802656S ALGEBRALLISET LUVUT

ALGEBRAIC NUMBERS

Tapani Matala-aho

MATEMATIIKKA/LUTK/OULUN YLIOPISTO

2020

Sisältö

1 ABSTRACT

Algebrallisten lukujen teoria on kiinteä osa matematiikan lukuteoriaa.

2 INTRODUCTION/JOHDANTO

2.1 Kurssikuvaus

Aluksi kerrataan renkaiden ja kuntien perusteita, joista edetään kuntalaajennuksiin. Erityiseen tarkasteluun otetaan jaollisuus kokonaisalueessa, jonka sovelluksiin törmätään polynomialgebrassa ja kokonaisten algebrallisten lukujen teoriassa.

Algebrallisten lukujen teoria lepää vahvasti polynomialgebraan, josta käsitellään polynomien nollakohtia ja jaollisuutta.

Algebrallisen luvun määritelmä yleistetään kuntalaajennuksien algebrallisiin alkioihin, joista edetään algebrallisiin kuntiin. Tärkeinpinä algebrallisina kuntina saadaan lukukunnat, jotka ovat äärellisesti generoituja kompleksisten algebrallisten lukujen kunnan A alikuntia. Erityisesti tutkitaan neliökuntia.

Edelleen tarkastellaan kokonaisten algebrallisten lukujen jaollisuutta ja tekijöihinjakoa, joita sovelletaan Diofantoksen yhtälöiden ratkaisemiseen.

2.2 Course overview

First we revise some basics of rings and fields which are needed to proceed ahead field extensions. In particular, divisibility in an integral domain is carefully studied yielding to applications in the theory of polynomial algebra and algebraic integers. The theory of algebraic numbers is strongly based on polynomial algebra,

where the properties of zeros and divisibility of polynomials are considered. The definition of an algebraic number will be generalized to the algebraic elements of field extensions going forward to algebraic fields.Considered as most important algebraic fields we get number fields which are finitely generated subfields of the field A of all complex algebraic numbers. In particular, we study quadratic number fields.

Further, we shall consider the divisibility and factorization of algebraic integers with some applications to Diophantine equations.

2.3 BASICS/POHJATIEDOT

Esitiedot:

Algebran ja Lineaarialgebran aineopintokurssit sekä Lukuteorian perusteet.

Kurssilla käytetään Lukuteorian perusteet kurssin merkintöjä.

Notations and basics of Number Theory from the course: Basics of Number Theory.

2.4 LÄHTEITÄ/REFERENCES

I.N. Stewart and D.O. Tall: Algebraic number theory.

Daniel Marcus: Number fields.

J.B. Fraleigh: Abstract algebra.

Michael Artin: Algebra.

Number Theory Web/LINK
American Mathematical Monthly/LINK

2.5 Algebralliset luvut

Määritelmä 1. Algebralliset luvut saadaan rationaalikertoimisten ei-vakiopolynomien nollakohtina./ Algebraic numbers are zeros of non-constant polynomials with rational coefficients.

Esimerkki 1.

Luvut/Numbers

$$-1; \tag{2.1}$$

$$i; \tag{2.2}$$

$$2^{1/3} + 3^{1/2} \tag{2.3}$$

ovat algebrallisia lukuja/are algebraic numbers.

Esimerkki 2.

$$e^{i\pi/m}, \quad m \in \mathbb{Z} \setminus \{0\}; \tag{2.4}$$

$$\sin(\pi/m),\ \cos(\pi/m),\ \tan(\pi/m), \quad m \in \mathbb{Z} \setminus \{0\}; \tag{2.5}$$

ovat algebrallisia lukuja.

Esimerkki 3.

Myös polynomiyhtälön/Also roots of the polynomial equation

$$2^{1/3}x^4 + 3^{1/2}x + 1 = 0 \tag{2.6}$$

juuret ovat algebrallisia lukuja/are algebraic numbers.

Merkintä 1. Olkoon $f : A \to B$ ja $C \subseteq B$. Tällöin joukon C alkukuva/pre-image on joukko

$$f^{-1}(C) = \{x \in A |\ f(x) \in C\}. \tag{2.7}$$

Erityisesti

$$f^{-1}(\{0\}) = \{x \in A |\ f(x) = 0\}. \tag{2.8}$$

Gauss todisti, että kompleksikertoimisella ei-vakiopolynomilla on aina asteen verran kompleksisia nollakohtia.

Lause 1. ALGEBRAN PERUSLAUSE/FUNDAMENTAL THEOREM OF ALGEBRA.
Olkoon/Let $d = \deg p(x) \in \mathbb{Z}^+$ ja

$$p(x) = p_0 + p_1 x + ... + p_d x^d \ \in \mathbb{C}[x], \tag{2.9}$$

tällöin/then

$$\#p^{-1}(\{0\}) = \deg p(x) = d \tag{2.10}$$

eli/or

$$p(x) = p_d(x - \alpha_1) \cdots (x - \alpha_d), \quad \alpha_1, ..., \alpha_d \ \in \mathbb{C}. \tag{2.11}$$

Tällä kurssilla keskitytäänkin kompleksisiin algebrallisiin lukuihin/complex algebraic numbers.

3 Perusteita/Basics

Olkoon K kunta/field ja $d \in \mathbb{Z}^+$. Polynomi

$$p(x) = p_0 + p_1 x + ... + x^d \ \in K[x], \quad d = \deg p(x) \geq 1, \tag{3.1}$$

on pääpolynomi/monic polynomial. Käytetään astetta d olevien pääpolynomien joukolle merkintää

$$K[x]_d = \{p(x) = p_0 + p_1 x + ... + x^d \ \in K[x]\}. \tag{3.2}$$

Määritellään (kompleksiset) algebralliset luvut rationaalilukujen kunnan suhteen.

Määritelmä 2. Joukko

$$\mathbb{A}_d = \{\alpha \ \in \mathbb{C} |\ p(\alpha) = 0,\ p(x) \in \mathbb{Q}[x]_d\} \tag{3.3}$$

on korkeintaan astetta d olevien algebrallisten lukujen joukko. Edelleen

$$\mathbb{A} = \cup_{d=1}^{\infty} \mathbb{A}_d \tag{3.4}$$

on kaikkien (kompleksisten) algebrallisten lukujen joukko.

Määritelmä 3. Olkoon $K \subseteq \mathbb{C}$ ja $p(x) \ \in K[x]$. Tällöin

$$Z(p) = p^{-1}(\{0\}) = \{\alpha \ \in \mathbb{C} |\ p(\alpha) = 0\} \tag{3.5}$$

on polynomin $p(x)$ nollajoukko/zero set.

Lause 2.

$$\mathbb{A}_1 = \mathbb{Q}. \tag{3.6}$$

Merkintä 2. Olkoon $D \in \mathbb{Z}$. Tällöin

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} |\ a, b \in \mathbb{Q}\}. \tag{3.7}$$

Lause 3.

$$\mathbb{A}_2 = \bigcup_{D \in \mathbb{Z}} \mathbb{Q}(\sqrt{D}). \tag{3.8}$$

Todistus.

4 Renkaat ja kunnat

4.1 Rengas/Ring

Tällä kurssilla tarkastellaan ykkösellisiä kommutatiivisia renkaita.

Olkoon R joukko, jossa on ainakin kaksi alkiota, $\#R \geq 2$. Oletetaan, että joukossa R on määritelty laskutoimitus/binary operation $+$ eli kuvaus/or mapping

$$+ : R \times R \to R, \quad (a, b) \to a + b,$$

missä $a + b \in R$, kun $a \in R$ ja $b \in R$ sekä laskutoimitus $*$ eli kuvaus

$$* : R \times R \to R, \quad (a, b) \to a * b,$$

missä $a * b \in R$, kun $a \in R$ ja $b \in R$.

4.1.1 Commutative ring with unity

Määritelmä 4.

Kolmikko $(R, +, *)$ on ykkösellinen kommutatiivinen rengas/a commutative ring with unity , jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun/Addition aksiomit:

1. $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in R$ (liitännäisyys/associativity).
2. $a + b = b + a$ kaikilla $a, b \in R$ (vaihdannaisuus/commutativity).
3. On olemassa nolla-alkio/zero-element $0 \in R$, jolle
   $0 + a = a$ kaikilla $a \in R$.
4. Kaikilla $a \in R$ on olemassa vasta-alkio/inverse $-a \in R$, jolle
   $a + (-a) = 0$.

4.1.2 Ykkösellinen kommutatiivinen rengas

2. Kertolaskun aksiomit:

1. $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in R$ (liitännäisyys).
2. $a * b = b * a$ kaikilla $a, b \in R$ (vaihdannaisuus).
3. On olemassa ykkösalkio/unit-element $1 \in R$, jolle
   $1 * a = a$ kaikilla $a \in K$.

3. Osittelulaki/distribution law:

1. $a * (b + c) = a * b + a * c$ kaikilla $a, b, c \in R$.

Määritelmän 4 mukaista joukkoa R kutsutaan ykköselliseksi kommutatiiviseksi renkaaksi
ja annettuja ehtoja sanotaan rengas-aksiomeiksi/ring-axioms.

Aksiomit 1a–d sanovat, että $(R, +)$ on Abelin ryhmä/Abelian group, jonka laskutoimitusta + kutsutaan yhteenlaskuksi.

Voidaankin sanoa, että $(R, +)$ on renkaan R yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Mutta $R = (R, *)$ EI/NOT ole kertolaskun $*$ suhteen (välttämättä/necessarily) ryhmä/group. Kertolaskun neutraalialkio on ykkös-alkio 1.

Merkintä 3. Yleensä kertolasku $*$ jätetään merkitsemättä eli tehdään samaistus:

$$a * b = ab.$$

Määritelmä 5. Olkoon R ykkösellinen rengas. Joukko

$$R^* = \{\text{yksiköt}\} = \{u \in R \mid \exists\ u^{-1} \in R :\ uu^{-1} = 1\} \tag{4.1}$$

on renkaan R yksikköryhmä (unit group).

Usein käytetään esitystä

$$R^* = \{u \in R \mid \exists\, v \in R :\ uv = 1\}, \tag{4.2}$$

jolloin pätee

$$u \in R^* \quad \Rightarrow \quad 1 = uv, \quad u, v \in R^*. \tag{4.3}$$

Jos $R = K$ kunta/field, niin $K^* = K \backslash \{0\}$.

4.2 Kokonaisalue, Integral Domain

Määritelmä 6. Renkaan R alkio $a \neq 0$ on nollantekijä (zero divisor), jos $\exists\, b \in R\backslash\{0\}$ s.e. $ab = 0$ tai $ba = 0$.

Määritelmä 7. Kommutatiivinen ykkösellinen rengas D on kokonaisalue/integral domain, mikäli D:ssä ei ole nollantekijöitä eli ehdosta
$ab = 0$, $a, b \in D$ aina seuraa $a = 0$ tai $b = 0$.

4.3 Kunta/Field

Määritelmä 8.

Kolmikko $(K, +, *)$ on kunta, jos laskutoimitukset toteuttavat seuraavat aksiomit eli ehdot:

1. Yhteenlaskun aksiomit:

1. $a + (b + c) = (a + b) + c$ kaikilla $a, b, c \in K$ (liitännäisyys).
2. $a + b = b + a$ kaikilla $a, b \in K$ (vaihdannaisuus).
3. On olemassa nolla-alkio $0 \in K$, jolle
   $0 + a = a$ kaikilla $a \in K$.

4. Kaikilla $a \in K$ on olemassa vasta-alkio $-a \in K$, jolle
$a + (-a) = 0$.

2. Kertolaskun aksiomit:

1. $a * (b * c) = (a * b) * c$ kaikilla $a, b, c \in K$ (liitännäisyys).
2. $a * b = b * a$ kaikilla $a, b \in K$ (vaihdannaisuus).
3. On olemassa ykkösalkio $1 \in K$, jolle
$1 * a = a$ kaikilla $a \in K$.
4. Kaikilla $a \in K^* = K \setminus \{0\}$ on olemassa käänteisalkio $a^{-1} \in K^*$, jolle
$a * a^{-1} = 1$.

3. Osittelulaki:

1. $a * (b + c) = a * b + a * c$ kaikilla
2. $a, b, c \in K$.

Määritelmän 8 mukaista joukkoa K kutsutaan kunnaksi
ja annettuja ehtoja sanotaan kunta-aksiomeiksi.

Aksiomit 1a–d sanovat, että $(K, +)$ on Abelin ryhmä, jonka laskutoimitusta $+$ kutsutaan yhteenlaskuksi.
Voidaankin sanoa, että $(K, +)$ on kunnan K yhteenlaskuryhmä, jonka neutraalialkio on nolla-alkio 0.

Edelleen, aksiomit 2a–d sanovat, että $(K^*, *)$ on Abelin ryhmä, jonka laskutoimitusta $*$ kutsutaan kertolaskuksi.
Sanotaan siis, että $(K^*, *)$ on kunnan K kertolaskuryhmä, jonka neutraalialkio on ykkös-alkio 1.

LYHYESTI: Kolmikko $(K, +, \cdot)$, $\#K \geq 2$ on *kunta*, jos:

1. $(K, +)$ on Abelin ryhmä (additiivinen ryhmä),
2. $(K^*, *)$ on Abelin ryhmä (multiplikatiivinen ryhmä), $K^* = K \setminus \{0\}$.
3. $a(b + c) = ab + ac, \ \forall a, b, c \in K$.

Erityisesti, kunta on kommutatiivinen ykkösellinen rengas.

Edelleen kunnassa on aina vähintään kaksi alkiota, nimittäin $0, 1 \in K$, $0 \neq 1$.

Esimerkki 4.

Field K is an integral domain.

Proof: Let

$$ab = 0, \tag{4.4}$$

where $a, b \in K$. Antithesis: $a \neq 0$ and $b \neq 0$.

Because K is a field, then $a^{-1} \in K$. Multiplying (4.4) by a^{-1} gives

$$a^{-1}ab = a^{-1} \cdot 0 \quad \Rightarrow \quad b = 0. \tag{4.5}$$

A contradiction. □

Esimerkki 5.

The fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$, where $p \in \mathbb{P}$, are integral domains.

Esimerkki 6.

Any subring S of a field K is an integral domain.

Esimerkki 7.

$\mathbb{Z}$ is an integral domain.

Esimerkki 8.

The set

$$\mathbb{Z}[i] = \{a + ib |\ a, b \in \mathbb{Z}\} \tag{4.6}$$

of Gaussian integers is an integral domain and its unit group is

$$\mathbb{Z}[i]^* = \{1, i, -1, -i\}. \tag{4.7}$$

Esimerkki 9.

The set

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} |\ a, b \in \mathbb{Z}\} \tag{4.8}$$

is an integral domain and its unit group is

$$\mathbb{Z}[\sqrt{-5}]^* = \{1, -1\}. \tag{4.9}$$

4.3.1 Karakteristika

Määritelmä 9. Kunnan K karakteristika

$$\text{char } K = \begin{cases} p \Leftrightarrow \exists\ p \in \mathbb{P} :\ p1 = 0; \\ 0 \Leftrightarrow \nexists\ n \in \mathbb{Z}^+ :\ n1 = 0. \end{cases}$$

5 Jaollisuus kokonaisalueessa

Olkoon D kokonaisalue/Let D be an integral domain.

Määritelmä 10. Olkoot $a, b \in D$. Tällöin

$$b|a \quad \Leftrightarrow \quad \exists c \in D : \quad a = bc. \tag{5.1}$$

Kun $b|a$, niin b jakaa (divides) a:n eli b on a:n tekijä (factor).

Merkitään: $b \nmid a$, kun b ei jaa a:ta.

Esimerkki 10.

$$0|0, \quad 0 \nmid a \neq 0. \tag{5.2}$$

Merkintä 4. Olkoot $d, b \in D$ ja $s \in \mathbb{N}$, tällöin

$$d^s||b \ \Leftrightarrow\ d^s|b\ ja\ d^{s+1} \nmid b. \tag{5.3}$$

Lemma 1. Olkoot $a, b, c \in D, a \neq 0$. Tällöin

$$ab = ac \quad \Rightarrow \quad b = c. \tag{5.4}$$

Todistus.

$$ab = ac \quad \Rightarrow \quad a(b-c) = 0,\ a \neq 0, \quad \Rightarrow \quad b - c = 0. \quad \square \tag{5.5}$$

Määritelmä 11. Alkiot $a, b \in D$ ovat liitännäisiä (associates) eli

$$a \sim b \quad \Leftrightarrow \quad \exists \quad u \in D^* :\ b = ua. \tag{5.6}$$

Lemma 2. Relaatio $\sim$ on ekvivalenssirelaatio eli

$$a \sim a; \tag{5.7}$$

$$a \sim b \quad \Leftrightarrow \quad b \sim a; \tag{5.8}$$

$$a \sim b, \quad b \sim c \quad \Rightarrow \quad a \sim c. \tag{5.9}$$

Todistus. 5.8:

$$\begin{aligned} a \sim b \quad \Leftrightarrow \quad & b = ua,\ u \in D^* \quad \Leftrightarrow \\ & \exists \quad v \in D^* :\ uv = 1,\ b = ua \quad \Leftrightarrow \quad vb = vua = a \\ & \Leftrightarrow \quad a = vb,\ v \in D^* \quad \Leftrightarrow \quad b \sim a. \quad \square \end{aligned} \tag{5.10}$$

Muut kohdat laskareissa.

Merkintä 5. Alkion $a \in D$ määräämä ekvivalenssiluokka on

$$[a] = \{b \in D |\ b \sim a\}, \tag{5.11}$$

missä a on luokan $[a]$ edustaja.

