802656S ALGEBRALLISET LUVUT OSA II
ALGEBRAIC NUMBERS PART II

Tapani Matala-aho
MATEMATIIKKA/LUTK/OULUN YLIOPISTO

KEVÄT 2020

Määritelmä 1

Olkoon R rengas. Formaali lauseke

$$P(t_1, ..., t_m) = \sum_{Finite} p_{i_1,...,i_m} t_i^{i_1} \cdots t_m^{i_m}, \quad p_{i_1,...,i_m} \in R \tag{1.1}$$

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

$$\deg P(t_1, ..., t_m) = \max\{i_1 + ... + i_m\}. \tag{1.2}$$

Käytetään kaikkien R-kertoimisten polynomien joukolle merkintää

$$R[t_1, ..., t_m]. \tag{1.3}$$

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

$$p^{\lambda}(t_1, ..., t_m) = p(t_{\lambda(1)}, ..., t_{\lambda(m)}). \tag{1.4}$$

Määritelmä 2

Polynomi p on symmetrinen, jos

$$p(t_{\lambda(1)}, ..., t_{\lambda(m)}) = p(t_1, ..., t_m) \quad \forall\ \lambda \in S_m. \tag{1.5}$$

Perusfunktiot

Määritelmä 3

Polynomit

$$s_k = s_k(t_1, ..., t_m) = \sum_{1 \leq j_1 < j_2 < ... < j_k \leq m} t_{j_1} t_{j_2} \cdots t_{j_k}, \quad k = 1, ..., m, \tag{1.6}$$

ovat symmetriset perusfunktiot/elementary symmtric polynomials.

Lemma 1

Symmetriset perusfunktiot $s_1, ..., s_m$ *ovat symmetrisiä polynomeja eli*

$$s_k(t_{\lambda(1)}, ..., t_{\lambda(m)}) = s_k(t_1, ..., t_m) \quad \forall\ \lambda \in S_m \tag{1.7}$$

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

Siten polynomeja

$$s_1 = t_1 + \ldots + t_m; \tag{1.8}$$

$$s_2 = t_1 t_2 + t_1 t_3 + \ldots + t_{m-1} t_m; \tag{1.9}$$

$$s_3 = t_1 t_2 t_3 + t_1 t_2 t_4 + \ldots + t_{m-2} t_{m-1} t_m; \tag{1.10}$$

...

$$s_m = t_1 t_2 \cdots t_{m-1} t_m; \tag{1.11}$$

voidaan kutsua myös symmetrisiksi peruspolynomeiksi.

Lause 1

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*

$$S(t_1, ..., t_m) = P(s_1(t_1, ..., t_m), ..., s_m(t_1, ..., t_m)). \qquad (1.12)$$

Olkoot $S \subseteq R$ renkaita. Oletetaan, että polynomi $a(x) = a_0 + a_1 x + ... + x^m \in S[x]$ jakaantuu polynomirenkaassa $R[x]$ seuraavasti

$$a(x) = (x - \alpha_1) \cdots (x - \alpha_m), \quad \alpha_1, ..., \alpha_m \in R. \tag{1.13}$$

Lause 2

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

$$b(\alpha_1, ..., \alpha_m) \in S. \tag{1.14}$$

Olkoot $K \subseteq L$ kuntia. Oletetaan, että polynomi $a(x) = a_0 + a_1 x + \ldots + a_m x^m \in K[x]$ jakaantuu polynomirenkaassa $L[x]$ seuraavasti

$$a(x) = a_m(x - \alpha_1) \cdots (x - \alpha_m), \quad \alpha_1, \ldots, \alpha_m \in L. \tag{1.15}$$

Lause 3

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

$$b(\alpha_1, \ldots, \alpha_m) \in K. \tag{1.16}$$

Esimerkki 1

Olkoon

$$x^2 + bx + c = (x - \alpha)(x - \beta) \in \mathbb{Q}[x]. \tag{1.17}$$

Tällöin

$$\alpha^2 + \beta^2 \in \mathbb{Q}, \tag{1.18}$$

$$\alpha^3 + 2\alpha\beta + \beta^3 \in \mathbb{Q}. \tag{1.19}$$

Määritelmä 4

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

$$L \times L \ \to L, \quad (\alpha, \beta) \ \to \alpha + \beta; \tag{2.1}$$

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

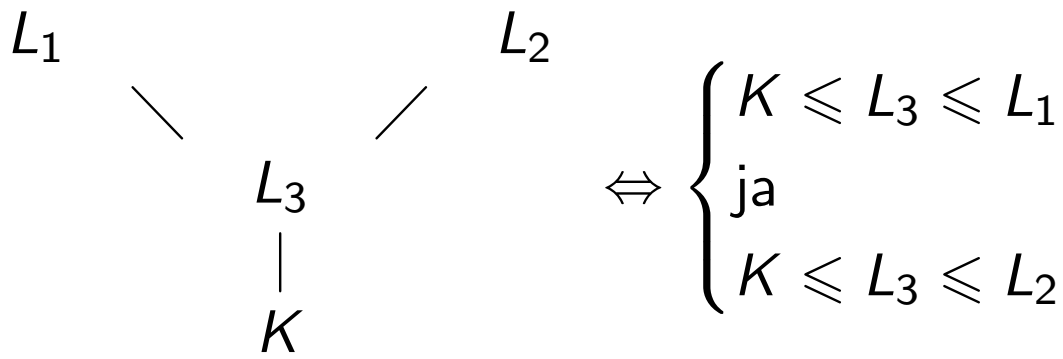
$$K \times L \ \to L, \quad (r, \alpha) \ \to r\alpha \tag{2.2}$$

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

Määritelmä 5

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

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



Lause 4

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

$$[L : K] = [L : M][M : K]. \tag{2.3}$$

Todistus. Olkoot

$$\begin{aligned} M &= \langle \alpha_1, ..., \alpha_r \rangle_K = K\alpha_1 + ... + K\alpha_r, \quad \dim_K M = r; \\ L &= \langle \beta_1, ..., \beta_s \rangle_M = M\beta_1 + ... + M\beta_s, \quad \dim_M L = s. \end{aligned} \tag{2.4}$$

Valitaan $\gamma \in L$. Sille pätee

$$\begin{aligned} \gamma &= \sum_{j=1}^{s} m_j \beta_j, \quad m_j \in M; \\ m_j &= \sum_{i=1}^{r} k_{ij} \alpha_i, \quad k_{ij} \in K \quad \Rightarrow \\ \gamma &= \sum_{i=1}^{r} \sum_{j=1}^{s} k_{ij} \alpha_i \beta_j \in K\alpha_1\beta_1 + ... + K\alpha_r\beta_s, \\ &\#\{\alpha_i \beta_j\} = rs. \end{aligned} \tag{2.5}$$

