



HAL
open science

Imaginärquadratische Einbettung von Maximalordnungen rationaler Quaternionenalgebren, und die nichtzyklischen endlichen Untergruppen der Bianchi-Gruppen

Norbert Krämer

► **To cite this version:**

Norbert Krämer. Imaginärquadratische Einbettung von Maximalordnungen rationaler Quaternionenalgebren, und die nichtzyklischen endlichen Untergruppen der Bianchi-Gruppen. 2013. hal-00720823v2

HAL Id: hal-00720823

<https://hal.science/hal-00720823v2>

Preprint submitted on 22 Dec 2013 (v2), last revised 20 Feb 2017 (v7)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Imaginärquadratische Einbettung von Ordnungen rationaler Quaternionenalgebren, und die nichtzyklischen endlichen Untergruppen der Bianchi-Gruppen

Norbert Krämer

22. Dezember 2013

Zusammenfassung

Seien k ein imaginärquadratischer Zahlkörper, F eine rationale Quaternionenalgebra und M eine Erweiterung von F zur k -Quaternionenalgebra. Wir klassifizieren die F -Ordnungen, die Durchschnitt von F mit einer M -Maximalordnung sind, und wir weisen nach, dass der Index eines solchen Durchschnitts in einer F -Maximalordnung eindeutig den Isomorphietyp der jeweiligen M -Maximalordnung bestimmt.

Wir setzen dann die Einbettungen der Ordnungen zweier rationaler Quaternionenalgebren F und F' in M -Maximalordnungen zueinander in Beziehung (Satz 5.8).

Damit können wir ermitteln, ob die Bianchi-Gruppe über der Hauptordnung von k 3-Dieder-, Tetraeder- oder maximalendliche 2-Diedergruppen enthält (Satz 6.5).

Inhaltsverzeichnis

1	Einleitung	2
2	Bezeichnungen und Grundlagen	3
3	Einbettung rationaler Quaternionenalgebren	5
4	Einbettung p-adischer Quaternionenordnungen	8
5	Einbettung rationaler Quaternionenordnungen	15
6	Die endlichen Untergruppen der Bianchi-Gruppen	20

Mathematics subject classification (2010):

11S45 Algebras and orders, and their zeta functions

11R52 Quaternion and other division algebras: arithmetic, zeta functions

11F06 Structure of modular groups and generalizations; arithmetic groups

20G07 Structure theory (Linear algebraic groups and related topics)

20G30 Linear algebraic groups over global fields and their integers

1 Einleitung

Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung \mathfrak{o} .

Seien F eine \mathbb{Q} -Quaternionenalgebra, $M \cong k \otimes_{\mathbb{Q}} F$ eine Erweiterung von F zur k -Quaternionenalgebra, \mathfrak{F} eine F -Maximalordnung und \mathfrak{M} eine M -Maximalordnung mit $\mathfrak{F} \subset \mathfrak{M}$.

Für eine F -Ordnung $\mathfrak{G} \subset \mathfrak{F}$ sei $\Lambda(\mathfrak{G}) := [\mathfrak{F} : \mathfrak{G}]$. Wir nennen \mathfrak{G} dann \mathfrak{o} -kompatibel, wenn \mathfrak{G}_p an allen Stellen p von \mathbb{Q} mit $p \mid \Lambda(\mathfrak{G})$ eine zu $\mathfrak{o}_p = \mathbb{Z}_p \mathfrak{o}$ isomorphe Ordnung enthält. Wir untersuchen Existenz und Struktur \mathfrak{o} -kompatibler F -Ordnungen (Satz 5.3 mit den Sätzen 4.1, 4.2 und 4.4), und wir zeigen, dass \mathfrak{G} genau dann \mathfrak{o} -kompatibel ist, wenn es eine M -Maximalordnung \mathfrak{N} mit $\mathfrak{G} = F \cap \mathfrak{N}$ gibt, und dass der Isomphietyp von \mathfrak{N} in Relation zu \mathfrak{M} dann nur vom Isomphietyp von F und von $\Lambda(\mathfrak{G})$ abhängt (Sätze 5.5 und 5.6).

Unser Hauptergebnis ist der nachstehende Satz 5.8, der die Einbettungen von Ordnungen zweier \mathbb{Q} -Quaternionenalgebren in M -Maximalordnungen zueinander in Beziehung setzt. Wir verwenden darin die folgenden Notationen: Für eine Stelle p von \mathbb{Q} und $a, b \in \mathbb{Q}_p^\times$ sei $\left(\frac{a, b}{p}\right)$ das Hilbert-Symbol. Sei $\left(\frac{F}{p}\right) := +1$ oder -1 , je nachdem, ob F an der Stelle p zerfällt oder verzweigt ist. Sei $\Sigma(F)$ das Produkt der endlichen Verzweigungsstellen von F , multipliziert mit -1 , falls F an der Stelle ∞ verzweigt ist. Sei $\Sigma_k(F)$ das Produkt der Verzweigungsstellen von F , die in k zerlegt sind. Und sei $\Lambda(\mathfrak{M} \cap \mathfrak{N}) := [\mathfrak{M} : (\mathfrak{M} \cap \mathfrak{N})]$. *Bemerkung:* Der Isomphietyp von \mathfrak{N} in Relation zu \mathfrak{M} hängt nur von der Gesamtheit der Hilbertsymbole $\left(\frac{\Lambda(\mathfrak{M} \cap \mathfrak{N}), -d}{p}\right)$ ab. \mathfrak{N} ist genau dann isomorph zu \mathfrak{M} , wenn es ein $f \in \mathbb{N}$ gibt mit: $f \mid \Sigma_k(F)$ und $\left(\frac{f\Lambda(\mathfrak{M} \cap \mathfrak{N}), -d}{p}\right) = 1$ für alle Stellen p (Lemma 5.4).

Satz 5.8. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*

Seien F, F' zwei \mathbb{Q} -Quaternionenalgebren, sei M eine gemeinsame Erweiterung von F und F' zur k -Quaternionenalgebra, und seien $\mathfrak{M}, \mathfrak{M}'$ zwei M -Maximalordnungen.

Dann gibt es ein $f \in \mathbb{N}$ mit $f \mid \Sigma_k(F)$, so dass für alle Stellen p von \mathbb{Q} gilt:

$$\left(\frac{\Sigma(F)\Lambda(F \cap \mathfrak{M})f\Lambda(\mathfrak{M} \cap \mathfrak{M}')\Sigma(F')\Lambda(F' \cap \mathfrak{M}'), -d}{p}\right) = \left(\frac{F}{p}\right) \left(\frac{F'}{p}\right).$$

Wir zeigen die oben genannten Aussagen über die Einbettungen $\mathfrak{G} = F \cap \mathfrak{N}$ und schließlich Satz 5.8, indem wir erstens (Kapitel 3) je zwei \mathbb{Q} -Quaternionenalgebren $F, F' \subset M$ zueinander in Beziehung setzen (Satz 3.4), zweitens (Kapitel 4) die lokalen Einbettungen $\mathfrak{G}_p = F_p \cap \mathfrak{N}_p$ an den endlichen Stellen p von \mathbb{Q} untersuchen, an denen M_p zerfällt, und drittens (Kapitel 5) die lokalen Sätze und Lemmata global synthetisieren und schließlich mit Satz 3.4 kombinieren. Für den Fall, dass k ein Zerfällungskörper von F ist, lassen sich die Sätze 3.4 und 5.8 auf die einfacheren Klassifizierungssätze 3.5 und 5.9 reduzieren.

Als Anwendung von Satz 5.9 können wir dann unter anderem klären, welche nichtzyklischen endlichen Untergruppen die Bianchi-Gruppe $PSL_2(\mathfrak{o}) = SL_2(\mathfrak{o})/\{\pm 1\}$ enthält:

Satz 6.5. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung \mathfrak{o} . Dann gilt:*

- (i) *$PSL_2(\mathfrak{o})$ enthält genau dann eine 3-Diedergruppe \mathcal{D}_3 , wenn $p \equiv 1 \pmod{3}$ für alle Primteiler $p \neq 3$ von d .*
- (ii) *$PSL_2(\mathfrak{o})$ enthält genau dann eine Tetraedergruppe \mathcal{T} , wenn $p \equiv 1$ oder $p \equiv 3 \pmod{8}$ für alle Primteiler $p \neq 2$ von d .*
- (iii) *$PSL_2(\mathfrak{o})$ enthält genau dann eine 2-Diedergruppe \mathcal{D}_2 , aber nicht die Tetraedergruppe \mathcal{T} mit $\mathcal{D}_2 \subset \mathcal{T} \subset PSL_2(k)$, wenn $p \equiv 1 \pmod{4}$ für alle Primteiler $p \neq 2$ von d .*

Unter Verwendung der Ergebnisse von [4] lassen sich nun für jedes d die Konjugationsklassenanzahlen der endlichen Untergruppen der Bianchi-Gruppe angeben (in Vorbereitung). Rahm hat in [6] die homologische Torsion und die Farrell-Tate-Kohomologie der Bianchi-Gruppen ermittelt und als Funktion dieser Konjugationsklassenanzahlen ausgedrückt.

Wir führen Satz 6.5 wie folgt auf Satz 5.8 zurück: Enthält $PSL_2(k)$ eine Untergruppe vom Isomorphietyp \mathcal{D}_3 , \mathcal{T} oder \mathcal{D}_2 , dann erzeugt deren Urbild in $SL_2(k)$ über \mathbb{Q} eine Quaternionenalgebra $F \subset M_2(k)$ und über \mathbb{Z} eine F -Ordnung \mathfrak{F} . Wir setzen dann die Einbettung von \mathfrak{F} in eine $M_2(k)$ -Maximalordnung in Beziehung zur Einbettung $M_2(\mathbb{Z}) \subset M_2(\mathfrak{o})$. Wir erhalten die Sätze 6.2.(ii), 6.2.(iii) und 6.3.(iii) sowie Satz 6.4 mit dem Spezialfall Satz 6.5.

Ich danke Alexander D. Rahm für seine Ratschläge und die technische Unterstützung, und Jürgen Rohlf für die kritische Durchsicht des Manuskripts und hilfreiche Vorschläge.

2 Bezeichnungen und Grundlagen

Für die in diesem Artikel benutzen zahlentheoretischen Grundlagen verweisen wir summarisch auf [1] für imaginärquadratische Zahlkörper) und [5] für Quaternionenalgebren. Für die speziellen Bezeichnungen und Grundlagen zu Bianchi-Gruppen siehe Kapitel 6.

In einer abelschen Gruppe G sei $G^{(2)}$ die Untergruppe der Quadrate. In einem Ring R mit Eins sei R^\times die Gruppe der multiplikativ invertierbaren Elemente. Für kommutatives R sei $M_2(R)$ die R -Algebra der 2×2 -Matrizen mit Koeffizienten in R . Für $z \in \mathbb{C}$ bezeichne $z \mapsto \bar{z}$ die komplexe Konjugation und $|z| = \sqrt{z\bar{z}}$ den Absolutbetrag.

Sei im Folgenden stets $d \in \mathbb{N}$ quadratfrei und $k = \mathbb{Q}(i\sqrt{d}) \subset \mathbb{C}$ ein imaginärquadratischer Zahlkörper mit Hauptordnung \mathfrak{o} und Diskriminante D . Die Einschränkung der komplexen Konjugation auf k stimmt mit der nichttrivialen Galois-Involution von k/\mathbb{Q} überein. Bezeichne I die Gruppe der \mathfrak{o} -Ideale und $H \subset I$ die Untergruppe der Hauptideale. Für $\mathfrak{a} \in I$ sei $N_{k|\mathbb{Q}}(\mathfrak{a}) \in \mathbb{Q}^+$ die Absolutnorm. Für $a \in k^\times$ ist dann $N_{k|\mathbb{Q}}(a\mathfrak{o}) = N_{k|\mathbb{Q}}(a)$.