Lemma 3. Olkoon D kokonaisalue ja $1, a, b \in D$. Tällöin

$$a \sim b \quad \Rightarrow \quad a|b; \tag{5.12}$$

$$a \sim 1 \quad \Leftrightarrow \quad a|1 \quad \Leftrightarrow \quad a \in D^*; \tag{5.13}$$

$$[1] = D^*; \tag{5.14}$$

$$[a] = aD^*; \tag{5.15}$$

$$a \sim b \quad \Leftrightarrow \quad a|b \quad \text{ja} \quad b|a. \tag{5.16}$$

Todistus. 5.13: Oletus $a \in D$.

$$a \sim 1 \quad \Rightarrow \quad 1 = ua,\ u \in D^* \subseteq D \quad \Rightarrow \quad a|1;$$

$$a|1 \quad \Rightarrow \quad \exists\, c \in D:\ 1 = ca \quad \Rightarrow\ c \in D^* \ \Rightarrow\ a \sim 1.$$

$$\rightsquigarrow \qquad a \sim 1 \quad \Leftrightarrow \quad a|1. \quad \square$$

$$a|1 \quad \Rightarrow \quad \exists\, c \in D:\ 1 = ca \quad \Rightarrow \quad a, c \in D^*;$$

$$a \in D^* \quad \Rightarrow \quad 1 = ua, u \in D \quad \Rightarrow \quad a|1.$$

$$\rightsquigarrow \qquad a|1 \quad \Leftrightarrow \quad a \in D^*. \quad \square$$

5.14:

$$b \in [1] \quad \Leftrightarrow \quad b \sim 1 \quad \Leftrightarrow \quad b \in D^*. \quad \square$$

5.15:

$$x \in [a] \quad \Leftrightarrow \quad x \sim a \quad \Leftrightarrow \quad a \sim x$$

$$\Leftrightarrow \quad x = ua,\ u \in D^* \quad \Leftrightarrow \quad x \in aD^*. \quad \square$$

5.16: Tarkastele ensin tapaus $b = 0$, jolloin myös $a = 0$.

$$a \sim b \quad \Leftrightarrow \quad b \sim a, \quad \Rightarrow \quad a|b \quad \text{ja} \quad b|a;$$

$$a|b \quad \text{ja} \quad b|a \quad \Rightarrow \quad b = ca,\ a = db,\ c, d \in D,$$

$$\Rightarrow \quad b = cdb \quad \Rightarrow \quad cd = 1 \quad \Rightarrow \quad c, d \in D^*,$$

$$\Rightarrow \quad a \sim b \quad \text{ja} \quad b \sim a. \quad \square$$

Huomautus 1. Olkoon $b \in D$. Tällöin

$$b = 1 \cdot b = u(u^{-1}b) \quad \forall\ u \in D^*. \tag{5.17}$$

Siten yksiköt ja alkion liitännäiset ovat aina tekijöinä.

Esimerkki 11.

Remember that the unit group of Gaussian integers was

$$\mathbb{Z}[i]^* = \{1, i, -1, -i\}. \tag{5.18}$$

Thus

$$2 - i \sim 1 + 2i \sim -2 + i \sim -1 - 2i \tag{5.19}$$

and the equivalence class

$$[2 - i] = \{2 - i, 1 + 2i, -2 + i, -1 - 2i\} \tag{5.20}$$

of $2 - i$ consists of four elements.

Määritelmä 12. Alkion $b \in D$ triviaalit tekijät/trivial factors q ovat kaikki/are all yksiköt/units ja liittännäiset/associates eli alkiot

$$q \in [1] \quad \text{ja} \quad q \in [b]. \tag{5.21}$$

Alkio $j \in D, j \neq 0, j \notin D^*$ on jaoton/irreducible, mikäli sillä on vain triviaaleja tekijöitä eli

$$q|j \quad \Leftrightarrow \quad q \in [1] \quad \text{tai} \quad q \in [j]. \tag{5.22}$$

Alkio $p \in D, p \neq 0, p \notin D^*$ on alkualkio/prime, mikäli

$$p|ab \quad \Rightarrow \quad p|a \quad \text{tai} \quad p|b \quad \forall a, b \in D. \tag{5.23}$$

Alkio $a \in D, a \notin D^*$ jakaantuu/is reducible, mikäli sillä on aito tekijä $d \in D$ eli

$$\exists\, d \in D: \quad d|a \quad \Rightarrow \quad d \notin [1] \quad \text{ja} \quad d \notin [a]. \tag{5.24}$$

Huomautus 2. Nolla-alkio jakaantuu/zero-element is reducible.

Merkintä 6. Asetetaan

$$J_D = \{j \in D |\ j \text{ on jaoton}\} \tag{5.25}$$

ja

$$P_D = \{p \in D |\ p \text{ on alkualkio}\}. \tag{5.26}$$

Lemma 4. Olkoot $a, b \in D$ ja $j, h \in J_D$. Tällöin

$$j = ab \quad \Rightarrow \quad a \sim 1 \quad \text{tai} \quad b \sim 1. \tag{5.27}$$

$$j = bh, \quad \Rightarrow \quad b \sim 1. \tag{5.28}$$

Todistus (5.27). Antithesis: $a \not\sim 1$ and $b \not\sim 1$

$$\Rightarrow \quad a, b \notin [1] \quad \Rightarrow \quad a, b \in [j] \tag{5.29}$$

because j is irreducible. Thus

$$a = d_1 j \quad b = d_2 j, \quad d_1, d_2 \in D^* \quad \Rightarrow \tag{5.30}$$

$$j = ab = d_1 d_2 j^2 \quad \Rightarrow \quad 1 = d_1 d_2 j \quad \Rightarrow \quad j \in D^* = [1]. \tag{5.31}$$

A contradiction. □

Määritelmä 13. Olkoot $a, b \in D$ annettu/be given. Tällöin alkio $d \in D$ on alkioiden a ja b suurin yhteinen tekijä (greatest common divisor) eli $d = \text{syt}(a,b) = \gcd(a,b) = (a,b)$ mikäli

$$d|a \quad \text{ja} \quad d|b; \tag{5.32}$$

$$c|a \quad \text{ja} \quad c|b \quad \Rightarrow \quad c|d. \tag{5.33}$$

Jos $(a,b) \sim 1$, niin sanotaan, että a ja b ovat keskenään jaottomia (relatively prime) ja merkitään $(a,b) = 1$ tai $a \perp b$.

Määritelmä 14. Olkoot $a, b \in D$ annettu. Tällöin alkio $f \in D$ on alkioiden a ja b pienin yhteinen jaettava (least common multiple) eli $f = \text{pyj}[a,b] = \text{lcm}[a,b] = [a,b]$ mikäli

$$a|f \quad \text{ja} \quad b|f; \tag{5.34}$$

$$a|g \quad \text{ja} \quad b|g \quad \Rightarrow \quad f|g. \tag{5.35}$$

Esimerkki 12.

$$(0,0) = 0, \quad [0,0] = 0. \tag{5.36}$$

Lemma 5. Olkoot $a \in D$ ja $j \in J_D$. Tällöin

$$j \not| a \quad \Rightarrow \quad (a,j) = 1. \tag{5.37}$$

Todistus. Antithesis: $(a,j) \neq 1$. Therefore $(a,j) = d \not\sim 1$ and

$$d|a \quad \text{and} \quad d|j, \quad j \in J_D. \tag{5.38}$$

Because j is irreducible, then $d \sim 1$ or $d \sim j$, hence $d \sim j$. Consequently

$$d = vj, \ v \in D^* \quad \text{and} \quad a = cd = cvj \quad \Rightarrow \quad j|a. \tag{5.39}$$

A contradiction. □

Määritelmä 15. Alkion $a \in D$ esitys jaottomien alkioiden tulona on yksikäsitteinen, jos ehdosta/ The representation of the element $a \in D$ by irreducible elements is unique, if from the condition

$$a = j_1 \cdots j_r = h_1 \cdots h_s, \quad j_l, h_k \in J_D \tag{5.40}$$

seuraa/follows

$$r = s \quad \text{ja} \quad h_k \sim j_l \quad \forall k = 1, ..., r \quad \text{jollakin } l = 1, ..., r. \tag{5.41}$$

Määritelmä 16. Kokonaisalue D on UFD eli yksikäsitteisen tekijöihinjaon alue/unique factorization domain, jos jokainen alkio $a \in D, a \neq 0, a \notin D^*$ voidaan esittää yksikäsitteisesti muodossa

$$a = j_1 \cdots j_r, \quad j_i \in J_D. \tag{5.42}$$

Lause 4. Olkoon D kokonaisalue/Let D be an ID. Tällöin/Then

$$P_D \subseteq J_D \tag{5.43}$$

eli alkualkiot ovat jaottomia/primes are irreducible..

Todistus. (5.43): Let $p \in P_D$. If $q|p$, then $p = qd_1$ for some $d_1 \in D$. Then

$$p|qd_1 \quad \Rightarrow \quad p|q \quad \text{or} \quad p|d_1 \tag{5.44}$$

because p is a prime.

If $p|q$, then $q = d_2 p$, $d_2 \in D$ and $q = d_2 q d_1$, where $q \neq 0$ by $p \neq 0$. So $1 = d_1 d_2$ meaning that $d_1, d_2 \in D^*$. Therefore $q \in [p]$.

If $p|d_1$, then (homework...) $q \in [1]$.

Thus $p \in J_D$. □

Lause 5. Olkoon D kokonaisalue. Tällöin

$$D = \text{UFD} \quad \Rightarrow \quad J_D \subseteq P_D \tag{5.45}$$

eli UFD:n jaottomat alkiot ovat alkualkiota/irreducibles are primes ja tällöin $J_D = P_D$.

Todistus: Olkoon $j \in J_D$ ja oletetaan, että $j|ab$, missä $a, b \in D$. Koska D =UFD, niin a:lla ja b:llä $\exists!$ esitykset

$$a = a_1 \cdots a_m, \quad b = b_1 \cdots b_n, \quad a_i, b_i \in J_D. \tag{5.46}$$

Siten

$$j|a_1 \cdots a_m b_1 \cdots b_n = j \cdot j_2 \cdots j_{m+n}, \tag{5.47}$$

josta seuraa että $j \sim a_i$, jollakin a_i tai $j \sim b_i$, jollakin b_i, koska D =UDF. Täten $j|a$ tai $j|b$.

Siispä $j \in P_D$. □

Huomautus 3. Yksikäsitteisessä tekijöihinjaon alueessa esitystä (5.42) sanotaan alkion a alkutekijähajotelmaksi. In UFD the representation (5.42) is called prime factorization.

Määritelmä 17. Olkoon D kokonaisalue ja $a \in D$. Jos jaottomalle alkiolle $j \in J_D$ pätee

$$j^m \| a, \quad m \in \mathbb{Z}_{\geq 0}, \tag{5.48}$$

niin luku m on alkion a tekijän j kertaluku/multiplicity of the factor.

Tietenkin, jos $j \not| a$, niin $m = 0$.

Lause 6. Olkoon D kokonaisalue. Tällöin

$$J_D \subseteq P_D \quad \Rightarrow \quad D = \text{UFD}. \tag{5.49}$$

Todistus: Let

$$a = j_1 \cdots j_r = h_1 \cdots h_s, \quad j_l, h_k \in J_D \tag{5.50}$$

Now irreducibles j_l and h_k are primes. Thus

$$j_1 | h_1 \cdots h_s \quad \Rightarrow \quad j_1 | h_1 \quad \text{or} \quad j_1 | h_2 \cdots h_s \ldots \tag{5.51}$$

and eventually $j_1 | h_{k_1}$ implying $j_1 \sim h_{k_1}$,...,$j_r \sim h_{k_r}$ and $r = s$. □

5.1 Jako- ja Eukleideen algoritmit kokonaisalueessa

5.1.1 Division algorithm/Euclidean domain

Olkoon nyt D kokonaisalue, jossa on ns. Eukleideen funktio $E: \ D \to \mathbb{N} \cup \{-\infty\}$ eli pätee

Jakoalgoritmi: Jos $a, b \in D$ on annettu ja $ab \neq 0, 0 \leq E(b) \leq E(a)$, niin $\exists\, q, r \in D$ s.e.

$$(J.A.) \quad a = qb + r \text{ ja } E(r) < E(b). \tag{5.52}$$

Tälläista aluetta sanotaan Eukleideen alueeksi/This kind of domain is called Euclidean domain/ED. (huomaa, että Eukleideen funktion määritelmä vaihtelee.)

Esimerkki 13. a)$D = \mathbb{Z}, \quad E(k) = |k|$.

b)$D = K[x], \quad E(p(x)) = \deg p(x)$.

Jakoalgoritmin nojalla saadaan

Eukleideen algoritmi=E.A.:

$$\begin{aligned}
&r_0 = a,\ r_1 = b && E(r_1) < E(r_0)\\
&r_0 = q_1 r_1 + r_2 && E(r_2) < E(r_1)\\
&\vdots\\
&r_k = q_{k+1} r_{k+1} + r_{k+2} && E(r_{k+2}) < E(r_{k+1})\\
&\vdots\\
&r_{n-1} = q_n r_n && \exists\, n \in \mathbb{N} :\ r_n \neq 0,\ r_{n+1} = 0\\
&r_n = \mathrm{syt}(a, b).
\end{aligned}$$

Tässä $n =$ Eukleideen algoritmin pituus/length.

Set now/Asetetaan nyt

$$R_k = \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix},\ Q_k = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix},\ k \in \mathbb{N}, \tag{5.53}$$

whereupon/jolloin

$$\det Q_k = -1, \quad {Q_k}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix}. \tag{5.54}$$

We see that/Nähdään, että

$$\text{E.A.} \Leftrightarrow R_k = Q_{k+1} R_{k+1},\ \forall k = 0, \ldots, n-1, \tag{5.55}$$

whereupon holds/jolloin pätee

$$R_0 = Q_1 Q_2 \cdots Q_k R_k. \tag{5.56}$$

Denote/Merkitään

$$S_0 = \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{5.57}$$

ja

$$S_k = \begin{pmatrix} s_k & t_k \\ s_{k+1} & t_{k+1} \end{pmatrix} = {Q_k}^{-1} \cdots {Q_2}^{-1} {Q_1}^{-1}, \tag{5.58}$$

jolloin

$$R_k = S_k R_0. \tag{5.59}$$

Nyt

$$S_{k+1} = Q_{k+1}^{-1} S_k \tag{5.60}$$

eli

$$\begin{pmatrix} s_{k+1} & t_{k+1} \\ s_{k+2} & t_{k+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{k+1} \end{pmatrix} \begin{pmatrix} s_k & t_k \\ s_{k+1} & t_{k+1} \end{pmatrix} = \begin{pmatrix} s_{k+1} & t_{k+1} \\ s_k - q_{k+1}s_{k+1} & t_k - q_{k+1}t_{k+1} \end{pmatrix} \tag{5.61}$$

$\Leftrightarrow$ Palautuskaavat eli rekursiot/recurrences:

$$\begin{cases} s_{k+2} = s_k - q_{k+1}s_{k+1}, \ k = 0, 1, \ldots \\ t_{k+2} = t_k - q_{k+1}t_{k+1}, \ k = 0, 1, \ldots \end{cases} \tag{5.62}$$

From formula/Yhtälöstä (5.59) we get/saadaan

$$r_n = s_n a + t_n b, \tag{5.63}$$

josta edelleen/further saadaan

Lause 7. Olkoon D Eukleideen alue/ED, silloin

$$\text{syt}(a, b) = s_n a + t_n b, \tag{5.64}$$

where/missä n on E.A:n pituus/lenght.

Usein riittää seuraava tulos/Usually the following formulation is enough

Lause 8. Let D be an ED. Then there exist $s, t \in D$ such that

$$\gcd(a, b) = sa + tb. \tag{5.65}$$

Lause 9. Olkoon D Eukleideen alue. Tällöin

$$J_D \subseteq P_D \tag{5.66}$$

eli jaottomat alkiot ovat alkualkioita/In ED irreducibles are primes.

Edelleen, Eukleideen alue on UFD.

Todistus. Let $j \in J_D$ and let us assume, that $j|ab$, where $a, d \in D$.

We should show that $j|a$ or $j|b$.

Suppose that $j \not| a$, then $j \perp a$ by Lemma 5. Then by Theorem 8 there exist $s, t \in D$ such that

$$1 = sa + tj \quad \Rightarrow \quad b = sab + tbj \quad \Rightarrow \quad j|b. \quad \square \tag{5.67}$$

Seuraus 1. .

A. $\mathbb{Z}$ on UFD, missä jaottomat alkiot ovat alkualkioita.

B. $K[x]$ on UFD, missä jaottomat alkiot ovat alkualkioita.

6 Polynomialgebraa

6.1 Polynomirengas

6.1.1 Polynomijoukko

Olkoon R ykkösellinen rengas. Tällöin R-kertoimisten polynomien joukolle käytetään merkintää

$$R[x] = \{P(x) \mid P(x) = \sum_{k=0}^{n} p_k x^k;\ p_k \in R,\ n \in \mathbb{N}\}.$$

Polynomia

$$0(x) = 0 + 0 \cdot x + 0 \cdot x^2 + \dots \tag{6.1}$$

kutsutaan nollapolynomiksi ja polynomia

$$1(x) = 1 + 0 \cdot x + 0 \cdot x^2 + \dots \tag{6.2}$$

ykköspolynomiksi. Ne ovat erikoistapauksia vakiopolynomista

$$c(x) = c + 0 \cdot x + 0 \cdot x^2 + \dots, \quad c \in R. \tag{6.3}$$

6.1.2 Laskutoimitukset

Määritelmä 18. Olkoot $P(x) = \sum_{k=0}^{n} p_k x^k, \quad Q(x) = \sum_{k=0}^{n} q_k x^k \in R[x]$, jolloin asetetaan

$$\begin{aligned} P(x) = Q(x) &\Leftrightarrow \forall k(p_k = q_k); \\ P(x) + Q(x) &= \sum_{k \geqslant 0} (p_k + q_k) x^k; \\ P(x) \cdot Q(x) &= \sum_{k \geqslant 0} r_k x^k, \end{aligned}$$

$$r_k = \sum_{i=0}^{k} p_i q_{k-i} = \sum_{i+j=k} p_i q_j, \tag{6.4}$$

joka on Cauchyn kertosääntö.

6.1.3 Polynomial ring/degree

Lause 10. Tällöin $(R[x], +, \cdot)$ on rengas, missä $0(x)$ on yhteenlaskun nolla-alkio ja $1(x)$ on kertolaskun ykkösalkio.

Määritelmä 19. Jos $p_n \neq 0$, niin polynomin $P(x) = \sum_{k=0}^{n} p_k x^k$ aste/degree on

$$\deg P(x) = n, \tag{6.5}$$

lisäksi asetetaan/set

$$\deg 0(x) = -\infty. \tag{6.6}$$

6.1.4 Astekaava/Degree formula

Huomautus 4.

$$\begin{aligned} &-\infty + (-\infty) = -\infty \\ &-\infty + k = -\infty, \quad \forall\ k \in \mathbb{Z}. \end{aligned} \tag{6.7}$$

Lause 11. Degree formula.

Olkoon D kokonaisalue ja $P(x), Q(x) \in D[x]$. Tällöin

$$\deg P(x)Q(x) = \deg P(x) + \deg Q(x). \tag{6.8}$$

Lause 12. .