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

$$\sum_{i=1}^{r}\sum_{j=1}^{s} h_{ij}\alpha_i\beta_j = 0, \quad h_{ij} \in K \quad \Rightarrow$$

$$\sum_{j=1}^{s}\left(\sum_{i=1}^{r} h_{ij}\alpha_i\right)\beta_j = 0, \quad \text{missä } \{\beta_j\} \text{ on kanta/M} \quad \Rightarrow \tag{2.6}$$

$$\sum_{i=1}^{r} h_{ij}\alpha_i = 0, \quad \text{missä } \{\alpha_i\} \text{ on kanta/K} \quad \Rightarrow$$

$$h_{ij} = 0, \quad \forall \quad i,j. \quad \square$$

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

Määritelmä 6

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

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc. \tag{2.7}$$

Lause 5

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

Määritelmä 7

Ekvivalenssiluokille

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

sovitaan yhteenlasku

$$[a_1, b_1] + [a_2, b_2] = [a_1 b_2 + a_2 b_1, b_1 b_2] \tag{2.8}$$

ja kertolasku

$$[a_1, b_1][a_2, b_2] = [a_1 a_2, b_1 b_2] \tag{2.9}$$

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 6

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

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

$$\{\frac{a}{1} |\ a \in D\} \cong D, \tag{2.10}$$

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

$$ab^{-1} = \frac{a}{1}\left(\frac{b}{1}\right)^{-1} = \frac{a}{1}\frac{1}{b} = \frac{a}{b} \tag{2.11}$$

Esimerkki 2

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

Määritelmä 8

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

Nyt rationaalilukujen supistamis-/cancellation

$$\frac{ac}{bc} = \frac{a}{b} \tag{2.12}$$

ja laventamislaki/convert

$$\frac{a}{b} = \frac{da}{db} \tag{2.13}$$

seuraa suoraan Määritelmästä 7.

Esimerkki 3

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

Määritelmä 9

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

Tällöin pätevät ylläesitetyt supistussäännöt, jolloin mm.

$$\frac{(x^2-1)x}{(x-1)x^2} = \frac{x+1}{x} = 1 + \frac{1}{x}. \tag{2.14}$$

Esimerkki 4

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 7

$$K((T)) \cong Q(K[[T]]). \tag{2.15}$$

Näillä rakenteilla on seuraavat suhteet:

$$K[T] \subset K(T) \subset K((T)), \tag{2.16}$$

$$K[T] \subset K[[T]] \subset K((T)). \tag{2.17}$$

Määritelmä 10

Formaali derivaatta

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

on lineaarinen kuvaus, jolle pätee

$$DT^k = kT^{k-1} \quad \forall \quad k \in \mathbb{Z}. \tag{2.18}$$

Määritelmä 11

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

$$p(\alpha) = 0 \tag{3.1}$$

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

Esimerkki 5

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

$$p(\pi) = 0, \quad p(x) = x - \pi \in \mathbb{R}[x], \tag{3.2}$$

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

Määritelmä 12

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

$$M_\alpha(\alpha) = 0. \tag{3.3}$$

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

$$\deg \alpha = \deg_K \alpha = n \geq 1. \tag{3.4}$$

Lause 8

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

$$M_\alpha(x) = A_1(x)A_2(x), \quad \deg A_1(x), \deg A_2(x) \leq n-1. \tag{3.5}$$

Koska

$$0 = M_\alpha(\alpha) = A_1(\alpha)A_2(\alpha), \tag{3.6}$$

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

$$A_i(\alpha) = 0, \quad \deg A_i(x) \leq n-1. \quad \text{Ristiriita.} \tag{3.7}$$

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

$$M_\alpha(x) \underset{K[x]}{\mid} N_\alpha(x) \quad \text{ja} \quad N_\alpha(x) \underset{K[x]}{\mid} M_\alpha(x). \tag{3.8}$$

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

Määritelmä 13

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

$$M_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \quad a_i \in \mathbb{Q}, \tag{3.9}$$

oleva jaoton pääpolynomi.

Kokonainen algebrallinen luku

Määritelmä 14

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

$$M_\alpha(x) \in \mathbb{Z}[x]_n. \tag{3.10}$$

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

Siten kokonaisen astetta n olevan algebrallisen luvun minimipolynomi on muotoa

$$M_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \quad a_i \in \mathbb{Z}, \tag{3.11}$$

oleva jaoton pääpolynomi.

Algebraic integer

Esimerkki 6

$$\frac{1+\sqrt{5}}{2} \tag{3.12}$$

on 2. asteen kokonainen algebrallinen luku.

Esimerkki 7

$$x^3 - 2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) \tag{3.13}$$

Lauseen **??** 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 15

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

$$\alpha_1, ..., \alpha_n \in \mathbb{C}. \tag{3.14}$$

Määritelmä 16

Algebrallisen luvun α liittolukuihin liittyvät monomorfiat ovat kuntamorfismit

$$\sigma_1, ..., \sigma_n : \ \mathbb{K} = \mathbb{Q}(\alpha) \to \mathbb{C}; \tag{3.15}$$

joille pätee:

$$\sigma_i \quad \text{on injektio;} \tag{3.16}$$

$$\sigma_i(x + y) = \sigma_i(x) + \sigma_i(y); \tag{3.17}$$

$$\sigma_i(xy) = \sigma_i(x)\sigma_i(y); \tag{3.18}$$

$$\sigma_i|_{\mathbb{Q}} = \mathrm{Id} : \mathbb{Q} \to \mathbb{Q} \quad \text{identtinen kuvaus} \tag{3.19}$$

$$\sigma_i(\alpha) = \alpha_i, \quad i = 1, ..., n. \tag{3.20}$$

Lisäksi usein kiinnitetään

$$\sigma_1 = \mathrm{Id}|_{\mathbb{K}}, \quad \sigma_1(\alpha) = \alpha. \tag{3.21}$$

Määritelmä 17

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

Lause 9

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

$$\sigma(a) = a \quad \forall a \in \mathbb{Q}. \tag{3.22}$$

$$\sigma(a\alpha + b\beta) = a\sigma(\alpha) + b\sigma(\beta), \quad \forall a, b \in \mathbb{Q}, \alpha, \beta \in \mathbb{K}. \tag{3.23}$$

$$\sigma(p(\beta)) = p(\sigma(\beta)) \quad \forall \beta \in \mathbb{K}, \quad p(x) \in \mathbb{Q}[x]. \tag{3.24}$$

Määritelmä 18

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

$$S[\alpha_1, ..., \alpha_m] = \bigcap_{S \cup \{\alpha_1, ..., \alpha_m\} \subseteq V \leqslant R} V, \tag{3.25}$$

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

$$S[\alpha] = \{s_0 + s_1\alpha + s_2\alpha^2 + ... + s_n\alpha^n \mid s_i \in S,\ n \in \mathbb{N}\} \tag{3.26}$$

on yhden muuttujan α polynomirengas.

