universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Ganzheitsbasen von kubischen und biquadratischen Zahlkörpern“

verfasst von / submitted by

Daniel Klocker, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2018 / Vienna 2018

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 066 821
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Mathematik
Betreut von / Supervisor:	ao. Univ.-Prof. Mag. Dr. Christoph Baxa

Zusammenfassung

Diese Masterarbeit behandelt eine Problemstellung der algebraischen Zahlentheorie. Thema der Arbeit sind Ganzheitsbasen und die Diskriminanten von kubischen und biquadratischen Zahlkörpern. Es werden p-ganze Basen für alle Primzahlen p für kubische und biquadratische Zahlkörper angeführt. Aus diesen p-ganzen Basen werden Ganzheitsbasen gebildet und die Diskriminanten berechnet.

Abstract

This master thesis deals with a problem of algebraic number theory. It is devoted to integral bases and the discriminants of cubic and biquadratic number fields. For every prime p it provides p-bases of cubic and biquadratic fields. Integral bases are created from the p-bases and the discriminants calculated.

Danksagung

Ich bedanke mich bei ao. Univ.-Prof. Mag. Dr. Christoph Baxa für die Betreuung dieser Masterarbeit. Des Weiteren gilt mein Dank meiner Familie, die mich immer unterstützt.

Inhaltsverzeichnis

1 Einleitung

Die vorliegende Arbeit behandelt eine Problemstellung der algebraischen Zahlentheorie. Thema der Arbeit sind Ganzheitsbasen und die Diskriminanten von kubischen und biquadratischen Zahlkörpern. Sei in diesen einleitenden Worten K ein algebraischer Zahlkörper. Sei zudem $\omega_0, \omega_1, \ldots, \omega_{[K:\mathbb{Q}]-1} \in O_K$, $\left(\omega_0, \omega_1, \ldots, \omega_{[K:\mathbb{Q}]-1}\right)$ eine Basis von K über $\mathbb{Q}$, $\theta \in \mathbb{C}$, θ algebraisch über $\mathbb{Q}$, $r \in \mathbb{Z}$, $s \in \mathbb{Z}$, $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$ und $(r \not\equiv 0 \pmod{p^2}$ oder $s \not\equiv 0 \pmod{p^3})$ für alle Primzahlen p. Sei des Weiteren $m, n \in \mathbb{Z}$, m quadratfrei, n quadratfrei, $m \neq n$ und einer der folgenden drei Punkte erfüllt:

1. $m \equiv n \equiv 1 \pmod{4}$
2. $m \equiv 2 \pmod{4}$ und $n \equiv 1 \pmod{2}$
3. $m \equiv n \equiv 3 \pmod{4}$

In dieser Masterarbeit wird eine Ganzheitsbasis und die Diskriminante des kubischen Zahlkörpers $\mathbb{Q}(\theta)$ angeführt[1]. Alle kubischen Zahlkörper sind in dieser Form darstellbar[2]. Es wird zudem eine Ganzheitsbasis und die Diskriminante des biquadratischen Zahlkörpers $\mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ angeführt[3]. Alle biquadratischen Zahlkörper sind in dieser Form darstellbar[4].

Die vorliegende Arbeit stützt sich auf die Doktorarbeit von Alaca [1]. In [1] wird eine Methode präsentiert, um Ganzheitsbasen zu berechnen. Es wird für alle Primzahlen p eine p-ganze Basis gefunden und eine Ganzheitsbasis aus den p-ganzen Basen gebildet. In der vorliegenden Arbeit wird auch so vorgegangen.

In der Arbeit von Williams [4] führt Williams eine Basis für den biquadratischen Zahlkörper $\mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ an und beweist diese. Die vorliegende Arbeit geht jedoch einen anderen Weg und wendet die Theorie von Alaca in [1] an. In [1] wird von einem primitiven Element μ und der Basis $\left(1, \mu, \mu^2, \ldots, \mu^{[K:\mathbb{Q}]-1}\right)$ von K über $\mathbb{Q}$ ausgegangen. Dies wäre für den biquadratischen Zahlkörper $\mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ und die Basis

$$\left(1, \sqrt{m} + \sqrt{n}, \left(\sqrt{m} + \sqrt{n}\right)^2, \left(\sqrt{m} + \sqrt{n}\right)^3\right)$$

von $\mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ über $\mathbb{Q}$ möglich. In dieser Arbeit wird jedoch versucht, die Methode in [1] auf den biquadratischen Zahlkörper $\mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ und die Basis $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ von $\mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ über $\mathbb{Q}$ anzuwenden. Um dies zu ermöglichen, wird die Theorie etwas

[1] Siehe Satz 5.5.1 und Satz 5.6.8.
[2] Siehe Satz 5.1.6.
[3] Siehe Satz 6.4.1 und Satz 6.5.2.
[4] Siehe Satz 6.1.5.

allgemeiner für eine Basis von K über $\mathbb{Q}$, deren Elemente in O_K sind, formuliert[5]. Der zentrale Satz 1.3.4 in [1] lässt sich mit zusätzlich geforderten Bedingungen auch bezüglich einer Basis von K über $\mathbb{Q}$, deren Elemente in O_K sind, formulieren. Dies geschieht in dem Satz 4.0.5. Dieser Satz liefert ein Werkzeug, um eine p-ganze Basis von K für eine Primzahl p finden zu können. Er zeigt, dass es unter gewissen Voraussetzungen ausreichend ist, für alle $k \in \{0, 1, \ldots, [K : \mathbb{Q}] - 1\}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad k bezüglich $\left(\omega_0, \omega_1, \ldots, \omega_{[K:\mathbb{Q}]-1}\right)$ zu suchen[6] und diese Elemente von K bereits eine p-ganze Basis bilden. Des Weiteren hilft der Satz 4.0.5 die Potenzen der Primfaktoren von der Diskriminante eines algebraischen Zahlkörpers zu bestimmen. Der Satz 4.0.9 erlaubt es, aus geeigneten p-ganzen Basen eine Ganzheitsbasis zu bilden.

Im Kapitel 5 werden kubische Zahlkörper betrachtet. Dieses Kapitel folgt zum Teil der Doktorarbeit von Alaca [1]. Die erhaltenen p-ganzen Basen stimmen für alle Primzahlen p mit den p-ganzen Basen aus den Sätzen 2.2.1, 2.3.1 und 2.4.1 in [1] überein. Die Ganzheitsbasen unterscheiden sich nur in einem Fall geringfügig von den Ganzheitsbasen in Satz 2.6.1 in [1]. Zur Berechnung der p-ganzen Basen werden etwas andere Fallunterscheidungen getroffen. Dies führt zum Teil zu anderen Rechnungen.

Im Kapitel 6 werden biquadratische Zahlkörper betrachtet. Wie in der Arbeit von Williams [4] wird von gegebenen m und n von obiger Gestalt ausgegangen. Trotz unterschiedlicher Herangehensweisen ergeben sich, bis auf einen Fall, dieselben Ganzheitsbasen wie in dem Satz 2 in [4].

Es folgt in diesem Kapitel 1 zuerst eine Auswahl an Notationen und Definitionen, die in dieser Arbeit verwendet werden, und dann einige grundlegende Sätze. Einige Beweise dieser Sätze sind in dem Buch von Fischer [3] oder in dem Buch von Alaca und Williams [2] zu finden.

1.1 Notation und Definitionen

Natürliche Zahlen ($\mathbb{N}$) $\mathbb{N} = \{0, 1, 2, \ldots\}$

Identische Abbildung ($id_{M,\mathbb{C}}$) Sei M eine Teilmenge von $\mathbb{C}$, dann ist $id_{M,\mathbb{C}}$ jene Abbildung von M nach $\mathbb{C}$, für die gilt, dass $id_{M,\mathbb{C}}(\alpha) = \alpha$ für alle $\alpha \in M$ ist.

Einschränkung ($f|_N$) Seien M_0, M_1, N Mengen. Sei $N \subseteq M_0$ und f eine Abbildung von M_0 nach M_1, dann ist $f|_N$ jene Abbildung von N nach M_1, für die gilt, dass $f|_N(x) = f(x)$ für alle x in N ist.

Kronecker Delta ($\delta_{i,j}$) Sei $i, j \in \mathbb{Z}$, dann ist

$$\delta_{i,j} = \begin{cases} 1 & \text{wenn } i = j \\ 0 & \text{wenn } i \neq j \end{cases}$$

Menge aller $m \times n$ Matrizen ($M(m, n, N)$) Sei N eine Teilmenge von $\mathbb{C}$. Seien $m, n \in \mathbb{N} \setminus \{0\}$. Dann ist $M(m, n, N)$ die Menge aller $m \times n$ Matrizen mit Elementen aus N.

[5] Siehe Kapitel 3 und Kapitel 4.

[6] Siehe Definitionen 4.0.2 und Definition 4.0.3.

Transponierte (A^T) Seien $m, n \in \mathbb{N} \setminus \{0\}$. Sei $A \in M(m, n, \mathbb{C})$, dann ist A^T die transponierte Matrix von A.

Einheitsmatrix (I_m) Sei $m \in \mathbb{N} \setminus \{0\}$, dann ist $I_m = (\delta_{i,j})_{1 \leq i,j \leq m}$ die $m \times m$ Einheitsmatrix.

Polynomring ($R[T]$) Sei R ein Ring, dann ist $R[T]$ der Polynomring mit Koeffizienten aus R und der Variable T.

Minor ($M_{A,i,j}$) Sei $n \in \mathbb{N} \setminus \{0\}$ und $A \in M(n, n, \mathbb{C})$. Sei $a_{i,j} \in \mathbb{C}$ für alle $i, j \in \{1, 2, \ldots, n\}$. Sei $A = (a_{i,j})_{1 \leq i,j \leq n}$. Dann ist $M_{A,i,j} = 1$, wenn $n = 1$ ist und

$$M_{A,i,j} = \det \begin{pmatrix} a_{1,1} & \ldots & a_{1,j-1} & a_{1,j+1} & \ldots & a_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \ldots & a_{i-1,j-1} & a_{i-1,j+1} & \ldots & a_{i-1,n} \\ a_{i+1,1} & \ldots & a_{i+1,j-1} & a_{i+1,j+1} & \ldots & a_{i+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n,1} & \ldots & a_{n,j-1} & a_{n,j+1} & \ldots & a_{n,n} \end{pmatrix}$$

für alle $i, j \in \{1, 2, \ldots, n\}$, wenn $n \geq 2$ ist.

Adjunkte ($\mathrm{adj}(A)$) Sei $n \in \mathbb{N} \setminus \{0\}$ und $A \in M(n, n, \mathbb{C})$. Sei $a_{i,j} \in \mathbb{C}$ für alle $i, j \in \{1, 2, \ldots, n\}$. Sei $A = (a_{i,j})_{1 \leq i,j \leq n}$. Sei $b_{i,j} = (-1)^{i+j} M_{A,i,j}$ für alle $i, j \in \{1, 2, \ldots, n\}$. Sei $B = (b_{i,j})_{1 \leq i,j \leq n}$, dann ist $\mathrm{adj}(A) := B^T$.

Minimalpolynom ($\mathrm{irr}_{\alpha,\mathbb{Q}}$) Sei $\alpha \in \mathbb{C}$ und α algebraisch über $\mathbb{Q}$, dann ist $\mathrm{irr}_{\alpha,\mathbb{Q}}(T) \in \mathbb{Q}[T]$ das Minimalpolynom von α über $\mathbb{Q}$.

ganz über R Sei R ein Teilring von $\mathbb{C}$, $1 \in R$, und $s \in \mathbb{C}$, dann heißt s genau dann ganz über R, wenn es ein normiertes Polynom $P \in R[T]$ gibt, sodass $P(s) = 0$ ist.

ganzalgebraisch α heißt genau dann ganzalgebraisch, wenn $\alpha \in \mathbb{C}$ ist und α ganz über $\mathbb{Z}$ ist.

O Es ist O die Menge aller ganzalgebraischen Elemente von $\mathbb{C}$.

O_K Sei K ein algebraischer Zahlkörper, dann ist $O_K = O \cap K$.

Ganzheitsbasis Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$ und $[K : \mathbb{Q}] = n$, dann heißt $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ genau dann Ganzheitsbasis von K, wenn alle drei folgenden Punkte erfüllt sind:

1. $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$
2. Es ist $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$.
3. Wenn $\alpha \in O_K$ ist, dann gibt es $x_0, x_1, \ldots, x_{n-1} \in \mathbb{Z}$, sodass $\alpha = \sum_{i=0}^{n-1} x_i \omega_i$ ist.

Einbettung von K in $\mathbb{C}$ Sei K ein algebraischer Zahlkörper, dann heißt σ genau dann eine Einbettung von K in $\mathbb{C}$, wenn σ ein Ringmonomorphismus von K nach $\mathbb{C}$ ist.

Körperpolynom ($\mathrm{fld}_{\alpha,K}$) Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$ und $[K : \mathbb{Q}] = n$. Seien $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}$ alle Einbettungen von K in $\mathbb{C}$. Sei $\alpha \in K$, dann ist $\mathrm{fld}_{\alpha,K}(T) \in \mathbb{Q}[T]$ und

$$\mathrm{fld}_{\alpha,K}(T) = \prod_{i=0}^{n-1} (T - \sigma_i(\alpha)).$$

Diskriminante ($d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$) Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$ und $[K : \mathbb{Q}] = n$. Seien $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in K$. Seien $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}$ die paar-

weise verschiedenen Einbettungen von K in $\mathbb{C}$. Dann ist $d(\alpha_0, \alpha_1 \ldots, \alpha_{n-1}) = \left(\det\left(\left(\sigma_i\left(\alpha_j\right)\right)_{0\leq i,j\leq n-1}\right)\right)^2$.

Diskriminante ($d(K)$) Sei K ein algebraischer Zahlkörper, dann ist $d(K) = d\left(\alpha_0, \alpha_1, \ldots, \alpha_{[K:\mathbb{Q}]-1}\right)$ für eine Ganzheitsbasis $\left(\alpha_0, \alpha_1, \ldots, \alpha_{[K:\mathbb{Q}]-1}\right)$ von K.

p-Bewertung (ν_p) Sei p eine Primzahl, dann ist ν_p jene Abbildung, für die alle drei folgenden Punkte erfüllt sind:

1. $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$
2. Für alle $a \in \mathbb{Q} \setminus \{0\}$ gibt es ein $r \in \mathbb{Z}$ und ein $s \in \mathbb{N} \setminus \{0\}$, sodass $p \nmid r$, $p \nmid s$ und $a = p^{\nu_p(a)} \frac{r}{s}$ ist.
3. $\nu_p(0) = \infty$

Konventionen zu ∞ Sei $n \in \mathbb{Z}$ und $m \in \mathbb{N} \setminus \{0\}$, dann ist $n + \infty = \infty + n = \infty + \infty = \infty$, $m \cdot \infty = \infty \cdot m = \infty \cdot \infty = \infty$ und $\infty \geq n$.

quadratfrei Sei $n \in \mathbb{Z}$, dann heißt n genau dann quadratfrei, wenn für alle Primzahlen p gilt, dass $\nu_p(n) \leq 1$ ist.

1.2 Sätze

Satz 1.2.1. *Sei $n \in \mathbb{N} \setminus \{0\}$, $A \in M(n, n, \mathbb{C})$ und A invertierbar, dann ist $A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A)$.*

Satz 1.2.2. *Sei R ein Teilring von $\mathbb{C}$, $n \in \mathbb{N} \setminus \{0\}$ und $A \in M(n, n, R)$, dann ist $\det(A) \in R$.*

Satz 1.2.3 (Cramersche Regel)**.** *Sei $n \in \mathbb{N} \setminus \{0\}$, $A \in M(n, n, \mathbb{C})$ und $\det(A) \neq 0$. Seien $x_0, x_1, \ldots, x_{n-1} \in \mathbb{C}$. Sei $b_0, b_1 \ldots, b_{n-1} \in \mathbb{C}$. Sei $A(x_0, x_1, \ldots, x_{n-1})^T = (b_0, b_1, \ldots, b_{n-1})^T$. Sei*

$$B_i = \begin{pmatrix} a_{0,0} & \ldots & a_{0,i-1} & b_0 & a_{0,i+1} & \ldots & a_{0,n-1} \\ a_{1,0} & \ldots & a_{1,i-1} & b_1 & a_{1,i+1} & \ldots & a_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n-1,0} & \ldots & a_{n-1,i-1} & b_{n-1} & a_{n-1,i+1} & \ldots & a_{n-1,n-1} \end{pmatrix}$$

für alle $i \in \{0, 1, \ldots, n-1\}$. Dann ist $x_i = \frac{\det(B_i)}{\det(A)}$ für alle $i \in \{0, 1, \ldots, n-1\}$.

Satz 1.2.4. *Sei $P(T) \in \mathbb{Z}[T]$ und $P(T)$ normiert, dann sind die folgenden beiden Punkte äquivalent:*

1. *Es ist $P(T)$ irreduzibel über $\mathbb{Q}$.*
2. *Es ist $P(T)$ irreduzibel über $\mathbb{Z}$.*

Satz 1.2.5. *Sei $x \in \mathbb{Z}$ und $x \equiv 1 \pmod 2$, dann ist $x^2 \equiv 1 \pmod 8$.*

Beweis. Sei $x_0 \in \mathbb{Z}$ und $x = 2x_0 + 1$. Es ist

$$x^2 = (2x_0 + 1)^2 = 4x_0^2 + 4x_0 + 1 = 4x_0(x_0 + 1) + 1 \equiv 1 \pmod 8.$$

□

Satz 1.2.6. *Sei $x \in \mathbb{Z}$, $m \in \mathbb{N} \setminus \{0\}$ und $x \equiv 2^m \pmod{2^{m+1}}$, dann ist $x^2 \equiv 2^{2m} \pmod{2^{2m+2}}$.*

Beweis. Es ist

$$0 \equiv (x - 2^m)^2 = x^2 - 2 \cdot 2^m x + 2^{2m} \equiv x^2 - 2 \cdot 2^m \cdot 2^m + 2^{2m} = x^2 - 2^{2m} \pmod{2^{2m+2}}.$$

□

Satz 1.2.7. *Sei $x \in \mathbb{Z}$, dann ist $x^3 \equiv x \pmod{3}$.*

Beweis. Es ist $0^3 = 0$, $1^3 = 1$ und $2^3 = 8 \equiv 2 \pmod{3}$. □

Satz 1.2.8. *Sei $m \in \mathbb{N} \setminus \{0\}$. Seien $x, y \in \mathbb{Z}$. Sei $x \equiv y \pmod{3^m}$, dann ist $x^3 \equiv y^3 \pmod{3^{m+1}}$.*

Beweis. Es ist $x^3 = (x-y)^3 + 3x^2y - 3xy^2 + y^3 \equiv 3y^3 - 3y^3 + y^3 = y^3 \pmod{3^{m+1}}$. □

Satz 1.2.9 (Chinesischer Restsatz)**.** *Sei $n \in \mathbb{N} \setminus \{0\}$. Seien $m_0, m_1, \ldots, m_{n-1} \in \mathbb{N} \setminus \{0\}$. Sei $\mathrm{ggT}(m_i, m_j) = 1$ für alle $i, j \in \{0, 1, \ldots, n-1\}$, für die $i \neq j$ gilt. Seien $x_0, x_1, \ldots, x_{n-1} \in \mathbb{Z}$. Dann gibt es ein $X \in \mathbb{Z}$, sodass $X \equiv x_i \pmod{m_i}$ für alle $i \in \{0, 1, \ldots, n-1\}$ ist.*

Satz 1.2.10. *Sei $\alpha \in \mathbb{C}$ und α algebraisch über $\mathbb{Q}$, dann ist α genau dann ganzalgebraisch, wenn $\mathrm{irr}_{\alpha,\mathbb{Q}}(T) \in \mathbb{Z}[T]$ ist.*

Satz 1.2.11. $O \cap \mathbb{Q} = \mathbb{Z}$

Satz 1.2.12. *Sei R ein Teilring von $\mathbb{C}$ und $1 \in R$. Sei S die Menge aller Elemente von $\mathbb{C}$, die ganz über R sind. Dann ist S ein Teilring von $\mathbb{C}$.*

Satz 1.2.13. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$ und $[K : \mathbb{Q}] = n$, dann ist die Anzahl der Einbettungen von K in $\mathbb{C}$ gleich n.*

Satz 1.2.14. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$, $[K : \mathbb{Q}] = n$, $\theta \in K$, $K = \mathbb{Q}(\theta)$, σ eine Einbettungen von K in $\mathbb{C}$, dann ist $\sigma(\theta)$ eine Nullstelle von $\mathrm{irr}_{\theta,\mathbb{Q}}(T)$.*

Satz 1.2.15. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$, $[K : \mathbb{Q}] = n$, $\alpha \in K$ und $s = \frac{n}{deg(\mathrm{irr}_{\alpha,\mathbb{Q}}(T))}$, dann ist $\mathrm{fld}_{\alpha,K}(T) = (\mathrm{irr}_{\alpha,\mathbb{Q}}(T))^s$.*

Satz 1.2.16. *Sei K ein algebraischer Zahlkörper, σ eine Einbettung von K in $\mathbb{C}$ und $\alpha \in O_K$, dann ist $\sigma(\alpha)$ ganzalgebraisch.*

Satz 1.2.17. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$ und $[K : \mathbb{Q}] = n$. Seien $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in K$. Dann ist $d(\alpha_0, , \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Q}$.*

Satz 1.2.18. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$ und $[K : \mathbb{Q}] = n$. Seien $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in O_K$. Dann ist $d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}$.*

Satz 1.2.19. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$ und $[K : \mathbb{Q}] = n$. Seien $\alpha_0, \alpha_1, \ldots \alpha_{n-1} \in K$. Seien $\beta_0, \beta_1, \ldots, \beta_{n-1} \in K$. Sei $A \in M(n, n, \mathbb{Q})$ und*

$$(\beta_0, \beta_1, \ldots, \beta_{n-1})^T = A (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})^T,$$

dann ist

$$d(\beta_0, \beta_1, \ldots, \beta_{n-1}) = (\det(A))^2 d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}).$$

Satz 1.2.20. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$ und $[K : \mathbb{Q}] = n$. Seien $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in K$. Seien $\beta_0, \beta_1, \ldots, \beta_{n-1} \in K$. Sei $a_{i,j} \in \mathbb{Q}$ für alle $i \in \{0, 1, \ldots, n-1\}$ und $j \in \{0, 1, \ldots, i\}$. Sei*

$$\beta_i = \sum_{j=0}^{i} a_{i,j} \alpha_j$$

für alle $i \in \{0, 1, \ldots, n-1\}$. Dann ist

$$d(\beta_0, \beta_1, \ldots, \beta_{n-1}) = \left(\prod_{i=0}^{n-1} a_{i,i}^2 \right) d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}).$$

Beweis. Sei

$$A = \begin{pmatrix} a_{0,0} & 0 & \ldots & \ldots & 0 \\ a_{1,0} & a_{1,1} & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_{n-2,0} & a_{n-2,1} & \ldots & a_{n-2,n-2} & 0 \\ a_{n-1,0} & a_{n-1,1} & \ldots & \ldots & a_{n-1,n-1} \end{pmatrix}.$$

Es ist $(\beta_0, \beta_1, \ldots, \beta_{n-1})^T = A (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})^T$ und $\det(A) = \prod_{i=0}^{n-1} a_{i,i}$. Aus dem Satz 1.2.19 folgt, dass $d(\beta_0, \beta_1, \ldots, \beta_{n-1}) = (\det(A))^2 d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ ist. Es ist

$$d(\beta_0, \beta_1, \ldots, \beta_{n-1}) = \left(\prod_{i=0}^{n-1} a_{i,i}^2 \right) d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}).$$

□

Satz 1.2.21. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$ und $[K : \mathbb{Q}] = n$. Seien $\alpha_0, \alpha_1 \ldots, \alpha_{n-1} \in O_K$. Sei $d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \neq 0$, dann ist $|d(K)| \leq |d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})|$.*

Satz 1.2.22. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$ und $[K : \mathbb{Q}] = n$. Seien $\alpha_0, \alpha_1, \ldots \alpha_{n-1} \in O_K$. Dann sind die beiden folgenden Punkte äquivalent:*

1. *Es ist $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ eine Ganzheitsbasis von K.*

2. $d(K) = d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$

Satz 1.2.23. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$ und $[K : \mathbb{Q}] = n$. Seien $\alpha_0, \alpha_1, \ldots \alpha_{n-1} \in O_K$. Sei $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ eine Ganzheitsbasis von K und $\beta \in O_K$. Seien $x_0, x_1, \ldots, x_{n-1} \in \mathbb{Z}$. Sei $j \in \{0,1,\ldots,n-1\}$, $x_j \in \{-1,1\}$ und $\beta = \sum_{i=0}^{n-1} x_i \alpha_i$, dann ist $(\alpha_0, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_{n-1})$ eine Ganzheitsbasis von K.*

Beweis. Sei

$$A = \begin{pmatrix} 1 & 0 & & & \ldots & \ldots & & & 0 \\ 0 & 1 & 0 & & & \ldots & & & 0 \\ \vdots & \ddots & \ddots & \ddots & & & & & \vdots \\ 0 & \ldots & 0 & 1 & 0 & & \ldots & & 0 \\ x_0 & \ldots & \ldots & x_{j-1} & x_j & x_{j+1} & \ldots & \ldots & x_{n-1} \\ 0 & & \ldots & & 0 & 1 & 0 & \ldots & 0 \\ \vdots & & & & & \ddots & \ddots & \ddots & \vdots \\ 0 & & & \ldots & & & 0 & 1 & 0 \\ 0 & & & \ldots & \ldots & & & 0 & 1 \end{pmatrix}.$$

Es ist $\det(A) = x_j \in \{-1,1\}$ und

$$(\alpha_0, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_{n-1})^T = A\,(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})^T.$$

Aus dem Satz 1.2.19 folgt, dass

$$d(\alpha_0 \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_{n-1}) = d(\alpha_0, \ldots, \alpha_{n-1})$$

ist. Es ist

$$d(\alpha_0, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_{n-1}) = d(\alpha_0, \ldots, \alpha_{n-1}) = d(K).$$

Aus dem Satz 1.2.22 folgt, dass $(\alpha_0, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_{n-1})$ eine Ganzheitsbasis von K ist. □

Satz 1.2.24. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0\}$ und $[K : \mathbb{Q}] = n$. Seien $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in K$, dann sind die beiden folgenden Punkte äquivalent:*

1. *Es ist $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ linear unabhängig über $\mathbb{Q}$.*
2. *$d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \neq 0$*

Satz 1.2.25. *Sei K ein algebraischer Zahlkörper, $m \in \mathbb{Z} \setminus \{0,1\}$, m quadratfrei und $K = \mathbb{Q}(\sqrt{m})$, dann sind die beiden folgenden Punkte erfüllt:*

1. *Wenn $m \not\equiv 1 \pmod 4$ ist, dann ist $\left(1, \sqrt{m}\right)$ eine Ganzheitsbasis von K.*
2. *Wenn $m \equiv 1 \pmod 4$ ist, dann ist $\left(1, \frac{1+\sqrt{m}}{2}\right)$ eine Ganzheitsbasis von K.*

Satz 1.2.26. *Sei p eine Primzahl. Sei $a, b \in \mathbb{Q}$. Dann sind alle drei folgenden Punkte erfüllt:*

1. *$\nu_p(ab) = \nu_p(a) + \nu_p(b)$*

2. $\nu_p(a) = \infty \Leftrightarrow a = 0$
3. $\nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}$

Satz 1.2.27. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$ und $K = \mathbb{Q}(\theta)$, dann ist $d(1, \theta, \theta^2) = 4r^3 - 27s^2 \neq 0$.*

Satz 1.2.28. *Sei p eine Primzahl und $n \in \mathbb{N} \setminus \{0\}$. Seien $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$. Dann gibt es ein $k \in \{0, 1, \ldots, n-1\}$, sodass $\nu_p\left(\sum_{i=0}^{n-1} a_i\right) \geq \nu_p(a_k)$ ist.*

Beweis. Es wird Induktion nach n durchgeführt.

Anfang Wenn $n = 1$ ist, dann ist $\sum_{i=0}^{n-1} a_i = a_0$.

Sei $n \geq 2$.

Annahme Wenn $b_0, b_1, \ldots, b_{n-2} \in \mathbb{Q}$ ist, dann gibt es ein $l \in \{0, 1, \ldots, n-2\}$, sodass

$$\nu_p\left(\sum_{i=0}^{n-2} b_i\right) \geq \nu_p(b_l)$$

ist.

Schritt Aus der Induktionsannahme folgt, dass es ein $m \in \{0, 1, \ldots, n-2\}$ gibt, sodass

$$\nu_p\left(\sum_{i=0}^{n-2} a_i\right) \geq \nu_p(a_m)$$

ist. Aus dem Punkt 3 des Satzes 1.2.26 folgt, dass

$$\nu_p\left(\sum_{i=0}^{n-1} a_i\right) \geq \min\left\{\nu_p(a_{n-1}), \nu_p\left(\sum_{i=0}^{n-2} a_i\right)\right\}$$

ist. Es ist

$$\nu_p\left(\sum_{i=0}^{n-1} a_i\right) \geq \min\left\{\nu_p(a_{n-1}), \nu_p\left(\sum_{i=0}^{n-2} a_i\right)\right\} \geq \min\{\nu_p(a_{n-1}), \nu_p(a_m)\}.$$

□

Satz 1.2.29. *Seien $m, n \in \mathbb{Z} \setminus \{0\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$ und $a \in \mathbb{Q}$, dann ist $\frac{m}{n} \neq a^2$.*

Beweis. Angenommen es ist $\frac{m}{n} = a^2$. Sei $r \in \mathbb{Z} \setminus \{0\}$, $s \in \mathbb{N} \setminus \{0\}$, $\operatorname{ggT}(r, s) = 1$ und $a = \frac{r}{s}$. Sei $u \in \mathbb{Z} \setminus \{0\}$, $v \in \mathbb{N} \setminus \{0\}$, $\operatorname{ggT}(u, v) = 1$ und $\frac{m}{n} = \frac{u}{v}$. Es folgt, dass u quadratfrei ist und v quadratfrei ist. Es ist $\frac{u}{v} = \frac{m}{n} = a^2 = \frac{r^2}{s^2}$. Es ist $u = r^2$ und $v = s^2$. Es ist $u = v = 1$. Es folgt, dass $m = n$ ist. Dies ist ein Widerspruch. □

2 ganz über $\mathbb{Z}_{(p)}$

Dieses Kapitel folgt zum Teil der Doktorarbeit von Alaca [1]. Wenn K ein algebraischer Zahlkörper, $\alpha \in K$ und p eine Primzahl ist, dann ist $\alpha \in O_{p,K}$ äquivalent zu der Definition „α is a p-integral element of K“ in [1][1].

Definition 2.0.1 (p-ganz)**.** *Sei p eine Primzahl und $a \in \mathbb{Q}$, dann heißt a genau dann p-ganz, wenn $\nu_p(a) \geq 0$ ist.*

Definition 2.0.2 ($\mathbb{Z}_{(p)}$)**.** *Sei p eine Primzahl, dann ist $\mathbb{Z}_{(p)}$ die Menge aller p-ganzen Elemente von $\mathbb{Q}$.*

Satz 2.0.3. *Sei p eine Primzahl, dann ist $\mathbb{Z}_{(p)}$ ein Teilring von $\mathbb{Q}$.*

Beweis. Seien $a_0, a_1 \in \mathbb{Z}_{(p)}$. Aus dem Punkt 3 des Satzes 1.2.26 folgt, dass

$$\nu_p(a_0 - a_1) \geq \min\left\{\nu_p(a_0), \nu_p(-a_1)\right\}$$

ist. Es ist

$$\nu_p(a_0 - a_1) \geq \min\left\{\nu_p(a_0), \nu_p(-a_1)\right\} = \min\left\{\nu_p(a_0), \nu_p(a_1)\right\} \geq 0.$$

Es ist $a_0 - a_1 \in \mathbb{Z}_{(p)}$. Seien $b_0, b_1 \in \mathbb{Z}_{(p)}$. Es folgt, dass $\nu_p(b_0 b_1) = \nu_p(b_0) + \nu_p(b_1) \geq 0$ ist. Es ist $b_0 b_1 \in \mathbb{Z}_{(p)}$. Da $\nu_p(0) = \infty \geq 0$ ist, ist $0 \in \mathbb{Z}_{(p)}$. Es folgt, dass $\mathbb{Z}_{(p)}$ ein Teilring von $\mathbb{Q}$ ist. □

Satz 2.0.4. $\bigcap_{p \text{ Primzahl}} \mathbb{Z}_{(p)} = \mathbb{Z}$

Beweis. Sei

$$N = \bigcap_{p \text{ Primzahl}} \mathbb{Z}_{(p)}.$$

Sei $a \in N$. Sei $r \in \mathbb{Z}$, $s \in \mathbb{N} \setminus \{0\}$, $\mathrm{ggT}(r, s) = 1$ und $a = \frac{r}{s}$. Für alle Primzahlen p gilt, dass $p \nmid s$ ist. Es ist $s = 1$ und $a \in \mathbb{Z}$. Da $a \in N$ beliebig war, folgt, dass $N \subseteq \mathbb{Z}$ ist. Es ist $\mathbb{Z} \subseteq N$. Es ist $N = \mathbb{Z}$. □

Die Menge O_p, die in der folgenden Definition für eine Primzahl p definiert wird, unterscheidet sich von der Menge O_p in der Doktorarbeit von Alaca [1]. Alaca unterdrückt den algebraischen Zahlkörper K in seiner Notation. Die Menge O_p in [1] entspricht für alle Primzahlen p der Menge $O_{p,K} = K \cap O_p$ für einen gegebenen Zahlkörper K.[2]

[1] Siehe Definition 2.0.6 und Bemerkung 2.0.10.
[2] Siehe Bemerkung 2.0.10.

Definition 2.0.5 (O_p)**.** *Sei p eine Primzahl, dann ist*

$$O_p = \left\{ \alpha \in \mathbb{C} \mid \alpha \text{ ist ganz über } \mathbb{Z}_{(p)} \right\}.$$

Definition 2.0.6 ($O_{p,K}$)**.** *Sei K ein algebraischer Zahlkörper und p eine Primzahl, dann ist $O_{p,K} = K \cap O_p$.*

Der Punkt 2 des folgenden Satzes stammt im Wesentlichen aus der Doktorarbeit von Alaca [1][3]. Die Beweisidee des Punktes 3 des folgenden Satzes stammt aus dem Beweis des Satzes 4.2.3 in dem Buch von Alaca und Williams [2].

Satz 2.0.7. *Sei p eine Primzahl, dann sind alle drei folgenden Punkte erfüllt:*

1. $O \subseteq O_p$
2. O_p *ist ein Teilring von* $\mathbb{C}$.
3. $\mathbb{Q} \cap O_p = \mathbb{Z}_{(p)}$

Beweis.

1 Sei $\alpha \in O$. Sei $P(T) \in \mathbb{Z}[T]$, $P(T)$ normiert und $P(\alpha) = 0$. Da $\mathbb{Z} \subseteq \mathbb{Z}_{(p)}$ ist, ist $P(T) \in \mathbb{Z}_{(p)}[T]$. Es ist $\alpha \in O_p$.

2 Aus dem Satz 2.0.3 folgt, dass $\mathbb{Z}_{(p)}$ ein Teilring von $\mathbb{Q}$ ist. Es ist $1 \in \mathbb{Z}_{(p)}$. Aus dem Satz 1.2.12 folgt, dass O_p ein Teilring von $\mathbb{C}$ ist.

3 Sei $a \in \mathbb{Q} \cap O_p$. Sei $r \in \mathbb{Z}$, $s \in \mathbb{N} \setminus \{0\}$, $\operatorname{ggT}(r,s) = 1$ und $a = \frac{r}{s}$. Sei $Q(T) \in \mathbb{Z}_{(p)}[T]$, $Q(T)$ normiert und $Q(a) = 0$. Sei $n \in \mathbb{N} \setminus \{0\}$, ($u_i \in \mathbb{Z}$, $v_i \in \mathbb{N} \setminus \{0\}$, $p \nmid v_i$ und $\operatorname{ggT}(u_i, v_i) = 1$ für alle $i \in \{0, 1, \ldots, n-1\}$) und

$$Q(T) = \left(\sum_{j=0}^{n-1} \frac{u_j}{v_j} T^j \right) + T^n.$$

Es gilt, dass

$$0 = Q(a) = Q\left(\frac{r}{s}\right) = \left(\sum_{i=0}^{n-1} \frac{u_i}{v_i} \left(\frac{r}{s}\right)^i \right) + \left(\frac{r}{s}\right)^n \tag{2.1}$$

ist. Sei $w_i = v_0 \ldots v_{i-1} v_{i+1} \ldots v_{n-1}$ für alle $i \in \{0, 1, \ldots, n-1\}$. Durch Multiplikation der Gleichung (2.1) mit $s^n v_0 v_1 \ldots v_{n-1}$ folgt, dass

$$0 = \left(\sum_{i=0}^{n-1} r^i s^{n-i} u_i w_i \right) + r^n v_0 v_1 \ldots v_{n-1} = s \left(\sum_{i=0}^{n-1} r^i s^{n-i-1} u_i w_i \right) + r^n v_0 v_1 \ldots v_{n-1} \tag{2.2}$$

ist. Aus der Gleichung (2.2) folgt, dass $p \nmid s$ ist. Es folgt, dass $a \in \mathbb{Z}_{(p)}$ ist. Da a beliebig war in $\mathbb{Q} \cap O_p$, folgt, dass $\mathbb{Q} \cap O_p \subseteq \mathbb{Z}_{(p)}$ ist. Es ist $\mathbb{Z}_{(p)} \subseteq \mathbb{Q} \cap O_p$. Es folgt, dass $\mathbb{Q} \cap O_p = \mathbb{Z}_{(p)}$ ist.

□

[3] Siehe Punkt ii) des Satzes 1.2.1 in [1].

Satz 2.0.8. *Sei p eine Primzahl, $\alpha \in \mathbb{C}$ und α algebraisch über $\mathbb{Q}$, dann sind die beiden folgenden Punkte äquivalent:*

1. $\alpha \in O_p$
2. $\mathrm{irr}_{\alpha,\mathbb{Q}}(T) \in \mathbb{Z}_{(p)}[T]$

Beweis.

(1 ⇒ 2) Sei $n = deg(\mathrm{irr}_{\alpha,\mathbb{Q}}(T))$. Seien $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$ und

$$\mathrm{irr}_{\alpha,\mathbb{Q}}(T) = \left(\sum_{j=0}^{n-1} a_j T^j\right) + T^n.$$

Sei $P(T) \in \mathbb{Z}_{(p)}[T]$, $P(T)$ normiert und $P(\alpha) = 0$. Seien $\beta_0, \beta_1, \ldots, \beta_{n-1} \in \mathbb{C}$ und

$$\mathrm{irr}_{\alpha,\mathbb{Q}}(T) = \prod_{i=0}^{n-1} (T - \beta_i).$$

Es ist

$$a_{n-k} = (-1)^k \sum_{0 \le i_1 < i_2 < \ldots < i_k \le n-1} \beta_{i_1} \ldots \beta_{i_k}$$

für alle $k \in \{1, 2, \ldots, n\}$. Es gibt ein $Q(T) \in \mathbb{Q}[T]$, sodass $P(T) = \mathrm{irr}_{\alpha,\mathbb{Q}}(T)\, Q(T)$ ist. Es folgt, dass $P(\beta_i) = 0$ ist für alle $i \in \{0, 1, \ldots, n-1\}$. Es ist $\beta_0, \beta_1, \ldots, \beta_{n-1} \in O_p$. Da O_p ein Ring ist, sind $a_0, a_1, \ldots, a_{n-1} \in O_p$. Aus dem Punkt 3 des Satzes 2.0.7 folgt, dass $\mathbb{Q} \cap O_p = \mathbb{Z}_{(p)}$ ist. Es ist $a_i \in \mathbb{Q} \cap O_p = \mathbb{Z}_{(p)}$ für alle $i \in \{0, 1, \ldots, n-1\}$. Es ist $\mathrm{irr}_{\alpha,\mathbb{Q}}(T) \in \mathbb{Z}_{(p)}[T]$.

(2 ⇒ 1) Es ist $\mathrm{irr}_{\alpha,\mathbb{Q}}(T)$ normiert und $\mathrm{irr}_{\alpha,\mathbb{Q}}(\alpha) = 0$. Es folgt, dass $\alpha \in O_p$ ist.

□

Satz 2.0.9. *Sei K ein algebraischer Zahlkörper, p eine Primzahl und $\alpha \in K$, dann sind die beiden folgenden Punkte äquivalent:*

1. $\alpha \in O_{p,K}$
2. $\mathrm{fld}_{\alpha,K}(T) \in \mathbb{Z}_{(p)}[T]$

Beweis.

(1 ⇒ 2) Aus dem Satz 2.0.8 folgt, dass $\mathrm{irr}_{\alpha,\mathbb{Q}}(T) \in \mathbb{Z}_{(p)}[T]$ ist. Aus dem Satz 1.2.15 folgt, dass es ein $s \in \mathbb{N} \setminus \{0\}$ gibt, sodass $\mathrm{fld}_{\alpha,K}(T) = (\mathrm{irr}_{\alpha,\mathbb{Q}}(T))^s$ ist. Es ist $\mathrm{fld}_{\alpha,K}(T) \in \mathbb{Z}_{(p)}[T]$.

(2 ⇒ 1) Die Abbildung $id_{K,\mathbb{C}}$ ist eine Einbettung von K in $\mathbb{C}$. Es ist $\mathrm{fld}_{\alpha,K}(\alpha) = 0$. Es ist $\alpha \in O_{p,K}$.

□

Bemerkung 2.0.10. *Sei K ein algebraischer Zahlkörper, $\alpha \in K$ und p eine Primzahl. Der Satz 2.0.9 dieses Kapitels und der Satz 1.2.2 in der Doktorarbeit von Alaca [1] zeigen, dass $\alpha \in O_{p,K}$ äquivalent zu der Definition „α is a p-integral element of K“ in [1] ist.*

Satz 2.0.11. $O = \bigcap_{p \text{ Primzahl}} O_p$

Beweis. Sei

$$M = \bigcap_{p \text{ Primzahl}} O_p$$

Aus dem Punkt 1 des Satzes 2.0.7 folgt, dass $O \subseteq M$ ist. Sei $\alpha \in M$. Aus dem Satz 2.0.8 folgt, dass

$$\operatorname{irr}_{\alpha,\mathbb{Q}}(T) \in \bigcap_{p \text{ Primzahl}} \left(\mathbb{Z}_{(p)}[T]\right)$$

ist. Aus dem Satz 2.0.4 folgt, dass

$$\bigcap_{p \text{ Primzahl}} \mathbb{Z}_{(p)} = \mathbb{Z}$$

ist. Es ist

$$\bigcap_{p \text{ Primzahl}} \left(\mathbb{Z}_{(p)}[T]\right) = \left(\bigcap_{p \text{ Primzahl}} \mathbb{Z}_{(p)}\right)[T] = \mathbb{Z}[T].$$

Es ist $\operatorname{irr}_{\alpha,\mathbb{Q}}(T) \in \mathbb{Z}[T]$. Es ist $\alpha \in O$. Da $\alpha \in M$ beliebig war, ist $M \subseteq O$. Es folgt, dass $O = M$ ist. □

Die folgende Definition stammt im Wesentlichen aus der Doktorarbeit von Alaca [1][4].

Definition 2.0.12 (p-ganze Basis)**.** *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$, $[K:\mathbb{Q}] = n$ und p eine Primzahl, dann heißt $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ genau dann p-ganze Basis von K, wenn alle drei folgenden Punkte erfüllt sind:*

1. *$\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_{p,K}$*
2. *Es ist $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$.*
3. *Wenn $\alpha \in O_{p,K}$ ist, dann gibt es $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_{(p)}$, sodass $\alpha = \sum_{i=0}^{n-1} a_i \omega_i$ ist.*

Der folgende Satz stammt im Wesentlichen aus der Doktorarbeit von Alaca [1][5]. Der Beweis folgt dem Beweis des Satzes 1.3.2 in [1].

Satz 2.0.13. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$ und $[K:\mathbb{Q}] = n$. Seien $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in K$. Dann sind die beiden folgenden Punkte äquivalent:*

1. *Es ist $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ eine Ganzheitsbasis von K.*

[4] Siehe Definition 1.3.1 in [1].
[5] Siehe Satz 1.3.2 in [1].

2. *Es ist* $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ *eine p-ganze Basis von K für alle Primzahlen p.*

Beweis.

(1 ⇒ 2) Sei p eine Primzahl. Aus dem Punkt 1 des Satzes 2.0.7 folgt, dass $O \subseteq O_p$ ist. Es ist $\alpha_i \in O_K \subseteq O_{p,K}$ für alle $i \in \{0, 1, \ldots, n-1\}$. Sei $\beta \in O_{p,K}$. Es gibt ein $P(T) \in \mathbb{Z}_{(p)}[T]$, sodass $P(T)$ normiert ist und $P(\beta) = 0$ ist. Sei $m = deg(P(T))$. Sei $b_0, b_1, \ldots, b_{m-1} \in \mathbb{Z}_{(p)}$ und

$$P(T) = \left(\sum_{i=0}^{m-1} b_i T^i \right) + T^m.$$

Sei $r_i \in \mathbb{Z}$, $s_i \in \mathbb{N} \setminus \{0\}$, $\mathrm{ggT}(r_i, s_i) = 1$ und $b_i = \frac{r_i}{s_i}$ für alle $i \in \{0, 1, \ldots, m-1\}$. Sei $d = \prod_{i=0}^{m-1} s_i$, $\gamma = d\beta$, $Q(T) \in \mathbb{Z}[T]$ und

$$Q(T) = \left(\sum_{i=0}^{m-1} b_i d^{m-i} T^i \right) + T^m.$$

Es ist $Q(\gamma) = Q(d\beta) = d^m P(\beta) = 0$. Es ist $\gamma \in O_K$. Da $b_0, b_1, \ldots, b_{m-1} \in \mathbb{Z}_{(p)}$ ist, folgt, dass $p \nmid s_i$ für alle $i \in \{0, 1, \ldots, m-1\}$ ist. Es ist $p \nmid d$. Sei $x_0, x_1, \ldots, x_{n-1} \in \mathbb{Z}$ und $\gamma = \sum_{i=0}^{n-1} x_i \alpha_i$. Es folgt, dass

$$\beta = \frac{\gamma}{d} = \sum_{i=0}^{n-1} \frac{x_i}{d} \alpha_i$$

ist. Es ist $\frac{x_i}{d} \in \mathbb{Z}_{(p)}$ für alle $i \in \{0, 1, \ldots, n-1\}$. Es ist $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ eine p-ganze Basis von K.

(2 ⇒ 1) Aus dem Satz 2.0.11 folgt, dass

$$O = \bigcap_{p \text{ Primzahl}} O_p$$

ist. Es ist

$$\alpha_i \in \bigcap_{p \text{ Primzahl}} O_p = O$$

für alle $i \in \{0, 1, \ldots, n-1\}$. Es sind $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in O_K$. Sei $\theta \in O_K$. Seien $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$ und

$$\theta = \sum_{i=0}^{n-1} a_i \alpha_i.$$

Da $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ für alle Primzahlen p eine p-ganze Basis von K ist, gilt für alle Primzahlen p, dass $a_i \in \mathbb{Z}_{(p)}$ für alle $i \in \{0, 1, \ldots, n-1\}$ ist. Aus dem Satz 2.0.4 folgt, dass

$$\bigcap_{p \text{ Primzahl}} \mathbb{Z}_{(p)} = \mathbb{Z}$$

ist. Es ist

$$a_i \in \bigcap_{p \text{ Primzahl}} \mathbb{Z}_{(p)} = \mathbb{Z}$$

für alle $i \in \{0, 1, \ldots, n-1\}$. Es ist $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ eine Ganzheitsbasis von K.

