{p}_r \subseteq \mathfrak{a}_2.$$

Yhdistämällä saadaan

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a},$$

mikä on ristiriita, sillä $\mathfrak{a}$ valittiin sellaiseksi, että tällaisia alkuideaaleja ei ole.

Kohdassa 4.8 todettiin, että $\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}$. Seuraavaksi on tarkoituksena todistaa inkluusio myös toiseen suuntaan, jolloin saadaan varmistettua ryhmärakenne.

4.10 Murtoideaalit kertolaskulla muodostavat Abelin ryhmän

Renkaan $\mathfrak{O}$ nollasta eroavat murtoideaalit muodostavat Abelin ryhmän kertolaskun suhteen.

Hajautetaan todistus useampaan osaan ja todistetaan asteittain:

(a) Jos $\mathfrak{a}$ on renkaan $\mathfrak{O}$ aito ideaali (eli $\mathfrak{a} \neq \mathfrak{O}$), niin $\mathfrak{a}^{-1} \supsetneqq \mathfrak{O}$,
(b) Jos $\mathfrak{a} \neq 0$ on renkaan $\mathfrak{O}$ ideaali ja $\mathfrak{a}S \subseteq \mathfrak{a}$ jollekin kunnan K osajoukolle S, niin $S \subseteq \mathfrak{O}$,
(c) Jos $\mathfrak{p}$ on maksimaalinen renkaan $\mathfrak{O}$ ideaali, niin $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{O}$,

(d) Kaikille rankaan $\mathfrak{O}$ ideaaleille $\mathfrak{a} \neq 0$ pätee $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}$,
(e) Jokaisella renkaan $\mathfrak{O}$ murtoideaalilla $\mathfrak{a}$ on käänteisalkio $\mathfrak{a}^{-1}$ kertolaskun suhteen siten, että $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}$.

Todistus:

(a) Koska $\mathfrak{a} \subseteq \mathfrak{p}$ jollekin maksimaaliselle ideaalille $\mathfrak{p}$ ja $\mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, niin riittää osoittaa, että $\mathfrak{p} \neq \mathfrak{O}$ maksimaaliselle ideaalille $\mathfrak{p}$. Riittää siis löytää jokin ei-algebrallinen kokonaisluku joukosta $\mathfrak{p}^{-1}$. Olkoon $a \in \mathfrak{p}$, $a \neq 0$. Kohdan 4.9 nojalla löydetään alkuideaalit $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, joille

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \langle a \rangle.$$

Valitaan näistä alkuideaalikokoelmista se, jossa r on mahdollisimman pieni. Koska $\langle a \rangle \subseteq \mathfrak{p}$ ja $\mathfrak{p}$ on alkuideaali kohdan 4.4 nojalla, täytyy olla $\mathfrak{p}_i \subseteq \mathfrak{p}$ jollekin i. Voidaan olettaa, että $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Täten $\mathfrak{p}_1 = \mathfrak{p}$, koska alkuideaalit ovat maksimaalisia kohdan 4.5 (c) nojalla ja koska r oli valittu mahdollisimman pieneksi, niin

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq \langle a \rangle.$$

Näin ollen $\mathfrak{p}_2 \cdots \mathfrak{p}_r \backslash \langle a \rangle \neq \emptyset$ ja voidaan valita $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \backslash \langle a \rangle$. Kuitenkin

$$b\mathfrak{p} \subseteq \langle a \rangle, \text{ joten } ba^{-1}\mathfrak{p} \subseteq \mathfrak{O} \text{ ja } ba^{-1} \in \mathfrak{p}^{-1}.$$

Nyt $b \notin a\mathfrak{O}$ ja siten $ba^{-1} \notin \mathfrak{O}$, eli $\mathfrak{p}^{-1} \neq \mathfrak{O}$.