Määritelmä 19

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

$$\langle K, \alpha_1, ..., \alpha_m \rangle = \bigcap_{K \cup \{\alpha_1, ..., \alpha_m\} \subseteq M \leqslant L} M, \tag{3.27}$$

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

Lause 10

$$\langle K, \alpha_1, ..., \alpha_m \rangle = K(\alpha_1, ..., \alpha_m) := \tag{3.28}$$

$$\left\{ \frac{A}{B} \middle| \ A, B \in K[\alpha_1, ..., \alpha_m], \ B \neq 0 \right\}.$$

Lause 11

$$\langle K, \alpha \rangle = K(\alpha) := \left\{ \frac{A(\alpha)}{B(\alpha)} \middle| \; A(\alpha), B(\alpha) \in K[\alpha], \; B \neq 0 \right\}. \tag{3.29}$$

Lause 12

Jos α on transkendenttinen K:n suhteen, niin

$$K[\alpha] \cong K[x] \tag{3.30}$$

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

$$K(\alpha) \cong K(x) \tag{3.31}$$

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

Määritelmä 20

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

Merkintä 1

$$K\alpha_1 + ... + K\alpha_m := \{k_1\alpha_1 + ... + k_m\alpha_m |\ k_1, ..., k_m \in K\}; \tag{4.1}$$

$$K[\beta]_n := K\beta^0 + K\beta^1 + ... + K\beta^n. \tag{4.2}$$

Välittömästi

$$K[\beta]_n \subseteq K[\beta] = K\beta^0 + K\beta^1 + ... \tag{4.3}$$

Lause 13

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

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

$$K[\beta] = K[\beta]_{s-1} \quad ja \quad \dim_K K[\beta] = s; \quad (4.4)$$

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

$$C. \qquad [L : K] = r < \infty \quad \Rightarrow \quad \deg_K \beta = s | r; \qquad (4.5)$$

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

Lause 14

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

$$A. \qquad \langle K, \alpha \rangle = K[\alpha] = K + K\alpha + \ldots + K\alpha^{n-1}; \tag{4.6}$$

$$B. \qquad [\langle K, \alpha \rangle : K] = \deg_K \alpha = n; \tag{4.7}$$

$$C. \qquad \beta \in \langle K, \alpha \rangle \quad \Rightarrow \quad \deg_K \beta = k | n; \tag{4.8}$$

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

Todistus.
Lause 13 A. "$\Rightarrow$": Olkoon $\deg_K \beta = s$. Osoitetaan aluksi, että

$$K[\beta] = K[\beta]_{s-1} = K\beta^0 + K\beta^1 + \ldots + K\beta^{s-1}. \tag{4.9}$$

Olkoon β:n minimipolynomi

$$M_\beta(x) = b_0 x^0 + \ldots + x^s \in K[x]$$
$$\text{ja} \quad a(\beta) \in K[\beta], \quad a(x) \in K[x]. \tag{4.10}$$

Jakoalgoritmin nojalla

$$a(x) = q(x)M_\beta(x) + r(x), \quad \deg r(x) \leq s-1 \quad \Rightarrow$$
$$a(\beta) = q(\beta)M_\beta(\beta) + r(\beta) = r(\beta) \in K[\beta]_{s-1} \quad \Rightarrow$$
$$K[\beta] \subseteq K[\beta]_{s-1} \quad \Rightarrow \quad K[\beta] = K[\beta]_{s-1}. \quad (4.11)$$

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

$$k_0\beta^0 + k_1\beta^1 + ... + k_{s-1}\beta^{s-1} = 0,$$
$$k_0, ..., k_{s-1} \in K, \ k_i \neq 0, \text{ jollakin } i = 0, ..., s-1 \quad \Rightarrow$$
$$\deg_K \beta \leq s-1. \quad \text{Ristiriita.} \quad \Rightarrow$$
$$\dim_K K[\beta] = \dim_K K[\beta]_{s-1} = s. \quad \square \quad (4.12)$$

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

$$K[\beta]_{s-1} = K\beta^0 + K\beta^1 + ... + K\beta^{s-1}, \tag{4.13}$$

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

$$p(x) \in K[x], \quad 1 \leq \deg p(x) \leq s-1, \quad p(\beta) = 0, \quad \Rightarrow$$

$\{\beta^0, \beta^1, ..., \beta^{s-1}\}$ olisi lin. sidottu. Ristiriita

$$\Rightarrow \quad \deg_K \beta \geq s. \tag{4.14}$$

Toisaalta

$$\beta^s \in K[\beta] = K[\beta]_{s-1} \quad \Rightarrow$$

$$\beta^s = k_0\beta^0 + k_1\beta^1 + ... + k_{s-1}\beta^{s-1} \quad \Rightarrow \deg_K \beta \leq s. \tag{4.15}$$

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

Todistus. Lause 13 C:
B. kohdasta saadaan, että $K[\beta]$ on L:n alikunta. Koska $[L : K] = r < \infty$, niin A. kohdan nojalla

$$\dim_K K[\beta] := s \leq \dim_K L = r \quad \Rightarrow \quad \deg_K \beta = s \leq r. \tag{4.16}$$

Nyt $K \leqslant K[\beta] \leqslant L$ muodostaa kuntatornin. Siten Lauseen 4 nojalla

$$[L : K] = [L : K[\beta]][K[\beta] : K] \quad \Rightarrow \quad r = vs, \quad v = [L : K[\beta]]. \tag{4.17}$$

Niinpä

$$s|r. \quad \square \tag{4.18}$$

Huomautus 1

Lauseen 11 nojalla

$$\langle K, \alpha \rangle = K(\alpha) = \left\{ \frac{A(\alpha)}{B(\alpha)} |\ A(\alpha), B(\alpha) \in K[\alpha],\ B \neq 0 \right\}. \qquad (4.19)$$

mutta Lauseen 14 A. kohdan nojalla algebrallisen luvun määräämässä laajennuskunnassa kaikki α:n rationaalilausekkeet palautuvat α:n polynomilausekkeiksi.