□

Der folgende Satz und der Satz 2.0.17 sind mit dem Satz 1.3.1 in der Doktorarbeit von Alaca [1] vergleichbar.

Satz 2.0.14. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$, $[K : \mathbb{Q}] = n$ und p eine Primzahl und $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ eine p-ganze Basis von K. Seien $\beta_0, \beta_1, \ldots, \beta_{n-1} \in O_{p,K}$. Dann ist $\nu_p(d(\alpha_0, \alpha_1 \ldots, \alpha_{n-1})) \leq \nu_p(d(\beta_0, \beta_1, \ldots, \beta_{n-1}))$.*

Beweis. Sei $A \in M\left(n, n, \mathbb{Z}_{(p)}\right)$ und $(\beta_0, \beta_1, \ldots, \beta_{n-1})^T = A(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})^T$. Aus dem Satz 1.2.19 folgt, dass $d(\beta_0, \beta_1, \ldots, \beta_{n-1}) = (\det(A))^2 d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ ist. Aus dem Satz 1.2.2 folgt, dass $\det(A) \in \mathbb{Z}_{(p)}$ ist. Es ist $\nu_p(\det(A)) \geq 0$. Es ist

$$\nu_p(d(\beta_0, \beta_1, \ldots, \beta_{n-1})) = \nu_p\left(\det(A)^2 d(\alpha_0, \alpha_1 \ldots, \alpha_{n-1})\right) = 2\nu_p(\det(A)) + \nu_p(d(\alpha_0, \alpha_1 \ldots, \alpha_{n-1})).$$

Es ist $\nu_p(d(\beta_0, \beta_1, \ldots, \beta_{n-1})) \geq \nu_p(d(\alpha_0, \alpha_1 \ldots, \alpha_{n-1}))$. □

Satz 2.0.15. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$, $[K : \mathbb{Q}] = n$, p eine Primzahl und $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ eine p-ganze Basis von K. Sei $\beta_0, \beta_1, \ldots, \beta_{n-1} \in K$. Sei $A \in M\left(n, n, \mathbb{Z}_{(p)}\right)$ und $(\beta_0, \beta_1 \ldots, \beta_{n-1})^T = A \cdot (\alpha_0, \alpha_1 \ldots, \alpha_{n-1})^T$, dann sind die beiden folgenden Punkte äquivalent:*

1. *Es ist $(\beta_0, \beta_1, \ldots, \beta_{n-1})$ eine p-ganze Basis von K.*
2. *$\nu_p(\det(A)) = 0$*

Beweis.

(1 ⇒ 2) Sei $B \in M\left(n, n, \mathbb{Z}_{(p)}\right)$ und $(\alpha_0, \alpha_1 \ldots, \alpha_{n-1})^T = B(\beta_0, \beta_1, \ldots, \beta_{n-1})^T$. Es ist

$$(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})^T = B(\beta_0, \beta_1, \ldots, \beta_{n-1})^T = BA(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})^T.$$

Da $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ eine Basis von K über $\mathbb{Q}$ ist, folgt, dass $BA = I_n$ ist. Es ist $\det(B)\det(A) = \det(BA) = \det(I_n) = 1$. Es ist

$$\nu_p(\det(A)) + \nu_p(\det(B)) = \nu_p(\det(B)\det(A)) = \nu_p(1) = 0.$$

Aus dem Satz 1.2.2 folgt, dass $\nu_p(\det(A)) \geq 0$ und $\nu_p(\det(B)) \geq 0$ ist. Es ist $\nu_p(\det(A)) = 0$.

(2 $\Rightarrow$ 1) Da $\det(A) \neq 0$ ist, folgt, dass A invertierbar ist. Aus dem Satz 1.2.1 folgt, dass $A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A)$ ist. Aus dem Satz 1.2.2 folgt, dass $M_{A,i,j} \in \mathbb{Z}_{(p)}$ für alle $i, j \in \{1, 2, \ldots, n\}$ ist. Es ist $\operatorname{adj}(A) \in M\left(n, n, \mathbb{Z}_{(p)}\right)$. Es ist $\frac{1}{\det(A)} \in \mathbb{Z}_{(p)}$ und $A^{-1} \in M\left(n, n, \mathbb{Z}_{(p)}\right)$. Aus dem Satz 1.2.24 folgt, dass $d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \neq 0$ ist. Aus dem Satz 1.2.19 folgt, dass

$$d(\beta_0, \beta_1, \ldots, \beta_{n-1}) = (\det(A))^2 \, d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$$

ist. Es ist

$$d(\beta_0, \beta_1, \ldots, \beta_{n-1}) = (\det(A))^2 \, d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \neq 0.$$

Aus dem Satz 1.2.24 folgt, dass $(\beta_0, \beta_1, \ldots, \beta_{n-1})$ linear unabhängig über $\mathbb{Q}$ ist. Da $[K : \mathbb{Q}] = n$ ist, folgt, dass $(\beta_0, \beta_1, \ldots, \beta_{n-1})$ eine Basis von K über $\mathbb{Q}$ ist. Aus dem Punkt 2 des Satzes 2.0.7 folgt, dass O_p ein Teilring von $\mathbb{C}$ ist. Es ist $\beta_i \in O_{p,K}$ für alle $i \in \{0, 1, \ldots, n-1\}$. Es ist $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})^T = A^{-1} (\beta_0, \beta_1, \ldots, \beta_{n-1})^T$. Es ist $(\beta_0, \beta_1, \ldots, \beta_{n-1})$ eine p-ganze Basis von K.

□

Satz 2.0.16. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0, 1\}$, $[K : \mathbb{Q}] = n$, p eine Primzahl, $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ eine p-ganze Basis von K und $\beta \in K$. Seien $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_{(p)}$. Sei $j \in \{0, 1, \ldots, n-1\}$, $\nu_p(a_j) = 0$ und $\beta = \sum_{i=0}^{n-1} a_i \alpha_i$, dann ist $(\alpha_0, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_{n-1})$ eine p-ganze Basis von K.*

Beweis. Sei

$$A = \begin{pmatrix} 1 & 0 & & & \ldots & \ldots & & & 0 \\ 0 & 1 & 0 & & & \ldots & & & 0 \\ \vdots & \ddots & \ddots & \ddots & & & & & \vdots \\ 0 & \ldots & 0 & 1 & 0 & & \ldots & & 0 \\ a_0 & \ldots & \ldots & a_{j-1} & a_j & a_{j+1} & \ldots & \ldots & a_{n-1} \\ 0 & & \ldots & & 0 & 1 & 0 & \ldots & 0 \\ \vdots & & & & & \ddots & \ddots & \ddots & \vdots \\ 0 & & & \ldots & & & 0 & 1 & 0 \\ 0 & & & \ldots & \ldots & & & 0 & 1 \end{pmatrix}.$$

Es ist $\det(A) = a_j$ und $(\alpha_0, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_{n-1})^T = A(\alpha_0, \ldots, \alpha_{n-1})^T$. Aus dem Satz 2.0.15 folgt, dass $(\alpha_0, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_{n-1})$ eine p-ganze Basis von K ist. □

Der Satz 2.0.14 und der folgende Satz sind mit dem Satz 1.3.1 in der Doktorarbeit von Alaca [1] vergleichbar.

Satz 2.0.17. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0, 1\}$, $[K : \mathbb{Q}] = n$, p eine Primzahl und $(\alpha_0, \alpha_1 \ldots, \alpha_{n-1})$ eine p-ganze Basis von K. Seien $\beta_0, \beta_1, \ldots, \beta_{n-1} \in O_{p,K}$. Dann sind die beiden folgenden Punkte äquivalent:*

1. *Es ist* $(\beta_0, \beta_1, \ldots, \beta_{n-1})$ *eine p-ganze Basis von K.*
2. $\nu_p\left(d\left(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\right)\right) = \nu_p\left(d\left(\beta_0, \beta_1, \ldots, \beta_{n-1}\right)\right)$

Beweis. Sei $A \in M\left(n, n, \mathbb{Z}_{(p)}\right)$ und $\left(\beta_0, \beta_1, \ldots, \beta_{n-1}\right)^T = A\left(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\right)^T$. Aus dem Satz 1.2.19 folgt, dass

$$d\left(\beta_0, \beta_1 \ldots, \beta_{n-1}\right) = \left(\det\left(A\right)\right)^2 d\left(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\right)$$

ist. Es folgt, dass $\nu_p\left(d\left(\beta_0, \beta_1, \ldots, \beta_{n-1}\right)\right) = 2\,\nu_p\left(\det\left(A\right)\right) + \nu_p\left(d\left(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\right)\right)$ ist.

(1 $\Rightarrow$ 2) Aus dem Satz 2.0.15 folgt, dass $\nu_p\left(\det\left(A\right)\right) = 0$ ist. Es folgt, dass

$$\nu_p\left(d\left(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\right)\right) = \nu_p\left(d\left(\beta_0, \beta_1, \ldots, \beta_{n-1}\right)\right)$$

ist.

(2 $\Rightarrow$ 1) Es folgt, dass $\nu_p\left(\det\left(A\right)\right) = 0$ ist. Aus dem Satz 2.0.15 folgt, dass $\left(\beta_0, \beta_1, \ldots, \beta_{n-1}\right)$ eine p-ganze Basis von K ist.

□

3 minimal-ganzalgebraisch

Dieses Kapitel folgt zum Teil dem Abschnitt 7.2 in dem Buch von Alaca und Williams [2]. Einige Sätze werden nicht für eine Basis $\left(1, \theta, \ldots, \theta^{n-1}\right)$ über $\mathbb{Q}$ für ein primitives Element $\theta \in O_K$ gezeigt, sondern etwas allgemeiner für eine beliebige Basis über $\mathbb{Q}$ mit ganzalgebraischen Elementen.

Die folgende Definition ist mit der Definition 7.2.1 in [2] vergleichbar, wenn $(\omega_0, \omega_1, \ldots, \omega_{n-1}) = \left(1, \theta, \ldots, \theta^{n-1}\right)$ für ein primitives Element $\theta \in O_K$ ist.

Definition 3.0.1 (minimal-ganzalgebraisches Element von K vom Grad k)**.** *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ und $k \in \{0, 1, \ldots, n-1\}$, dann heißt α genau dann minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$, wenn $\alpha \in O_K$ ist und es $a_0, a_1, \ldots, a_k \in \mathbb{Q}$ gibt, sodass alle drei folgenden Punkte erfüllt sind:*

1. $a_k > 0$
2. $\alpha = \sum_{i=0}^{k} a_i \omega_i$
3. *Wenn $b_0, b_1, \ldots, b_k \in \mathbb{Q}$ ist, $b_k > 0$ und $\sum_{i=0}^{k} b_i \omega_i \in O_K$ ist, dann ist $a_k \leq b_k$.*

Der folgende Satz stammt im Wesentlichen aus dem Buch von Alaca und Williams [2][1]. Der Beweis folgt im Wesentlichen dem Beweis des Satzes 7.2.1 in [2].

Satz 3.0.2. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ und $\alpha \in O_K$, dann gibt es $x_0, x_1, \ldots, x_{n-1} \in \mathbb{Z}$, sodass beide folgenden Punkte erfüllt sind:*

1. $\alpha = \sum_{i=0}^{n-1} \frac{x_i}{d(\omega_0, \omega_1, \ldots, \omega_{n-1})} \omega_i$
2. *Es ist $d(\omega_0, \omega_1, \ldots, \omega_{n-1}) \mid x_i^2$ für alle $i \in \{0, 1, \ldots, n-1\}$.*

Beweis. Aus dem Satz 1.2.18 folgt, dass $d(\omega_0, \omega_1 \ldots, \omega_{n-1}) \in \mathbb{Z}$ ist. Aus dem Satz 1.2.24 folgt, dass $d(\omega_0, \omega_1, \ldots, \omega_{n-1}) \neq 0$ ist. Sei $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$ und

$$\alpha = \sum_{i=0}^{n-1} a_i \omega_i.$$

[1] Siehe Satz 7.2.1 in [2].

Seien $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}$ alle Einbettungen von K in $\mathbb{C}$. Es ist

$$\sigma_i(\alpha) = \sum_{j=0}^{n-1} a_j \sigma_i(\omega_j)$$

für alle $i \in \{0,1,\ldots,n-1\}$. Sei $A = \left(\sigma_i(\omega_j)\right)_{0 \leq i,j \leq n-1}$. Es ist $A(a_0, a_1, \ldots, a_{n-1})^T = (\sigma_0(\alpha), \sigma_1(\alpha), \ldots, \sigma_{n-1}(\alpha))^T$. Sei

$$B_i = \begin{pmatrix} \sigma_0(\omega_0) & \ldots & \sigma_0(\omega_{i-1}) & \sigma_0(\alpha) & \sigma_0(\omega_{i+1}) & \ldots & \sigma_0(\omega_{n-1}) \\ \sigma_1(\omega_0) & \ldots & \sigma_1(\omega_{i-1}) & \sigma_1(\alpha) & \sigma_1(\omega_{i+1}) & \ldots & \sigma_1(\omega_{n-1}) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_n(\omega_0) & \ldots & \sigma_n(\omega_{i-1}) & \sigma_n(\alpha) & \sigma_n(\omega_{i+1}) & \ldots & \sigma_n(\omega_{n-1}) \end{pmatrix}$$

für alle $i \in \{0,1,\ldots,n-1\}$. Aus dem Satz 1.2.3 folgt, dass $a_i = \frac{\det(B_i)}{\det(A)}$ für alle $i \in \{0,1,\ldots,n-1\}$ ist. Es ist $(\det(A))^2 = d(\omega_0, \omega_1, \ldots, \omega_{n-1})$. Es ist

$$(\det(B_i))^2 = a_i^2 (\det(A))^2 = a_i^2 d(\omega_0, \omega_1, \ldots, \omega_{n-1}) \in \mathbb{Q}$$

für alle $i \in \{0,1,\ldots,n-1\}$. Aus dem Satz 1.2.16 folgt, dass $\sigma_i(\omega_j)$ ganzalgebraisch für alle $i,j \in \{0,1,\ldots,n-1\}$ ist und $\sigma_k(\alpha)$ ganzalgebraisch für alle $k \in \{0,1,\ldots,n-1\}$ ist. Es ist $B_i \in M(n,n,O)$ für alle $i \in \{0,1,\ldots,n-1\}$. Aus dem Satz 1.2.2 folgt, dass $\det(B_i)$ ganzalgebraisch für alle $i \in \{0,1,\ldots,n-1\}$ ist. Aus dem Satz 1.2.11 folgt, dass $O \cap \mathbb{Q} = \mathbb{Z}$ ist. Es ist

$$a_i^2 d(\omega_0, \omega_1, \ldots, \omega_{n-1}) = (\det(B_i))^2 \in O \cap \mathbb{Q} = \mathbb{Z}$$

für alle $i \in \{0,1,\ldots,n-1\}$. Sei $r_i \in \mathbb{Z}$, $s_i \in \mathbb{N} \setminus \{0\}$, $\mathrm{ggT}(r_i, s_i) = 1$ und $a_i = \frac{r_i}{s_i}$ für alle $i \in \{0,1,\ldots,n-1\}$. Es folgt, dass $s_i^2 \mid d(\omega_0, \omega_1, \ldots, \omega_{n-1})$ für alle $i \in \{0,1,\ldots,n-1\}$ ist. Sei $x_i = a_i d(\omega_0, \omega_1, \ldots, \omega_{n-1})$ für alle $i \in \{0,1,\ldots,n-1\}$. Es ist $x_i \in \mathbb{Z}$ für alle $i \in \{0,1,\ldots,n-1\}$. Es ist

$$\alpha = \sum_{i=0}^{n-1} \frac{x_i}{d(\omega_0, \omega_1, \ldots, \omega_{n-1})} \omega_i.$$

Es gilt, dass

$$\frac{x_i^2}{d(\omega_0, \omega_1, \ldots, \omega_{n-1})} = r_i^2 \frac{d(\omega_0, \omega_1, \ldots, \omega_{n-1})}{s_i^2} \in \mathbb{Z}$$

für alle $i \in \{0,1,\ldots,n-1\}$ ist. Es folgt, dass $d(\omega_0, \omega_1, \ldots, \omega_{n-1}) \mid x_i^2$ für alle $i \in \{0,1,\ldots,n-1\}$ ist. □

Satz 3.0.3. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ und $k \in \{0,1,\ldots,n-1\}$. Seien $a_0, a_1, \ldots, a_k \in \mathbb{Q}$. Seien $b_0, b_1, \ldots, b_k \in \mathbb{Q}$. Sei $\sum_{i=0}^{k} a_i \omega_i \in O_K$, $\sum_{i=0}^{k} b_i \omega_i \in O_K$ und $a_k \neq b_k$, dann ist $|a_k - b_k| \geq \frac{1}{|d(\omega_0, \omega_1, \ldots, \omega_{n-1})|}$.*

Beweis. Aus dem Satz 1.2.4 folgt, dass $d(\omega_0, \omega_1, \ldots, \omega_{n-1}) \neq 0$ ist. Aus dem Satz 3.0.2 folgt, dass es $x_i \in \mathbb{Z}$ und $y_i \in \mathbb{Z}$ für alle $i \in \{0, 1, \ldots, n-1\}$ gibt, sodass

$$\sum_{i=0}^{k} a_i \omega_i = \sum_{j=0}^{n-1} \frac{x_j}{d(\omega_0, \omega_1, \ldots, \omega_{n-1})} \omega_j$$

und

$$\sum_{i=0}^{k} b_i \omega_i = \sum_{j=0}^{n-1} \frac{y_j}{d(\omega_0, \omega_1, \ldots, \omega_{n-1})} \omega_j$$

ist. Es folgt, dass $a_k = \frac{x_k}{d(\omega_0, \omega_1, \ldots, \omega_{n-1})}$ und $b_k = \frac{y_k}{d(\omega_0, \omega_1, \ldots, \omega_{n-1})}$ ist. Es ist

$$|a_k - b_k| = \left| \frac{x_k - y_k}{d(\omega_0, \omega_1, \ldots, \omega_{n-1})} \right| \geq \frac{1}{|d(\omega_0, \omega_1, \ldots, \omega_{n-1})|}.$$

□

Die Notation „S_k“ in dem Beweis des folgenden Satzes stammt aus dem Abschnitt 7.2 in dem Buch von Alaca und Williams [2].

Satz 3.0.4. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0, 1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ und $k \in \{0, 1, \ldots, n-1\}$, dann gibt es ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$.*

Beweis. Sei

$$S_k = \left\{ a \in \mathbb{Q} \mid \exists b_0, \ldots, b_{k-1} \in \mathbb{Q} : \sum_{i=0}^{k-1} b_i \omega_i + a\omega_k \in O_K \right\}.$$

Da $\omega_k \in O_K$ ist, folgt, dass $1 \in S_k \cap \{a \in \mathbb{Q} \mid a > 0\}$ ist und $S_k \cap \{a \in \mathbb{Q} \mid a > 0\} \neq \emptyset$ ist. Sei

$$c = \inf\left(S_k \cap \{a \in \mathbb{Q} \mid a > 0\}\right).$$

Aus dem Satz 3.0.3 folgt, dass $c \in S_K \cap \{a \in \mathbb{Q} \mid a > 0\}$ ist. Sei $b_0, b_1, \ldots, b_{k-1} \in \mathbb{Q}$ und $\sum_{i=0}^{k-1} b_i \omega_i + c\omega_k \in O_K$. Es ist $\sum_{i=0}^{k-1} b_i \omega_i + c\omega_k$ ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$. □

Satz 3.0.5. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0, 1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$, $k \in \{0, 1, \ldots, n-1\}$, $l \in \{k, k+1, \ldots, n-1\}$, $L = \mathbb{Q}(\omega_0, \omega_1, \ldots, \omega_l)$ und $(\omega_0, \omega_1, \ldots, \omega_l)$ eine Basis von L über $\mathbb{Q}$. Sei $a_0, a_1, \ldots, a_k \in \mathbb{Q}$. Dann sind die beiden folgenden Punkte äquivalent:*

1. *Es ist $\sum_{i=0}^{k} a_i \omega_i$ ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$.*

2. *Es ist* $\sum_{i=0}^{k} a_i\omega_i$ *ein minimal-ganzalgebraisches Element von* L *vom Grad* k *bezüglich* $(\omega_0, \omega_1, \ldots, \omega_l)$.

Beweis. Sei $\alpha = \sum_{i=0}^{k} a_i\omega_i$.

(1 ⇒ 2) Es ist $a_k > 0$. Es ist $\alpha \in O \cap L = O_L$. Wenn $b_0, b_1, \ldots, b_k \in \mathbb{Q}$ ist, $b_k > 0$ und $\sum_{i=0}^{k} b_i\omega_i \in O_L$ ist, dann ist $\sum_{i=0}^{k} b_i\omega_i \in O_L \subseteq O_K$ und $a_k \leq b_k$. Es ist α ein minimal-ganzalgebraisches Element von L vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_l)$.

(2 ⇒ 1) Es ist $a_k > 0$. Es ist $\alpha \in O \cap K = O_K$. Wenn $c_0, c_1, \ldots, c_k \in \mathbb{Q}$ ist, $c_k > 0$ und $\sum_{i=0}^{k} c_i\omega_i \in O_K$ ist, dann ist $\sum_{i=0}^{k} c_i\omega_i \in O \cap L = O_L$ und $a_k \leq c_k$. Es ist α ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$.

□

Satz 3.0.6. *Sei* K *ein algebraischer Zahlkörper,* $n \in \mathbb{N} \setminus \{0, 1\}$ *und* $[K : \mathbb{Q}] = n$. *Seien* $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. *Sei* $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ *eine Basis von* K *über* $\mathbb{Q}$. *Sei* $a_i^{(l)} \in \mathbb{Q}$ *für alle* $l \in \{0, 1, \ldots, n-1\}$ *und alle* $i \in \{0, 1, \ldots, l\}$. *Sei* $a_l^{(l)} > 0$ *für alle* $l \in \{0, 1, \ldots, n-1\}$. *Sei* $\alpha_l = \sum_{i=0}^{l} a_i^{(l)}\omega_i$ *für alle* $l \in \{0, 1, \ldots, n-1\}$. *Sei* $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ *eine Ganzheitsbasis von* K *und* $k \in \{0, 1, \ldots, n-1\}$, *dann ist* α_k *ein minimal-ganzalgebraisches Element von* K *vom Grad* k *bezüglich* $(\omega_0, \omega_1, \ldots, \omega_{n-1})$.

Beweis. Sei $b_0, b_1, \ldots, b_k \in \mathbb{Q}$, $b_k > 0$ und $\sum_{i=0}^{k} b_i\omega_i \in O_K$. Da $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ eine Ganzheitsbasis von K ist, gibt es $x_0, x_1, \ldots, x_{n-1} \in \mathbb{Z}$, sodass

$$\sum_{i=0}^{k} b_i\omega_i = \sum_{j=0}^{n-1} x_j \left(\sum_{i=0}^{j} a_i^{(j)}\omega_i \right)$$

ist. Wenn $x_{n-1} \neq 0$ ist, dann sei $l = n - 1$. Wenn $x_{n-1} = 0$ ist, dann sei

$$l = \min \left\{ j \in \{0, 1, \ldots, n-1\} \mid x_{j+1} = x_{j+2} = \ldots = x_{n-1} = 0 \right\}.$$

Es gilt, dass

$$\sum_{i=0}^{k} b_i\omega_i = \sum_{j=0}^{l} x_j \left(\sum_{i=0}^{j} a_i^{(j)}\omega_i \right) = \sum_{j=0}^{l-1} x_j \left(\sum_{i=0}^{j} a_i^{(j)}\omega_i \right) + x_l \left(\sum_{i=0}^{l-1} a_i^{(l)}\omega_i \right) + x_l a_l^{(l)}\omega_l$$

ist. Da $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ ist, folgt, dass $l = k$ und $x_l a_l^{(l)} = b_k$ ist. Es folgt, dass $a_k^{(k)} | b_k$ und $a_k^{(k)} \leq b_k$ ist. Es ist α_k ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$. □

Die Beweisidee des folgenden Satzes stammt aus dem Satz 7.2.7 in dem Buch von Alaca und Williams [2].

Lemma 3.0.7. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$. Sei M_l für alle $l \in \{0,1,\ldots,n-1\}$ die Menge aller $A \in M(n,n,\mathbb{Q})$, für die es $a_{i,j} \in \mathbb{Q}$ für alle $i,j \in \{0,1,\ldots,n-1\}$ gibt, sodass die folgenden fünf Punkte erfüllt sind:*

1. *$A = \left(a_{i,j}\right)_{0 \leq i,j \leq n-1}$*
2. *$a_{i,l} \geq 0$ für alle $i \in \{0,1,\ldots,l\}$*
3. *Wenn $l \neq n-1$ ist, dann ist $a_{i,j} = 0$ für alle $i \in \{0,1,\ldots,l\}$ und alle $j \in \{l+1, l+2, \ldots, n-1\}$.*
4. *Wenn $l \leq n-3$ ist, dann ist $a_{i,j} = 0$ für alle $i \in \{l+1, l+2, \ldots, n-2\}$ und $j \in \{i+1, i+2, \ldots, n-1\}$.*
5. *Es ist $\left(A\left(\omega_0, \omega_1, \ldots, \omega_{n-1}\right)^T\right)^T$ eine Ganzheitsbasis von K.*

Sei $k \in \{1,2,\ldots,n-1\}$ und $M_k \neq \emptyset$, dann ist $M_{k-1} \neq \emptyset$.

Beweis. Wenn $A \in M_k$ ist, $a_{i,j} \in \mathbb{Q}$ für alle $i,j \in \{0,1,\ldots,n-1\}$ ist und $A = \left(a_{i,j}\right)_{0 \leq i,j \leq n-1}$ ist, dann gibt es ein $l \in \{0,1,\ldots,k\}$, sodass $a_{l,k} \neq 0$ ist. Sei f eine Abbildung von M_k nach $\mathbb{Q}$. Wenn $A \in M_k$ ist, $a_{i,j} \in \mathbb{Q}$ für alle $i,j \in \{0,1,\ldots,n-1\}$ ist und $A = \left(a_{i,j}\right)_{0 \leq i,j \leq n-1}$ ist, dann sei

$$f(A) = \min\left(\{a_{i,k} \mid i \in \{0,1,\ldots,k\}\} \setminus \{0\}\right).$$

Aus dem Satz 3.0.3 folgt, dass das Minimum der Menge $\{f(A) \mid A \in M_k\}$ existiert. Sei $A \in M_k$, $a_{i,j} \in \mathbb{Q}$ für alle $i,j \in \{0,1,\ldots,n-1\}$, $A = \left(a_{i,j}\right)_{0 \leq i,j \leq n-1}$ und

$$a_{k,k} = \min\left\{f(A) \mid A \in M_k\right\}.$$

Sei $m_i = \left\lfloor \frac{a_{i,k}}{a_{k,k}} \right\rfloor$ für alle $i \in \{0,1,\ldots,k-1\}$. Sei

$$B = \begin{pmatrix}
1 & 0 & \ldots & \ldots & 0 & -m_0 & 0 & \ldots & \ldots & 0 \\
0 & 1 & \ddots & & 0 & -m_1 & 0 & \ldots & \ldots & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots & & & \vdots \\
\vdots & & \ddots & \ddots & 0 & \vdots & \vdots & & & \vdots \\
\vdots & & & \ddots & 1 & -m_{k-1} & \vdots & & & \vdots \\
\vdots & & & & \ddots & 1 & 0 & & & \vdots \\
\vdots & & & & & \ddots & 1 & \ddots & & \vdots \\
\vdots & & & & & & \ddots & \ddots & \ddots & \vdots \\
\vdots & & & & & & & \ddots & 1 & 0 \\
0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 0 & 1
\end{pmatrix}.$$

Es ist $\det(B) = 1$. Aus dem Satz 1.2.19 folgt, dass

$$d\left(\left(BA\left(\omega_0, \omega_1, \ldots, \omega_{n-1}\right)^T\right)^T\right) = d\left(\left(A\left(\omega_0, \omega_1, \ldots, \omega_{n-1}\right)^T\right)^T\right)$$

ist. Es ist

$$d\left(\left(BA\left(\omega_0, \omega_1, \ldots, \omega_{n-1}\right)^T\right)^T\right) = d\left(\left(A\left(\omega_0, \omega_1, \ldots, \omega_{n-1}\right)^T\right)^T\right) = d(K).$$

Aus dem Satz 1.2.22 folgt, dass $\left(BA\left(\omega_0, \omega_1, \ldots, \omega_{n-1}\right)^T\right)^T$ eine Ganzheitsbasis von K ist. Es ist

$$0 \leq \frac{a_{i,k}}{a_{k,k}} - m_i = \frac{a_{i,k}}{a_{k,k}} - \left\lfloor \frac{a_{i,k}}{a_{k,k}} \right\rfloor < 1$$

für alle $i \in \{0, 1, \ldots, k-1\}$. Es folgt, dass $0 \leq a_{i,k} - m_i a_{k,k} < a_{k,k}$ für alle $i \in \{0, 1, \ldots, k-1\}$ ist. Es ist

$$\left(\sum_{j=0}^{k} a_{i,j}\omega_j\right) - m_i\left(\sum_{j=0}^{k} a_{k,j}\omega_j\right) = \left(\sum_{j=0}^{k-1}\left(a_{i,j} - m_i a_{k,j}\right)\omega_j\right) + \left(a_{i,k} - m_i a_{k,k}\right)\omega_k$$

für alle $i \in \{0, 1, \ldots, k-1\}$. Es ist $BA \in M_k$. Auf Grund der Minimalitätseigenschaft folgt, dass $a_{i,k} - m_i a_{k,k} = 0$ für alle $i \in \{0, 1, \ldots, k-1\}$ ist. Sei

$$c_{i,i} = \begin{cases} 1 & \text{wenn } a_{i,k-1} - m_i a_{k,k-1} \geq 0 \\ -1 & \text{wenn } a_{i,k-1} - m_i a_{k,k-1} < 0 \end{cases}$$

für alle $i \in \{0, 1, \ldots, k-1\}$. Sei $c_{i,i} = 1$ für alle $i \in \{k, k+1, \ldots, n-1\}$. Sei $c_{i,j} = 0$ für alle $i, j \in \{0, 1, \ldots, n-1\}$, für die $i \neq j$ gilt. Sei $C = \left(c_{i,j}\right)_{0 \leq i,j \leq n-1}$. Es ist $\det(C) \in \{-1, 1\}$. Aus dem Satz 1.2.19 folgt, dass

$$d\left(CBA\left(\omega_0, \omega_1, \ldots, \omega_{n-1}\right)^T\right)^T = d\left(BA\left(\omega_0, \omega_1, \ldots, \omega_{n-1}\right)^T\right)^T$$

ist. Es ist

$$d\left(CBA\left(\omega_0, \omega_1, \ldots, \omega_{n-1}\right)^T\right)^T = d\left(BA\left(\omega_0, \omega_1, \ldots, \omega_{n-1}\right)^T\right)^T = d(K).$$

Aus dem Satz 1.2.22 folgt, dass $\left(CBA\left(\omega_0, \omega_1, \ldots, \omega_{n-1}\right)^T\right)^T$ eine Ganzheitsbasis von K ist. Es ist $CAB \in M_{k-1}$. □

Lemma 3.0.8. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0, 1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ und $z \in \{0, 1, \ldots, n-1\}$, dann gibt es $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in O_K$ und $a_{i,j} \in \mathbb{Q}$ für alle $i \in \{0, 1, \ldots, n-1\}$ und alle $j \in \{0, 1, \ldots, \max\{n-1-z, i\}\}$, sodass $\alpha_i = \sum_{j=0}^{\max\{n-1-z,i\}} a_{i,j}\omega_j$ für alle $i \in \{0, 1, \ldots, n-1\}$ ist und $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ eine Ganzheitsbasis von K ist.*

Beweis. Es wird Induktion nach z durchgeführt.

Anfang Sei $z = 0$. Sei $\left(\alpha_0^{(0)}, \alpha_1^{(0)}, \ldots, \alpha_{n-1}^{(0)}\right)$ eine Ganzheitsbasis von K. Es gibt $a_{i,j}^{(0)} \in \mathbb{Q}$ für alle $i, j \in \{0, 1, \ldots, n-1\}$, sodass $\alpha_i^{(0)} = \sum_{j=0}^{n-1} a_{i,j}^{(0)} \omega_j$ für alle $i \in \{0, 1, \ldots, n-1\}$ ist. Das Lemma 3.0.8 ist für $z = 0$ gezeigt.

Sei $z \in \{1, 2, \ldots, n-1\}$.

Annahme Es gibt $\alpha_0^{(z-1)}, \alpha_1^{(z-1)}, \ldots, \alpha_{n-1}^{(z-1)} \in O_K$ und $a_{i,j}^{(z-1)} \in \mathbb{Q}$ für alle $i \in \{0, 1, \ldots, n-1\}$ und alle $j \in \{0, 1, \ldots, \max\{n-z, i\}\}$, sodass

$$\alpha_i^{(z-1)} = \sum_{j=0}^{\max\{n-z,i\}} a_{i,j}^{(z-1)} \omega_j$$

für alle $i \in \{0, 1, \ldots, n-1\}$ ist und $\left(\alpha_0^{(z-1)}, \alpha_1^{(z-1)}, \ldots, \alpha_{n-1}^{(z-1)}\right)$ eine Ganzheitsbasis von K ist.

Schritt $(z-1 \to z)$ O.B.d.A sei $a_{i,n-z}^{(z-1)} \geq 0$ für alle $i \in \{0, 1, \ldots, n-z\}$. Sei $a_{i,j}^{(z-1)} = 0$ für alle $i \in \{0, 1, \ldots, n-2\}$ und alle

$$j \in \{\max\{n-z, i\} + 1, \max\{n-z, i\} + 2, \ldots, n-1\}.$$

Sei $A = \left(a_{i,j}^{(z-1)}\right)_{0 \leq i,j \leq n-1}$. Sei M_l wie in Lemma 3.0.7 für alle $l \in \{0, 1, \ldots, n-1\}$ die Menge aller $B \in M(n, n, \mathbb{Q})$, für die es $b_{i,j} \in \mathbb{Q}$ für alle $i, j \in \{0, 1, \ldots, n-1\}$ gibt, sodass die folgenden fünf Punkte erfüllt sind:

1. $B = \left(b_{i,j}\right)_{0 \leq i,j \leq n-1}$
2. $b_{i,l} \geq 0$ für alle $i \in \{0, 1, \ldots, l\}$
3. Wenn $l \neq n-1$ ist, dann ist $b_{i,j} = 0$ für alle $i \in \{0, 1, \ldots, l\}$ und alle $j \in \{l+1, l+2, \ldots, n-1\}$.
4. Wenn $l \leq n-3$ ist, dann ist $b_{i,j} = 0$ für alle $i \in \{l+1, l+2, \ldots, n-2\}$ und $j \in \{i+1, i+2, \ldots, n-1\}$.
5. Es ist $\left(B\left(\omega_0, \omega_1, \ldots, \omega_{n-1}\right)^T\right)^T$ eine Ganzheitsbasis von K.

Es ist $A \in M_{n-z}$. Aus dem Lemma 3.0.7 folgt, dass es ein $C \in M_{n-1-z}$ gibt. Sei $c_{i,j} \in \mathbb{Q}$ und $C = \left(c_{i,j}\right)_{0 \leq i,j \leq n-1}$. Sei $\alpha_i^{(z)} = \sum_{j=0}^{\max\{n-1-z,i\}} c_{i,j} \omega_j$ für alle $i \in \{0, 1, \ldots, n-1\}$. Es ist $\left(\alpha_0^{(z)}, \alpha_1^{(z)}, \ldots, \alpha_{n-1}^{(z)}\right)$ eine Ganzheitsbasis von K.

□

Satz 3.0.9. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0, 1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$, dann gibt es $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in O_K$ und $a_{i,j} \in \mathbb{Q}$ für alle $i \in \{0, 1, \ldots, n-1\}$ und $j \in \{0, 1, \ldots, i\}$, sodass*

$\alpha_i = \sum_{j=0}^{i} a_{i,j}\omega_j$ *für alle* $i \in \{0, 1, \ldots, n-1\}$ *ist und* $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ *eine Ganzheitsbasis von* K *ist.*

Beweis. Wird in dem Satz 3.0.8 $z = n - 1$ gewählt, dann folgt der Satz 3.0.9. □

Der folgende Satz ist mit dem Satz 7.2.7 in dem Buch von Alaca und Williams [2] vergleichbar, wenn $(\omega_0, \omega_1, \ldots, \omega_{n-1}) = \left(1, \theta, \ldots, \theta^{n-1}\right)$ für ein primitives Element $\theta \in O_K$ ist. Der Beweis folgt zum Teil dem Beweis des Satzes 7.2.7 in [2], wobei der Beweis für die Basis $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ von K über $\mathbb{Q}$ verallgemeinert wird. Es wird ein Teil des Beweises in den Satz 3.0.9 ausgelagert.

Satz 3.0.10. *Sei* K *ein algebraischer Zahlkörper,* $n \in \mathbb{N} \setminus \{0, 1\}$ *und* $[K : \mathbb{Q}] = n$. *Seien* $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. *Sei* $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ *eine Basis von* K *über* $\mathbb{Q}$. *Sei* α_k *ein minimal-ganzalgebraisches Element von* K *vom Grad* k *bezüglich* $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ *für alle* $k \in \{0, 1, \ldots, n-1\}$. *Dann ist* $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ *eine Ganzheitsbasis von* K.

Beweis. Aus dem Satz 3.0.9 folgt, dass es $\beta_0, \beta_1, \ldots, \beta_{n-1} \in O_K$ und $b_{i,j} \in \mathbb{Q}$ für alle $i \in \{0, 1, \ldots, n-1\}$ und alle $j \in \{0, 1, \ldots, i\}$ gibt, sodass $\beta_i = \sum_{j=0}^{i} b_{i,j}\omega_j$ für alle $i \in \{0, 1, \ldots, n-1\}$ ist und $(\beta_0, \beta_1, \ldots, \beta_{n-1})$ eine Ganzheitsbasis von K ist. O.B.d.A sei $b_{i,i} \geq 0$ für alle $i \in \{0, 1, \ldots, n-1\}$. Aus dem Satz 1.2.20 folgt, dass

$$d(\beta_0, \beta_1, \ldots, \beta_{n-1}) = b_{0,0}^2 \ldots b_{n-1,n-1}^2 d(\omega_0, \omega_1, \ldots, \omega_{n-1})$$

ist. Es ist

$$d(K) = d(\beta_0, \beta_1, \ldots, \beta_{n-1}) = b_{0,0}^2 b_{1,1}^2 \ldots b_{n-1,n-1}^2 d(\omega_0, \omega_1, \ldots, \omega_{n-1}).$$

Sei $a_{i,j} \in \mathbb{Q}$ für alle $i \in \{0, 1, \ldots, n-1\}$ und alle $j \in \{0, 1, \ldots, i\}$ und $\alpha_i = \sum_{j=0}^{i} a_{i,j}\omega_j$ für alle $i \in \{0, 1, \ldots, n-1\}$. Aus dem Satz 1.2.20 folgt, dass

$$d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) = a_{0,0}^2 a_{1,1}^2 \ldots a_{n-1,n-1}^2 d(\omega_0, \omega_1, \ldots, \omega_{n-1})$$

ist. Aus dem Satz 1.2.24 folgt, dass $d(\omega_0, \omega_1, \ldots, \omega_{n-1}) \neq 0$ ist. Es ist $d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \neq 0$. Aus dem Satz 1.2.21 folgt, dass $|d(K)| \leq |d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})|$ ist. Es folgt, dass

$$b_{0,0} b_{1,1} \ldots b_{n-1,n-1} \leq a_{0,0} a_{1,1} \ldots a_{n-1,n-1}$$

ist. Da α_k für alle $k \in \{0, 1, \ldots, n-1\}$ ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ ist, gilt, dass $a_{i,i} \leq b_{i,i}$ für alle $i \in \{0, 1, \ldots, n-1\}$ ist. Es folgt, dass $a_{i,i} = b_{i,i}$ für alle $i \in \{0, 1, \ldots, n-1\}$ ist. Es ist $d(K) = d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$. Aus dem Satz 1.2.22 folgt, dass $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ eine Ganzheitsbasis von K ist. □

Der folgende Satz ist mit dem Satz 7.2.3 in dem Buch von Alaca und Williams [2] vergleichbar, wenn $(\omega_0, \omega_1, \ldots, \omega_{n-1}) = \left(1, \theta, \ldots, \theta^{n-1}\right)$ für ein primitives Element $\theta \in O_K$ ist. Der Beweis folgt im Wesentlichen dem Beweis des Satzes 7.2.3 in [2], wobei der Beweis für die Basis $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ von K über $\mathbb{Q}$ verallgemeinert wird.

Satz 3.0.11. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ und $k \in \{0, 1, \ldots, n-1\}$. Sei $a_i \in \mathbb{Q}$ und $b_i \in \mathbb{Q}$ für alle $i \in \{0, 1, \ldots, k\}$. Sei $\sum_{i=0}^{k} a_i \omega_i$ ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ und $\sum_{i=0}^{k} b_i \omega_i \in O_K$, dann gibt es ein $z \in \mathbb{Z}$, sodass $z a_k = b_k$ ist.*

Beweis. Es ist $a_k > 0$. Sei $m = \min\{l \in \mathbb{N} \setminus \{0\} \mid l b_k \in \mathbb{Z},\ l a_k \in \mathbb{N}\}$. Es gibt $q, r \in \mathbb{Z}$, sodass $m b_k = q m a_k + r$ und $0 \leq r < m a_k$ ist. Es ist $b_k = q a_k + \frac{r}{m}$ und $0 \leq \frac{r}{m} < a_k$. Es gilt, dass

$$\left(\sum_{i=0}^{k-1} (b_i - q a_i)\, \omega_i\right) + \frac{r}{m}\omega_k = \left(\sum_{i=0}^{k-1} (b_i - q a_i)\, \omega_i\right) + (b_k - q a_k)\, \omega_k = \left(\sum_{i=0}^{k} b_i \omega_i\right) - q \left(\sum_{i=0}^{k} a_i \omega_i\right) \in O_K$$

ist. Es ist $\frac{r}{m} \leq 0$ oder $\frac{r}{m} \geq a_k$. Es folgt, dass $\frac{r}{m} = 0$ und $b_k = q a_k$ ist. □

Der folgende Satz ist mit dem Satz 7.2.4 in dem Buch von Alaca und Williams [2] vergleichbar, wenn $(\omega_0, \omega_1, \ldots, \omega_{n-1}) = \left(1, \theta, \ldots, \theta^{n-1}\right)$ für ein primitives Element $\theta \in O_K$ ist.

Satz 3.0.12. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ und $k \in \{0, 1, \ldots, n-1\}$. Seien $a_0, a_1, \ldots, a_k \in \mathbb{Q}$. Sei $\sum_{i=0}^{k} a_i \omega_i$ ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$, dann gibt es ein $d \in \mathbb{N} \setminus \{0\}$, sodass $a_k = \frac{1}{d}$ ist.*

Beweis. Sei $\alpha = \sum_{i=0}^{k} a_i \omega_i$. Es ist $a_k > 0$. Da $\omega_k \in O_K$ ist, folgt, dass $a_k \leq 1$ ist. Sei $m = \max\{l \in \mathbb{N} \setminus \{0\} \mid l a_k \leq 1\}$. Es ist $(1 + m)\, a_k > 1$. Es folgt, dass $1 - m a_k < a_k$ ist. Es ist $-m \left(\sum_{i=0}^{k-1} a_i \omega_i\right) + (1 - m a_k)\, \omega_k = -m\alpha + \omega_k \in O_K$. Da α ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ ist, folgt, dass $1 - m a_k \leq 0$ ist. Es ist $1 - m a_k \geq 0$ und $1 - m a_k = 0$. Sei $r, s \in \mathbb{N} \setminus \{0\}$, $\mathrm{ggT}(r, s) = 1$ und $a_k = \frac{r}{s}$. Es ist $0 = 1 - m a_k = 1 - m\frac{r}{s}$ und $s = mr$. Da $\mathrm{ggT}(r, s) = 1$ ist, folgt, dass $r = 1$ ist. □

Satz 3.0.13. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$, $\omega_0 = 1$ und α ein minimal-ganzalgebraisches Element von K vom Grad 0 bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$, dann ist $\alpha = 1$.*

Beweis. Es ist $\alpha \in \mathbb{Q} \cap O = \mathbb{Z}$. Aus dem Satz 3.0.12 folgt, dass $\alpha = 1$ ist. □

Der folgende Satz stammt im Wesentlichen aus dem Buch von Alaca und Williams [2][2]. Der Beweis folgt im Wesentlichen dem Beweis des Satzes 7.2.5 in [2].

Satz 3.0.14. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N}$, $n \geq 3$, $[K : \mathbb{Q}] = n$, $\theta \in O_K$, $K = \mathbb{Q}(\theta)$ und $k \in \{2, 3, \ldots, n-1\}$. Seien $a_0, a_1, \ldots, a_{k-2} \in \mathbb{Q}$. Seien $b_0, b_1, \ldots, b_{k-1} \in \mathbb{Q}$. Seien $d_{k-1}, d_k \in \mathbb{N} \setminus \{0\}$. Sei $\alpha = \sum_{i=0}^{k-2} a_i \theta^i + \frac{1}{d_{k-1}} \theta^{k-1}$ und $\beta = \sum_{i=0}^{k-1} b_i \theta^i + \frac{1}{d_k} \theta^k$. Sei α ein minimal-ganzalgebraisches Element von K vom Grad $k-1$ bezüglich $(1, \theta, \ldots, \theta^{n-1})$ und β ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(1, \theta, \ldots, \theta^{n-1})$, dann ist $d_{k-1} \mid d_k$.*

Beweis. Es ist $\sum_{i=0}^{k-2} a_i \theta^{i+1} + \frac{1}{d_{k-1}} \theta^k = \alpha\theta \in O_K$. Aus dem Satz 3.0.11 folgt, dass es ein $x \in \mathbb{Z}$ gibt, sodass $\frac{1}{d_{k-1}} = x \frac{1}{d_k}$ ist. Es folgt, dass $d_k = x d_{k-1}$ ist. Es ist $d_{k-1} \mid d_k$. □

Der folgende Satz ist mit einem Teil des Satzes 7.2.6 in dem Buch von Alaca und Williams [2] vergleichbar. Der Beweis des folgenden Satzes folgt zum Teil dem Beweis des Satzes 7.2.6 in [2].

Satz 3.0.15. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$, $[K : \mathbb{Q}] = n$, $\theta \in O_K$, $K = \mathbb{Q}(\theta)$, $k \in \{1, 2, \ldots, n-1\}$ und α ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(1, \theta, \ldots, \theta^{n-1})$, dann gibt es $x_0, x_1, \ldots, x_{k-1} \in \mathbb{Z}$ und $d \in \mathbb{N} \setminus \{0\}$, sodass*

$$\alpha = \frac{x_0 + x_1\theta + \ldots + x_{k-1}\theta^{k-1} + \theta^k}{d}$$

ist.

Beweis. Es wird Induktion nach k durchgeführt.

Anfang Sei $k = 1$. Seien $a_0, a_1 \in \mathbb{Q}$ und $\alpha = a_0 + a_1\theta$. Aus dem Satz 3.0.12 folgt, dass es ein $d_1 \in \mathbb{N} \setminus \{0\}$ gibt, sodass $a_1 = \frac{1}{d_1}$ ist. Es ist $d_1 a_0 = d_1\alpha - \theta \in O_K$. Aus dem Satz 1.2.11 folgt, dass $O \cap \mathbb{Q} = \mathbb{Z}$ ist. Es ist $d_1 a_0 \in O \cap \mathbb{Q} = \mathbb{Z}$. Es ist $\alpha = \frac{d_1 a_0 + \theta}{d_1}$.

Sei $k \in \{2, 3, \ldots, n-1\}$.

[2] Siehe Satz 7.2.5 in [2].