(b) Näytetään, että jos $\mathfrak{a}\theta \subseteq \mathfrak{a}$, kun $\theta \in S$, niin $\theta \in \mathfrak{O}$. Koska $\mathfrak{O}$ on noetherilainen, $\mathfrak{a} = \langle a_1, \ldots, a_m \rangle$, missä ainakin yksi $a_i \neq 0$. Tällöin ehdosta $\mathfrak{a}\theta \subseteq \mathfrak{a}$ seuraa

$$\begin{aligned} a_1\theta &= b_{11}a_1 + \ldots b_{1m}a_m \\ &\vdots \\ a_m\theta &= b_{m1}a_1 + \ldots b_{mm}a_m \end{aligned}$$

Koska yhtälöillä

$$\begin{aligned} (b_{11} - \theta)x_1 + \ldots + b_{1m}x_m &= 0 \\ &\vdots \\ b_{m1}x_1 + \ldots + (b_{mm} - \theta)x_m &= 0 \end{aligned}$$

on jokin nollasta poikkeava ratkaisu $x_1 = a_1, \ldots, x_m = a_m$, niin niitä vastaavan matriisin determinantin täytyy olla 0. Näin saadaan luvulle θ perusmuotoinen polynomiyhtälö, jonka kertoimet ovat renkaassa $\mathfrak{O}$, joten

$\theta \in \mathfrak{O}$ kohdan 4.5 (b) nojalla.

(c) Kohdan 4.8 perusteella havaitaan, että $\mathfrak{p}\mathfrak{p}^{-1}$ on ideaali ja $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{O}$. Koska $\mathfrak{p}$ on maksimaalinen, niin joko $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ tai $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{O}$. Jos $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, niin (b)-kohdan mukaan $\mathfrak{p}^{-1} \subseteq \mathfrak{O}$, mikä on ristiriita (a)-kohdan kanssa, joten täytyy olla $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{O}$.

(d) Vastaoletus: Olkoon $\mathfrak{a}$ suurin ideaali siten, että $\mathfrak{a}\mathfrak{a}^{-1} \neq \mathfrak{O}$. Tällöin $\mathfrak{a} \subseteq \mathfrak{p}$ jollekin maksimaaliselle ideaalille $\mathfrak{p}$. Kohdan 4.8 mukaan $\mathfrak{O} \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, joten

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}.$$

Erityisesti ehdosta $\mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{O}$ seuraa, että $\mathfrak{a}\mathfrak{p}^{-1}$ on ideaali. Jos olisi $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, niin olisi $\mathfrak{p}^{-1} \subseteq \mathfrak{O}$ (b)-kohdan nojalla ja tämä on ristiriita (a)-kohdan kanssa. Täytyy siis olla $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ ja maksimaalisuusehdon soveltamisesta ideaaliin $\mathfrak{a}$ seuraa, että joukolle $\mathfrak{a}\mathfrak{p}^{-1}$ pätee

$$\mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = \mathfrak{O}.$$

Ideaalin $\mathfrak{a}^{-1}$ määritelmän mukaan ylläoleva tarkoittaa, että

$$\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1}.$$

Täten $\mathfrak{O} = \mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}$. Tämä on ristiriitaista ideaalin $\mathfrak{a}$ valinnan suhteen, joten $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}$ kaikilla $\mathfrak{a} \neq 0$.

(e) Koska $\mathfrak{a}$ on murtoideaali, niin on olemassa ideaali $\mathfrak{b}$ ja alkio $c \in \mathfrak{O}\backslash\{0\}$ siten, että $\mathfrak{a} = c^{-1}\mathfrak{b}$. Asetetaan $\mathfrak{a}' = c\mathfrak{b}^{-1}$, jolloin $\mathfrak{a}\mathfrak{a}' = \mathfrak{O}$.