Sei p stets eine Stelle von \mathbb{Q} , d.h. eine Primzahl $p \in \mathbb{N}$ oder die unendliche Stelle $p = \infty$. Sei \mathfrak{p} stets eine Stelle von k , d.h. ein Primideal $\mathfrak{p} \subset \mathfrak{o}$ oder die unendliche Stelle $\mathfrak{p} = \infty$.

Ist p eine endliche Stelle von \mathbb{Q} , dann ist k auf natürliche Weise eingebettet in die halbeinfache quadratische Erweiterung $k_p \cong \mathbb{Q}_p \otimes_{\mathbb{Q}} k$ von \mathbb{Q}_p , mit der Hauptordnung $\mathfrak{o}_p = \mathbb{Z}_p \mathfrak{o}$. Die Galois-Involution $a \mapsto \bar{a}$ von k/\mathbb{Q} setzt sich auf natürliche Weise auf k_p/\mathbb{Q}_p fort. Ist p verzweigt oder träge in k mit Primteiler \mathfrak{p} , dann ist auf natürliche Weise $k_p = k_{\mathfrak{p}}$ und $\mathfrak{o}_p = \mathfrak{o}_{\mathfrak{p}}$. Für die jeweils einzige unendliche Stelle von \mathbb{Q} und k ist $\mathbb{Q}_{\infty} = \mathbb{R}$ und $k_{\infty} = \mathbb{C}$. Ist p zerlegt in k mit den Primteilern \mathfrak{p} und $\bar{\mathfrak{p}}$, dann ist $k_p \cong k_{\mathfrak{p}} \times k_{\bar{\mathfrak{p}}}$ und $\mathfrak{o}_p \cong \mathfrak{o}_{\mathfrak{p}} \times \mathfrak{o}_{\bar{\mathfrak{p}}}$.

Für eine Stelle p von \mathbb{Q} und $a, b \in \mathbb{Q}_p^{\times}$ sei $\left(\frac{a, b}{p}\right)$ das Hilbert-Symbol.

Für Rechenregeln zum Hilbert-Symbol siehe [1, Kapitel I, § 6, Formeln (9)-(13), Satz 7].

Ist F eine \mathbb{Q} -Quaternionenalgebra, dann ist F auf natürliche Weise eingebettet in die p -Komponente $F_p \cong \mathbb{Q}_p \otimes_{\mathbb{Q}} F$ von F . Wir identifizieren \mathbb{Q} und \mathbb{Q}_p mit den Zentren von F und F_p . Für $p \in \mathbb{N}$ und einen \mathbb{Z} -Modul $\mathfrak{F} \subset F$ ist $\mathfrak{F}_p = \mathbb{Z}_p \mathfrak{F}$ die p -Komponente von \mathfrak{F} . Für eine Stelle \mathfrak{p} von k und eine k -Quaternionenalgebra M sei analog $M \subset M_{\mathfrak{p}} \cong k_{\mathfrak{p}} \otimes_k M$ sowie $k \subset M$ und $k_{\mathfrak{p}} \subset M_{\mathfrak{p}}$. Ist $\mathfrak{p} \subset \mathfrak{o}$ und $\mathfrak{M} \subset M$ ein \mathfrak{o} -Modul, so ist $\mathfrak{M}_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}} \mathfrak{M}$.

Sind $p \in \mathbb{N}$ eine Primzahl, F eine \mathbb{Q} -Quaternionenalgebra und $M \cong k \otimes_{\mathbb{Q}} F$ eine Erweiterung von F zur k -Quaternionenalgebra, dann bezeichne $M_p \cong k_p \otimes_k M \cong k_p \otimes_{\mathbb{Q}} F$ die p -Komponente von M . Auf natürliche Weise ist $M \subset M_p$ und wir identifizieren k_p mit dem Zentrum von M_p . Ist p verzweigt oder träge in k mit Primteiler \mathfrak{p} , dann ist auf natürliche Weise $M_p = M_{\mathfrak{p}}$, und für einen \mathfrak{o} -Modul $\mathfrak{M} \subset M$ gilt $\mathfrak{M}_p = \mathfrak{M}_{\mathfrak{p}}$. Ist p zerlegt in k mit den Primteilern \mathfrak{p} und $\bar{\mathfrak{p}}$, dann ist $M_p \cong M_{\mathfrak{p}} \times M_{\bar{\mathfrak{p}}} \cong F_p \times F_p$ und $\mathfrak{M}_p = \mathfrak{o}_p \mathfrak{M} \cong \mathfrak{M}_{\mathfrak{p}} \times \mathfrak{M}_{\bar{\mathfrak{p}}}$.

Für ein Element A einer Quaternionenalgebra Q bezeichne A^* das konjugierte Element. $N(A) = AA^*$ und $S(A) = A + A^*$ sind dann die (reduzierte) Norm und die Spur von A .

Ist K ein Körper und $Q \cong M_2(K)$ eine K -Quaternionenalgebra, dann heißen, in dieser Reihenfolge, $U_{11}, U_{12}, U_{21}, U_{22} \in Q$ Matriceseinheiten in Q , wenn für alle $r, s \in \{1, 2\}$ gilt: $U_{r1}U_{1s} = U_{r2}U_{2s} = U_{rs} \neq 0$ und $U_{r1}U_{2s} = U_{r2}U_{1s} = 0$. Dann ist $\{U_{11}, U_{12}, U_{21}, U_{22}\}$ eine Basis von Q über K , und für ein $A = \alpha U_{11} + \beta U_{12} + \gamma U_{21} + \delta U_{22} \in Q$ mit $\alpha, \beta, \gamma, \delta \in K$ gilt bezüglich dieser Matriceseinheiten die Gleichung (oder Darstellung) $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Für eine Darstellung bezüglich Matriceseinheiten gelten die bekannten Matrix-Rechenregeln.

Lemma 2.1. *Sei K ein \mathfrak{p} -adischer Zahlkörper mit Hauptordnung \mathfrak{D} und Primelement Π , und sei Q eine K -Quaternionenalgebra.*

- (i) *Seien $A, B \in Q$ mit $N(A) = N(B)$ und $S(A) = S(B)$ sowie $S(A)^2 \neq 4N(A)$. Dann gibt es ein $J \in Q^{\times}$ mit $JAJ^{-1} = B$.*

- (ii) Seien $\mathfrak{R}, \mathfrak{R}'$ zwei Q -Maximalordnungen. Wenn Q zerfällt, dann gibt es ein $r \in \mathbb{N}_0$ und Matrizeeinheiten in Q , bezüglich derer $\mathfrak{R} = \begin{pmatrix} \mathfrak{D} & \mathfrak{D} \\ \mathfrak{D} & \mathfrak{D} \end{pmatrix}$, $\mathfrak{R}' = \begin{pmatrix} \mathfrak{D} & \Pi^{-r}\mathfrak{D} \\ \Pi^r\mathfrak{D} & \mathfrak{D} \end{pmatrix}$.

Beweis.

- (i) Falls $K[A]$ Körper ist, siehe [5, Theorem 2.9.8].
Andernfalls zerfällt Q , wir können $Q = M_2(K)$ annehmen. Das charakteristische Polynom von A hat dann in K zwei Nullstellen $a \neq b$. Nun folgt leicht, dass es $X, Y \in GL_2(K)$ gibt mit $XAX^{-1} = YBY^{-1} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Wir setzen $J := Y^{-1}X$.
- (ii) Siehe [3, Seite 135, Beweis von Satz 7, Fall b)].

□

3 Einbettung rationaler Quaternionenalgebren

Definition 3.1. Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$. Sei F eine \mathbb{Q} -Quaternionenalgebra, und sei M eine Erweiterung von F zur k -Quaternionenalgebra.

- (i) Ist p eine Stelle von \mathbb{Q} , dann sei $\left(\frac{F}{p}\right) := +1$ oder -1 ,
je nachdem, ob F an der Stelle p zerfällt oder verzweigt ist.
- (ii) Sei $\Sigma(F)$ das Produkt der endlichen Verzweigungsstellen von F ,
multipliziert mit -1 , falls F an der Stelle ∞ verzweigt ist.
- (iii) Sei $\Sigma_k(F)$ das Produkt der Verzweigungsstellen von F , die in k zerlegt sind.
- (iv) Sei $\Phi_F : M \rightarrow M$ die Abbildung mit $\Phi_F(A + i\sqrt{d}B) := A - i\sqrt{d}B$ für $A, B \in F$.

Lemma 3.2. Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$. Sei F eine \mathbb{Q} -Quaternionenalgebra, und sei M eine Erweiterung von F zur k -Quaternionenalgebra. Dann gilt:

- (i) M ist an einer Stelle \mathfrak{p} von k genau dann verzweigt, wenn $\mathfrak{p} \mid \Sigma_k(F)$ gilt.
- (ii) Eine \mathbb{Q} -Quaternionenalgebra E kann genau dann in M eingebettet werden,
wenn $\Sigma_k(E) = \Sigma_k(F)$ gilt.
- (iii) Es gibt bis auf Isomorphie genau eine \mathbb{Q} -Quaternionenalgebra E
mit $\Sigma_k(E) = \Sigma_k(F)$ und $|\Sigma(E)| = \Sigma_k(E)$.

Beweis.

- (i) Wenn $p \neq \infty$ in k verzweigt oder träge ist, dann zerfällt M_p ,
siehe [5, Theorem 2.6.5]. Außerdem gilt $M_\infty \cong M_2(\mathbb{C})$.
Wenn $p \neq \infty$ in k zerlegt ist mit $p\mathfrak{o} = \mathfrak{p}\bar{\mathfrak{p}}$, dann gilt $M_p \cong M_{\mathfrak{p}} \times M_{\bar{\mathfrak{p}}} \cong F_p \times F_p$.

(ii) folgt aus (i), siehe [5, Theorem 2.7.5].

(iii) Sei S die Menge der Stellen p von \mathbb{Q} mit $p \mid \Sigma_k(F)$. Dann hat S oder $S \cup \{\infty\}$ eine gerade Anzahl von Elementen. Die Behauptung folgt mit [5, Theorem 7.3.6].

□

Lemma 3.3. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*

Sei E eine \mathbb{Q} -Quaternionenalgebra, und sei p eine Stelle von \mathbb{Q} . Sei p in k nicht zerlegt.

Dann gibt es ein $\tau \in \mathbb{Z}$ mit $\left(\frac{\tau, -d}{p}\right) = -1$, so dass $\mathbb{Q}(\sqrt{\tau})$ Zerfällungskörper von E ist.

Beweis. Wir bestimmen τ so, dass alle endlichen Verzweigungsstellen von E in $\mathbb{Q}(\sqrt{\tau})$ verzweigt sind und dass $\tau < 0$ gilt, falls E an der Stelle ∞ verzweigt ist. (Dann ist $\mathbb{Q}(\sqrt{\tau})_q$ Zerfällungskörper von E_q für alle Verzweigungsstellen q von E , siehe [5, Theorem 2.6.5].)

Falls $\left(\frac{\Sigma(E), -d}{p}\right) = -1$, sei $\tau = \Sigma(E)$. Im Folgenden nehmen wir $\left(\frac{\Sigma(E), -d}{p}\right) = 1$ an.