Annahme Wenn β ein minimal-ganzalgebraisches Element von K vom Grad $k-1$ bezüglich $(1, \theta, \ldots, \theta^{n-1})$ ist, dann gibt es $y_0, y_1, \ldots, y_{k-2} \in \mathbb{Z}$ und $d_{k-1} \in \mathbb{N} \setminus \{0\}$, sodass $\beta = \frac{y_0 + y_1\theta + \ldots + y_{k-2}\theta^{k-2} + \theta^{k-1}}{d_{k-1}}$ ist.

Schritt Sei α ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $(1, \theta, \ldots, \theta^{n-1})$. Sei $b_0, b_1, \ldots, b_k \in \mathbb{Q}$ und $\alpha = \sum_{i=0}^{k} b_i\theta^i$. Aus dem Satz 3.0.12 folgt, dass es ein $d_k \in \mathbb{N} \setminus \{0\}$ gibt, sodass $b_k = \frac{1}{d_k}$ ist. Sei γ ein minimal-ganzalgebraisches Element von K vom Grad $k-1$ bezüglich $(1, \theta, \ldots, \theta^{n-1})$. Aus der Induktionsannahme folgt, dass es $z_0, z_1, \ldots, z_{k-2} \in \mathbb{Z}$ und $d_{k-1} \in \mathbb{N} \setminus \{0\}$ gibt, sodass

$$\gamma = \frac{1}{d_{k-1}} \left(\left(\sum_{i=0}^{k-2} z_i\theta^i \right) + \theta^{k-1} \right)$$

ist. Aus dem Satz 3.0.14 folgt, dass $d_{k-1} \mid d_k$ ist. Sei $\lambda = \frac{d_k}{d_{k-1}} b_0 + \sum_{i=1}^{k-1} \frac{d_k b_i - z_{i-1}}{d_{k-1}} \theta^i$. Es ist

$$\lambda = \frac{d_k}{d_{k-1}} \sum_{i=0}^{k-1} b_i\theta^i - \frac{1}{d_{k-1}} \sum_{i=0}^{k-2} z_i\theta^{i+1} =$$

$$\frac{d_k}{d_{k-1}} \left(\left(\sum_{i=0}^{k-1} b_i\theta^i \right) + \frac{1}{d_k}\theta^k \right) - \frac{\theta}{d_{k-1}} \left(\left(\sum_{i=0}^{k-2} z_i\theta^i \right) + \theta^{k-1} \right) = \frac{d_k}{d_{k-1}}\alpha - \theta\gamma.$$

Es ist $\lambda \in O_K$. Aus dem Satz 3.0.11 folgt, dass es ein $u \in \mathbb{Z}$ gibt, sodass $\frac{d_k b_{k-1} - z_{k-2}}{d_{k-1}} = \frac{u}{d_{k-1}}$ ist. Es folgt, dass $d_k b_{k-1} - z_{k-2} = u$ ist und $d_k b_{k-1} \in \mathbb{Z}$ ist. Sei $m = 1 + z_{k-2} - d_k b_{k-1}$. Sei $\mu = \lambda + m\gamma$. Es ist $\mu \in O_K$. Es gilt, dass

$$\mu = \frac{1}{d_{k-1}} \left(d_k b_0 + mz_0 + \left(\sum_{i=1}^{k-2} \left(d_k b_i - z_{i-1} + mz_i \right) \theta^i \right) + \theta^{k-1} \right)$$

ist. Es ist μ ein minimal-ganzalgebraisches Element von K vom Grad $k-1$ bezüglich $(1, \theta, \ldots, \theta^{n-1})$. Aus der Induktionsannahme folgt, dass es $v_0, v_1, \ldots, v_{k-2} \in \mathbb{Z}$ gibt, sodass

$$\mu = \frac{1}{d_{k-1}} \left(\left(\sum_{i=0}^{k-2} v_i\theta^i \right) + \theta^{k-1} \right)$$

ist. Werden die Koeffizienten verglichen, dann folgt, dass $v_0 = d_k b_0 + mz_0$ und $v_i = d_k b_i - z_{i-1} + mz_i$ für alle $i \in \{1, 2, \ldots, k-2\}$ ist. Es folgt, dass $d_k b_i \in \mathbb{Z}$ für alle $i \in \{0, 1, \ldots, k-1\}$ ist. Es ist

$$\alpha = \left(\sum_{i=0}^{k-1} b_i\theta^i \right) + \frac{1}{d_k}\theta^k = \frac{1}{d_k} \left(\left(\sum_{i=0}^{k-1} d_k b_i\theta^i \right) + \theta^k \right).$$

□

4 minimal-ganz über $\mathbb{Z}_{(p)}$

Dieses Kapitel folgt zum Teil der Doktorarbeit von Alaca [1]. Einige Sätze werden nicht für eine Basis $\left(1,\theta,\ldots,\theta^{n-1}\right)$ über $\mathbb{Q}$ für ein primitives Element $\theta \in O_K$ gezeigt, sondern etwas allgemeiner für eine beliebige Basis über $\mathbb{Q}$ mit ganzalgebraischen Elementen.

Der folgende Satz ist mit dem Lemma 1.3.1 in der Doktorarbeit von Alaca [1] vergleichbar, wenn $(\omega_0,\omega_1,\ldots,\omega_{n-1}) = \left(1,\theta,\ldots,\theta^{n-1}\right)$ für ein primitives Element $\theta \in O_K$ ist. Der Beweis folgt im Wesentlichen dem Beweis des Lemmas 1.3.1 in [1], wobei der Beweis für die Basis $(\omega_0,\omega_1,\ldots,\omega_{n-1})$ von K über $\mathbb{Q}$ verallgemeinert wird.

Satz 4.0.1. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N}\setminus\{0,1\}$ und $[K:\mathbb{Q}] = n$. Seien $\omega_0,\omega_1,\ldots,\omega_{n-1} \in O_K$. Sei $(\omega_0,\omega_1,\ldots,\omega_{n-1})$ eine Basis von K über $\mathbb{Q}$, p eine Primzahl, $k \in \{0,1,\ldots,n-1\}$ und $l \in \mathbb{N}$. Wenn $k \geq 1$ ist, dann seien $x_0,x_1,\ldots,x_{k-1} \in \mathbb{Z}$. Sei $\alpha \in O_{p,K}$. Wenn $k = 0$ ist, dann sei $\alpha = \frac{\omega_k}{p^l}$. Wenn $k \geq 1$ ist, dann sei*

$$\alpha = \frac{1}{p^l}\left(\left(\sum_{i=0}^{k-1} x_i\omega_i\right) + \omega_k\right).$$

Dann ist $l \leq \frac{\nu_p(d(\omega_0,\omega_1,\ldots,\omega_{n-1}))-\nu_p(d(K))}{2}$.

Beweis. Sei $(\beta_0,\beta_1,\ldots,\beta_{n-1})$ eine p-ganze Basis von K. Sei $A \in M(n,n,\mathbb{Q})$ und $(\omega_0,\ldots,\omega_{k-1},\alpha,\omega_{k+1},\ldots\omega_{n-1})^T = A\,(\omega_0,\omega_1,\ldots,\omega_{n-1})^T$. Es ist $\det(A) = \frac{1}{p^l}$. Aus dem Satz 1.2.19 folgt, dass $d(\omega_0,\ldots,\omega_{k-1},\alpha,\omega_{k+1},\ldots\omega_{n-1}) = (\det(A))^2\, d(\omega_0,\omega_1,\ldots,\omega_{n-1})$ ist. Aus dem Satz 2.0.14 folgt, dass

$$\nu_p\left(d\left(\omega_0,\ldots,\omega_{k-1},\alpha,\omega_{k+1},\ldots\omega_{n-1}\right)\right) \geq \nu_p\left(d\left(\beta_0,\beta_1,\ldots,\beta_{n-1}\right)\right)$$

ist. Es ist

$$\nu_p\left(d\left(\omega_0,\omega_1,\ldots,\omega_{n-1}\right)\right) - 2l = \nu_p\left(\left(\det(A)\right)^2 d\left(\omega_0,\omega_1,\ldots,\omega_{n-1}\right)\right) =$$
$$\nu_p\left(d\left(\omega_0,\ldots,\omega_{k-1},\alpha,\omega_{k+1},\ldots\omega_{n-1}\right)\right) \geq \nu_p\left(d\left(\beta_0,\beta_1,\ldots,\beta_{n-1}\right)\right) = \nu_p\left(d\left(K\right)\right).$$

Es ist $l \leq \frac{1}{2}\left(\nu_p\left(d\left(\omega_0,\omega_1,\ldots,\omega_{n-1}\right)\right) - \nu_p\left(d\left(K\right)\right)\right)$. □

Definition 4.0.2 (minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad k)**.** *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N}\setminus\{0,1\}$ und $[K:\mathbb{Q}] = n$. Seien $\omega_0,\omega_1,\ldots,\omega_{n-1} \in O_K$. Sei $(\omega_0,\omega_1,\ldots,\omega_{n-1})$ eine Basis von K über $\mathbb{Q}$, p eine Primzahl und $k \in \{1,2,\ldots,n-1\}$,*

dann heißt α genau dann minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$, wenn $\alpha \in O_{p,K}$ ist und es ein $l \in \mathbb{N}$ und $x_0, x_1, \ldots, x_{k-1} \in \mathbb{Z}$ gibt, sodass

$$\alpha = \frac{1}{p^l} \left(\left(\sum_{i=0}^{k-1} x_i \omega_i \right) + \omega_k \right)$$

ist und für alle $y_0, y_1, \ldots, y_{k-1} \in \mathbb{Z}$ gilt, dass

$$\frac{1}{p^{l+1}} \left(\left(\sum_{i=0}^{k-1} y_i \omega_i \right) + \omega_k \right) \notin O_{p,K}$$

ist.

Definition 4.0.3 (minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 0)**.** *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ und p eine Primzahl, dann heißt α genau dann minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 0 bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$, wenn $\alpha \in O_{p,K}$ ist und es ein $l \in \mathbb{N}$ gibt, sodass $\alpha = \frac{1}{p^l}\omega_0$ ist und $\frac{1}{p^{l+1}}\omega_0 \notin O_{p,K}$ ist.*

Satz 4.0.4. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ und p eine Primzahl. Sei $x_j^{(i)} \in \mathbb{Z}$ für alle $i \in \{1, 2, \ldots, n-1\}$ und alle $j \in \{0, 1, \ldots, i\}$. Seien $m_0, m_1, \ldots, m_{n-1} \in \mathbb{N}$. Sei $\alpha_0 = \frac{1}{p^{m_0}}\omega_0$. Sei $\alpha_i = \frac{1}{p^{m_i}} \left(\left(\sum_{j=0}^{i-1} x_j^{(i)} \omega_j \right) + \omega_i \right)$ für alle $i \in \{1, 2, \cdots, n-1\}$. Sei $(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$ eine p-ganze Basis von K und $k \in \{0, 1, \ldots, n-1\}$, dann ist α_k ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$.*

Beweis. Angenommen α_k ist kein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad k bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$. Es gibt $y_0, y_1, \ldots, y_{k-1} \in \mathbb{Z}$, sodass $\frac{1}{p^{m_k+1}} \left(\left(\sum_{i=0}^{k-1} y_i \omega_i \right) + \omega_k \right) \in O_{p,K}$ ist. Da $(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$ eine p-ganze Basis von K ist, gibt es $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_{(p)}$, sodass

$$\frac{1}{p^{m_k+1}} \left(\left(\sum_{i=0}^{k-1} y_i \omega_i \right) + \omega_k \right) = \sum_{i=0}^{n-1} \frac{a_i}{p^{m_i}} \left(\left(\sum_{j=0}^{i-1} x_j^{(i)} \omega_j \right) + \omega_i \right)$$

ist. Wenn $a_{n-1} \neq 0$ ist, dann sei $l = n-1$. Wenn $a_{n-1} = 0$ ist, dann sei

$$l = \min \left\{ i \in \{0, 1, \ldots, n-1\} \mid a_{i+1} = a_{i+2} = \ldots = a_{n-1} = 0 \right\}.$$

Es ist

$$\frac{1}{p^{m_k+1}}\left(\left(\sum_{i=0}^{k-1} y_i\omega_i\right)+\omega_k\right)=\sum_{i=0}^{n-1}\frac{a_i}{p^{m_i}}\left(\left(\sum_{j=0}^{i-1} x_j^{(i)}\omega_j\right)+\omega_i\right)=$$
$$\sum_{i=0}^{l}\frac{a_i}{p^{m_i}}\left(\left(\sum_{j=0}^{i-1} x_j^{(i)}\omega_j\right)+\omega_i\right)=$$
$$\left(\sum_{i=0}^{l-1}\frac{a_i}{p^{m_i}}\left(\left(\sum_{j=0}^{i-1} x_j^{(i)}\omega_j\right)+\omega_i\right)\right)+\frac{a_l}{p^{m_l}}\left(\sum_{j=0}^{l-1} x_j^{(l)}\omega_j\right)+\frac{a_l}{p^{m_l}}\omega_l.$$

Da $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ ist, folgt, dass $l = k$ und $\frac{a_k}{p^{m_k}} = \frac{1}{p^{m_k+1}}$ ist. Es ist $a_k = \frac{1}{p} \notin \mathbb{Z}_{(p)}$. Dies ist ein Widerspruch. □

Der folgende Satz ist mit dem Satz 1.3.4 in der Doktorarbeit von Alaca [1] vergleichbar, wenn $(\omega_0, \omega_1, \ldots, \omega_{n-1}) = \left(1, \theta, \ldots, \theta^{n-1}\right)$ für ein primitives Element $\theta \in O_K$ ist. Die nötigen Voraussetzungen können gekürzt werden, wenn $(\omega_0, \omega_1, \ldots, \omega_{n-1}) = \left(1, \theta, \ldots, \theta^{n-1}\right)$ ist, da der Satz 3.0.14 und der Satz 3.0.15 angewendet werden können. Der Beweis des folgenden Satzes folgt zum Teil dem Beweis des Satzes 1.3.4 in [1], wobei der Beweis für die Basis $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ von K über $\mathbb{Q}$ verallgemeinert wird. Der Beweis wird etwas kürzer, da der Satz 4.0.4 zur Verfügung steht.

Satz 4.0.5. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0, 1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ und p eine Primzahl. Sei $y_j^{(i)} \in \mathbb{Z}$ für alle $i \in \{1, 2, \ldots, n-1\}$ und alle $j \in \{0, 1, \ldots, i-1\}$. Seien $d_0, d_1, \ldots, d_{n-1} \in \mathbb{N} \setminus \{0\}$. Sei $\beta_0 = \frac{1}{d_0}\omega_0$. Sei $\beta_i = \frac{1}{d_i}\left(\left(\sum_{j=0}^{i-1} y_j^{(i)}\omega_j\right)+\omega_i\right)$ für alle $i \in \{1, 2, \cdots, n-1\}$. Sei β_i ein minimal-ganzalgebraisches Element von K vom Grad i bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ für alle $i \in \{0, 1, \ldots, n-1\}$. Sei $d_{i-1} \mid d_i$ für alle $i \in \{1, 2, \ldots, n-1\}$. Seien $k_0, k_1, \ldots, k_{n-1} \in \mathbb{N}$. Sei $x_j^{(i)} \in \mathbb{Z}$ für alle $i \in \{1, 2, \ldots, n-1\}$ und alle $j \in \{0, 1, \ldots, i-1\}$. Sei $\alpha_0 = \frac{1}{p^{k_0}}\omega_0$. Sei $\alpha_i = \frac{1}{p^{k_i}}\left(\left(\sum_{j=0}^{i-1} x_j^{(i)}\omega_j\right)+\omega_i\right)$ für alle $i \in \{1, 2, \cdots, n-1\}$. Sei α_i ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad i bezüglich $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ für alle $i \in \{0, 1, \ldots, n-1\}$. Dann sind alle drei folgenden Punkte erfüllt:*

1. $0 \leq k_0 \leq k_1 \leq \ldots \leq k_{n-1}$
2. *Es ist $(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$ eine p-ganze Basis von K.*
3. $\nu_p\left(d(K)\right) = \nu_p\left(d(\omega_0, \omega_1, \ldots, \omega_{n-1})\right) - 2\left(\sum_{i=0}^{n-1} k_i\right)$

Beweis. Aus dem Satz 3.0.10 folgt, dass $(\beta_0, \beta_1, \ldots, \beta_{n-1})$ eine Ganzheitsbasis von K ist.

Aus dem Satz 1.2.20 folgt, dass

$$d(\beta_0, \beta_1, \ldots, \beta_{n-1}) = \left(\prod_{i=0}^{n-1} \frac{1}{d_i^2} \right) d(\omega_0, \omega_1, \ldots, \omega_{n-1})$$

ist. Es ist

$$d(K) = d(\beta_0, \beta_1, \ldots, \beta_{n-1}) = \left(\prod_{i=0}^{n-1} \frac{1}{d_i^2} \right) d(\omega_0, \omega_1, \ldots, \omega_{n-1}).$$

Es ist $d(\omega_0, \omega_1, \ldots, \omega_{n-1}) = \left(\prod_{i=0}^{n-1} d_i^2 \right) d(K)$. Aus dem Satz 2.0.13 folgt, dass $(\beta_0, \beta_1, \ldots, \beta_{n-1})$ eine p-ganze Basis von K ist. Sei $m_i = \nu_p(d_i)$ für alle $i \in \{0, 1, \ldots, n-1\}$. Sei $b_{i,j} = \frac{\delta_{i,j} d_i}{p^{m_i}}$ für alle $i, j \in \{0, 1, \ldots, n-1\}$. Sei $B = \left(b_{i,j}\right)_{0 \leq i,j \leq n-1}$. Sei $\gamma_i = \sum_{j=0}^{n-1} b_{ij} \beta_j$ für alle $i \in \{0, 1, \ldots, n-1\}$. Es ist $\det(B) = \prod_{i=0}^{n-1} \frac{d_i}{p^{m_i}} \neq 0$. Es ist

$$\nu_p(\det(B)) = \nu_p \left(\prod_{i=0}^{n-1} \frac{d_i}{p^{m_i}} \right) = \sum_{i=0}^{n-1} \nu_p \left(\frac{d_i}{p^{m_i}} \right) = 0.$$

Aus dem Satz 2.0.15 folgt, dass $(\gamma_0, \gamma_1, \ldots, \gamma_{n-1})$ eine p-ganze Basis von K ist. Da $d_{i-1} \mid d_i$ für alle $i \in \{1, 2, \ldots, n-1\}$ ist, folgt, dass $m_{i-1} = \nu_p(d_{i-1}) \leq \nu_p(d_i) = m_i$ für alle $i \in \{1, 2, \ldots, n-1\}$ ist. Es ist

$$\gamma_i = \sum_{j=0}^{n-1} b_{ij} \beta_j = b_{ii} \beta_i = \frac{1}{p^{m_i}} \left(\left(\sum_{j=0}^{i-1} y_j^{(i)} \omega_j \right) + \omega_i \right)$$

für alle $i \in \{0, 1, \ldots, n-1\}$. Es ist $m_i \leq k_i$ für alle $i \in \{0, 1, \ldots, n-1\}$. Aus dem Satz 2.0.14 folgt, dass $\nu_p\left(d(\gamma_0, \gamma_1, \ldots, \gamma_{n-1})\right) \leq \nu_p\left(d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})\right)$ ist. Aus dem Satz 1.2.20 folgt, dass

$$d(\gamma_0, \gamma_1, \ldots, \gamma_{n-1}) = \left(\prod_{i=0}^{n-1} \frac{1}{p^{2m_i}} \right) d(\omega_0, \omega_1, \ldots, \omega_{n-1})$$

und

$$d(\alpha_0, \alpha_1 \ldots, \alpha_{n-1}) = \left(\prod_{i=0}^{n-1} \frac{1}{p^{2k_i}} \right) d(\omega_0, \omega_1, \ldots, \omega_{n-1})$$

ist. Es ist

$$(-2) \left(\sum_{i=0}^{n-1} m_i \right) + \nu_p\left(d(\omega_0, \omega_1, \ldots, \omega_{n-1})\right) =$$
$$\nu_p\left(d(\gamma_0, \gamma_1, \ldots, \gamma_{n-1})\right) \leq \nu_p\left(d(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})\right) =$$
$$(-2) \left(\sum_{i=0}^{n-1} k_i \right) + \nu_p\left(d(\omega_0, \omega_1, \ldots, \omega_{n-1})\right).$$

Es ist $\sum_{i=0}^{n-1} m_i \geq \sum_{i=0}^{n-1} k_i$. Da $m_i \leq k_i$ für alle $i \in \{0,1,\ldots,n-1\}$ ist, folgt, dass $m_i = k_i$ für alle $i \in \{0,1,\ldots,n-1\}$ ist. Es ist $k_{i-1} = m_{i-1} \leq m_i = k_i$ für alle $i \in \{1,2,\ldots,n-1\}$. Der Punkt 1 ist gezeigt. Es ist $d(\alpha_0,\alpha_1\ldots,\alpha_{n-1}) = d(\gamma_0,\gamma_1,\ldots,\gamma_{n-1})$. Aus dem Satz 2.0.17 folgt, dass $(\alpha_0,\alpha_1\ldots,\alpha_{n-1})$ eine p-ganze Basis von K ist. Der Punkt 2 ist gezeigt. Es ist

$$\nu_p\left(d(K)\right) = \nu_p\left(d(\alpha_0,\alpha_1,\ldots,\alpha_{n-1})\right) = \nu_p\left(\left(\prod_{i=0}^{n-1}\frac{1}{p^{2k_i}}\right)d(\omega_0,\omega_1,\ldots,\omega_{n-1})\right) =$$
$$\nu_p\left(d(\omega_0,\omega_1,\ldots,\omega_{n-1})\right) - 2\left(\sum_{i=0}^{n-1} k_i\right).$$

Der Punkt 3 ist gezeigt. □

Die Beweisidee des folgenden Satzes stammt aus dem Beweis des Satzes 1.3.5 in der Doktorarbeit von Alaca [1].

Satz 4.0.6. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N}\setminus\{0,1\}$ und $[K:\mathbb{Q}] = n$. Seien $\omega_0,\omega_1,\ldots,\omega_{n-1} \in O_K$. Sei $(\omega_0,\omega_1,\ldots,\omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ und p eine Primzahl. Sei $x_j^{(i)}, X_j^{(i)} \in \mathbb{Z}$ für alle $i \in \{1,2,\ldots,n-1\}$ und alle $j \in \{0,1,\ldots,i-1\}$. Sei $k_0,k_1,\ldots,k_{n-1} \in \mathbb{N}$. Sei*

$$\alpha_i = \frac{1}{p^{k_i}}\left(\left(\sum_{j=0}^{i-1} x_j^{(i)}\omega_j\right) + \omega_i\right)$$
$$\gamma_i = \frac{1}{p^{k_i}}\left(\left(\sum_{j=0}^{i-1} X_j^{(i)}\omega_j\right) + \omega_i\right)$$

für alle $i \in \{0,1,\ldots,n-1\}$. Sei $(\alpha_0,\alpha_1,\ldots,\alpha_{n-1})$ eine p-ganze Basis von K. Sei $X_j^{(i)} \equiv x_j^{(i)} \pmod{p^{k_i}}$ für alle $i \in \{1,2,\ldots,n-1\}$ und alle $j \in \{0,1,\ldots,i-1\}$. Dann ist $(\gamma_0,\gamma_1,\ldots,\gamma_{n-1})$ eine p-ganze Basis von K.

Beweis. Sei $t_j^{(i)} \in \mathbb{Z}$ und $X_j^{(i)} = x_j^{(i)} + p^{k_i}t_j^{(i)}$ für alle $i \in \{1,2,\ldots,n-1\}$ und alle $j \in \{0,1,\ldots,i-1\}$. Es ist

$$\sum_{j=0}^{i-1} t_j^{(i)}\omega_j \in O_K \subseteq O_{p,K}$$

für alle $i \in \{1,2,\ldots,n-1\}$. Es ist

$$\gamma_i = \frac{1}{p^{k_i}}\left(\left(\sum_{j=0}^{i-1} X_j^{(i)}\omega_j\right) + \omega_i\right) = \frac{1}{p^{k_i}}\left(\left(\sum_{j=0}^{i-1}\left(x_j^{(i)} + p^{k_i}t_j^{(i)}\right)\omega_j\right) + \omega_i\right) =$$
$$\alpha_i + \sum_{j=0}^{i-1} t_j^{(i)}\omega_j \in O_{p,K}$$

für alle $i \in \{1,2,\ldots,n-1\}$. Da $(\alpha_0,\alpha_1,\ldots,\alpha_{n-1})$ eine p-ganze Basis von K ist, folgt, dass es ein $A \in M\left(n,n,\mathbb{Z}_{(p)}\right)$ gibt, sodass $(\gamma_0,\gamma_1,\ldots,\gamma_{n-1})^T = A\,(\alpha_0,\alpha_1,\ldots,\alpha_{n-1})^T$ ist. Sei $a_{i,j} \in \mathbb{Z}_{(p)}$ für alle $i,j \in \{0,1,\ldots,n-1\}$ und $A = \left(a_{i,j}\right)_{0\leq i,j\leq n-1}$. Da $(\omega_0,\omega_1\ldots,\omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ ist, folgt, dass $a_{i,j} = 0$ für alle $i \in \{0,1,\ldots,n-2\}$ und für alle $j \in \{i+1,i+2,\ldots,n-1\}$ ist und $a_{i,i} = 1$ für alle $i \in \{0,1,\ldots,n-1\}$ ist. Es ist $\det(A) = 1$ und $\nu_p(\det(A)) = 0$. Aus dem Satz 2.0.15 folgt, dass $(\gamma_0,\gamma_1,\ldots,\gamma_{n-1})$ eine p-ganze Basis von K ist. □

Satz 4.0.7. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N}\setminus\{0,1\}$ und $[K:\mathbb{Q}] = n$. Seien $\omega_0,\omega_1,\ldots,\omega_{n-1} \in O_K$. Sei $(\omega_0,\omega_1,\ldots,\omega_{n-1})$ eine Basis von K über $\mathbb{Q}$ und p eine Primzahl. Sei $x_j^{(i)} \in \mathbb{Z}$ für alle $i \in \{1,2,\ldots,n-1\}$ und alle $j \in \{0,1,\ldots,i-1\}$. Sei $k_0,k_1,\ldots,k_{n-1} \in \mathbb{N}$. Sei*

$$\alpha_i = \frac{1}{p^{k_i}}\left(\left(\sum_{j=0}^{i-1} x_j^{(i)}\omega_j\right) + \omega_i\right)$$

für alle $i \in \{0,1,\ldots,n-1\}$. Sei $(\alpha_0,\alpha_1\ldots,\alpha_{n-1})$ eine p-ganze Basis von K und $(\omega_0,\omega_1\ldots,\omega_{n-1})$ eine p-ganze Basis von K, dann ist $k_i = 0$ für alle $i \in \{0,1,\ldots,n-1\}$.

Beweis. Sei $A \in M\left(n,n,Z_{(p)}\right)$ und $(\alpha_0,\alpha_1\ldots,\alpha_{n-1})^T = A\,(\omega_0,\omega_1,\ldots,\omega_{n-1})^T$. Es ist $\det(A) = \prod_{i=0}^{n-1}\frac{1}{p^{k_i}}$. Aus dem Satz 2.0.15 folgt, dass $\nu_p(\det(A)) = 0$ ist. Es ist $k_i = 0$ für alle $i \in \{0,1,\ldots,n-1\}$. □

Satz 4.0.8. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N}\setminus\{0,1\}$ und $[K:\mathbb{Q}] = n$. Seien $\omega_0,\omega_1,\ldots,\omega_{n-1} \in O_K$. Sei $(\omega_0,\omega_1,\ldots,\omega_{n-1})$ eine Basis von K über $\mathbb{Q}$. Sei $x_j^{(i,p)} \in \mathbb{Z}$ für alle $i \in \{1,2,\ldots,n-1\}$, alle $j \in \{0,1,\ldots,i-1\}$ und alle Primzahlen p. Sei $k_{i,p} \in \mathbb{N}$ und*

$$\alpha_{i,p} = \frac{1}{p^{k_{i,p}}}\left(\left(\sum_{j=0}^{i-1} x_j^{(i,p)}\omega_j\right) + \omega_i\right)$$

für alle $i \in \{0,1,\ldots,n-1\}$ und alle Primzahlen p. Sei $\left(\alpha_{0,p},\alpha_{1,p}\ldots,\alpha_{n-1,p}\right)$ eine p-ganze Basis von K für alle Primzahlen p. Sei $l \in \{0,1,\ldots,n-1\}$, dann ist

$$\left|\left\{p \mid p \text{ Primzahl}, k_{l,p} \neq 0\right\}\right| < \infty$$

und $\prod_{p \text{ Primzahl}} p^{k_{l,p}} < \infty$.

Beweis. Sei $(\beta_0,\beta_1,\ldots,\beta_{n-1})$ eine Ganzheitsbasis von K, $A \in M(n,n,\mathbb{Z})$ und $(\omega_0,\omega_1,\ldots,\omega_{n-1})^T = A\,(\beta_0,\beta_1,\ldots,\beta_{n-1})^T$. Es ist $\det(A) \in \mathbb{Z}$. Es ist $\det(A) \neq 0$. Aus dem Satz 2.0.15 folgt, dass $(\omega_0,\omega_1,\ldots,\omega_{n-1})$ eine q-ganze Basis von K ist, für alle

Primzahlen q, für die gilt, dass $q \nmid \det(A)$ ist. Aus dem Satz 4.0.7 folgt, dass $k_{l,q} = 0$ ist für alle Primzahlen q, für die gilt, dass $q \nmid \det(A)$ ist. Es ist

$$\prod_{p \text{ Primzahl}} p^{k_{l,p}} = \prod_{p \text{ Primzahl, } p \mid \det(A)} p^{k_{l,p}} \in \mathbb{N} \setminus \{0\}.$$

□

Der folgende Satz ist mit dem Satz 1.3.6 in der Doktorarbeit von Alaca [1] vergleichbar, wenn $(\omega_0, \omega_1, \ldots, \omega_{n-1}) = \left(1, \theta, \ldots, \theta^{n-1}\right)$ für ein primitives Element $\theta \in O_K$ ist. Die Vorarbeit für den Beweis, in Form der Sätze 4.0.6, 4.0.7 und 4.0.8, ist etwas anders aufgebaut als der Beweis des Satzes 1.3.6 in [1]. Die Beweisidee stammt jedoch aus den Beweisen der Sätze 1.3.5 und 1.3.6 in [1].

Satz 4.0.9. *Sei K ein algebraischer Zahlkörper, $n \in \mathbb{N} \setminus \{0,1\}$ und $[K : \mathbb{Q}] = n$. Seien $\omega_0, \omega_1, \ldots, \omega_{n-1} \in O_K$. Sei $(\omega_0, \omega_1, \ldots, \omega_{n-1})$ eine Basis von K über $\mathbb{Q}$. Sei $X_j^{(i)} \in \mathbb{Z}$ für alle $i \in \{1, 2, \ldots, n-1\}$ und alle $j \in \{0, 1, \ldots, i-1\}$. Sei $x_j^{(i,p)} \in \mathbb{Z}$ für alle $i \in \{1, 2, \ldots, n-1\}$, alle $j \in \{0, 1, \ldots, i-1\}$ und alle Primzahlen p. Sei $k_{i,p} \in \mathbb{N}$ und*

$$\alpha_{i,p} = \frac{1}{p^{k_{i,p}}} \left(\left(\sum_{j=0}^{i-1} x_j^{(i,p)} \omega_j \right) + \omega_i \right)$$

für alle $i \in \{0, 1, \ldots, n-1\}$ und alle Primzahlen p. Sei $\left(\alpha_{0,p}, \alpha_{1,p}, \ldots, \alpha_{n-1,p}\right)$ eine p-ganze Basis von K für alle Primzahlen p. Sei $X_j^{(i)} \equiv x_j^{(i,p)} \pmod{p^{k_{i,p}}}$ für alle $i \in \{1, 2, \ldots, n-1\}$, alle $j \in \{0, 1, \ldots, i-1\}$ und alle Primzahlen p. Sei $s_i = \prod_{p \text{ Primzahl}} p^{k_{i,p}}$ und

$$\gamma_i = \frac{1}{s_i} \left(\left(\sum_{j=0}^{i-1} X_j^{(i)} \omega_j \right) + \omega_i \right)$$

für alle $i \in \{0, 1, \ldots, n-1\}$. Dann ist $(\gamma_0, \gamma_1, \ldots, \gamma_{n-1})$ eine Ganzheitsbasis von K.

Beweis. Aus dem Satz 4.0.6 folgt, dass $\left(\frac{s_0}{p^{k_{0,p}}} \gamma_0, \frac{s_1}{p^{k_{1,p}}} \gamma_1, \ldots, \frac{s_{n-1}}{p^{k_{n-1,p}}} \gamma_{n-1} \right)$ eine p-ganze Basis von K für alle Primzahl p ist. Sei $A_p = \left(\frac{\delta_{i,j} p^{k_{i,p}}}{s_i} \right)_{0 \le i,j \le n-1}$ für alle Primzahlen p. Es ist

$$A_p \left(\frac{s_0}{p^{k_{0,p}}} \gamma_0, \frac{s_1}{p^{k_{1,p}}} \gamma_1, \ldots, \frac{s_{n-1}}{p^{k_{n-1,p}}} \gamma_{n-1} \right)^T = (\gamma_0, \gamma_1, \ldots, \gamma_{n-1})^T,$$

$A_p \in M\left(n, n, \mathbb{Z}_{(p)}\right)$ und $\nu_p\left(\det\left(A_p\right)\right) = 0$ für alle Primzahlen p. Aus dem Satz 2.0.15 folgt, dass $(\gamma_0, \gamma_1, \ldots, \gamma_{n-1})$ eine p-ganze Basis von K für alle Primzahlen p ist. Aus dem Satz 2.0.13 folgt, dass $(\gamma_0, \gamma_1, \ldots, \gamma_{n-1})$ eine Ganzheitsbasis von K ist. □

Satz 4.0.10. *Sei $k_p \in \mathbb{N}$ und $x_p \in \mathbb{Z}$ für alle Primzahlen p. Sei $|\{p \mid p \text{ Primzahl}, k_p \neq 0\}| < \infty$, dann gibt es ein $X \in \mathbb{Z}$, sodass $X \equiv x_p \pmod{p^{k_p}}$ für alle Primzahlen p ist.*

Beweis. Der Satz 4.0.10 folgt aus dem Satz 1.2.9. □

5 kubische Zahlkörper

5.1 Einleitung

Dieses Kapitel folgt zum Teil dem Kapitel 2 in der Doktorarbeit von Alaca [1]. Der Aufbau des Kapitels 2 in [1] wird zum Teil übernommen. Die Idee, die kubischen Zahlkörper auf eine Form wie in dem Satz 5.1.6 zu reduzieren, stammt aus [1].

Definition 5.1.1 (kubischer Zahlkörper)**.** *Sei K ein algebraischer Zahlkörper, dann heißt K genau dann kubisch, wenn $[K : \mathbb{Q}] = 3$ ist.*

Die Notation in der folgenden Definition lehnt sich an die Notation (2.1.7) in dem Satz 2.1.1 in [1] und an die Notation in dem Satz 2.1.2 in [1] an.

Definition 5.1.2. *Es ist*

$$X_3(T_0, T_1, S_0, S_1, S_2), Y_3(T_0, T_1, S_0, S_1, S_2), Z_3(T_0, T_1, S_0, S_1, S_2) \in \mathbb{Z}[T_0, T_1, S_0, S_1, S_2].$$

Es ist

$$U(T_0, T_1, S_1, S_2), V(T_0, T_1, S_1, S_2) \in \mathbb{Z}[T_0, T_1, S_1, S_2].$$

Es ist

$$\begin{aligned}
X_3(T_0, T_1, S_0, S_1, S_2) =& 2T_0S_2 + 3S_0,\\
Y_3(T_0, T_1, S_0, S_1, S_2) =& T_0^2S_2^2 + 4T_0S_0S_2 - T_0S_1^2 + 3T_1S_1S_2 + 3S_0^2,\\
Z_3(T_0, T_1, S_0, S_1, S_2) =& T_0^2S_0S_2^2 + T_0T_1S_1S_2^2 + 2T_0S_0^2S_2 - T_0S_0S_1^2 + T_1^2S_2^3 + 3T_1S_0S_1S_2\\
&- T_1S_1^3 + S_0^3,\\
U(T_0, T_1, S_1, S_2) =& -2T_0^2S_2 + 9T_1S_1 \text{ und}\\
V(T_0, T_1, S_1, S_2) =& 2T_0S_1 - 3T_1S_2.
\end{aligned}$$

Satz 5.1.3. *Seien $r, s, x, y, z \in \mathbb{Z}$. Dann sind alle fünf folgenden Punkte erfüllt:*

1. $X_3(r, s, x, y, z) = 2rz + 3x$
2. $Y_3(r, s, x, y, z) = r^2z^2 + 4rxz - ry^2 + 3syz + 3x^2$
3. $Z_3(r, s, x, y, z) = r^2xz^2 + rsyz^2 + 2rx^2z - rxy^2 + s^2z^3 + 3sxyz - sy^3 + x^3$
4. $U(r, s, y, z) = -2r^2z + 9sy$
5. $V(r, s, y, z) = 2ry - 3sz$

Satz 5.1.4. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 + rT^2 + sT + t$, $K = \mathbb{Q}(\theta)$, $\mu = r + 3\theta$, $x = 3r^2 - 9s$ und $y = 2r^3 - 9rs + 27t$, dann ist $K = \mathbb{Q}(\mu)$ und $\operatorname{irr}_{\mu,\mathbb{Q}}(T) = T^3 - xT + y$.*

Beweis. Sei $P(T) = T^3 - xT + y$. Es ist

$$\begin{aligned} P(\mu) = (r+3\theta)^3 - x(r+3\theta) + y = (r+3\theta)^3 - \left(3r^2 - 9s\right)(r+3\theta) + 2r^3 - 9rs + 27t = \\ r^3 + 9r^2\theta + 27r\theta^2 + 27\theta^3 - 3r^3 - 9r^2\theta + 9rs + 27s\theta + 2r^3 - 9rs + 27t = \\ 27\left(\theta^3 + r\theta^2 + s\theta + t\right) = 27\,\mathrm{irr}_{\theta,\mathbb{Q}}(\theta) = 0. \end{aligned}$$

Es ist $K = \mathbb{Q}(\mu)$. Es ist $P(T) = \mathrm{irr}_{\mu,\mathbb{Q}}(T)$. □

Die Idee für den folgenden Satz stammt aus der Doktorarbeit von Alaca [1].

Satz 5.1.5. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\mathrm{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$, p eine Primzahl, $v_p(r) \geq 2$, $v_p(s) \geq 3$, $\mu = \frac{\theta}{p}$, $x = \frac{r}{p^2}$ und $y = \frac{s}{p^3}$, dann ist $\mu \in O_K$, $K = \mathbb{Q}(\mu)$ und $\mathrm{irr}_{\mu,\mathbb{Q}}(T) = T^3 - xT + y$.*

Beweis. Sei $P(T) = T^3 - xT + y$. Es ist $P(\mu) = \frac{1}{p^3}\left(\theta^3 - r\theta + s\right) = 0$. Es ist $K = \mathbb{Q}(\mu)$. Es ist $P(T) = \mathrm{irr}_{\mu,\mathbb{Q}}(T)$. □

Das Resultat des folgenden Satzes wird zu Beginn des Abschnittes 2.1 in der Doktorarbeit von Alaca [1] angeführt[1].

Satz 5.1.6. *Sei K ein kubischer Zahlkörper, dann gibt es ein $\theta \in O_K$ und $r, s \in \mathbb{Z}$, sodass $K = \mathbb{Q}(\theta)$, $\mathrm{irr}_{\theta,K} = T^3 - rT + s$ und ($v_p(r) \leq 1$ oder $v_p(s) \leq 2$) ist.*

Beweis. Sei M die Menge aller (μ, x, y), für die gilt, dass $\mu \in O_K$, $x, y \in \mathbb{Z}$, $K = \mathbb{Q}(\mu)$ und $\mathrm{irr}_{\mu,\mathbb{Q}}(T) = T^3 - xT + y$ ist. Es gibt ein $\lambda \in O_K$, sodass $K = \mathbb{Q}(\lambda)$ ist. Aus dem Satz 5.1.4 folgt, dass $M \neq \emptyset$ ist. Sei $m_{(\mu,x,y)} = \min\left\{v_p(x) - 1, v_p(y) - 2\right\}$ für alle $(\mu, x, y) \in M$. Es ist $m_{(\mu,x,y)} \in \mathbb{Z}$ für alle $(\mu, x, y) \in M$. Sei

$$n = \min\left\{m_{(\mu,x,y)} \mid (\mu, x, y) \in M\right\}.$$

Sei $\theta \in O_K$, $r, s \in \mathbb{Z}$, $(\theta, r, s) \in M$ und $m_{(\theta,r,s)} = n$.

Angenommen es ist $n \geq 1$.

Es ist $v_p(r) - 1 \geq 1$ und $v_p(s) - 2 \geq 1$. Es folgt, dass $v_p(r) \geq 2$ und $v_p(s) \geq 3$ ist. Aus dem Satz 5.1.5 folgt, dass $\left(\frac{\theta}{p}, \frac{r}{p^2}, \frac{s}{p^3}\right) \in M$ ist. Es ist

$$m_{\left(\frac{\theta}{p}, \frac{r}{p^2}, \frac{s}{p^3}\right)} < m_{(\theta,r,s)} = n.$$

Dies ist ein Widerspruch.

Es ist $n \leq 0$. Es folgt, dass $v_p(r) - 1 \leq 0$ oder $v_p(s) - 2 \leq 0$ ist. Es ist $v_p(r) \leq 1$ oder $v_p(s) \leq 2$. □

[1] Siehe Gleichung (2.1.2).

Satz 5.1.7. *Sei p eine Primzahl. Seien $r, s, u, v, w \in \mathbb{Z}$. Sei $r \not\equiv 0 \pmod{p^2}$ oder $s \not\equiv 0 \pmod{p^3}$. Wenn $x \not\equiv 0 \pmod{p}$ ist, dann sei ($u \not\equiv 0 \pmod{p}$ und $v \not\equiv 0 \pmod{p}$). Wenn $w \not\equiv 0 \pmod{p}$ ist, dann sei $s \equiv 0 \pmod{p}$. Sei $ru \equiv 0 \pmod{p^2}$ und $sv + s^2 w \equiv 0 \pmod{p^3}$, dann ist $x \equiv 0 \pmod{p}$.*

Beweis. Angenommen es ist $x \not\equiv 0 \pmod{p}$. Es folgt, dass $u \not\equiv 0 \pmod{p}$ und $v \not\equiv 0 \pmod{p}$ ist. Es folgt, dass $r \equiv 0 \pmod{p^2}$ ist. Es folgt, dass $s \not\equiv 0 \pmod{p^3}$ ist. Es ist $0 \equiv sv + s^2 w = s(v + sw) \pmod{p^3}$. Es folgt, dass $v + sw \equiv 0 \pmod{p^{3-\nu_p(s)}}$ ist. Es ist $sw \not\equiv 0 \pmod{p}$. Es folgt, dass $w \not\equiv 0 \pmod{p}$ und $s \not\equiv 0 \pmod{p}$ ist. Dies ist ein Widerspruch. □

Der folgende Satz stammt im Wesentlichen aus der Doktorarbeit von Alaca [1][2]. Der Beweis folgt im Wesentlichen dem Beweis des Satzes 2.1.1 in [1].

Satz 5.1.8. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$, p eine Primzahl und $m \in \mathbb{N} \setminus \{0\}$. Seien $x, y, z \in \mathbb{Z}$. Sei $\alpha = \frac{x+y\theta+z\theta^2}{p^m}$, dann sind die beiden folgenden Punkte äquivalent:*

1. $\alpha \in O_{p,K}$
2. $X_3(r,s,x,y,z) \equiv 0 \pmod{p^m}$, $Y_3(r,s,x,y,z) \equiv 0 \pmod{p^{2m}}$ *und* $Z_3(r,s,x,y,z) \equiv 0 \pmod{p^{3m}}$

Beweis. Seien σ_0, σ_1, σ_2 die Einbettungen von K in $\mathbb{C}$ und $\sigma_0 = id_{K,\mathbb{C}}$. Sei $\theta_1 = \sigma_1(\theta)$ und $\theta_2 = \sigma_2(\theta)$. Aus dem Satz 1.2.15 folgt, dass

$$\operatorname{irr}_{\theta,\mathbb{Q}}(T) = \operatorname{fld}_{\theta,K}(T) = (T-\theta)(T-\theta_1)(T-\theta_2)$$

ist. Es ist

$$\begin{aligned} \theta\theta_1\theta_2 &= -s \\ \theta\theta_1 + \theta\theta_2 + \theta_1\theta_2 &= -r \\ \theta + \theta_1 + \theta_2 &= 0 \end{aligned}$$

Es ist

$$\begin{aligned} \theta^2 + \theta_1^2 + \theta_2^2 = (\theta + \theta_1 + \theta_2)^2 - 2(\theta\theta_1 + \theta\theta_2 + \theta_1\theta_2) &= 2r, \\ \theta^2\theta_1^2 + \theta^2\theta_2^2 + \theta_1^2\theta_2^2 = (\theta\theta_1 + \theta\theta_2 + \theta_1\theta_2)^2 - 2\theta\theta_1\theta_2(\theta + \theta_1 + \theta_2) &= r^2 \end{aligned}$$

und

$$\begin{aligned} \theta\theta_1^2 + \theta^2\theta_1 + \theta\theta_2^2 + \theta^2\theta_2 + \theta_1\theta_2^2 + \theta_1^2\theta_2 &= \\ \theta\theta_1(\theta_1 + \theta) + \theta\theta_2(\theta_2 + \theta) + \theta_1\theta_2(\theta_2 + \theta_1) = -3\theta\theta_1\theta_2 &= 3s. \end{aligned}$$

[2] Siehe Satz 2.1.1 in [1].