A. Olkoon $R = D$ kokonaisalue. Tällöin polynomirengas $D[x]$ on kokonaisalue.

B. Olkoon $R = K$ kunta. Tällöin polynomirengas $K[x]$ on kokonaisalue.

Todistus: Olkoon $a(x)b(x) = 0(x)$. Astekaavan nojalla

$$\deg a(x)b(x) = \deg a(x) + \deg b(x) = \deg 0(x) = -\infty. \tag{6.9}$$

Jos olisi $a(x) \neq 0(x)$ ja $b(x) \neq 0(x)$, niin

$$0 \leq \deg a(x) + \deg b(x) = -\infty. \tag{6.10}$$

Ristiriita. □

Lause 13. Olkoon K kunta.

A. Polynomirenkaan $K[x]$ yksikköryhmä on K^* eli

$$K[x]^* = K^*. \tag{6.11}$$

B. Polynomi $j(x) \in K[x] \setminus K$ on jaoton täsmälleen silloin, kun sen ainoat tekijät ovat vakioita k tai polynomeja $k \cdot j(x)$, missä $k \in K \setminus \{0\}$.
C. Edelleen, polynomi $a(x) \in K[x] \setminus \{0(x)\}$ on jaollinen täsmälleen silloin, kun sillä on tekijä $d(x) \in K[x]$, jolle pätee

$$1 \leq \deg d(x) \leq \deg a(x) - 1. \tag{6.12}$$

D. Erityisesti ensimmäisen asteen polynomit ovat jaottomia.

Todistus. A: $a(x) \in K[x]^* \quad \Rightarrow \quad \exists\, b(x) \in K[x]$ such that

$$a(x)b(x) = 1 \quad \Rightarrow \quad \deg a(x) = \deg b(x) = 0 \quad \Rightarrow \quad a(x), b(x) \in K^*. \quad \square$$

Todistus. B: $j(x) = a(x)b(x) \in J_{K[x]} \quad \Rightarrow$

$$a(x) \in [1] = K[x]^* = K^* \quad \Rightarrow \quad a(x) = k, \quad k \in K^*$$

or

$$a(x) \in [j(x)] = j(x)K^* \quad \Rightarrow \quad a(x) = kj(x), \quad k \in K^*. \quad \square$$

Todistus. C: Let $a(x) \in K[x] \setminus \{0\}$ be reducible. Then there exists $d(x), b(x) \in K[x] \setminus \{0\}$ such that

$$a(x) = d(x)b(x), \quad d(x) \notin [1] \quad \text{and} \quad d(x) \notin [a(x)] \quad \Rightarrow$$

$$d(x) \notin K^* \quad \text{and} \quad d(x) \notin a(x)K^*.$$

If $\deg d(x) = 0$, then $d(x) \in K^*$; a contradiction.
If $\deg d(x) = \deg a(x)$, then by the degree formula $\deg b(x) = 0$ implying $b(x) = k \in K^*$. Thus $a(x) = kd(x)$ and then $d(x) \in [a(x)]$; a contradiction. $\square$

Todistus. D: Homework.

6.2 Renkaan $R[x]$ yksikköryhmästä/On the unit group of the ring $R[x]$

Let R be commutative ring with a unit. Let us study its unit group $R[x]^*$. Pick $a(x) = a_0+a_1x+...+a_Ax^A \in R[x]^*$, then there exists $b(x) = b_0+b_1x+...+b_Bx^B \in R[x]^*$ such that

$$1 = a(x)b(x) = (a_0 + a_1x + ... + a_Ax^A)(b_0 + b_1x + ... + b_Bx^B). \tag{6.13}$$

If $a_1 = ... = a_A = 0$, then $a(x) \in R^*$. Otherwise there exists an $A \geq 1$ such that $a_A \neq 0$. Then

$$\begin{aligned} &a_0b_0 = 1 \\ &a_0b_1 + a_1b_0 = 0 \\ &a_0b_2 + a_1b_1 + a_2b_0 = 0 \\ &\dots \\ &a_{A-2}b_B + a_{A-1}b_{B-1} + a_Ab_{B-2} = 0 \\ &a_{A-1}b_B + a_Ab_{B-1} = 0 \\ &a_Ab_B = 0 \end{aligned} \tag{6.14}$$

Multiply the second last by a_A to get

$$a_{A-1}a_Ab_B + a_A^2b_{B-1} = 0 \quad \Rightarrow \quad a_A^2b_{B-1} = 0 \tag{6.15}$$

$$\begin{aligned} &\dots \\ &a_{A-2}b_B + a_{A-1}b_{B-1} + a_Ab_{B-2} = 0 \\ &a_{A-1}b_B + a_Ab_{B-1} = 0 \\ &a_Ab_B = 0 \end{aligned} \tag{6.16}$$

Multiply the third last by a_A^2 to get

$$a_{A-2}a_A^2b_B + a_{A-1}a_A^2b_{B-1} + a_A^3b_{B-2} = 0 \quad \Rightarrow \quad a_A^3b_{B-2} = 0 \tag{6.17}$$

and so on to the situation

$$\begin{aligned} &\dots \\ &a_0 b_B + a_1 b_{B-1} + ... + a_A b_0 = 0, \quad A \leq B \\ &a_A^A b_1 = 0 \end{aligned} \tag{6.18}$$

or

$$\begin{aligned} &\dots \\ &a_c b_B + a_1 b_{B-1} + ... + a_A b_0 = 0, \quad A = B + c, c > 0, \\ &a_A^A b_1 = 0. \end{aligned} \tag{6.19}$$

Anyway, multiply now by a_A^A. Then you get

$$a_A^{A+1} b_0 = 0, \tag{6.20}$$

where $b_0 \in R^*$ meaning that $b_0 \neq 0$. Then multiplying by b_0^{-1} we are in the situation $a_A^{A+1} = 0$.

Thus if

$$r^K \neq 0 \quad \forall\ r \in R \setminus \{0\},\ K \geq 2, \tag{6.21}$$

then $a(x) = a_0 \in R^*$.

Otherwise: if there exists such an element $r \in R \setminus \{0\}$ that

$$r^K = 0 \quad \text{for some} \quad K \geq 2, \tag{6.22}$$

then you may find a non-constant unit polynomial $a(x)$ i.e $a(x) \in R[x]^* \setminus R^*$.

6.2.1 $\mathbb{Z}_m[x]^*$

Esimerkki 14.

$$\mathbb{Z}_{10}[x]^* = \mathbb{Z}_{10}^*.$$

Esimerkki 15.

$$1 + 10x\ \in \mathbb{Z}_{20}[x]^*.$$

6.3 Jakoalgoritmi/Division algorithm

Lause 14. Division algorithm. Olkoon K kunta. Olkoon $a(x), b(x) \in K[x]$, $a(x)b(x) \neq 0(x)$ ja $\deg b(x) \leq \deg a(x)$.
Tällöin $\exists\ q(x), r(x) \in K[x]$ s.e.

$$[J.A.] \quad a(x) = q(x)b(x) + r(x), \quad \deg r(x) < \deg b(x). \tag{6.23}$$

Edelleen, $K[x]$ on Eukleideen alue!

Huomautus 5. Jos D ei ole kunta, niin jakoalgoritmi ei välttämättä päde polynomirenkaassa $D[x]$!!
If D is not a field, then the division algorithm does not work necessarily in the polynomial ring $D[x]$!!

Polynomien $a(x)$ ja $b(x)$ suurin yhteinen tekijä $d(x) = \text{s.y.t.}(a(x), b(x))$ voidaan valita pääpolynomiksi.

Eukleideen algoritmin nojalla saadaan, että on olemassa sellaiset polynomit $s(x), t(x) \in K[x]$, että

$$d(x) = s(x)a(x) + t(x)b(x). \tag{6.24}$$

Määritelmä 20. Polynomin

$$p(x) = \sum_{k=0}^{n} p_k x^k \in K[x]$$

(formaali) derivaatta $Dp(x)$on polynomi

$$Dp(x) = \sum_{k=1}^{n} k p_k x^{k-1} \in K[x]. \tag{6.25}$$

Lemma 6. Olkoon K kunta, $p(x) \in K[x]$ ja $\deg p(x) \geq 1$. Tällöin

$$\deg Dp(x) = \deg p(x) - 1, \quad \deg p(x) \geq 1; \tag{6.26}$$

$$p(x) \not| Dp(x). \tag{6.27}$$

Lause 15. Olkoon K kunta ja $a(x), b(x), c(x) \in K[x]$. Tällöin

$$a = b^2 c, \quad b \not\sim 1 \quad \Leftrightarrow \quad d = \mathrm{syt}(a, Da) \not\sim 1. \tag{6.28}$$

Todistus.

Olkoon $a = b^2 c$, $b \not\sim 1$. Koska $Da = b(2cDb + bDc)$, niin $b|\mathrm{syt}(a, Da)$ ja siten $\mathrm{syt}(a, Da) \not\sim 1$.

Olkoon $d = \mathrm{syt}(a, Da) \not\sim 1$. Tällöin on olemassa $p \in P_{K[x]}$, $p|d$. Siten $a = ps$ ja $Da = pr$. Toisaalta $Da = (Dp)s + pDs$, joten $pr = (Dp)s + pDs$. Koska $p \nmid Dp$ ja p on alkualkio, niin $p|s$. Niinpä $s = ph$ ja $a = ps = p^2 h$, jollakin h ja $p \not\sim 1$. □

Väite (6.28) on yhtäpitävää seuraavan väitteen kanssa:
Polynomi on neliövapaa täsmälleen silloin kun sillä ei ole yhteisiä tekijöitä derivaattansa kanssa.

Claim (6.28) is equivalent to following claim:
A polynomial is square-free exactly when it does not have common factors with its derivative.

Esimerkki 16. Olkoon $p(x) = x^5 + 2x^3 + x \in \mathbb{Q}[x]$. Laskemalla saadaan/by calculating

$$syt(p, Dp) \not\sim 1 \quad \Rightarrow \tag{6.29}$$

polynomilla $p(x)$ on useampikertainen tekijä/higher order factor/multiple factor renkaassa $\mathbb{Q}[x]$.

6.4 Polynomien nollakohdista

Lause 16. Olkoon K kunta ja $p(x) \in K[x]$, $1 \leq \deg p(x)$. Tällöin

$$p(\alpha) = 0,\ \alpha \in K \Leftrightarrow (x-\alpha) \underset{K[x]}{|} p(x). \tag{6.30}$$

Todistus. "$\Diamond \rightarrow$": Olkoon $p(\alpha) = 0,\ \alpha \in K$. Jakoalgoritmin nojalla

$$p(x) = q(x)(x-\alpha) + r(x), \quad \deg r(x) < \deg(x-\alpha) = 1, \tag{6.31}$$

joten $r(x) \in K$ on vakio. Edelleen

$$0 = p(\alpha) = q(\alpha)(\alpha-\alpha) + r(\alpha) = r(\alpha),$$
$$\Rightarrow \quad r(x) = 0(x) \quad \Rightarrow \quad (x-\alpha) \underset{K[x]}{|} p(x). \tag{6.32}$$

"$\leftarrow \triangle$":

$$(x-\alpha) \underset{K[x]}{|} p(x) = (x-\alpha)h(x), \qquad \Rightarrow \quad p(\alpha) = 0,\ \alpha \in K. \quad \square \tag{6.33}$$

Huomautus 6. Olkoon K on kunta ja $p(x) \in K[x]$, $\deg p(x) = 2$ tai $\deg p(x) = 3$. Jos $p(x)$ jakaantuu/is reducible polynomirenkaassa $K[x]$, niin sillä on 1. asteen tekijä/then it has first degree factor ja Lauseen 16 nojalla $p(\alpha) = 0,\ \alpha \in K$. Jos nollakohtaa ei ole K:ssa/If there is no zero in K, niin $p(x)$ on jaoton/irreducible polynomirenkaassa $K[x]$.

Laajennetaan Määritelmää 3.

Määritelmä 21. Olkoon $K \subseteq L$ kuntia ja $p(x) \in K[x]$. Tällöin

$$Z_L(p) = \{\alpha\ \in L |\ p(\alpha) = 0\} \tag{6.34}$$

on polynomin $p(x)$ nollajoukko L:ssä.

Määritelmä 22. Olkoon $\alpha \in L$, $K \subseteq L$ kuntia ja $p(x)\ \in K[x]$. Jos

$$(x-\alpha)^m \underset{L[x]}{\|} p(x), \quad m \in \mathbb{N}, \tag{6.35}$$

niin $m = m_L(\alpha, p(x))$ on polynomin $p(x)$ nollakohdan $\alpha \in L$ kertaluku/order of zero/multiplicity of zero. Edelleen

$$n_L(p(x)) = \sum_{p(\alpha_i)=0,\ \alpha_i \in L} m_L(\alpha_i, p(x)). \tag{6.36}$$

nollakohtien lukumäärä/number of zeros joukossa L.

Lause 17. Olkoon K kunta, char K=0, $\alpha \in K$ ja $p(x) \in K[x]$ ja $m \in \mathbb{N}$. Tällöin

$$(x-\alpha)^m \underset{K[x]}{\parallel} p(x) \quad \Leftrightarrow \tag{6.37}$$

$$D^k p(\alpha) = 0 \quad \forall\ k = 0, ..., m-1 \quad , D^m p(\alpha) \neq 0. \tag{6.38}$$

Huomautus 7. Lause 17 EI päde esimerkiksi polynomirenkaassa $\mathbb{Z}_p[x]$.

Esimerkki 17. Olkoon $p(x) = (x-1)^3(x+1/2)^5$. Polynomin $p(x)$ nollakohdat ovat $\alpha_1 = 1$ ja $\alpha_2 = -1/2$. Nollakohtien kertaluvut ovat

$$m_{\mathbb{Q}}(\alpha_1, p(x)) = 3, \quad m_{\mathbb{Q}}(\alpha_2, p(x)) = 5 \tag{6.39}$$

ja nollakohtien lukumäärä

$$n_{\mathbb{Q}} = 3 + 5 = 8. \tag{6.40}$$

Esimerkki 18. Olkoon $(x^2+1)(x^2-2) \in \mathbb{R}[x]$. Nyt nollakohtien lukumäärät ovat

$$n_{\mathbb{Q}} = 0 < 4 = \deg p(x). \tag{6.41}$$

$$n_{\mathbb{R}} = m(-\sqrt{2}) + m(\sqrt{2}) = 2 < 4 = \deg p(x). \tag{6.42}$$

$$n_{\mathbb{C}} = 4 = \deg p(x). \tag{6.43}$$

Lause 18. Olkoon K kunta, $p(x) \in K[x]$ ja $\deg p(x) \geq 1$. Tällöin pätee

$$n_K(p(x)) \leq \deg p(x). \tag{6.44}$$

Todistus:

1. Jos $\nexists$ nolla-kohtaa, niin $m_K(\alpha, p(x)) = 0$, kaikilla $\alpha \in K$. Siten $n_K(p(x)) = 0 < 1 \leq \deg p(x)$.

2. Olkoot $\beta_1, ..., \beta_k$ erillisiä nollakohtia, jolloin

$$m_j := m_K(\beta_j, p(x)) \geq 1 \quad \text{ja} \quad (x - \beta_j)^{m_j} \underset{K[x]}{\parallel} p(x), \quad j = 1, ..., k. \tag{6.45}$$

Siten

$$p(x) = (x - \beta_1)^{m_1} p_2(x), \quad p_2(\beta_1) \neq 0 \quad \Rightarrow \quad p_2(\beta_2) = 0, \tag{6.46}$$

$$p_2(x) = (x - \beta_2)^{m_2} p_3(x), \quad p_3(\beta_2) \neq 0 \quad \Rightarrow \quad p_3(\beta_3) = 0 \quad ... \tag{6.47}$$

... Lopulta

$$p(x) = (x - \beta_1)^{m_1} \cdots (x - \beta_k)^{m_k} p_{k+1}(x), \quad \deg p_{k+1}(x) \geq 0. \tag{6.48}$$

Astekaavalla saadaan

$$\begin{aligned} \deg p(x) &= m_1 + ... + m_k + \deg p_{k+1}(x) \\ &\geq m_1 + ... + m_k = n_K(p(x)). \quad \square \end{aligned} \tag{6.49}$$

Lause 19. ALGEBRAN PERUSLAUSE.

Olkoon $p(x) \in \mathbb{C}[x]$, $\deg p(x) \geq 1$, tällöin

$$n_{\mathbb{C}}(p(x)) = \deg p(x). \tag{6.50}$$

Lause 20. Olkoot $K \subseteq L$ kuntia, $p(x) \in K[x]$ ja $p(x) \in J_{K[x]}$. Tällöin

$$m_L(\alpha, p(x)) \leq 1 \quad \forall \alpha \in L. \tag{6.51}$$

Todistus. Koska $p \in J_{K[x]}$, niin $\deg p(x) \geq 1$ ja siten $p \not| Dp$. Täten Lemman 5 nojalla $p \perp Dp$ ja edelleen Lauseen 8 nojalla

$$\mathrm{syt}_{K[x]}(p, Dp) = 1 = sp + tDp, \quad s, t \in K[x] \subseteq L[x]. \tag{6.52}$$

Jos nyt

$$d \underset{L[x]}{\mid} p \quad \text{ja} \quad d \underset{L[x]}{\mid} Dp \tag{6.53}$$

niin yhtälön (6.52) mukaan $d \underset{L[x]}{\mid} 1$. Siten myös

$$\mathrm{syt}_{L[x]}(p, Dp) = 1. \tag{6.54}$$

Tällöin Lauseen 15 nojalla $\nexists$ neliötekijää renkaassa $L[x]$, joten $\nexists$ sellaista $\alpha \in L$, että

$$(x - \alpha)^2 \underset{L[x]}{\mid} p(x). \tag{6.55}$$

Siten:

Jos $p(\alpha) = 0$, niin $m_L(\alpha, p(x)) = 1$ ja

jos $p(\alpha) \neq 0$, niin $m_L(\alpha, p(x)) = 0$. □

Lause 21. Olkoon K kunta, $p(x), q(x) \in K[x]$, $p(x) \in J_{K[x]}$ sekä $p(\alpha) = q(\alpha) = 0$. Tällöin

$$p(x) \underset{K[x]}{\mid} q(x). \tag{6.56}$$

Todistus. Koska p on jaoton, niin

$$d = \mathrm{syt}_{K[x]}(p, q) = 1 \quad \text{tai} \quad p. \tag{6.57}$$

Jos $d = 1$, niin $1 = s(x)p(x) + t(x)q(x)$ ja edelleen $1 = s(\alpha)p(\alpha) + t(\alpha)q(\alpha) = 0$. Ristiriita.