4.11 Jaollisuus ideaaleilla

Olkoot $\mathfrak{a}$ ja $\mathfrak{b}$ renkaan $\mathfrak{O}$ ideaaleja. Sanotaan, että ideaali $\mathfrak{a}$ jakaa ideaalin $\mathfrak{b}$, jos on olemassa ideaali $\mathfrak{c} \subseteq \mathfrak{O}$ siten, että $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Tätä merkitään $\mathfrak{a}|\mathfrak{b}$. Tällöin on myös voimassa

$$\mathfrak{a}|\mathfrak{b} \text{ jos ja vain jos } \mathfrak{a} \supseteq \mathfrak{b},$$

sillä voidaan valita $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b}$. Tuloksesta voi nähdä, että ideaalin $\mathfrak{b}$ tekijät ovat siis ne ideaalit, jotka sisältävät ideaalin $\mathfrak{b}$. Nyt myös alkuideaaleille saadaan tutunlainen esitys, sillä jos $\mathfrak{p}$ on alkuideaali, niin ehdosta

$$\mathfrak{p}|\mathfrak{a}\mathfrak{b} \text{ seuraa, että } \mathfrak{p}|\mathfrak{a} \text{ tai } \mathfrak{p}|\mathfrak{b},$$

jolloin määritelmä on samanlainen kuin algebrallisille luvuillekin.
Merkintään voi vielä tehdä pienen lisäyksen: Jos $\mathfrak{a}$ on renkaan $\mathfrak{O}$ ideaali ja $b \in \mathfrak{O}$ siten, että $\mathfrak{a}|\langle b\rangle$, niin sanotaan, että ideaali $\mathfrak{a}$ jakaa luvun b ja merkitään $\mathfrak{a}|b$. Tällä merkintätavalla voidaan alkuideaaleille kirjoittaa, että ehdosta $\mathfrak{p}|\mathfrak{a}b$ seuraa $\mathfrak{p}|\mathfrak{a}$ tai $\mathfrak{p}|b$. Tekijöihinjaon yhteys alkioiden ja pääideaalien välillä käy näin selvemmäksi.

Nyt voidaan todistaa aritmetiikan peruslause ideaaleille liki identtisellä tavalla kuin se alussa todistettiin kokonaisluvuille.

4.12 Ideaalien yksikäsitteinen tekijöihinjako

Renkaan $\mathfrak{O}$ nollasta eroavat ideaalit voidaan kirjoittaa järjestystä vaille yksikäsitteisesti alkuideaalien tulona.

Todistus:

(i) Olemassaolo: Jokainen $\mathfrak{a} \neq 0$ on alkuideaalien tulo.
Vastaoletus: Olkoon $\mathfrak{a}$ mahdollisimman suuri niiden ideaalien joukosta, joita ei voi esittää alkuideaalien tulona. Tällöin $\mathfrak{a}$ ei tietenkään voi olla alkuideaali, mutta täytyy olla $\mathfrak{a} \subset \mathfrak{p}$ jollekin maksimaaliselle (eli alku)ideaalille ja kuten kohdassa 4.10 (d), $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{O}$. Koska $\mathfrak{a}$ oletettiin mahdollisimman suureksi, niin

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \cdots \mathfrak{p}_r,$$

missä $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ ovat alkuideaaleja ja täten $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r$, mikä on ristiriita ideaalin $\mathfrak{a}$ valinnan kanssa.

(ii) Alkutekijäesitys on yksikäsitteinen.
Alkuideaalien määritelmän nojalla, jos $\mathfrak{p}$ on alkuideaali ja $\mathfrak{p}|\mathfrak{a}\mathfrak{b}$, niin $\mathfrak{p}|\mathfrak{a}$ tai $\mathfrak{p}|\mathfrak{b}$. Jos nyt jollain ideaalilla $\mathfrak{a}$ on kaksi alkuideaaliesitystä $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ ja $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ siten, että

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s,$$

niin $\mathfrak{p}_1$ jakaa jonkin ideaalin $\mathfrak{q}_i$ ja maksimaalisuuden nojalla $\mathfrak{p}_1 = \mathfrak{q}_i$. Voidaan siis kertoa puolittain käänteisideaalilla $\mathfrak{p}_1^{-1}$ ja käyttää induktiota, jolloin väite seuraa.