Sei $\alpha_1 = \frac{x+y\theta_1+z\theta_1^2}{p^m}$ und $\alpha_2 = \frac{x+y\theta_2+z\theta_2^2}{p^m}$. Es ist $\sigma_1(\alpha) = \alpha_1$, $\sigma_2(\alpha) = \alpha_2$ und $\mathrm{fld}_{\alpha,K} = (T-\alpha)(T-\alpha_1)(T-\alpha_2)$. Sei $a,b,c \in \mathbb{Q}$ und $\mathrm{fld}_{\alpha,K} = T^3 + aT^2 + bT + c$. Es ist

$$\begin{aligned} a &= -(\alpha+\alpha_1+\alpha_2) \\ b &= \alpha\alpha_1 + \alpha\alpha_2 + \alpha_1\alpha_2 \\ c &= -\alpha\alpha_1\alpha_2 \end{aligned}$$

Es ist

$$\begin{aligned} a = -(\alpha+\alpha_1+\alpha_2) = -\left[3x + y(\theta+\theta_1+\theta_2) + z\left(\theta^2+\theta_1^2+\theta_2^2\right)\right]/p^m = \\ -(3x+2rz)/p^m = \frac{-X_3(r,s,x,y,z)}{p^m}. \end{aligned}$$

Es ist

$$\begin{aligned} b = \alpha\alpha_1 + \alpha\alpha_2 + \alpha_1\alpha_2 = \\ \frac{1}{p^{2m}}\left[3x^2 + 2xz\left(\theta^2+\theta_1^2+\theta_2^2\right) + y^2(\theta\theta_1+\theta\theta_2+\theta_1\theta_2) + \right. \\ \left. yz\left(\theta\theta_1^2+\theta^2\theta_1+\theta\theta_2^2+\theta^2\theta_2+\theta_1\theta_2^2+\theta_1^2\theta_2\right) + z^2\left(\theta^2\theta_1^2+\theta^2\theta_2^2+\theta_1^2\theta_2^2\right)\right] = \\ \frac{1}{p^{2m}}\left(3x^2+4rxz-ry^2+3syz+r^2z^2\right) = \frac{Y_3(r,s,x,y,z)}{p^{2m}} \end{aligned}$$

und

$$\begin{aligned} c = -\alpha\alpha_1\alpha_2 = \\ -\left[x^3 + x^2z\left(\theta^2+\theta_1^2+\theta_2^2\right) + xy^2(\theta\theta_1+\theta\theta_2+\theta_1\theta_2)\right. \\ +xyz\left(\theta\theta_1^2+\theta^2\theta_1+\theta\theta_2^2+\theta^2\theta_2+\theta_1\theta_2^2+\theta_1^2\theta_2\right) + xz^2\left(\theta^2\theta_1^2+\theta^2\theta_2^2+\theta_1^2\theta_2^2\right) + y^3\theta\theta_1\theta_2 \\ \left.+y^2z\left(\theta\theta_1\theta_2^2+\theta\theta_1^2\theta_2+\theta^2\theta_1\theta_2\right) + yz^2\left(\theta\theta_1^2\theta_2^2+\theta^2\theta_1\theta_2^2+\theta^2\theta_1^2\theta_2\right) + z^3\theta^2\theta_1^2\theta_2^2\right]/p^{3m} = \\ -\left(x^3+2rx^2z-rxy^2+3sxyz+r^2xz^2-sy^3+rsyz^2+s^2z^3\right)/p^{3m} = \frac{-Z_3(s,s,x,y,z)}{p^{3m}}. \end{aligned}$$

Es ist $a \in \mathbb{Z}_{(p)}$ genau dann, wenn $X_3(r,s,x,y,z) \equiv 0 \pmod{p^m}$ ist. Es ist $b \in \mathbb{Z}_{(p)}$ genau dann, wenn $Y_3(r,s,x,y,z) \equiv 0 \pmod{p^{2m}}$ ist. Es ist $c \in \mathbb{Z}_{(p)}$ genau dann, wenn $Z_3(r,s,x,y,z) \equiv 0 \pmod{p^{3m}}$ ist. Aus dem Satz 2.0.9 folgt der Satz 5.1.8. □

Der folgende Satz stammt im Wesentlichen aus der Doktorarbeit von Alaca [1][3]. Der Beweis folgt im Wesentlichen dem Beweis des Satzes 2.1.2 in [1].

Satz 5.1.9. *Sei $r \in \mathbb{Z} \setminus \{0\}$. Seien $s,x,y,z \in \mathbb{Z}$. Sei $\Delta = 4r^3 - 27s^2$, dann ist*

$$Y_3(r,s,x,y,z) = \frac{1}{12r^2}\left(4r^2X_3(r,s,x,y,z)^2 - U(r,s,y,z)^2 - 3y^2\Delta\right)$$

[3] Siehe Satz 2.1.2 in [1].

und

$$\begin{aligned} &Z_3(r,s,x,y,z) = \\ &\frac{1}{4\cdot 27r^3}\Big(4r^3X_3(r,s,x,y,z)^3 - 3rX_3(r,s,x,y,z)\,U(r,s,y,z)^2 - 9ry^2\Delta X_3(r,s,x,y,z) \\ &-3U(r,s,y,z)^3 + 2rz^2\Delta U(r,s,y,z) - 9y^2\Delta U(r,s,y,z) + 27sV(r,s,y,z)^3 \\ &+18sz^2\Delta V(r,s,y,z) - z^3\Delta^2\Big) \end{aligned}$$

Beweis. Es ist

$$\begin{aligned} \frac{1}{12r^2}\left(4r^2X_3(r,s,x,y,z)^2 - U(r,s,y,z)^2 - 3y^2\Delta\right) = \\ \frac{1}{12r^2}\left(4r^2(2rz+3x)^2 - \left(-2r^2z+9sy\right)^2 - 3y^2\left(4r^3-27s^2\right)\right) = \\ r^2z^2 + 4rxz - ry^2 + 3syz + 3x^2 = Y_3(r,s,x,y,z). \end{aligned}$$

Es ist

$$\begin{aligned} &\frac{1}{4\cdot 27r^3}\Big(4r^3(2rz+3x)^3 - 3r(2rz+3x)\left(-2r^2z+9sy\right)^2 - 9ry^2\left(4r^3-27s^2\right)(2rz+3x) \\ &-3\left(-2r^2z+9sy\right)^3 + 2rz^2\left(4r^3-27s^2\right)\left(-2r^2z+9sy\right) - 9y^2\left(4r^3-27s^2\right)\left(-2r^2z+9sy\right) \\ &+27s(2ry-3sz)^3 + 18sz^2\left(4r^3-27s^2\right)(2ry-3sz) - z^3\left(4r^3-27s^2\right)^2\Big) = \\ &r^2xz^2 + rsyz^2 + 2rx^2z - rxy^2 + s^2z^3 + 3sxyz - sy^3 + x^3 = Z_3(r,s,x,y,z). \end{aligned}$$

□

Der folgende Satz stammt im Wesentlichen aus der Doktorarbeit von Alaca [1][4].

Satz 5.1.10. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r,s \in \mathbb{Z}$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$, $\Delta = 4r^3 - 27s^2$ und p eine Primzahl. Seien $i,j \in \mathbb{N}$. Seien $u,x,y \in \mathbb{Z}$. Sei $\frac{u+\theta}{p^i}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 1 bezüglich $\left(1,\theta,\theta^2\right)$ und $\frac{x+y\theta+\theta^2}{p^j}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 2 bezüglich $\left(1,\theta,\theta^2\right)$, dann sind die drei folgenden Punkte erfüllt:*

1. $i \leq j$
2. $\left(1, \frac{u+\theta}{p^i}, \frac{x+y\theta+\theta^2}{p^j}\right)$ *ist eine p-ganze Basis von K,*
3. $\nu_p(d(K)) = \nu_p(\Delta) - 2(i+j)$

Beweis. Sei α_k für alle $k \in \{0,1,2\}$ ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $\left(1,\theta,\theta^2\right)$. Aus dem Satz 3.0.13 folgt, dass $\alpha_0 = 1$ ist. Aus dem Satz 3.0.15 folgt, dass es $r_{10}, r_{20}, r_{21} \in \mathbb{Z}$ und $d_1, d_2 \in \mathbb{N} \setminus \{0\}$ gibt, sodass $\alpha_1 = \frac{r_{10}+\theta}{d_1}$ und $\alpha_2 = \frac{r_{20}+r_{21}\theta+\theta^2}{d_2}$ ist. Aus dem Satz 3.0.14 folgt, dass $d_1 \mid d_2$ ist. Es ist 1 ein minimal-ganzes Element von K über

[4] Siehe Satz 2.1.2 in [1].

$\mathbb{Z}_{(p)}$ vom Grad 0 bezüglich $\left(1,\theta,\theta^2\right)$. Aus dem Punkt 1 des Satzes 4.0.5 folgt, dass $i \leq j$ ist. Aus dem Punkt 2 des Satzes 4.0.5 folgt, dass $\left(1, \frac{u+\theta}{p^i}, \frac{x+y\theta+\theta^2}{p^j}\right)$ eine p-ganze Basis von K ist. Aus dem Punkt 3 des Satzes 4.0.5 folgt, dass $\nu_p\left(d\left(K\right)\right) = \nu_p\left(d\left(1,\theta,\theta^2\right)\right) - 2\left(i+j\right)$ ist. Aus dem Satz 1.2.27 folgt, dass $d\left(1,\theta,\theta^2\right) = 4r^3 - 27s^2 = \Delta$ ist. Es ist $\nu_p\left(d\left(K\right)\right) = \nu_p\left(\Delta\right) - 2\left(i+j\right)$. □

Satz 5.1.11. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r,s \in \mathbb{Z}$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}\left(T\right) = T^3 - rT + s$, $K = \mathbb{Q}\left(\theta\right)$, $\Delta = 4r^3 - 27s^2$ und p eine Primzahl. Seien $i,j \in \mathbb{N}$. Seien $u,x,y \in \mathbb{Z}$. Sei $\frac{u+\theta}{p^i} \in O_{p,K}$ und $\frac{x+y\theta+\theta^2}{p^j} \in O_{p,K}$, dann ist $i+j \leq \frac{\nu_p(\Delta)}{2}$.*

Beweis. Sei $k,l \in \mathbb{N}$, $v,z_0,z_1 \in \mathbb{Z}$, $\frac{v+\theta}{p^k}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 1 bezüglich $\left(1,\theta,\theta^2\right)$ und $\frac{z_0+z_1\theta+\theta^2}{p^l}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 2 bezüglich $\left(1,\theta,\theta^2\right)$. Es ist $i \leq k$ und $j \leq l$. Es ist $d\left(K\right) \in \mathbb{Z}$ und $\nu_p\left(d\left(K\right)\right) \geq 0$. Aus dem Punkt 3 des Satzes 5.1.10 folgt, dass $\nu_p\left(d\left(K\right)\right) = \nu_p\left(\Delta\right) - 2\left(k+l\right)$ ist. Es ist $i+j \leq k+l = \frac{\nu_p(\Delta)-\nu_p(d(K))}{2} \leq \frac{\nu_p(\Delta)}{2}$. □

Satz 5.1.12. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r,s \in \mathbb{Z}$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}\left(T\right) = T^3 - rT + s$, $K = \mathbb{Q}\left(\theta\right)$, $\Delta = 4r^3 - 27s^2$ und p eine Primzahl. Seien $i,j \in \mathbb{N}$. Seien $u,x,y \in \mathbb{Z}$. Sei $\frac{u+\theta}{p^i} \in O_{p,K}$, $\frac{x+y\theta+\theta^2}{p^j} \in O_{p,K}$ und $i+j = \left\lfloor \frac{\nu_p(\Delta)}{2} \right\rfloor$, dann ist $\left(1, \frac{u+\theta}{p^i}, \frac{x+y\theta+\theta^2}{p^j}\right)$ ist eine p-ganze Basis von K.*

Beweis. Sei $k,l \in \mathbb{N}$, $v,z_0,z_1 \in \mathbb{Z}$, $\frac{v+\theta}{p^k}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 1 bezüglich $\left(1,\theta,\theta^2\right)$ und $\frac{z_0+z_1\theta+\theta^2}{p^l}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 2 bezüglich $\left(1,\theta,\theta^2\right)$. Es ist $i \leq k$ und $j \leq l$. Aus dem Satz 5.1.11 folgt, dass $k+l \leq \frac{\nu_p(\Delta)}{2}$ ist. Es ist $k+l \leq \left\lfloor \frac{\nu_p(\Delta)}{2} \right\rfloor = i+j$. Es folgt, dass $i+j = k+l$, $i = k$ und $j = l$ ist. Es ist $\frac{u+\theta}{p^i}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 1 bezüglich $\left(1,\theta,\theta^2\right)$ und $\frac{x+y\theta+\theta^2}{p^j}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 2 bezüglich $\left(1,\theta,\theta^2\right)$. Aus dem Satz 5.1.10 folgt, dass $\left(1, \frac{u+\theta}{p^i}, \frac{x+y\theta+\theta^2}{p^j}\right)$ eine p-ganze Basis von K ist. □

5.2 2-ganze Basen

Satz 5.2.1. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r,s \in \mathbb{Z}$. Sei $\nu_2\left(r\right) \leq 1$ oder $\nu_2\left(s\right) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}\left(T\right) = T^3 - rT + s$, $K = \mathbb{Q}\left(\theta\right)$ und $x \in \mathbb{Z}$, dann ist $\frac{x+\theta}{2} \notin O_{2,K}$.*

Beweis. Angenommen es ist $\frac{x+\theta}{2} \in O_{2,K}$. Aus dem Satz 5.1.8 folgt, dass $X_3\left(r,s,x,1,0\right) \equiv 0 \pmod 2$, $Y_3\left(r,s,x,1,0\right) \equiv 0 \pmod 4$ und $Z_3\left(r,s,x,1,0\right) \equiv 0 \pmod 8$ ist. Es ist

$$0 \equiv X_3\left(r,s,x,1,0\right) = 3x \pmod 2$$

und $x \equiv 0 \pmod 2$. Es ist

$$0 \equiv Y_3(r,s,x,1,0) = -r + 3x^2 \equiv -r \pmod 4$$

und $r \equiv 0 \pmod 4$ ist. Es ist $v_2(s) \leq 2$. Es ist

$$0 \equiv Z_3(r,s,x,1,0) = -rx - s + x^3 \equiv -s \pmod 8.$$

Es ist $v_2(s) \geq 3$. Dies ist ein Widerspruch. □

Satz 5.2.2. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r,s \in \mathbb{Z}$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$ und $K = \mathbb{Q}(\theta)$. Seien $x,y \in \mathbb{Z}$. Sei $\frac{x+y\theta+\theta^2}{2} \in O_{2,K}$, dann ist einer der beiden folgenden Punkte erfüllt:*

1. *$r \not\equiv 3 \pmod 4$ und $s \equiv 0 \pmod 4$*
2. *$r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$ und $y \equiv 1 \pmod 2$.*

Beweis. Aus dem Satz 5.1.8 folgt, dass $X_3(r,s,x,y,1) \equiv 0 \pmod 2$, $Y_3(r,s,x,y,1) \equiv 0 \pmod 4$ und $Z_3(r,s,x,y,1) \equiv 0 \pmod 8$ ist. Sei $\Delta = 4r^3 - 27s^2$. Aus dem Satz 5.1.11 folgt, dass $v_2(\Delta) \geq 2$ ist. Es ist $0 \equiv \Delta \equiv s \pmod 2$. Es folgt, dass

$$0 \equiv X_3(r,s,x,y,1) = 2r + 3x \equiv x \pmod 2$$

ist.

Fall $s \equiv 0 \pmod 4$:
Es ist $3 - y^2 \not\equiv 0 \pmod 4$. Es ist

$$0 \equiv Y_3(r,s,x,y,1) = r^2 + 4rx - ry^2 + 3sy + 3x^2 \equiv r^2 - ry^2 = r\left(r - y^2\right) \pmod 4.$$

Es folgt, dass $r \not\equiv 3 \pmod 4$ ist.
Fall $s \equiv 2 \pmod 4$:
Es ist

$$0 \equiv Y_3(r,s,x,y,1) = r^2 + 4rx - ry^2 + 3sy + 3x^2 \equiv r^2 - ry^2 + 2y \pmod 4$$

und $r^2 \equiv ry^2 - 2y \pmod 4$. Es ist

$$\begin{aligned} 0 \equiv Z_3(r,s,x,y,1) = \\ r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3 \equiv \\ r^2x + rsy - rxy^2 + 4 + 2xy - sy^3 \equiv \left(ry^2 - 2y\right)x + rsy - rxy^2 + 4 + 2xy - sy^3 = \\ rsy + 4 - sy^3 \pmod 8. \end{aligned}$$

Es ist

$$rsy + 4 - sy^3 \equiv 0 \pmod 8. \tag{5.1}$$

Es ist

$$\begin{aligned} 0 \equiv r\left(rsy + 4 - sy^3\right) = r^2sy + 4r - rsy^3 \equiv \left(ry^2 - 2y\right)sy + 4r - rsy^3 = -2sy^2 + 4r \equiv \\ 4y + 4r = 4(y + r) \pmod 8. \end{aligned}$$

Es ist $r \equiv y \pmod{2}$. Aus (5.1) folgt, dass $r \equiv y \equiv 1 \pmod{2}$ ist. Es ist

$$0 \equiv rsy + 4 - sy^3 \equiv rsy + 4 - sy = sy(r-1) + 4 \equiv 2(r-1) + 4 = 2r + 2 \pmod{8}.$$

Es ist $r \equiv 3 \pmod{4}$.

□

Satz 5.2.3. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $v_2(r) \leq 1$ oder $v_2(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$, $r \equiv 0 \pmod{2}$ und $s \equiv 0 \pmod{4}$. Seien $x, y \in \mathbb{Z}$. Dann ist $\frac{x+y\theta+\theta^2}{4} \notin O_{2,K}$.*

Beweis. Angenommen es ist $\frac{x+y\theta+\theta^2}{4} \in O_{2,K}$. Aus dem Satz 5.1.8 folgt, dass $X_3(r,s,x,y,1) \equiv 0 \pmod{4}$, $Y_3(r,s,x,y,1) \equiv 0 \pmod{16}$ und $Z_3(r,s,x,y,1) \equiv 0 \pmod{64}$ ist. Es ist

$$0 \equiv X_3(r,s,x,y,1) = 2r + 3x \equiv 3x \pmod{4}$$

und $x \equiv 0 \pmod{4}$. Es ist

$$0 \equiv Y_3(r,s,x,y,1) = r^2 + 4rx - ry^2 + 3sy + 3x^2 \equiv -ry^2 \equiv ry \pmod{4}.$$

Es ist

$$0 \equiv Z_3(r,s,x,y,1) = r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3 \equiv -sy^3 \equiv sy \pmod{8}.$$

Es ist

$$ry \equiv 0 \pmod{4}$$
$$sy \equiv 0 \pmod{8}$$

Aus dem Satz 5.1.7 folgt, dass $y \equiv 0 \pmod{2}$ ist. Es ist

$$0 \equiv Y_3(r,s,x,y,1) = r^2 + 4rx - ry^2 + 3sy + 3x^2 \equiv r^2 \pmod{8},$$

$r \equiv 0 \pmod{4}$ und $s \not\equiv 0 \pmod{8}$. Es ist

$$0 \equiv Z_3(r,s,x,y,1) = r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3 \equiv s^2 \pmod{32}$$

und $s \equiv 0 \pmod{8}$. Dies ist ein Widerspruch. □

Satz 5.2.4. *Seien $r, s \in \mathbb{Z}$. Sei $r \equiv 3 \pmod{4}$, $s \equiv 2 \pmod{4}$ und $\Delta = 4r^3 - 27s^2$, dann ist $v_2(\Delta) \geq 4$.*

Beweis. Es ist

$$\Delta = 4r^3 - 27s^2 = 4r^3 - 27(s-2)^2 - 4 \cdot 27s + 4 \cdot 27 \equiv 4 \cdot 27 - 8 \cdot 27 + 4 \cdot 27 = 0 \pmod{16}.$$

□

Satz 5.2.5. *Sei $P(T) \in \mathbb{Z}[T]$ und $P(T) = T^3 - 3T + 2$, dann ist $P(T)$ reduzibel über $\mathbb{Q}$.*

Beweis. $P(T) = T^3 - 3T + 2 = (T^2 + T - 2)(T - 1)$ □

Satz 5.2.6. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\nu_2(r) \leq 1$ oder $\nu_2(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$, $\Delta = 4r^3 - 27s^2$, $r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$ und $m = \left\lfloor \frac{\nu_2(\Delta)}{2} \right\rfloor$. Seien $x, y \in \mathbb{Z}$. Sei $\frac{x+y\theta+\theta^2}{2^m} \in O_{2,K}$, dann ist $\nu_2(\Delta) \equiv 0 \pmod 2$ und $\frac{\Delta}{2^{\nu_2(\Delta)}} = 1 \pmod 4$.*

Beweis. Aus dem Satz 5.2.4 folgt, dass $\nu_2(\Delta) \geq 4$ ist. Aus dem Satz 5.2.2 folgt, dass $y \equiv 1 \pmod 2$ ist. Aus dem Satz 5.1.8 folgt, dass $X_3(r,s,x,y,1) \equiv 0 \pmod{2^m}$, $Y_3(r,s,x,y,1) \equiv 0 \pmod{2^{2m}}$ und $Z_3(r,s,x,y,1) \equiv 0 \pmod{2^{3m}}$ ist. Aus dem Satz 5.1.9 folgt, dass

$$-Y_3(r,s,x,y,1) = \frac{1}{12r^2}\left(-4r^2X_3(r,s,x,y,1)^2 + U_3(r,s,y,1)^2 + 3y^2\Delta\right)$$

ist. Es ist

$$0 \equiv -12r^2Y_3(r,s,x,y,1) = -4r^2X_3(r,s,x,y,1)^2 + U_3(r,s,y,1)^2 + 3y^2\Delta \equiv U(r,s,y,1)^2 + 3y^2\Delta \pmod{2^{2m+2}}.$$

Es ist $m+1 = \left\lfloor \frac{\nu_2(\Delta)}{2} \right\rfloor + 1 > \frac{\nu_2(\Delta)}{2}$. Es folgt, dass $2m+2 > \nu_2(\Delta)$ und $3y^2\Delta \not\equiv 0 \pmod{2^{2m+2}}$ ist. Es folgt, dass

$$2(\nu_2(U(r,s,y,1))) = \nu_2\left(U(r,s,y,1)^2\right) = \nu_2\left(3y^2\Delta\right) = \nu_2(\Delta)$$

ist. Es ist $\nu_2(\Delta) \equiv 0 \pmod 2$ und $m = \left\lfloor \frac{\nu_2(\Delta)}{2} \right\rfloor = \frac{\nu_2(\Delta)}{2} = \nu_2(U(r,s,y,1))$. Es ist $\nu_2(\Delta) = 2m$ und $U(r,s,y,1) \equiv 2^m \pmod{2^{m+1}}$. Aus dem Satz 1.2.6 folgt, dass $U(r,s,y,1)^2 \equiv 2^{2m} \pmod{2^{2m+2}}$ ist. Es ist

$$0 \equiv U(r,s,y,1)^2 + 3y^2\Delta \equiv 2^{2m} + 3y^2\Delta = 2^{2m}\left(1 + 3y^2\frac{\Delta}{2^{\nu_2(\Delta)}}\right) \pmod{2^{2m+2}}.$$

Es ist $1 + 3y^2\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 0 \pmod 4$. Es ist $1 + y^2 \not\equiv 0 \pmod 4$ und $\frac{\Delta}{2^{\nu_2(\Delta)}} \not\equiv 3 \pmod 4$. Es ist $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 1 \pmod 4$. □

Der Beweis des folgenden Satzes folgt einem Teil des Beweises des „Case A8“ und einem Teil des Beweises des „Case A9“ des Satzes 2.2.1 in der Doktorarbeit von Alaca [1].

Satz 5.2.7. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$, $r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$, $\Delta = 4r^3 - 27s^2$ und $m = \left\lfloor \frac{\nu_2(\Delta)}{2} \right\rfloor - 1$. Seien $x, y \in \mathbb{Z}$. Sei $3x \equiv -2r \pmod{2^m}$ und $ry \equiv 3\frac{s}{2} \pmod{2^m}$, dann ist $\frac{x+y\theta+\theta^2}{2^m} \in O_{2,K}$.*

Beweis. Es ist

$$X_3(r,s,x,y,1) = 2r + 3x \equiv 2r - 2r = 0 \pmod{2^m}.$$

Es ist $m \leq \frac{\nu_2(\Delta)}{2} - 1$. Es folgt, dass $2m+2 \leq \nu_2(\Delta)$ und $\Delta \equiv 0 \pmod{2^{2m+2}}$ ist. Es ist

$$3sU(r,s,y,1) = 3s\left(-2r^2 + 9sy\right) = -6r^2s + 27s^2y = -6r^2s + \left(4r^3 - \Delta\right)y \equiv$$
$$-6r^2s + 4r^2(ry) \equiv -6r^2s + 4r^2 \cdot 3\frac{s}{2} = 0 \pmod{2^{m+2}}.$$

Es ist $U(r,s,y,1) \equiv 0 \pmod{2^{m+1}}$. Es ist $V(r,s,y,1) = 2ry - 3s \equiv 0 \pmod{2^{m+1}}$. Aus dem Satz 5.1.9 folgt, dass

$$12r^2Y_3(r,s,x,y,1) = 4r^2X_3(r,s,x,y,1)^2 - U(r,s,y,1)^2 - 3y^2\Delta$$

ist. Es ist $12r^2Y_3(r,s,x,y,1) \equiv 0 \pmod{2^{2m+2}}$. Es folgt, dass $Y_3(r,s,x,y,1) \equiv 0 \pmod{2^{2m}}$ ist. Aus dem Satz 5.1.9 folgt, dass

$$4 \cdot 27r^3Z_3(r,s,x,y,1) =$$
$$4r^3X_3(r,s,x,y,1)^3 - 3rX_3(r,s,x,y,1)U(r,s,y,1)^2 - 9ry^2\Delta X_3(r,s,x,y,1)$$
$$-3U(r,s,y,1)^3 + 2r\Delta U(r,s,y,1) - 9y^2\Delta U(r,s,y,1) + 27sV(r,s,y,1)^3$$
$$+18s\Delta V(r,s,y,1) - \Delta^2$$

ist. Es ist $4 \cdot 27r^3Z_3(r,s,x,y,1) \equiv 0 \pmod{2^{3m+2}}$. Es ist $Z_3(r,s,x,y,1) \equiv 0 \pmod{2^{3m}}$. Aus dem Satz 5.1.8 folgt, dass $\frac{x+y\theta+\theta^2}{2^m} \in O_{2,K}$ ist. □

Der Beweis des folgenden Satzes folgt im Wesentlichen dem Beweis des „Case A10“ des Satzes 2.2.1 in der Doktorarbeit von Alaca [1].

Satz 5.2.8. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r,s \in \mathbb{Z}$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$, $r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$, $\Delta = 4r^3 - 27s^2$, $\nu_2(\Delta) \equiv 0 \pmod 2$, $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 1 \pmod 4$ und $m = \frac{\nu_2(\Delta)}{2}$. Seien $x,y \in \mathbb{Z}$. Sei $3x \equiv -2r \pmod{2^m}$ und $ry \equiv 3\frac{s}{2} + 2^{m-1} \pmod{2^m}$, dann ist $\frac{x+y\theta+\theta^2}{2^m} \in O_{2,K}$.*

Beweis. Aus dem Satz 5.2.4 folgt, dass $\nu_2(\Delta) \geq 4$ ist. Es folgt, dass $y \equiv 1 \pmod 2$ und $y^2 \equiv 1 \pmod 4$ ist. Es ist

$$X_3(r,s,x,y,1) = 2r + 3x \equiv 2r - 2r = 0 \pmod{2^m}.$$

Es ist $2m = \nu_2(\Delta)$ und $\Delta \equiv 0 \pmod{2^{2m}}$. Es ist

$$3sU(r,s,y,1) = 3s\left(-2r^2 + 9sy\right) = -6r^2s + 27s^2y = -6r^2s + \left(4r^3 - \Delta\right)y \equiv$$
$$-6r^2s + 4r^2(ry) \equiv -6r^2s + 4r^2\left(3\frac{s}{2} + 2^{m-1}\right) = 2^{m+1}r^2 \equiv 2^{m+1} \pmod{2^{m+2}}.$$

Es ist $U(r,s,y,1) \equiv 2^m \pmod{2^{m+1}}$. Aus dem Satz 1.2.6 folgt, dass $U(r,s,y,1)^2 \equiv 2^{2m} \pmod{2^{2m+2}}$ ist. Es ist

$$V(r,s,y,1) = 2ry - 3s \equiv 3s + 2^m - 3s = 2^m \pmod{2^{m+1}}.$$

Aus dem Satz 1.2.6 folgt, dass $V(r,s,x,y,1)^2 \equiv 2^{2m} \pmod{2^{2m+2}}$ ist. Aus dem Satz 5.1.9 folgt, dass $12r^2Y_3(r,s,x,y,1) = 4r^2X_3(r,s,x,y,1)^2 - U(r,s,y,1)^2 - 3y^2\Delta$ ist. Es ist

$$\begin{aligned}12r^2Y_3(r,s,x,y,1) = 4r^2X_3(r,s,x,y,1)^2 - U(r,s,y,1)^2 - 3y^2\Delta \equiv -2^{2m} + \Delta = \\ -2^{2m}\left(1 - \frac{\Delta}{2^{2m}}\right) \equiv -2^{2m}(1-1) = 0 \pmod{2^{2m+2}}.\end{aligned}$$

Es folgt, dass $Y_3(r,s,x,y,1) \equiv 0 \pmod{2^{2m}}$ ist. Aus dem Satz 5.1.9 folgt, dass

$$\begin{aligned}4 \cdot 27r^3Z_3(r,s,x,y,1) = \\ 4r^3X_3(r,s,x,y,1)^3 - 3rX_3(r,s,x,y,1)U(r,s,y,1)^2 - 9ry^2\Delta X_3(r,s,x,y,1) \\ -3U(r,s,y,1)^3 + 2r\Delta U(r,s,y,1) - 9y^2\Delta U(r,s,y,1) + 27sV(r,s,y,1)^3 \\ +18s\Delta V(r,s,y,1) - \Delta^2\end{aligned}$$

ist. Es ist

$$\begin{aligned}4 \cdot 27r^3Z_3(r,s,x,y,1) = \\ 4r^3X_3(r,s,x,y,1)^3 - 3rX_3(r,s,x,y,1)U(r,s,y,1)^2 - 9ry^2\Delta X_3(r,s,x,y,1) \\ -3U(r,s,y,1)^3 + 2r\Delta U(r,s,y,1) - 9y^2\Delta U(r,s,y,1) + 27sV(r,s,y,1)^3 \\ +18s\Delta V(r,s,y,1) - \Delta^2 \equiv \\ 3X_3(r,s,x,y,1)2^{2m} + \Delta X_3(r,s,x,y,1) + 2^{2m}U(r,s,y,1) + 2 \cdot 2^{2m} \cdot 2^m \\ +3\Delta U(r,s,y,1) + 2 \cdot 2^{3m} = \\ 2^{2m}X_3(r,s,x,y,1)\left(3 + \frac{\Delta}{2^{2m}}\right) + 2^{2m}U(r,s,y,1)\left(1 + 3\frac{\Delta}{2^{2m}}\right) + 2^{3m+2} \equiv 0 \\ \pmod{2^{3m+2}}.\end{aligned}$$

Es folgt, dass $Z_3(r,s,x,y,1) \equiv 0 \pmod{2^{3m}}$ ist. Aus dem Satz 5.1.8 folgt, dass $\frac{x+y\theta+\theta^2}{2^m} \in O_{2,K}$ ist. □

Die 2-ganzen Basen des folgenden Satzes stimmen mit den 2-ganzen Basen des Satzes 2.2.1 in der Doktorarbeit von Alaca [1] überein. Wenn eine der Voraussetzungen der Punkte 1, 2, 3 oder 5 des folgenden Satzes erfüllt ist, dann stimmen die 2-ganzen Basen auch mit den 2-ganzen Basen des Korollars 2.2.1 in [1] überein. Im Falle, dass die Voraussetzung des Punktes 4 erfüllt ist, stellt Alaca etwas strengere Bedingungen an x_0 und y_0 in dem Korollar 2.2.1 in [1][5].

[5] Alaca verwendet andere Variablennamen.

Satz 5.2.9. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\nu_2(r) \leq 1$ oder $\nu_2(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$ und $\Delta = 4r^3 - 27s^2$, dann sind alle fünf folgenden Punkte erfüllt:*

1. *Wenn ($r \not\equiv 3 \pmod 4$ und $s \not\equiv 0 \pmod 4$) oder ($r \equiv 3 \pmod 4$ und $s \not\equiv 2 \pmod 4$) ist, dann ist $\left(1, \theta, \theta^2\right)$ eine 2-ganze Basis von K.*
2. *Wenn $r \equiv 0 \pmod 2$ und $s \equiv 0 \pmod 4$ ist, dann ist $\left(1, \theta, \frac{\theta^2}{2}\right)$ eine 2-ganze Basis von K.*
3. *Wenn $r \equiv 1 \pmod 4$ und $s \equiv 0 \pmod 4$ ist, dann ist $\left(1, \theta, \frac{\theta+\theta^2}{2}\right)$ eine 2-ganze Basis von K.*
4. *Wenn $r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$, ($\nu_2(\Delta) \equiv 1 \pmod 2$ oder $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 3 \pmod 4$), $m_0 = \left\lfloor \frac{\nu_2(\Delta)}{2} \right\rfloor - 1$, $x_0, y_0 \in \mathbb{Z}$, $3x_0 \equiv -2r \pmod{2^{m_0}}$ und $ry_0 \equiv 3\frac{s}{2} \pmod{2^{m_0}}$ ist, dann ist $\left(1, \theta, \frac{x_0+y_0\theta+\theta^2}{2^{m_0}}\right)$ eine 2-ganze Basis von K.*
5. *Wenn $r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$, $\nu_2(\Delta) \equiv 0 \pmod 2$, $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 1 \pmod 4$, $m_1 = \frac{\nu_2(\Delta)}{2}$, $x_1, y_1 \in \mathbb{Z}$, $3x_1 \equiv -2r \pmod{2^{m_1}}$ und $ry_1 \equiv 3\frac{s}{2} + 2^{m_1-1} \pmod{2^{m_1}}$ ist, dann ist $\left(1, \theta, \frac{x_1+y_1\theta+\theta^2}{2^{m_1}}\right)$ eine 2-ganze Basis von K.*

Beweis. Es ist 1 ein minimal-ganzes Element von K über $\mathbb{Z}_{(2)}$ vom Grad 0 bezüglich $\left(1, \theta, \theta^2\right)$. Aus dem Satz 5.2.1 folgt, dass θ ein minimal-ganzes Element von K über $\mathbb{Z}_{(2)}$ vom Grad 1 bezüglich $\left(1, \theta, \theta^2\right)$ ist.

1 Aus dem Satz 5.2.2 folgt, dass θ^2 ein minimal-ganzes Element von K über $\mathbb{Z}_{(2)}$ vom Grad 2 bezüglich $\left(1, \theta, \theta^2\right)$ ist. Aus dem Satz 5.1.10 folgt, dass $\left(1, \theta, \theta^2\right)$ eine 2-ganze Basis von K ist.

2 Es ist $X_3(r, s, 0, 0, 1) = 2r \equiv 0 \pmod 2$, $Y_3(r, s, 0, 0, 1) = r^2 \equiv 0 \pmod 4$ und $Z_3(r, s, 0, 0, 1) = s^2 \equiv 0 \pmod 8$. Aus dem Satz 5.1.8 folgt, dass $\frac{\theta^2}{2} \in O_{2,K}$ ist. Aus dem Satz 5.2.3 folgt, dass $\frac{\theta^2}{2}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(2)}$ vom Grad 2 bezüglich $\left(1, \theta, \theta^2\right)$ ist. Aus dem Satz 5.1.10 folgt, dass $\left(1, \theta, \frac{\theta^2}{2}\right)$ eine 2-ganze Basis von K ist.

3 Es ist $X_3(r, s, 0, 1, 1) = 2r \equiv 0 \pmod 2$, $Y_3(r, s, 0, 1, 1) = r^2 - r + 3s \equiv 0 \pmod 4$ und $Z_3(r, s, 0, 1, 1) = rs + s^2 - s \equiv s - s = 0 \pmod 8$. Aus dem Satz 5.1.8 folgt, dass $\frac{\theta+\theta^2}{2} \in O_{2,K}$ ist. Es ist $\nu_2(\Delta) = \nu_2\left(4r^3 - 27s^2\right) = 2$. Aus dem Satz 5.1.12 folgt, dass $\left(1, \theta, \frac{\theta+\theta^2}{2}\right)$ eine 2-ganze Basis von K ist.

4 Aus dem Satz 5.2.7 folgt, dass $\frac{x_0+y_0\theta+\theta^2}{2^m} \in O_{2,K}$ ist. Aus dem Satz 5.2.6 folgt, dass $\frac{x_0+y_0\theta+\theta^2}{2^m}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(2)}$ vom Grad 2 bezüglich $\left(1, \theta, \theta^2\right)$ ist. Aus dem Satz 5.1.10 folgt, dass $\left(1, \theta, \frac{x_0+y_0\theta+\theta^2}{2^m}\right)$ eine 2-ganze Basis von K ist.

5 Aus dem Satz 5.2.8 folgt, dass $\frac{x_1+y_1\theta+\theta^2}{2^m} \in O_{2,K}$ ist. Aus dem Satz 5.1.12 folgt, dass $\left(1, \theta, \frac{x_1+y_1\theta+\theta^2}{2^m}\right)$ eine 2-ganze Basis von K ist.

□

Satz 5.2.10. *Sei $r, s \in \mathbb{Z}$, dann gilt einer der fünf folgenden Punkte:*

1. *($r \not\equiv 3 \pmod 4$ und $s \not\equiv 0 \pmod 4$) oder ($r \equiv 3 \pmod 4$ und $s \not\equiv 2 \pmod 4$)*
2. $r \equiv 0 \pmod 2$ *und* $s \equiv 0 \pmod 4$
3. $r \equiv 1 \pmod 4$ *und* $s \equiv 0 \pmod 4$
4. $r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$ *und* ($\nu_2(\Delta) \equiv 1 \pmod 2$ *oder* $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 3 \pmod 4$)
5. $r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$, $\nu_2(\Delta) \equiv 0 \pmod 2$ *und* $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 1 \pmod 4$

Beweis. Angenommen die Punkte 1 bis 5 sind alle nicht erfüllt. Da der Punkt 2 nicht erfüllt ist, folgt, dass $r \not\equiv 0 \pmod 2$ oder $s \not\equiv 0 \pmod 4$ ist. Da der Punkt 3 nicht erfüllt ist, folgt, dass $r \not\equiv 1 \pmod 4$ oder $s \not\equiv 0 \pmod 4$ ist. Es folgt, dass $r \equiv 3 \pmod 4$ oder $s \not\equiv 0 \pmod 4$ ist. Da der Punkt 1 nicht erfüllt ist, folgt, dass $r \equiv 3 \pmod 4$ oder $s \equiv 0 \pmod 4$ ist. Es ist $r \equiv 3 \pmod 4$. Da der Punkt 1 nicht erfüllt ist, folgt, dass $s \equiv 2 \pmod 4$ ist. Da der Punkt 4 nicht erfüllt ist, folgt, dass $\nu_2(\Delta) \equiv 0 \pmod 2$ und $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 1 \pmod 4$ ist. Der Punkt 5 ist erfüllt. Dies ist ein Widerspruch. □

5.3 3-ganze Basen

Satz 5.3.1. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\nu_3(r) \leq 1$ oder $\nu_3(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$ und $x \in \mathbb{Z}$, dann sind die beiden folgenden Punkte äquivalent:*

1. $\frac{x+\theta}{3} \in O_{3,K}$
2. $r \equiv 3 \pmod 9$, $s^2 \equiv r + 1 \pmod{27}$ *und* $x \equiv s \pmod 3$

Beweis.

(1 ⇒ 2) Aus dem Satz 5.1.8 folgt, dass $X_3(r, s, x, 1, 0) \equiv 0 \pmod 3$, $Y_3(r, s, x, 1, 0) \equiv 0 \pmod 9$ und $Z_3(r, s, x, 1, 0) \equiv 0 \pmod{27}$ ist. Es ist

$$0 \equiv Y_3(r, s, x, 1, 0) = -r + 3x^2 \equiv -r \pmod 3$$

und $r \equiv 0 \pmod 3$. Es ist

$$0 \equiv Z_3(r, s, x, 1, 0) = -rx - s + x^3 \equiv -s + x \pmod 3$$

und $x \equiv s \pmod 3$. Es ist

$$0 \equiv Y_3(r, s, x, 1, 0) = -r + 3x^2 \equiv -r + 3s^2 \pmod 9$$

und $r \equiv 3s^2 \pmod{9}$. Es ist $s \not\equiv 0 \pmod{27}$. Es ist

$$\begin{aligned} Z_3(r,s,x,1,0) = -rx - s + x^3 = -rx - s + x(x-s)^2 + 2sx^2 - s^2x = \\ -rx - s + x(x-s)^2 + 2s(x-s)^2 + 4s^2x - 2s^3 - s^2x = \\ -rx - s + x(x-s)^2 + 2s(x-s)^2 + 3s^2x - 2s^3 = \\ -r(x-s) - rs - s + x(x-s)^2 + 2s(x-s)^2 + 3s^2(x-s) + s^3 \equiv \\ -3s^2(x-s) - rs - s + s(x-s)^2 + 2s(x-s)^2 + 3s^2(x-s) + s^3 = \\ -rs - s + 3s(x-s)^2 + s^3 \equiv -rs - s + s^3 = s\left(-r - 1 + s^2\right) \pmod{27}. \end{aligned} \tag{5.2}$$

Es ist

$$0 \equiv Z_3(r,s,x,1,0) \equiv s\left(-r - 1 + s^2\right) \pmod{27},$$

$0 \equiv -r - 1 + s^2 \equiv -1 + s^2 \pmod{3}$, $s^2 \equiv 1 \pmod{3}$ und $s \not\equiv 0 \pmod{3}$. Es ist $s^2 \equiv r + 1 \pmod{27}$ und $0 \equiv -r - 1 + s^2 \equiv -3s^2 - 1 + s^2 = -2s^2 - 1 \pmod{9}$. Es ist $s^2 \equiv 4 \pmod{9}$ und $r \equiv s^2 - 1 \equiv 4 - 1 = 3 \pmod{9}$.

(2 $\Rightarrow$ 1) Es ist $x^2 \equiv s^2 \equiv 1 \pmod{3}$. Es ist $X_3(r,s,x,1,0) = 3x \equiv 0 \pmod{3}$ und

$$Y_3(r,s,x,1,0) = -r + 3x^2 \equiv -3 + 3 = 0 \pmod{9}.$$

Wie in (5.2) ergibt sich folgende Rechnung:

$$\begin{aligned} Z_3(r,s,x,1,0) = -rx - s + x^3 = -rx - s + x(x-s)^2 + 2sx^2 - s^2x = \\ -rx - s + x(x-s)^2 + 2s(x-s)^2 + 4s^2x - 2s^3 - s^2x = \\ -rx - s + x(x-s)^2 + 2s(x-s)^2 + 3s^2x - 2s^3 = \\ -r(x-s) - rs - s + x(x-s)^2 + 2s(x-s)^2 + 3s^2(x-s) + s^3 \equiv \\ -3s^2(x-s) - rs - s + s(x-s)^2 + 2s(x-s)^2 + 3s^2(x-s) + s^3 = \\ -rs - s + 3s(x-s)^2 + s^3 \equiv -rs - s + s^3 = s\left(-r - 1 + s^2\right) \pmod{27}. \end{aligned}$$

Es ist $Z_3(r,s,x,1,0) \equiv 0 \pmod{27}$. Aus dem Satz 5.1.8 folgt, dass $\frac{x+\theta}{3} \in O_{3,K}$ ist.

□

Satz 5.3.2. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $v_3(r) \leq 1$ oder $v_3(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$ und $K = \mathbb{Q}(\theta)$. Seien $x, y \in \mathbb{Z}$. Sei $\frac{x+y\theta+\theta^2}{3} \in O_{3,K}$. Dann ist $r \equiv 0 \pmod{3}$ und ($s \equiv 0 \pmod{9}$ oder $r + 1 \equiv s^2 \pmod{9}$).*

Beweis. Aus dem Satz 5.1.8 folgt, dass $X_3(r,s,x,y,1) \equiv 0 \pmod{3}$, $Y_3(r,s,x,y,1) \equiv 0 \pmod{9}$ und $Z_3(r,s,x,y,1) \equiv 0 \pmod{27}$ ist. Es ist

$$0 \equiv X_3(r,s,x,y,1) = 2r + 3x \equiv 2r \pmod{3}$$

und $r \equiv 0 \pmod{3}$.

Fall $s \equiv 0 \pmod 3$:
Es ist

$$0 \equiv Z_3(r,s,x,y,1) = r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3 \equiv x^3 \equiv x \pmod 3.$$

Es ist

$$0 \equiv Y_3(r,s,x,y,1) = r^2 + 4rx - ry^2 + 3sy + 3x^2 \equiv -ry^2 \pmod 9$$

und $ry \equiv 0 \pmod 9$. Es ist

$$0 \equiv Z_3(r,s,x,y,1) = r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3 \equiv s^2 - sy^3 \pmod{27}.$$

Es folgt, dass

$$ry \equiv 0 \pmod 9$$
$$sy^3 - s^2 \equiv 0 \pmod{27}$$

ist. Aus dem Satz 5.1.7 folgt, dass $y \equiv 0 \pmod 3$ ist. Es ist $0 \equiv sy^3 - s^2 \equiv -s^2 \pmod{27}$ und $s \equiv 0 \pmod 9$.

Fall $s \not\equiv 0 \pmod 3$:
Es folgt, dass $s^2 \equiv 1 \pmod 3$ ist. Es ist

$$0 \equiv Z_3(r,s,x,y,1) = r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3 \equiv 1 - sy + x \pmod 3$$

und $x \equiv sy - 1 \pmod 3$. Aus dem Satz 1.2.8 folgt, dass $x^3 = (sy-1)^3 \pmod 9$ ist.

Fall $sy \not\equiv 2 \pmod 3$ **und** $s \not\equiv 0 \pmod 3$:
Es ist

$$\begin{aligned}
0 \equiv Z_3(r,s,x,y,1) = r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3 \equiv \\
rsy + 2r(sy-1)^2 - r(sy-1)y^2 + s^2 + 3s(sy-1)y - sy^3 + (sy-1)^3 = \\
rsy + 2rs^2y^2 - 4rsy + 2r - rsy^3 + ry^2 + s^2 + 3s^2y^2 - 3sy - sy^3 + s^3y^3 - 3s^2y^2 \\
+3sy - 1 = \\
-3rsy + 2rs^2y^2 + 2r - rsy^3 + ry^2 + s^2 - sy^3 + s^3y^3 - 1 \equiv \\
-ry^2 - r - rsy + ry^2 + s^2 - sy^3 + s^3y^3 - 1 = \\
-r(sy+1) + s^2 + sy^3(s^2-1) - 1 \equiv \\
-r(sy+1) + s^2 + sy(s^2-1) - 1 = -r(sy+1) + (sy+1)(s^2-1) = \\
(sy+1)(-r + s^2 - 1) \pmod 9.
\end{aligned}$$

Es ist $r + 1 \equiv s^2 \pmod 9$.

Fall $sy \equiv 2 \pmod 3$:
Es folgt, dass $x \equiv 1 \pmod 3$, $y \equiv -s \pmod 3$ und $y^2 \equiv 1 \pmod 3$ ist. Es ist

$$\begin{aligned} 0 \equiv Z_3(r,s,x,y,1) = r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3 = \\ r^2(x-1) - r(s+y)^2 + 3r(sy+1) + 2r(x-1)^2 - r(x-1)(y^2-1) + 3r(x-1) \\ -s(s+y)^3 + 3s(s^2-1)(s+y) + 3(s^2-1)(y^2-1) + 3(s+y)^2 \\ +3(sy+1)(x-1) + (x-1)^3 + 3(x-1)^2 + r^2 + rs^2 - r - 2s^4 + 4s^2 - 2 \equiv \\ r^2 + rs^2 - r - 2s^4 + 4s^2 - 2 = \left(s^2 - r - 1\right)\left(-2s^2 - r + 2\right) = \\ \left(s^2 - r - 1\right)\left(-r - 2\left(s^2 - 1\right)\right) \equiv \left(s^2 - r - 1\right)\left(-r + s^2 - 1\right) = \\ \left(s^2 - r - 1\right)^2 \pmod{27}. \end{aligned}$$

Es ist $r + 1 \equiv s^2 \pmod 9$.