Niinpä $d = p$ ja siten $p|q$. □

6.5 Polynomien jaottomuudesta/tekijöihinjaosta

Seuraavassa käytetään jakojäännösluokkia $\overline{a} \in \mathbb{Z}_n$. Huomaa, että kun $p \in \mathbb{P}$, niin $\mathbb{Z}_p$ on kunta.

Määritelmä 23. Olkoon $n \in \mathbb{Z}_{\geq 2}$ ja $a(x) = a_0 + a_1 x + ... + a_d x^d \in \mathbb{Z}[x]$. Kuvaus

$$r_n(a_0 + a_1 x + ... + a_d x^d) = \overline{a}_0 + \overline{a}_1 x + ... + \overline{a}_d x^d \tag{6.58}$$

$$r_n : \ \mathbb{Z}[x] \to \mathbb{Z}_n[x], \quad r_n(a(x)) = \overline{a}(x),$$

on reduktio $\pmod{n}$.

Lause 22. Reduktio

$$r_n : \ \mathbb{Z}[x] \to \mathbb{Z}_n[x], \quad r_n(a(x)) = \overline{a}(x),$$

on rengasmorfismi.

Määritelmä 24. Vektori $(a_0, ..., a_A) \in \mathbb{Z}^{m+1}$ ja polynomi $a(x) = a_0 + a_1 x + ... + a_A x^A \in \mathbb{Z}[x]$ ovat primitiivisiä, jos

$$syt(a_0, ..., a_A) = 1. \tag{6.59}$$

Joskus vaaditaan, että primitiiviselle polynomille pätee lisäksi $a_A \geq 1$.

Lemma 7. Olkoot $a(x) \in \mathbb{Z}[x]$ ja $B, C \in \mathbb{Z}$.

A. Jos $a(x)$ on primitiivinen, niin

$$B \underset{\mathbb{Z}[x]}{|} C \cdot a(x) \quad \Rightarrow \quad B \underset{\mathbb{Z}}{|} C. \tag{6.60}$$

B. Jos $D = \text{syt}(a_0, ..., a_A)$, niin

$$a(x) = D \cdot b(x), \quad b(x) \in \mathbb{Z}[x], \tag{6.61}$$

missä polynomi $b(x)$ on primitiivinen.

C. Kohtien A. ja B. polynomit voi korvata vastaavilla vektoreilla/polynomials may be replaced by corresponding vectors.

Lemma 8. Olkoot $b(x)$ ja $c(x)$ primitiivisiä. Tällöin $b(x)c(x)$ on primitiivinen

Todistus. Olkoon

$$a(x) = b(x)c(x) = a_0 + a_1x + ... + a_Ax^A \in \mathbb{Z}[x] \tag{6.62}$$

ja

$$syt(a_0, ..., a_A) = d \geq 2 \quad \Rightarrow \quad \exists \quad p \in \mathbb{P}, \quad p|d. \tag{6.63}$$

Otetaan reduktio $\pmod p$, jolloin

$$\overline{a}(x) = \overline{0}(x) = \overline{b}(x)\overline{c}(x) \quad \in \mathbb{Z}_p[x]. \tag{6.64}$$

Nyt $\mathbb{Z}_p[x]$ on kokonaisalue, joten

$$\overline{b}(x) = \overline{0}(x) \quad \text{tai} \quad \overline{c}(x) = \overline{0}(x). \tag{6.65}$$

Siten

$$p|syt(b_0, ..., b_B) \quad \text{tai} \quad p|syt(c_0, ..., c_C) \tag{6.66}$$

mikä on ristiriita. □

Merkintä 7. A. Olkoon $B = \frac{q}{r} \in \mathbb{Q}$, $q \in \mathbb{Z}$, $r \in \mathbb{Z}^+$, $q \perp r$. Tällöin

$$den(B) := r \tag{6.67}$$

on rationaaliluvun B nimittäjä.

Olkoot $\text{den}(B_j) = r_j$, $j = 1, ..., m$, rationaalilukujen B_j nimittäjiä. Tällöin

$$pyn(B_1, ..., B_m) := pyj(r_1, ..., r_m) \tag{6.68}$$

on lukujen $B_1, ..., B_m$ pienin yhteinen nimittäjä (least common denominator=lcd).

Lemma 9. Olkoon

$B(x) = B_0 + B_1x + ... + B_mx^m \in \mathbb{Q}[x]$ ja

$$R := pyn(B_0, B_1, ..., B_m), \quad Q := syt(RB_0, ..., RB_m). \tag{6.69}$$

Tällöin polynomi

$$\frac{R}{Q}B(x) := b_0 + b_1x + ... + b_mx^m \in \mathbb{Z}[x] \tag{6.70}$$

on primitiivinen. Edelleen $R \perp Q$.

Todistus: Koska

$$\frac{R}{Q}B_j = b_j, \quad j = 0, 1, ..., m, \tag{6.71}$$

niin

$$(RB_0, ..., RB_m) = Q \cdot (b_0, b_1, ..., b_m), \tag{6.72}$$

missä $Q = syt(RB_0, ..., RB_m)$. Siten Lemman 7 nojalla $(b_0, b_1, ..., b_m)$ ja edelleen polynomi $b_0 + b_1x + ... + b_mx^m$ ovat primitiivisiä.
Tutkitaan väitettä $R \perp Q$. Olkoon $d = syt(R, Q)$, siten $R = dr$ ja $Q = dq$, $r, q \in \mathbb{Z}^+$. Yhtälöstä (6.71) saadaan

$$Rq_j = Qr_jb_j \quad \Rightarrow \quad rq_j = qr_jb_j, \quad j = 0, 1, ..., m. \tag{6.73}$$

Koska $q_j \perp r_j$, niin $r_j|r$ aina, kun $j = 0, 1, ..., m$. Siten $R = dr|r$, josta $d = 1$. □

Esimerkki 19.

$$B(x) = 7 + \frac{21}{5}x + \frac{14}{3}x^2, \quad R = 15, \quad Q = 7. \tag{6.74}$$

Lause 23. Gaussin lemma. Olkoon $a(x) \in \mathbb{Z}[x]$ primitiivinen ja $\deg a(x) \geq 2$. Jos $a(x)$ jakaantuu polynomirenkaassa/reducible in the polynomial ring $\mathbb{Q}[x]$, niin on olemassa sellaiset primitiiviset polynomit

$$b(x), c(x) \in \mathbb{Z}[x], \quad \text{että} \quad a(x) = b(x)c(x). \tag{6.75}$$

Todistus. Oletetaan, että

$$a(x) = B(x)C(x), \quad B(x), C(x) \in \mathbb{Q}[x]. \tag{6.76}$$

Lemman 9 nojalla on olemassa sellaiset $R, Q, T, S \in \mathbb{Z}^+$, että

$$\frac{R}{Q}B(x) := b(x) \in \mathbb{Z}[x],$$
$$\frac{T}{S}C(x) := c(x) \in \mathbb{Z}[x],$$
$$R \perp Q, \quad T \perp S, \tag{6.77}$$

missä $b(x)$ ja $c(x)$ ovat primitiivisiä. Edelleen

$$RTa(x) = QSb(x)c(x). \tag{6.78}$$

Koska $R \perp Q$ ja $a(x)$ on primitiivinen, niin $Q|T = Qt$ ja vastaavasti $S|R = Qr$. Siispä

$$rta(x) = b(x)c(x), \tag{6.79}$$

missä $b(x)c(x)$ on primitiivinen, joten $rt = 1$ ja lopulta $a(x) = b(x)c(x)$. □

Gaussin lemman nojalla polynomin $a(x) \in \mathbb{Z}[x]$ jaollisuutta voidaan tarkastella polynomirenkaassa $\mathbb{Z}[x]$. Siten polynomi on jaoton renkaassa $\mathbb{Q}[x]$, jos se on jaoton renkaassa $\mathbb{Z}[x]$. Edelleen saadaan tulos

Lause 24. Olkoon $a(x) \in \mathbb{Z}[x]$. Tällöin saadaan yksikäsitteinen esitys

$$a(x) = Aa_1(x) \cdots a_n(x), \quad A \in \mathbb{Z}, \tag{6.80}$$

missä $a_1(x), ..., a_k(x) \in \mathbb{Z}[x]$ ovat primitiivisiä jaottomia polynomeja.

Lause 25. Olkoot $p \in \mathbb{P}$, $a(x) \in \mathbb{Z}[x]$, $\overline{a}(x) \in \mathbb{Z}_p[x]$ ja $A = \deg a(x) = \deg \overline{a}(x)$. Jos $\overline{a}(x)$ on jaoton polynomirenkaassa $\mathbb{Z}_p[x]$, niin $a(x)$ on jaoton polynomirenkaassa $\mathbb{Q}[x]$.

Todistus. Vastaoletus eli olkoon

$$a(x) = b(x)c(x), \quad B = \deg b(x) \geq 1, \; C = \deg c(x) \geq 1. \tag{6.81}$$

Otetaan reduktio $\pmod p$, jolloin

$$\overline{a}(x) = \overline{b}(x)\overline{c}(x) \quad \in \mathbb{Z}_p[x]. \tag{6.82}$$

Koska

$$\deg \overline{b}(x) \leq B, \quad \deg \overline{c}(x) \leq C \tag{6.83}$$

ja

$$\deg \overline{b}(x) + \deg \overline{c}(x) = \deg \overline{a}(x) = A, \tag{6.84}$$

niin

$$\deg \overline{b}(x) = B \geq 1, \quad \deg \overline{c}(x) = C \geq 1. \tag{6.85}$$

Siten $\overline{a}(x)$ jakaantuu polynomirenkaassa $\mathbb{Z}_p[x]$.

Ristiriita. □

Lause 26. Eisensteinin kriteeri. Olkoon

$$a(x) = a_0 + a_1 x + ... + a_A x^A \in \mathbb{Z}[x], \quad \deg a(x) = A \geq 2.$$

Jos on olemassa sellainen $p \in \mathbb{P}$, että

$$p|a_i \quad \forall\ i = 0, 1, ..., A-1, \quad p^2 \not| a_0, \quad p \not| a_A, \tag{6.86}$$

niin $a(x)$ on jaoton polynomirenkaassa $\mathbb{Q}[x]$.

Todistus. Olkoon

$$a(x) = b(x)c(x) \in \mathbb{Z}[x] \tag{6.87}$$

eli

$$a_0 + a_1 x + ... + a_A x^A = (b_0 + b_1 x + ... + b_B x^B)(c_0 + ... + c_C x^C) \tag{6.88}$$

ja

$$B = \deg b(x) \geq 1,\ C = \deg c(x) \geq 1, \quad B + C = A. \tag{6.89}$$

Nyt

$$p|a_0 = b_0c_0, \quad p^2 \not| a_0 \quad \Rightarrow \quad \text{joko} \quad p|b_0 \quad \text{tai} \quad p|c_0. \tag{6.90}$$

Tarkastellaan tapaus

$$p|b_0 \quad \text{ja} \quad p \not| c_0. \tag{6.91}$$

Koska

$$p|a_1 = b_0c_1 + b_1c_0, \quad \Rightarrow \quad p|b_1 \tag{6.92}$$

...

$$p|a_B = b_0c_B + ... + b_Bc_0, \quad \Rightarrow \quad p|b_B. \tag{6.93}$$

Mutta

$$a_A = b_Bc_C, \quad \Rightarrow \quad p|a_A. \tag{6.94}$$

Ristiriita. □

Lause 27. Olkoon

$$a(x) = a_0 + a_1x + ... + a_Ax^A \in \mathbb{Z}[x]$$

ja

$$a(r/s) = 0, \quad r, s \in \mathbb{Z}, \quad r \perp s, \tag{6.95}$$

tällöin

$$r|a_0, \quad s|a_A, \tag{6.96}$$

Tämän avulla voidaan etsiä polynomin mahdolliset rationaali-nollakohdat.

Todistus. Yhtälö (6.95) on yhtäpitävää yhtälön

$$s^Aa_0 + s^{A-1}ra_1 + ... + sr^{A-1}a_{A-1} + r^Aa_A = 0 \tag{6.97}$$

kanssa. Koska $r \perp s$, niin välttämättä $r|a_0$ ja $s|a_A$. □

Lause 28. Olkoon K kunta, $p(x) \in K[x]$, $p(x) \in J_{K[x]}$, $\deg p(x) = d$ ja $k \in K$. Tällöin

$$p^*(x) = x^d p(1/x) \in J_{K[x]}, \quad \vec{p}_k(x) = p(x+k) \in J_{K[x]}. \tag{6.98}$$

Esimerkki 20.

Tarkastellaan polynomin

$$a(x) = 4x^3 - 2x^2 + 3x + 5 \in \mathbb{Z}[x] \tag{6.99}$$

tekijöihinjakoa. Jos 3. asteen polynomi jakaantuu, niin sillä on ainakin yksi 1. asteen tekijä, joten

$$a(x) = b(x)c(x), \quad \deg b(x) = 1. \tag{6.100}$$

Valitaan $p = 3$ ja otetaan reduktio $\pmod 3$ eli

$$\overline{a}(x) = \overline{b}(x)\overline{c}(x) \quad \in \mathbb{Z}_3[x], \quad \deg \overline{b}(x) = 1. \tag{6.101}$$

Tällöin

$$\overline{b}(x) \underset{\mathbb{Z}_3[x]}{|} \overline{a}(x) = x^3 + x^2 + 2, \quad \deg \overline{b}(x) = 1. \tag{6.102}$$

Lauseen 16 nojalla polynomilla $\overline{a}(x)$ on nollakohta kunnassa $\mathbb{Z}_3$. Mutta

$$\overline{a}(0) = 2, \quad \overline{a}(1) = 1, \quad \overline{a}(2) = 2. \tag{6.103}$$

Ristiriita. Siten $a(x)$ on jaoton polynomirenkaassa $\mathbb{Z}[x]$ ja edelleen myös renkaassa $\mathbb{Q}[x]$.

Esimerkki 21. Eisensteinin kriteerin, $p = 7$, nojalla

$$a(x) = 7 + 7x - 14x^3 + 2x^5 \in J_{\mathbb{Q}[x]}. \tag{6.104}$$

Käyttämällä lausetta 28 saadaan

$$b(x) = x^5 a(1/x) = 2 - 14x^2 + 7x^4 + 7x^5 \in J_{\mathbb{Q}[x]}; \tag{6.105}$$

$$b(x-1) = 2 - 14(x-1)^2 + 7(x-1)^4 + 7(x-1)^5 \in J_{\mathbb{Q}[x]}; \tag{6.106}$$

Esimerkki 22.

Olkoon $p \in \mathbb{P}$. Tällöin

$$a(x) = 1 + x + x^2 + ... + x^{p-1} \in J_{\mathbb{Q}[x]}. \tag{6.107}$$

Todistus. Aluksi saadaan

$$a(x) = \frac{x^p - 1}{x - 1}, \tag{6.108}$$

mihin sijoitetaan $x = t + 1$. Tällöin

$$a(x) = a(t+1) = \frac{(t+1)^p - 1}{t} = \\ t^{p-1} + \binom{p}{p-1} t^{t-2} + ... + \binom{p}{2} t + \binom{p}{1}. \tag{6.109}$$

Lukuteorian perusteet kurssin nojalla

$$p \left| \binom{p}{k} \right. \quad \forall\ 1 \leq k \leq p-1. \tag{6.110}$$

Nyt Eisensteinen kriteerin ehdot ovat voimassa, joten
$a(t+1)$ on jaoton ja siten myös $a(x)$ on jaoton polynomirenkaassa $\mathbb{Q}[x]$.

6.5.1 Reducibility in $\mathbb{C}[x]$ and $\mathbb{R}[x]$

Let

$$a(x) = a_0 + a_1 x + ... + a_A x^A \in \mathbb{C}[x], \quad \deg a(x) \geq 1, \tag{6.111}$$

then

$$a(x) = a_A (x - \alpha_1) \cdots (x - \alpha_A), \quad \alpha_1, ..., \alpha_A \in \mathbb{C} \tag{6.112}$$

by the Fundamental Theorem of Algebra. Consider now

$$a(x) = a_0 + a_1 x + ... + a_A x^A \in \mathbb{R}[x], \quad \deg a(x) \geq 1. \tag{6.113}$$

Then we have

$$a(z) = 0 \quad \Leftrightarrow \quad a(\overline{z}) = 0 \tag{6.114}$$

because

$$0 = \overline{a(z)} = a_0 + a_1\overline{z} + ... + a_A\overline{z}^A. \tag{6.115}$$

Therefore, non-real complex roots exist in pairs:
$\beta_j \neq \overline{\beta_j}$, $\beta_j \in \{\alpha_1, ..., \alpha_A\}$. Consequently

$$a(x) = a_A(x-\alpha_1)\cdots(x-\alpha_h)\cdot(x-\beta_1)(x-\overline{\beta_1})\cdots(x-\beta_k)(x-\overline{\beta_k}),$$
$$\alpha_1, ..., \alpha_h \in \mathbb{R}, \quad \beta_1, ..., \beta_k \in \mathbb{C}\setminus\mathbb{R}, \quad h+2k = A. \tag{6.116}$$

Write $\beta = a + ib$, where $a, b \in \mathbb{R}$ and compute

$$(x-\beta_1)(x-\overline{\beta_1}) = (x-a-ib)(x-a+ib) = (x-a)^2 + b^2 \in \mathbb{R}[x]. \tag{6.117}$$

Hence

$$a(x) = a_A(x-\alpha_1)\cdots(x-\alpha_h)\cdot((x-a_1)^2+b_1^2)\cdots((x-a_k)^2+b_k^2),$$
$$(x-\alpha_1), ..., (x-\alpha_h), ((x-a_1)^2+b_1^2), \ldots, ((x-a_k)^2+b_k^2) \in \mathbb{R}[x].$$

In other words: Any non-constant polynomial with real coefficients, factors in $\mathbb{R}[x]$ into first and second degree polynomials.

7 Symmetriset polynomit

Määritelmä 25. Olkoon R rengas. Formaali lauseke

$$P(t_1, ..., t_m) = \sum_{Finite} p_{i_1,...,i_m} t_i^{i_1} \cdots t_m^{i_m}, \quad p_{i_1,...,i_m} \in R \tag{7.1}$$

on m. muuttujan R-kertoiminen polynomi, missä $t_1, ..., t_m$ ovat polynomin muuttujia.