Esimerkki 8

Tarkastellaan kuntalaajennusta

$$\mathbb{L} := \langle \mathbb{Q}, 2^{1/2}, 2^{1/3} \rangle = \langle \langle \mathbb{Q}, 2^{1/2} \rangle, 2^{1/3} \rangle. \tag{4.20}$$

Merkitään

$$\mathbb{M}_2 := \langle \mathbb{Q}, 2^{1/2} \rangle, \quad \mathbb{M}_3 := \langle \mathbb{Q}, 2^{1/3} \rangle. \tag{4.21}$$

Aluksi

$$M_{\alpha_1} = x^2 - 2 = (x - \alpha_1)(x - \alpha_2), \quad \alpha_1 = 2^{1/2},$$
$$M_{\alpha_1} \in J_{\mathbb{Q}[x]}, \quad \deg_{\mathbb{Q}} M_{\alpha_1} = 2,$$
$$\Rightarrow \quad [\mathbb{M}_2 : \mathbb{Q}] = 2; \quad (4.22)$$

$$M_{\beta_1} = x^3 - 2 = (x - \beta_1)(x - \beta_2)(x - \beta_3), \ \beta_1 = 2^{1/3},$$
$$M_{\beta_1} \in J_{\mathbb{Q}[x]}, \quad \deg_{\mathbb{Q}} M_{\beta_1} = \deg_{\mathbb{Q}} M_{\beta_2} = \deg_{\mathbb{Q}} M_{\beta_3} = 3,$$
$$\Rightarrow \quad [\mathbb{M}_3 : \mathbb{Q}] = 3. \quad (4.23)$$

Lauseen 14 C kohdan nojalla

$$\beta_1, \beta_2, \beta_3 \notin \mathbb{M}_2, \quad \alpha_1, \alpha_2 \notin \mathbb{M}_3. \quad (4.24)$$

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

Niinpä

$$[\mathbb{L} : \mathbb{M}_2] = [\langle \mathbb{M}_2, 2^{1/3} \rangle : \langle \mathbb{Q}, 2^{1/2} \rangle] = 3. \tag{4.25}$$

Edelleen Lauseen 4 mukaan

$$[\mathbb{L} : \mathbb{Q}] = [\mathbb{L} : \mathbb{M}_2][\mathbb{M}_2 : \mathbb{Q}] = 6. \tag{4.26}$$

Vastaavasti kuten Lauseen 4 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

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

Siten

$$\langle \mathbb{Q}, 2^{1/2}, 2^{1/3}\rangle = \langle \mathbb{Q}, 2^{1/6}\rangle \tag{4.27}$$

eli

$$\mathbb{Q}(2^{1/2}, 2^{1/3}) = \mathbb{Q}(2^{1/6}). \tag{4.28}$$

Lemma 2

Olkoot

$$[\langle K, \alpha_i \rangle : K] = n_i, \quad i = 1, ..., r. \tag{4.29}$$

Tällöin

$$[\langle K, \alpha_1, ..., \alpha_r \rangle : K] \leq n_1 \cdots n_r. \tag{4.30}$$

Lause 15

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

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 16

$$\mathbb{A} \leqslant \mathbb{C}. \tag{5.1}$$

Seuraus 1

Jos $\alpha, \beta \in \mathbb{A}$, *niin*

$$\alpha \pm \beta,\ \alpha\beta,\ \alpha/\beta \in \mathbb{A}. \tag{5.2}$$

Algebran peruslauseen **??** 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 17

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

$$a(x) \in \mathbb{A}[x] \setminus \{0(x)\}, \quad a(\omega) = 0 \quad \Rightarrow \quad \omega \in \mathbb{A}. \tag{5.3}$$

Lause 18

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

$$\mathbb{K} = \mathbb{Q}(\tau). \tag{6.1}$$

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

$$\mathbb{K} = \mathbb{Q}(\alpha, \beta) \tag{6.2}$$

ja osoitetaan, että

$$\mathbb{K} = \mathbb{Q}(\alpha + c\beta), \quad \text{jollakin} \quad c \in \mathbb{Q}. \tag{6.3}$$

Olkoot

$$M_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in \mathbb{Q}[x];$$
$$M_\beta(x) = (x - \beta_1) \cdots (x - \beta_m) \in \mathbb{Q}[x]. \tag{6.4}$$

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

$$\gamma := \alpha + c\beta \neq \alpha_i + c\beta_j, \quad \forall (i, j) \neq (1, 1). \tag{6.5}$$

a). Välittömästi

$$\gamma := \alpha + c\beta \in \mathbb{Q}(\alpha, \beta) \quad \Rightarrow \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha, \beta). \tag{6.6}$$

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

$$\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\gamma). \tag{6.7}$$

Tarkastellaan polynomeja

$$\begin{aligned} r(x) = M_\alpha(\gamma - cx) \in \mathbb{Q}(\gamma)[x], \quad \deg r(x) = n, \\ r(\beta) = M_\alpha(\gamma - c\beta) = M_\alpha(\alpha) = 0; \\ M_\beta(\beta) = 0, \quad M_\beta(x) \in \mathbb{Q}[x], \end{aligned} \tag{6.8}$$

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

Asetetaan nyt

$$r(\tau) = M_\beta(\tau) = 0 \quad \Rightarrow \quad \tau = \beta_k;$$
$$0 = r(\tau) = M_\alpha(\gamma - c\tau) \quad \Rightarrow \quad \gamma - c\tau = \alpha_h$$
$$\Rightarrow \quad \gamma = \alpha_h + c\tau = \alpha_h + c\beta_k$$
$$\Rightarrow \quad \gamma = \alpha + c\beta \Rightarrow \quad \tau = \beta. \quad (6.9)$$

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

$$d(x) = s.y.t(r(x), M_\beta(x)) \in \mathbb{Q}(\gamma)[x]. \quad (6.10)$$

Jos olisi

$$\deg d(x) \geq 2 \quad \Rightarrow$$
$$d(x) = (x - \beta)(x - \kappa)q(x), \quad \beta, \kappa \in \mathbb{C} \quad \Rightarrow$$
$$r(\kappa) = M_\beta(\kappa) = 0 \quad \Rightarrow \quad \kappa = \beta \quad \Rightarrow$$
$$(x - \beta)^2 \underset{\mathbb{C}[x]}{\|} M_\beta(x) \quad (6.11)$$

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

$$d(x) = (x - \beta) \in \mathbb{Q}(\gamma)[x] \quad \Rightarrow$$
$$\beta \in \mathbb{Q}(\gamma) \quad \Rightarrow \quad \alpha = \gamma - c\beta \in \mathbb{Q}(\gamma) \quad \Rightarrow$$
$$\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\gamma). \quad \square \qquad (6.12)$$

Esimerkki 9

$$\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i - \sqrt{2}). \qquad (6.13)$$