□

Satz 5.3.3. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $v_3(r) \leq 1$ oder $v_3(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$ und $K = \mathbb{Q}(\theta)$. Seien $x, y \in \mathbb{Z}$. Sei $\frac{x+y\theta+\theta^2}{9} \in O_{3,K}$. Dann ist $r \equiv 3 \pmod 9$ und $r + 1 = s^2 \pmod{27}$.*

Beweis. Sei $\Delta = 4r^3 - 27s^2$. Aus dem Satz 5.1.11 folgt, dass $2 \leq \frac{v_3(\Delta)}{2}$ ist und $\Delta \equiv 0 \pmod{3^4}$ ist. Es ist

$$0 \equiv \Delta\left(s^2 - 1\right) = \left(4r^3 - 27s^2\right)\left(s^2 - 1\right) \equiv 4r^3\left(s^2 - 1\right) \pmod{3^4}.$$

Es ist $r\left(s^2 - 1\right)^2 \equiv 0 \pmod 9$. Aus dem Satz 5.1.8 folgt, dass $X_3(r,s,x,y,1) \equiv 0 \pmod 9$, $Y_3(r,s,x,y,1) \equiv 0 \pmod{3^4}$ und $Z_3(r,s,x,y,1) \equiv 0 \pmod{3^6}$ ist. Es ist

$$\begin{aligned} 0 \equiv Y_3(r,s,x,y,1)\left(s^2-1\right)^2 = \left(r^2 + 4rx - ry^2 + 3sy + 3x^2\right)\left(s^2-1\right)^2 \equiv \\ 3x^2\left(s^2-1\right)^2 \pmod 9 \end{aligned}$$

und $x\left(s^2 - 1\right) \equiv 0 \pmod 3$. Es ist

$$\begin{aligned} 0 \equiv Z_3(r,s,x,y,1)\left(s^2-1\right)^2 = \\ \left(r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3\right)\left(s^2-1\right)^2 \equiv -sy\left(s^2-1\right)^2 \pmod 9 \end{aligned}$$

und $sy\left(s^2 - 1\right)^2 \equiv 0 \pmod 9$. Es ist

$$\begin{aligned} 0 \equiv Y_3(r,s,x,y,1)\left(s^2-1\right)^4 = \left(r^2 + 4rx - ry^2 + 3sy + 3x^2\right)\left(s^2-1\right)^4 \equiv \\ -ry^2\left(s^2-1\right)^4 \pmod{27} \end{aligned}$$

und $ry\left(s^2-1\right)^3 \equiv 0 \pmod{27}$. Es ist

$$\begin{aligned} 0 \equiv Z_3(r,s,x,y,1)\left(s^2-1\right)^3 = \\ \left(r^2x+rsy+2rx^2-rxy^2+s^2+3sxy-sy^3+x^3\right)\left(s^2-1\right)^3 \equiv \\ s^2\left(s^2-1\right)^3-sy^3\left(s^2-1\right)^2 \pmod{27}. \end{aligned}$$

Es ist

$$\begin{aligned} r\left(s^2-1\right)^2 &\equiv 0 \pmod{9} \\ sy^3\left(s^2-1\right)^2-s^2\left(s^2-1\right)^3 &\equiv 0 \pmod{27}. \end{aligned} \tag{5.3}$$

Aus dem Satz 5.1.7 folgt, dass $y\left(s^2-1\right) \equiv 0 \pmod{3}$ ist. Es ist

$$0 \equiv \left(sy^3\left(s^2-1\right)^2-s^2\left(s^2-1\right)^2\right)\left(s^2-1\right) \equiv -s^2\left(s^2-1\right)^3 \pmod{27}$$

und $s\left(s^2-1\right)^2 \equiv 0 \pmod{9}$. Es ist

$$\begin{aligned} 0 \equiv Z_3(r,s,x,y,1)\left(s^2-1\right)^4 = \\ \left(r^2x+rsy+2rx^2-rxy^2+s^2+3sxy-sy^3+x^3\right)\left(s^2-1\right)^4 \equiv x^3\left(s^2-1\right)^4 \left(\mathrm{mod}\ 3^4\right) \end{aligned}$$

und $x\left(s^2-1\right)^2 \equiv 0 \pmod{9}$. Es ist

$$\begin{aligned} 0 \equiv Z_3(r,s,x,y,1)\left(s^2-1\right)^5 = \\ \left(r^2x+rsy+2rx^2-rxy^2+s^2+3sxy-sy^3+x^3\right)\left(s^2-1\right)^5 \equiv s^2\left(s^2-1\right)^5 \pmod{3^5} \end{aligned}$$

und $s\left(s^2-1\right)^3 \equiv 0 \pmod{27}$. Es ist

$$\begin{aligned} r\left(s^2-1\right)^2 &\equiv 0 \pmod{9} \\ s\left(s^2-1\right)^3 &\equiv 0 \pmod{27} \end{aligned} \tag{5.4}$$

Aus dem Satz 5.1.7 folgt, dass $s^2-1 \equiv 0 \pmod{3}$ ist. Es ist $s \not\equiv 0 \pmod{3}$. Aus dem Satz 5.3.2 folgt, dass $r \equiv 0 \pmod{3}$ und $r+1 \equiv s^2 \pmod{9}$ ist. Es ist

$$\begin{aligned} 0 \equiv \Delta = 4r^3-27s^2 = 4(r-3)^3+36r^2-4\cdot 27r+4\cdot 27-27s^2 \equiv \\ 4(r-3)^3+4\cdot 27-27 = 4(r-3)^3+3^4 \equiv 4(r-3)^3 \left(\mathrm{mod}\ 3^4\right) \end{aligned}$$

und $r \equiv 3 \pmod{9}$. Es ist $s^2 \equiv r+1 \equiv 3+1 = 4 \pmod{9}$. Es ist

$$0 \equiv X_3(r,s,x,y,1) = 2r+3x \equiv 6+3x \pmod{9}$$

und $x \equiv 1 \pmod{3}$. Es ist

$$\begin{aligned} 0 \equiv Y_3(r,s,x,y,1) = r^2+4rx-ry^2+3sy+3x^2 \equiv \\ 3-3y^2+3sy+3 = 6-3y^2+3sy \pmod{9} \end{aligned}$$

und $y \not\equiv 0 \pmod 3$. Es ist $0 \equiv 6 - 3y^2 + 3sy \equiv 6 - 3 + 3sy = 3 + 3sy \pmod 9$, $sy \equiv 2 \pmod 3$ und $y \equiv -s \pmod 3$. Es ist

$$\begin{aligned}
0 \equiv Z_3(r,s,x,y,1) = r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3 = \\
(r-3)^2(x-1) + (r-3)^2 - (r-3)(s+y)^2(x-1) + 2(r-3)s(s+y)(x-1) \\
-(r-3)(s^2-4)(x-1) - (r-3)(s+y)^2 + 3(r-3)s(s+y) - 2(r-3)(s^2-4) \\
+2(r-3)(x-1)^2 + 6(r-3)(x-1) - s(s+y)^3 + 3(s+y)^2(s^2-4) - 3s(s+y)(s^2-4) \\
+(s^2-4)^2 - 3(s+y)^2(x-1) + 9s(s+y)(x-1) - 6(s^2-4)(x-1) + 9(s+y)^2 \\
+(x-1)^3 + 9(x-1)^2 \equiv \\
-s(s+y)^3 + (x-1)^3 \equiv (-s(s+y) + x - 1)^3 \pmod{3^4}.
\end{aligned}$$

Es ist $x - 1 \equiv s(s+y) \pmod 9$. Es ist

$$\begin{aligned}
0 \equiv Y_3(r,s,x,y,1) = r^2 + 4rx - ry^2 + 3sy + 3x^2 = \\
(r-3)^2 - (r-3)(s+y)^2 + 2(r-3)s(s+y) - (r-3)(s^2-4) + 4(r-3)(x-1) \\
+6(r-3) - 3(s+y)^2 + 9s(s+y) - 6(s^2-4) + 3(x-1)^2 + 18(x-1) \equiv \\
2(r-3)s(s+y) + (r-3)s(s+y) + 6(r-3) - 3(s+y)^2 + 9s(s+y) - 6(s^2-4) \\
+3(s+y)^2 + 18s(s+y) = \\
3(r-3)s(s+y) + 6(r-3) + 27s(s+y) - 6(s^2-4) \equiv 6(r-3) - 6(s^2-4) = \\
6(r+1-s^2) \pmod{3^4}.
\end{aligned}$$

Es folgt, dass $r + 1 \equiv s^2 \pmod{27}$ ist. □

Satz 5.3.4. *Seien $r, s \in \mathbb{Z}$. Sei $r \equiv 3 \pmod 9$, $s^2 \equiv r + 1 \pmod{27}$ und $\Delta = 4r^3 - 27s^2$, dann ist $\nu_3(\Delta) \geq 6$.*

Beweis. Es ist

$$\begin{aligned}
\Delta = 4r^3 - 27s^2 \equiv 4r^3 - 27(r+1) = 4r(r-3)^2 + 24r^2 - 36r - 27r - 27 = \\
4r(r-3)^2 + 24(r-3)^2 + 144r - 8 \cdot 27 - 63r - 27 = 4r(r-3)^2 + 24(r-3)^2 + 81r - 3^5 = \\
4r(r-3)^2 + 24(r-3)^2 + 81(r-3) \equiv 12(r-3)^2 + 24(r-3)^2 = \\
36(r-3)^2 \equiv 0 \pmod{3^6}.
\end{aligned}$$

□

Der Beweis des folgenden Satzes folgt einem Teil des Beweises des „Case 11“ des Satzes 2.3.1 in der Doktorarbeit von Alaca [1].

Satz 5.3.5. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$, $\Delta = 4r^3 - 27s^2$, $r \equiv 3 \pmod 9$, $s^2 \equiv r + 1 \pmod{27}$ und $m = \left\lfloor \frac{\nu_3(\Delta)}{2} \right\rfloor - 1$. Seien $x, y \in \mathbb{Z}$. Sei $x \equiv -2\frac{r}{3} \pmod{3^m}$ und $2\frac{r}{3}y \equiv s \pmod{3^{m+1}}$, dann ist $\frac{x+y\theta+\theta^2}{3^m} \in O_{3,K}$.*

Beweis. Es ist $2m+2 \leq \nu_3(\Delta)$. Es folgt, dass $\Delta \equiv 0 \pmod{3^{2m+2}}$ ist. Es ist

$$X_3(r,s,x,y,1) = 2r+3x \equiv 2r-2r = 0 \pmod{3^{m+1}}$$

und

$$3sU(r,s,y,1) = 3s\left(-2r^2+9sy\right) = -6r^2s+27s^2y = -6r^2s+\left(4r^3-\Delta\right)y \equiv$$
$$-6r^2s+4r^3y \equiv -6r^2s+2r^2\cdot 3s = 0 \pmod{3^{m+4}}.$$

Es folgt, dass $U(r,s,y,1) \equiv 0 \pmod{3^{m+3}}$ ist. Es ist

$$V(r,s,y,1) = 2ry-3s \equiv 0 \pmod{3^{m+2}}.$$

Aus dem Satz 5.1.9 folgt, dass

$$12r^2Y_3(r,s,x,y,1) = 4r^2X_3(r,s,x,y,1)^2 - U(r,s,y,1)^2 - 3y^2\Delta$$

ist. Es ist $12r^2Y_3(r,s,x,y,1) \equiv 0 \pmod{3^{2m+3}}$. Es folgt, dass $Y_3(r,s,x,y,1) \equiv 0 \pmod{3^{2m}}$ ist. Aus dem Satz 5.1.9 folgt, dass

$$4\cdot 27r^3Z_3(r,s,x,y,1) =$$
$$4r^3X_3(r,s,x,y,1)^3 - 3rX_3(r,s,x,y,1)U(r,s,y,1)^2 - 9ry^2\Delta X_3(r,s,x,y,1)$$
$$-3U(r,s,y,1)^3 + 2r\Delta U(r,s,y,1) - 9y^2\Delta U(r,s,y,1) + 27sV(r,s,y,1)^3$$
$$+18s\Delta V(r,s,y,1) - \Delta^2$$

ist. Es ist $4\cdot 27r^3Z_3(r,s,x,y,1) \equiv 0 \pmod{3^{3m+6}}$. Es ist $Z_3(r,s,x,y,1) \equiv 0 \pmod{3^{3m}}$. Aus dem Satz 5.1.8 folgt, dass $\frac{x+y\theta+\theta^2}{3^m} \in O_{3,K}$ ist. □

Die 3-ganzen Basen des folgenden Satzes stimmen mit den 3-ganzen Basen des Satzes 2.3.1 und dem Korollar 2.3.1 in der Doktorarbeit von Alaca [1] überein.

Satz 5.3.6. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r,s \in \mathbb{Z}$. Sei $\nu_3(r) \leq 1$ oder $\nu_3(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$ und $\Delta = 4r^3 - 27s^2$, dann sind alle vier folgenden Punkte erfüllt:*

1. *Wenn $r \not\equiv 0 \pmod 3$ oder ($s \not\equiv 0 \pmod 9$ und $s^2 \not\equiv r+1 \pmod 9$) ist, dann ist $(1,\theta,\theta^2)$ eine 3-ganze Basis von K.*
2. *Wenn $r \equiv 0 \pmod 3$ und $s \equiv 0 \pmod 9$ ist, dann ist $\left(1,\theta,\frac{\theta^2}{3}\right)$ eine 3-ganze Basis von K.*
3. *Wenn $r \equiv 0 \pmod 3$, $s^2 \equiv r+1 \pmod 9$ und ($r \not\equiv 3 \pmod 9$ oder $s^2 \not\equiv r+1 \pmod{27}$) ist, dann ist $\left(1,\theta,\frac{1-s\theta+\theta^2}{3}\right)$ eine 3-ganze Basis von K.*
4. *Wenn $r \equiv 3 \pmod 9$, $s^2 \equiv r+1 \pmod{27}$, $m = \left\lfloor \frac{\nu_3(\Delta)}{2} \right\rfloor - 1$, $x,y \in \mathbb{Z}$, $x \equiv -2\frac{r}{3} \pmod{3^m}$, $2\frac{r}{3}y \equiv s \pmod{3^{m+1}}$ ist, dann ist $\left(1,\frac{s+\theta}{3},\frac{x+y\theta+\theta^2}{3^m}\right)$ eine 3-ganze Basis von K.*

Beweis. Es ist 1 ein minimal-ganzes Element von K über $\mathbb{Z}_{(3)}$ vom Grad 0 bezüglich $\left(1,\theta,\theta^2\right)$.

1 Aus dem Satz 5.3.1 folgt, dass θ ein minimal-ganzes Element von K über $\mathbb{Z}_{(3)}$ vom Grad 1 bezüglich $\left(1,\theta,\theta^2\right)$ ist. Aus dem Satz 5.3.2 folgt, dass θ^2 ein minimal-ganzes Element von K über $\mathbb{Z}_{(3)}$ vom Grad 2 bezüglich $\left(1,\theta,\theta^2\right)$ ist. Aus dem Punkt 2 des Satzes 5.1.10 folgt, dass $\left(1,\theta,\theta^2\right)$ eine 3-ganze Basis von K ist.

2 Aus dem Satz 5.3.1 folgt, dass θ ein minimal-ganzes Element von K über $\mathbb{Z}_{(3)}$ vom Grad 1 bezüglich $\left(1,\theta,\theta^2\right)$ ist. Es folgt, dass $X_3\left(r,s,0,0,1\right) = 2r \equiv 0 \pmod 3$, $Y_3\left(r,s,0,0,1\right) = r^2 \equiv 0 \pmod 9$ und $Z_3\left(r,s,0,0,1\right) = s^2 \equiv 0 \pmod{27}$. Aus dem Satz 5.1.8 folgt, dass $\frac{\theta^2}{3} \in O_{3,K}$ ist. Aus dem Satz 5.3.3 folgt, dass $\frac{\theta^2}{3}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(3)}$ vom Grad 2 bezüglich $\left(1,\theta,\theta^2\right)$ ist. Aus dem Punkt 2 des Satzes 5.1.10 folgt, dass $\left(1,\theta,\frac{\theta^2}{3}\right)$ eine 3-ganze Basis von K ist.

3 Aus dem Satz 5.3.1 folgt, dass θ ein minimal-ganzes Element von K über $\mathbb{Z}_{(3)}$ vom Grad 1 bezüglich $\left(1,\theta,\theta^2\right)$ ist. Es ist $s^2 = 1 \pmod 3$. Es ist $X_3\left(r,s,1,-s,1\right) = 2r+3 \equiv 0 \pmod 3$, $Y_3\left(r,s,1,-s,1\right) = r^2+4r-rs^2-3s^2+3 \equiv r-r-3+3 = 0 \pmod 9$ und

$$\begin{aligned} Z_3\left(r,s,1,-s,1\right) = r^2-rs^2+2r-rs^2+s^2-3s^2+s^4+1 = \\ r^2-2rs^2+2r-2s^2+s^2\left(s^2-1\right)+s^2+1 \equiv \\ r^2-2rs^2+2r-2s^2+(r+1)\left(s^2-1\right)+s^2+1 = r^2-rs^2+r \equiv \\ r^2-r\left(r+1\right)+r = 0 \pmod{27}. \end{aligned}$$

Aus dem Satz 5.1.8 folgt, dass $\frac{1-s\theta+\theta^2}{3} \in O_{3,K}$ ist. Aus dem Satz 5.3.3 folgt, dass $\frac{1-s\theta+\theta^2}{3}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(3)}$ vom Grad 2 bezüglich $\left(1,\theta,\theta^2\right)$ ist. Aus dem Punkt 2 des Satzes 5.1.10 folgt, dass $\left(1,\theta,\frac{1-s\theta+\theta^2}{3}\right)$ eine 3-ganze Basis von K ist.

4 Aus dem Satz 5.3.1 folgt, dass $\frac{s+\theta}{3} \in O_{3,K}$ ist. Aus dem Satz 5.3.5 folgt, dass $\frac{x+y\theta+\theta^2}{3^m} \in O_{3,K}$ ist. Es ist $1+m = \left\lfloor \frac{\nu_3(\Delta)}{2} \right\rfloor$. Aus dem Satz 5.1.12 folgt, dass $\left(1,\frac{s+\theta}{3},\frac{x+y\theta+\theta^2}{3^m}\right)$ eine 3-ganze Basis von K ist.

□

Satz 5.3.7. *Seien $r,s \in \mathbb{Z}$. Dann gilt einer der vier folgenden Punkte:*

1. $r \not\equiv 0 \pmod 3$ *oder* ($s \not\equiv 0 \pmod 9$ *und* $s^2 \not\equiv r+1 \pmod 9$)
2. $r \equiv 0 \pmod 3$ *und* $s \equiv 0 \pmod 9$
3. $r \equiv 0 \pmod 3$, $s^2 \equiv r+1 \pmod 9$ *und* ($r \not\equiv 3 \pmod 9$ *oder* $s^2 \not\equiv r+1 \pmod{27}$)
4. $r \equiv 3 \pmod 9$ *und* $s^2 \equiv r+1 \pmod{27}$

Beweis. Angenommen die Punkte 1 bis 4 sind alle nicht erfüllt. Da der Punkt 1 nicht erfüllt ist, folgt, dass $r \equiv 0 \pmod 3$ ist. Da der Punkt 2 nicht erfüllt ist, folgt, dass $s \not\equiv 0 \pmod 9$ ist. Da der Punkt 1 nicht erfüllt ist, folgt, dass $s^2 \equiv r+1 \pmod 9$ ist. Da der Punkt 3 nicht

erfüllt ist, folgt, dass $r \equiv 3 \pmod{9}$ und $s^2 \equiv r+1 \pmod{27}$ ist. Der Punkt 4 ist erfüllt. Dies ist ein Widerspruch. □

5.4 p-ganze Basen für $p \geq 5$

Satz 5.4.1. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei p eine Primzahl und $p \geq 5$. Sei $\nu_p(r) \leq 1$ oder $\nu_p(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$ und $x \in \mathbb{Z}$, dann ist $\frac{x+\theta}{p} \notin O_{p,K}$.*

Beweis. Angenommen es ist $\frac{x+\theta}{p} \in O_{p,K}$. Aus dem Satz 5.1.8 folgt, dass $X_3(r,s,x,1,0) \equiv 0 \pmod{p}$, $Y_3(r,s,x,1,0) \equiv 0 \pmod{p^2}$ und $Z_3(r,s,x,1,0) \equiv 0 \pmod{p^3}$ ist. Es ist $0 \equiv X_3(r,s,x,1,0) = 3x \pmod{p}$. Es folgt, dass $x \equiv 0 \pmod{p}$ ist. Es ist

$$0 \equiv Y_3(r,s,x,1,0) = -r + 3x^2 \equiv -r \pmod{p^2}.$$

Es folgt, dass $r \equiv 0 \pmod{p^2}$ ist. Es folgt, dass $s \not\equiv 0 \pmod{p^3}$ ist. Es ist

$$0 \equiv Z_3(r,s,x,1,0) = -rx - s + x^3 \equiv -s \pmod{p^3}.$$

Es folgt, dass $s \equiv 0 \pmod{p^3}$ ist. Dies ist ein Widerspruch. □

Satz 5.4.2. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei p eine Primzahl und $p \geq 5$. Sei $\nu_p(r) \leq 1$ oder $\nu_p(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$ und $r \equiv 0 \pmod{p}$. Seien $x, y \in \mathbb{Z}$. Sei $\frac{x+y\theta+\theta^2}{p} \in O_{p,K}$. Dann ist $s \equiv 0 \pmod{p^2}$ und $x \equiv y \equiv 0 \pmod{p}$.*

Beweis. Aus dem Satz 5.1.11 folgt, dass $1 \leq \frac{\nu_p(\Delta)}{2}$ ist. Es ist

$$0 \equiv \Delta = 4r^3 - 27s^2 \equiv -27s^2 \pmod{p}$$

und $s \equiv 0 \pmod{p}$. Aus dem Satz 5.1.8 folgt, dass $X_3(r,s,x,y,1) \equiv 0 \pmod{p}$, $Y_3(r,s,x,y,1) \equiv 0 \pmod{p^2}$ und $Z_3(r,s,x,y,1) \equiv 0 \pmod{p^3}$ ist. Es folgt, dass $0 \equiv X_3(r,s,x,y,1) = 2r + 3x \equiv 3x \pmod{p}$ und $x \equiv 0 \pmod{p}$ ist. Es ist

$$0 \equiv Z_3(r,s,x,y,1) = r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3 \equiv -sy^3 \pmod{p^2}$$

und $sy \equiv 0 \pmod{p^2}$. Es ist

$$0 \equiv Y_3(r,s,x,y,1) = r^2 + 4rx - ry^2 + 3sy + 3x^2 = -ry^2 \pmod{p^2}$$

und $ry \equiv 0 \pmod{p^2}$. Es ist

$$0 \equiv Z_3(r,s,x,y,1) = r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3 \equiv s^2 - sy^3 \pmod{p^3}.$$

Es ist

$$ry \equiv 0 \pmod{p^2}$$
$$sy^3 - s^2 \equiv 0 \pmod{p^3}.$$

Aus dem Satz 5.1.7 folgt, dass $y \equiv 0 \pmod{p}$ ist. Es ist $0 \equiv s^2 - sy^3 \equiv s^2 \pmod{p^3}$ und $s \equiv 0 \pmod{p^2}$. □

Satz 5.4.3. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei p eine Primzahl, $p \geq 5$, $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$ und $r \not\equiv 0 \pmod{p}$. Seien $x, y \in \mathbb{Z}$. Sei $\frac{x+y\theta+\theta^2}{p} \in O_{p,K}$. Dann ist $s \not\equiv 0 \pmod{p}$.*

Beweis. Sei $\Delta = 4r^3 - 27s^2$. Aus dem Satz 5.1.11 folgt, dass $1 \leq \frac{\nu_p(\Delta)}{2}$ ist. Es ist $4r^3 - 27s^2 = \Delta \equiv 0 \pmod{p^2}$. Es folgt, dass $s \not\equiv 0 \pmod{p}$ ist. □

Satz 5.4.4. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei p eine Primzahl und $p \geq 5$. Sei $\nu_p(r) \leq 1$ oder $\nu_p(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$ und $K = \mathbb{Q}(\theta)$. Seien $x, y \in \mathbb{Z}$. Sei $\frac{x+y\theta+\theta^2}{p^2} \in O_{p,K}$. Dann ist $r \not\equiv 0 \pmod{p}$ und $s \not\equiv 0 \pmod{p}$.*

Beweis. Angenommen es ist $r \equiv 0 \pmod{p}$ oder es ist $s \equiv 0 \pmod{p}$. Aus dem Satz 5.1.8 folgt, dass $X_3(r, s, x, y, 1) \equiv 0 \pmod{p^2}$, $Y_3(r, s, x, y, 1) \equiv 0 \pmod{p^4}$ und $Z_3(r, s, x, y, 1) \equiv 0 \pmod{p^6}$ ist. Aus dem Satz 5.4.3 folgt, dass $r \equiv 0 \pmod{p}$ ist. Aus dem Satz 5.4.2 folgt, dass $s \equiv 0 \pmod{p^2}$ und $x \equiv y \equiv 0 \pmod{p}$ ist. Es ist $0 \equiv X_3(r, s, x, y, 1) = 2r + 3x \pmod{p^2}$ und $2r \equiv -3x \pmod{p^2}$. Es ist

$$\begin{aligned} 0 \equiv 4Y_3(r, s, x, y, 1) = 4\left(r^2 + 4rx - ry^2 + 3sy + 3x^2\right) \equiv 4\left(r^2 + 4rx + 3x^2\right) = \\ 4r^2 + 16rx + 12x^2 \equiv 9x^2 - 24x^2 + 12x^2 = -3x^2 \pmod{p^3}. \end{aligned}$$

Es folgt, dass $x \equiv 0 \pmod{p^2}$ ist. Es ist $2r \equiv -3x \equiv 0 \pmod{p^2}$ und $r \equiv 0 \pmod{p^2}$. Es folgt, dass $s \not\equiv 0 \pmod{p^3}$ ist. Es ist

$$0 \equiv Z_3(r, s, x, y, 1) = r^2x + rsy + 2rx^2 - rxy^2 + s^2 + 3sxy - sy^3 + x^3 \equiv s^2 \pmod{p^5}$$

und $s \equiv 0 \pmod{p^3}$. Dies ist ein Widerspruch. □

Der Beweis des folgenden Satzes folgt einem Teil des Beweises des „Case C5“ des Satzes 2.4.1 in der Doktorarbeit von Alaca [1].

Satz 5.4.5. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei p eine Primzahl und $p \geq 5$. Sei $\nu_p(r) \leq 1$ oder $\nu_p(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$, $\Delta = 4r^3 - 27s^2$, $r \not\equiv 0 \pmod{p}$, $s \not\equiv 0 \pmod{p}$ und $m = \left\lfloor \frac{\nu_p(\Delta)}{2} \right\rfloor$. Seien $x, y \in \mathbb{Z}$. Sei $3x \equiv -2r \pmod{p^m}$ und $2ry \equiv 3s \pmod{p^m}$, dann ist $\frac{x+y\theta+\theta^2}{p^m} \in O_{p,K}$.*

Beweis. Es ist $2m \leq \nu_p(\Delta)$. Es folgt, dass $\Delta \equiv 0 \pmod{p^{2m}}$ ist. Es folgt, dass $X_3(r, s, x, y, 1) = 2r + 3x \equiv 2r - 2r = 0 \pmod{p^m}$ und

$$\begin{aligned} 3sU(r, s, y, 1) = 3s\left(-2r^2 + 9sy\right) = -6r^2s + 27s^2y = -6r^2s + \left(4r^3 - \Delta\right)y \equiv \\ -6r^2s + 4r^3y = -6r^2s + 2ry \cdot 2r^2 \equiv -6r^2s + 3s \cdot 2r^2 = 0 \pmod{p^m} \end{aligned}$$

ist. Es folgt, dass $U(r, s, y, 1) \equiv 0 \pmod{p^m}$ ist. Es ist $V(r, s, y, 1) = 2ry - 3s \equiv 0 \pmod{p^m}$. Aus dem Satz 5.1.9 folgt, dass

$$12r^2Y_3(r, s, x, y, 1) = 4r^2X_3(r, s, x, y, 1)^2 - U(r, s, y, 1)^2 - 3y^2\Delta$$

ist. Es ist $12r^2Y_3(r,s,x,y,1) \equiv 0 \pmod{p^{2m}}$. Es folgt, dass $Y_3(r,s,x,y,1) \equiv 0 \pmod{p^{2m}}$ ist. Aus dem Satz 5.1.9 folgt, dass

$$\begin{aligned} 4 \cdot 27r^3 Z_3(r,s,x,y,1) = \\ 4r^3 X_3(r,s,x,y,1)^3 - 3rX_3(r,s,x,y,1)\, U(r,s,y,1)^2 - 9ry^2 \Delta X_3(r,s,x,y,1) \\ -3U(r,s,y,1)^3 + 2r\Delta U(r,s,y,1) - 9y^2 \Delta U(r,s,y,1) + 27sV(r,s,y,1)^3 \\ +18s\Delta V(r,s,y,1) - \Delta^2 \end{aligned}$$

ist. Es ist $4 \cdot 27r^3 Z_3(r,s,x,y,1) \equiv 0 \pmod{p^{3m}}$. Es folgt, dass $Z_3(r,s,x,y,1) \equiv 0 \pmod{p^{3m}}$ ist. Aus dem Satz 5.1.8 folgt, dass $\frac{x+y\theta+\theta^2}{p^m} \in O_{p,K}$ ist. □

Die p-ganzen Basen des folgenden Satzes stimmen für alle Primzahlen $p \geq 5$ mit den p-ganzen Basen des Satzes 2.4.1 und dem Korollar 2.4.1 in der Doktorarbeit von Alaca [1] überein.

Satz 5.4.6. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r,s \in \mathbb{Z}$. Sei p eine Primzahl und $p \geq 5$. Sei $\nu_p(r) \leq 1$ oder $\nu_p(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$ und $\Delta = 4r^3 - 27s^2$, dann sind alle drei folgenden Punkte erfüllt:*

1. *Wenn ($r \equiv 0 \pmod{p}$ und $s \not\equiv 0 \pmod{p^2}$) oder ($r \not\equiv 0 \pmod{p}$ und $s \equiv 0 \pmod{p}$) ist, dann ist $(1,\theta,\theta^2)$ eine p-ganze Basis von K.*
2. *Wenn $r \equiv 0 \pmod{p}$ und $s \equiv 0 \pmod{p^2}$ ist, dann ist $\left(1,\theta,\frac{\theta^2}{p}\right)$ eine p-ganze Basis von K.*
3. *Wenn $r \not\equiv 0 \pmod{p}$, $s \not\equiv 0 \pmod{p}$, $m = \left\lfloor \frac{\nu_p(\Delta)}{2} \right\rfloor$, $x,y \in \mathbb{Z}$, $3x \equiv -2r \pmod{p^m}$, $2ry \equiv 3s \pmod{p^m}$ ist, dann ist $\left(1,\theta,\frac{x+y\theta+\theta^2}{p^m}\right)$ eine p-ganze Basis von K.*

Beweis. Es ist 1 ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 0 bezüglich $(1,\theta,\theta^2)$. Aus dem Satz 5.4.1 folgt, dass θ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 1 bezüglich $(1,\theta,\theta^2)$ ist.

1 Aus dem Satz 5.4.2 und dem Satz 5.4.3 folgt, dass θ^2 ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 2 bezüglich $(1,\theta,\theta^2)$ ist. Aus dem Punkt 2 des Satzes 5.1.10 folgt, dass $(1,\theta,\theta^2)$ eine p-ganze Basis von K ist.

2 Es ist $X_3(r,s,0,0,1) = 2r \equiv 0 \pmod{p}$, $Y_3(r,s,0,0,1) = r^2 \equiv 0 \pmod{p^2}$ und $Z_3(r,s,0,0,1) = s^2 \equiv 0 \pmod{p^3}$. Aus dem Satz 5.1.8 folgt, dass $\frac{\theta^2}{p} \in O_{p,K}$ ist. Aus dem Satz 5.4.4 folgt, dass $\frac{\theta^2}{p}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 2 bezüglich $(1,\theta,\theta^2)$ ist. Aus dem Punkt 2 des Satzes 5.1.10 folgt, dass $\left(1,\theta,\frac{\theta^2}{p}\right)$ eine p-ganze Basis von K ist.

3 Aus dem Satz 5.4.5 folgt, dass $\frac{x+y\theta+\theta^2}{p^m} \in O_{p,K}$ ist. Aus dem Satz 5.1.12 folgt, dass $\left(1,\theta,\frac{x+y\theta+\theta^2}{p^m}\right)$ eine p-ganze Basis von K ist.

□

5.5 Ganzheitsbasen

Die Ganzheitsbasen des folgenden Satzes stimmen mit den Ganzheitsbasen des Satzes 2.6.1 in der Doktorarbeit von Alaca [1] überein, wenn $r \not\equiv 3 \pmod 4$, $s \not\equiv 2 \pmod 4$ oder ($\nu_2(\Delta) \equiv 0 \pmod 2$ und $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 1 \pmod 4$) ist. Wenn $r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$ und ($\nu_2(\Delta) \equiv 1 \pmod 2$ oder $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 3 \pmod 4$) ist, dann stellt Alaca etwas strengere Bedingungen an x_0 und y_0 in dem Satz 2.6.1 in [1][6].

Satz 5.5.1. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\nu_q(r) \leq 1$ oder $\nu_q(s) \leq 2$ für jede Primzahl q. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$ und $\Delta = 4r^3 - 27s^2$. Seien $n, w \in \mathbb{Z}$. Sei*

$$(n,w) = \begin{cases} (1,s) & \text{wenn } r \equiv 3 \pmod 9 \text{ und } s^2 \equiv r+1 \pmod{27} \\ (0,0) & \text{sonst} \end{cases}$$

Sei

$$m_2 = \begin{cases} 1 & \text{wenn } r \not\equiv 3 \pmod 4 \text{ und } s \equiv 0 \pmod 4 \\ \left\lfloor \frac{\nu_2(\Delta)}{2} \right\rfloor - 1 & \text{wenn } r \equiv 3 \pmod 4, s \equiv 2 \pmod 4 \text{ und} \\ & (\nu_2(\Delta) \equiv 1 \pmod 2 \text{ oder } \frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 3 \pmod 4) \\ \frac{\nu_2(\Delta)}{2} & \text{wenn } r \equiv 3 \pmod 4, s \equiv 2 \pmod 4, \nu_2(\Delta) \equiv 0 \pmod 2 \\ & \text{und } \frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 1 \pmod 4 \\ 0 & \text{sonst} \end{cases}$$

Sei

$$m_3 = \begin{cases} 0 & \text{wenn } r \not\equiv 0 \pmod 3 \text{ oder} \\ & (s \not\equiv 0 \pmod 9 \text{ und } s^2 \not\equiv r+1 \pmod 9) \\ \left\lfloor \frac{\nu_3(\Delta)}{2} \right\rfloor - 1 & \text{wenn } r \equiv 3 \pmod 9 \text{ und } s^2 \equiv r+1 \pmod{27} \\ 1 & \text{sonst} \end{cases}$$

Für alle Primzahlen p, für die $p \geq 5$ gilt, sei

$$m_p = \begin{cases} 1 & \text{wenn } r \equiv 0 \pmod p \text{ und } s \equiv 0 \pmod{p^2} \\ \left\lfloor \frac{\nu_p(\Delta)}{2} \right\rfloor & \text{wenn } r \not\equiv 0 \pmod p \text{ und } s \not\equiv 0 \pmod p \\ 0 & \text{sonst} \end{cases}$$

Wenn $r \equiv 3 \pmod 4$ und $s \equiv 2 \pmod 4$ ist, dann sei $t_2 \in \mathbb{Z}$ und $3t_2 \equiv -2r \pmod{2^{m_2}}$. Wenn $r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$ und ($\nu_2(\Delta) \equiv 1 \pmod 2$ oder $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 3 \pmod 4$) ist, dann sei $u_{2,0} \in \mathbb{Z}$ und $ru_{2,0} \equiv 3\frac{s}{2} \pmod{2^{m_2}}$. Wenn $r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$, $\nu_2(\Delta) \equiv 0 \pmod 2$ und $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 1 \pmod 4$ ist, dann sei $u_{2,1} \in \mathbb{Z}$ und $ru_{2,1} \equiv 3\frac{s}{2} + 2^{m_2-1} \pmod{2^{m_2}}$. Wenn $r \equiv 3 \pmod 9$ und $s^2 \equiv r+1 \pmod{27}$ ist, dann sei $t_3, u_3 \in \mathbb{Z}$, $t_3 \equiv -2\frac{r}{3} \pmod{3^{m_3}}$ und $2\frac{r}{3}u_3 \equiv s \pmod{3^{m_3+1}}$. Wenn $r \not\equiv 0 \pmod p$ und $s \not\equiv 0 \pmod p$ ist, für eine Primzahl

[6] Alaca verwendet andere Variablennamen.

p, für die $p \geq 5$ gilt, dann sei $t_p, u_p \in \mathbb{Z}$, $3t_p \equiv -2r \pmod{p^{m_p}}$ und $2ru_p \equiv 3s \pmod{p^{m_p}}$. Sei

$$(x_2, y_2) = \begin{cases} (0,1) & \text{wenn } r \equiv 1 \pmod 4 \text{ und } s \equiv 0 \pmod 4 \\ (t_2, u_{2,0}) & \text{wenn } r \equiv 3 \pmod 4, s \equiv 2 \pmod 4 \text{ und} \\ & (\nu_2(\Delta) \equiv 1 \pmod 2 \text{ oder } \frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 3 \pmod 4) \\ (t_2, u_{2,1}) & \text{wenn } r \equiv 3 \pmod 4, s \equiv 2 \pmod 4, \nu_2(\Delta) \equiv 0 \pmod 2 \\ & \text{und } \frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 1 \pmod 4 \\ (0,0) & \text{sonst} \end{cases}$$

Sei

$$(x_3, y_3) = \begin{cases} (1, -s) & \text{wenn } r \equiv 0 \pmod 3, s^2 \equiv r+1 \pmod 9 \text{ und} \\ & (r \not\equiv 3 \pmod 9 \text{ oder } s^2 \not\equiv r+1 \pmod{27}) \\ (t_3, u_3) & \text{wenn } r \equiv 3 \pmod 9 \text{ und } s^2 \equiv r+1 \pmod{27} \\ (0,0) & \text{sonst} \end{cases}$$

Für alle Primzahlen p, für die $p \geq 5$ gilt, sei

$$(x_p, y_p) = \begin{cases} (t_p, u_p) & \text{wenn } r \not\equiv 0 \pmod p \text{ und } s \not\equiv 0 \pmod p \\ (0,0) & \text{sonst} \end{cases}$$

Sei $\mathcal{X} \in \mathbb{Z}$ und $\mathcal{X} \equiv x_p \pmod{p^{m_p}}$ für alle Primzahlen p. Sei $\mathcal{Y} \in \mathbb{Z}$ und $\mathcal{Y} \equiv y_p \pmod{p^{m_p}}$ für alle Primzahlen p. Dann ist $\left(1, \frac{w+\theta}{3^n}, \frac{\mathcal{X}+\mathcal{Y}\theta+\theta^2}{\prod_{p \text{ Primzahl}} p^{m_p}}\right)$ eine Ganzheitsbasis von K.

Beweis. Aus dem Satz 5.2.9 und dem Satz 5.2.10 folgt, dass $\left(1, \theta, \frac{x_2+y_2\theta+\theta^2}{2^{m_2}}\right)$ eine 2-ganze Basis von K ist. Aus dem Satz 5.3.6 und dem Satz 5.3.7 folgt, dass $\left(1, \frac{w+\theta}{3^n}, \frac{x_3+y_3\theta+\theta^2}{3^{m_3}}\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.4.6 folgt, dass $\left(1, \theta, \frac{x_p+y_p\theta+\theta^2}{2^{m_p}}\right)$ für alle Primzahlen p, für die $p \geq 5$ gilt, eine p-ganze Basis von K ist. Aus dem Satz 4.0.9 folgt, dass $\left(1, \frac{w+\theta}{3^n}, \frac{\mathcal{X}+\mathcal{Y}\theta+\theta^2}{\prod_{p \text{ Primzahl}} p^{m_p}}\right)$ eine Ganzheitsbasis von K ist. □

5.6 Diskriminante

Satz 5.6.1. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$, $\Delta = 4r^3 - 27s^2$ und p eine Primzahl. Seien $i, j \in \mathbb{N}$. Seien $u, x, y \in \mathbb{Z}$. Sei $\left(1, \frac{u+\theta}{p^i}, \frac{x+y\theta+\theta^2}{p^j}\right)$ eine p-ganze Basis von K, dann ist $\nu_p(d(K)) = \nu_p(\Delta) - 2(i+j)$.*

Beweis. Aus dem Satz 4.0.4 folgt, dass $\frac{u+\theta}{p^i}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 1 bezüglich $\left(1,\theta,\theta^2\right)$ und $\frac{x+y\theta+\theta^2}{p^j}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 2 bezüglich $\left(1,\theta,\theta^2\right)$ ist. Aus dem Punkt 3 des Satzes 5.1.10 folgt, dass $\nu_p\left(d\left(K\right)\right)=\nu_p\left(\Delta\right)-2\left(i+j\right)$ ist. □

Die Idee für die Fallunterscheidungen des folgenden Satzes stammt aus dem Satz 2.5.1 in der Doktorarbeit von Alaca [1].

Satz 5.6.2. *Sei $\theta\in\mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r,s\in\mathbb{Z}$. Sei $\nu_2\left(r\right)\leq 1$ oder $\nu_2\left(s\right)\leq 2$. Sei $\mathrm{irr}_{\theta,\mathbb{Q}}\left(T\right)=T^3-rT+s$, $K=\mathbb{Q}\left(\theta\right)$ und $\Delta=4r^3-27s^2$, dann sind alle drei folgenden Punkte erfüllt:*

1. *Wenn $s\equiv 1\pmod 2$, ($r\equiv 1\pmod 4$ und $s\equiv 0\pmod 4$) oder ($r\equiv 3\pmod 4$, $s\equiv 2\pmod 4$, $\nu_2\left(\Delta\right)\equiv 0\pmod 2$ und $\frac{\Delta}{2^{\nu_2(\Delta)}}\equiv 1\pmod 4$) ist, dann ist $\nu_2\left(d\left(K\right)\right)=0$.*
2. *Wenn ($r\equiv 0\pmod 2$ und $s\equiv 2\pmod 4$), ($r\equiv 0\pmod 2$ und $s\equiv 4\pmod 8$), ($r\equiv 3\pmod 4$ und $s\equiv 0\pmod 4$) oder ($r\equiv 3\pmod 4$, $s\equiv 2\pmod 4$, $\nu_2\left(\Delta\right)\equiv 0\pmod 2$ und $\frac{\Delta}{2^{\nu_2(\Delta)}}\equiv 3\pmod 4$) ist, dann ist $\nu_2\left(d\left(K\right)\right)=2$.*
3. *Wenn $\nu_2\left(\Delta\right)\equiv 1\pmod 2$ ist, dann ist $\nu_2\left(d\left(K\right)\right)=3$.*

Beweis.

Fall $s\equiv 1\pmod 2$:
Es ist $\nu_2\left(\Delta\right)=0$. Aus dem Punkt 1 des Satzes 5.2.9 folgt, dass $\left(1,\theta,\theta^2\right)$ eine 2-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_2\left(d\left(K\right)\right)=\nu_2\left(\Delta\right)=0$ ist.

Fall $r\equiv 1\pmod 4$ **und** $s\equiv 0\pmod 4$:
Es ist $\nu_2\left(\Delta\right)=2$. Aus dem Punkt 3 des Satzes 5.2.9 folgt, dass $\left(1,\theta,\frac{\theta+\theta^2}{2}\right)$ eine 2-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_2\left(d\left(K\right)\right)=\nu_2\left(\Delta\right)-2=0$ ist.

Fall $r\equiv 3\pmod 4$, $s\equiv 2\pmod 4$, $\nu_2\left(\Delta\right)\equiv 0\pmod 2$ **und** $\frac{\Delta}{2^{\nu_2(\Delta)}}\equiv 1\pmod 4$:
Sei $m_0=\frac{\nu_2(\Delta)}{2}$, $x_0,y_0\in\mathbb{Z}$, $3x_0\equiv -2r\pmod{2^{m_0}}$ und $ry_0\equiv 3\frac{s}{2}+2^{m_0-1}\pmod{2^{m_0}}$. Aus dem Punkt 5 des Satzes 5.2.9 folgt, dass $\left(1,\theta,\frac{x_0+y_0\theta+\theta^2}{2^{m_0}}\right)$ eine 2-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_2\left(d\left(K\right)\right)=\nu_2\left(\Delta\right)-2\frac{\nu_2(\Delta)}{2}=0$ ist.

Fall $r\equiv 0\pmod 2$ **und** $s\equiv 2\pmod 4$:
Es ist $\nu_2\left(\Delta\right)=2$. Aus dem Punkt 1 des Satzes 5.2.9 folgt, dass $\left(1,\theta,\theta^2\right)$ eine 2-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_2\left(d\left(K\right)\right)=\nu_2\left(\Delta\right)=2$ ist.

Fall $r\equiv 0\pmod 2$ **und** $s\equiv 4\pmod 8$:
Es ist $\nu_2\left(\Delta\right)=4$. Aus dem Punkt 2 des Satzes 5.2.9 folgt, dass $\left(1,\theta,\frac{\theta^2}{2}\right)$ eine 2-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_2\left(d\left(K\right)\right)=\nu_2\left(\Delta\right)-2=2$ ist.

Fall $r\equiv 3\pmod 4$ **und** $s\equiv 0\pmod 4$:
Es ist $\nu_2\left(\Delta\right)=2$. Aus dem Punkt 1 des Satzes 5.2.9 folgt, dass $\left(1,\theta,\theta^2\right)$ eine 2-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_2\left(d\left(K\right)\right)=\nu_2\left(\Delta\right)=2$ ist.

Fall $r\equiv 3\pmod 4$, $s\equiv 2\pmod 4$, $\nu_2\left(\Delta\right)\equiv 0\pmod 2$ **und** $\frac{\Delta}{2^{\nu_2(\Delta)}}\equiv 3\pmod 4$:
Sei $m_1=\frac{\nu_2(\Delta)}{2}-1$, $x_1,y_1\in\mathbb{Z}$, $3x_1\equiv -2r\pmod{2^{m_1}}$ und $ry_1\equiv 3\frac{s}{2}\pmod{2_1^m}$. Aus

dem Punkt 4 des Satzes 5.2.9 folgt, dass $\left(1, \theta, \frac{x_1+y_1\theta+\theta^2}{2^{m_1}}\right)$ eine 2-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_2(d(K)) = \nu_2(\Delta) - 2\left(\frac{\nu_2(\Delta)}{2} - 1\right) = 2$ ist.

Fall $\nu_2(\Delta) \equiv 1 \pmod 2$:
Es ist $0 \equiv \Delta = 4r^3 - 27s^2 \equiv -27s^2 \pmod 2$ und $s \equiv 0 \pmod 2$.

Fall $s \equiv 0 \pmod 4$ **und** $\nu_2(\Delta) \equiv 1 \pmod 2$:
Da $\nu_2\left(4r^3 - 27s^2\right) = \nu_2(\Delta) \neq 2$ ist, folgt, dass $r \equiv 0 \pmod 2$ ist. Da

$$\nu_2\left(4r^3 - 27s^2\right) = \nu_2(\Delta) \neq 4$$

ist, folgt, dass $s \equiv 0 \pmod 8$ ist. Es folgt, dass $r \equiv 2 \pmod 4$ ist. Es ist $\nu_2(\Delta) = 5$. Aus dem Punkt 2 des Satzes 5.2.9 folgt, dass $\left(1, \theta, \frac{\theta^2}{2}\right)$ eine 2-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_2(d(K)) = \nu_2(\Delta) - 2 = 5 - 2 = 3$ ist.

Fall $s \equiv 2 \pmod 4$ **und** $\nu_2(\Delta) \equiv 1 \pmod 2$:
Da $\nu_2\left(4r^3 - 27s^2\right) = \nu_2(\Delta) \neq 2$ ist, folgt, dass $r \equiv 1 \pmod 2$ ist.

Fall $r \equiv 1 \pmod 4$, $s \equiv 2 \pmod 4$ **und** $\nu_2(\Delta) \equiv 1 \pmod 2$:
Es ist

$$\Delta = 4r^3 - 27s^2 \equiv 4 + s^2 = 4 + s(s-2) + 2s \equiv 4 + 2(s-2) + 2s = 4s \equiv 4 \cdot 2 = 8 \pmod{16},$$

Es folgt, dass $\nu_2(\Delta) = 3$. Aus dem Punkt 1 des Satzes 5.2.9 folgt, dass $(1, \theta, \theta^2)$ eine 2-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_2(d(K)) = \nu_2(\Delta) = 3$ ist.