4.13 Ideaalin normin ominaisuuksia

Olkoon $\mathfrak{a}$ renkaan $\mathfrak{O}$ ideaali, $\mathfrak{a} \neq 0$. Tällöin
(a) Jos normi $N(\mathfrak{a}) = |\mathfrak{O}/\mathfrak{a}|$ on alkuluku, niin myös $\mathfrak{a}$ on alkuideaali

(b) $N(\mathfrak{a})$ on ideaalin $\mathfrak{a}$ alkio, eli $\mathfrak{a}|N(\mathfrak{a})$
(c) Jos $\mathfrak{a}$ on alkuideaali, se jakaa täsmälleen yhden alkuluvun $p \in \mathbb{Z}$ ja tällöin $N(\mathfrak{a}) = p^m$, missä $m \leq n$ (n on kunnan K aste, $\mathfrak{O} = \mathfrak{O}_K$).

Todistus:

(a) Ehdosta $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2$ seuraa $N(\mathfrak{a}) = N(\mathfrak{p}_1\mathfrak{p}_2) = N(\mathfrak{p}_1)N(\mathfrak{p}_2)$ kohdan 2.12 nojalla. Koska $N(\mathfrak{a})$ on alkuluku, niin $N(\mathfrak{p}_1) = N(\mathfrak{a})$ tai $N(\mathfrak{p}_2) = N(\mathfrak{a})$ Voidaan olettaa, että $N(\mathfrak{p}_1) = N(\mathfrak{a})$, jolloin $N(\mathfrak{p}_2) = 1$, eli $\mathfrak{p}_2 = \mathfrak{O}$, joten ideaali $\mathfrak{a}$ on ainoa itsensä tekijä ja siten alkuideaali.

(b) Määritelmä: $N(\mathfrak{a}) = |\mathfrak{O}/\mathfrak{a}| =: r$. Jos $x \in \mathfrak{O}$, niin $r(x + \mathfrak{a})$ on tekijärenkaan $\mathfrak{O}/\mathfrak{a}$ nolla-alkio, sillä ryhmien alkioiden kertaluvut jakavat aina ryhmän kertaluvun. Siten rx on ideaalin $\mathfrak{a}$ alkio ja sijoittamalla $x = 1$ saadaan väite.

(c) Kohdan (b) nojalla

$$\mathfrak{a}|N(\mathfrak{a}) = P_1^{m_1} \cdots p_r^{m_r},$$

joten $\mathfrak{a}|\langle p_i\rangle$, missä $p_i \in \mathbb{P}$. Jos $p, q \in \mathbb{P}$, syt$(p, q) = 1$ ja $\mathfrak{a}|p$ ja $\mathfrak{a}|q$, niin löytyy alkiot $u, v \in \mathbb{Z}$ siten, että

$$up + vq = 1,$$

joten $\mathfrak{a}|1$, eli $\mathfrak{a} = \mathfrak{O}$, mikä on ristiriita. Siis $\mathfrak{a}$ ei voi jakaa kahta alkulukua. Täten $N(\mathfrak{a})|N(\langle p\rangle) = p^n$, joten $N(\mathfrak{a}) = p^m$ jollekin $m \leq n$.

4.14 Lemma

Olkoon D kokonaisalue ja $\mathfrak{p} = \langle p\rangle \subseteq D$ pääideaali. Tällöin $\mathfrak{p}$ on alkuideaali jos ja vain jos p on alkuluku tai $p = 0$.