Conjugates, field polynomial

Lause 19

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

$$\sigma_i : \mathbb{K} \to \mathbb{C}, \quad i = 1, ..., m. \tag{6.14}$$

Huomautus 2

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

Esimerkki 10

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

$$\sigma_2(2^{1/3}), \sigma_3(2^{1/3}) \notin \mathbb{K}. \tag{6.15}$$

Field polynomial

Määritelmä 21

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

$$K_\beta(x) = \prod_{i=1}^{m}(x - \sigma_i(\beta)), \tag{6.16}$$

missä luvut

$$\sigma_i(\beta) \in \mathbb{C} \tag{6.17}$$

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

Lause 20

$$K_\beta(x) \in \mathbb{Q}[x]. \tag{6.18}$$

Todistus: Symmetristen polynomien peruslauseeseen nojautuen. Kerrataan vielä, että Määritelmän 15 mukaan algebrallisen luvun β liittoluvut eli konjugaatit ovat minimipolynomin $M_\beta(x) \in \mathbb{Q}[x]$ nollakohdat

$$\beta_1, ..., \beta_{\boldsymbol{d}} \in \mathbb{C}. \tag{6.19}$$

Seuraavassa

$$\deg K_\beta(x) = m, \quad \deg M_\beta(x) = d. \tag{6.20}$$

Lause 21

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

$$M_\beta(x) \underset{\mathbb{Q}[x]}{\mid} K_\beta(x); \tag{6.21}$$

$$K_\beta(x) = M_\beta(x)^{m/d}, \quad m/d \in \mathbb{Z}^+. \tag{6.22}$$

Seuraus 2

$$\{\sigma_1(\beta), ..., \sigma_m(\beta)\} = \{\beta_1, ..., \beta_d\}; \tag{6.23}$$

$$\beta \in \mathbb{Q} \quad \Leftrightarrow \quad \sigma_1(\beta) = ... = \sigma_m(\beta); \tag{6.24}$$

$$\mathbb{Q}(\beta) = \mathbb{K} \quad \Leftrightarrow \quad \sigma_i(\beta) \neq \sigma_j(\beta) \quad \forall\ i \neq j. \tag{6.25}$$

Määritelmä 22

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

$$\Delta(\gamma_1, ..., \gamma_m) = (\det(\sigma_i(\gamma_j))_{i=1,...,m,j=1,...,m})^2 = \tag{6.26}$$

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

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

$$\delta(\beta) = \Delta(1, \beta, ..., \beta^{m-1}) = \tag{6.27}$$

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

Lause 22

$$\Delta(\gamma_1, ..., \gamma_m) \in \mathbb{Q}. \tag{6.28}$$

Lause 23

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

$$\dim_{\mathbb{Q}} \mathbb{Q}(\gamma_1, ..., \gamma_m) = m \quad \Leftrightarrow \quad \Delta(\gamma_1, ..., \gamma_m) \neq 0. \tag{6.29}$$

Lause 24

$$\delta(\beta) = \prod_{i<j} (\sigma_i(\beta) - \sigma_j(\beta))^2; \tag{6.30}$$

$$\delta(\beta) \neq 0 \quad \Leftrightarrow \quad \deg_{\mathbb{Q}}(\beta) = m; \tag{6.31}$$

$$\delta(\beta) \neq 0 \quad \Leftrightarrow \quad \mathbb{Q}(\beta) = \mathbb{K}. \tag{6.32}$$

Norm and trace

Määritelmä 23

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

$$N(\beta) = N_{\mathbb{K}}(\beta) = \prod_{i=1}^{m} \sigma_i(\beta) \tag{6.33}$$

ja jälki/trace

$$T(\beta) = T_{\mathbb{K}}(\beta) = \sum_{i=1}^{m} \sigma_i(\beta). \tag{6.34}$$

Lause 25

$$N_{\mathbb{K}}(\beta), \quad T_{\mathbb{K}}(\beta) \in \mathbb{Q}. \tag{6.35}$$

$$N_{\mathbb{K}}(\beta) \neq 0 \quad \Leftrightarrow \quad \beta \neq 0. \tag{6.36}$$

Todistus. (6.35):

$$K_\beta(x) = x^m - T(\beta)x^{m-1} + \ldots + (-1)^m N(\beta) \in \mathbb{Q}[x]. \tag{6.37}$$

(6.36): Koska σ_i on injektio, niin

$$\sigma_i(x) = 0 \quad \Leftrightarrow \quad x = 0. \quad \square \tag{6.38}$$

Lause 26

$$N(\alpha\beta) = N(\alpha)N(\beta) \tag{6.39}$$

$$T(r\alpha + s\beta) = rT(\alpha) + sT(\beta); \tag{6.40}$$

$$N(r) = r^m, \quad T(r) = mr; \tag{6.41}$$

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

Esimerkki 11

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

$$3^{1/2} \notin \mathbb{K} = \mathbb{Q}(2^{1/2}) = \mathbb{Q}[2^{1/2}]. \tag{6.42}$$

Huomaa, että

$$[\mathbb{Q}(2^{1/2}) : \mathbb{Q}] = [\mathbb{Q}(3^{1/2}) : \mathbb{Q}] = 2. \tag{6.43}$$

Tehdään vastaoletus

$$3^{1/2} \in \mathbb{Q}[2^{1/2}] = \mathbb{Q} + 2^{1/2}\mathbb{Q} \tag{6.44}$$

eli

$$3^{1/2} = a + b2^{1/2}, \quad a, b \in \mathbb{Q}. \tag{6.45}$$

Otetaan jälki

$$T_{\mathbb{K}}(3^{1/2}) = T_{\mathbb{K}}(a) + T_{\mathbb{K}}(b2^{1/2}) = 2a + bT_{\mathbb{K}}(2^{1/2}). \tag{6.46}$$

Toisaalta/On the other hand. Tuloksen (6.22) 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

$$x^2 - 2 = x^2 - T_{\mathbb{K}}(2^{1/2})x + N_{\mathbb{K}}(2^{1/2});$$
$$x^2 - 3 = x^2 - T_{\mathbb{K}}(3^{1/2})x + N_{\mathbb{K}}(3^{1/2}), \quad (6.47)$$

josta

$$T_{\mathbb{K}}(2^{1/2}) = T_{\mathbb{K}}(3^{1/2}) = 0. \quad (6.48)$$

Sijoittamalla yhtälöön (6.46) saadaan

$$a = 0 \quad \Rightarrow \quad 3^{1/2} = b2^{1/2}, \quad b \in \mathbb{Q}$$
$$\Rightarrow \quad (3/2)^{1/2} = b \quad \Rightarrow$$
$$T_{\mathbb{K}}((3/2)^{1/2}) = 2b. \quad (6.49)$$

Toisaalta

$$K_{(3/2)^{1/2}}(x) = x^2 - T_{\mathbb{K}}((3/2)^{1/2})x + N_{\mathbb{K}}((3/2)^{1/2});$$
$$M_{(3/2)^{1/2}}(x) = x^2 - 3/2 \quad \Rightarrow$$
$$T_{\mathbb{K}}((3/2)^{1/2}) = 0 \quad \Rightarrow \quad b = 0$$
$$\Rightarrow \quad 3^{1/2} = 0. \quad (6.50)$$

Ristiriita. □

Lause 27

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*

$$\Delta(1, \tau, ..., \tau^{m-1}) = (-1)^{m(m-1)/2} N(DM_\tau(\tau)). \tag{6.51}$$