Fall $r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$ **und** $\nu_2(\Delta) \equiv 1 \pmod 2$:
Sei $m_2 = \frac{\nu_2(\Delta)-3}{2}$, $x_2, y_2 \in \mathbb{Z}$, $3x_2 \equiv -2r \pmod{2^{m_2}}$ und $ry_2 \equiv 3\frac{s}{2} \pmod{2^{m_2}}$. Es ist $m_2 = \frac{\nu_2(\Delta)-3}{2} = \left\lfloor \frac{\nu_2(\Delta)}{2} \right\rfloor - 1$. Aus dem Punkt 4 des Satzes 5.2.9 folgt, dass $\left(1, \theta, \frac{x_2+y_2\theta+\theta^2}{2^{m_2}}\right)$ eine 2-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_2(d(K)) = \nu_2(\Delta) - 2\left(\frac{\nu_2(\Delta)-3}{2}\right) = 3$ ist.

□

Satz 5.6.3. *Sei $r, s \in \mathbb{Z}$. Sei $\nu_2(r) \leq 1$ oder $\nu_2(s) \leq 2$. Sei $\Delta = 4r^3 - 27s^2$, dann ist einer der drei folgenden Punkte erfüllt:*

1. $s \equiv 1 \pmod 2$, *(*$r \equiv 1 \pmod 4$ *und* $s \equiv 0 \pmod 4$*) oder (*$r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$, $\nu_2(\Delta) \equiv 0 \pmod 2$ *und* $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 1 \pmod 4$*)*
2. *(*$r \equiv 0 \pmod 2$ *und* $s \equiv 2 \pmod 4$*)*, *(*$r \equiv 0 \pmod 2$ *und* $s \equiv 4 \pmod 8$*)*, *(*$r \equiv 3 \pmod 4$ *und* $s \equiv 0 \pmod 4$*) oder (*$r \equiv 3 \pmod 4$, $s \equiv 2 \pmod 4$, $\nu_2(\Delta) \equiv 0 \pmod 2$ *und* $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 3 \pmod 4$*)*
3. $\nu_2(\Delta) \equiv 1 \pmod 2$

Beweis. Angenommen die Punkte 1, 2 und 3 sind alle nicht erfüllt. Da der Punkt 1 nicht erfüllt ist, folgt, dass $s \equiv 0 \pmod 2$ ist. Da der Punkt 3 nicht erfüllt ist, folgt, dass $\nu_2(\Delta) \equiv 0 \pmod 2$ ist. Wenn $r \equiv 1 \pmod 4$ und $s \equiv 2 \pmod 4$ ist, dann ist

$$\Delta = 4r^3 - 27s^2 \equiv 4 + s^2 = 4 + s(s-2) + 2s \equiv 4 + 2(s-2) + 2s = 4s \equiv 4 \cdot 2 = 8 \pmod{16}$$

und $\nu_2(\Delta) = 3$. Es folgt, dass $r \not\equiv 1 \pmod 4$ oder $s \not\equiv 2 \pmod 4$ ist. Es ist $r \not\equiv 1 \pmod 4$ oder $s \equiv 0 \pmod 4$. Da der Punkt 1 nicht erfüllt ist, folgt, dass $r \not\equiv 1 \pmod 4$ oder $s \not\equiv 0 \pmod 4$ ist. Es ist $r \not\equiv 1 \pmod 4$. Wenn $r \equiv 0 \pmod 2$ und $s \equiv 0 \pmod 8$ ist, dann ist $r \equiv 2 \pmod 4$ und $\nu_2(\Delta) = \nu_2\left(4r^3\right) = 5$. Es folgt, dass $r \equiv 1 \pmod 2$ oder $s \not\equiv 0 \pmod 8$ ist. Da der Punkt 2 nicht erfüllt ist, folgt, dass $r \equiv 1 \pmod 2$ oder $s \not\equiv 4 \pmod 8$ ist. Es ist $r \equiv 1 \pmod 2$ oder $s \not\equiv 0 \pmod 4$. Da der Punkt 2 nicht erfüllt ist, folgt, dass $r \equiv 1 \pmod 2$ oder $s \not\equiv 2 \pmod 4$ ist. Es ist $r \equiv 1 \pmod 2$. Es folgt, dass $r \equiv 3 \pmod 4$ ist. Da der Punkt 2 nicht erfüllt ist, folgt, dass $s \not\equiv 0 \pmod 4$ ist. Es ist $s \equiv 2 \pmod 4$. Da der Punkt 1 nicht erfüllt ist, folgt, dass $\frac{\Delta}{2^{\nu_2(\Delta)}} \not\equiv 1 \pmod 4$ ist. Es ist $\frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 3 \pmod 4$. Der Punkt 2 ist erfüllt. Dies ist ein Widerspruch. □

Die Idee für die Fallunterscheidungen des folgenden Satzes stammt aus dem Satz 2.5.1 in der Doktorarbeit von Alaca [1].

Satz 5.6.4. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\nu_3(r) \leq 1$ oder $\nu_3(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$ und $\Delta = 4r^3 - 27s^2$, dann sind alle fünf folgenden Punkte erfüllt*

1. *Wenn $r \not\equiv 0 \pmod 3$ oder ($r \equiv 3 \pmod 9$, $s^2 \equiv r + 1 \pmod{27}$ und $\nu_3(\Delta) \equiv 0 \pmod 2$) ist, dann ist $\nu_3(d(K)) = 0$.*
2. *Wenn ($\nu_3(r) = 1$ und $s \equiv 0 \pmod 9$), ($r \equiv 0 \pmod 3$, $r \not\equiv 3 \pmod 9$ und $s^2 \equiv r + 1 \pmod 9$) oder ($r \equiv 3 \pmod 9$, $s^2 \equiv r + 1 \pmod{27}$ und $\nu_3(\Delta) \equiv 1 \pmod 2$) ist, dann ist $\nu_3(d(K)) = 1$.*
3. *Wenn $\nu_3(r) = \nu_3(s) = 1$, ($r \equiv 0 \pmod 3$, $r \not\equiv 3 \pmod 9$, $s \not\equiv 0 \pmod 3$ und $s^2 \not\equiv r + 1 \pmod 9$) oder ($r \equiv 3 \pmod 9$, $s^2 \equiv 4 \pmod 9$ und $s^2 \not\equiv r + 1 \pmod{27}$) ist, dann ist $\nu_3(d(K)) = 3$.*
4. *Wenn $\nu_3(r) = \nu_3(s) = 2$ oder ($r \equiv 3 \pmod 9$, $s \not\equiv 0 \pmod 3$ und $s^2 \not\equiv 4 \pmod 9$) ist, dann ist $\nu_3(d(K)) = 4$.*
5. *Wenn $s \equiv 0 \pmod 3$ und $\nu_3(s) < \nu_3(r)$ ist, dann ist $\nu_3(d(K)) = 5$.*

Beweis.

Fall $r \not\equiv 0 \pmod 3$:
Es ist $\nu_3(\Delta) = \nu_3\left(4r^3 - 27s^2\right) = 0$. Aus dem Punkt 1 des Satzes 5.3.6 folgt, dass $\left(1, \theta, \theta^2\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_3(d(K)) = \nu_3(\Delta) = 0$ ist.

Fall $r \equiv 3 \pmod 9$, $s^2 \equiv r + 1 \pmod{27}$ **und** $\nu_3(\Delta) \equiv 0 \pmod 2$:
Sei $m_0 = \frac{\nu_3(\Delta)}{2} - 1$, $x_0, y_0 \in \mathbb{Z}$, $x_0 \equiv -2\frac{r}{3} \pmod{3^{m_0}}$, $2\frac{r}{3}y_0 \equiv s \pmod{3^{m_0+1}}$. Aus dem Punkt 4 des Satzes 5.3.6 folgt, dass $\left(1, \frac{s+\theta}{3}, \frac{x_0 + y_0\theta + \theta^2}{3^{m_0}}\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_3(d(K)) = \nu_3(\Delta) - 2\left(1 + \frac{\nu_3(\Delta)}{2} - 1\right) = 0$ ist.

Fall $\nu_3(r) = 1$ **und** $s \equiv 0 \pmod 9$:
Es ist $\nu_3(\Delta) = \nu_3\left(4r^3 - 27s^2\right) = 3$. Aus dem Punkt 2 des Satzes 5.3.6 folgt, dass $\left(1, \theta, \frac{\theta^2}{3}\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_3(d(K)) = \nu_3(\Delta) - 2 = 1$ ist.

Fall $r \equiv 0 \pmod 3$, $r \not\equiv 3 \pmod 9$ **und** $s^2 \equiv r + 1 \pmod 9$:
Es ist $\Delta = 4r^3 - 27s^2 \equiv r^3 - 27 \pmod{3^4}$. Wenn $r \equiv 0 \pmod 9$ ist, dann ist $\Delta \equiv -27 \pmod{3^4}$. Wenn $r \equiv 6 \pmod 9$ ist, dann ist $\Delta \equiv 6^3 - 27 \equiv -27 - 27 \equiv 27 \pmod{3^4}$. Es ist $\nu_3(\Delta) = 3$. Aus dem Punkt 3 des Satzes 5.3.6 folgt, dass $\left(1, \theta, \frac{1 - s\theta + \theta^2}{3}\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_3(d(K)) = \nu_3(\Delta) - 2 = 1$ ist.

Fall $r \equiv 3 \pmod 9$, $s^2 \equiv r + 1 \pmod{27}$ **und** $\nu_3(\Delta) \equiv 1 \pmod 2$:
Sei $m_1 = \frac{\nu_3(\Delta) - 3}{2}$, $x_1, y_1 \in \mathbb{Z}$, $x_1 \equiv -2\frac{r}{3} \pmod{3^{m_1}}$, $2\frac{r}{3}y_1 \equiv s \pmod{3^{m_1+1}}$. Aus dem Punkt 4 des Satzes 5.3.6 folgt, dass $\left(1, \frac{s+\theta}{3}, \frac{x_1 + y_1\theta + \theta^2}{3^{m_1}}\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_3(d(K)) = \nu_3(\Delta) - 2\left(1 + \frac{\nu_3(\Delta) - 3}{2}\right) = 1$ ist.

Fall $\nu_3(r) = \nu_3(s) = 1$:
Es ist $\nu_3(\Delta) = \nu_3\left(4r^3 - 27s^2\right) = 3$. Es ist $s^2 \equiv 0 \not\equiv r + 1 \pmod 9$. Aus dem Punkt 1 des Satzes 5.3.6 folgt, dass $\left(1, \theta, \theta^2\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_3(d(K)) = \nu_3(\Delta) = 3$ ist.

Fall $r \equiv 0 \pmod 3$, $r \not\equiv 3 \pmod 9$, $s \not\equiv 0 \pmod 3$ **und** $s^2 \not\equiv r + 1 \pmod 9$:
Es ist $\Delta = 4r^3 - 27s^2 \equiv r^3 - 27 \pmod{3^4}$. Wenn $r \equiv 0 \pmod 9$ ist, dann ist $\Delta \equiv -27 \pmod{3^4}$. Wenn $r \equiv 6 \pmod 9$ ist, dann ist $\Delta \equiv 6^3 - 27 \equiv -27 - 27 \equiv 27 \pmod{3^4}$. Es ist $\nu_3(\Delta) = 3$. Aus dem Punkt 1 des Satzes 5.3.6 folgt, dass $\left(1, \theta, \theta^2\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_3(d(K)) = \nu_3(\Delta) = 3$ ist.

Fall $r \equiv 3 \pmod 9$, $s^2 \equiv 4 \pmod 9$ **und** $s^2 \not\equiv r + 1 \pmod{27}$:
Es ist

$$\begin{aligned}
\Delta = 4r^3 - 27s^2 = 4r(r-3)^2 + 24r^2 - 36r - 27s^2 \equiv 12(r-3)^2 + 24r^2 - 36r - 27s^2 = \\
12(r-3)^2 + 24(r-3)^2 + 16 \cdot 9r - 8 \cdot 27 - 4 \cdot 9r - 27s^2 = \\
36(r-3)^2 + 4 \cdot 27r - 8 \cdot 27 - 27s^2 \equiv 4 \cdot 27r - 8 \cdot 27 - 27s^2 = 27\left(4r - 8 - s^2\right) = \\
27\left(4(r-3) + 4 - s^2\right) \equiv 27\left(r - 3 + 4 - s^2\right) = 27\left(r + 1 - s^2\right) \pmod{3^6}.
\end{aligned}$$

Es ist $\nu_3(\Delta) = 5$. Aus dem Punkt 3 des Satzes 5.3.6 folgt, dass $\left(1, \theta, \frac{1 - s\theta + \theta^2}{3}\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_3(d(K)) = \nu_3(\Delta) - 2 = 3$ ist.

Fall $\nu_3(r) = \nu_3(s) = 2$:
Es ist $\nu_3(\Delta) = \nu_3\left(4r^3 - 27s^2\right) = 6$. Aus dem Punkt 2 des Satzes 5.3.6 folgt, dass $\left(1, \theta, \frac{\theta^2}{3}\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_3(d(K)) = \nu_3(\Delta) - 2 = 6 - 2 = 4$ ist.

Fall $r \equiv 3 \pmod 9$, $s \not\equiv 0 \pmod 3$ **und** $s^2 \not\equiv 4 \pmod 9$

Es ist

$$\begin{aligned}\Delta = 4r^3 - 27s^2 = 4r^2(r-3) + 12r^2 - 27s^2 = 4r^2(r-3) + 12r(r-3) + 36r - 27s^2 = \\ 4r^2(r-3) + 12r(r-3) + 36(r-3) + 4 \cdot 27 - 27s^2 \equiv \\ 4 \cdot 9(r-3) + 4 \cdot 9(r-3) + 4 \cdot 9(r-3) + 4 \cdot 27 - 27s^2 = \\ 4 \cdot 27(r-3) + 27\left(4 - s^2\right) \equiv 27\left(4 - s^2\right) \pmod{3^5}.\end{aligned}$$

Es ist $\nu_3(\Delta) = 4$. Aus dem Punkt 1 des Satzes 5.3.6 folgt, dass $\left(1, \theta, \theta^2\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_3(d(K)) = \nu_3(\Delta) = 4$ ist.

Fall $\nu_3(s) = 2 < \nu_3(r)$
Es ist $\nu_3(\Delta) = \nu_3\left(4r^3 - 27s^2\right) = 7$. Aus dem Punkt 2 des Satzes 5.3.6 folgt, dass $\left(1, \theta, \frac{\theta^2}{3}\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_3(d(K)) = \nu_3(\Delta) - 2 = 7 - 2 = 5$ ist.

Fall $\nu_3(s) = 1 < \nu_3(r)$
Es ist $\nu_3(\Delta) = \nu_3\left(4r^3 - 27s^2\right) = 5$. Aus dem Punkt 1 des Satzes 5.3.6 folgt, dass $\left(1, \theta, \theta^2\right)$ eine 3-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_3(d(K)) = \nu_3(\Delta) = 5$ ist.

□

Satz 5.6.5. *Sei $r, s \in \mathbb{Z}$. Sei $\nu_3(r) \leq 1$ oder $\nu_3(s) \leq 2$. Sei $\Delta = 4r^3 - 27s^2$, dann ist einer der fünf folgenden Punkte erfüllt:*

1. $r \not\equiv 0 \pmod 3$ *oder* ($r \equiv 3 \pmod 9$, $s^2 \equiv r + 1 \pmod{27}$ *und* $\nu_3(\Delta) \equiv 0 \pmod 2$)
2. ($\nu_3(r) = 1$ *und* $s \equiv 0 \pmod 9$), ($r \equiv 0 \pmod 3$, $r \not\equiv 3 \pmod 9$ *und* $s^2 \equiv r + 1 \pmod 9$) *oder* ($r \equiv 3 \pmod 9$, $s^2 \equiv r + 1 \pmod{27}$ *und* $\nu_3(\Delta) \equiv 1 \pmod 2$)
3. $\nu_3(r) = \nu_3(s) = 1$, ($r \equiv 0 \pmod 3$, $r \not\equiv 3 \pmod 9$, $s \not\equiv 0 \pmod 3$ *und* $s^2 \not\equiv r + 1 \pmod 9$) *oder* ($r \equiv 3 \pmod 9$, $s^2 \equiv 4 \pmod 9$ *und* $s^2 \not\equiv r + 1 \pmod{27}$)
4. $\nu_3(r) = \nu_3(s) = 2$ *oder* ($r \equiv 3 \pmod 9$, $s \not\equiv 0 \pmod 3$ *und* $s^2 \not\equiv 4 \pmod 9$)
5. $s \equiv 0 \pmod 3$ *und* $\nu_3(s) < \nu_3(r)$

Beweis. Angenommen die Punkte 1, 2, 3, 4 und 5 sind alle nicht erfüllt. Da der Punkt 1 nicht erfüllt ist, folgt, dass $r \equiv 0 \pmod 3$ ist. Wenn $\nu_3(r) = \nu_3(s)$ ist, dann ist $\nu_3(r) \in \{1, 2\}$. Da der Punkt 3 und der Punkt 4 nicht erfüllt sind, folgt, dass $\nu_3(r) \neq \nu_3(s)$ ist. Es ist $\nu_3(s) < \nu_3(r)$ oder $\nu_3(r) = 1$. Da der Punkt 2 nicht erfüllt ist, folgt, dass $\nu_3(r) \neq 1$ oder $s \not\equiv 0 \pmod 9$ ist. Wenn $\nu_3(r) = 1$ ist, dann ist $\nu_3(s) < \nu_3(r)$. Es ist $\nu_3(s) < \nu_3(r)$. Da der Punkt 5 nicht erfüllt ist, folgt, dass $s \not\equiv 0 \pmod 3$ ist. Da der Punkt 2 nicht erfüllt ist, folgt, dass $r \equiv 3 \pmod 9$ oder $s^2 \not\equiv r + 1 \pmod 9$ ist. Da der Punkt 3 nicht erfüllt ist, folgt, dass $r \equiv 3 \pmod 9$ oder $s^2 \equiv r + 1 \pmod 9$ ist. Es ist $r \equiv 3 \pmod 9$. Da der Punkt 1 nicht erfüllt ist, folgt, dass $s^2 \not\equiv r + 1 \pmod{27}$ oder $\nu_3(\Delta) \equiv 1 \pmod 2$ ist. Da der Punkt 2 nicht erfüllt ist, folgt, dass $s^2 \not\equiv r + 1 \pmod{27}$ oder $\nu_3(\Delta) \equiv 0 \pmod 2$ ist. Es folgt, dass $s^2 \not\equiv r + 1 \pmod{27}$ ist. Da der Punkt 3 nicht erfüllt ist, folgt, dass $s^2 \not\equiv 4 \pmod 9$ ist. Der Punkt 4 ist erfüllt. Dies ist ein Widerspruch. □

Die Idee für die Fallunterscheidungen des folgenden Satzes stammt aus dem Satz 2.5.1 in der Doktorarbeit von Alaca [1].

Satz 5.6.6. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei p eine Primzahl und $p \geq 5$. Sei $\nu_p(r) \leq 1$ oder $\nu_p(s) \leq 2$. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$ und $\Delta = 4r^3 - 27s^2$, dann sind alle drei folgenden Punkte erfüllt:*

1. *Wenn ($s \not\equiv 0 \pmod{p}$ und $\nu_p(\Delta) \equiv 0 \pmod{2}$) oder ($r \not\equiv 0 \pmod{p}$ und $s \equiv 0 \pmod{p}$) ist, dann ist $\nu_p(d(K)) = 0$.*
2. *Wenn $\nu_p(\Delta) \equiv 1 \pmod{2}$ ist, dann ist $\nu_p(d(K)) = 1$.*
3. *Wenn $s \equiv 0 \pmod{p}$ und $\nu_p(s) \leq \nu_p(r)$ ist, dann ist $\nu_p(d(K)) = 2$.*

Beweis.

Fall ($r \equiv 0 \pmod{p}$ und $s \not\equiv 0 \pmod{p}$) oder ($r \not\equiv 0 \pmod{p}$ und $s \equiv 0 \pmod{p}$):
Es ist $\nu_p(\Delta) = \nu_p\left(4r^3 - 27s^2\right) = 0$. Aus dem Punkt 1 des Satzes 5.4.6 folgt, dass $\left(1, \theta, \theta^2\right)$ eine p-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_p(d(K)) = \nu_p(\Delta) = 0$ ist.

Fall $r \not\equiv 0 \pmod{p}$, $s \not\equiv 0 \pmod{p}$ und $\nu_p(\Delta) \equiv 0 \pmod{2}$:
Sei $m_0 = \frac{\nu_p(\Delta)}{2}$, $x_0, y_0 \in \mathbb{Z}$, $3x_0 \equiv -2r \pmod{p^{m_0}}$, $2ry_0 \equiv 3s \pmod{p^{m_0}}$. Aus dem Punkt 3 des Satzes 5.4.6 folgt, dass $\left(1, \theta, \frac{x_0 + y_0\theta + \theta^2}{p^{m_0}}\right)$ eine p-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_p(d(K)) = \nu_p(\Delta) - 2\frac{\nu_p(\Delta)}{2} = 0$ ist.

Fall $r \equiv 0 \pmod{p}$ und $\nu_p(\Delta) \equiv 1 \pmod{2}$:
Es ist $\nu_p(\Delta) \neq \nu_p\left(-27s^2\right)$. Es folgt, dass $r \not\equiv 0 \pmod{p^2}$, $s \equiv 0 \pmod{p^2}$ und $\nu_p(\Delta) = \nu_p\left(4r^3 - 27s^2\right) = 3$ ist. Aus dem Punkt 2 des Satzes 5.4.6 folgt, dass $\left(1, \theta, \frac{\theta^2}{p}\right)$ eine p-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_p(d(K)) = \nu_p(\Delta) - 2 = 3 - 2 = 1$ ist.

Fall $r \not\equiv 0 \pmod{p}$ und $\nu_p(\Delta) \equiv 1 \pmod{2}$:
Es ist $s \not\equiv 0 \pmod{p}$. Sei $m_1 = \frac{\nu_p(\Delta) - 1}{2}$, $x_1, y_1 \in \mathbb{Z}$, $3x_1 \equiv -2r \pmod{p^{m_1}}$, $2ry_1 \equiv 3s \pmod{p^{m_1}}$. Aus dem Punkt 3 des Satzes 5.4.6 folgt, dass $\left(1, \theta, \frac{x_1 + y_1\theta + \theta^2}{p^{m_1}}\right)$ eine p-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_p(d(K)) = \nu_p(\Delta) - 2\frac{\nu_p(\Delta) - 1}{2} = 1$ ist.

Fall $\nu_p(s) = 1 \leq \nu_p(r)$:
Es ist $\nu_p(\Delta) = \nu_p\left(4r^3 - 27s^2\right) = 2$. Aus dem Punkt 1 des Satzes 5.4.6 folgt, dass $\left(1, \theta, \theta^2\right)$ eine p-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_p(d(K)) = \nu_p(\Delta) = 2$ ist.

Fall $\nu_p(s) = 2 \leq \nu_p(r)$:
Es ist $\nu_p(\Delta) = \nu_p\left(4r^3 - 27s^2\right) = 4$. Aus dem Punkt 2 des Satzes 5.4.6 folgt, dass $\left(1, \theta, \frac{\theta^2}{p}\right)$ eine p-ganze Basis von K ist. Aus dem Satz 5.6.1 folgt, dass $\nu_p(d(K)) = \nu_p(\Delta) - 2 = 4 - 2 = 2$ ist.

□

Satz 5.6.7. *Seien $r, s \in \mathbb{Z}$. Sei p eine Primzahl und $p \geq 5$. Sei $\nu_p(r) \leq 1$ oder $\nu_p(s) \leq 2$. Sei $\Delta = 4r^3 - 27s^2$, dann ist einer der drei folgenden Punkte erfüllt:*

1. *($s \not\equiv 0 \pmod{p}$ und $\nu_p(\Delta) \equiv 0 \pmod{2}$) oder ($r \not\equiv 0 \pmod{p}$ und $s \equiv 0 \pmod{p}$)*
2. *$\nu_p(\Delta) \equiv 1 \pmod{2}$*
3. *$s \equiv 0 \pmod{p}$ und $\nu_p(s) \leq \nu_p(r)$*

Beweis. Angenommen die Punkte 1, 2 und 3 sind alle nicht erfüllt. Da der Punkt 2 nicht erfüllt ist, folgt, dass $\nu_p(\Delta) \equiv 0 \pmod{2}$ ist. Da der Punkt 1 nicht erfüllt ist, folgt, dass $s \equiv 0 \pmod{p}$ ist. Da der Punkt 1 nicht erfüllt ist, folgt, dass $r \equiv 0 \pmod{p}$ ist. Da der Punkt 3 nicht erfüllt ist, folgt, dass $\nu_p(r) < \nu_p(s)$ ist. Da $\nu_p(r) \leq 1$ oder $\nu_p(s) \leq 2$ ist, folgt, dass $\nu_p(r) = 1$ ist. Es ist $\nu_p(\Delta) = \nu_p\left(4r^3 - 27s^2\right) = \nu_p\left(4r^3\right) = 3 \not\equiv 0 \pmod{2}$. Dies ist ein Widerspruch. □

Der folgende Satz stammt im Wesentlichen aus der Doktorarbeit von Alaca [1][7].

Satz 5.6.8. *Sei $\theta \in \mathbb{C}$ und θ algebraisch über $\mathbb{Q}$. Seien $r, s \in \mathbb{Z}$. Sei $\nu_q(r) \leq 1$ oder $\nu_q(s) \leq 2$ für jede Primzahl q. Sei $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = T^3 - rT + s$, $K = \mathbb{Q}(\theta)$ und $\Delta = 4r^3 - 27s^2$. Sei*

$$u = \begin{cases} 0 & \text{wenn } s \equiv 1 \pmod{2}, \\ & (r \equiv 1 \pmod{4} \text{ und } s \equiv 0 \pmod{4}) \text{ oder} \\ & (r \equiv 3 \pmod{4}, s \equiv 2 \pmod{4}, \nu_2(\Delta) \equiv 0 \pmod{2} \text{ und } \frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 1 \pmod{4}) \\ 2 & \text{wenn } (r \equiv 0 \pmod{2} \text{ und } s \equiv 2 \pmod{4}), \\ & (r \equiv 0 \pmod{2} \text{ und } s \equiv 4 \pmod{8}), \\ & (r \equiv 3 \pmod{4} \text{ und } s \equiv 0 \pmod{4}) \text{ oder} \\ & (r \equiv 3 \pmod{4}, s \equiv 2 \pmod{4}, \nu_2(\Delta) \equiv 0 \pmod{2} \text{ und } \frac{\Delta}{2^{\nu_2(\Delta)}} \equiv 3 \pmod{4}) \\ 3 & \text{wenn } \nu_2(\Delta) \equiv 1 \pmod{2} \end{cases}$$

und

$$v = \begin{cases} 0 & \text{wenn } r \not\equiv 0 \pmod{3} \text{ oder} \\ & (r \equiv 3 \pmod{9}, s^2 \equiv r + 1 \pmod{27} \text{ und } \nu_3(\Delta) \equiv 0 \pmod{2}) \\ 1 & \text{wenn } (\nu_3(r) = 1 \text{ und } s \equiv 0 \pmod{9}), \\ & (r \equiv 0 \pmod{3}, r \not\equiv 3 \pmod{9} \text{ und } s^2 \equiv r + 1 \pmod{9}) \text{ oder} \\ & (r \equiv 3 \pmod{9}, s^2 \equiv r + 1 \pmod{27} \text{ und } \nu_3(\Delta) \equiv 1 \pmod{2}) \\ 3 & \text{wenn } \nu_3(r) = \nu_3(s) = 1, \\ & (r \equiv 0 \pmod{3}, r \not\equiv 3 \pmod{9}, s \not\equiv 0 \pmod{3} \text{ und } s^2 \not\equiv r + 1 \pmod{9}) \text{ oder} \\ & (r \equiv 3 \pmod{9}, s^2 \equiv 4 \pmod{9} \text{ und } s^2 \not\equiv r + 1 \pmod{27}) \\ 4 & \text{wenn } \nu_3(r) = \nu_3(s) = 2 \text{ oder} \\ & (r \equiv 3 \pmod{9}, s \not\equiv 0 \pmod{3} \text{ und } s^2 \not\equiv 4 \pmod{9}) \\ 5 & \text{wenn } s \equiv 0 \pmod{3} \text{ und } \nu_3(s) < \nu_3(r) \end{cases}$$

[7] Siehe Satz 2.5.1 in [1].

Dann ist

$$d(K) = \operatorname{sgn}(\Delta)\, 2^u 3^v \Bigg(\prod_{\substack{p \text{ Primzahl,} \\ p \geq 5, \\ \nu_p(\Delta) \equiv 1 \pmod 2}} p \Bigg) \Bigg(\prod_{\substack{q \text{ Primzahl,} \\ q \geq 5, \\ 1 \leq \nu_q(s) \leq \nu_q(r)}} q^2 \Bigg) \tag{5.5}$$

Beweis. Aus dem Satz 5.6.3 folgt, dass u definiert ist. Aus dem Satz 5.6.5 folgt, dass v definiert ist. Sei $(\alpha_0, \alpha_1, \alpha_2)$ eine Ganzheitsbasis von K, $A \in M(3, \mathbb{Z})$ und $\left(1, \theta, \theta^2\right)^T = A\left(\alpha_0, \alpha_1, \alpha_2\right)^T$. Aus dem Satz 1.2.19 folgt, dass

$$d\left(1, \theta, \theta^2\right) = \det(A)^2\, d\left(\alpha_0, \alpha_1, \alpha_2\right)$$

ist. Es ist

$$d\left(1, \theta, \theta^2\right) = \det(A)^2\, d\left(\alpha_0, \alpha_1, \alpha_2\right) = \det(A)^2\, d(K).$$

Aus dem Satz 1.2.27 folgt, dass $d\left(1, \theta, \theta^2\right) = \Delta$ ist. Es ist

$$\operatorname{sgn}(\Delta) = \operatorname{sgn}(d\left(1, \theta, \theta^2\right)) = \operatorname{sgn}(\det(A)^2\, d(K)) = \operatorname{sgn}(d(K)).$$

Aus dem Satz 5.6.2 folgt, dass $\nu_2(d(K)) = u$ ist. Aus dem Satz 5.6.4 folgt, dass $\nu_3(d(K)) = v$ ist. Aus dem Satz 5.6.6 und dem Satz 5.6.7 folgt, dass $\nu_{p_0}(d(K)) = 0$ ist für alle Primzahlen $p_0 \geq 5$, die ($\nu_{p_0}(\Delta) \equiv 1 \pmod 2$ oder $1 \leq \nu_{p_0}(s) \leq \nu_{p_0}(r)$) nicht erfüllen. Aus dem Satz 5.6.6 folgt, dass $\nu_{p_1}(d(K)) = 1$ ist für alle Primzahlen $p_1 \geq 5$, die $\nu_{p_1}(\Delta) \equiv 1 \pmod 2$ erfüllen. Aus dem Satz 5.6.6 folgt, dass $\nu_{p_2}(d(K)) = 2$ ist für alle Primzahlen $p_2 \geq 5$, die $1 \leq \nu_{p_2}(s) \leq \nu_{p_2}(r)$ erfüllen. Es folgt die Gleichung (5.5). □

5.7 Beispiele

Satz 5.7.1. *Seien $r, s \in \mathbb{Z}$. Sei $P(T) \in \mathbb{Z}(T)$ und $P(T) = T^3 - rT + s$, dann sind die beiden folgenden Punkte äquivalent:*

1. *Es ist $P(T)$ irreduzibel über $\mathbb{Q}$.*
2. *Für alle $u, v \in \mathbb{Z}$ gilt, dass $u^2 - v \neq r$ oder $uv \neq s$ ist.*

Beweis.

(1 ⇒ 2) Angenommen es gibt $u, v \in \mathbb{Z}$, sodass $u^2 - v = r$ und $uv = s$ ist. Es ist

$$\begin{aligned}\left(T^2 - uT + v\right)(T + u) &= T^3 + uT^2 - uT^2 - u^2T + vT + uv = \\ &T^3 - \left(u^2 - v\right)T + uv = T^3 - rT + s.\end{aligned}$$

Es ist $P(T)$ nicht irreduzibel über $\mathbb{Q}$. Dies ist ein Widerspruch.

(2 $\Rightarrow$ 1) Angenommen $P(T)$ ist nicht irreduzibel über $\mathbb{Q}$. Aus dem Satz 1.2.4 folgt, dass $P(T)$ nicht irreduzibel über $\mathbb{Z}$ ist. Es gibt $x, y, z \in \mathbb{Z}$, sodass $P(T) = T^3 - rT + s = \left(T^2 + zT + y\right)(T + x)$ ist. Es ist

$$T^3 - rT + s = \left(T^2 + zT + y\right)(T + x) = T^3 + xT^2 + zT^2 + xzT + yT + xy = T^3 + (x + z)T^2 + (xz + y)T + xy.$$

Werden die Koeffizienten verglichen, dann folgt, dass $x + z = 0$, $xz + y = -r$ und $xy = s$ ist. Es ist $z = -x$, $x^2 - y = r$ und $xy = s$. Dies ist ein Widerspruch.

□

Die Ganzheitsbasis $\left(1, \theta, \frac{\theta^2}{3}\right)$ und die Diskriminante des algebraischen Zahlkörpers $\mathbb{Q}(\theta)$ des folgenden Satzes wird auch in dem Beispiel 7.3.6 in dem Buch von Alaca und Williams [2] angeführt und bewiesen. Die Ganzheitsbasis $\left(1, \theta, \frac{\theta^2}{3}\right)$ und die Diskriminante des algebraischen Zahlkörpers $\mathbb{Q}(\theta)$ des folgenden Satzes scheint als Zahlenbeispiel in der Tabelle D in dem Kapitel 2.7 in der Doktorarbeit von Alaca [1] auf.

Satz 5.7.2. *Sei $P(T) = T^3 - 3T + 9$, $\theta \in \mathbb{C}$, $P(\theta) = 0$ und $K = \mathbb{Q}(\theta)$, dann ist $\left(1, \theta, \frac{\theta^2}{3}\right)$ eine Ganzheitsbasis von K und $d(K) = -231$.*

Beweis. Sei $r = 3$ und $s = 9$. Für alle $u, v \in \mathbb{Z}$ gilt, dass $u^2 - v \neq 3$ oder $uv \neq 9$ ist. Aus dem Satz 5.7.1 folgt, dass $P(T)$ irreduzibel über $\mathbb{Q}$ ist. Es folgt, dass $\mathrm{irr}_{\theta,\mathbb{Q}}(T) = P(T)$ ist. Sei $\Delta = 4r^3 - 27s^2$. Es ist $\Delta = 4 \cdot 27 - 27 \cdot 81 = -27 \cdot 77 = -3^3 \cdot 7 \cdot 11 = -2079$. Sei $n = w = m_2 = 0$ und $m_3 = 1$. Sei $m_p = 0$ für alle Primzahlen $p \geq 5$. Sei $x_2 = y_2 = x_3 = y_3 = 0$. Sei $x_p = y_p = 0$ für alle Primzahlen $p \geq 5$. Es ist $x_q \equiv 0 \pmod{q^{m_q}}$ und $y_q \equiv 0 \pmod{q^{m_q}}$ für alle Primzahlen q. Aus dem Satz 5.5.1 folgt, dass $\left(1, \theta, \frac{\theta^2}{3}\right)$ eine Ganzheitsbasis von K ist. Aus dem Satz 5.6.8 folgt, dass

$$d(K) = \mathrm{sgn}(\Delta) \cdot 2^0 \cdot 3^1 \cdot 7 \cdot 11 = -3 \cdot 7 \cdot 11 = -231$$

ist. □

Die Ganzheitsbasis $\left(1, \theta, \frac{\theta+\theta^2}{2}\right)$ und die Diskriminante des algebraischen Zahlkörpers $\mathbb{Q}(\theta)$ des folgenden Satzes wird auch in dem Beispiel 7.3.7 in dem Buch von Alaca und Williams [2] angeführt und bewiesen. Die Ganzheitsbasis $\left(1, \theta, \frac{\theta+\theta^2}{2}\right)$ und die Diskriminante des algebraischen Zahlkörpers $\mathbb{Q}(\theta)$ des folgenden Satzes scheint als Zahlenbeispiel in der Tabelle D in dem Kapitel 2.7 in der Doktorarbeit von Alaca [1] auf.

Satz 5.7.3. *Sei $P(T) = T^3 - T + 4$, $\theta \in \mathbb{C}$, $P(\theta) = 0$ und $K = \mathbb{Q}(\theta)$, dann ist $\left(1, \theta, \frac{\theta+\theta^2}{2}\right)$ eine Ganzheitsbasis von K und $d(K) = -107$.*

Beweis. Sei $r = 1$ und $s = 4$. Für alle $u, v \in \mathbb{Z}$ gilt, dass $u^2 - v \neq 1$ oder $uv \neq 4$ ist. Aus dem Satz 5.7.1 folgt, dass $P(T)$ irreduzibel über $\mathbb{Q}$ ist. Es folgt, dass $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = P(T)$ ist. Sei $\Delta = 4r^3 - 27s^2$. Es ist $\Delta = 4 - 27 \cdot 16 = -428 = -2^2 \cdot 107$. Sei $n = w = 0$, $m_2 = 1$ und $m_3 = 0$. Sei $m_p = 0$ für alle Primzahlen $p \geq 5$. Sei $x_2 = 0$, $y_2 = 1$ und $x_3 = y_3 = 0$. Sei $x_p = y_p = 0$ für alle Primzahlen $p \geq 5$. Es ist $x_q \equiv 0 \pmod{q^{m_q}}$ und $y_q \equiv 1 \pmod{q^{m_q}}$ für alle Primzahlen q. Aus dem Satz 5.5.1 folgt, dass $\left(1, \theta, \frac{\theta+\theta^2}{2}\right)$ eine Ganzheitsbasis von K ist. Aus dem Satz 5.6.8 folgt, dass $d(K) = \operatorname{sgn}(\Delta) \cdot 2^0 \cdot 3^0 \cdot 107 = -107$ ist. □

Die Ganzheitsbasis $\left(1, \frac{-236+\theta}{3}, \frac{4+5\theta+\theta^2}{18}\right)$ und die Diskriminante des algebraischen Zahlkörpers $\mathbb{Q}(\theta)$ des folgenden Satzes scheint als Zahlenbeispiel in der Tabelle D in dem Kapitel 2.7 in der Doktorarbeit von Alaca [1] auf.

Satz 5.7.4. *Sei $P(T) = T^3 - 21T - 236$, $\theta \in \mathbb{C}$, $P(\theta) = 0$ und $K = \mathbb{Q}(\theta)$, dann ist $\left(1, \frac{-236+\theta}{3}, \frac{4+5\theta+\theta^2}{18}\right)$ eine Ganzheitsbasis von K, $\left(1, \frac{1+\theta}{3}, \frac{4+5\theta+\theta^2}{18}\right)$ eine Ganzheitsbasis von K und $d(K) = -503$.*

Beweis. Sei $r = 21$ und $s = -236$. Es ist $r = 21 = 3 \cdot 7$ und $s = -236 = -2^2 \cdot 59$. Für alle $u, v \in \mathbb{Z}$ gilt, dass $u^2 - v \neq 21$ oder $uv \neq -236$ ist. Aus dem Satz 5.7.1 folgt, dass $P(T)$ irreduzibel über $\mathbb{Q}$ ist. Es folgt, dass $\operatorname{irr}_{\theta,\mathbb{Q}}(T) = P(T)$ ist. Sei $\Delta = 4r^3 - 27s^2$. Es ist $\Delta = 4 \cdot 21^3 - 27 \cdot 236^2 = -1466748 = -2^2 \cdot 3^6 \cdot 503$. Es ist $r = 21 \equiv 3 \pmod{9}$, $s^2 = 236^2 = 55696 = 2062 \cdot 27 + 22 \equiv 22 = r + 1 \pmod{27}$. Sei $n = 1$, $w = -236$, $m_2 = 1$ und $m_3 = 2$. Es ist $m_3 = 2 = \left\lfloor \frac{\nu_3(\Delta)}{2} \right\rfloor - 1$. Sei $m_p = 0$ für alle Primzahlen $p \geq 5$. Sei $x_2 = 0$, $y_2 = 1$, $x_3 = 4$ und $y_3 = 14$. Es ist $-2\frac{r}{3} = -14 \equiv 4 = x_3 \pmod{9}$ und

$$2\frac{r}{3}y_3 = 14^2 = 196 = 7 \cdot 27 + 7 \equiv 7 \equiv -27 \cdot 9 + 7 = -236 = s \pmod{27}.$$

Sei $x_p = y_p = 0$ für alle Primzahlen $p \geq 5$. Es ist $x_q \equiv 4 \pmod{q^{m_q}}$ für alle Primzahlen q. Es ist $5 \equiv 1 \pmod{2}$ und $5 \equiv 14 \pmod{9}$. Es ist $y_q \equiv 5 \pmod{q^{m_q}}$ für alle Primzahlen q. Aus dem Satz 5.5.1 folgt, dass $\left(1, \frac{-236+\theta}{3}, \frac{4+5\theta+\theta^2}{18}\right)$ eine Ganzheitsbasis von K ist. Es ist $79 + \frac{-236+\theta}{3} = \frac{237-236+\theta}{3} = \frac{1+\theta}{3}$. Aus dem Satz 1.2.23 folgt, dass $\left(1, \frac{1+\theta}{3}, \frac{4+5\theta+\theta^2}{18}\right)$ eine Ganzheitsbasis von K ist. Aus dem Satz 5.6.8 folgt, dass

$$d(K) = \operatorname{sgn}(\Delta) \cdot 2^0 \cdot 3^0 \cdot 503 = -503$$

ist. □

Die Ganzheitsbasis $\left(1, \frac{1+\theta}{3}, \frac{-2-\theta+\theta^2}{18}\right)$ des algebraischen Zahlkörpers $\mathbb{Q}(\theta)$ des folgenden Satzes wird auch in dem Beispiel 7.3.9 in dem Buch von Alaca und Williams [2] angeführt und bewiesen.

Satz 5.7.5. *Sei $P(T) = T^3 - 21T - 236$, $\theta \in \mathbb{C}$, $P(\theta) = 0$ und $K = \mathbb{Q}(\theta)$, dann ist $\left(1, \frac{1+\theta}{3}, \frac{-2-\theta+\theta^2}{18}\right)$ eine Ganzheitsbasis von K.*

Beweis. Aus dem Beispiel 5.7.4 folgt, dass $\left(1, \frac{1+\theta}{3}, \frac{4+5\theta+\theta^2}{18}\right)$ eine Ganzheitsbasis von K ist. Es ist $(-1)\,\frac{1+\theta}{3} + \frac{4+5\theta+\theta^2}{18} = \frac{-2-\theta+\theta^2}{18}$. Aus dem Satz 1.2.23 folgt, dass $\left(1, \frac{1+\theta}{3}, \frac{-2-\theta+\theta^2}{18}\right)$ eine Ganzheitsbasis von K ist. □

6 biquadratische Zahlkörper

6.1 Einleitung

Dieses Kapitel folgt zu Beginn des Abschnittes 6.1 zum Teil der Arbeit von Williams [4]. Die Idee, die biquadratischen Zahlkörper auf eine Form wie in dem Satz 6.1.5 zu reduzieren, stammt aus [4]. Trotz unterschiedlicher Herangehensweisen ergeben sich fast die gleichen Ganzheitsbasen wie in [4][1]. Auch die Diskriminanten der biquadratischen Zahlkörper wurden bereits in [4] angeführt. Die Sätze 6.1.6, 6.1.9, 6.1.10, 6.1.12 und 6.1.16 sind Standardresultate zu biquadratischen Zahlkörpern. Einige Resultate dieser Sätze werden in der Einleitung von der Arbeit von Williams [4] angeführt.

Definition 6.1.1 (biquadratischer Zahlkörper)**.** *K heißt genau dann biquadratischer Zahlkörper, wenn es $m, n \in \mathbb{Z} \setminus \{0, 1\}$ gibt, sodass m quadratfrei, n quadratfrei, $m \neq n$ und $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ ist.*

Definition 6.1.2. *Es ist*

$$W_4\left(T_0, T_1, S_0, S_1, S_2, S_3\right), X_4\left(T_0, T_1, S_0, S_1, S_2, S_3\right), Y_4\left(T_0, T_1, S_0, S_1, S_2, S_3\right), \\ Z_4\left(T_0, T_1, S_0, S_1, S_2, S_3\right) \in \mathbb{Z}\left[T_0, T_1, S_0, S_1, S_2, S_3\right].$$

Es ist

$$\begin{aligned}
W_4\left(T_0, T_1, S_0, S_1, S_2, S_3\right) =& 4S_0, \\
X_4\left(T_0, T_1, S_0, S_1, S_2, S_3\right) =& 2\left(-T_0T_1S_3^2 - T_0S_1^2 - T_1S_2^2 + 3S_0^2\right), \\
Y_4\left(T_0, T_1, S_0, S_1, S_2, S_3\right) =& 4\left(T_0T_1S_0S_3^2 - 2T_0T_1S_1S_2S_3 + T_0S_0S_1^2 + T_1S_0S_2^2 - S_0^3\right) \text{ und} \\
Z_4\left(T_0, T_1, S_0, S_1, S_2, S_3\right) =& T_0^2T_1^2S_3^4 - 2T_0^2T_1S_1^2S_3^2 + T_0^2S_1^4 - 2T_0T_1^2S_2^2S_3^2 - 2T_0T_1S_0^2S_3^2 \\
&+ 8T_0T_1S_0S_1S_2S_3 - 2T_0T_1S_1^2S_2^2 - 2T_0S_0^2S_1^2 + T_1^2S_2^4 \\
&- 2T_1S_0^2S_2^2 + S_0^4.
\end{aligned}$$

Satz 6.1.3. *Seien $m, n, w, x, y, z \in \mathbb{Z}$. Dann sind alle vier folgenden Punkte erfüllt:*

1. $W_4\left(m, n, w, x, y, z\right) = 4w$
2. $X_4\left(m, n, w, x, y, z\right) = 2\left(-mnz^2 - mx^2 - ny^2 + 3w^2\right)$
3. $Y_4\left(m, n, w, x, y, z\right) = 4\left(mnwz^2 - 2mnxyz + mwx^2 + nwy^2 - w^3\right)$
4. $\begin{aligned} Z_4\left(m, n, w, x, y, z\right) =& m^2n^2z^4 - 2m^2nx^2z^2 + m^2x^4 - 2mn^2y^2z^2 - 2mnw^2z^2 \\ &+ 8mnwxyz - 2mnx^2y^2 - 2mw^2x^2 + n^2y^4 - 2nw^2y^2 + w^4 \end{aligned}$

[1] Siehe Satz 6.4.1.

Das folgende Lemma stammt im Wesentlichen aus der Arbeit von Williams [4][2].

Lemma 6.1.4. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$, $l = \mathrm{ggT}(m,n)$, $m_0 = \frac{m}{l}$, $n_0 = \frac{n}{l}$, dann gibt es für die Restklassen von m, n und $m_0 n_0$ Modulo 4 die folgenden zehn Möglichkeiten:*

m	n	$m_0 n_0$
1	1	1
1	2	2
1	3	3
2	1	2
2	2	1
2	2	3
2	3	2
3	1	3
3	2	2
3	3	1

Beweis. Die Behauptung ist leicht nachzurechnen. □

Der folgende Satz stammt im Wesentlichen aus der Arbeit von Williams [4][3]. Die Beweisidee des Beweises des folgenden Satzes stammt aus [4].