- Falls $p \neq \infty$ in k verzweigt ist, gibt es ein zu $D\Sigma(E)$ teilerfremdes $\varepsilon \in \mathbb{N}$ mit $\left(\frac{\varepsilon, -d}{p}\right) = -1$. Dann sei $\tau = \varepsilon\Sigma(E)$.
- Falls $p \neq \infty$ in k träge ist, gilt $p \nmid \Sigma(E)$, denn sonst wäre $\left(\frac{\Sigma(E)/p, -d}{p}\right) = -1$, Widerspruch. Dann sei $\tau = p\Sigma(E)$.
- Falls $p = \infty$ ist, sei $\tau = -\Sigma(E)$.

□

Satz 3.4. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$. Sei E eine \mathbb{Q} -Quaternionenalgebra, und sei M eine Erweiterung von E zur k -Quaternionenalgebra. Dann gilt:*

(i) Φ_E ist ein \mathbb{Q} -Algebrenautomorphismus von M mit $E = \{A \in M \mid \Phi_E(A) = A\}$ und $\Phi_E(\lambda A) = \overline{\lambda}\Phi_E(A)$ und $\Phi_E^2(A) = A$ sowie $\Phi_E(A^*) = \Phi_E(A)^*$ für $\lambda \in k$, $A \in M$.

(ii) Sei $T \in M^\times$ mit $\Phi_E(T) = T^*$.

Dann ist $F(T) := \{A \in M \mid T\Phi_E(A)T^{-1} = A\}$ eine \mathbb{Q} -Quaternionenalgebra mit $\Phi_{F(T)}(A) = T\Phi_E(A)T^{-1}$ für $A \in M$.

Es gilt $N(T) \in \mathbb{Q}^\times$ und $\left(\frac{N(T), -d}{p}\right) = \left(\frac{E}{p}\right) \left(\frac{F(T)}{p}\right)$ für alle Stellen p von \mathbb{Q} .

(iii) Sei umgekehrt $F \subset M$ eine \mathbb{Q} -Quaternionenalgebra.

Dann ist $F = F(T)$ für ein $T \in M^\times$ mit $\Phi_E(T) = T^*$.

T ist bis auf einen Faktor aus \mathbb{Q}^\times eindeutig bestimmt.

Beweis. Wir kürzen $\Phi := \Phi_E$ ab.

(i) rechnet man leicht nach.

- (ii) $F(T)$ ist eine \mathbb{Q} -Algebra und via Zuordnungsvorschrift $A \mapsto i\sqrt{d}A$ als \mathbb{Q} -Vektorraum isomorph zu $F(T)^- = \{A \in M \mid T\Phi(A)T^{-1} = -A\}$. Es gilt $T\Phi(T) \in \mathbb{Q}^\times$; und mithilfe der Zerlegung $A = (A + T\Phi(A)T^{-1})/2 + (A - T\Phi(A)T^{-1})/2$ folgt, dass $M = F(T) \oplus F(T)^-$ gilt. $F(T)$ hat über \mathbb{Q} die Dimension 4 und ist wegen $i\sqrt{d} \notin F(T)$ und $M \cong k \otimes_{\mathbb{Q}} F(T)$ eine zentrale und einfache \mathbb{Q} -Algebra.

Sei nun p eine Stelle von \mathbb{Q} .

Falls p in k zerlegt ist, gilt $\left(\frac{N(T), -d}{p}\right) = 1$ und $\left(\frac{E}{p}\right) = \left(\frac{F(T)}{p}\right)$, siehe Lemma 3.2.(ii). Im Folgenden können wir also annehmen, dass p in k nicht zerlegt ist. Φ ist auf natürliche Weise zu einem \mathbb{Q}_p -Algebrenautomorphismus von M_p fortsetzbar.

- Im Fall $\left(\frac{E}{p}\right) \left(\frac{F(T)}{p}\right) = 1$ ist E_p isomorph zu $F(T)_p$. Einen Isomorphismus $E_p \rightarrow F(T)_p$ können wir zu einem k_p -Algebrenautomorphismus von M_p fortsetzen. Also gibt es ein $J \in M_p^\times$ mit $F(T)_p = JE_pJ^{-1}$. Für alle $A \in E_p$ gilt dann $JAJ^{-1} = \Phi_{F(T)}(JAJ^{-1}) = T\Phi(JAJ^{-1})T^{-1} = T\Phi(J)A\Phi(J)^{-1}T^{-1}$. Also gibt es ein $\lambda \in k_p^\times$ mit $T = \lambda J\Phi(J)^{-1}$ und $N(T) = T\Phi(T) = \lambda\bar{\lambda}$.

Sei τ wie in Lemma 3.3. Dann gibt es ein $U \in E^\times$ mit $U^2 = \tau$.

Wir setzen $T' = i\sqrt{d}U$. Dann ist $\Phi(T') = T'^*$ und $N(T') = d\tau$.

Daher gilt $\left(\frac{N(T'), -d}{p}\right) = -1$, und deshalb gilt notwendig $\left(\frac{E}{p}\right) \left(\frac{F(T')}{p}\right) = -1$.

- Im Fall $\left(\frac{E}{p}\right) \left(\frac{F(T)}{p}\right) = -1$ ist $F(T')_p$ isomorph zu $F(T)_p$, also gibt es ein $J \in M_p^\times$ mit $JAJ^{-1} = \Phi_{F(T)}(JAJ^{-1})$ für alle $A \in F(T')_p$, also mit $JAJ^{-1} = T\Phi(J)\Phi(A)\Phi(J)^{-1}T^{-1} = T\Phi(J)T'^{-1}\Phi_{F(T')}(A)T'\Phi(J)^{-1}T^{-1}$. Also gibt es ein $\lambda \in k_p^\times$ mit $T = \lambda JT'\Phi(J)^{-1}$ und $N(T) = T\Phi(T) = \lambda\bar{\lambda}N(T')$.

- (iii) Wegen $\Phi_F(\Phi(\lambda A)) = \lambda\Phi_F(\Phi(A))$ für $\lambda \in k$, $A \in M$ ist $\Phi_F \circ \Phi$ ein k -Algebrenautomorphismus von M . Nach [5, Corollary 2.9.9] gibt es also ein $T \in M^\times$ mit $\Phi_F(A) = T\Phi(A)T^{-1}$ für alle $A \in M$, und aus $\Phi_F^2(A) = \Phi^2(A) = A$ folgt dann $T\Phi(T) \in k^\times$. Sei $\Phi(T) = \lambda T^*$ mit $\lambda \in k^\times$. Dann ist $T = \Phi(\lambda T^*) = \bar{\lambda}\lambda T$, und daher gilt $\bar{\lambda}\lambda = 1$. Also gibt es ein $\mu \in k^\times$ mit $\lambda = \mu\bar{\mu}^{-1}$. Wir ersetzen T durch μT . Dann ist $\Phi(T) = T^*$, und offensichtlich gilt $\Phi_F = \Phi_{F(T)}$, also $F = F(T)$.

□

Satz 3.5. Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Diskriminante D .

Sei F eine \mathbb{Q} -Quaternionenalgebra mit Zerfällungskörper k .

Dann gibt es ein $\tau \in \mathbb{Q}^\times$, so dass F isomorph ist zu $F(\tau) := \left\{ \begin{pmatrix} a & b \\ \tau\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in k \right\}$.

Damit gilt $\left(\frac{F}{p}\right) = \left(\frac{\tau, -d}{p}\right)$ für alle Stellen p von \mathbb{Q} . Man kann o.B.d.A. annehmen, dass $\tau \in \mathbb{Z}$ quadratfrei und teilerfremd zu D ist, und dass $\tau \equiv 1 \pmod{4}$ gilt, falls $2 \mid d$.

Beweis. Seien $E = M_2(\mathbb{Q})$ und $M = M_2(k)$. Dann sind E eine \mathbb{Q} -Quaternionenalgebra mit $\left(\frac{E}{p}\right) = 1$ für alle Stellen p von \mathbb{Q} und M eine Erweiterung von E zur k -Quaternionenalgebra. Für $A = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in M$ gilt $\Phi_E(A) = \begin{pmatrix} \overline{a'} & \overline{b'} \\ \overline{c'} & \overline{d'} \end{pmatrix}$. Nach Voraussetzung kann F in M eingebettet werden, und nach Satz 3.4.(iii) gibt es ein $T \in M^\times$ mit $\Phi_E(T) = T^*$, so dass F isomorph ist zu $F(T)$. Nach Satz 3.4.(ii) hängt die Isomorphieklasse von F nur davon ab, welche Werte $\left(\frac{N(T), -d}{p}\right)$ für die Stellen p von \mathbb{Q} annimmt.

Sei $\tau = N(T)/d$. Wir können dann zunächst T durch $i\sqrt{d} \begin{pmatrix} 0 & 1 \\ \tau & 0 \end{pmatrix}$ ersetzen.

Damit folgt leicht $F(T) = F(\tau)$ und $\left(\frac{F}{p}\right) = \left(\frac{\tau, -d}{p}\right)$ für alle Stellen p von \mathbb{Q} .

Es gibt genau ein $r \in \mathbb{Q}^+$, so dass $\tau r^2 \in \mathbb{Z}$ quadratfrei ist. Wir ersetzen τ durch τr^2 . Sei g der größte gemeinsame Teiler von τ und d , und sei $\tau = g\tau'$ und $d = gd'$. Wegen $\left(\frac{d + g^2, -d}{p}\right) = 1$ gilt $\left(\frac{\tau, -d}{p}\right) = \left(\frac{g^2\tau'(d' + g), -d}{p}\right)$. Falls $g > 1$ ist, ersetzen wir τ durch den quadratfreien Anteil von $\tau'(d' + g)$. Dann ist τ teilerfremd zu d . Falls τ und D einen gemeinsamen Teiler $g' > 1$ haben, ist $g' = 2$ und $d \equiv 1 \pmod{4}$, und wir ersetzen τ durch den quadratfreien Anteil von $\tau(d+1)/4$. Dann ist τ teilerfremd zu D . Falls $2 \mid d$ und $\tau \not\equiv 1 \pmod{4}$, ist $d \equiv 2 \pmod{4}$ und $\tau \equiv 3 \pmod{4}$. In diesem Fall ersetzen wir schließlich τ durch den quadratfreien Anteil von $\tau(d+1)$. □

4 Einbettung p -adischer Quaternionenordnungen

Satz 4.1. *Sei p eine endliche Stelle von \mathbb{Q} .*

Seien F_p eine \mathbb{Q}_p -Quaternionenalgebra, \mathfrak{F}_p eine F_p -Maximalordnung und $K_p, K'_p \subset F_p$ zwei quadratische Körpererweiterungen von \mathbb{Q}_p mit den Hauptordnungen $\mathfrak{D}_p, \mathfrak{D}'_p \subset \mathfrak{F}_p$. Sei p verzweigt in K_p und träge in K'_p . Sei $\Pi \in \mathfrak{D}_p$ Primelement, und sei $\mathfrak{D}'_p = \mathbb{Z}_p[\Omega]$.