Lause 28

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

$$\Delta(\gamma_1, ..., \gamma_m) = \det(T(\gamma_i \gamma_j)). \tag{6.52}$$

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 29

$$\mathbb{B} \leqslant \mathbb{A}. \tag{7.1}$$

Seuraus 3

Jos $\alpha, \beta \in \mathbb{B}$, *niin*

$$\alpha \pm \beta, \ \alpha\beta \ \in \mathbb{B}. \tag{7.2}$$

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

Lause 30

Olkoon

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

$$b(\omega) = 0 \quad \Rightarrow \quad \omega \in \mathbb{B}. \tag{7.3}$$

Esimerkki 12

$$\alpha^2 = \alpha + 1, \quad \beta^5 + \alpha\beta^2 + 5 = 0 \tag{7.4}$$

$$\omega^2 - \beta = 0 \quad \Rightarrow \quad \omega \in \mathbb{B}. \tag{7.5}$$

Lause 31

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

$$d\alpha \in \mathbb{B}. \tag{7.6}$$

Määritelmä 24

Lauseen 31 mukainen luku $d \in \mathbb{Z}^+$ *on algebrallisen luvun* α *nimittäjä eli* $\text{den}\ \alpha = d$.

Esimerkki 13

Olkoon

$$5\alpha^2 + \alpha + 1 = 0, \quad \Rightarrow \quad (5\alpha)^2 + 5\alpha + 5 = 0 \quad \Rightarrow \tag{7.7}$$

$$5\alpha \in \mathbb{B}, \quad \text{den}\ \alpha = 5. \tag{7.8}$$

Määritelmä 25

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

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{K} \cap \mathbb{B} \tag{7.9}$$

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

Esimerkki 14

$$\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}. \tag{7.10}$$

Esimerkki 15

$$2^{1/7} \notin \mathbb{Q}. \tag{7.11}$$

Vastaoletus

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

$$\textit{Lisäksi} \quad 1 < 2^{1/7} < 2. \quad \textit{Ristiriita.} \quad \square \tag{7.12}$$

Esimerkki 16

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

$$2^{1/n} + 3^{1/n} \notin \mathbb{Q}. \tag{7.13}$$

Rationaaliset kokonaisluvut muodostavat alirenkaan kokonaisten algebrallisten lukujen renkaille.

Lause 32

$$\mathbb{Z} \leqslant \mathbb{Z}_{\mathbb{K}} \leqslant \mathbb{B}. \tag{7.14}$$

Edelleen

Lause 33

Olkoon $\beta \in \mathbb{Z}_{\mathbb{K}}$, *tällöin*

$$\mathbb{Z}[\beta] \leqslant \mathbb{Z}_{\mathbb{K}}. \tag{7.15}$$

Huomautus 3

Usein pätee kuitenkin

$$\mathbb{Z}_{\mathbb{K}} \neq \mathbb{Z}[\beta]. \tag{7.16}$$

Esimerkki 17

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

$$\frac{1+\sqrt{5}}{2} \in \mathbb{Z}_{\mathbb{K}}, \quad \frac{1+\sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}]. \tag{7.17}$$

Lause 34

Ei vaadita. Olkoon $\mathbb{K}$ lukukunta. Tällöin

$$\mathbb{K} = \mathbb{Q}(\lambda), \quad \lambda \in \mathbb{Z}_{\mathbb{K}}. \tag{7.18}$$

Lause 35

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

$$\Delta(\lambda_1, ..., \lambda_m) \in \mathbb{Z} \setminus \{0\}. \tag{7.19}$$

Lause 36

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 37

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 26

Lauseen 37 mukainen $\mathbb{Z}_{\mathbb{K}}$:n kanta $\mathbb{Z}$:n yli on kunnan $\mathbb{K}$ kokonaislukujen kanta.

Lause 38

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 18

$$\Delta\left(1, \frac{1+\sqrt{5}}{2}\right) = 5 \quad \Rightarrow \quad \left\{1, \frac{1+\sqrt{5}}{2}\right\} \tag{7.20}$$

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

Lause 39

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

$$N_{\mathbb{K}}(\beta), \quad T_{\mathbb{K}}(\beta) \in \mathbb{Z}; \tag{8.1}$$

$$N_{\mathbb{K}}(\beta) \neq 0 \quad \Leftrightarrow \quad \beta \neq 0. \tag{8.2}$$

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

Lause 40

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

$$a \underset{\mathbb{Z}_{\mathbb{K}}}{\mid} b \quad \Rightarrow \quad N(a) \underset{\mathbb{Z}}{\mid} N(b); \tag{8.3}$$

$$a \in \mathbb{Z}_{\mathbb{K}}^* \quad \Leftrightarrow \quad N(a) = \pm 1; \tag{8.4}$$

$$a \sim b \quad \Rightarrow \quad N(a) = \pm N(b); \tag{8.5}$$

$$|N(a)| \in \mathbb{P} \quad \Rightarrow \quad a \in J_{\mathbb{Z}_{\mathbb{K}}}. \tag{8.6}$$

Todistus.

8.3: Olkoon

$$b = ca, \quad a, b, c \in \mathbb{Z}_{\mathbb{K}} \tag{8.7}$$

Koska σ_i on homomorfia, niin

$$\sigma_i(b) = \sigma_i(c)\sigma_i(a) \quad \forall\ i = 1, ..., m \quad \Rightarrow \tag{8.8}$$

$$N(b) = \prod_{i=1}^{m} \sigma_i(b) = \prod_{i=1}^{m} \sigma_i(c) \prod_{i=1}^{m} \sigma_i(a) = N(c)N(a), \tag{8.9}$$

missä

$$N(b), N(c), N(a) \in \mathbb{Z} \quad \Rightarrow \quad N(a) \underset{\mathbb{Z}}{|} N(b). \quad \square \tag{8.10}$$

8.4: Olkoon ensin

$$a \in \mathbb{Z}_{\mathbb{K}}^* \quad \Rightarrow \quad a \underset{\mathbb{Z}_{\mathbb{K}}}{\mid} 1. \tag{8.11}$$

Kohdan (8.3) nojalla saadaan

$$N(a) \underset{\mathbb{Z}}{\mid} N(1) = 1 \quad \Rightarrow \quad N(a) = \pm 1. \tag{8.12}$$

Olkoon sitten

$$N(a) = \pm 1. \tag{8.13}$$

Siten

$$a\sigma_2(a) \cdots \sigma_m(a) = \pm 1, \quad \Rightarrow \quad c = \sigma_2(a) \cdots \sigma_m(a) \in \mathbb{K}. \tag{8.14}$$

Toisaalta, koska

$$a \in \mathbb{Z}_{\mathbb{K}} \subseteq \mathbb{B} \quad \Rightarrow \quad \sigma_2(a), \ldots, \sigma_m(a) \in \mathbb{B} \quad \Rightarrow \quad c \in \mathbb{B}. \tag{8.15}$$

Siispä

$$c \in \mathbb{K} \cap \mathbb{B} = \mathbb{Z}_{\mathbb{K}}, \quad \pm c \cdot a = 1 \quad \Rightarrow \tag{8.16}$$

$$a \underset{\mathbb{Z}_{\mathbb{K}}}{\mid} 1 \quad \Rightarrow \quad a \in \mathbb{Z}_{\mathbb{K}}^*. \tag{8.17}$$

Kohta (8.4) todistettu. □

Huomaa, että vaikka $a \in \mathbb{Z}_{\mathbb{K}}$, niin voi olla $\sigma_i(a) \notin \mathbb{Z}_{\mathbb{K}}$, vertaa Esimerkki 10. Kuitenkin $\sigma_i(a) \in \mathbb{B}$.