Satz 6.1.5. *Sei K ein biquadratischer Zahlkörper, dann gibt es $m, n \in \mathbb{Z} \setminus \{0,1\}$, sodass m quadratfrei, n quadratfrei, $m \neq n$, $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ und einer der drei folgenden Punkte erfüllt ist:*

1. $m \equiv n \equiv 1 \pmod 4$
2. $m \equiv 2 \pmod 4$ *und* $n \equiv 1 \pmod 2$
3. $m \equiv n \equiv 3 \pmod 4$

Beweis. Sei $x, y \in \mathbb{Z} \setminus \{0,1\}$, x quadratfrei, y quadratfrei, $x \neq y$ und $K = \mathbb{Q}\left(\sqrt{x}, \sqrt{y}\right)$. Sei $l = \mathrm{ggT}(x,y)$, $x_0 = \frac{x}{l}$ und $y_0 = \frac{y}{l}$. Es ist $x_0 y_0 \in \mathbb{Z} \setminus \{0,1\}$, $x_0 y_0$ quadratfrei, $x \neq x_0 y_0$ und $y \neq x_0 y_0$. Es ist

$$\mathbb{Q}\left(\sqrt{x_0 y_0}, \sqrt{y}\right) = \mathbb{Q}\left(\sqrt{y}, \sqrt{x_0 y_0}\right) = \mathbb{Q}\left(\sqrt{y}, \sqrt{x}\right) = K = \mathbb{Q}\left(\sqrt{x}, \sqrt{y}\right) = \mathbb{Q}\left(\sqrt{x}, \sqrt{x_0 y_0}\right) = \mathbb{Q}\left(\sqrt{x_0 y_0}, \sqrt{x}\right).$$

Mit Hilfe des Lemmas 6.1.4 kann ein m und ein n gefunden werden, sodass einer der Punkte 1, 2 oder 3 erfüllt ist. □

Satz 6.1.6. *Seien $m, n \in \mathbb{Q}$. Sei $m \neq n$, dann ist $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n})$.*

[2] Siehe Seite 519 in [4].
[3] Siehe (1) auf der Seite 520 in [4].

Beweis.

($\subseteq$) Es ist $\frac{\sqrt{m}+\sqrt{n}}{m-n}\left(\sqrt{m}-\sqrt{n}\right)=1$. Es ist $\sqrt{m}-\sqrt{n}=\frac{m-n}{\sqrt{m}+\sqrt{n}}\in\mathbb{Q}(\sqrt{m}+\sqrt{n})$. Es folgt, dass

$$\sqrt{m}=\frac{1}{2}(\sqrt{m}+\sqrt{n}+\sqrt{m}-\sqrt{n})\in\mathbb{Q}(\sqrt{m}+\sqrt{n})$$

und

$$\sqrt{n}=\frac{1}{2}(\sqrt{m}+\sqrt{n}-(\sqrt{m}-\sqrt{n}))\in\mathbb{Q}(\sqrt{m}+\sqrt{n})$$

ist. Es ist $\mathbb{Q}(\sqrt{m},\sqrt{n})\subseteq\mathbb{Q}(\sqrt{m}+\sqrt{n})$.

($\supseteq$) Es ist $\sqrt{m}+\sqrt{n}\in\mathbb{Q}(\sqrt{m},\sqrt{n})$. Es ist $\mathbb{Q}(\sqrt{m}+\sqrt{n})\subseteq\mathbb{Q}(\sqrt{m},\sqrt{n})$.

□

Lemma 6.1.7. *Seien $m,n\in\mathbb{Z}\setminus\{0,1\}$. Sei m quadratfrei, n quadratfrei, $m\neq n$ und $P(T)=T^4-2(m+n)T^2+(m-n)^2$, dann ist $P\left(\sqrt{m}+\sqrt{n}\right)=0$.*

Beweis.

$$\begin{aligned}P\left(\sqrt{m}+\sqrt{n}\right)=\left(\sqrt{m}+\sqrt{n}\right)^4-2(m+n)\left(\sqrt{m}+\sqrt{n}\right)^2+(m-n)^2=\\ m^2+4m\sqrt{m}\sqrt{n}+6mn+4n\sqrt{m}\sqrt{n}+n^2-2\left(m+n\right)\left(m+2\sqrt{m}\sqrt{n}+n\right)\\ +m^2-2mn+n^2=\\ 2m^2+4m\sqrt{m}\sqrt{n}+4mn+4n\sqrt{m}\sqrt{n}+2n^2-2m^2-4m\sqrt{m}\sqrt{n}-2mn-2mn\\ -4n\sqrt{m}\sqrt{n}-2n^2=\\ 0\end{aligned}$$

□

Lemma 6.1.8. *Sei K ein biquadratischer Zahlkörper, dann ist $[K:\mathbb{Q}]\neq 2$.*

Beweis. Angenommen es ist $[K:\mathbb{Q}]=2$. Sei $m,n\in\mathbb{Z}\setminus\{0,1\}$, m quadratfrei, n quadratfrei, $m\neq n$ und $K=\mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$. Aus dem Satz 1.2.29 folgt, dass $\sqrt{m}\notin\mathbb{Q}$ ist. Es ist $\left(1,\sqrt{m}\right)$ linear unabhängig über $\mathbb{Q}$ und $\left(1,\sqrt{m}\right)$ eine Basis von K über $\mathbb{Q}$. Es gibt $a,b\in\mathbb{Q}$, sodass $\sqrt{n}=a+b\sqrt{m}$ ist. Es ist $n=a^2+2ab\sqrt{m}+b^2m$. Es folgt, dass $a^2+b^2m-n=0$ und $2ab=0$ ist. Aus dem Satz 1.2.29 folgt, dass $n\neq a^2$ und $b^2\neq\frac{n}{m}$ ist. Es ist $b\neq 0$. Es folgt, dass $a=0$ ist. Es ist $b^2m-n=0$ und $b^2=\frac{n}{m}$. Dies ist ein Widerspruch. □

Satz 6.1.9. *Sei K ein biquadratischer Zahlkörper, dann ist $[K:\mathbb{Q}]=4$.*

Beweis. Seien $m,n\in\mathbb{Z}\setminus\{0,1\}$, m quadratfrei, n quadratfrei, $m\neq n$ und $K=\mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$. Sei $P(T)=T^4-2(m+n)T^2+(m-n)^2$. Aus dem Lemma 6.1.7 folgt, dass $P\left(\sqrt{m}+\sqrt{n}\right)=0$ ist. Es ist $[K:\mathbb{Q}]\leq 4$. Es ist $\mathbb{Q}\left(\sqrt{m}\right)$ ein Teilkörper von K. Es ist $\left[\mathbb{Q}\left(\sqrt{m}\right):\mathbb{Q}\right]=2$. Es folgt, dass $2\mid[K:\mathbb{Q}]$ ist. Es ist $[K:\mathbb{Q}]\in\{2,4\}$. Aus dem Satz 6.1.8 folgt, dass $[K:\mathbb{Q}]\neq 2$ ist. Es ist $[K:\mathbb{Q}]=4$. □

Satz 6.1.10. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei und $m \neq n$, dann ist* $\operatorname{irr}_{\sqrt{m}+\sqrt{n},\mathbb{Q}}(T) = T^4 - 2(m+n)T^2 + (m-n)^2$.

Beweis. Sei $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$. Aus dem Satz 6.1.6 folgt, dass $K = \mathbb{Q}\left(\sqrt{m}+\sqrt{n}\right)$ ist. Sei $P(T) = T^4 - 2(m+n)T^2 + (m-n)^2$. Aus dem Lemma 6.1.7, folgt, dass $P\left(\sqrt{m}+\sqrt{n}\right) = 0$ ist. Aus dem Satz 6.1.9 folgt, dass $[K : \mathbb{Q}] = 4$ ist. Es ist $P(T) = \operatorname{irr}_{\sqrt{m}+\sqrt{n},\mathbb{Q}}(T)$. □

Satz 6.1.11. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$ und $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$, dann ist $\left(1, \sqrt{n}\right)$ eine Basis von K über $\mathbb{Q}(\sqrt{m})$.*

Beweis. Es ist

$$4 = [K : \mathbb{Q}] = \left[K : \mathbb{Q}\left(\sqrt{m}\right)\right]\left[\mathbb{Q}\left(\sqrt{m}\right) : \mathbb{Q}\right] = 2\left[K : \mathbb{Q}\left(\sqrt{m}\right)\right]$$

und $\left[K : \mathbb{Q}\left(\sqrt{m}\right)\right] = 2$. Es ist $\mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right) \neq \mathbb{Q}\left(\sqrt{m}\right)$ und $\sqrt{n} \notin \mathbb{Q}\left(\sqrt{m}\right)$. Es folgt, dass $\left(1, \sqrt{n}\right)$ linear unabhängig über $\mathbb{Q}(m)$ und $\left(1, \sqrt{n}\right)$ eine Basis von K über $\mathbb{Q}\left(\sqrt{m}\right)$ ist. □

Satz 6.1.12. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$ und $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$, dann ist $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ eine Basis von K über $\mathbb{Q}$.*

Beweis. Es ist $\left(1, \sqrt{m}\right)$ eine Basis von $\mathbb{Q}\left(\sqrt{m}\right)$ über $\mathbb{Q}$. Aus dem Satz 6.1.11 folgt, dass $\left(1, \sqrt{n}\right)$ eine Basis von K über $\mathbb{Q}\left(\sqrt{m}\right)$ ist. Es folgt, dass $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ eine Basis von K über $\mathbb{Q}$ ist. □

Satz 6.1.13. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$, $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ und $\epsilon_0, \epsilon_1 \in \{-1, 1\}$, dann gibt es genau eine Einbettung σ von K in $\mathbb{C}$, für die gilt, dass $\sigma\left(\sqrt{m}\right) = \epsilon_0\sqrt{m}$ und $\sigma\left(\sqrt{n}\right) = \epsilon_1\sqrt{n}$ ist.*

Beweis. Sei M die Menge aller Einbettungen von K in $\mathbb{C}$. Aus dem Satz 6.1.9 folgt, dass $[K : \mathbb{Q}] = 4$ ist. Aus dem Satz 1.2.13 folgt, dass $|M| = 4$ ist. Es ist $\tau|_{\mathbb{Q}\left(\sqrt{m}\right)}$ eine Einbettung von $\mathbb{Q}\left(\sqrt{m}\right)$ in $\mathbb{C}$ für alle $\tau \in M$. Es ist $\tau|_{\mathbb{Q}\left(\sqrt{n}\right)}$ eine Einbettung von $\mathbb{Q}\left(\sqrt{n}\right)$ in $\mathbb{C}$ für alle $\tau \in M$. Aus dem Satz 1.2.14 folgt, dass für alle $\tau \in M$ gilt, dass $\tau\left(\sqrt{m}\right) \in \left\{\sqrt{m}, -\sqrt{m}\right\}$ und $\tau\left(\sqrt{n}\right) \in \left\{\sqrt{n}, -\sqrt{n}\right\}$ ist. Wenn $\phi_0, \phi_1 \in M$, $\phi_0\left(\sqrt{m}\right) = \phi_1\left(\sqrt{m}\right)$ und $\phi_0\left(\sqrt{n}\right) = \phi_1\left(\sqrt{n}\right)$ ist, dann ist

$$\phi_0\left(\sqrt{m}\sqrt{n}\right) = \phi_0\left(\sqrt{m}\right)\phi_0\left(\sqrt{n}\right) = \phi_1\left(\sqrt{m}\right)\phi_1\left(\sqrt{n}\right) = \phi_1\left(\sqrt{m}\sqrt{n}\right)$$

und $\phi_0 = \phi_1$. Da $|M| = 4$ ist, gibt es eine Einbettung σ von K in $\mathbb{C}$, für die gilt, dass $\sigma\left(\sqrt{m}\right) = \epsilon_0\sqrt{m}$ und $\sigma\left(\sqrt{n}\right) = \epsilon_1\sqrt{n}$ ist. □

Satz 6.1.14. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$, $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ und $\sigma_{i,j}$ für alle $i, j \in \{0,1\}$ jene Einbettung von K in $\mathbb{C}$, für die gilt, dass*

$$\sigma_{i,j}\left(\sqrt{m}\right) = (-1)^i\sqrt{m}$$

und

$$\sigma_{i,j}\left(\sqrt{n}\right) = (-1)^j\sqrt{n}$$

ist, dann sind $\sigma_{0,0}$, $\sigma_{0,1}$, $\sigma_{1,0}$ und $\sigma_{1,1}$ alle Einbettungen von K in $\mathbb{C}$.

Beweis. Aus dem Satz 6.1.9 folgt, dass $[K:\mathbb{Q}]=4$ ist. Aus dem Satz 1.2.13 folgt, dass es vier Einbettungen von K in $\mathbb{C}$ gibt. Aus dem Satz 6.1.13 folgt, dass $\sigma_{0,0}$, $\sigma_{0,1}$, $\sigma_{1,0}$ und $\sigma_{1,1}$ alle Einbettungen von K in $\mathbb{C}$ sind. □

Satz 6.1.15. *Seien $m,n\in\mathbb{Z}\setminus\{0,1\}$. Sei m quadratfrei, n quadratfrei, $m\neq n$, $K=\mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$, p eine Primzahl und $k\in\mathbb{N}$. Seien $w,x,y,z\in\mathbb{Z}$. Sei $\alpha=\frac{1}{p^k}\left(w+x\sqrt{m}+y\sqrt{n}+z\sqrt{m}\sqrt{n}\right)$, dann ist*

$$\begin{aligned}\operatorname{fld}_{\alpha,K}(T)=\\ T^4-\frac{1}{p^k}W_4(m,n,w,x,y,z)\,T^3+\frac{1}{p^{2k}}X_4(m,n,w,x,y,z)\,T^2+\frac{1}{p^{3k}}Y_4(m,n,w,x,y,z)\,T\\ +\frac{1}{p^{4k}}Z_4(m,n,w,x,y,z)\end{aligned}$$

Beweis. Sei $\sigma_{i,j}$ für alle $i,j\in\{0,1\}$ jene Einbettung von K in $\mathbb{C}$, für die gilt, dass $\sigma\left(\sqrt{m}\right)=(-1)^i\sqrt{m}$ und $\sigma\left(\sqrt{n}\right)=(-1)^j\sqrt{n}$ ist. Aus dem Satz 6.1.14 folgt, dass $\sigma_{0,0},\sigma_{0,1},\sigma_{1,0},\sigma_{1,1}$ alle Einbettungen von K in $\mathbb{C}$ sind. Sei $\beta_0=p^k\sigma_{0,0}(\alpha)$, $\beta_1=p^k\sigma_{0,1}(\alpha)$, $\beta_2=p^k\sigma_{1,0}(\alpha)$ und $\beta_3=p^k\sigma_{1,1}(\alpha)$. Es ist $\beta_0=w+x\sqrt{m}+y\sqrt{n}+z\sqrt{m}\sqrt{n}$, $\beta_1=w+x\sqrt{m}-y\sqrt{n}-z\sqrt{m}\sqrt{n}$, $\beta_2=w-x\sqrt{m}+y\sqrt{n}-z\sqrt{m}\sqrt{n}$ und $\beta_3=w-x\sqrt{m}-y\sqrt{n}+z\sqrt{m}\sqrt{n}$. Es ist $\operatorname{fld}_{\alpha,K}(T)=\prod_{i=0}^{3}\left(T-\frac{1}{p^k}\beta_i\right)$. Wenn das Produkt $\prod_{i=0}^{3}\left(T-\frac{1}{p^k}\beta_i\right)$ ausmultipliziert und vereinfacht wird, dann ergibt sich, dass

$$\begin{aligned}\operatorname{fld}_{\alpha,K}(T)=\prod_{i=0}^{3}\left(T-\frac{1}{p^k}\beta_i\right)=\\ T^4-\frac{4}{p^k}wT^3+\frac{2}{p^{2k}}\left(-mnz^2-mx^2-ny^2+3w^2\right)T^2\\ +\frac{4}{p^{3k}}\left(mnwz^2-2mnxyz+mwx^2+nwy^2-w^3\right)T\\ +\frac{1}{p^{4k}}\Big(m^2n^2z^4-2m^2nx^2z^2+m^2x^4-2mn^2y^2z^2-2mnw^2z^2+8mnwxyz-2mnx^2y^2\\ -2mw^2x^2+n^2y^4-2nw^2y^2+w^4\Big)=\\ T^4-\frac{1}{p^k}W_4(m,n,w,x,y,z)\,T^3+\frac{1}{p^{2k}}X_4(m,n,w,x,y,z)\,T^2+\frac{1}{p^{3k}}Y_4(m,n,w,x,y,z)\,T\\ +\frac{1}{p^{4k}}Z_4(m,n,w,x,y,z)\end{aligned}$$

ist. □

Satz 6.1.16. *Seien $m,n\in\mathbb{Z}\setminus\{0,1\}$. Sei m quadratfrei, n quadratfrei, $m\neq n$ und $K=\mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$, dann ist $d\left(1,\sqrt{m},\sqrt{n},\sqrt{m}\sqrt{n}\right)=2^8m^2n^2=256m^2n^2$.*

Beweis. Aus dem Satz 6.1.14 folgt, dass

$$d\left(1,\sqrt{m},\sqrt{n},\sqrt{m}\sqrt{n}\right)=\left(\det\begin{pmatrix}1&\sqrt{m}&\sqrt{n}&\sqrt{m}\sqrt{n}\\1&\sqrt{m}&-\sqrt{n}&-\sqrt{m}\sqrt{n}\\1&-\sqrt{m}&\sqrt{n}&-\sqrt{m}\sqrt{n}\\1&-\sqrt{m}&-\sqrt{n}&\sqrt{m}\sqrt{n}\end{pmatrix}\right)^2$$

ist. Es ist

$$d\left(1,\sqrt{m},\sqrt{n},\sqrt{m}\sqrt{n}\right)=\left(\det\begin{pmatrix}1&\sqrt{m}&\sqrt{n}&\sqrt{m}\sqrt{n}\\1&\sqrt{m}&-\sqrt{n}&-\sqrt{m}\sqrt{n}\\1&-\sqrt{m}&\sqrt{n}&-\sqrt{m}\sqrt{n}\\1&-\sqrt{m}&-\sqrt{n}&\sqrt{m}\sqrt{n}\end{pmatrix}\right)^2=2^8m^2n^2=256m^2n^2.$$

□

Satz 6.1.17. *Seien $m,n\in\mathbb{Z}\setminus\{0,1\}$. Sei m quadratfrei, n quadratfrei, $m\neq n$, $K=\mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$ und α ein minimal-ganzalgebraisches Element von K vom Grad 1 bezüglich $\left(1,\sqrt{m},\sqrt{n},\sqrt{m}\sqrt{n}\right)$, dann sind die beiden folgenden Punkte erfüllt:*

1. *Wenn $m\not\equiv 1 \pmod 4$ ist, dann gibt es ein $x\in\mathbb{Z}$, sodass $\alpha=x+\sqrt{m}$ ist.*
2. *Wenn $m\equiv 1 \pmod 4$ ist, dann gibt es ein $y\in\mathbb{Z}$, sodass $\alpha=\frac{y+\sqrt{m}}{2}$.*

Beweis. Seien $a_0,a_1\in\mathbb{Q}$ und $\alpha=a_0+a_1\sqrt{m}$. Aus dem Satz 3.0.12 folgt, dass es ein $d\in\mathbb{N}\setminus\{0\}$ gibt, sodass $a_1=\frac{1}{d}$ ist. Es ist $\alpha=a_0+\frac{1}{d}\sqrt{m}$.

1 Aus dem Satz 1.2.25 folgt, dass $\left(1,\sqrt{m}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{m}\right)$ ist. Es ist $a_0\in\mathbb{Z}$ und $\frac{1}{d}\in\mathbb{Z}$. Es folgt, dass $d=1$ ist.

2 Aus dem Satz 1.2.25 folgt, dass $\left(1,\frac{1+\sqrt{m}}{2}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{m}\right)$ ist. Aus dem Satz 3.0.6 folgt, dass $\frac{1+\sqrt{m}}{2}$ ein minimal-ganzalgebraisches Element von $\mathbb{Q}(\sqrt{m})$ vom Grad 1 bezüglich $\left(1,\sqrt{m}\right)$ ist. Es ist $d=2$. Aus dem Satz 1.2.11 folgt, dass $O\cap\mathbb{Q}=\mathbb{Z}$ ist. Es ist $a_0-\frac{1}{2}=\alpha-\frac{1+\sqrt{m}}{2}\in O\cap\mathbb{Q}=\mathbb{Z}$. Sei $z=a_0-\frac{1}{2}$. Es ist $a_0=\frac{2z+1}{2}$ und $\alpha=\frac{2z+1+\sqrt{m}}{2}$.

□

Satz 6.1.18. *Seien $m,n\in\mathbb{Z}\setminus\{0,1\}$. Sei m quadratfrei, n quadratfrei, $m\neq n$ und $K=\mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$. Wenn $m\equiv 1\ (mod\ 4)$ ist, dann sei $n\equiv 1\ (mod\ 4)$. Sei $(\omega_0,\omega_1,\omega_2,\omega_3)=\left(1,\sqrt{m},\sqrt{n},\sqrt{m}\sqrt{n}\right)$ und $k\in\{2,3\}$. Seien $a_0,a_1,\ldots,a_{k-2}\in\mathbb{Q}$. Seien $b_0,b_1,\ldots,b_{k-1}\in\mathbb{Q}$. Seien $d_{k-1},d_k\in\mathbb{N}\setminus\{0\}$. Sei $\alpha=\sum_{i=0}^{k-2}a_i\omega_i+\frac{1}{d_{k-1}}\omega_{k-1}$, $\beta=\sum_{i=0}^{k-1}b_i\omega_i+\frac{1}{d_k}\omega_k$, α ein minimal-ganzalgebraisches Element von K vom Grad $k-1$ bezüglich $\left(1,\sqrt{m},\sqrt{n},\sqrt{m}\sqrt{n}\right)$ und β ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $\left(1,\sqrt{m},\sqrt{n},\sqrt{m}\sqrt{n}\right)$, dann ist $d_{k-1}\mid d_k$.*

Beweis.

Fall $k = 2$ **und** $m \not\equiv 1 \pmod 4$:
Aus dem Punkt 1 des Satzes 6.1.17 folgt, dass $d_1 = 1$ ist. Es ist $d_1 \mid d_2$.

Fall $k = 2$ **und** $m \equiv 1 \pmod 4$:
Aus dem Punkt 2 des Satzes 6.1.17 folgt, dass $d_1 = 2$ ist. Da $m \equiv 1 \pmod 4$ ist, folgt, dass $n \equiv 1 \pmod 4$ ist. Aus dem Satz 1.2.25 folgt, dass $\left(1, \frac{1+\sqrt{n}}{2}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{n}\right)$ ist. Es ist $\frac{1+\sqrt{n}}{2} \in O_{\mathbb{Q}\left(\sqrt{n}\right)} \subseteq O_K$. Aus dem Satz 3.0.11 folgt, dass es ein $x \in \mathbb{Z}$ gibt, sodass $\frac{1}{2} = x\frac{1}{d_2}$. Es ist $d_2 = 2x$ und $d_1 \mid d_2$.

Fall $k = 3$:
Es ist

$$\alpha = \sum_{i=0}^{k-2} a_i\omega_i + \frac{1}{d_{k-1}}\omega_{k-1} = a_0 + a_1\sqrt{m} + \frac{1}{d_2}\sqrt{n} \in O_K.$$

Es ist $a_1 m + a_0\sqrt{m} + \frac{1}{d_2}\sqrt{m}\sqrt{n} = \sqrt{m}\alpha \in O_K$. Aus dem Satz 3.0.11 folgt, dass es ein $y \in \mathbb{Z}$ gibt, sodass $\frac{1}{d_2} = y\frac{1}{d3}$ ist. Es ist $d_3 = yd_2$ und $d_2 \mid d_3$.

□

Lemma 6.1.19. *Seien $m, n \in \mathbb{Z} \setminus \{0, 1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$ und $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$. Wenn $m \equiv 1 \pmod 4$ ist, dann sei $n \equiv 1 \pmod 4$. Seien $r_0, r_1 \in \mathbb{Z}$. Seien $s_0, s_1 \in \mathbb{N} \setminus \{0\}$. Sei $\operatorname{ggT}(r_0, s_0) = 1$, $\operatorname{ggT}(r_1, s_1) = 1$, $d_2 \in \mathbb{N} \setminus \{0\}$ und $\frac{r_0}{s_0} + \frac{r_1}{s_1}\sqrt{m} + \frac{1}{d_2}\sqrt{n}$ ein minimal-ganzalgebraisches Element von K vom Grad 2 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$, dann ist $s_0 \mid d_2$ und $s_1 \mid d_2$.*

Beweis. Sei $\alpha = \frac{r_0}{s_0} + \frac{r_1}{s_1}\sqrt{m} + \frac{1}{d_2}\sqrt{n}$.

Fall $m \not\equiv 1 \pmod 4$:
Es ist $\frac{d_2 r_0}{s_0} + \frac{d_2 r_1}{s_1}\sqrt{m} + \sqrt{n} = d_2\alpha \in O$. Es ist $\frac{d_2 r_0}{s_0} + \frac{d_2 r_1}{s_1}\sqrt{m} = d_2\alpha - \sqrt{n} \in O$. Es ist $\frac{d_2 r_0}{s_0} + \frac{d_2 r_1}{s_1}\sqrt{m} \in O_{\mathbb{Q}\left(\sqrt{m}\right)}$. Aus dem Satz 1.2.25 folgt, dass $\left(1, \sqrt{m}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{m}\right)$ ist. Es folgt, dass $\frac{d_2 r_0}{s_0} \in \mathbb{Z}$ und $\frac{d_2 r_1}{s_1} \in \mathbb{Z}$ ist. Es ist $s_0 \mid d_2$ und $s_1 \mid d_2$.

Fall $m \equiv 1 \pmod 4$:
Es ist $n \equiv 1 \pmod 4$. Aus dem Satz 1.2.25 folgt, dass $\left(1, \frac{1+\sqrt{m}}{2}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{m}\right)$ ist. Aus dem Satz 3.0.6 folgt, dass $\frac{1+\sqrt{m}}{2}$ ein minimal-ganzalgebraisches Element von $\mathbb{Q}(\sqrt{m})$ vom Grad 1 bezüglich $\left(1, \sqrt{m}\right)$ ist. Aus dem Satz 3.0.5 folgt, dass $\frac{1+\sqrt{m}}{2}$ ein minimal-ganzalgebraisches Element von K vom Grad 1 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ ist. Aus dem Satz 6.1.18 folgt, dass $2 \mid d_2$ ist. Es ist $\frac{d_2 r_0}{2s_0} + \frac{d_2 r_1}{2s_1}\sqrt{m} + \frac{1}{2}\sqrt{n} = \frac{d_2}{2}\alpha \in O_K$. Es ist $\frac{d_2 r_0}{2s_0} - \frac{1}{2} + \frac{d_2 r_1}{2s_1}\sqrt{m} = \frac{d_2}{2}\alpha - \frac{1+\sqrt{n}}{2} \in O_K$. Es ist $\frac{d_2 r_0}{2s_0} - \frac{1}{2} - \frac{d_2 r_1}{2s_1} + \frac{d_2 r_1}{s_1}\frac{1+\sqrt{m}}{2} = \frac{d_2 r_0}{2s_0} - \frac{1}{2} + \frac{d_2 r_1}{2s_1}\sqrt{m} \in O_{\mathbb{Q}\left(\sqrt{m}\right)}$. Da $\left(1, \frac{1+\sqrt{m}}{2}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{m}\right)$ ist, folgt, dass $\frac{d_2 r_0}{2s_0} - \frac{1}{2} - \frac{d_2 r_1}{2s_1} \in \mathbb{Z}$ und $\frac{d_2 r_1}{s_1} \in \mathbb{Z}$ ist. Es ist $s_1 \mid d_2$. Es ist $\frac{d_2 r_0}{s_0} = 2\left(\frac{d_2 r_0}{2s_0} - \frac{1}{2} - \frac{d_2 r_1}{2s_1}\right) + 1 + \frac{d_2 r_1}{s_1} \in \mathbb{Z}$. Es ist $s_0 \mid d_2$.

□

Lemma 6.1.20. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$ und $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$. Wenn $m \equiv 1 \pmod 4$ ist, dann sei $n \equiv 1 \pmod 4$. Seien $r_0, r_1, r_2 \in \mathbb{Z}$. Seien $s_0, s_1, s_2 \in \mathbb{N} \setminus \{0\}$. Sei $\operatorname{ggT}(r_0, s_0) = 1$, $\operatorname{ggT}(r_1, s_1) = 1$, $\operatorname{ggT}(r_2, s_2) = 1$, $d_3 \in \mathbb{N} \setminus \{0\}$ und $\frac{r_0}{s_0} + \frac{r_1}{s_1}\sqrt{m} + \frac{r_2}{s_2}\sqrt{n} + \frac{1}{d_3}\sqrt{m}\sqrt{n}$ ein minimal-ganzalgebraisches Element von K vom Grad 3 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$, dann sind alle drei folgenden Punkte erfüllt:*

1. $s_2 \mid d_3$
2. $s_1 \mid d_3$
3. $s_0 \mid d_3$

Beweis. Sei $\alpha = \frac{r_0}{s_0} + \frac{r_1}{s_1}\sqrt{m} + \frac{r_2}{s_2}\sqrt{n} + \frac{1}{d_3}\sqrt{m}\sqrt{n}$.

1 Aus dem Satz 6.1.19 folgt, dass es $t_0, t_1 \in \mathbb{Z}$ und $d_2 \in \mathbb{N} \setminus \{0\}$ gibt, sodass $\frac{t_0 + t_1\sqrt{m} + \sqrt{n}}{d_2}$ ein minimal-ganzalgebraisches Element von K vom Grad 2 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ ist. Es ist

$$\frac{t_1 m + t_0\sqrt{m} + \sqrt{m}\sqrt{n}}{d_2} = \sqrt{m}\,\frac{t_0 + t_1\sqrt{m} + \sqrt{n}}{d_2} \in O_K.$$

Aus dem Satz 6.1.18 folgt, dass es ein $x \in \mathbb{Z}$ gibt, sodass $d_3 = x d_2$ ist. Es ist $\frac{x r_0}{s_0} + \frac{x r_1}{s_1}\sqrt{m} + \frac{x r_2}{s_2}\sqrt{n} + \frac{1}{d_2}\sqrt{m}\sqrt{n} = x\alpha \in O_K$. Es ist

$$\frac{x r_0}{s_0} - \frac{t_1 m}{d_2} + \left(\frac{x r_1}{s_1} - \frac{t_0}{d_2}\right)\sqrt{m} + \frac{x r_2}{s_2}\sqrt{n} = \frac{x r_0}{s_0} + \frac{x r_1}{s_1}\sqrt{m} + \frac{x r_2}{s_2}\sqrt{n} + \frac{1}{d_2}\sqrt{m}\sqrt{n} - \frac{t_1 m + t_0\sqrt{m} + \sqrt{m}\sqrt{n}}{d_2}$$

und $\frac{x r_0}{s_0} - \frac{t_1 m}{d_2} + \left(\frac{x r_1}{s_1} - \frac{t_0}{d_2}\right)\sqrt{m} + \frac{x r_2}{s_2}\sqrt{n} \in O_K$. Aus dem Satz 3.0.11 folgt, dass es ein $y \in \mathbb{Z}$ gibt, sodass $\frac{x r_2}{s_2} = \frac{y}{d_2}$ ist. Es ist $r_2 d_3 = x r_2 d_2 = y s_2$. Es folgt, dass $s_2 \mid r_2 d_3$ ist. Es ist $s_2 \mid d_3$.

2 und 3 Aus dem Punkt 1 folgt, dass $s_2 \mid d_3$ ist.

Fall $m \not\equiv 1 \pmod 4$:
Es ist

$$\frac{d_3 r_0}{s_0} + \frac{d_3 r_1}{s_1}\sqrt{m} = d_3\left(\frac{r_0}{s_0} + \frac{r_1}{s_1}\sqrt{m} + \frac{r_2}{s_2}\sqrt{n} + \frac{1}{d_3}\sqrt{m}\sqrt{n}\right) - \frac{d_3 r_2}{s_2}\sqrt{n} - \sqrt{m}\sqrt{n}$$

und $\frac{d_3 r_0}{s_0} + \frac{d_3 r_1}{s_1}\sqrt{m} \in O$. Aus dem Satz 1.2.25 folgt, dass $\left(1, \sqrt{m}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{m}\right)$ ist. Es ist $\frac{d_3 r_0}{s_0} \in \mathbb{Z}$ und $\frac{d_3 r_1}{s_1} \in \mathbb{Z}$. Es folgt, dass $s_0 \mid d_3$ und $s_1 \mid d_3$ ist.

Fall $m \equiv 1 \pmod 4$:
Es ist $n \equiv 1 \pmod n$. Aus dem Satz 1.2.25 folgt, dass $\frac{1+\sqrt{m}}{2} \in O$ und $\frac{1+\sqrt{n}}{2} \in O$

ist. Es ist $\frac{\sqrt{n}+\sqrt{m}\sqrt{n}}{2} = \sqrt{n}\frac{1+\sqrt{m}}{2} \in O_K$. Aus dem Satz 3.0.11 folgt, dass es ein $z \in \mathbb{Z}$ gibt, sodass $\frac{1}{2} = \frac{z}{d_3}$ ist. Es ist $2z = d_3$ und $2 \mid d_3$. Es ist

$$\begin{aligned}\frac{d_3r_0}{2s_0} + \frac{1}{2} - \frac{d_3r_2}{2s_2} - \frac{d_3r_1}{2s_1} + \frac{d_3r_1}{s_1}\frac{1+\sqrt{m}}{2} = \frac{d_3r_0}{2s_0} + \frac{1}{2} - \frac{d_3r_2}{2s_2} + \frac{d_3r_1}{2s_1}\sqrt{m} = \\ \frac{d_3r_0}{2s_0} + \frac{d_3r_1}{2s_1}\sqrt{m} + \frac{d_3r_2}{2s_2}\sqrt{n} + \frac{1}{2}\sqrt{m}\sqrt{n} - \frac{d_3r_2}{2s_2} - \frac{d_3r_2}{2s_2}\sqrt{n} + \frac{1}{2} - \frac{1}{2}\sqrt{m}\sqrt{n} = \\ \frac{d_3}{2}\left(\frac{r_0}{s_0} + \frac{r_1}{s_1}\sqrt{m} + \frac{r_2}{s_2}\sqrt{n} + \frac{1}{d_3}\sqrt{m}\sqrt{n}\right) - \frac{d_3r_2}{s_2}\frac{1+\sqrt{n}}{2} + \frac{1-\sqrt{m}\sqrt{n}}{2} = \\ \frac{d_3}{2}\alpha - \frac{d_3r_2}{s_2}\frac{1+\sqrt{n}}{2} + \frac{1+\sqrt{m}}{2} - \sqrt{m}\frac{1+\sqrt{n}}{2} \in O\end{aligned}$$

und $\frac{d_3r_0}{2s_0} + \frac{1}{2} - \frac{d_3r_2}{2s_2} - \frac{d_3r_1}{2s_1} + \frac{d_3r_1}{s_1}\frac{1+\sqrt{m}}{2} \in O_{\mathbb{Q}(\sqrt{m})}$. Aus dem Satz 1.2.25 folgt, dass $\left(1, \frac{1+\sqrt{m}}{2}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{m}\right)$ ist. Es ist $\frac{d_3r_0}{2s_0} + \frac{1}{2} - \frac{d_3r_2}{2s_2} - \frac{d_3r_1}{2s_1} \in \mathbb{Z}$ und $\frac{d_3r_1}{s_1} \in \mathbb{Z}$. Es ist $s_1 \mid d_3$. Es ist

$$\frac{d_3r_0}{s_0} = 2\left(\frac{d_3r_0}{2s_0} + \frac{1}{2} - \frac{d_3r_2}{2s_2} - \frac{d_3r_1}{2s_1}\right) - 1 + \frac{d_3r_2}{s_2} + \frac{d_3r_1}{s_1} \in \mathbb{Z}.$$

Es folgt, dass $s_0 \mid d_3$ ist.

□

Satz 6.1.21. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$ und $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$. Wenn $m \equiv 1 \pmod 4$ ist, dann sei $n \equiv 1 \pmod 4$. Sei $k \in \{1,2,3\}$, $(\omega_0, \omega_1, \omega_2, \omega_3) = \left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ und α ein minimal-ganzalgebraisches Element von K vom Grad k bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$, dann gibt es $x_0, x_1, \ldots, x_{k-1} \in \mathbb{Z}$ und $d \in \mathbb{N} \setminus \{0\}$, sodass*

$$\alpha = \frac{1}{d}\left(\left(\sum_{i=0}^{k-1} x_i\omega_i\right) + \omega_k\right)$$

ist.

Beweis. Der Satz 6.1.21 folgt aus den Sätzen 6.1.17, 6.1.19 und 6.1.20. □

Satz 6.1.22. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$ und $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$. Wenn $m \equiv 1 \pmod 4$ ist, dann sei $n \equiv 1 \pmod 4$. Sei $(\omega_0, \omega_1, \omega_2, \omega_3) = \left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ und p eine Primzahl. Seien $k_1, k_2, k_3 \in \mathbb{N}$. Sei $x_j^{(i)} \in \mathbb{Z}$ für alle $i \in \{1,2,3\}$ und alle $j \in \{0,1,\ldots,i-1\}$. Sei*

$$\alpha_i = \frac{1}{p^{k_i}}\left(\left(\sum_{j=0}^{i-1} x_j^{(i)}\omega_j\right) + \omega_i\right)$$

für alle $i \in \{1,2,3\}$. Sei für alle $i \in \{1,2,3\}$ mindestens einer der beiden folgenden Punkte erfüllt:

(a) *Es ist* α_i *ein minimal-ganzes Element von* K *über* $\mathbb{Z}_{(p)}$ *vom Grad* i *bezüglich* $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$.
(b) $i \neq 3$, $\alpha_i \in O_{p,K}$ *und* $k_i = k_{i+1}$

Dann sind alle drei folgenden Punkte erfüllt:

1. $0 \leq k_1 \leq k_2 \leq k_3$
2. *Es ist* $(1, \alpha_1, \alpha_2, \alpha_3)$ *eine p-ganze Basis von K.*
3. $\nu_p\left(d(K)\right) = \nu_p\left(2^8 m^2 n^2\right) - 2\left(\sum_{i=1}^{3} k_i\right)$

Beweis. Sei β_i ein minimal-ganzalgebraisches Element von K vom Grad i bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ für alle $i \in \{0,1,2,3\}$. Aus dem Satz 6.1.21 folgt, dass es $d_1, d_2, d_3 \in \mathbb{N} \setminus \{0\}$ und $y_j^{(i)} \in \mathbb{Z}$ für alle $i \in \{1,2,3\}$ und alle $j \in \{0,1,\ldots,i-1\}$ gibt, sodass

$$\beta_i = \frac{1}{d_i}\left(\left(\sum_{j=0}^{i-1} y_j^{(i)} \omega_i\right) + \omega_i\right)$$

ist. Aus dem Satz 6.1.18 folgt, dass $d_{i-1} \mid d_i$ für alle $i \in \{2,3\}$ ist. Aus dem Satz 3.0.13 folgt, dass $\beta_0 = 1$ ist. Sei $d_0 = 1$. Es ist $\beta_0 = \frac{1}{d_0}$ und $d_0 \mid d_1$. Es ist 1 ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 0 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$. Sei $l_1 \in \mathbb{N}$, $z_0^{(1)} \in \mathbb{Z}$ und $\frac{z_0^{(1)} + \sqrt{m}}{p^{l_1}}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 1 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$. Sei $l_2 \in \mathbb{N}$, $z_0^{(2)}, z_1^{(2)} \in \mathbb{Z}$ und $\frac{z_0^{(2)} + z_1^{(2)}\sqrt{m} + \sqrt{n}}{p^{l_2}}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 2 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$. Es ist α_3 ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 3 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$. Aus dem Punkt 1 des Satzes 4.0.5 folgt, dass $l_1 \leq l_2 \leq k_3$ ist. Wenn $k_2 = k_3$ ist, dann ist $l_2 = k_2 = k_3$ und α_2 ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 2 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$. Es ist α_2 ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 2 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ und $l_2 = k_2$. Wenn $k_1 = k_2$ ist, dann ist $l_1 = k_1 = k_2$ und α_1 ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 1 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$. Es ist α_1 ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 1 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$. Aus dem Satz 6.1.16 folgt, dass $d\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right) = 2^8 m^2 n^2$ ist. Aus dem Satz 4.0.5 folgt der Satz 6.1.22. □

Satz 6.1.23. *Seien* $m, n \in \mathbb{Z} \setminus \{0,1\}$. *Sei* m *quadratfrei,* n *quadratfrei,* $m \neq n$ *und* $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$. *Wenn* $m \equiv 1 \pmod 4$ *ist, dann sei* $n \equiv 1 \pmod 4$. *Sei* $(\omega_0, \omega_1, \omega_2, \omega_3) = \left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ *und* p *eine Primzahl. Sei* $k_1, k_2, k_3 \in \mathbb{N}$. *Sei* $x_j^{(i)} \in \mathbb{Z}$ *für alle* $i \in \{1,2,3\}$ *und alle* $j \in \{0,1,\ldots,i-1\}$. *Sei*

$$\frac{1}{p^{k_i}}\left(\left(\sum_{j=0}^{i-1} x_j^{(i)} \omega_j\right) + \omega_i\right) \in O_{p,K}$$

für alle $i \in \{1,2,3\}$. *Sei* $\sum_{i=1}^{3} k_i = \frac{\nu_p\left(2^8 m^2 n^2\right)}{2}$, *dann ist*

$$\left(1, \frac{x_0^{(1)} + \sqrt{m}}{p^{k_1}}, \frac{x_0^{(2)} + x_1^{(2)}\sqrt{m} + \sqrt{n}}{p^{k_2}}, \frac{x_0^{(3)} + x_1^{(3)}\sqrt{m} + x_2^{(3)}\sqrt{n} + \sqrt{m}\sqrt{n}}{p_2^k}\right)$$

eine p-ganze Basis von K.

Beweis. Sei $\alpha_i = \frac{1}{p^{k_i}}\left(\left(\sum_{j=0}^{i-1} x_j^{(i)}\omega_j\right) + \omega_i\right)$ für alle $i \in \{1,2,3\}$. Sei $l_1, l_2, l_3 \in \mathbb{N}$, $y_j^{(i)} \in \mathbb{Z}$ für alle $i \in \{1,2,3\}$ und alle $j \in \{0,1,\ldots,i-1\}$ und

$$\frac{1}{p^{l_i}}\left(\left(\sum_{j=0}^{i-1} y_j^{(i)}\omega_j\right) + \omega_i\right)$$

ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad i bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ für alle $i \in \{1,2,3\}$. Es ist $k_i \leq l_i$ für alle $i \in \{1,2,3\}$. Aus dem Punkt 3 des Satzes 6.1.22 folgt, dass $\nu_p\left(d(K)\right) = \nu_p\left(2^8 m^2 n^2\right) - 2\left(\sum_{i=1}^{3} l_i\right)$ ist. Es ist

$$\sum_{i=1}^{3} k_i \leq \sum_{i=1}^{3} l_i = \frac{\nu_p\left(2^8 m^2 n^2\right) - \nu_p\left(d\left(K\right)\right)}{2} = \sum_{i=1}^{3} k_i - \frac{\nu_p\left(d\left(K\right)\right)}{2}.$$

Es folgt, dass $\nu_p\left(d\left(K\right)\right) = 0$ und $\sum_{i=1}^{3} k_i = \sum_{i=1}^{3} l_i$ ist. Es ist $k_i = l_i$ für alle $i \in \{1,2,3\}$. Es ist α_i ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad i bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ für alle $i \in \{1,2,3\}$. Aus dem Satz 6.1.22 folgt, dass $(1, \alpha_1, \alpha_2, \alpha_3)$ eine p-ganze Basis von K ist. □

Satz 6.1.24. *Seien* $m, n \in \mathbb{Z} \setminus \{0,1\}$. *Sei m quadratfrei, n quadratfrei,* $m \neq n$, $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$, *p eine Primzahl und* $k \in \mathbb{N}$. *Seien* $w, x, y, z \in \mathbb{Z}$. *Sei* $\alpha = \frac{1}{p^k}\left(w + x\sqrt{m} + y\sqrt{n} + z\sqrt{m}\sqrt{n}\right)$, *dann sind die beiden folgenden Punkte äquivalent:*

1. $\alpha \in O_{p,K}$
2. $W_4(m,n,w,x,y,z) \equiv 0 \pmod{p^k}$, $X_4(m,n,w,x,y,z) \equiv 0 \pmod{p^{2k}}$, $Y_4(m,n,w,x,y,z) \equiv 0 \pmod{p^{3k}}$ *und* $Z_4(m,n,w,x,y,z) \equiv 0 \pmod{p^{4k}}$

Beweis. Aus dem Satz 2.0.9 folgt, dass genau dann $\alpha \in O_{p,K}$ ist, wenn $\mathrm{fld}_{\alpha,K}(T) \in \mathbb{Z}_{(p)}[T]$ ist. Aus dem Satz 6.1.15 folgt, dass

$$\mathrm{fld}_{\alpha,K}(T) = T^4 - \frac{1}{p^k}W_4(m,n,w,x,y,z)\,T^3 + \frac{1}{p^{2k}}X_4(m,n,w,x,y,z)\,T^2 + \frac{1}{p^{3k}}Y_4(m,n,w,x,y,z)\,T + \frac{1}{p^{4k}}Z_4(m,n,w,x,y,z)$$

ist. Es ist $\mathrm{fld}_{\alpha,K}(T) \in \mathbb{Z}_{(p)}[T]$ genau dann, wenn $W_4(m,n,w,x,y,z) \equiv 0 \pmod{p^k}$, $X_4(m,n,w,x,y,z) \equiv 0 \pmod{p^{2k}}$, $Y_4(m,n,w,x,y,z) \equiv 0 \pmod{p^{3k}}$ und $Z_4(m,n,w,x,y,z) \equiv 0 \pmod{p^{4k}}$ ist. □

6.2 2-ganze Basen

Satz 6.2.1. *Seien $m,n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$, $K = \mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$ und $m \not\equiv 1 \pmod 4$, dann ist $\frac{w+\sqrt{m}}{2} \notin O_{2,K}$ für alle $w \in \mathbb{Z}$.*

Beweis. Angenommen es gibt ein $w \in \mathbb{Z}$, sodass $\frac{w+\sqrt{m}}{2} \in O_{2,K}$ ist. Aus dem Satz 6.1.24 folgt, dass $Z_4(m,n,w,1,0,0) \equiv 0 \pmod{16}$ ist. Es ist

$$0 \equiv Z_4(m,n,w,1,0,0) = m^2 - 2mw^2 + w^4 = \left(m - w^2\right)^2 \pmod{16}.$$

Es folgt, dass $m \equiv w^2 \pmod 4$ ist. Es ist $m \equiv 0 \pmod 4$ oder $m \equiv 1 \pmod 4$. Dies ist ein Widerspruch. □

Satz 6.2.2. *Seien $m,n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$, $K = \mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$, $m \equiv 2 \pmod 4$ und $n \equiv 3 \pmod 4$, dann ist $\frac{w+x\sqrt{m}+\sqrt{n}}{2} \notin O_{2,K}$ für alle $w,x \in \mathbb{Z}$.*

Beweis. Angenommen es ist $w,x \in \mathbb{Z}$ und $\frac{w+x\sqrt{m}+\sqrt{n}}{2} \in O_{2,K}$. Aus dem Satz 6.1.24 folgt, dass $Z_4(m,n,w,x,1,0) \equiv 0 \pmod{16}$ ist. Es ist

$$0 \equiv Z_4(m,n,w,x,1,0) = m^2x^4 - 2mnx^2 - 2mw^2x^2 + n^2 - 2nw^2 + w^4 \equiv 1 + w \pmod 2$$

und $w \equiv 1 \pmod 2$. Es ist

$$\begin{aligned}
0 \equiv Z_4(m,n,w,x,1,0) = m^2x^4 - 2mnx^2 - 2mw^2x^2 + n^2 - 2nw^2 + w^4 \equiv \\
m^2x^2 - 6mx^2 - 2mx^2 + n^2 - 2nw^2 + w^4 = \\
m(m-2)x^2 + 2mx^2 - 8mx^2 + n(n-3) + 3n - 2(n-3)w^2 - 6w^2 + w^2\left(w^2-1\right) \\
+w^2 = \\
m(m-2)x^2 - 6mx^2 + n(n-3) + 3n - 2(n-3)w^2 - 5w^2 + w^2\left(w^2-1\right) \equiv \\
2(m-2)x^2 - 6mx^2 + 3(n-3) + 3n - 2(n-3) - 5w^2 + w^2 - 1 = \\
2mx^2 - 4x^2 - 6mx^2 + 3n - 9 + 3n - 2n + 6 - 4w^2 - 1 = \\
-4mx^2 - 4x^2 + 4n - 4 - 4w^2 \equiv \\
8x^2 - 4x^2 + 12 - 4 - 4 = 4\left(x^2+1\right) \pmod{16}.
\end{aligned}$$

Es ist $x^2 + 1 \equiv 0 \pmod 4$ ist. Dies ist ein Widerspruch. □

Satz 6.2.3. *Seien $m,n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$ und $K = \mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$, dann sind alle vier folgenden Punkte erfüllt:*

1. *Wenn* $m \equiv 2 \pmod 4$ *und* $n \equiv 1 \pmod 2$ *ist, dann ist* $\frac{w_0+x_0\sqrt{m}+y_0\sqrt{n}+\sqrt{m}\sqrt{n}}{4} \notin O_{2,K}$ *für alle* $w_0, x_0, y_0 \in \mathbb{Z}$.
2. *Wenn* $m \equiv 2 \pmod 4$ *und* $n \equiv 1 \pmod 2$ *ist, dann ist* $\frac{\sqrt{m}+\sqrt{m}\sqrt{n}}{2} \in O_{2,K}$.
3. *Wenn* $m \equiv n \equiv 3 \pmod 4$ *ist, dann ist* $\frac{w_1+x_1\sqrt{m}+y_1\sqrt{n}+\sqrt{m}\sqrt{n}}{4} \notin O_{2,K}$ *für alle* $w_1, x_1, y_1 \in \mathbb{Z}$.