Todistus:

Olkoon $\mathfrak{p}$ alkuideaali, eli ehdosta $\mathfrak{ab} \subseteq \mathfrak{p}$ seuraa aina $\mathfrak{a} \subseteq \mathfrak{p}$ tai $\mathfrak{b} \subseteq \mathfrak{p}$. Jos $p = 0$, niin tällöin $a = 0$ tai $b = 0$. Oletetaan siis, että $p \neq 0$ ja tehdään vastaoletus: $p|nk$ joillakin $n, k \in D\backslash\{0\}$, mutta $p \nmid n$ ja $p \nmid k$. Nyt kuitenkin kohdan 3.7 (a) nojalla

$$\langle n \cdot k\rangle = \langle n\rangle\langle k\rangle \subseteq \langle p\rangle.$$

Jos nyt $\langle n\rangle \subseteq \langle p\rangle$, niin edelleen kohdan 3.7 (a) nojalla $p|n$ ja jos $\langle k\rangle \subseteq \langle p\rangle$, niin $p|k$. Siten $\langle n\rangle \nsubseteq \langle p\rangle$ ja $\langle k\rangle \nsubseteq \langle p\rangle$, mikä on ristiriita, koska $\langle p\rangle$ oletettiin

alkuideaaliksi.

Jos $\mathfrak{p} = 0$, niin ehdosta $\mathfrak{ab} \subseteq \mathfrak{p}$ seuraa aina, että $\mathfrak{a} = 0$ tai $\mathfrak{b} = 0$, eli erityisesti $\mathfrak{a} \subseteq \mathfrak{p}$ tai $\mathfrak{b} \subseteq \mathfrak{p}$, joten $\mathfrak{p}$ on alkuideaali.

Jos taas p on alkuluku, niin tarkastellaan tekijärengasta $D/\mathfrak{p}$. Olkoot $x, y \in D/\mathfrak{p}$, eli $x = \mathfrak{a} + \mathfrak{p}$ ja $y = \mathfrak{b} + \mathfrak{p}$, missä $\mathfrak{a}, \mathfrak{b} \in D$. Nyt koska p on alkuluku, eli ehdosta $p|\mathfrak{ab}$ seuraa, että $p|\mathfrak{a}$ tai $p|\mathfrak{b}$, niin

$$xy = (\mathfrak{a} + \mathfrak{p}) \cdot (\mathfrak{b} + \mathfrak{p}) = \mathfrak{ab} + \mathfrak{p} \neq \mathfrak{p},$$

kun $\mathfrak{a} \notin \mathfrak{p}$ ja $\mathfrak{b} \notin \mathfrak{p}$. Tekijärenkaan nolla-alkiot ovat siis luvun p moninkerrat. Nyt siis $D/\mathfrak{p}$ on kokonaisalue ja kohdan 4.3 (d) mukaan $\mathfrak{p}$ on alkuideaali.

4.15 Yksikäsitteisen tekijöihinjaon karakterisointi

Renkaassa $\mathfrak{O}$ tekijöihinjako jaottomiin on yksikäsitteistä täsmälleen silloin kun jokainen renkaan $\mathfrak{O}$ ideaali on pääideaali.

Todistus:

Kohdassa 3.18 osoitettiin, että tekijöihinjako on yksikäsitteistä, jos jokainen ideaali on pääideaali.

Jos tekijöihinjako on yksikäsitteistä, niin riittää osoittaa, että jokainen alkuideaali on pääideaali, sillä kaikki muut ideaalit voidaan esittää alkuideaalien tulona, jolloin ne olisivat pääideaalien tuloina pääideaaleja.