Polynomin P aste on

$$\deg P(t_1, ..., t_m) = \max\{i_1 + ... + i_m\}. \tag{7.2}$$

Käytetään kaikkien R-kertoimisten polynomien joukolle merkintää

$$R[t_1, ..., t_m]. \tag{7.3}$$

Olkoon $< i_1, ..., i_m >$ termin $p_{i_1,...,i_m} t_i^{i_1} \cdots t_m^{i_m}$ eksponentti. Tällöin termejä voidaan vertailla kuten yhden muuttujan tapauksessa vastinpotensseja. Siten joukkoon $R[t_1, ..., t_m]$ voidaan määritellä luonnollisella tavalla identtisyys sekä yhteen- ja kertolaskut.

Voidaan todistaa, että kolmikko $(R[t_1, ..., t_m], +, \cdot)$ on rengas.

Olkoon S_M joukon $\{1, 2, ..., m\}$ permutaatioryhmä. Jos $\lambda \in S_m$, niin merkitään

$$p^{\lambda}(t_1, ..., t_m) = p(t_{\lambda(1)}, ..., t_{\lambda(m)}). \tag{7.4}$$

Määritelmä 26. Polynomi p on symmetrinen, jos

$$p(t_{\lambda(1)}, ..., t_{\lambda(m)}) = p(t_1, ..., t_m) \quad \forall\ \lambda \in S_m. \tag{7.5}$$

7.1 Perusfunktiot

Määritelmä 27. Polynomit

$$s_k = s_k(t_1, ..., t_m) = \tag{7.6}$$

$$\sum_{1 \le j_1 < j_2 < ... < j_k \le m} t_{j_1} t_{j_2} \cdots t_{j_k}, \quad k = 1, ..., m,$$

ovat symmetriset perusfunktiot/elementary symmtric polynomials.

Lemma 10. Symmetriset perusfunktiot $s_1, ..., s_m$ ovat symmetrisiä polynomeja eli

$$s_k(t_{\lambda(1)}, ..., t_{\lambda(m)}) = s_k(t_1, ..., t_m) \quad \forall\ \lambda \in S_m \tag{7.7}$$

aina, kun $k = 1, ..., m$.

Siten polynomeja

$$s_1 = t_1 + ... + t_m; \tag{7.8}$$

$$s_2 = t_1t_2 + t_1t_3 + ... + t_{m-1}t_m; \tag{7.9}$$

$$s_3 = t_1t_2t_3 + t_1t_2t_4 + ... + t_{m-2}t_{m-1}t_m; \tag{7.10}$$

...

$$s_m = t_1t_2 \cdots t_{m-1}t_m; \tag{7.11}$$

voidaan kutsua myös symmetrisiksi peruspolynomeiksi.

Lause 29. Symmetristen polynomien peruslause.
Jokainen renkaan $R[t_1, ..., t_m]$ symmetrinen polynomi $S(t_1, ..., t_m)$ voidaan esittää symmetristen perusfunktioiden $s_1 = s_1(t_1, ..., t_m), ..., s_m = s_m(t_1, ..., t_m)$ polynomina eli on olemassa sellainen
$P(s_1, ..., s_m) \in R[s_1, ..., s_m]$, että

$$S(t_1, ..., t_m) = P(s_1(t_1, ..., t_m), ..., s_m(t_1, ..., t_m)). \tag{7.12}$$

Olkoot $S \subseteq R$ renkaita. Oletetaan, että polynomi $a(x) = a_0 + a_1x + ... + x^m \in S[x]$ jakaantuu polynomirenkaassa $R[x]$ seuraavasti

$$a(x) = (x - \alpha_1) \cdots (x - \alpha_m), \quad \alpha_1, ..., \alpha_m \in R. \tag{7.13}$$

Lause 30. Olkoon $b(t_1, ..., t_m) \in S[t_1, ..., t_m]$ symmetrinen polynomi. Tällöin

$$b(\alpha_1, ..., \alpha_m) \in S. \tag{7.14}$$

Olkoot $K \subseteq L$ kuntia. Oletetaan, että polynomi $a(x) = a_0 + a_1x + ... + a_mx^m \in K[x]$ jakaantuu polynomirenkaassa $L[x]$ seuraavasti

$$a(x) = a_m(x - \alpha_1) \cdots (x - \alpha_m), \quad \alpha_1, ..., \alpha_m \in L. \tag{7.15}$$

Lause 31. Olkoon $b(t_1, ..., t_m) \in K[t_1, ..., t_m]$ symmetrinen polynomi. Tällöin

$$b(\alpha_1, ..., \alpha_m) \in K. \tag{7.16}$$

Esimerkki 23. Olkoon

$$x^2 + bx + c = (x - \alpha)(x - \beta) \in \mathbb{Q}[x]. \tag{7.17}$$

Tällöin

$$\alpha^2 + \beta^2 \in \mathbb{Q}, \tag{7.18}$$

$$\alpha^3 + 2\alpha\beta + \beta^3 \in \mathbb{Q}. \tag{7.19}$$

8 Kuntalaajennus/Field extension

8.1 Kuntalaajennus

Määritelmä 28. Kunta K on kunnan L alikunta/sub field eli kunta L on kunnan K laajennus/extension $\Leftrightarrow$ K ja L ovat kuntia sekä $K \subseteq L$.

Tällä kurssilla kuntalaajennukselle käytetään merkintöjä
$L : K$ ja $K \leqslant L$.

Kun $L : K$, niin L voidaan tulkita lineaariavaruudeksi kunnan K yli asettamalla yhteenlasku/we can interpret L as a vector space over K by setting addition

$$L \times L \ \to L, \quad (\alpha, \beta) \ \to \alpha + \beta; \tag{8.1}$$

ja skalaarilla $r \in K$ kertominen/scalar multiplication

$$K \times L \ \to L, \quad (r, \alpha) \ \to r\alpha \tag{8.2}$$

käyttäen kunnan L yhteen- ja kertolaskuja/by using the fiel operations.

Määritelmä 29. Kuntalaajennuksen aste/degree of field extension eli $[L : K] = \dim_K L$. äärellinen/finite, jos $[L : K] < \infty$.

8.2 Kuntatorni/Field tower

Jos $K \leqslant M \leqslant L$, niin kuntaa M sanotaan välikunnaksi/intermediate field.

$$\begin{array}{ccc} L_1 & & L_2 \\ & \diagdown \quad \diagup & \\ & L_3 & \\ & | & \\ & K & \end{array} \quad \Leftrightarrow \begin{cases} K \leqslant L_3 \leqslant L_1 \\ \text{ja} \\ K \leqslant L_3 \leqslant L_2 \end{cases}$$

Lause 32. Olkoon $K \leqslant M \leqslant L$ kuntatorni. Tällöin

$$[L : K] = [L : M][M : K]. \tag{8.3}$$

Todistus. Olkoot

$$\begin{aligned} M = \langle \alpha_1, ..., \alpha_r \rangle_K = K\alpha_1 + ... + K\alpha_r, \quad \dim_K M = r; \\ L = \langle \beta_1, ..., \beta_s \rangle_M = M\beta_1 + ... + M\beta_s, \quad \dim_M L = s. \end{aligned} \tag{8.4}$$

Valitaan $\gamma \in L$. Sille pätee

$$\begin{aligned} \gamma &= \sum_{j=1}^{s} m_j \beta_j, \quad m_j \in M; \\ m_j &= \sum_{i=1}^{r} k_{ij} \alpha_i, \quad k_{ij} \in K \quad \Rightarrow \\ \gamma &= \sum_{i=1}^{r} \sum_{j=1}^{s} k_{ij} \alpha_i \beta_j \in K\alpha_1\beta_1 + ... + K\alpha_r\beta_s, \\ &\#\{\alpha_i\beta_j\} = rs. \end{aligned} \tag{8.5}$$

Osoitetaan vielä, että $\{\alpha_i\beta_j\}$ on lineaarisesti vapaa.

Asetetaan

$$\begin{aligned}
&\sum_{i=1}^{r}\sum_{j=1}^{s} h_{ij}\alpha_i\beta_j = 0, \quad h_{ij} \in K \quad \Rightarrow \\
&\sum_{j=1}^{s}\left(\sum_{i=1}^{r} h_{ij}\alpha_i\right)\beta_j = 0, \quad \text{missä } \{\beta_j\} \text{ on kanta/M} \quad \Rightarrow \\
&\sum_{i=1}^{r} h_{ij}\alpha_i = 0, \quad \text{missä } \{\alpha_i\} \text{ on kanta/K} \quad \Rightarrow \\
&h_{ij} = 0, \quad \forall \quad i,j. \quad \square
\end{aligned} \tag{8.6}$$

8.3 Osamääräkunta

Tarkennetaan hieman rationaalilukujen ja rationaalifunktioiden käsitteitä ja sitä kautta niillä operointia.

Määritelmä 30. Olkoon D kokonaisalue ja $a, b, c, d \in D$, $bd \neq 0$. Asetetaan relaatio

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc. \tag{8.7}$$

Lause 33. Relaatio $\sim$ on ekvivalenssirelaatio joukossa $D \times (D \setminus \{0\}) = \mathcal{D}$.

Määritelmä 31. Ekvivalenssiluokille

$$[a, b] = \{(c, d) \in \mathcal{D} |\ (c, d) \sim (a, b)\}$$

sovitaan yhteenlasku

$$[a_1, b_1] + [a_2, b_2] = [a_1b_2 + a_2b_1, b_1b_2] \tag{8.8}$$

ja kertolasku

$$[a_1, b_1][a_2, b_2] = [a_1a_2, b_1b_2] \tag{8.9}$$

aina, kun $(a_1, b_1), (a_2, b_2) \in \mathcal{D}$.

Merkitään vielä

$$a/b = \frac{a}{b} = [a, b] \quad \text{ja} \quad Q(D) = \{a/b|\ (a, b) \in \mathcal{D}\}.$$

Voidaan todistaa, että

Lause 34. Kolmikko $(Q(D), +, \cdot)$ on kunta.

Sanotaan, että $Q(D)$ on D:n osamääräkunta (quotient field, field of fractions). Tällöin pätee rengasisomorfiatulos

$$\{\frac{a}{1}|\ a \in D\} \cong D, \tag{8.10}$$

jonka nojalla voidaan merkitä $a = a/1$. Edelleen

$$ab^{-1} = \frac{a}{1}\left(\frac{b}{1}\right)^{-1} = \frac{a}{1}\frac{1}{b} = \frac{a}{b} \tag{8.11}$$

Esimerkki 24.

Olkoon $D = \mathbb{Z}$, joka on kokonaisalue. Tällöin saadaan osamääräkunta $Q(\mathbb{Z})$, jonka avulla rationaalilukujoukko saadaan määriteltyä tarkasti.

Määritelmä 32. Rationaalilukujen kunta $\mathbb{Q} = Q(\mathbb{Z})$.

Nyt rationaalilukujen supistamis-/cancellation

$$\frac{ac}{bc} = \frac{a}{b} \tag{8.12}$$

ja laventamislaki/convert

$$\frac{a}{b} = \frac{da}{db} \tag{8.13}$$

seuraa suoraan Määritelmästä 31.

Esimerkki 25.

Olkoon K kunta, jolloin polynomirengas $D = K[x]$ on kokonaisalue.

Määritelmä 33. Rationaalifunktioiden kunta $K(x) = Q(K[x])$.

Tällöin pätevät ylläesitetyt supistussäännöt, jolloin mm.

$$\frac{(x^2-1)x}{(x-1)x^2} = \frac{x+1}{x} = 1 + \frac{1}{x}. \tag{8.14}$$

Esimerkki 26.

Olkoon K kunta, jolloin formaalien sarjojen joukko $D = K[[T]]$ on kokonaisalue. Tällöin saadaan osamääräkunta, joka on isomorfinen formaalien Laurentin sarjojen kunnan kanssa eli

Lause 35.

$$K((T)) \cong Q(K[[T]]). \tag{8.15}$$

Näillä rakenteilla on seuraavat suhteet:

$$K[T] \subset K(T) \subset K((T)), \tag{8.16}$$

$$K[T] \subset K[[T]] \subset K((T)). \tag{8.17}$$

Määritelmä 34. Formaali derivaatta

$$D: \ K((T)) \to K((T))$$

on lineaarinen kuvaus, jolle pätee

$$DT^k = kT^{k-1} \quad \forall \quad k \in \mathbb{Z}. \tag{8.18}$$

9 Algebralliset luvut

9.1 Algebralliset alkiot alikunnan suhteen

Määritelmä 35. Olkoot $K \subseteq L$ kuntia ja $\alpha \in L$. Jos on olemassa sellainen $p(x) \in K[x] \setminus K$, että

$$p(\alpha) = 0 \tag{9.1}$$

niin α on algebrallinen kunnan/algebraic over the field K suhteen (yli).
Muutoin α on transkendenttinen/transcendental over kunnan K suhteen.

Esimerkki 27. A. Tiedetään, että π on transkendenttinen rationaalilukujen kunnan $\mathbb{Q}$ suhteen.
B. Koska

$$p(\pi) = 0, \quad p(x) = x - \pi \in \mathbb{R}[x], \tag{9.2}$$

niin välittömästi nähdään, että π on algebrallinen reaalilukujen kunnan $\mathbb{R}$ suhteen.

Määritelmä 36. Olkoot $K \subseteq L$ kuntia ja $\alpha \in L$. Algebrallisen luvun α minimipolynomi on asteeltaan pienin mahdollinen pääpolynomi/lowest degree monic polynomial $M_\alpha(x) \in K[x] \setminus K$, jolle pätee

$$M_\alpha(\alpha) = 0. \tag{9.3}$$

Olkoon $\deg M_\alpha(x) = n$, tällöin algebrallisen luvun α aste/degree kunnan K yli on

$$\deg \alpha = \deg_K \alpha = n \geq 1. \tag{9.4}$$

Lause 36. Olkoon $K \subseteq L$ kuntia ja $\alpha \in L$. Algebrallisen luvun α minimipolynomi $M_\alpha(x) \in K[x]_n$ on yksikäsitteinen ja jaoton/unique and irreducible polynomirenkaassa $K[x]$.

Todistus. Jos $M_\alpha(x)$ jakaantuu, niin

$$M_\alpha(x) = A_1(x)A_2(x), \quad \deg A_1(x), \deg A_2(x) \leq n - 1. \tag{9.5}$$

Koska

$$0 = M_\alpha(\alpha) = A_1(\alpha)A_2(\alpha), \tag{9.6}$$

niin olisi olemassa polynomi $A_i(x) \in K[x]$:

$$A_i(\alpha) = 0, \quad \deg A_i(x) \leq n - 1. \quad \text{Ristiriita.} \tag{9.7}$$

Yksikäsitteisyys: Olkoot $M_\alpha(x), N_\alpha(x) \in K[x]_n$ alkion α minimipolynomeja. Koska ne ovat jaottomia ja $M_\alpha(\alpha) = N_\alpha(\alpha) = 0$, niin Lauseen **??** nojalla

$$M_\alpha(x) \underset{K[x]}{\mid} N_\alpha(x) \quad \text{ja} \quad N_\alpha(x) \underset{K[x]}{\mid} M_\alpha(x). \tag{9.8}$$

Täten $M_\alpha(x) = k \cdot N_\alpha(x)$ ja edelleen $M_\alpha(x) = N_\alpha(x)$. □

Määritelmä 37. Olkoon $\alpha \in \mathbb{C}$ astetta $\deg \alpha = n$ oleva algebrallinen luku kunnan $\mathbb{Q}$ yli. Tällöin sanotaan, että α on astetta $\deg \alpha = n$ oleva algebrallinen luku.

Jos $\alpha \in \mathbb{C}$ ei ole algebrallinen luku, niin α on transkendenttiluku.

Olkoon α on astetta $\deg \alpha = n$ oleva algebrallinen luku. Tällöin α:n minimipolynomi $M_\alpha(x) \in \mathbb{Q}[x]_n$ on jaoton polynomirenkaassa ja sen aste $\deg M_\alpha(x) = n$. Siten astetta n olevan algebrallisen luvun minimipolynomi on muotoa

$$M_\alpha(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0, \quad a_i \in \mathbb{Q}, \tag{9.9}$$

oleva jaoton pääpolynomi.

9.1.1 Kokonainen algebrallinen luku/Algebraic integer

Määritelmä 38. Olkoon $\alpha \in \mathbb{C}$ astetta $\deg \alpha = n$ oleva algebrallinen luku, jonka minimipolynomi

$$M_\alpha(x) \in \mathbb{Z}[x]_n. \tag{9.10}$$

Tällöin α on astetta $\deg \alpha = n$ oleva kokonainen algebrallinen luku/algebraic integer.

Siten kokonaisen astetta n olevan algebrallisen luvun minimipolynomi on muotoa

$$M_\alpha(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0, \quad a_i \in \mathbb{Z}, \tag{9.11}$$

oleva jaoton pääpolynomi.

Esimerkki 28.

$$\frac{1+\sqrt{5}}{2} \tag{9.12}$$

on 2. asteen kokonainen algebrallinen luku.

Esimerkki 29.

$$x^3 - 2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) \tag{9.13}$$

Lauseen 20 nojalla jaottomalla polynomilla nollakohdat ovat erillisiä. Olkoot $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n \in \mathbb{C}$. minimipolynomin $M_\alpha(x)$ nollakohdat, jotka ovat siis erillisiä eli $\alpha_i \neq \alpha_j$, kun $i \neq j$.

Määritelmä 39. Algebrallisen luvun α liittoluvut eli konjugaatit ovat minimipolynomin $M_\alpha(x)$ nollakohdat

$$\alpha_1, ..., \alpha_n \in \mathbb{C}. \tag{9.14}$$

Määritelmä 40.

Algebrallisen luvun α liittolukuihin liittyvät monomorfiat ovat kuntamorfismit

$$\sigma_1, ..., \sigma_n : \ \mathbb{K} = \mathbb{Q}(\alpha) \to \mathbb{C}; \tag{9.15}$$

joille pätee:

$$\sigma_i \quad \text{on injektio;} \tag{9.16}$$

$$\sigma_i(x+y) = \sigma_i(x) + \sigma_i(y); \tag{9.17}$$

$$\sigma_i(xy) = \sigma_i(x)\sigma_i(y); \tag{9.18}$$

$$\sigma_i|_{\mathbb{Q}} = \mathrm{Id} : \mathbb{Q} \to \mathbb{Q} \quad \text{identtinen kuvaus} \tag{9.19}$$

$$\sigma_i(\alpha) = \alpha_i, \quad i = 1, ..., n. \tag{9.20}$$

Lisäksi usein kiinnitetään

$$\sigma_1 = \mathrm{Id}|_{\mathbb{K}}, \quad \sigma_1(\alpha) = \alpha. \tag{9.21}$$

Määritelmä 41. Olkoon $\mathbb{Q} \leqslant \mathbb{K} \leqslant \mathbb{C}$ ja $[\mathbb{K} : \mathbb{Q}] < \infty$, tällöin $\mathbb{K}$ on lukukunta.