- (i) *Sei \mathfrak{G}_p eine F_p -Ordnung mit $\mathfrak{D}_p \subset \mathfrak{G}_p \subset \mathfrak{F}_p$.
Dann gibt es ein $r \in \mathbb{N}_0$ mit $\mathfrak{G}_p = \mathfrak{D}_p + \mathfrak{D}_p\Pi^r\Omega$ und $[\mathfrak{F}_p : \mathfrak{G}_p] = [\mathfrak{D}_p : \mathfrak{D}_p\Pi^r] = p^r$.*
- (ii) *Sei \mathfrak{G}_p eine F_p -Ordnung mit $\mathfrak{D}'_p \subset \mathfrak{G}_p \subset \mathfrak{F}_p$.
Dann gibt es ein $r \in \mathbb{N}_0$ mit $\mathfrak{G}_p = \mathfrak{D}'_p + p^r\mathfrak{D}'_p\Pi$ und $[\mathfrak{F}_p : \mathfrak{G}_p] = [\mathfrak{D}'_p : p^r\mathfrak{D}'_p] = p^{2r}$.*
- (iii) *Sei $r \in \mathbb{N}_0$. Dann sind $\mathfrak{D}_p + \mathfrak{D}_p\Pi^r\Omega$ und $\mathfrak{D}'_p + p^r\mathfrak{D}'_p\Pi$ jeweils F_p -Ordnungen.*

Bemerkung: Eine quadratische Körpererweiterung von \mathbb{Q}_p ist stets in F_p einbettbar, und ihre Hauptordnung ist stets in eine F_p -Maximalordnung einbettbar. Alle F_p -Maximalordnungen sind isomorph zueinander. Die Voraussetzungen von Satz 4.1 sind also erfüllbar.

Beweis.

- (i) Wir zeigen zuerst durch Widerspruch, dass $\{1, \Pi, \Omega, \Pi\Omega\}$ eine \mathbb{Z}_p -Basis von \mathfrak{F}_p ist. Wir nehmen also an, dass es $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_p$ gibt, nicht alle durch p teilbar, mit $A := \alpha + \beta\Pi + \gamma\Omega + \delta\Pi\Omega \in p\mathfrak{F}_p$. Wir multiplizieren A von links mit Π^* . Wegen $p \mid N(\Pi) = \Pi^*\Pi$ gilt dann auch $B := \alpha\Pi^* + \gamma\Pi^*\Omega \in p\mathfrak{F}_p$, also $p^2 \mid N(B)$. Wegen $p^2 \nmid N(\Pi)$ folgt $p \mid N(\alpha + \gamma\Omega)$. Daraus folgt $\alpha + \gamma\Omega \in p\mathfrak{D}'_p$, also $\alpha, \gamma \in p\mathbb{Z}_p$. Dann gilt auch $C := \beta\Pi + \delta\Pi\Omega \in p\mathfrak{F}_p$. Wie für B folgt $\beta, \delta \in p\mathbb{Z}_p$, Widerspruch. $\{1, \Pi, \Omega, \Pi\Omega\}$ ist eine \mathbb{Z}_p -Basis und $\{1, \Omega\}$ eine \mathfrak{D}_p -Basis des Linksmoduls \mathfrak{F}_p .
- Sei $\mathfrak{B}_p = \{B \in K_p \mid B\Omega \in \mathfrak{G}_p\}$.
Wegen $\mathfrak{D}_p \subset \mathfrak{G}_p \subset \mathfrak{F}_p$ ist \mathfrak{B}_p ein ganzes \mathfrak{D}_p -Ideal, also gilt $\mathfrak{B}_p = \mathfrak{D}_p\Pi^r$ mit $r \in \mathbb{N}_0$.
Nach Konstruktion gilt $\mathfrak{B}_p\Omega \subset \mathfrak{G}_p$, wegen $\mathfrak{D}_p \subset \mathfrak{G}_p$ also $\mathfrak{D}_p + \mathfrak{B}_p\Omega \subset \mathfrak{G}_p$.
Seien umgekehrt $A, B \in K_p$ mit $A + B\Omega \in \mathfrak{G}_p$.
Aus $\mathfrak{G}_p \subset \mathfrak{F}_p$ folgt dann $A, B \in \mathfrak{D}_p$, und wegen $\mathfrak{D}_p \subset \mathfrak{G}_p$ ist $B\Omega \in \mathfrak{G}_p$, also $B \in \mathfrak{B}_p$.
Da p in K_p verzweigt ist, gilt $[\mathfrak{D}_p : \mathfrak{D}_p\Pi] = p$ und $[\mathfrak{F}_p : \mathfrak{G}_p] = [\mathfrak{D}_p : \mathfrak{B}_p] = p^r$.
- (ii) Wie in (i) folgt, dass $\{1, \Omega, \Pi, \Omega\Pi\}$ eine \mathbb{Z}_p -Basis von \mathfrak{F}_p ist. (Man multipliziere mit Π^* von rechts statt von links.) Analog folgt dann, dass $\{1, \Pi\}$ eine \mathfrak{D}'_p -Basis des Linksmoduls \mathfrak{F}_p ist, und dass $\mathfrak{G}_p = \mathfrak{D}'_p + \mathfrak{B}'_p\Pi$ für ein ganzes \mathfrak{D}'_p -Ideal $\mathfrak{B}'_p = p^r\mathfrak{D}'_p$ ist, mit $r \in \mathbb{N}_0$. Wegen $[\mathfrak{D}'_p : p\mathfrak{D}'_p] = p^2$ ist dann $[\mathfrak{F}_p : \mathfrak{G}_p] = [\mathfrak{D}'_p : \mathfrak{B}'_p] = p^{2r}$.
- (iii) Zum Beweis, dass $\mathfrak{G}_p := \mathfrak{D}_p + \mathfrak{D}_p\Pi^r\Omega$ eine F_p -Ordnung ist, müssen wir nur zeigen, dass \mathfrak{G}_p multiplikativ abgeschlossen ist. Seien also $A_1, A_2 \in \mathfrak{D}_p$ und $B_1, B_2 \in \mathfrak{D}_p\Pi^r$. Da \mathfrak{F}_p multiplikativ abgeschlossen ist, ist $\Omega(A_2 + B_2\Omega) = A' + B'\Omega$ mit $A', B' \in \mathfrak{D}_p$. Dann ist $(A_1 + B_1\Omega)(A_2 + B_2\Omega) = A'' + B''\Omega$ mit $A'' = A_1A_2 + B_1A' \in \mathfrak{D}_p$ und $B'' = A_1B_2 + B_1B' \in \mathfrak{D}_p\Pi^r$. Genauso folgt, dass $\mathfrak{D}'_p + p^r\mathfrak{D}'_p\Pi$ eine F_p -Ordnung ist.

□

Satz 4.2. *Sei p eine endliche Stelle von \mathbb{Q} .*

Seien $F_p \cong M_2(\mathbb{Q}_p)$ eine \mathbb{Q}_p -Quaternionenalgebra, \mathfrak{F}_p eine F_p -Maximalordnung und $K_p \subset F_p$ eine halbeinfache quadratische Erweiterung von \mathbb{Q}_p mit Hauptordnung $\mathfrak{D}_p \subset \mathfrak{F}_p$. Sei p zerlegt in K_p , sei also K_p kein Körper.

- (i) *Sei \mathfrak{G}_p eine F_p -Ordnung mit $\mathfrak{D}_p \subset \mathfrak{G}_p \subset \mathfrak{F}_p$.*

Dann gibt es Matrizeseinheiten in F_p , bezüglich derer $\mathfrak{D}_p = \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$ gilt.

Diesbezüglich gibt es dann $r, s \in \mathbb{Z}$ mit $[\mathfrak{F}_p : \mathfrak{G}_p] = p^{r+s}$ und $\mathfrak{G}_p = \begin{pmatrix} \mathbb{Z}_p & p^s\mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$.

Man kann überdies die Matrizeseinheiten so wählen, dass $r \in \mathbb{N}_0$ und $s = 0$ gilt.

- (ii) *Sei $r \in \mathbb{N}_0$. Dann gibt es Matrizeseinheiten in F_p , bezüglich derer gilt:*

$$\mathfrak{G}_p := \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix} \text{ ist eine } F_p\text{-Ordnung mit } \mathfrak{D}_p \subset \mathfrak{G}_p \subset \mathfrak{F}_p.$$

Beweis.

(i) Je zwei zerfallende halbeinfache quadratische Erweiterungen von \mathbb{Q}_p sind isomorph zueinander. Nach Lemma 2.1.(i) gibt es Matrizeeinheiten $U_{11}, U_{12}, U_{21}, U_{22} \in F_p$, bezüglich derer $\mathfrak{D}_p = \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$ gilt. Für $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathfrak{G}_p$ mit $\alpha, \beta, \gamma, \delta \in \mathbb{Q}_p$ gilt dann $\beta U_{12} = U_{11} A U_{22} \in \mathfrak{G}_p$ und $\gamma U_{21} = U_{22} A U_{11} \in \mathfrak{G}_p$ sowie $\alpha, \delta \in \mathbb{Z}_p$. Also ist $\{U_{11}, p^s U_{12}, p^r U_{21}, U_{22}\}$ mit geeigneten $r, s \in \mathbb{Z}$ eine \mathbb{Z}_p -Basis von \mathfrak{G}_p . Da \mathfrak{G}_p die Diskriminante $p^{2(r+s)} \mathbb{Z}_p$ hat, gilt $[\mathfrak{F}_p : \mathfrak{G}_p] = p^{r+s}$. Bezüglich der Matrizeeinheiten $U_{11}, p^s U_{12}, p^{-s} U_{21}, U_{22}$ gilt schließlich $\mathfrak{D}_p = \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$ und $\mathfrak{G}_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^{r+s} \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$.

(ii) Nach (i) kann man Matrizeeinheiten in F_p so wählen, dass $\mathfrak{D}_p = \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$ und $\mathfrak{F}_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ gilt. Man rechnet leicht nach, dass \mathfrak{G}_p eine F_p -Ordnung ist. □

Lemma 4.3. *Sei p eine endliche Stelle von \mathbb{Q} , und sei F_p eine \mathbb{Q}_p -Quaternionenalgebra. Seien $\mathfrak{F}_p, \mathfrak{F}'_p$ zwei F_p -Maximalordnungen und $K_p, K'_p \subset F_p$ zwei halbeinfache quadratische Erweiterungen von \mathbb{Q}_p mit den Hauptordnungen $\mathfrak{D}_p \subset \mathfrak{F}_p, \mathfrak{D}'_p \subset \mathfrak{F}'_p$. Seien $\mathfrak{G}_p, \mathfrak{G}'_p$ zwei F_p -Ordnungen mit $\mathfrak{D}_p \subset \mathfrak{G}_p \subset \mathfrak{F}_p, \mathfrak{D}'_p \subset \mathfrak{G}'_p \subset \mathfrak{F}'_p$ und $[\mathfrak{F}_p : \mathfrak{G}_p] = [\mathfrak{F}'_p : \mathfrak{G}'_p]$. Dann gilt: Ein Isomorphismus $\mathfrak{D}_p \rightarrow \mathfrak{D}'_p$ lässt sich zu einem Isomorphismus $\mathfrak{G}_p \rightarrow \mathfrak{G}'_p$ fortsetzen.*

Beweis. Ein Isomorphismus $\mathfrak{D}_p \rightarrow \mathfrak{D}'_p$ lässt sich nach Lemma 2.1.(i) zu einem Automorphismus $j : F_p \rightarrow F_p$ fortsetzen. Dann gilt $K'_p \cap j(\mathfrak{F}_p) = K'_p \cap \mathfrak{F}'_p$. Also gibt es ein $X \in K_p'^{\times}$ mit $Xj(\mathfrak{F}_p)X^{-1} = \mathfrak{F}'_p$, siehe [3, Satz 7], und $\mathfrak{D}'_p \subset Xj(\mathfrak{G}_p)X^{-1} \subset \mathfrak{F}'_p$.

Falls K_p Körper ist, folgt mit Satz 4.1, dass $Xj(\mathfrak{G}_p)X^{-1} = \mathfrak{G}'_p$.