8.5: Nyt

$$b = ua, \quad u \in \mathbb{Z}_{\mathbb{K}}^* \quad \Rightarrow \quad N(u) = \pm 1 \quad \Rightarrow \tag{8.18}$$

$$N(b) = N(u)N(a) = \pm N(a). \quad \square \tag{8.19}$$

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

$$a = bc, \quad b, c \notin \mathbb{Z}_{\mathbb{K}}^*, \ b, c \neq 0, \quad \Rightarrow \tag{8.20}$$

$$|N(b)|, |N(c)| \geq 2 \quad \Rightarrow \quad |N(a)| = |N(b)||N(c)| \notin \mathbb{P}. \tag{8.21}$$

Ristiriita. $\square$

Lause 41

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

$$ab = c^k, \quad a \perp b. \tag{8.22}$$

Tällöin

$$a \sim d^k, \quad b \sim e^k, \tag{8.23}$$

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

Algebrallisten lukujen tutkimisen päämotiivi on alkujaan ollut Diofantoksen yhtälöiden ratkaiseminen.

Esimerkki 19

$$y^2 + 2 = x^3, \quad 2 \not| y, \tag{9.1}$$

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

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

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3. \tag{9.2}$$

II. Kokonaislukujen rengas on

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\sqrt{-2}. \tag{9.3}$$

III. Sen yksikköryhmä on

$$\mathbb{Z}_{\mathbb{K}}^{*} = \{\pm 1\}. \tag{9.4}$$

IV. Kokonaisalue

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\sqrt{-2}. \tag{9.5}$$

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

V. Olkoon

$$D = syt(y - \sqrt{-2}, y + \sqrt{-2}),$$

$$D = a + b\sqrt{-2} \in \mathbb{Z}_{\mathbb{K}} \quad \Rightarrow \quad (9.6)$$

$$D \underset{\mathbb{Z}_{\mathbb{K}}}{\mid} 2y, \quad D \underset{\mathbb{Z}_{\mathbb{K}}}{\mid} 2\sqrt{-2} \quad \Rightarrow \quad (9.7)$$

$$N(D) \underset{\mathbb{Z}}{\mid} N(2y), \quad N(D) \underset{\mathbb{Z}}{\mid} N(2\sqrt{-2}),$$

$$N(D) = (a + b\sqrt{-2})(a - b\sqrt{-2}) = a^2 + 2b^2 \quad \Rightarrow \quad (9.8)$$

$$a^2 + 2b^2 \underset{\mathbb{Z}}{\mid} 4y^2, \quad a^2 + 2b^2 \underset{\mathbb{Z}}{\mid} -8 \quad \Rightarrow \quad (9.9)$$

$$D = \pm 1, \pm 2, \pm\sqrt{-2}. \quad (9.10)$$

Jos esimerkiksi

$$\sqrt{-2} \underset{\mathbb{Z}_{\mathbb{K}}}{\mid} y - \sqrt{-2} \quad \Rightarrow$$

$$y - \sqrt{-2} = \sqrt{-2}(e + f\sqrt{-2}), \quad e, f \in \mathbb{Z} \quad \Rightarrow$$

$$2f = -y, \quad \text{Ei käy.} \tag{9.11}$$

Vastaavasti päätellään, että vain

$$D = \pm 1 \underset{\mathbb{Z}_{\mathbb{K}}}{\mid} y - \sqrt{-2}, y + \sqrt{-2}, \quad \Rightarrow \tag{9.12}$$

$$y - \sqrt{-2} \ \perp \ y + \sqrt{-2}, \quad \Rightarrow \tag{9.13}$$

$$y + \sqrt{-2} = (c + d\sqrt{-2})^3, \quad c + d\sqrt{-2} \in \mathbb{Z}_{\mathbb{K}}, \quad c, d \in \mathbb{Z}$$

$$\Rightarrow \quad 1 = d(3c^2 - 2d) \quad \Rightarrow \quad d = \pm 1, \quad d = 1, c = \pm 1;$$

$$y = c^3 - 6cd^2 \quad \Rightarrow \quad y = \pm 5$$

$$\Rightarrow \quad x = 3, \ y = \pm 5. \ \square \tag{9.14}$$

Jokainen neliökunta on esitettävissä muodossa

$$\mathbb{K} = \mathbb{Q}(\sqrt{d}), \quad d \in \mathbb{Z}, \tag{10.1}$$

missä d on neliövapaa tästä eteenpäin.

Lause 42

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

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\lambda, \tag{10.2}$$

missä

$$\lambda = \sqrt{d}, \quad d \equiv 2,\ 3 \pmod 4; \tag{10.3}$$

$$\lambda = \frac{1+\sqrt{d}}{2}, \quad d \equiv 1 \pmod 4; \tag{10.4}$$

$$\Delta = 4d, \quad d \equiv 2,\ 3 \pmod 4; \tag{10.5}$$

$$\Delta = d, \quad d \equiv 1 \pmod 4. \tag{10.6}$$

Todistus. Tarkastellaan kokonaislukua

$$\beta = r + s\sqrt{d} \in \mathbb{Z}_{\mathbb{K}}, \quad r, s \in \mathbb{Q} \quad \Rightarrow$$

$$T(\beta) = 2r \in \mathbb{Z} \quad \Rightarrow \quad r \in \frac{1}{2}\mathbb{Z} \quad \Rightarrow \quad r = \frac{a}{2},\ a \in \mathbb{Z};$$

$$N(\beta) = r^2 - ds^2 \in \mathbb{Z} \quad \Rightarrow \quad d(2s)^2 = (2r)^2 - 4N(\beta) \in \mathbb{Z},$$

$$\text{missä} \quad 2s = \frac{k}{l}, \quad k \perp l, \quad \Rightarrow$$

$$d(2s)^2 = \frac{dk^2}{l^2} \in \mathbb{Z}, \quad \text{missä d on neliövapaa} \quad \Rightarrow \quad l = 1,$$

$$\Rightarrow \quad 2s \in \mathbb{Z} \quad \Rightarrow \quad s = \frac{b}{2},\ b \in \mathbb{Z}. \quad (10.7)$$