Lause 37. Olkoon $\mathbb{K}$ lukukunta ja $\sigma : \mathbb{K} \to \mathbb{C}$ monomorfia. Tällöin

$$\sigma(a) = a \quad \forall a \in \mathbb{Q}. \tag{9.22}$$

$$\sigma(a\alpha + b\beta) = a\sigma(\alpha) + b\sigma(\beta), \quad \forall a, b \in \mathbb{Q}, \alpha, \beta \in \mathbb{K}. \tag{9.23}$$

$$\sigma(p(\beta)) = p(\sigma(\beta)) \quad \forall \beta \in \mathbb{K}, \quad p(x) \in \mathbb{Q}[x]. \tag{9.24}$$

9.2 Alkiolla laajentaminen

Määritelmä 42. Olkoon $S \leqslant R$ rengaslaajennus/ring extension ja $\alpha_1, ..., \alpha_m \in R$. Tällöin asetetaan

$$S[\alpha_1, ..., \alpha_m] = \bigcap_{S \cup \{\alpha_1, ..., \alpha_m\} \subseteq V \leqslant R} V, \tag{9.25}$$

joka on suppein R:n alirengas sisältäen alirenkaan S sekä alkiot $\alpha_1, ..., \alpha_m$. Thinnest sub ring containing ...

Nähdään, että $S[\alpha_1, ..., \alpha_m]$ koostuu alkioiden $\alpha_1, ..., \alpha_m$ polynomilausekkeista. Erityisesti

$$S[\alpha] = \{s_0 + s_1\alpha + s_2\alpha^2 + ... + s_n\alpha^n | \ s_i \in S, \ n \in \mathbb{N}\} \tag{9.26}$$

on yhden muuttujan α polynomirengas.

Määritelmä 43. Olkoon $K \leqslant L$ kuntalaajennus ja $\alpha_1, ..., \alpha_m \in L$. Tällöin asetetaan

$$\langle K, \alpha_1, ..., \alpha_m \rangle = \bigcap_{K \cup \{\alpha_1, ..., \alpha_m\} \subseteq M \leqslant L} M, \tag{9.27}$$

joka on suppein L:n alikunta sisältäen alikunnan K sekä alkiot $\alpha_1, ..., \alpha_m$.

Lause 38.

$$\langle K, \alpha_1, ..., \alpha_m \rangle = K(\alpha_1, ..., \alpha_m) := \tag{9.28}$$
$$\left\{ \frac{A}{B} |\ A, B \in K[\alpha_1, ..., \alpha_m],\ B \neq 0 \right\}.$$

Lause 39.

$$\langle K, \alpha \rangle = K(\alpha) := \left\{ \frac{A(\alpha)}{B(\alpha)} |\ A(\alpha), B(\alpha) \in K[\alpha],\ B \neq 0 \right\}. \tag{9.29}$$

Lause 40. Jos α on transkendenttinen K:n suhteen, niin

$$K[\alpha] \cong K[x] \tag{9.30}$$

eli renkaat $K[\alpha]$ ja $K[x]$ ovat isomorfiset. Edelleen

$$K(\alpha) \cong K(x) \tag{9.31}$$

eli kunnat $K(\alpha)$ ja $K(x)$ ovat isomorfiset.

10 Algebralliset kunnat

Määritelmä 44. Kuntalaajennus $L : K$ on algebrallinen, jos jokainen L:n alkio on algebrallinen K:n suhteen.

Merkintä 8.

$$K\alpha_1 + ... + K\alpha_m := \{k_1\alpha_1 + ... + k_m\alpha_m |\ k_1, ..., k_m \in K\}; \tag{10.1}$$

$$K[\beta]_n := K\beta^0 + K\beta^1 + ... + K\beta^n. \tag{10.2}$$

Välittömästi

$$K[\beta]_n \subseteq K[\beta] = K\beta^0 + K\beta^1 + ... \tag{10.3}$$

Lause 41. Olkoon $L : K$ ja $\beta \in L$. Tällöin

$$A. \qquad \deg_K \beta = s \quad \Leftrightarrow$$

$$K[\beta] = K[\beta]_{s-1} \quad \text{ja} \quad \dim_K K[\beta] = s; \quad (10.4)$$

B. Jos β on algebrallinen K:n suhteen, niin $K[\beta]$ on kunta;

$$C. \qquad [L : K] = r < \infty \quad \Rightarrow \quad \deg_K \beta = s|r; \qquad (10.5)$$

D. äärellinen kuntalaajennus $L : K$ on algebrallinen.

Lause 42. Olkoon $L : K$, $\alpha \in L$ algebrallinen K:n yli ja $\deg_K \alpha = n$. Tällöin

$$A. \qquad \langle K, \alpha \rangle = K[\alpha] = K + K\alpha + ... + K\alpha^{n-1}; \qquad (10.6)$$

$$B. \qquad [\langle K, \alpha \rangle : K] = \deg_K \alpha = n; \qquad (10.7)$$

$$C. \qquad \beta \in \langle K, \alpha \rangle \quad \Rightarrow \quad \deg_K \beta = k|n; \qquad (10.8)$$

D. Kuntalaajennus $\langle K, \alpha \rangle$ on algebrallinen.

Todistus.

Lause 41 A. "$\Rightarrow$": Olkoon $\deg_K \beta = s$. Osoitetaan aluksi, että

$$K[\beta] = K[\beta]_{s-1} = K\beta^0 + K\beta^1 + ... + K\beta^{s-1}. \qquad (10.9)$$

Olkoon β:n minimipolynomi

$$M_\beta(x) = b_0 x^0 + ... + x^s \in K[x]$$

$$\text{ja} \quad a(\beta) \in K[\beta], \quad a(x) \in K[x]. \quad (10.10)$$

Jakoalgoritmin nojalla

$$a(x) = q(x)M_\beta(x) + r(x), \quad \deg r(x) \leq s-1 \quad \Rightarrow$$
$$a(\beta) = q(\beta)M_\beta(\beta) + r(\beta) = r(\beta) \in K[\beta]_{s-1} \quad \Rightarrow$$
$$K[\beta] \subseteq K[\beta]_{s-1} \quad \Rightarrow \quad K[\beta] = K[\beta]_{s-1}. \quad (10.11)$$

Näytetään vielä, että $\{\beta^0, \beta^1, ..., \beta^{s-1}\}$ muodostaa kannan. Nimittäin, jos asetetaan

$$k_0\beta^0 + k_1\beta^1 + ... + k_{s-1}\beta^{s-1} = 0,$$
$$k_0, ..., k_{s-1} \in K, \ k_i \neq 0, \text{ jollakin } i = 0, ..., s-1 \quad \Rightarrow$$
$$\deg_K \beta \leq s-1. \quad \text{Ristiriita.} \quad \Rightarrow$$
$$\dim_K K[\beta] = \dim_K K[\beta]_{s-1} = s. \quad \square \quad (10.12)$$

"$\Leftarrow$": Olkoon $K[\beta] = K[\beta]_{s-1}$ ja $\dim_K K[\beta] = s$. Siten $\dim_K K[\beta]_{s-1} = s$ ja

$$K[\beta]_{s-1} = K\beta^0 + K\beta^1 + ... + K\beta^{s-1}, \quad (10.13)$$

missä $\{\beta^0, \beta^1, ..., \beta^{s-1}\}$ ovat lineaarisesti riippumattomia K:n yli. Jos olisi

$$p(x) \in K[x], \quad 1 \leq \deg p(x) \leq s-1, \quad p(\beta) = 0, \quad \Rightarrow$$
$$\{\beta^0, \beta^1, ..., \beta^{s-1}\} \quad \text{olisi lin. sidottu.} \quad \text{Ristiriita}$$
$$\Rightarrow \quad \deg_K \beta \geq s. \quad (10.14)$$

Toisaalta

$$\beta^s \in K[\beta] = K[\beta]_{s-1} \quad \Rightarrow$$
$$\beta^s = k_0\beta^0 + k_1\beta^1 + ... + k_{s-1}\beta^{s-1} \quad \Rightarrow \deg_K \beta \leq s. \quad (10.15)$$

$$\rightsquigarrow \deg_K \beta = s. \quad \square$$

Todistus. Lause 41 C:

B. kohdasta saadaan, että $K[\beta]$ on L:n alikunta. Koska $[L:K] = r < \infty$, niin A. kohdan nojalla

$$\dim_K K[\beta] := s \leq \dim_K L = r \quad \Rightarrow \quad \deg_K \beta = s \leq r. \tag{10.16}$$

Nyt $K \leqslant K[\beta] \leqslant L$ muodostaa kuntatornin. Siten Lauseen 32 nojalla

$$[L:K] = [L:K[\beta]][K[\beta]:K] \quad \Rightarrow \quad r = vs, \quad v = [L:K[\beta]]. \tag{10.17}$$

Niinpä

$$s|r. \quad \square \tag{10.18}$$

Huomautus 8.

Lauseen 39 nojalla

$$\langle K, \alpha \rangle = K(\alpha) = \left\{ \frac{A(\alpha)}{B(\alpha)} |\ A(\alpha), B(\alpha) \in K[\alpha],\ B \neq 0 \right\}. \tag{10.19}$$

mutta Lauseen 42 A. kohdan nojalla algebrallisen luvun määräämässä laajennuskunnassa kaikki α:n rationaalilausekkeet palautuvat α:n polynomilausekkeiksi.

Esimerkki 30.

Tarkastellaan kuntalaajennusta

$$\mathbb{L} := \langle \mathbb{Q}, 2^{1/2}, 2^{1/3} \rangle = \langle \langle \mathbb{Q}, 2^{1/2} \rangle, 2^{1/3} \rangle. \tag{10.20}$$

Merkitään

$$\mathbb{M}_2 := \langle \mathbb{Q}, 2^{1/2} \rangle, \quad \mathbb{M}_3 := \langle \mathbb{Q}, 2^{1/3} \rangle. \tag{10.21}$$

Aluksi

$$\begin{aligned} M_{\alpha_1} = x^2 - 2 = (x - \alpha_1)(x - \alpha_2), \quad \alpha_1 = 2^{1/2}, \\ M_{\alpha_1} \in J_{\mathbb{Q}[x]}, \quad \deg_{\mathbb{Q}} M_{\alpha_1} = 2, \\ \Rightarrow \quad [\mathbb{M}_2 : \mathbb{Q}] = 2; \end{aligned} \tag{10.22}$$

$$M_{\beta_1} = x^3 - 2 = (x-\beta_1)(x-\beta_2)(x-\beta_3),\ \beta_1 = 2^{1/3},$$
$$M_{\beta_1} \in J_{\mathbb{Q}[x]}, \quad \deg_{\mathbb{Q}} M_{\beta_1} = \deg_{\mathbb{Q}} M_{\beta_2} = \deg_{\mathbb{Q}} M_{\beta_3} = 3,$$
$$\Rightarrow \quad [\mathbb{M}_3 : \mathbb{Q}] = 3. \quad (10.23)$$

Lauseen 42 C kohdan nojalla

$$\beta_1, \beta_2, \beta_3 \notin \mathbb{M}_2, \quad \alpha_1, \alpha_2 \notin \mathbb{M}_3. \quad (10.24)$$

Siten polynomilla $x^3 - 2$ ei ole nollakohtia kunnassa $\mathbb{M}_2$, joten $x^3 - 2$ on jaoton polynomirenkaassa $\mathbb{M}_2[x]$.

Niinpä

$$[\mathbb{L} : \mathbb{M}_2] = [\langle \mathbb{M}_2, 2^{1/3} \rangle : \langle \mathbb{Q}, 2^{1/2} \rangle] = 3. \quad (10.25)$$

Edelleen Lauseen 32 mukaan

$$[\mathbb{L} : \mathbb{Q}] = [\mathbb{L} : \mathbb{M}_2][\mathbb{M}_2 : \mathbb{Q}] = 6. \quad (10.26)$$

Vastaavasti kuten Lauseen 32 todistuksessa

$$\mathbb{M}_2 = \langle 1, 2^{1/2} \rangle_{\mathbb{Q}} = \mathbb{Q} \cdot 1 + \mathbb{Q} 2^{1/2}, \quad \dim_{\mathbb{Q}} \mathbb{M}_2 = 2;$$
$$\mathbb{L} = \langle 1, 2^{1/3}, 2^{2/3} \rangle_{\mathbb{M}_2} = \mathbb{M}_2 \cdot 1 + \mathbb{M}_2 2^{1/3} + \mathbb{M}_2 2^{2/3}, \quad \dim_{\mathbb{M}_2} \mathbb{L} = 3.$$

Josta saadaan

$$\mathbb{L} = \mathbb{Q} \cdot 1 + \mathbb{Q} 2^{1/2} + \mathbb{Q} 2^{1/3} + \mathbb{Q} 2^{1/2} 2^{1/3} + \mathbb{Q} 2^{2/3} + \mathbb{Q} 2^{1/2} 2^{2/3}$$
$$= \langle 1, 2^{1/6}, 2^{2/6}, 2^{3/6}, 2^{4/6}, 2^{5/6} \rangle_{\mathbb{Q}},$$
$$\dim_{\mathbb{Q}} \mathbb{L} = 6.$$

Siten

$$\langle \mathbb{Q}, 2^{1/2}, 2^{1/3} \rangle = \langle \mathbb{Q}, 2^{1/6} \rangle \quad (10.27)$$

eli

$$\mathbb{Q}(2^{1/2}, 2^{1/3}) = \mathbb{Q}(2^{1/6}). \quad (10.28)$$

Lemma 11. Olkoot

$$[\langle K, \alpha_i \rangle : K] = n_i, \quad i = 1, ..., r. \tag{10.29}$$

Tällöin

$$[\langle K, \alpha_1, ..., \alpha_r \rangle : K] \leq n_1 \cdots n_r. \tag{10.30}$$

Lause 43. Kuntalaajennus $L : K$ on äärellinen täsmälleen silloin kun $L = \langle K, \alpha_1, ..., \alpha_r \rangle$ ja L on algebrallinen K:n yli.

11 Algebralliset luvut $\mathbb{A}$

Kerrataan, että joukko $\mathbb{A} \subseteq \mathbb{C}$ koostuu kaikista algebrallisista luvuista kunnan $\mathbb{Q}$ yli. Seuraava tulos osoittaa, että algebrallisten lukujen joukko $\mathbb{A}$ on kompleksilukujen kunnan alikunta.

Lause 44.

$$\mathbb{A} \leqslant \mathbb{C}. \tag{11.1}$$

Seuraus 2. Jos $\alpha, \beta \in \mathbb{A}$, niin

$$\alpha \pm \beta, \ \alpha\beta, \ \alpha/\beta \in \mathbb{A}. \tag{11.2}$$

Algebran peruslauseen 19 nojalla $\mathbb{C}$ on algebrallisesti suljettu eli jos τ on algebrallinen $\mathbb{C}$:n suhteen, niin $\tau \in \mathbb{C}$.

Seuraava tulos osoittaa, että jos $\omega \in \mathbb{C}$ on algebrallinen kunnan $\mathbb{A}$ suhteen, niin $\omega \in \mathbb{A}$.

Lause 45. Algebrallisten lukujen joukko $\mathbb{A}$ on algebrallisesti suljettu eli

$$a(x) \in \mathbb{A}[x] \setminus \{0(x)\}, \quad a(\omega) = 0 \quad \Rightarrow \quad \omega \in \mathbb{A}. \tag{11.3}$$

12 Lukukunnat

Lause 46. Olkoon $\mathbb{K}$ on lukukunta. Tällöin on olemassa sellainen $\tau \in \mathbb{K}$, että

$$\mathbb{K} = \mathbb{Q}(\tau). \tag{12.1}$$

Siten lukukunnat ovat yksinkertaisia $\mathbb{Q}$:n laajennuksia eli yhden alkion generoimia laajennuksia. Number fields are generated by a single element.

Todistus. Induktiolla.

Tarkastellan tapausta

$$\mathbb{K} = \mathbb{Q}(\alpha, \beta) \tag{12.2}$$

ja osoitetaan, että

$$\mathbb{K} = \mathbb{Q}(\alpha + c\beta), \quad \text{jollakin} \quad c \in \mathbb{Q}. \tag{12.3}$$

Olkoot

$$M_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in \mathbb{Q}[x];$$
$$M_\beta(x) = (x - \beta_1) \cdots (x - \beta_m) \in \mathbb{Q}[x]. \tag{12.4}$$

Tällöin on olemassa sellainen $c \in \mathbb{Q}$, että

$$\gamma := \alpha + c\beta \neq \alpha_i + c\beta_j, \quad \forall (i,j) \neq (1,1). \tag{12.5}$$

a). Välittömästi

$$\gamma := \alpha + c\beta \in \mathbb{Q}(\alpha, \beta) \quad \Rightarrow \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha, \beta). \tag{12.6}$$

b). Osoitetaan (mutta ei niin välittömästi), että

$$\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\gamma). \tag{12.7}$$

Tarkastellaan polynomeja

$$r(x) = M_\alpha(\gamma - cx) \in \mathbb{Q}(\gamma)[x], \quad \deg r(x) = n,$$
$$r(\beta) = M_\alpha(\gamma - c\beta) = M_\alpha(\alpha) = 0;$$
$$M_\beta(\beta) = 0, \quad M_\beta(x) \in \mathbb{Q}[x], \quad (12.8)$$

missä polynomin $M_\beta(x)$ kaikki nollakohdat β_j ovat yksinkertaisia.