Falls K_p zerfällt, gibt es nach Satz 4.2 Matrizeeinheiten in F_p und $r, s, r', s' \in \mathbb{Z}$ mit $r + s = r' + s'$, bezüglich derer gilt: $\mathfrak{D}'_p = \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$, $Xj(\mathfrak{G}_p)X^{-1} = \begin{pmatrix} \mathbb{Z}_p & p^s \mathbb{Z}_p \\ p^r \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ und

$\mathfrak{G}'_p = \begin{pmatrix} \mathbb{Z}_p & p^{s'} \mathbb{Z}_p \\ p^{r'} \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$. Mit $Y := \begin{pmatrix} p^r & 0 \\ 0 & p^{r'} \end{pmatrix} \in K_p'^{\times}$ folgt $YXj(\mathfrak{G}_p)X^{-1}Y^{-1} = \mathfrak{G}'_p$. □

Satz 4.4. *Sei p eine endliche Stelle von \mathbb{Q} , und sei F_p eine \mathbb{Q}_p -Quaternionenalgebra. Sei \mathfrak{F}_p eine F_p -Maximalordnung, und sei $\mathfrak{G}_p \subset \mathfrak{F}_p$ eine F_p -Ordnung mit $[\mathfrak{F}_p : \mathfrak{G}_p] = p$.*

(i) *Falls F_p Divisionsalgebra ist, gilt $\mathfrak{G}_p = \{A \in \mathfrak{F}_p \mid S(A)^2 - 4N(A) \in p\mathbb{Z}_p\}$.*

(ii) *Falls F_p zerfällt, gibt es Matrizeeinheiten in F_p , bezüglich derer $\mathfrak{G}_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$.*

Beweis.

(i) Seien $K_p, K'_p \subset F_p$ quadratische Körpererweiterungen von \mathbb{Q}_p mit den Hauptordnungen $\mathfrak{D}_p, \mathfrak{D}'_p$. Sei p verzweigt in K_p und träge in K'_p . Sei $\Pi \in \mathfrak{D}_p$ Primelement,

und sei $\mathfrak{D}'_p = \mathbb{Z}_p[\Omega]$. Da \mathfrak{F}_p die einzige F_p -Maximalordnung ist, gilt $K_p \cap \mathfrak{F}_p = \mathfrak{D}_p$ und $K'_p \cap \mathfrak{F}_p = \mathfrak{D}'_p$. Wir zeigen zunächst durch Widerspruch, dass $\Pi \in \mathfrak{G}_p$.

Es gibt $\alpha, \beta, \gamma, \beta', \gamma', \gamma'' \in \mathbb{Z}_p$, so dass $\{1, \alpha\Omega + \beta\Omega\Pi + \gamma\Pi, \beta'\Omega\Pi + \gamma'\Pi, \gamma''\Pi\}$ eine \mathbb{Z}_p -Basis von \mathfrak{G}_p ist. Falls $\Pi \notin \mathfrak{G}_p$, können wir wegen $[\mathfrak{F}_p : \mathfrak{G}_p] = p$ annehmen, dass $\alpha = \beta' = 1, \gamma'' = p, \beta = 0$. Und wir können Ω durch $\Omega + \gamma'$ ersetzen, also annehmen, dass $\{1, \Omega + \gamma\Pi, \Omega\Pi, p\Pi\}$ eine \mathbb{Z}_p -Basis von \mathfrak{G}_p ist. Wegen $\Pi^{-1}\mathfrak{F}_p\Pi = \mathfrak{F}_p$ ist $N(\Omega)\Pi = (\Omega + \gamma\Pi)^*\Omega\Pi - \gamma\Pi^*\Omega\Pi = (\Omega + \gamma\Pi)^*\Omega\Pi - \gamma N(\Pi)\Pi^{-1}\Omega\Pi \in \mathfrak{G}_p + p\mathfrak{F}_p$, und deshalb $\Pi \in \mathfrak{G}_p + p\mathfrak{F}_p \subset \mathfrak{G}_p$, Widerspruch.

Nach Satz 4.1.(i) gilt also $\mathfrak{G}_p = \mathfrak{D}_p + \mathfrak{D}_p\Pi\Omega$, und $\{1, \Pi, p\Omega, \Pi\Omega\}$ ist eine \mathbb{Z}_p -Basis von \mathfrak{G}_p . Damit folgt, dass $K_p \cap \mathfrak{G}_p = \mathfrak{D}_p = \{A \in K_p \cap \mathfrak{F}_p \mid (S(A)^2 - 4N(A)) \in p\mathbb{Z}_p\}$ und $K'_p \cap \mathfrak{G}_p = \mathbb{Z}_p + p\mathbb{Z}_p\Omega = \{A \in K'_p \cap \mathfrak{F}_p \mid (S(A)^2 - 4N(A)) \in p\mathbb{Z}_p\}$.

Sei nun $A \in \mathfrak{F}_p$ beliebig. Dann ist A in einer quadratischen Körpererweiterung $K''_p \subset F_p$ von \mathbb{Q}_p enthalten. p ist entweder verzweigt oder träge in K''_p . Wir können o.B.d.A. annehmen, dass $K''_p = K_p$ oder $K''_p = K'_p$, womit die Behauptung folgt.

(ii) siehe [3, Satz 3]

□

Lemma 4.5. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*

Seien F eine \mathbb{Q} -Quaternionenalgebra, \mathfrak{F} eine F -Maximalordnung, M eine Erweiterung von F zur k -Quaternionenalgebra und p eine endliche Stelle von \mathbb{Q} . Sei p in k verzweigt. Dann gibt es genau eine M_p -Maximalordnung \mathfrak{M}_p mit $\mathfrak{F}_p \subset \mathfrak{M}_p$.

Beweis. Angenommen, es gibt M_p -Maximalordnungen $\mathfrak{M}_p \neq \mathfrak{M}'_p$ mit $\mathfrak{F}_p \subset \mathfrak{M}_p \cap \mathfrak{M}'_p$.

Sei $\pi \in \mathfrak{o}_p$ ein Primelement. Die k_p -Algebra M_p zerfällt, siehe etwa Lemma 3.2.(i).

Nach Lemma 2.1.(ii) gibt es ein $r \in \mathbb{N}$ und Matriceseinheiten in M_p , bezüglich derer gilt:

$\mathfrak{M}_p = \begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ und $\mathfrak{M}'_p = \begin{pmatrix} \mathfrak{o}_p & \pi^{-r}\mathfrak{o}_p \\ \pi^r\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$. Sei $K_p \subset F_p$ eine quadratische Körpererweiterung von \mathbb{Q}_p mit Hauptordnung $\mathfrak{D}_p \subset \mathfrak{F}_p$. Sei p träge in K_p , und sei $\mathfrak{D}_p = \mathbb{Z}_p[\Omega]$.

Es ist $\Omega = \begin{pmatrix} \alpha & \beta \\ \pi\gamma & \delta \end{pmatrix}$ mit $\alpha, \beta, \gamma, \delta \in \mathfrak{o}_p$. Für die Diskriminante Δ von Ω gilt dann $\Delta = S(\Omega)^2 - 4N(\Omega) = (\alpha - \delta)^2 + 4\pi\beta\gamma \equiv (\alpha - \delta)^2 \pmod{4\pi}$. Mit dem Newton-Verfahren folgt $\Delta \in \mathfrak{o}_p^{\times(2)}$. Aber $\Delta \notin \mathbb{Z}_p^{\times(2)}$, und, da p in k verzweigt ist, $\Delta \notin \mathfrak{o}_p^{\times(2)}$, Widerspruch. □

Lemma 4.6. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung \mathfrak{o} .*

Seien F eine \mathbb{Q} -Quaternionenalgebra, M eine Erweiterung von F zur k -Quaternionenalgebra und \mathfrak{N} eine M -Maximalordnung. Sei p eine endliche Stelle von \mathbb{Q} mit $p \nmid \Sigma_k(F)$.

(i) *Dann enthält $F_p \cap \mathfrak{N}_p$ eine zu \mathfrak{o}_p isomorphe Ordnung.*

(ii) *Sei \mathfrak{F} eine F -Maximalordnung mit $F \cap \mathfrak{N} \subset \mathfrak{F}$. Dann gibt es eine M -Maximalordnung \mathfrak{M} mit $\mathfrak{F} \subset \mathfrak{M}$, so dass $[\mathfrak{F}_p : (F_p \cap \mathfrak{N}_p)] = [\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)]$.*

Beweis. Sei $\mathfrak{G} = F \cap \mathfrak{N}$, und sei \mathfrak{F} eine F -Maximalordnung mit $\mathfrak{G} \subset \mathfrak{F}$.

• Sei p in k verzweigt oder träge:

k_p ist quadratische Körpererweiterung von \mathbb{Q}_p , und es gilt $M_p \cong M_2(k_p)$, siehe Lemma 3.2.(i). Sei $\mathfrak{o}_p = \mathbb{Z}_p[\omega]$, und sei $\pi \in \mathfrak{o}_p$ ein Primelement. Falls p in k verzweigt ist, sei $\omega = \pi$. Falls p in k träge ist, sei $\pi = p$. Sei vorläufig \mathfrak{M} eine beliebige M -Maximalordnung mit $\mathfrak{F} \subset \mathfrak{M}$. Es gibt ein $r \in \mathbb{N}_0$ und Matrizeseinheiten $U_{11}, U_{12}, U_{21}, U_{22} \in M_p$, bezüglich derer gilt: $\mathfrak{M}_p = \begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ und $\mathfrak{N}_p = \begin{pmatrix} \mathfrak{o}_p & \pi^{-r} \mathfrak{o}_p \\ \pi^r \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$. Die natürliche Einbettung $\mathfrak{F} \hookrightarrow \mathfrak{M}$ induziert eine injektive Abbildung $\mathfrak{F}_p/\mathfrak{G}_p \rightarrow \mathfrak{M}_p/(\mathfrak{M}_p \cap \mathfrak{N}_p)$.

Wir zeigen die Behauptungen zuerst für den Fall, dass $p \nmid \pi^r$. Dann ist

- entweder $r = 0$, also $\mathfrak{M}_p = \mathfrak{N}_p$ und $\mathfrak{G}_p = \mathfrak{F}_p$. Hier ist nichts weiter zu zeigen.
- oder $r = 1$ und p verzweigt in k .

Dann ist $[\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)] = p$, also $\mathfrak{G}_p = \mathfrak{F}_p$ oder $[\mathfrak{F}_p : \mathfrak{G}_p] = p$.

Falls $\mathfrak{G}_p = \mathfrak{F}_p$ gilt, ersetzen wir die p -Komponente \mathfrak{M}_p der vorläufigen Maximalordnung \mathfrak{M} durch \mathfrak{N}_p . Falls $[\mathfrak{F}_p : \mathfrak{G}_p] = p$ gilt, ist \mathfrak{G}_p nach Satz 4.4 bis auf Isomorphie eindeutig bestimmt. Nach Satz 4.1 enthält \mathfrak{G}_p also eine zu \mathfrak{o}_p isomorphe Ordnung.

Wir können nun also davon ausgehen, dass $p \mid \pi^r$ oder gleichwertig $p^2 \leq [\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)]$.

(i) Wir konstruieren (unabhängig von r) ein $U \in \mathfrak{G}_p$, so dass $\mathbb{Z}_p[U]$ isomorph zu \mathfrak{o}_p ist.

F_p und $\begin{pmatrix} k_p & k_p \\ 0 & k_p \end{pmatrix}$ haben als \mathbb{Q}_p -Algebren die Dimensionen 4 und 6. Ihr Durchschnitt hat also eine Dimension ≥ 2 . Daher gibt es $a, b, c \in k_p$ mit $U := \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in F_p \setminus \mathbb{Q}_p$.

Wir zeigen zunächst, dass wir $c = \bar{a}$ annehmen können.