Beweis.

1 Angenommen es ist $w_0, x_0, y_0 \in \mathbb{Z}$ und $\frac{w_0+x_0\sqrt{m}+y_0\sqrt{n}+\sqrt{m}\sqrt{n}}{4} \in O_{2,K}$. Aus dem Satz 6.1.24 folgt, dass $X_4(m,n,w_0,x_0,y_0,1) \equiv 0 \pmod{16}$, $Y_4(m,n,w_0,x_0,y_0,1) \equiv 0 \pmod{2^6}$ und $Z_4(m,n,w_0,x_0,y_0,1) \equiv 0 \pmod{2^8}$ ist. Es ist

$$\begin{aligned} 0 \equiv \frac{1}{4}Y_4(m,n,w_0,x_0,y_0,1) = mnw_0 - 2mnx_0y_0 + mw_0x_0^2 + nw_0y_0^2 - w_0^3 \equiv \\ mnw_0 + mw_0x_0^2 + nw_0y_0^2 - w_0^3 = -w_0\left(-mn - mx_0^2 - ny_0^2 + 3w_0^2\right) + 2w_0^3 = \\ \frac{-w_0}{2}X_4(m,n,w_0,x_0,y_0,1) + 2w_0^3 \equiv 2w_0^3 \pmod 4 \end{aligned}$$

und $w_0 \equiv 0 \pmod 2$. Es ist

$$0 \equiv \frac{1}{2}X_4(m,n,w_0,x_0,y_0,1) = -mn - mx_0^2 - ny_0^2 + 3w_0^2 \equiv y_0 \pmod 2.$$

Es ist

$$\begin{aligned} 0 \equiv \frac{1}{2}X_4(m,n,w_0,x_0,y_0,1) = -mn - mx_0^2 - ny_0^2 + 3w_0^2 \equiv \\ 2 + 2x_0^2 \equiv 2(x_0+1) \pmod 4 \end{aligned}$$

und $x_0 \equiv 1 \pmod 2$. Es ist $x_0^2 \equiv 1 \pmod 4$ und $x_0^4 \equiv 1 \pmod 8$. Es ist

$$\begin{aligned} 0 \equiv \frac{1}{2}X_4(m,n,w_0,x_0,y_0,1) = -mn - mx_0^2 - ny_0^2 + 3w_0^2 \equiv -mn - m + y_0^2 + w_0^2 = \\ -m(n+1) + y_0^2 + w_0^2 \equiv 2(n+1) + y_0^2 + w_0^2 \pmod 8. \end{aligned}$$

Es ist

$$\begin{aligned} 0 \equiv \frac{1}{4}Y_4(m,n,w_0,x_0,y_0,1) = mnw_0 - 2mnx_0y_0 + mw_0x_0^2 + nw_0y_0^2 - w_0^3 \equiv \\ mnw_0 + 4y_0 + mw_0 + w_0y_0^2 + w_0^3 = mw_0(n+1) + 4y_0 + w_0y_0^2 + w_0^3 \equiv \\ 2w_0(n+1) + 4y_0 + w_0y_0^2 + w_0^3 = w_0\left(2(n+1) + y_0^2 + w_0^2\right) + 4y_0 \equiv 4y_0 \pmod{16} \end{aligned}$$

und $y_0 \equiv 0 \pmod 4$. Es ist $0 \equiv 2(n+1) + y_0^2 + w_0^2 \equiv 2(n+1) + w_0^2 \pmod 8$. Es ist

$$\begin{aligned} 0 \equiv Z_4(m,n,w_0,x_0,y_0,1) = \\ m^2n^2 - 2m^2nx_0^2 + m^2x_0^4 - 2mn^2y_0^2 - 2mnw_0^2 + 8mnw_0x_0y_0 - 2mnx_0^2y_0^2 - 2mw_0^2x_0^2 + \\ n^2y_0^4 - 2nw_0^2y_0^2 + w_0^4 \equiv \\ m^2n^2 - 2m^2n + m^2 + 4w_0^2 + 4w_0^2 + w_0^4 = m^2(n-1)^2 + 8w_0^2 + w_0^4 \equiv \\ 4(n-1)^2 + w_0^4 = \left(2(n-1) + w_0^2\right)^2 - 4(n-1)w_0^2 \equiv \left(2(n-1) + w_0^2\right)^2 \pmod{2^5}. \end{aligned}$$

Es folgt, dass $2(n-1)+w_0^2 \equiv 0 \pmod 8$ ist. Es ist

$$0 \equiv 2(n+1)+w_0^2+2(n-1)+w_0^2 = 4n+2w_0^2 \equiv 4 \pmod 8.$$

Dies ist ein Widerspruch.

2 Es ist $W_4(m,n,0,1,0,1) = 0$, $X_4(m,n,0,1,0,1) = 2(-mn-m) \equiv 0 \pmod 4$, $Y_4(m,n,0,1,0,1) = 0$ und

$$Z_4(m,n,0,1,0,1) = m^2n^2-2m^2n+m^2 = m^2(n-1)^2 \equiv 0 \pmod{16}.$$

Aus dem Satz 6.1.24 folgt, dass $\frac{\sqrt{m}+\sqrt{m}\sqrt{n}}{2} \in O_{2,K}$ ist.

3 Angenommen es ist $w_1, x_1, y_1 \in \mathbb{Z}$ und $\frac{w_1+x_1\sqrt{m}+y_1\sqrt{n}+\sqrt{m}\sqrt{n}}{4} \in O_{2,K}$. Aus dem Satz 6.1.24 folgt, dass $X_4(m,n,w_1,x_1,y_1,1) \equiv 0 \pmod{16}$ und $Z_4(m,n,w_1,x_1,y_1,1) \equiv 0 \pmod{2^8}$ ist. Es ist

$$0 \equiv \frac{1}{2}X_4(m,n,w_1,x_1,y_1,1) = -mn-mx_1^2-ny_1^2+3w_1^2 \pmod 8$$

und $mx_1^2 \equiv -mn-ny_1^2+3w_1^2 \pmod 8$. Es ist

$$\begin{aligned}
0 \equiv Z_4(m,n,w_1,x_1,y_1,1) = \\
m^2n^2-2m^2nx_1^2+m^2x_1^4-2mn^2y_1^2-2mnw_1^2+8mnw_1x_1y_1-2mnx_1^2y_1^2-2mw_1^2x_1^2 \\
+n^2y_1^4-2nw_1^2y_1^2+w_1^4 \equiv \\
m^2n^2-2mn\left(-mn-ny_1^2+3w_1^2\right)+\left(-mn-ny_1^2+3w_1^2\right)^2-2mn^2y_1^2-2mnw_1^2 \\
-2ny_1^2\left(-mn-ny_1^2+3w_1^2\right)-2w_1^2\left(-mn-ny_1^2+3w_1^2\right)+n^2y_1^4-2nw_1^2y_1^2+w_1^4 = \\
m^2n^2+2m^2n^2+2mn^2y_1^2-6mnw_1^2+m^2n^2+2mn^2y_1^2-6mnw_1^2+n^2y_1^4-6nw_1^2y_1^2 \\
+9w_1^4-2mn^2y_1^2-2mnw_1^2+2mn^2y_1^2+2n^2y_1^4-6nw_1^2y_1^2+2mnw_1^2+2nw_1^2y_1^2-6w_1^4 \\
+n^2y_1^4-2nw_1^2y_1^2+w_1^4 = \\
4m^2n^2+4mn^2y_1^2-12mnw_1^2+4n^2y_1^4-12nw_1^2y_1^2+4w_1^4 \equiv \\
4(1+y_1+w_1+y_1+w_1y_1+w_1) \equiv 4(1+w_1y_1) \pmod 8.
\end{aligned}$$

Es ist $w_1y_1+1 \equiv 0 \pmod 2$. Es folgt, dass $w_1 \equiv y_1 \equiv 1 \pmod 2$ ist. Es ist

$$\begin{aligned}
0 \equiv \frac{1}{2}X_4(m,n,w_1,x_1,y_1,1) = -mn-mx_1^2-ny_1^2+3w_1^2 \equiv \\
1+x_1+1+1 \equiv x_1+1 \pmod 2
\end{aligned}$$

und $x_1 \equiv 1 \pmod 2$. Aus dem Satz 1.2.5 folgt, dass $w_1^2 \equiv x_1^2 \equiv y_1^2 \equiv 1 \pmod 8$ ist. Es ist

$$\begin{aligned}
0 \equiv \frac{1}{2}X_4(m,n,w_1,x_1,y_1,1) = -mn-mx_1^2-ny_1^2+3w_1^2 \equiv -mn-m-n+3 = \\
-m(n+1)-n+3 \equiv n+1-n+3 = 4 \pmod 8.
\end{aligned}$$

Dies ist ein Widerspruch.

□

Satz 6.2.4. *Seien $m,n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$ und $K = \mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$, dann sind alle vier folgenden Punkte erfüllt:*

1. *Wenn $m \equiv n \equiv 1 \pmod 4$ ist, dann ist $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m}\sqrt{n}}{4}\right)$ eine 2-ganze Basis von K.*
2. *Wenn $m \equiv 2 \pmod 4$ und $n \equiv 1 \pmod 4$ ist, dann ist $\left(1, \sqrt{m}, \frac{1+\sqrt{n}}{2}, \frac{\sqrt{m}+\sqrt{m}\sqrt{n}}{2}\right)$ eine 2-ganze Basis von K.*
3. *Wenn $m \equiv 2 \pmod 4$ und $n \equiv 3 \pmod 4$ ist, dann ist $\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}+\sqrt{m}\sqrt{n}}{2}\right)$ eine 2-ganze Basis von K.*
4. *Wenn $m \equiv n \equiv 3 \pmod 4$ ist, dann ist $\left(1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{m}\sqrt{n}}{2}\right)$ eine 2-ganze Basis von K.*

Beweis.

1 Aus dem Satz 1.2.25 folgt, dass $\frac{1+\sqrt{m}}{2} \in O$ und $\frac{1+\sqrt{n}}{2} \in O$ ist. Es ist $\frac{1+\sqrt{m}}{2} \in O_K \subseteq O_{2,K}$ und $\frac{1+\sqrt{n}}{2} \in O_K \subseteq O_{2,K}$. Es ist

$$\begin{aligned}
W_4(m,n,1,1,1,1) = 4 \equiv 0 \pmod 4,\\
X_4(m,n,1,1,1,1) = 2(-mn-m-n+3) =\\
2(-(m-1)(n-1)-2m-2n+4) \equiv 2(-2-2+4) = 0 \pmod{16},\\
Y_4(m,n,1,1,1,1) = 4(mn-2mn+m+n-1) = 4(-mn+m+n-1) =\\
-4(m-1)(n-1) \equiv 0 \pmod{2^6}
\end{aligned}$$

und

$$\begin{aligned}
Z_4(m,n,1,1,1,1) =\\
m^2n^2-2m^2n+m^2-2mn^2-2mn+8mn-2mn-2m+n^2-2n+1 =\\
m^2n^2-2m^2n+m^2-2mn^2+4mn-2m+n^2-2n+1 =\\
\left(m^2-2m+1\right)\left(n^2-2n+1\right) = (m-1)^2(n-1)^2 \equiv 0 \pmod{2^8}.
\end{aligned}$$

Aus dem Satz 6.1.24 folgt, dass $\frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m}\sqrt{n}}{4} \in O_{2,K}$ ist. Es ist $\frac{\nu_2\left(2^8m^2n^2\right)}{2} = 4$. Aus dem Satz 6.1.23 folgt, dass $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m}\sqrt{n}}{4}\right)$ eine 2-ganze Basis von K ist.

2 Aus dem Satz 6.2.1 folgt, dass $\frac{w_{0,1}+\sqrt{m}}{2} \notin O_{2,K}$ für alle $w_{0,1} \in \mathbb{Z}$ ist. Es folgt, dass $\sqrt{m}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(2)}$ vom Grad 1 bezüglich $\left(1,\sqrt{m},\sqrt{n},\sqrt{m}\sqrt{n}\right)$ ist. Aus dem Satz 1.2.25 folgt, dass $\frac{1+\sqrt{n}}{2} \in O$ ist. Es ist $\frac{1+\sqrt{n}}{2} \in O_K \subseteq O_{2,K}$. Aus dem Punkt 2 des Satzes 6.2.3 folgt, dass $\frac{\sqrt{m}+\sqrt{m}\sqrt{n}}{2} \in O_{2,K}$ ist. Aus dem Punkt 1 des Satzes 6.2.3 folgt, dass $\frac{w_{0,3}+x_{0,3}\sqrt{m}+y_{0,3}\sqrt{n}+\sqrt{m}\sqrt{n}}{4} \notin O_{2,K}$ für alle $w_{0,3},x_{0,3},y_{0,3} \in \mathbb{Z}$ ist. Es folgt, dass $\frac{\sqrt{m}+\sqrt{m}\sqrt{n}}{2}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(2)}$ vom Grad 3 bezüglich $\left(1,\sqrt{m},\sqrt{n},\sqrt{m}\sqrt{n}\right)$ ist. Aus dem Punkt 2 des Satzes 6.1.22 folgt, dass $\left(1, \sqrt{m}, \frac{1+\sqrt{n}}{2}, \frac{\sqrt{m}+\sqrt{m}\sqrt{n}}{2}\right)$ eine 2-ganze Basis von K ist.

3 Aus dem Satz 6.2.2 folgt, dass $\frac{w_{1,2}+x_{1,2}\sqrt{m}+\sqrt{n}}{2} \notin O_{p,K}$ für alle $w_{1,2}, x_{1,2} \in \mathbb{Z}$ ist. Es folgt, dass $\sqrt{n}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(2)}$ vom Grad 2 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ ist. Aus dem Punkt 2 des Satzes 6.2.3 folgt, dass $\frac{\sqrt{m}+\sqrt{m}\sqrt{n}}{2} \in O_{2,K}$ ist. Aus dem Punkt 1 des Satzes 6.2.3 folgt, dass $\frac{w_{1,3}+x_{1,3}\sqrt{m}+y_{1,3}\sqrt{n}+\sqrt{m}\sqrt{n}}{4} \notin O_{2,K}$ für alle $w_{1,3}, x_{1,3}, y_{1,3} \in \mathbb{Z}$ ist. Es folgt, dass $\frac{\sqrt{m}+\sqrt{m}\sqrt{n}}{2}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(2)}$ vom Grad 3 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ ist. Aus dem Punkt 2 des Satzes 6.1.22 folgt, dass $\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}+\sqrt{m}\sqrt{n}}{2}\right)$ eine 2-ganze Basis von K ist.

4 Aus dem Satz 6.2.1 folgt, dass $\frac{w_{2,1}+\sqrt{m}}{2} \notin O_{2,K}$ für alle $w_{2,1} \in \mathbb{Z}$ ist. Es ist $\sqrt{m}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(2)}$ vom Grad 1 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$. Es ist $W_4(m,n,0,1,1,0) = 0$,

$$X_4(m,n,0,1,1,0) = 2(-m-n) \equiv 0 \pmod 4,$$

$Y_4(m,n,0,1,1,0) = 0$ und

$$Z_4(m,n,0,1,1,0) = m^2 - 2mn + n^2 = (m-n)^2 \equiv 0 \pmod{16}.$$

Aus dem Satz 6.1.24 folgt, dass $\frac{\sqrt{m}+\sqrt{n}}{2} \in O_{2,K}$ ist. Es ist $W_4(m,n,1,0,0,1) = 4 \equiv 0 \pmod 2$,

$$X_4(m,n,1,0,0,1) = 2(-mn+3) \equiv 0 \pmod 4,$$

$Y_4(m,n,1,0,0,1) = 4(mn-1) \equiv 0 \pmod 8$ und

$$Z_4(m,n,1,0,0,1) = m^2n^2 - 2mn + 1 = (mn-1)^2 \equiv 0 \pmod{16}.$$

Aus dem Satz 6.1.24 folgt, dass $\frac{1+\sqrt{m}\sqrt{n}}{2} \in O_{2,K}$ ist. Aus dem Punkt 3 des Satzes 6.2.3 folgt, dass $\frac{w_{2,3}+x_{2,3}\sqrt{m}+y_{2,3}\sqrt{n}+\sqrt{m}\sqrt{n}}{4} \notin O_{2,K}$ für alle $w_{2,3}, x_{2,3}, y_{2,3} \in \mathbb{Z}$ ist. Es folgt, dass $\frac{1+\sqrt{m}\sqrt{n}}{2}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(2)}$ vom Grad 3 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ ist. Aus dem Punkt 2 des Satzes 6.1.22 folgt, dass $\left(1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{m}\sqrt{n}}{2}\right)$ eine 2-ganze Basis von K ist.

□

6.3 p-ganze Basen für $p \geq 3$

Satz 6.3.1. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$, $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$, p eine Primzahl, $p \geq 3$ und $l = \mathrm{ggT}(m,n)$, dann sind alle drei folgenden Punkte erfüllt:*

1. *Wenn $p \mid l$ ist, dann ist $\frac{w_0+x_0\sqrt{m}+\sqrt{n}}{p} \notin O_{p,K}$ für alle $w_0, x_0 \in \mathbb{Z}$.*
2. *Wenn $p \nmid l$ ist, dann ist $\frac{w_1+x_1\sqrt{m}+y_1\sqrt{n}+\sqrt{m}\sqrt{n}}{p} \notin O_{p,K}$ für alle $w_1, x_1, y_1 \in \mathbb{Z}$.*
3. *Wenn $p \mid l$ ist, dann ist $\frac{w_2+x_2\sqrt{m}+y_2\sqrt{n}+\sqrt{m}\sqrt{n}}{p^2} \notin O_{p,K}$ für alle $w_2, x_2, y_2 \in \mathbb{Z}$.*

Beweis.

1 Angenommen es ist $w_0, x_0 \in \mathbb{Z}$ und $\frac{w_0+x_0\sqrt{m}+\sqrt{n}}{p} \in O_{p,K}$. Aus dem Satz 6.1.24 folgt, dass $W_4(m,n,w_0,x_0,1,0) \equiv 0 \pmod{p}$, $X_4(m,n,w_0,x_0,1,0) \equiv 0 \pmod{p^2}$ und $Z_4(m,n,w_0,x_0,1,0) \equiv 0 \pmod{p^4}$ ist. Es ist $0 \equiv W_4(m,n,w_0,x_0,1,0) = 4w_0 \pmod{p}$ und $w_0 \equiv 0 \pmod{p}$. Es ist

$$0 \equiv \frac{1}{2}X_4(m,n,w_0,x_0,1,0) = -mx_0^2 - n + 3w_0^2 \equiv -mx_0^2 - n \pmod{p^2}.$$

Es ist

$$0 \equiv Z_4(m,n,w_0,x_0,1,0) = m^2x_0^4 - 2mnx_0^2 - 2mw_0^2x_0^2 + n^2 - 2nw_0^2 + w_0^4 \equiv m^2x_0^4 - 2mnx_0^2 + n^2 = \left(mx_0^2 - n\right)^2 \pmod{p^3}$$

und $mx_0^2 - n \equiv 0 \pmod{p^2}$. Es ist $0 \equiv -mx_0^2 - n + mx_0^2 - n = -2n \pmod{p^2}$ und $n \equiv 0 \pmod{p^2}$. Dies ist ein Widerspruch

2 Angenommen es ist $w_1, x_1, y_1 \in \mathbb{Z}$ und $\frac{w_1+x_1\sqrt{m}+y_1\sqrt{n}+\sqrt{m}\sqrt{n}}{p} \in O_{p,K}$. Aus dem Satz 6.1.24 folgt, dass $W_4(m,n,w_1,x_1,y_1,1) \equiv 0 \pmod{p}$, $X_4(m,n,w_1,x_1,y_1,1) \equiv 0 \pmod{p^2}$, $Y_4(m,n,w_1,x_1,y_1,1) \equiv 0 \pmod{p^3}$ und $Z_4(m,n,w_1,x_1,y_1,1) \equiv 0 \pmod{p^4}$ ist. Es ist $0 \equiv W_4(m,n,w_1,x_1,y_1,1) = 4w_1 \pmod{p}$. Es folgt, dass $w_1 \equiv 0 \pmod{p}$ ist. Es ist

$$0 \equiv -\frac{1}{2}X_4(m,n,w_1,x_1,y_1,1) = mn + mx_1^2 + ny_1^2 - 3w_1^2 \equiv mn + mx_1^2 + ny_1^2 \pmod{p^2}.$$

Es ist

$$0 \equiv \frac{1}{4}Y_4(m,n,w_1,x_1,y_1,1) = mnw_1 - 2mnx_1y_1 + mw_1x_1^2 + nw_1y_1^2 - w_1^3 = w_1\left(mn + mx_1^2 + ny_1^2\right) - 2mnx_1y_1 - w_1^3 \equiv -2mnx_1y_1 \pmod{p^3}.$$

Es folgt, dass $mnx_1y_1 \equiv 0 \pmod{p^3}$ und $x_1y_1 \equiv 0 \pmod{p^2}$ ist. Es ist

$$\begin{aligned} 0 \equiv Z_4(m,n,w_1,x_1,y_1,1) = \\ m^2n^2 - 2m^2nx_1^2 + m^2x_1^4 - 2mn^2y_1^2 - 2mnw_1^2 + 8mnw_1x_1y_1 - 2mnx_1^2y_1^2 - 2mw_1^2x_1^2 \\ +n^2y_1^4 - 2nw_1^2y_1^2 + w_1^4 \equiv \\ m^2n^2 - 2m^2nx_1^2 + m^2x_1^4 - 2mn^2y_1^2 - 2mnw_1^2 - 2mw_1^2x_1^2 + n^2y_1^4 - 2nw_1^2y_1^2 = \\ \left(mn + mx_1^2 + ny_1^2\right)^2 - 4m^2nx_1^2 - 4mn^2y_1^2 - 2mnx_1^2y_1^2 - 2w_1^2\left(mn + mx_1^2 + ny_1^2\right) \equiv \\ -4m^2nx_1^2 - 4mn^2y_1^2 = -4mn\left(mx_1^2 + ny_1^2\right) \pmod{p^4}. \end{aligned}$$

Es folgt, dass $mx_1^2 + ny_1^2 \equiv 0 \pmod{p^3}$ ist. Es ist $0 \equiv mn + mx_1^2 + ny_1^2 \equiv mn \pmod{p^2}$. Dies ist ein Widerspruch

3 Angenommen es ist $w_2, x_2, y_2 \in \mathbb{Z}$ und $\frac{w_2+x_2\sqrt{m}+y_2\sqrt{n}+\sqrt{m}\sqrt{n}}{p^2} \in O_{p,K}$. Aus dem Satz 6.1.24 folgt, dass $W_4(m,n,w_2,x_2,y_2,1) \equiv 0 \pmod{p^2}$, $X_4(m,n,w_2,x_2,y_2,1) \equiv 0 \pmod{p^4}$ und $Y_4(m,n,w_2,x_2,y_2,1) \equiv 0 \pmod{p^6}$ ist. Es ist

$$0 \equiv W_4(m,n,w_2,x_2,y_2,1) = 4w_2 \pmod{p^2}$$

und $w_2 \equiv 0 \pmod{p^2}$ ist. Es ist

$$0 \equiv -\frac{1}{2}X_4(m,n,w_2,x_2,y_2,1) = mn + mx_2^2 + ny_2^2 - 3w_2^2 \equiv mn + mx_2^2 + ny_2^2 \pmod{p^4}.$$

Es ist

$$0 \equiv \frac{1}{4}Y_4(m,n,w_2,x_2,y_2,1) = mnw_2 - 2mnx_2y_2 + mw_2x_2^2 + nw_2y_2^2 - w_2^3 = w_2\left(mn + mx_2^2 + ny_2^2\right) - 2mnx_2y_2 - w_2^3 \equiv -2mnx_2y_2 \pmod{p^6}.$$

Es ist $x_2y_2 \equiv 0 \pmod{p^4}$. Es ist

$$0 \equiv x_2\left(mn + mx_2^2 + ny_2^2\right) = mnx_2 + mx_2^3 + nx_2y_2^2 \equiv mx_2^3 \pmod{p^2}$$

und $x_2 \equiv 0 \pmod{p}$. Es ist $0 \equiv mn + mx_2^2 + ny_2^2 \equiv ny_2^2 \pmod{p^2}$ und $y_2 \equiv 0 \pmod{p}$. Es ist $0 \equiv mn + mx_2^2 + ny_2^2 \equiv mn \pmod{p^3}$. Dies ist ein Widerspruch.

□

Satz 6.3.2. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$, $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$, p eine Primzahl, $p \geq 3$ und $l = \operatorname{ggT}(m,n)$, dann sind die beiden folgenden Punkte erfüllt:*

1. *Wenn $p \nmid l$ ist, dann ist $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ eine p-ganze Basis von K.*
2. *Wenn $p \mid l$ ist, dann ist $\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}\sqrt{n}}{p}\right)$ eine p-ganze Basis von K.*

Beweis.

1 Aus dem Punkt 2 des Satzes 6.3.1 folgt, dass $\sqrt{m}\sqrt{n}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 3 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ ist. Aus dem Punkt 2 des Satzes 6.1.22 folgt, dass $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ eine p-ganze Basis von K ist.

2 Aus dem Punkt 1 des Satzes 6.3.1 folgt, dass $\sqrt{n}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 2 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ ist. Es ist $W_4(m,n,0,0,0,1) = 0$, $X_4(m,n,0,0,0,1) = -2mn \equiv 0 \pmod{p^2}$, $Y_4(m,n,0,0,0,1) = 0$ und $Z_4(m,n,0,0,0,1) = m^2n^2 \equiv 0 \pmod{p^4}$. Aus dem Satz 6.1.24 folgt, dass $\frac{\sqrt{m}\sqrt{n}}{p} \in O_{p,K}$ ist. Aus dem Punkt 3 des Satzes 6.3.1 folgt, dass $\frac{\sqrt{m}\sqrt{n}}{p}$ ein minimal-ganzes Element von K über $\mathbb{Z}_{(p)}$ vom Grad 3 bezüglich $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ ist. Aus dem Satz 6.1.22 folgt, dass $\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}\sqrt{n}}{p}\right)$ eine p-ganze Basis von K ist.

□

6.4 Ganzheitsbasen

Die Ganzheitsbasen in den Punkten 1, 3, 4 und 5 des folgenden Satzes stimmen mit den Ganzheitsbasen des Satzes 2 in der Arbeit von Williams [4] überein. Im Satz 6.4.2 wird dieselbe Ganzheitsbasis wie in [4] auch für den Fall, dass die Voraussetzungen des Punktes 2 des Satzes 6.4.1 gegeben sind, erreicht.

Satz 6.4.1. *Seien $m, n \in \mathbb{Z} \setminus \{0, 1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$, $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$, $l = \operatorname{ggT}(m, n)$, $m_0 = \frac{m}{l}$, $n_0 = \frac{n}{l}$ und $\sqrt{m}\sqrt{n} = l\sqrt{m_0}\sqrt{n_0}$, dann sind alle fünf folgenden Punkte erfüllt:*

1. *Wenn $m \equiv n \equiv l \equiv 1 \pmod 4$ ist, dann ist $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_0}\sqrt{n_0}}{4}\right)$ eine Ganzheitsbasis von K.*
2. *Wenn $m \equiv n \equiv 1 \pmod 4$ und $l \equiv 3 \pmod 4$ ist, dann ist*

$$\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{-1-\sqrt{m}-\sqrt{n}+\sqrt{m_0}\sqrt{n_0}}{4}\right)$$

   eine Ganzheitsbasis von K.
3. *Wenn $m \equiv 2 \pmod 4$ und $n \equiv 1 \pmod 4$ ist, dann ist $\left(1, \sqrt{m}, \frac{1+\sqrt{n}}{2}, \frac{\sqrt{m}+\sqrt{m_0}\sqrt{n_0}}{2}\right)$ eine Ganzheitsbasis von K.*
4. *Wenn $m \equiv 2 \pmod 4$ und $n \equiv 3 \pmod 4$ ist, dann ist $\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}+\sqrt{m_0}\sqrt{n_0}}{2}\right)$ eine Ganzheitsbasis von K.*
5. *Wenn $m \equiv n \equiv 3 \pmod 4$ ist, dann ist $\left(1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{m_0}\sqrt{n_0}}{2}\right)$ eine Ganzheitsbasis von K.*

Beweis. Aus dem Satz 6.3.2 folgt, dass $\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$ eine p-ganze Basis von K ist für alle Primzahlen p, für die $p \geq 3$ und $p \nmid l$ gilt. Aus dem Satz 6.3.2 folgt, dass $\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}\sqrt{n}}{q}\right)$ eine q-ganze Basis von K ist für alle Primzahlen q, für die $q \geq 3$ und $q \mid l$ gilt.

1 Aus dem Punkt 1 des Satzes 6.2.4 folgt, dass $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m}\sqrt{n}}{4}\right)$ eine 2-ganze Basis von K ist. Es ist $\frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_0}\sqrt{n_0}}{4} = \frac{l+l\sqrt{m}+l\sqrt{n}+\sqrt{m}\sqrt{n}}{4l}$. Aus dem Satz 4.0.9 folgt, dass $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{l+l\sqrt{m}+l\sqrt{n}+\sqrt{m}\sqrt{n}}{4l}\right)$ eine Ganzheitsbasis von K ist.

2 Aus dem Punkt 1 des Satzes 6.2.4 folgt, dass $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m}\sqrt{n}}{4}\right)$ eine 2-ganze Basis von K ist. Es ist $\frac{-1-\sqrt{m}-\sqrt{n}+\sqrt{m_0}\sqrt{n_0}}{4} = \frac{-l-l\sqrt{m}-l\sqrt{n}+\sqrt{m}\sqrt{n}}{4l}$. Es ist $-l \equiv 1 \pmod 4$. Aus dem Satz 4.0.9 folgt, dass $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{-l-l\sqrt{m}-l\sqrt{n}+\sqrt{m}\sqrt{n}}{4l}\right)$ eine Ganzheitsbasis von K ist.

3 Es folgt, dass $l \equiv 1 \pmod 2$ ist. Aus dem Punkt 2 des Satzes 6.2.4 folgt, dass $\left(1, \sqrt{m}, \frac{1+\sqrt{n}}{2}, \frac{\sqrt{m}+\sqrt{m}\sqrt{n}}{2}\right)$ eine 2-ganze Basis von K ist. Es ist $\frac{\sqrt{m}+\sqrt{m_0}\sqrt{n_0}}{2} = \frac{l\sqrt{m}+\sqrt{m}\sqrt{n}}{2l}$. Aus dem Satz 4.0.9 folgt, dass $\left(1, \sqrt{m}, \frac{1+\sqrt{n}}{2}, \frac{l\sqrt{m}+\sqrt{m}\sqrt{n}}{2l}\right)$ eine Ganzheitsbasis von K ist.

4 Es folgt, dass $l \equiv 1 \pmod 2$ ist. Aus dem Punkt 3 des Satzes 6.2.4 folgt, dass $\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}+\sqrt{m}\sqrt{n}}{2}\right)$ eine 2-ganze Basis von K ist. Es ist $\frac{\sqrt{m}+\sqrt{m_0}\sqrt{n_0}}{2} = \frac{l\sqrt{m}+\sqrt{m}\sqrt{n}}{2l}$. Aus dem Satz 4.0.9 folgt, dass $\left(1, \sqrt{m}, \sqrt{n}, \frac{l\sqrt{m}+\sqrt{m_0}\sqrt{n_0}}{2l}\right)$ eine Ganzheitsbasis von K ist.

5 Es folgt, dass $l \equiv 1 \pmod 2$ ist. Aus dem Punkt 4 des Satzes 6.2.4 folgt, dass $\left(1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{m}\sqrt{n}}{2}\right)$ eine 2-ganze Basis von K ist. Es ist $\frac{1+\sqrt{m_0}\sqrt{n_0}}{2} = \frac{l+\sqrt{m}\sqrt{n}}{2l}$. Aus dem Satz 4.0.9 folgt, dass $\left(1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{l+\sqrt{m}\sqrt{n}}{2l}\right)$ eine Ganzheitsbasis von K ist.

□

Satz 6.4.2. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$, $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$, $l = \operatorname{ggT}(m,n)$, $m_0 = \frac{m}{l}$, $n_0 = \frac{n}{l}$, $\sqrt{m}\sqrt{n} = l\sqrt{m_0}\sqrt{n_0}$, $m \equiv n \equiv 1 \pmod 4$ und $l \equiv 3 \pmod 4$, dann ist $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_0}\sqrt{n_0}}{4}\right)$ eine Ganzheitsbasis von K.*

Beweis. Aus dem Punkt 2 des Satzes 6.4.1 folgt, dass $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{-1-\sqrt{m}-\sqrt{n}+\sqrt{m_0}\sqrt{n_0}}{4}\right)$ eine Ganzheitsbasis von K ist. Es ist $\frac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_0}\sqrt{n_0}}{4} = \frac{1+\sqrt{n}}{2} + \frac{-1-\sqrt{m}-\sqrt{n}+\sqrt{m_0}\sqrt{n_0}}{4}$. Aus dem Satz 1.2.23 folgt, dass $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_0}\sqrt{n_0}}{4}\right)$ eine Ganzheitsbasis von K ist. □

6.5 Diskriminante

Satz 6.5.1. *Seien $m, n \in \mathbb{Z} \setminus \{0,1\}$. Sei m quadratfrei, n quadratfrei, $m \neq n$ und $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$. Wenn $m \equiv 1 \pmod 4$ ist, dann sei $n \equiv 1 \pmod 4$. Sei $l = \operatorname{ggT}(m,n)$, $m_0 = \frac{m}{l}$, $n_0 = \frac{n}{l}$ und $\sqrt{m}\sqrt{n} = l\sqrt{m_0}\sqrt{n_0}$. Seien $d_1, d_2, d_3 \in \mathbb{N}$. Seien $a_0^{(1)}, a_0^{(2)}, a_1^{(2)}, a_0^{(3)}, a_1^{(3)}, a_2^{(3)} \in \mathbb{Q}$. Sei $\alpha_1 = a_0^{(1)} + \frac{1}{d_1}\sqrt{m}$,*

$$\alpha_2 = a_0^{(2)} + a_1^{(2)}\sqrt{m} + \frac{1}{d_2}\sqrt{n}$$

und

$$\alpha_3 = a_0^{(3)} + a_1^{(3)}\sqrt{m} + a_2^{(3)}\sqrt{n} + \frac{1}{d_3}\sqrt{m_0}\sqrt{n_0}.$$

Sei $(1, \alpha_1, \alpha_2, \alpha_3)$ *eine Ganzheitsbasis von K, dann ist*

$$d(K) = \frac{2^8 l^2 m_0^2 n_0^2}{\left(\prod_{n=1}^{3} d_i^2\right)}.$$

Beweis. Es ist

$$\begin{pmatrix} 1 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a_0^{(1)} & \frac{1}{d_1} & 0 & 0 \\ a_0^{(2)} & a_1^{(2)} & \frac{1}{d_2} & 0 \\ a_0^{(3)} & a_1^{(3)} & a_2^{(3)} & \frac{1}{d_3 l} \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{m} \\ \sqrt{n} \\ \sqrt{m}\sqrt{n} \end{pmatrix}.$$

Aus dem Satz 1.2.19 folgt, dass

$$d(1, \alpha_1, \alpha_2, \alpha_3) = \left(\prod_{n=1}^{3} \frac{1}{d_i^2}\right) \frac{1}{l^2} d\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right)$$

ist. Aus dem Satz 6.1.16 folgt, dass $d\left(1, \sqrt{m}, \sqrt{n}, \sqrt{m}\sqrt{n}\right) = 2^8 m^2 n^2$ ist. Es ist

$$d(K) = d(1, \alpha_1, \alpha_2, \alpha_3) = \frac{2^8 m^2 n^2}{\left(\prod_{n=1}^{3} d_i^2\right) l^2} = \frac{2^8 l^2 m_0^2 n_0^2}{\left(\prod_{n=1}^{3} d_i^2\right)}.$$

□

Satz 6.5.2. *Seien* $m, n \in \mathbb{Z} \setminus \{0, 1\}$. *Sei m quadratfrei, n quadratfrei,* $m \neq n$, $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$, $l = \operatorname{ggT}(m, n)$, $m_0 = \frac{m}{l}$, $n_0 = \frac{n}{l}$ *und* $\sqrt{m}\sqrt{n} = l\sqrt{m_0}\sqrt{n_0}$, *dann sind alle drei folgenden Punkte erfüllt:*

1. *Wenn* $m \equiv n \equiv 1 \pmod 4$ *ist, dann ist* $d(K) = l^2 m_0^2 n_0^2$.
2. *Wenn* ($m \equiv 2 \pmod 4$ *und* $n \equiv 1 \pmod 4$) *oder* $m \equiv n \equiv 3 \pmod 4$ *ist, dann ist* $d(K) = 16 l^2 m_0^2 n_0^2$.
3. *Wenn* $m \equiv 2 \pmod 4$ *und* $n \equiv 3 \pmod 4$ *ist, dann ist* $d(K) = 64 l^2 m_0^2 n_0^2$.

Beweis.

1 Aus dem Punkt 1 und dem Punkt 2 des Satzes 6.4.1 folgt, dass

$$\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_0}\sqrt{n_0}}{4}\right)$$

oder

$$\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{-1-\sqrt{m}-\sqrt{n}+\sqrt{m_0}\sqrt{n_0}}{4}\right)$$

eine Ganzheitsbasis von K ist. Aus dem Satz 6.5.1 folgt, dass $d(K) = \frac{2^8 l^2 m_0^2 n_0^2}{2^8}$ ist. Es ist $d(K) = l^2 m_0^2 n_0^2$.

2 Aus dem Punkt 3 und dem Punkt 5 des Satzes 6.4.1 folgt, dass

$$\left(1, \sqrt{m}, \frac{1+\sqrt{n}}{2}, \frac{\sqrt{m}+\sqrt{m_0}\sqrt{n_0}}{2}\right)$$

oder

$$\left(1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{m_0}\sqrt{n_0}}{2}\right)$$

eine Ganzheitsbasis von K ist. Aus dem Satz 6.5.1 folgt, dass $d(K) = \frac{2^8 l^2 m_0^2 n_0^2}{16}$ ist. Es ist $d(K) = 16 l^2 m_0^2 n_0^2$.

3 Aus dem Punkt 4 des Satzes 6.4.1 folgt, dass $\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}+\sqrt{m_0}\sqrt{n_0}}{2}\right)$ eine Ganzheitsbasis von K ist. Aus dem Satz 6.5.1 folgt, dass $d(K) = \frac{2^8 l^2 m_0^2 n_0^2}{4}$ ist. Es ist $d(K) = 64 l^2 m_0^2 n_0^2$.

□

6.6 Beispiele

Die Ganzheitsbasis $\left(1, \frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{13}}{2}, \frac{1+\sqrt{5}+\sqrt{13}+\sqrt{65}}{4}\right)$ des algebraischen Zahlkörpers $\mathbb{Q}\left(\sqrt{5}, \sqrt{13}\right)$ des folgenden Satzes wird auch in dem Beispiel 4 in der Arbeit von Williams [4] angeführt und bewiesen.

Satz 6.6.1. *Es ist* $\left(1, \frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{13}}{2}, \frac{1+\sqrt{5}+\sqrt{13}+\sqrt{65}}{4}\right)$ *eine Ganzheitsbasis von* $\mathbb{Q}\left(\sqrt{5}, \sqrt{13}\right)$ *und* $d\left(\mathbb{Q}\left(\sqrt{5}, \sqrt{13}\right)\right) = 4225$.

Beweis. Aus dem Punkt 1 des Satzes 6.4.1 folgt, dass $\left(1, \frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{13}}{2}, \frac{1+\sqrt{5}+\sqrt{13}+\sqrt{65}}{4}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{5}, \sqrt{13}\right)$ ist. Aus dem Punkt 1 des Satzes 6.5.2 folgt, dass $d\left(\mathbb{Q}\left(\sqrt{5}, \sqrt{13}\right)\right) = 25 \cdot 13^2 = 4225$ ist. □

Satz 6.6.2. *Es ist* $\left(1, \frac{1+\sqrt{21}}{2}, \frac{1+\sqrt{33}}{2}, \frac{-1-\sqrt{21}-\sqrt{33}+\sqrt{77}}{4}\right)$ *eine Ganzheitsbasis von* $\mathbb{Q}\left(\sqrt{21}, \sqrt{33}\right)$ *und* $d\left(\mathbb{Q}\left(\sqrt{21}, \sqrt{33}\right)\right) = 53361$.

Beweis. Es ist $21 = 3 \cdot 7$ und $33 = 3 \cdot 11$. Aus dem Punkt 2 des Satzes 6.4.1 folgt, dass $\left(1, \frac{1+\sqrt{21}}{2}, \frac{1+\sqrt{33}}{2}, \frac{-1-\sqrt{21}-\sqrt{33}+\sqrt{77}}{4}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{21}, \sqrt{33}\right)$ ist. Aus dem Punkt 1 des Satzes 6.5.2 folgt, dass $d\left(\mathbb{Q}\left(\sqrt{21}, \sqrt{33}\right)\right) = 3^2 \cdot 7^2 \cdot 11^2 = 53361$ ist. □

Satz 6.6.3. *Es ist* $\left(1, \sqrt{10}, \frac{1+\sqrt{5}}{2}, \frac{\sqrt{10}+\sqrt{2}}{2}\right)$ *eine Ganzheitsbasis von* $\mathbb{Q}\left(\sqrt{10}, \sqrt{5}\right)$ *und* $d\left(\mathbb{Q}\left(\sqrt{10}, \sqrt{5}\right)\right) = 1600$.

Beweis. Aus dem Punkt 3 des Satzes 6.4.1 folgt, dass $\left(1, \sqrt{10}, \frac{1+\sqrt{5}}{2}, \frac{\sqrt{10}+\sqrt{2}}{2}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{10}, \sqrt{5}\right)$ ist. Aus dem Punkt 2 des Satzes 6.5.2 folgt, dass $d\left(\mathbb{Q}\left(\sqrt{10}, \sqrt{5}\right)\right) = 16 \cdot 5^2 \cdot 2^2 = 1600.$ ist. □

Satz 6.6.4. *Es ist* $\left(1, \sqrt{2}, \sqrt{3}, \frac{\sqrt{2}+\sqrt{6}}{2}\right)$ *eine Ganzheitsbasis von* $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ *und* $d\left(\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)\right) = 2304.$

Beweis. Aus dem Punkt 4 des Satzes 6.4.1 folgt, dass $\left(1, \sqrt{2}, \sqrt{3}, \frac{\sqrt{2}+\sqrt{6}}{2}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ ist. Aus dem Punkt 3 des Satzes 6.5.2 folgt, dass $d\left(\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)\right) = 64 \cdot 4 \cdot 9 = 2304$ ist. □

Satz 6.6.5. *Es ist* $\left(1, \sqrt{2}, i, \frac{\sqrt{2}+\sqrt{2}i}{2}\right)$ *eine Ganzheitsbasis von* $\mathbb{Q}\left(\sqrt{2}, i\right)$ *und* $d\left(\mathbb{Q}\left(\sqrt{2}, i\right)\right) = 256.$

Beweis. Aus dem Punkt 4 des Satzes 6.4.1 folgt, dass $\left(1, \sqrt{2}, i, \frac{\sqrt{2}+\sqrt{2}i}{2}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{2}, i\right)$ ist. Aus dem Punkt 3 des Satzes 6.5.2 folgt, dass $d\left(\mathbb{Q}\left(\sqrt{2}, i\right)\right) = 64 \cdot 4 = 256$ ist. □

Satz 6.6.6. *Es ist* $\left(1, \sqrt{3}, \frac{\sqrt{3}+i}{2}, \frac{1+\sqrt{3}i}{2}\right)$ *eine Ganzheitsbasis von* $\mathbb{Q}\left(\sqrt{3}, i\right)$ *und* $d\left(\mathbb{Q}\left(\sqrt{3}, i\right)\right) = 144.$

Beweis. Aus dem Punkt 5 des Satzes 6.4.1 folgt, dass $\left(1, \sqrt{3}, \frac{\sqrt{3}+i}{2}, \frac{1+\sqrt{3}i}{2}\right)$ eine Ganzheitsbasis von $\mathbb{Q}\left(\sqrt{3}, i\right)$ ist. Aus dem Punkt 2 des Satzes 6.5.2 folgt, dass $d\left(\mathbb{Q}\left(\sqrt{3}, i\right)\right) = 16 \cdot 3^2 = 144$ ist. □

Literatur

[1] Şaban Alaca. »p-Integral bases of algebraic number fields«. Diss. Carleton University, 1994.

[2] Şaban Alaca und Kenneth S. Williams. *Introductory algebraic number theory*. Cambridge University Press, 2004. xvii+428.

[3] Gerd Fischer. *Lineare Algebra: Eine Einführung für Studienanfänger*. 18., aktualisierte Aufl. 2014. Springer Fachmedien Wiesbaden, 2014. xxii+384.

[4] Kenneth S. Williams. »Integers of biquadratic fields«. *Canadian Mathematical Bulletin* 13 (1970), S. 519–526.

Curriculum Vitae

Persönliche Daten

Name	Daniel Klocker, BSc
Geburtsdatum	24.02.1987
Geburtsort	Innsbruck
Staatsbürgerschaft	Österreich

Ausbildung

09/1997 - 06/2005	Bundesgymnasium Dornbirn
10/2006 - 04/2013	Diplomstudium Mathematik, Universität Wien, ohne Abschluss, Umstieg auf Bachelor- und Masterstudium
03/2013 - 10/2013	Bachelorstudium Mathematik, Universität Wien
Beginn 10/2013	Masterstudium Mathematik, Universität Wien