Asetetaan nyt

$$r(\tau) = M_\beta(\tau) = 0 \quad \Rightarrow \quad \tau = \beta_k;$$
$$0 = r(\tau) = M_\alpha(\gamma - c\tau) \quad \Rightarrow \quad \gamma - c\tau = \alpha_h$$
$$\Rightarrow \quad \gamma = \alpha_h + c\tau = \alpha_h + c\beta_k$$
$$\Rightarrow \quad \gamma = \alpha + c\beta \Rightarrow \quad \tau = \beta. \quad (12.9)$$

Siten yksinkertainen nollakohta β on ainoa yhteinen polynomien $r(x)$ ja $M_\beta(x)$ nollakohta. Olkoon

$$d(x) = s.y.t(r(x), M_\beta(x)) \in \mathbb{Q}(\gamma)[x]. \quad (12.10)$$

Jos olisi

$$\deg d(x) \geq 2 \quad \Rightarrow$$
$$d(x) = (x - \beta)(x - \kappa)q(x), \quad \beta, \kappa \in \mathbb{C} \quad \Rightarrow$$
$$r(\kappa) = M_\beta(\kappa) = 0 \quad \Rightarrow \quad \kappa = \beta \quad \Rightarrow$$
$$(x - \beta)^2 \underset{\mathbb{C}[x]}{\|} M_\beta(x) \quad (12.11)$$

Ristiriita. Siten $\deg d(x) = 1$ ja

$$d(x) = (x - \beta) \in \mathbb{Q}(\gamma)[x] \quad \Rightarrow$$
$$\beta \in \mathbb{Q}(\gamma) \quad \Rightarrow \quad \alpha = \gamma - c\beta \in \mathbb{Q}(\gamma) \quad \Rightarrow$$
$$\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\gamma). \quad \square \quad (12.12)$$

Esimerkki 31.

$$\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i - \sqrt{2}). \tag{12.13}$$

12.1 Liittoluvut, kuntapolynomi/Conjugates, field polynomial

Lause 47. Olkoon $\mathbb{K} = \mathbb{Q}(\tau)$ lukukunta ja $[\mathbb{K} : \mathbb{Q}] = m$. Tällöin on olemassa täsmälleen m eri monomorfismia

$$\sigma_i : \mathbb{K} \to \mathbb{C}, \quad i = 1, ..., m. \tag{12.14}$$

Huomautus 9. Vaikka $a \in \mathbb{K}$, niin voi olla $\sigma_i(a) \notin \mathbb{K}$, jollakin i.

Esimerkki 32. Olkoon $\mathbb{K} = \mathbb{Q}(2^{1/3})$, tällöin

$$\sigma_2(2^{1/3}), \sigma_3(2^{1/3}) \notin \mathbb{K}. \tag{12.15}$$

Määritelmä 45. Olkoon $\mathbb{K} = \mathbb{Q}(\tau)$ lukukunta ja $[\mathbb{K} : \mathbb{Q}] = m$. Alkion $\beta \in \mathbb{K}$ kuntapolynomi/field polynomial on

$$K_\beta(x) = \prod_{i=1}^{m} (x - \sigma_i(\beta)), \tag{12.16}$$

missä luvut

$$\sigma_i(\beta) \in \mathbb{C} \tag{12.17}$$

ovat luvun $\beta \in \mathbb{K}$ liittoluvut kunnan $\mathbb{K}$ suhteen/conjugates over $\mathbb{K}$.

Lause 48.

$$K_\beta(x) \in \mathbb{Q}[x]. \tag{12.18}$$

Todistus: Symmetristen polynomien peruslauseeseen nojautuen.

Kerrataan vielä, että Määritelmän 39 mukaan algebrallisen luvun β liittoluvut eli konjugaatit ovat minimipolynomin $M_\beta(x) \in \mathbb{Q}[x]$ nollakohdat

$$\beta_1, ..., \beta_d \in \mathbb{C}. \tag{12.19}$$

Seuraavassa

$$\deg K_\beta(x) = m, \quad \deg M_\beta(x) = d. \tag{12.20}$$

Lause 49. Olkoon $\beta \in \mathbb{K} = \mathbb{Q}(\tau)$ ja $[\mathbb{K} : \mathbb{Q}] = m$. Tällöin

$$M_\beta(x) \underset{\mathbb{Q}[x]}{\mid} K_\beta(x); \tag{12.21}$$

$$K_\beta(x) = M_\beta(x)^{m/d}, \quad m/d \in \mathbb{Z}^+. \tag{12.22}$$

Seuraus 3.

$$\{\sigma_1(\beta), ..., \sigma_m(\beta)\} = \{\beta_1, ..., \beta_d\}; \tag{12.23}$$

$$\beta \in \mathbb{Q} \quad \Leftrightarrow \quad \sigma_1(\beta) = ... = \sigma_m(\beta); \tag{12.24}$$

$$\mathbb{Q}(\beta) = \mathbb{K} \quad \Leftrightarrow \quad \sigma_i(\beta) \neq \sigma_j(\beta) \quad \forall\ i \neq j. \tag{12.25}$$

12.2 Diskriminantti/EI vaadita

Määritelmä 46.

Olkoon $\mathbb{K} = \mathbb{Q}(\tau)$ lukukunta ja $[\mathbb{K} : \mathbb{Q}] = m$. Lukujen $\gamma_1, ..., \gamma_m \in \mathbb{K}$ diskriminantti on

$$\Delta(\gamma_1, ..., \gamma_m) = (\det(\sigma_i(\gamma_j))_{i=1,...,m,j=1,...,m})^2 = \tag{12.26}$$

$$\begin{vmatrix} \sigma_1(\gamma_1) & \sigma_2(\gamma_1) & ... & \sigma_m(\gamma_1) \\ . & & ... & . \\ . & & ... & . \\ . & & ... & . \\ \sigma_1(\gamma_m) & \sigma_2(\gamma_m) & ... & \sigma_m(\gamma_m) \end{vmatrix}^2 .$$

Alkion $\beta \in \mathbb{K}$ diskriminantti on

$$\delta(\beta) = \Delta(1, \beta, ..., \beta^{m-1}) = \tag{12.27}$$

$$\begin{vmatrix} 1 & 1 & & 1 \\ \sigma_1(\beta) & \sigma_2(\beta) & ... & \sigma_m(\beta) \\ . & & ... & . \\ . & & ... & . \\ . & & ... & . \\ \sigma_1(\beta)^{m-1} & \sigma_2(\beta)^{m-1} & ... & \sigma_m(\beta)^{m-1} \end{vmatrix}^2 .$$

Lause 50.

$$\Delta(\gamma_1, ..., \gamma_m) \in \mathbb{Q}. \tag{12.28}$$

Lause 51. Lukujoukko $\{\gamma_1, ..., \gamma_m\}$ on $\mathbb{K}$:n kanta täsmälleen silloin kun sen diskriminantti ei häviä eli

$$\dim_{\mathbb{Q}} \mathbb{Q}(\gamma_1, ..., \gamma_m) = m \quad \Leftrightarrow \quad \Delta(\gamma_1, ..., \gamma_m) \neq 0. \tag{12.29}$$

Lause 52.

$$\delta(\beta) = \prod_{i<j} (\sigma_i(\beta) - \sigma_j(\beta))^2; \tag{12.30}$$

$$\delta(\beta) \neq 0 \quad \Leftrightarrow \quad \deg_{\mathbb{Q}}(\beta) = m; \tag{12.31}$$

$$\delta(\beta) \neq 0 \quad \Leftrightarrow \quad \mathbb{Q}(\beta) = \mathbb{K}. \tag{12.32}$$

12.3 Normi ja jälki/Norm and trace

Määritelmä 47. Olkoon $\mathbb{K} = \mathbb{Q}(\tau)$ lukukunta ja $[\mathbb{K} : \mathbb{Q}] = m$. Alkion $\beta \in \mathbb{K}$ normi on

$$N(\beta) = N_{\mathbb{K}}(\beta) = \prod_{i=1}^{m} \sigma_i(\beta) \tag{12.33}$$

ja jälki/trace

$$T(\beta) = T_{\mathbb{K}}(\beta) = \sum_{i=1}^{m} \sigma_i(\beta). \tag{12.34}$$

Lause 53.

$$N_{\mathbb{K}}(\beta), \quad T_{\mathbb{K}}(\beta) \in \mathbb{Q}. \tag{12.35}$$

$$N_{\mathbb{K}}(\beta) \neq 0 \quad \Leftrightarrow \quad \beta \neq 0. \tag{12.36}$$

Todistus. (12.35):

$$K_\beta(x) = x^m - T(\beta)x^{m-1} + ... + (-1)^m N(\beta) \in \mathbb{Q}[x]. \tag{12.37}$$

(12.36): Koska σ_i on injektio, niin

$$\sigma_i(x) = 0 \quad \Leftrightarrow \quad x = 0. \quad \square \tag{12.38}$$

Lause 54.

$$N(\alpha\beta) = N(\alpha)N(\beta) \tag{12.39}$$

$$T(r\alpha + s\beta) = rT(\alpha) + sT(\beta); \tag{12.40}$$

$$N(r) = r^m, \quad T(r) = mr; \tag{12.41}$$

kaikilla $\alpha, \beta \in \mathbb{K}$, $r, s \in \mathbb{Q}$.

Esimerkki 33.

Osoitetaan jälkifuntiota käyttäen, että/Let us show by using the trace function that

$$3^{1/2} \notin \mathbb{K} = \mathbb{Q}(2^{1/2}) = \mathbb{Q}[2^{1/2}]. \tag{12.42}$$

Huomaa, että

$$[\mathbb{Q}(2^{1/2}) : \mathbb{Q}] = [\mathbb{Q}(3^{1/2}) : \mathbb{Q}] = 2. \tag{12.43}$$

Tehdään vastaoletus

$$3^{1/2} \in \mathbb{Q}[2^{1/2}] = \mathbb{Q} + 2^{1/2}\mathbb{Q} \tag{12.44}$$

eli

$$3^{1/2} = a + b2^{1/2}, \quad a, b \in \mathbb{Q}. \tag{12.45}$$

Otetaan jälki

$$T_{\mathbb{K}}(3^{1/2}) = T_{\mathbb{K}}(a) + T_{\mathbb{K}}(b2^{1/2}) = 2a + bT_{\mathbb{K}}(2^{1/2}). \tag{12.46}$$

Toisaalta/On the other hand. Tuloksen (12.22) mukaan lukujen $2^{1/2}$ ja $3^{1/2}$ kuntapolynomit

$$K_{2^{1/2}}(x) = \prod_{i=1}^{2}(x - \sigma_i(2^{1/2})) = x^2 - T_{\mathbb{K}}(2^{1/2})x + N_{\mathbb{K}}(2^{1/2});$$

$$K_{3^{1/2}}(x) = \prod_{i=1}^{2}(x - \sigma_i(3^{1/2})) = x^2 - T_{\mathbb{K}}(3^{1/2})x + N_{\mathbb{K}}(3^{1/2})$$

kunnan $\mathbb{K}$ suhteen ovat vastaavien minimipolynomien/powers of corresponding minimal polynomials

$$M_{2^{1/2}}(x) = x^2 - 2; \quad M_{3^{1/2}}(x) = x^2 - 3$$

potensseja. Siten

$$x^2 - 2 = x^2 - T_{\mathbb{K}}(2^{1/2})x + N_{\mathbb{K}}(2^{1/2});$$

$$x^2 - 3 = x^2 - T_{\mathbb{K}}(3^{1/2})x + N_{\mathbb{K}}(3^{1/2}), \tag{12.47}$$

josta

$$T_{\mathbb{K}}(2^{1/2}) = T_{\mathbb{K}}(3^{1/2}) = 0. \tag{12.48}$$

Sijoittamalla yhtälöön (12.46) saadaan

$$a = 0 \quad \Rightarrow \quad 3^{1/2} = b2^{1/2}, \quad b \in \mathbb{Q}$$

$$\Rightarrow \quad (3/2)^{1/2} = b \quad \Rightarrow$$

$$T_{\mathbb{K}}((3/2)^{1/2}) = 2b. \tag{12.49}$$

Toisaalta

$$K_{(3/2)^{1/2}}(x) = x^2 - T_{\mathbb{K}}((3/2)^{1/2})x + N_{\mathbb{K}}((3/2)^{1/2});$$
$$M_{(3/2)^{1/2}}(x) = x^2 - 3/2 \quad \Rightarrow$$
$$T_{\mathbb{K}}((3/2)^{1/2}) = 0 \quad \Rightarrow \quad b = 0$$
$$\Rightarrow \quad 3^{1/2} = 0. \quad (12.50)$$

Ristiriita. □

Lause 55. EI vaadita. Olkoon $\mathbb{K} = \mathbb{Q}(\tau)$ lukukunta, $[\mathbb{K} : \mathbb{Q}] = m$ ja $M_\tau(x)$ minimipolynomi ja $DM_\tau(x)$ sen derivaatta. Tällöin

$$\Delta(1, \tau, ..., \tau^{m-1}) = (-1)^{m(m-1)/2} N(DM_\tau(\tau)). \quad (12.51)$$

Lause 56. EI vaadita. Olkoon $\mathbb{K} = \mathbb{Q}(\tau)$ lukukunta, $[\mathbb{K} : \mathbb{Q}] = m$ ja $\gamma_1, ..., \gamma_m \in \mathbb{K}$. Tällöin

$$\Delta(\gamma_1, ..., \gamma_m) = \det(T(\gamma_i \gamma_j)). \quad (12.52)$$

13 Kokonaiset algebralliset luvut $\mathbb{B}$

Joukko $\mathbb{B} \subseteq \mathbb{C}$ koostuu kaikista kokonaisista algebrallisista luvuista kunnan $\mathbb{Q}$ yli.

The set $\mathbb{B} \subseteq \mathbb{C}$ consists of all algebraic integers over $\mathbb{Q}$.

Seuraava tulos osoittaa, että kokonaisten algebrallisten lukujen joukko $\mathbb{B}$ on algebrallisten lukujen $\mathbb{A}$ kunnan alirengas.

Lause 57.

$$\mathbb{B} \leqslant \mathbb{A}. \quad (13.1)$$

Seuraus 4. Jos $\alpha, \beta \in \mathbb{B}$, niin

$$\alpha \pm \beta, \ \alpha\beta \ \in \mathbb{B}. \quad (13.2)$$

Kokonaisten algebrallisten lukujen joukko $\mathbb{B}$ on algebrallisesti suljettu/algebraicly closed eli

Lause 58. Olkoon

$$b(x) = x^n + ... + b_0 \in \mathbb{B}[x] \setminus \{0(x)\},$$

$$b(\omega) = 0 \quad \Rightarrow \quad \omega \in \mathbb{B}. \tag{13.3}$$

Esimerkki 34.

$$\alpha^2 = \alpha + 1, \quad \beta^5 + \alpha\beta^2 + 5 = 0 \tag{13.4}$$

$$\omega^2 - \beta = 0 \quad \Rightarrow \quad \omega \in \mathbb{B}. \tag{13.5}$$

Lause 59. Jos $\alpha \in \mathbb{A}$, niin $\exists$ pienin/smallest $d \in \mathbb{Z}^+$, että

$$d\alpha \in \mathbb{B}. \tag{13.6}$$

Määritelmä 48. Lauseen 59 mukainen luku $d \in \mathbb{Z}^+$ on algebrallisen luvun α nimittäjä eli den $\alpha = d$.

Esimerkki 35. Olkoon

$$5\alpha^2 + \alpha + 1 = 0, \quad \Rightarrow \quad (5\alpha)^2 + 5\alpha + 5 = 0 \quad \Rightarrow \tag{13.7}$$

$$5\alpha \in \mathbb{B}, \quad den\ \alpha = 5. \tag{13.8}$$

Määritelmä 49. Olkoon $\mathbb{K} = \mathbb{Q}(\tau)$ lukukunta. Tällöin

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{K} \cap \mathbb{B} \tag{13.9}$$

on $\mathbb{K}$:n kokonaislukujen rengas/ring of integers.

Esimerkki 36.

$$\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}. \tag{13.10}$$

Esimerkki 37.

$$2^{1/7} \notin \mathbb{Q}. \tag{13.11}$$

Vastaoletus

$$2^{1/7} \in \mathbb{Q}. \quad \text{Mutta} \quad 2^{1/7} \in \mathbb{B} \quad \Rightarrow \quad 2^{1/7} \in \mathbb{Z}.$$

$$\text{Lisäksi} \quad 1 < 2^{1/7} < 2. \quad \text{Ristiriita.} \quad \square \tag{13.12}$$

Esimerkki 38. Olkoon $n \in \mathbb{Z}_{\geq 2}$. Tällöin

$$2^{1/n} + 3^{1/n} \notin \mathbb{Q}. \tag{13.13}$$

Rationaaliset kokonaisluvut muodostavat alirenkaan kokonaisten algebrallisten lukujen renkaille.

Lause 60.

$$\mathbb{Z} \leqslant \mathbb{Z}_{\mathbb{K}} \leqslant \mathbb{B}. \tag{13.14}$$

Edelleen

Lause 61. Olkoon $\beta \in \mathbb{Z}_{\mathbb{K}}$, tällöin

$$\mathbb{Z}[\beta] \leqslant \mathbb{Z}_{\mathbb{K}}. \tag{13.15}$$

Huomautus 10. Usein pätee kuitenkin

$$\mathbb{Z}_{\mathbb{K}} \neq \mathbb{Z}[\beta]. \tag{13.16}$$

Esimerkki 39. $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ on lukukunta, missä

$$\frac{1+\sqrt{5}}{2} \in \mathbb{Z}_{\mathbb{K}}, \quad \frac{1+\sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}]. \tag{13.17}$$

Lause 62. EI vaadita. Olkoon $\mathbb{K}$ lukukunta. Tällöin

$$\mathbb{K} = \mathbb{Q}(\lambda), \quad \lambda \in \mathbb{Z}_{\mathbb{K}}. \tag{13.18}$$

Lause 63. EI vaadita. Olkoon $\mathbb{K} = \mathbb{Q}(\tau)$ lukukunta ja $[\mathbb{K} : \mathbb{Q}] = m$. Jos $\{\lambda_1, ..., \lambda_m\} \subseteq \mathbb{Z}_\mathbb{K}$ on $\mathbb{K}$:n kanta, niin

$$\Delta(\lambda_1, ..., \lambda_m) \in \mathbb{Z} \setminus \{0\}. \tag{13.19}$$

Lause 64. EI vaadita. Olkoon $\mathbb{K} = \mathbb{Q}(\tau)$ lukukunta ja $[\mathbb{K} : \mathbb{Q}] = m$. Tällöin on olemassa $\{\lambda_1, ..., \lambda_m\} \subseteq \mathbb{Z}_\mathbb{K}$, joka on $\mathbb{K}$:n kanta $\mathbb{Q}$:n yli.

Lause 65. EI vaadita. Olkoon $\mathbb{K} = \mathbb{Q}(\tau)$ lukukunta ja $[\mathbb{K} : \mathbb{Q}] = m$. Tällöin on olemassa $\{\lambda_1, ..., \lambda_m\} \subseteq \mathbb{Z}_\mathbb{K}$, joka on $\mathbb{Z}_\mathbb{K}$:n kanta $\mathbb{Z}$:n yli.