Olkoon $\mathfrak{p} \neq 0$ alkuideaali renkaassa $\mathfrak{O}$. Kohdan 4.13 (b) mukaan löytyy

$$\mathcal{N} \in \mathbb{Z},\ \mathcal{N} = N(\mathfrak{p})$$

siten, että $\mathfrak{p}|\mathcal{N}$. Oletuksen nojalla $\mathcal{N}$ voidaan esittää yksikäsitteisesti renkaan $\mathfrak{O}$ jaottomien alkioiden tulona

$$\mathcal{N} = \pi_1 \cdots \pi_s.$$

Koska $\mathfrak{p}|\mathcal{N}$ ja $\mathfrak{p}$ on alkuideaali, niin $\mathfrak{p}|\pi_i$ jollakin $i \in \{1, \ldots, s\}$. Koska tekijöihinjako on yksikäsitteistä renkaassa $\mathfrak{O}$, niin jaoton luku π_i on alkuluku kohdan 3.17 nojalla ja täten pääideaali $\langle \pi_i \rangle$ on alkuideaali kohdan 4.14 nojalla.

Nyt koska $\mathfrak{p}|\langle\pi_i\rangle$, missä sekä $\mathfrak{p}$, että $\langle\pi_i\rangle$ ovat alkuideaaleja ja tekijöihinjako on yksikäsitteistä, niin $\mathfrak{p} = \langle\pi_i\rangle$, joten $\mathfrak{p}$ on pääideaali.

Kohdan 4.15 perusteella nyt tiedetään milloin yksikäsitteinen tekijöihinjako onnistuu, nimittäin täsmälleen silloin kun kaikki renkaan $\mathfrak{O}$ ideaalit ovat pääideaaleja. On myös mahdollista "mitata" kuinka kaukana yksikäsitteisestä tekijöihinjaosta ollaan. Kirjallisuudesta [5] aiheeseen voi perehtyä tarkemmin ja tässä tutkielmassa todetaan vain tiivistetysti:
Jos $\mathcal{F}$ on renkaan $\mathfrak{O}$ murtoideaalien joukko ja $\mathcal{P}$ on saman renkaan päämurtoideaalien joukko, eli yhden alkion virittämien murtoideaalien joukko, niin tekijäryhmää

$$\mathcal{H} = \mathcal{F}/\mathcal{P}$$

sanotaan renkaan $\mathfrak{O}$ *luokkaryhmäksi*. Asetetaan

$$\mathfrak{h} = \mathfrak{h}(\mathfrak{O}) = |\mathcal{F}/\mathcal{P}|$$

ja kutsutaan lukua $\mathfrak{h}$ *luokkanumeroksi*. Tällöin on mahdollista osoittaa, että yksikäsitteinen tekijöihinjako on mahdollista täsmälleen silloin kun $\mathfrak{h} = 1$ ja että $\mathfrak{h}$ on aina äärellinen. Mitä suurempi $\mathfrak{h}$ on, sitä "kauempana" yksikäsitteisestä tekijöihinjaosta ollaan.

Nyt luvun $\mathfrak{h}$ äärelliseksi osoittamisesta päästään käsiksi sopiviin pääideaaleja koskeviin ehtoihin ja erityisesti voidaan osoittaa, että jokaisesta ideaalista saadaan pääideaali sopivassa kuntalaajennuksessa, jolloin kohdan 4.15 nojalla yksikäsitteinen tekijöihinjako on siis mahdollista. Näin päästään lähelle Kummerin käsitettä "ideaaliset luvut".

Viitteet

[1] Ian Stewart. *Galois Theory*. Chapman and Hall/CRC, CRC Press, 3rd edition, 2004.

[2] Tero Harju. äärellisesti generoitujen abelin ryhmien peruslause. Saatavilla Internetistä (http://users.utu.fi/harju/algebra/Abel.pdf), 2008.

[3] John B. Fraleigh. *A First Course in Abstract Algebra*. Addison Wesley, Pearson Education, 7th edition, 2003.

[4] Robert B. Ash. A course in algebraic number theory. Saatavilla Internetistä (http://www.math.uiuc.edu/~r-ash/ANT.html), 2003.

[5] Ian Stewart and David Tall. *Algebraic Number Theory and Fermat's Last Theorem*. A K Peters, Massachusetts, 3rd edition, 2002.