Falls $c \neq \bar{a}$, gilt $c - \bar{a} = S(U) - (a + \bar{a}) \in \mathbb{Q}_p^\times$, und wegen $a(c - \bar{a}) = N(U) - a\bar{a} \in \mathbb{Q}_p$ sind $a, c \in \mathbb{Q}_p$. Wir ersetzen U durch $U - c$, können also $c = 0$ und $a \neq 0$ annehmen. Man rechnet leicht nach, dass $UM_pU^* \subset k_pU_{12}$ und speziell $UU_{12}U^* = a^2U_{12}$. Also gilt $UM_pU^* \neq \{0\}$ und wegen $M_p = F_p + \omega F_p$ auch $UF_pU^* \neq \{0\}$. Sei $X \in F_p$ mit $UXU^* \neq 0$. Wir ersetzen U durch $UXU^* \in F_p$ und erhalten so $c = \bar{a} = 0$.

Wir können also $U = \begin{pmatrix} a & b \\ 0 & \bar{a} \end{pmatrix}$ annehmen, mit $a, b \in \mathfrak{o}_p$, nicht beide durch p teilbar.

Wir zeigen nun, dass wir $a = \omega$ annehmen können.

Es gibt $\alpha \in \mathbb{Z}_p$, $\beta \in \mathbb{Z}_p^\times$ und $s \in \mathbb{N}_0$ mit $a = \alpha$ oder $a = \alpha + \beta p^s \omega$. Sei $t \in \mathbb{N}_0$ maximal mit $p^t \mid (a - \alpha)$ und $p^t \mid b$. Wir ersetzen U durch $(U - \alpha)/(\beta p^t)$. Dann gilt $a = 0$ oder $a = p^s \omega$ mit $s \in \mathbb{N}_0$. Wir zeigen durch Widerspruch, dass $a \neq 0$, $s = 0$.

Andernfalls gilt $p^{-1}U \in \begin{pmatrix} \mathfrak{o}_p & p^{-1}\mathfrak{o}_p \\ 0 & \mathfrak{o}_p \end{pmatrix}$, wegen $p \mid \pi^r$ also $p^{-1}U \in \mathfrak{N}_p$. Daher gilt

$p^{-1}U \in F_p \cap \mathfrak{N}_p = \mathfrak{G}_p$, andererseits gilt wegen $p \nmid b$ aber $p^{-1}U \notin \mathfrak{M}_p$, und deshalb

$p^{-1}U \notin \mathfrak{F}_p$, Widerspruch. Wir können also $U = \begin{pmatrix} \omega & b \\ 0 & \bar{\omega} \end{pmatrix}$ annehmen, mit $b \in \mathfrak{o}_p$.

(ii) Wir zeigen, dass die natürliche Abbildung $\mathfrak{F}_p/\mathfrak{G}_p \rightarrow \mathfrak{M}_p/(\mathfrak{M}_p \cap \mathfrak{N}_p)$ bei geeigneter Wahl von \mathfrak{M}_p surjektiv ist. Dazu genügt es offenbar zu zeigen, dass die Abbildung

$f_{21} : \mathfrak{F}_p \rightarrow \mathfrak{o}_p$ mit der Zuordnungsvorschrift $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \gamma$ surjektiv ist.

- Falls p in k verzweigt ist, sei $K_p \subset F_p$ eine quadratische Körpererweiterung von \mathbb{Q}_p mit Hauptordnung $\mathfrak{D}_p \subset \mathfrak{F}_p$. Sei p träge in K_p , und sei $\mathfrak{D}_p = \mathbb{Z}_p[\Omega]$.

Es ist $\Omega = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ mit $\alpha, \beta, \gamma, \delta \in \mathfrak{o}_p$ und $\Omega U = \begin{pmatrix} \alpha\omega & \alpha b + \beta\bar{\omega} \\ \gamma\omega & \gamma b + \delta\bar{\omega} \end{pmatrix} \in \mathfrak{F}_p$.

Es gilt $\gamma \in \mathfrak{o}_p^\times$, denn sonst wäre $\mathfrak{F}_p \subset \begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ \pi\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$, im Widerspruch zu Lemma 4.5. Also ist $\{\gamma, \gamma\omega\}$ eine \mathbb{Z}_p -Basis von \mathfrak{o}_p , und $f_{21} : \mathfrak{F}_p \rightarrow \mathfrak{o}_p$ ist surjektiv.

- Falls p in k träge ist, sei $K_p \subset F_p$ quadratische Körpererweiterung von \mathbb{Q}_p mit Hauptordnung $\mathfrak{D}_p \subset \mathfrak{F}_p$. Sei p verzweigt in K_p , und sei $\Pi \in \mathfrak{D}_p$ Primelement.

Es ist $\Pi = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ mit $\alpha, \beta, \gamma, \delta \in \mathfrak{o}_p$. Falls $\gamma \in \mathfrak{o}_p^\times$, folgt wie in (i), dass f_{21} surjektiv ist. Wir dürfen also $\gamma = \gamma' p^s$ mit $\gamma' \in \mathfrak{o}_p^\times$, $s \in \mathbb{N}$ annehmen.

Bezüglich der Matriceseinheiten $U_{11}, p^{-s}U_{12}, p^sU_{21}, U_{22} \in M_p$ gilt dann:

$$U = \begin{pmatrix} \omega & p^s b \\ 0 & \bar{\omega} \end{pmatrix}, \Pi = \begin{pmatrix} \alpha & p^s \beta \\ \gamma' & \delta \end{pmatrix} \text{ und } \Pi U = \begin{pmatrix} \alpha\omega & p^s(\alpha b + \beta\bar{\omega}) \\ \gamma'\omega & p^s\gamma' b + \delta\bar{\omega} \end{pmatrix}.$$

Speziell gilt $\mathfrak{F}_p \subset \begin{pmatrix} \mathfrak{o}_p & p^s\mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$. Da \mathfrak{F}_p die Diskriminante \mathbb{Z}_p oder $p^2\mathbb{Z}_p$ hat,

ist $s = 1$ (und F_p Divisionsalgebra), also $\mathfrak{N}_p = \begin{pmatrix} \mathfrak{o}_p & p^{-(r-1)}\mathfrak{o}_p \\ p^{r-1}\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ und

$\mathfrak{M}_p = \begin{pmatrix} \mathfrak{o}_p & p\mathfrak{o}_p \\ p^{-1}\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$. Wir ersetzen die p -Komponente \mathfrak{M}_p der vorläufigen

Maximalordnung \mathfrak{M} durch $\begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$. Wegen $\gamma' \in \mathfrak{o}_p^\times$ ist f_{21} dann surjektiv.

- Sei p in k zerlegt:

Wegen $p \nmid \Sigma_k(F)$ gilt $F_p \cong M_2(\mathbb{Q}_p)$. Sei $p\mathfrak{o} = \mathfrak{p}\bar{\mathfrak{p}}$. Dann gilt $\mathfrak{N}_p \cong \mathfrak{N}_{\mathfrak{p}} \times \mathfrak{N}_{\bar{\mathfrak{p}}}$. Wegen $F_p \cong M_p \cong M_{\bar{\mathfrak{p}}}$ gibt es F_p -Maximalordnungen $\mathfrak{F}'_p, \mathfrak{F}''_p$ mit $\mathfrak{N}_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}}\mathfrak{F}'_p$ und $\mathfrak{N}_{\bar{\mathfrak{p}}} = \mathfrak{o}_{\bar{\mathfrak{p}}}\mathfrak{F}''_p$.

Es gibt ein $r \in \mathbb{N}_0$ und Matriceseinheiten in F_p , bezüglich derer $\mathfrak{F}'_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ und

$\mathfrak{F}''_p = \begin{pmatrix} \mathbb{Z}_p & p^{-r}\mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ gilt. Dann ist $\mathfrak{N}_p \cong \begin{pmatrix} \mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \\ \mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \end{pmatrix} \times \begin{pmatrix} \mathfrak{o}_{\bar{\mathfrak{p}}} & p^{-r}\mathfrak{o}_{\bar{\mathfrak{p}}} \\ p^r\mathfrak{o}_{\bar{\mathfrak{p}}} & \mathfrak{o}_{\bar{\mathfrak{p}}} \end{pmatrix}$. Daraus folgt

$\mathfrak{G}_p = F_p \cap \mathfrak{N}_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$. Also enthält \mathfrak{G}_p die zu \mathfrak{o}_p isomorphe Ordnung $\begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$.

Nach Satz 4.2 gilt $\mathfrak{F}_p = \begin{pmatrix} \mathbb{Z}_p & p^s\mathbb{Z}_p \\ p^{-s}\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ für ein $s \in \mathbb{Z}$. Wegen $\mathfrak{G}_p \subset \mathfrak{F}_p$ gilt $-r \leq s \leq 0$,

und es gilt $[\mathfrak{F}_p : \mathfrak{G}_p] = p^r$. Ist \mathfrak{M} eine M -Maximalordnung mit $\mathfrak{F} \subset \mathfrak{M}$, dann gilt

$\mathfrak{M}_p \cong \begin{pmatrix} \mathfrak{o}_{\mathfrak{p}} & p^s\mathfrak{o}_{\mathfrak{p}} \\ p^{-s}\mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \end{pmatrix} \times \begin{pmatrix} \mathfrak{o}_{\bar{\mathfrak{p}}} & p^s\mathfrak{o}_{\bar{\mathfrak{p}}} \\ p^{-s}\mathfrak{o}_{\bar{\mathfrak{p}}} & \mathfrak{o}_{\bar{\mathfrak{p}}} \end{pmatrix}$, und aus $\mathfrak{M}_p \cap \mathfrak{N}_p \cong \begin{pmatrix} \mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \\ p^{-s}\mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \end{pmatrix} \times \begin{pmatrix} \mathfrak{o}_{\bar{\mathfrak{p}}} & p^s\mathfrak{o}_{\bar{\mathfrak{p}}} \\ p^r\mathfrak{o}_{\bar{\mathfrak{p}}} & \mathfrak{o}_{\bar{\mathfrak{p}}} \end{pmatrix}$

folgt $[\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)] = p^{-s} p^{r+s} = p^r$. □

Lemma 4.7. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung \mathfrak{o} . Seien F eine \mathbb{Q} -Quaternionenalgebra und M eine Erweiterung von F zur k -Quaternionenalgebra, Sei p eine endliche Stelle von \mathbb{Q} , und sei \mathfrak{G}_p eine F_p -Ordnung, die eine zu \mathfrak{o}_p isomorphe Ordnung enthält.*

Dann gilt $p \nmid \Sigma_k(F)$, und es gibt eine M -Maximalordnung \mathfrak{N} mit $\mathfrak{G}_p = F_p \cap \mathfrak{N}_p$.

Beweis.