Siten

$$\beta = \frac{a + b\sqrt{d}}{2}, \quad a, b \in \mathbb{Z}. \quad (10.8)$$

Tutkitaan sitten mitä arvoja luvut a ja b saavat.
Tapaus 10.3 eli $d \equiv 2,\ 3 \pmod 4$:
Koska

$$N(\beta) = \frac{a^2 - db^2}{4} \in \mathbb{Z} \quad \Rightarrow$$

$$a^2 - db^2 \equiv 0 \pmod 4 \quad \Rightarrow$$

$$a \equiv b \equiv 0 \pmod 2 \quad \Rightarrow$$

$$\beta = \frac{a + b\sqrt{d}}{2} = A + B\sqrt{d}, \quad A, B \in \mathbb{Z}. \quad (10.9)$$

Tapaus 10.4 eli $d \equiv 1 \pmod 4$:
Koska

$$N(\beta) = \frac{a^2 - db^2}{4} \in \mathbb{Z} \quad \Rightarrow$$

$$a^2 \equiv b^2 \pmod 4 \quad \Rightarrow$$

$$a \equiv b \equiv 0 \pmod 2 \quad \text{tai} \quad a \equiv b \equiv 1 \pmod 2 \quad \Rightarrow \quad (10.10)$$

$$\beta = \frac{a + b\sqrt{d}}{2}, \quad a \equiv b \pmod 2, \ a, b \in \mathbb{Z}$$

$$\Rightarrow \quad \beta = A + B\frac{1 + \sqrt{d}}{2}, \quad A, B \in \mathbb{Z}. \quad \square \quad (10.11)$$

Yksikköryhmä

Seuraavassa

$$\omega = e^{\frac{2\pi}{3}i}. \tag{10.12}$$

Lause 43

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

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1, \pm i\}, \quad d = -1; \tag{10.13}$$

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1\}, \quad d = -2; \tag{10.14}$$

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1, \pm\omega, \pm\omega^2\}, \quad d = -3; \tag{10.15}$$

$$\mathbb{Z}_{\mathbb{K}}^* = \{\pm 1\}, \quad d \in \mathbb{Z}_{\leq -5}. \tag{10.16}$$

Esimerkiksi tapaus: $d = -5 \equiv 3 \pmod 4$, joten kokonaisluvut muotoa

$$\beta = A + B\sqrt{-5}, \quad A, B \in \mathbb{Z} \quad \Rightarrow$$
$$N(\beta) = A^2 + 5B^2 = 1 \quad \Rightarrow \quad A = \pm 1,\ B = 0 \quad \Rightarrow$$
$$\mathbb{Z}^*_{\mathbb{Q}(\sqrt{-5})} = \{\pm 1\}. \quad (10.17)$$

UFD/Eukleideen alue

Lause 44

Olkoon $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, *tällöin* $\mathbb{Z}_{\mathbb{K}}$ *on UFD, kun*

$$d = -1, -2, -3, -7, -11, \tag{10.18}$$

jotka ovat imaginaariset Eukleideen alueet ja lisäksi, kun

$$d = -19, -43, -67, -163. \tag{10.19}$$

Tässä kaikki, kun $d \leq -1$.

UFD/Eukleideen alue

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

$$\frac{a}{b} = x + iy, \quad x, y \in \mathbb{Q}. \tag{10.20}$$

Valitaan sellaiset $s, t \in \mathbb{Z}$, että

$$|x - s| \leq \frac{1}{2}, \quad |y - t| \leq \frac{1}{2}. \tag{10.21}$$

Olkoon

$$q = s + it, \quad a = qb + r, \quad r \in \mathbb{Z}[i]. \tag{10.22}$$

UFD/Eukleideen alue

Ottamalla normit saadaan

$$N(r) = N(b)N(x - s + i(y - t)) = N(b)((x - s)^2 + (y - t)^2) \quad (10.23)$$

$$\leq N(b)\frac{1}{2} \quad \Rightarrow \quad N(r) < N(b) \quad (10.24)$$

ja lisäksi

$$N : \ \mathbb{Z}[i] \to \mathbb{N}, \quad (10.25)$$

joten N on Eukleideen funktio. Edelleen, Lauseen **??** nojalla Eukleideen alue on aina UFD. □

Gaussin kokonaisluvut/alkuluvut

Määritelmä 27

Kunnan $\mathbb{K} = \mathbb{Q}(i)$, kokonaislukujen renkaan

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{Z}[i] \tag{10.26}$$

alkioita sanotaan Gaussin kokonaisluvuiksi. Edelleen jaottomat Gaussin kokonaisluvut ovat Gaussin alkulukuja.

Koska $\mathbb{Z}[i]$ on UFD, niin sen jaottomat alkiot ovat alkualkioita eli

$$P_{\mathbb{Z}[i]} = J_{\mathbb{Z}[i]}. \tag{10.27}$$

Gaussin kokonaisluvut/alkuluvut

Lause 45

$$\pi = a + ib \in P_{\mathbb{Z}[i]} \quad \Leftrightarrow \tag{10.28}$$

$$\pi \sim 1 + i; \tag{10.29}$$

$$\pi \sim a + ib, \quad a^2 + b^2 = p \in \mathbb{P}, \quad p \equiv 1 \pmod 4; \tag{10.30}$$

$$\pi \sim p \in \mathbb{P}, \quad p \equiv 3 \pmod 4. \tag{10.31}$$

Yksikköryhmä

Reaalisen neliökunnan yksikköryhmät ovat äärettömiä ja yleisessä tapauksessa varsin hankalasti määrättävissä. Niiden määräämiseen tarvitaan tietoa Pellin yhtälöiden ratkaisemisesta.

Lause 46

Olkoon $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}_{\geq 2}$. *Tällöin*

$$\mathbb{Z}_{\mathbb{K}}^* = \{x_k + y_k\sqrt{d} |\ x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k,\ k \in \mathbb{Z}\}, \tag{10.32}$$

missä $(x_1, y_1) \in \mathbb{Z}^2$ *on pienin positiivinen Pellin yhtälön*

$$x^2 - dy^2 = 1 \tag{10.33}$$

ratkaisu.

Kyseessä oleva pienin ratkaisu voidaan etsiä käyttäen ketjumurtolukujen teoriaa, katso kurssi: Ketjumurtoluvut.

UFD/Eukleideen alue

Lause 47

Olkoon $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, *tällöin* $\mathbb{Z}_{\mathbb{K}}$ *on UFD, kun*

$$d = 2, 3, 5, 6, 7, 13, 17, 21, 29, 33, 37, 41, 57, 73, \tag{10.34}$$

jotka ovat reaaliset Eukleideen alueet ja lisäksi, kun

$$d = 11, 14, 19, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67,$$

$$69, 71, 77, 83, 86, 89, 93, 94, 97. \tag{10.35}$$

Tässä vain kaikki, missä $2 \leq d \leq 100$.