Määritelmä 50. Lauseen 65 mukainen $\mathbb{Z}_\mathbb{K}$:n kanta $\mathbb{Z}$:n yli on kunnan $\mathbb{K}$ kokonaislukujen kanta.

Lause 66. EI vaadita. Olkoon $\{\lambda_1, ..., \lambda_m\} \subseteq \mathbb{Z}_\mathbb{K}$ kunnan $\mathbb{K}$ kanta. Jos $\Delta(\lambda_1, ..., \lambda_m)$ on neliövapaa, niin $\{\lambda_1, ..., \lambda_m\}$ on kunnan $\mathbb{K}$ kokonaislukujen kanta.

Esimerkki 40.

$$\Delta\left(1, \frac{1+\sqrt{5}}{2}\right) = 5 \quad \Rightarrow \quad \left\{1, \frac{1+\sqrt{5}}{2}\right\} \tag{13.20}$$

on $\mathbb{Q}(\sqrt{5})$:n kokonaislukujen kanta.

14 Jaollisuus renkaassa $\mathbb{Z}_\mathbb{K}$

Lause 67. Olkoon $\beta \in \mathbb{Z}_\mathbb{K}$, tällöin

$$N_\mathbb{K}(\beta), \quad T_\mathbb{K}(\beta) \in \mathbb{Z}; \tag{14.1}$$

$$N_\mathbb{K}(\beta) \neq 0 \quad \Leftrightarrow \quad \beta \neq 0. \tag{14.2}$$

Olkoon $\mathbb{Z}_\mathbb{K}^*$ kokonaislukujen renkaan $\mathbb{Z}_\mathbb{K}$ yksikköryhmä.

Lause 68. Olkoot $a, b \in \mathbb{Z}_{\mathbb{K}}$, tällöin

$$a \underset{\mathbb{Z}_{\mathbb{K}}}{|} b \quad \Rightarrow \quad N(a) \underset{\mathbb{Z}}{|} N(b); \tag{14.3}$$

$$a \in \mathbb{Z}_{\mathbb{K}}^* \quad \Leftrightarrow \quad N(a) = \pm 1; \tag{14.4}$$

$$a \sim b \quad \Rightarrow \quad N(a) = \pm N(b); \tag{14.5}$$

$$|N(a)| \in \mathbb{P} \quad \Rightarrow \quad a \in J_{\mathbb{Z}_{\mathbb{K}}}. \tag{14.6}$$

Todistus.

14.3: Olkoon

$$b = ca, \quad a, b, c \in \mathbb{Z}_{\mathbb{K}} \tag{14.7}$$

Koska σ_i on homomorfia, niin

$$\sigma_i(b) = \sigma_i(c)\sigma_i(a) \quad \forall\ i = 1, ..., m \quad \Rightarrow \tag{14.8}$$

$$N(b) = \prod_{i=1}^{m} \sigma_i(b) = \prod_{i=1}^{m} \sigma_i(c) \prod_{i=1}^{m} \sigma_i(a) = N(c)N(a), \tag{14.9}$$

missä

$$N(b), N(c), N(a) \in \mathbb{Z} \quad \Rightarrow \quad N(a) \underset{\mathbb{Z}}{|} N(b). \quad \square \tag{14.10}$$

14.4: Olkoon ensin

$$a \in \mathbb{Z}_{\mathbb{K}}^* \quad \Rightarrow \quad a \underset{\mathbb{Z}_{\mathbb{K}}}{|} 1. \tag{14.11}$$

Kohdan (14.3) nojalla saadaan

$$N(a) \underset{\mathbb{Z}}{|} N(1) = 1 \quad \Rightarrow \quad N(a) = \pm 1. \tag{14.12}$$

Olkoon sitten

$$N(a) = \pm 1. \tag{14.13}$$

Siten

$$a\sigma_2(a)\cdots\sigma_m(a) = \pm 1, \quad \Rightarrow \quad c = \sigma_2(a)\cdots\sigma_m(a) \in \mathbb{K}. \tag{14.14}$$

Toisaalta, koska

$$a \in \mathbb{Z}_{\mathbb{K}} \subseteq \mathbb{B} \quad \Rightarrow \quad \sigma_2(a), ..., \sigma_m(a) \in \mathbb{B} \quad \Rightarrow \quad c \in \mathbb{B}. \tag{14.15}$$

Siispä

$$c \in \mathbb{K} \cap \mathbb{B} = \mathbb{Z}_{\mathbb{K}}, \quad \pm c \cdot a = 1 \quad \Rightarrow \tag{14.16}$$

$$a \underset{\mathbb{Z}_{\mathbb{K}}}{\mid} 1 \quad \Rightarrow \quad a \in \mathbb{Z}_{\mathbb{K}}^*. \tag{14.17}$$

Kohta (14.4) todistettu. □

Huomaa, että vaikka $a \in \mathbb{Z}_{\mathbb{K}}$, niin voi olla $\sigma_i(a) \notin \mathbb{Z}_{\mathbb{K}}$, vertaa Esimerkki 32. Kuitenkin $\sigma_i(a) \in \mathbb{B}$.

14.5: Nyt

$$b = ua, \quad u \in \mathbb{Z}_{\mathbb{K}}^* \quad \Rightarrow \quad N(u) = \pm 1 \quad \Rightarrow \tag{14.18}$$

$$N(b) = N(u)N(a) = \pm N(a). \quad \square \tag{14.19}$$

14.6: Tässä $a \neq 0$. Vastaoletus: a jakaantuu eli

$$a = bc, \quad b, c \notin \mathbb{Z}_{\mathbb{K}}^*, \ b, c \neq 0, \quad \Rightarrow \tag{14.20}$$

$$|N(b)|, |N(c)| \geq 2 \quad \Rightarrow \quad |N(a)| = |N(b)||N(c)| \notin \mathbb{P}. \tag{14.21}$$

Ristiriita. □

Lause 69. Oletetaan, että D on UFD, $a, b, c \in D$ ja

$$ab = c^k, \quad a \perp b. \tag{14.22}$$

Tällöin

$$a \sim d^k, \quad b \sim e^k, \tag{14.23}$$

joillakin/with some $d, e \in D$.

15 Eräs Diofantoksen yhtälö/A Diophantine equation

Algebrallisten lukujen tutkimisen päämotiivi on alkujaan ollut Diofantoksen yhtälöiden ratkaiseminen.

Esimerkki 41.

$$y^2 + 2 = x^3, \quad 2 \not| y, \tag{15.1}$$

on Diofantoksen yhtälö eli sille haetaan kokonaislukuratkaisuja/seeking integer solutions.

I. Yhtälö hajoaa/Equation splits kunnassa $\mathbb{K} = \mathbb{Q}(\sqrt{-2})$ seuraavasti:

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3. \tag{15.2}$$

II. Kokonaislukujen rengas on

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\sqrt{-2}. \tag{15.3}$$

III. Sen yksikköryhmä on

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1\}. \tag{15.4}$$

IV. Kokonaisalue

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\sqrt{-2}. \tag{15.5}$$

on Normi-Eukleideen alue ja siten UFD. Siten siinä voi operoida kuten rationaalisten kokonaislukujen renkaassa (vrt. Lukuteorian perusteet: Pythagoraan yhtälön ratkaiseminen.)

V. Olkoon

$$D = syt(y - \sqrt{-2}, y + \sqrt{-2}),$$

$$D = a + b\sqrt{-2} \in \mathbb{Z}_{\mathbb{K}} \quad \Rightarrow \quad (15.6)$$

$$D \underset{\mathbb{Z}_{\mathbb{K}}}{\Big|} 2y, \quad D \underset{\mathbb{Z}_{\mathbb{K}}}{\Big|} 2\sqrt{-2} \quad \Rightarrow \qquad (15.7)$$

$$N(D) \underset{\mathbb{Z}}{\Big|} N(2y), \quad N(D) \underset{\mathbb{Z}}{\Big|} N(2\sqrt{-2}),$$

$$N(D) = (a + b\sqrt{-2})(a - b\sqrt{-2}) = a^2 + 2b^2 \quad \Rightarrow \quad (15.8)$$

$$a^2 + 2b^2 \underset{\mathbb{Z}}{\Big|} 4y^2, \quad a^2 + 2b^2 \underset{\mathbb{Z}}{\Big|} -8 \quad \Rightarrow \qquad (15.9)$$

$$D = \pm 1, \pm 2, \pm\sqrt{-2}. \qquad (15.10)$$

Jos esimerkiksi

$$\sqrt{-2} \underset{\mathbb{Z}_{\mathbb{K}}}{\Big|} y - \sqrt{-2} \quad \Rightarrow$$

$$y - \sqrt{-2} = \sqrt{-2}(e + f\sqrt{-2}), \quad e, f \in \mathbb{Z} \quad \Rightarrow$$

$$2f = -y, \quad \text{Ei käy.} \quad (15.11)$$

Vastaavasti päätellään, että vain

$$D = \pm 1 \underset{\mathbb{Z}_{\mathbb{K}}}{\Big|} y - \sqrt{-2}, y + \sqrt{-2}, \quad \Rightarrow \qquad (15.12)$$

$$y - \sqrt{-2} \ \perp \ y + \sqrt{-2}, \quad \Rightarrow \tag{15.13}$$

$$y + \sqrt{-2} = (c + d\sqrt{-2})^3, \quad c + d\sqrt{-2} \in \mathbb{Z}_{\mathbb{K}}, \quad c, d \in \mathbb{Z}$$

$$\Rightarrow \quad 1 = d(3c^2 - 2d) \quad \Rightarrow \quad d = \pm 1, \quad d = 1, c = \pm 1;$$

$$y = c^3 - 6cd^2 \quad \Rightarrow \quad y = \pm 5$$

$$\Rightarrow \quad x = 3, \ y = \pm 5. \quad \square \tag{15.14}$$

16 Neliökunnat

Jokainen neliökunta on esitettävissä muodossa

$$\mathbb{K} = \mathbb{Q}(\sqrt{d}), \quad d \in \mathbb{Z}, \tag{16.1}$$

missä d on neliövapaa tästä eteenpäin.

Lause 70.

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

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\lambda, \tag{16.2}$$

missä

$$\lambda = \sqrt{d}, \quad d \equiv 2, \ 3 \pmod 4; \tag{16.3}$$

$$\lambda = \frac{1 + \sqrt{d}}{2}, \quad d \equiv 1 \pmod 4; \tag{16.4}$$

$$\Delta = 4d, \quad d \equiv 2, \ 3 \pmod 4; \tag{16.5}$$

$$\Delta = d, \quad d \equiv 1 \pmod 4. \tag{16.6}$$

Todistus. Tarkastellaan kokonaislukua

$$\beta = r + s\sqrt{d} \in \mathbb{Z}_{\mathbb{K}}, \quad r, s \in \mathbb{Q} \quad \Rightarrow$$

$$T(\beta) = 2r \in \mathbb{Z} \quad \Rightarrow \quad r \in \frac{1}{2}\mathbb{Z} \quad \Rightarrow \quad r = \frac{a}{2},\ a \in \mathbb{Z};$$

$$N(\beta) = r^2 - ds^2 \in \mathbb{Z} \quad \Rightarrow \quad d(2s)^2 = (2r)^2 - 4N(\beta) \in \mathbb{Z},$$

$$\text{missä} \quad 2s = \frac{k}{l}, \quad k \perp l, \quad \Rightarrow$$

$$d(2s)^2 = \frac{dk^2}{l^2} \in \mathbb{Z}, \quad \text{missä d on neliövapaa} \quad \Rightarrow \quad l = 1,$$

$$\Rightarrow \quad 2s \in \mathbb{Z} \quad \Rightarrow \quad s = \frac{b}{2},\ b \in \mathbb{Z}. \quad (16.7)$$

Siten

$$\beta = \frac{a + b\sqrt{d}}{2}, \quad a, b \in \mathbb{Z}. \quad (16.8)$$

Tutkitaan sitten mitä arvoja luvut a ja b saavat.

Tapaus 16.3 eli $d \equiv 2,\ 3 \pmod 4$:

Koska

$$N(\beta) = \frac{a^2 - db^2}{4} \in \mathbb{Z} \quad \Rightarrow$$

$$a^2 - db^2 \equiv 0 \pmod 4 \quad \Rightarrow$$

$$a \equiv b \equiv 0 \pmod 2 \quad \Rightarrow$$

$$\beta = \frac{a + b\sqrt{d}}{2} = A + B\sqrt{d}, \quad A, B \in \mathbb{Z}. \quad (16.9)$$

Tapaus 16.4 eli $d \equiv 1 \pmod 4$:

Koska

$$N(\beta) = \frac{a^2 - db^2}{4} \in \mathbb{Z} \quad \Rightarrow$$

$$a^2 \equiv b^2 \pmod 4 \quad \Rightarrow$$

$$a \equiv b \equiv 0 \pmod 2 \quad \text{tai} \quad a \equiv b \equiv 1 \pmod 2 \quad \Rightarrow \quad (16.10)$$

$$\beta = \frac{a + b\sqrt{d}}{2}, \quad a \equiv b \pmod 2,\ a, b \in \mathbb{Z}$$

$$\Rightarrow \quad \beta = A + B\frac{1 + \sqrt{d}}{2}, \quad A, B \in \mathbb{Z}. \quad \square \tag{16.11}$$

16.1 Imaginaariset neliökunnat

16.1.1 Yksikköryhmä

Seuraavassa

$$\omega = e^{\frac{2\pi}{3}i}. \tag{16.12}$$

Lause 71. Olkoon $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, tällöin

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1, \pm i\}, \quad d = -1; \tag{16.13}$$

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1\}, \quad d = -2; \tag{16.14}$$

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1, \pm\omega, \pm\omega^2\}, \quad d = -3; \tag{16.15}$$

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1\}, \quad d \in \mathbb{Z}_{\leq -5}. \tag{16.16}$$

Esimerkiksi tapaus: $d = -5 \equiv 3 \pmod 4$, joten kokonaisluvut muotoa

$$\beta = A + B\sqrt{-5}, \quad A, B \in \mathbb{Z} \quad \Rightarrow$$

$$N(\beta) = A^2 + 5B^2 = 1 \quad \Rightarrow \quad A = \pm 1,\ B = 0 \quad \Rightarrow$$

$$\mathbb{Z}_{\mathbb{Q}(\sqrt{-5})}^* = \{\pm 1\}. \tag{16.17}$$

16.1.2 UFD/Eukleideen alue

Lause 72. Olkoon $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, tällöin $\mathbb{Z}_{\mathbb{K}}$ on UFD, kun

$$d = -1, -2, -3, -7, -11, \tag{16.18}$$

jotka ovat imaginaariset Eukleideen alueet ja lisäksi, kun

$$d = -19, -43, -67, -163. \tag{16.19}$$

Tässä kaikki, kun $d \leq -1$.

Todistus. Tapaus $d = -1$, jolloin $\mathbb{Z}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[i]$. Todistetaan, että $\mathbb{Z}[i]$ on Eukleideen alue.

Olkoot $a, b \in \mathbb{Z}[i]$, jolloin

$$\frac{a}{b} = x + iy, \quad x, y \in \mathbb{Q}. \tag{16.20}$$

Valitaan sellaiset $s, t \in \mathbb{Z}$, että

$$|x - s| \leq \frac{1}{2}, \quad |y - t| \leq \frac{1}{2}. \tag{16.21}$$

Olkoon

$$q = s + it, \quad a = qb + r, \quad r \in \mathbb{Z}[i]. \tag{16.22}$$

Ottamalla normit saadaan

$$N(r) = N(b)N(x - s + i(y - t)) = N(b)((x - s)^2 + (y - t)^2) \tag{16.23}$$

$$\leq N(b)\frac{1}{2} \quad \Rightarrow \quad N(r) < N(b) \tag{16.24}$$

ja lisäksi

$$N : \ \mathbb{Z}[i] \to \mathbb{N}, \tag{16.25}$$

joten N on Eukleideen funktio. Edelleen, Lauseen 9 nojalla Eukleideen alue on aina UFD. □

16.1.3 Gaussin kokonaisluvut/alkuluvut

Määritelmä 51. Kunnan $\mathbb{K} = \mathbb{Q}(i)$, kokonaislukujen renkaan

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{Z}[i] \tag{16.26}$$

alkioita sanotaan Gaussin kokonaisluvuiksi. Edelleen jaottomat Gaussin kokonaisluvut ovat Gaussin alkulukuja.

Koska $\mathbb{Z}[i]$ on UFD, niin sen jaottomat alkiot ovat alkualkioita eli

$$P_{\mathbb{Z}[i]} = J_{\mathbb{Z}[i]}. \tag{16.27}$$

Lause 73.

$$\pi = a + ib \in P_{\mathbb{Z}[i]} \quad \Leftrightarrow \tag{16.28}$$

$$\pi \sim 1 + i; \tag{16.29}$$

$$\pi \sim a + ib, \quad a^2 + b^2 = p \in \mathbb{P}, \quad p \equiv 1 \pmod 4; \tag{16.30}$$

$$\pi \sim p \in \mathbb{P}, \quad p \equiv 3 \pmod 4. \tag{16.31}$$

16.2 Reaaliset neliökunnat

16.2.1 Yksikköryhmä

Reaalisen neliökunnan yksikköryhmät ovat äärettömiä ja yleisessä tapauksessa varsin hankalasti määrättävissä. Niiden määräämiseen tarvitaan tietoa Pellin yhtälöiden ratkaisemisesta.

Lause 74. Olkoon $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}_{\geq 2}$. Tällöin

$$\mathbb{Z}_{\mathbb{K}}^* = \{x_k + y_k\sqrt{d} |\ x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k,\ k \in \mathbb{Z}\}, \tag{16.32}$$

missä $(x_1, y_1) \in \mathbb{Z}^2$ on pienin positiivinen Pellin yhtälön

$$x^2 - dy^2 = 1 \tag{16.33}$$

ratkaisu.

Kyseessä oleva pienin ratkaisu voidaan etsiä käyttäen ketjumurtolukujen teoriaa, katso kurssi: Ketjumurtoluvut.

16.2.2 UFD/Eukleideen alue

Lause 75. Olkoon $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, tällöin $\mathbb{Z}_\mathbb{K}$ on UFD, kun

$$d = 2, 3, 5, 6, 7, 13, 17, 21, 29, 33, 37, 41, 57, 73, \tag{16.34}$$

jotka ovat reaaliset Eukleideen alueet ja lisäksi, kun

$$d = 11, 14, 19, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67,$$

$$69, 71, 77, 83, 86, 89, 93, 94, 97. \tag{16.35}$$

Tässä vain kaikki, missä $2 \leq d \leq 100$.