• Sei p in k verzweigt oder träge:

F_p ist isomorph zur p -Komponente einer \mathbb{Q} -Quaternionenalgebra mit Zerfällungskörper k . Es gibt also ein $\tau \in \mathbb{Z}$ mit den Eigenschaften laut Satz 3.5 und Matrizeseinheiten in M_p ,

bezüglich derer $F_p = \left\{ \begin{pmatrix} a & b \\ \tau \bar{b} & \bar{a} \end{pmatrix} \mid a, b \in k_p \right\}$ gilt. Sei \mathfrak{N}' eine M -Maximalordnung mit

$\mathfrak{N}'_p = \begin{pmatrix} \mathfrak{o}_p & p^2 \mathfrak{o}_p \\ p^{-2} \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$, und sei $\mathfrak{G}' := F \cap \mathfrak{N}'$. Seien \mathfrak{F} eine F -Maximalordnung und \mathfrak{M}' eine

M -Maximalordnung mit $\mathfrak{G}' \subset \mathfrak{F} \subset \mathfrak{M}'$. Man prüft leicht nach, dass \mathfrak{G}'_p die Diskriminante $p^4 \tau^2 D^2 \mathbb{Z}_p$ hat. Also gilt $p^2 \leq [\mathfrak{F}_p : \mathfrak{G}'_p] \leq [\mathfrak{M}'_p : (\mathfrak{M}'_p \cap \mathfrak{N}'_p)]$. Sei $\mathfrak{o}_p = \mathbb{Z}_p[\omega]$, und sei $\pi \in \mathfrak{o}_p$

ein Primelement. Falls p in k verzweigt ist, sei $\omega = \pi$. Falls p in k träge ist, sei $\pi = p$. Wie im Beweis von Lemma 4.6 folgt, dass es $b, \alpha, \beta, \delta \in \mathfrak{o}_p$, $\gamma \in \mathfrak{o}_p^\times$ und Matrizeseinheiten in

M_p gibt, bezüglich derer $\left\{ 1, \begin{pmatrix} \omega & b \\ 0 & \bar{\omega} \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \alpha\omega & \alpha b + \beta\bar{\omega} \\ \gamma\omega & \gamma b + \delta\bar{\omega} \end{pmatrix} \right\}$ eine \mathbb{Z}_p -Basis von \mathfrak{F}_p

ist. Für $r \in \mathbb{N}_0$ sei nun $\mathfrak{N}(r)$ eine M -Maximalordnung mit $\mathfrak{N}(r)_p = \begin{pmatrix} \mathfrak{o}_p & \pi^{-r} \mathfrak{o}_p \\ \pi^r \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$, und

sei $\mathfrak{G}(r)_p := F_p \cap \mathfrak{N}(r)_p$. Dann gilt $[\mathfrak{F}_p : \mathfrak{G}(r)_p] = p^r$ oder $[\mathfrak{F}_p : \mathfrak{G}(r)_p] = p^{2r}$, je nachdem ob p in k verzweigt oder träge ist. Nach Satz 4.1 und Lemma 4.3 ist \mathfrak{G}_p isomorph zu $\mathfrak{G}(r)_p$ für ein $r \in \mathbb{N}_0$. Damit folgt die Behauptung.

• Sei p in k zerlegt:

Sei $p\mathfrak{o} = \mathfrak{p}\bar{\mathfrak{p}}$. Nach Satz 4.2 gibt es ein $r \in \mathbb{N}_0$ und Matrizeseinheiten in F_p , bezüglich

derer $\mathfrak{G}_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^r \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ gilt. Die Gleichung $\mathfrak{G}_p = F_p \cap \mathfrak{N}_p$ folgt unmittelbar, wenn man

diesbezüglich eine M -Maximalordnung \mathfrak{N} mit $\mathfrak{N}_p \cong \begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix} \times \begin{pmatrix} \mathfrak{o}_{\bar{p}} & p^{-r} \mathfrak{o}_{\bar{p}} \\ p^r \mathfrak{o}_{\bar{p}} & \mathfrak{o}_{\bar{p}} \end{pmatrix}$ wählt. □

Lemma 4.8. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Diskriminante D .*

Seien E eine \mathbb{Q} -Quaternionenalgebra und M eine Erweiterung von E zur k -Quaternionenalgebra. Sei $T \in M^\times$ ganz mit $\Phi_E(T) = T^$, $S(T) \in 4\mathbb{Z}$ und $S(T)^2 \neq 4N(T)$. Sei p eine endliche Stelle von \mathbb{Q} , an der E zerfällt, und sei $F(T) := \{A \in M \mid T\Phi_E(A)T^{-1} = A\}$.*

Dann gibt es eine E -Maximalordnung \mathfrak{E} und eine M -Maximalordnung \mathfrak{N} mit $\mathfrak{E} \subset \mathfrak{N}$,

so dass die $F(T)_p$ -Ordnung $F(T)_p \cap \mathfrak{N}_p$ die Diskriminante $D^2 d^2 N(T)^2 \mathbb{Z}_p$ hat.

Beweis. Wegen $\Phi_E(T) = T^*$ gibt es $\sigma, \alpha, \beta, \gamma \in \mathbb{Q}_p$ und Matrizeeinheiten in E_p mit $T = \begin{pmatrix} \sigma + \alpha i\sqrt{d} & \beta i\sqrt{d} \\ \gamma i\sqrt{d} & \sigma - \alpha i\sqrt{d} \end{pmatrix}$. Sei $\tau := (\alpha^2 + \beta\gamma)d = -(S(T)^2 - 4N(T))/4 \in \mathbb{Z}$. Dann gilt $\sigma \in 2\mathbb{Z}$ und $N(T) = \sigma^2 + \tau$. Wegen $\tau \neq 0$ gibt es $a, b \in \mathbb{Q}_p$ mit $j := a^2\beta - 2ab\alpha - b^2\gamma \neq 0$. Sei $J := \begin{pmatrix} a/d & b/d \\ a\alpha + b\gamma & a\beta - b\alpha \end{pmatrix}$. Dann ist $N(J) = j/d$ und $JTJ^{-1} = \begin{pmatrix} \sigma & i\sqrt{d}/d \\ \tau i\sqrt{d} & \sigma \end{pmatrix}$.

Also gibt es Matrizeeinheiten in E_p bezüglich derer $T = \begin{pmatrix} \sigma & i\sqrt{d}/d \\ \tau i\sqrt{d} & \sigma \end{pmatrix}$ gilt.

Diesbezüglich sei $\mathfrak{E}_p := M_2(\mathbb{Z}_p)$ und $\mathfrak{N}_p := M_2(\mathfrak{o}_p)$. Man rechnet elementar nach, dass $\left\{1, U := \begin{pmatrix} 0 & 1 \\ \tau d & 0 \end{pmatrix}, V := \begin{pmatrix} \sigma d & -i\sqrt{d} \\ \tau di\sqrt{d} & -\sigma d \end{pmatrix}, W := UV/d\right\}$ eine \mathbb{Z}_p -Basis einer $F(T)_p$ -Ordnung mit Diskriminante $16\tau^2 d^4 N(T)^2 \mathbb{Z}_p$ ist, und dass $\{1, U, V, W' := (\sigma U + W)/\tau\}$ eine \mathbb{Z}_p -Basis einer $F(T)_p$ -Ordnung $\mathfrak{G}_p \subset \mathfrak{N}_p$ mit Diskriminante $16d^4 N(T)^2 \mathbb{Z}_p$ ist.

Falls $p = 2$ in k verzweigt oder $p \neq 2$ ist, sieht man leicht ein, dass $\mathfrak{G}_p = F(T)_p \cap \mathfrak{N}_p$ gilt. Falls $p = 2$ in k träge oder zerlegt ist, ist $\{1, (U + V)/2, V, (1 + W')/2\}$ eine \mathbb{Z}_p -Basis der $F(T)_p$ -Ordnung $F(T)_p \cap \mathfrak{N}_p$, die in diesem Fall also die Diskriminante $d^4 N(T)^2 \mathbb{Z}_p$ hat. \square

5 Einbettung rationaler Quaternionenordnungen

Definition 5.1. *Ist K ein algebraischer Zahlkörper, Q eine K -Quaternionenalgebra, \mathfrak{R} eine Q -Maximalordnung und $\mathfrak{S} \subset \mathfrak{R}$ eine Q -Ordnung, dann sei $\Lambda(\mathfrak{S}) := [\mathfrak{R} : \mathfrak{S}]$.*

Definition 5.2. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung \mathfrak{o} . Sei F eine \mathbb{Q} -Quaternionenalgebra. Eine F -Ordnung \mathfrak{G} heißt \mathfrak{o} -kompatibel genau dann, wenn für alle Stellen p von \mathbb{Q} mit $p \mid \Lambda(\mathfrak{G})$ gilt: \mathfrak{G}_p enthält eine zu \mathfrak{o}_p isomorphe Ordnung.*

Satz 5.3. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung \mathfrak{o} und Idealgruppe I . Sei F eine \mathbb{Q} -Quaternionenalgebra, und sei \mathfrak{F} eine F -Maximalordnung.*

- (i) *Sei $\mathfrak{G} \subset \mathfrak{F}$ eine \mathfrak{o} -kompatible F -Ordnung. Dann ist $\Lambda(\mathfrak{G})$ teilerfremd zu $\Sigma_k(F)$, und es gilt $\Lambda(\mathfrak{G}) \in N_{k|\mathbb{Q}}(I)$.*
- (ii) *Sei $\lambda \in \mathbb{N}$ teilerfremd zu $\Sigma_k(F)$, und sei $\lambda \in N_{k|\mathbb{Q}}(I)$. Dann gibt es eine \mathfrak{o} -kompatible F -Ordnung $\mathfrak{G} \subset \mathfrak{F}$ mit $\Lambda(\mathfrak{G}) = \lambda$.*
- (iii) *Seien $\mathfrak{G}, \mathfrak{G}'$ zwei \mathfrak{o} -kompatible F -Ordnungen mit $\Lambda(\mathfrak{G}) = \Lambda(\mathfrak{G}')$. Für alle endlichen Stellen p von \mathbb{Q} gilt dann: \mathfrak{G}_p ist isomorph zu \mathfrak{G}'_p .*

Bemerkung: Wir haben die Struktur der \mathfrak{G}_p in den Sätzen 4.1, 4.2 und 4.4 dargelegt.

Beweis. Die Behauptungen (i) und (ii) folgen sofort durch globale Synthese der folgenden lokalen Resultate. Zu deren Beweis sei im Folgenden p stets eine endliche Stelle von \mathbb{Q} .

- (i) Falls $p \mid \Sigma_k(F)$, ist F_p eine Divisionsalgebra und die zerfallende quadratische Erweiterung k_p von \mathbb{Q}_p lässt sich nicht in F_p einbetten. Daher gilt $p \nmid \Lambda(\mathfrak{G})$.
Falls $p \nmid \Sigma_k(F)$, gibt es nach den Sätzen 4.1 und 4.2 ein $r \in \mathbb{N}_0$ mit $[\mathfrak{F}_p : \mathfrak{G}_p] = p^r$, falls p in k verzweigt oder zerlegt ist, und mit $[\mathfrak{F}_p : \mathfrak{G}_p] = p^{2r}$, falls p in k träge ist.
- (ii) Sei λ_p der p -Anteil von λ . Dann gibt es ein $r \in \mathbb{N}_0$ mit $\lambda_p = p^r$ oder mit $\lambda_p = p^{2r}$, je nachdem, ob p in k verzweigt oder zerlegt ist, oder ob p in k träge ist.
Falls $p \nmid \lambda$, sei $\mathfrak{G}_p = \mathfrak{F}_p$.
Falls $p \mid \lambda$, gilt $p \nmid \Sigma_k(F)$, und \mathfrak{F}_p enthält eine zu \mathfrak{o}_p isomorphe Ordnung \mathfrak{D}_p . Nach den Sätzen 4.1 und 4.2 gibt es eine F_p -Ordnung \mathfrak{G}_p mit $\mathfrak{D}_p \subset \mathfrak{G}_p$ und $[\mathfrak{F}_p : \mathfrak{G}_p] = \lambda_p$.
- (iii) Falls $p \mid \Sigma_k(F)$, ist $\mathfrak{G}_p = \mathfrak{G}'_p$ die F_p -Maximalordnung.
Falls $p \nmid \Sigma_k(F)$, gibt es nach Lemma 4.3 einen Isomorphismus $\mathfrak{G}_p \rightarrow \mathfrak{G}'_p$.

□

Lemma 5.4. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*

Sei F eine \mathbb{Q} -Quaternionenalgebra, sei M eine Erweiterung von F zur k -Quaternionenalgebra, und seien $\mathfrak{N}, \mathfrak{N}'$ zwei M -Maximalordnungen. Dann gilt:

- (i) $\Lambda(\mathfrak{N} \cap \mathfrak{N}') = N_{k|\mathbb{Q}}(N(\mathfrak{N}\mathfrak{N}'))^{-1}$.
- (ii) *Sei \mathfrak{M} eine M -Maximalordnung. Dann gilt $\Lambda(\mathfrak{N} \cap \mathfrak{N}')\Lambda(\mathfrak{N} \cap \mathfrak{M})\Lambda(\mathfrak{M} \cap \mathfrak{N}') \in \mathbb{Q}^{\times(2)}$.*
- (iii) *\mathfrak{N} ist genau dann isomorph zu \mathfrak{N}' , wenn es ein $f \in \mathbb{N}$ gibt mit:*
 $f \mid \Sigma_k(F)$ und $\left(\frac{f\Lambda(\mathfrak{N} \cap \mathfrak{N}')}{p}, -d \right) = 1$ für alle Stellen p von \mathbb{Q} .

Beweis.

- (i) Die Behauptung folgt sofort durch globale Synthese der folgenden lokalen Resultate.
Sei \mathfrak{p} eine endliche Stelle von k .
Falls $\mathfrak{p} \mid \Sigma_k(F)$, gilt $\mathfrak{N}_{\mathfrak{p}} = \mathfrak{N}'_{\mathfrak{p}}$, also $[\mathfrak{N}_{\mathfrak{p}} : (\mathfrak{N} \cap \mathfrak{N}')_{\mathfrak{p}}] = 1$ und $N(\mathfrak{N}\mathfrak{N}')_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}}$.
Falls $\mathfrak{p} \nmid \Sigma_k(F)$, gibt es nach Lemma 2.1.(ii) ein $r \in \mathbb{N}_0$ und Matrizeseinheiten in $M_{\mathfrak{p}}$, bezüglich derer gilt: $\mathfrak{N}_{\mathfrak{p}} = \begin{pmatrix} \mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \\ \mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \end{pmatrix}$ und $\mathfrak{N}'_{\mathfrak{p}} = \begin{pmatrix} \mathfrak{o}_{\mathfrak{p}} & \pi^{-r}\mathfrak{o}_{\mathfrak{p}} \\ \pi^r\mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \end{pmatrix}$.
Dann gilt $[\mathfrak{N}_{\mathfrak{p}} : (\mathfrak{N} \cap \mathfrak{N}')_{\mathfrak{p}}] = [\mathfrak{o}_{\mathfrak{p}} : \pi^r\mathfrak{o}_{\mathfrak{p}}] = N_{k|\mathbb{Q}}(\mathfrak{p}^r)$ und $N(\mathfrak{N}\mathfrak{N}')_{\mathfrak{p}} = \pi^{-r}\mathfrak{o}_{\mathfrak{p}} = \mathfrak{p}^{-r}\mathfrak{o}_{\mathfrak{p}}$.
- (ii) $\mathfrak{A} := (\mathfrak{N}\mathfrak{M}\mathfrak{N}'\mathfrak{N})^{-1} = (\mathfrak{N}\mathfrak{M}\mathfrak{M}\mathfrak{N}'\mathfrak{N}')^{-1}$ ist ein zweiseitiges ganzes \mathfrak{N} -Ideal und teilerfremd zu $\Sigma_k(F)$. Daher gibt es ein \mathfrak{o} -Ideal \mathfrak{a} mit $\mathfrak{A} = \mathfrak{N}\mathfrak{a}$, siehe dazu etwa [5, Lemma 6.7.5]. Nach [2, Teil VI, § 4, Satz 3] (Normenmultiplikationssatz) gilt dann $\mathfrak{a}^2 = N(\mathfrak{A}) = N(\mathfrak{N}'\mathfrak{N})^{-1}N(\mathfrak{M}\mathfrak{N}')^{-1}N(\mathfrak{N}\mathfrak{M})^{-1}$.
Nach (i) gilt also $\Lambda(\mathfrak{N}' \cap \mathfrak{N})\Lambda(\mathfrak{M} \cap \mathfrak{N}')\Lambda(\mathfrak{N} \cap \mathfrak{M}) = N_{k|\mathbb{Q}}(\mathfrak{a})^2 \in \mathbb{Q}^{\times(2)}$.
- (iii) Bezeichne R die von den Verzweigungsstellen von M erzeugte \mathfrak{o} -Idealgruppe.
Nach [5, Chapter 6.7] ist \mathfrak{N} genau dann isomorph zu \mathfrak{N}' , wenn $N(\mathfrak{N}\mathfrak{N}') \in RI^{(2)}H$, also wenn es ein o.B.d.A. ganzes $f \in R$ gibt mit $fN(\mathfrak{N}\mathfrak{N}')^{-1} \in I^{(2)}H$.

Nach [1, Kapitel III, § 8, Sätze 6 und 7] gilt $fN(\mathfrak{N}\mathfrak{N}')^{-1} \in I^{(2)}H$ genau dann, wenn $N_{k|\mathbb{Q}}(f)\Lambda(\mathfrak{N} \cap \mathfrak{N}') = N_{k|\mathbb{Q}}(fN(\mathfrak{N}\mathfrak{N}')^{-1}) \in N_{k|\mathbb{Q}}(k^\times)$, nach [1, Kapitel I, § 7, Satz 1] (Minkowski-Hasse) also genau dann, wenn $\left(\frac{N_{k|\mathbb{Q}}(f)\Lambda(\mathfrak{N} \cap \mathfrak{N}'), -d}{p}\right) = 1$ für alle p . Falls \mathfrak{N} isomorph zu \mathfrak{N}' ist, sei f der quadratfreie Anteil von $N_{k|\mathbb{Q}}(f)$. Nach Lemma 3.2.(i) gilt dann $f \mid \Sigma_k(F)$. Falls es umgekehrt ein $f \in \mathbb{N}$ gibt mit $f \mid \Sigma_k(F)$ und $\left(\frac{f\Lambda(\mathfrak{N} \cap \mathfrak{N}'), -d}{p}\right) = 1$ für alle Stellen p von \mathbb{Q} , gibt es ein $f \in R$ mit $f = N_{k|\mathbb{Q}}(f)$.

□

Satz 5.5. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung \mathfrak{o} . Sei F eine \mathbb{Q} -Quaternionenalgebra, und sei M eine Erweiterung von F zur k -Quaternionenalgebra.*

- (i) *Sei \mathfrak{N} eine M -Maximalordnung. Dann ist $F \cap \mathfrak{N}$ eine \mathfrak{o} -kompatible F -Ordnung.*
- (ii) *Sei umgekehrt \mathfrak{G} eine \mathfrak{o} -kompatible F -Ordnung. Dann gibt es eine M -Maximalordnung \mathfrak{N} mit $\mathfrak{G} = F \cap \mathfrak{N}$.*
- (iii) *Sei \mathfrak{N} eine M -Maximalordnung, und sei \mathfrak{F} eine F -Maximalordnung mit $F \cap \mathfrak{N} \subset \mathfrak{F}$. Dann gibt es eine M -Maximalordnung \mathfrak{M} mit $\mathfrak{F} \subset \mathfrak{M}$ und $\Lambda(F \cap \mathfrak{N}) = \Lambda(\mathfrak{M} \cap \mathfrak{N})$.*
- (iv) *Seien $\mathfrak{N}, \mathfrak{N}'$ zwei M -Maximalordnungen. Dann gilt: $\Lambda(F \cap \mathfrak{N})\Lambda(\mathfrak{N} \cap \mathfrak{N}')\Lambda(F \cap \mathfrak{N}') \in \mathbb{Q}^{\times(2)}$.*

Beweis. Sei im Folgenden p stets eine endliche Stelle von \mathbb{Q} .

- (i) Falls $p \mid \Sigma_k(F)$, ist $(F \cap \mathfrak{N})_p$ die F_p -Maximalordnung, also gilt speziell $p \nmid \Lambda(F \cap \mathfrak{N})$. Falls $p \nmid \Sigma_k(F)$, enthält $(F \cap \mathfrak{N})_p$ nach Lemma 4.6.(i) eine zu \mathfrak{o}_p isomorphe Ordnung.
- (ii) Falls $p \mid \Sigma_k(F)$, gilt $p \nmid \Lambda(\mathfrak{G})$, also ist \mathfrak{G}_p die F_p -Maximalordnung, und für jede M -Maximalordnung \mathfrak{N} gilt $\mathfrak{G}_p = (F \cap \mathfrak{N})_p$. Falls $p \nmid \Sigma_k(F)$, sei \mathfrak{N} eine M -Maximalordnung mit $\mathfrak{G}_p = (F \cap \mathfrak{N})_p$, siehe Lemma 4.7. Wir wählen \mathfrak{N} so, dass dies für alle $p \mid \Lambda(\mathfrak{G})$ gilt, und dass $\mathfrak{G}_p \subset \mathfrak{N}_p$ für $p \nmid \Lambda(\mathfrak{G})$.
- (iii) Falls $p \mid \Sigma_k(F)$, ist $(F \cap \mathfrak{N})_p = \mathfrak{F}_p$ die F_p -Maximalordnung, und es gilt $\mathfrak{M}_p = \mathfrak{N}_p$ für jede M -Maximalordnung \mathfrak{M} , also ist $[\mathfrak{F}_p : (F \cap \mathfrak{N})_p] = [\mathfrak{M}_p : (\mathfrak{M} \cap \mathfrak{N})_p] = 1$. Falls $p \nmid \Sigma_k(F)$, gibt es nach Lemma 4.6.(ii) eine M -Maximalordnung \mathfrak{M} mit $\mathfrak{F} \subset \mathfrak{M}$, so dass $[\mathfrak{F}_p : (F \cap \mathfrak{N})_p] = [\mathfrak{M}_p : (\mathfrak{M} \cap \mathfrak{N})_p]$. Wir wählen \mathfrak{M} so, dass dies für alle p mit $p \mid \Lambda(F \cap \mathfrak{N})$ gilt. Für $p \nmid \Lambda(F \cap \mathfrak{N})$ gilt $\mathfrak{F}_p = (F \cap \mathfrak{N})_p$, hier wählen wir $\mathfrak{M}_p = \mathfrak{N}_p$.
- (iv) Seien $\mathfrak{F}, \mathfrak{F}'$ zwei F -Maximalordnungen mit $F \cap \mathfrak{N} \subset \mathfrak{F}$ und $F \cap \mathfrak{N}' \subset \mathfrak{F}'$. Nach (iii) gibt es M -Maximalordnungen $\mathfrak{M}, \mathfrak{M}'$ mit $\mathfrak{F} \subset \mathfrak{M}$ und $\mathfrak{F}' \subset \mathfrak{M}'$ sowie mit $\Lambda(F \cap \mathfrak{N}) = \Lambda(\mathfrak{M} \cap \mathfrak{N})$ und $\Lambda(F \cap \mathfrak{N}') = \Lambda(\mathfrak{M}' \cap \mathfrak{N}')$. Mit Lemma 5.4.(ii) folgt: $\Lambda(\mathfrak{N} \cap \mathfrak{N}')\Lambda(F \cap \mathfrak{N})\Lambda(\mathfrak{M} \cap \mathfrak{N}') \in \mathbb{Q}^{\times(2)}$ und $\Lambda(\mathfrak{M} \cap \mathfrak{N}')\Lambda(\mathfrak{M} \cap \mathfrak{M}')\Lambda(F \cap \mathfrak{N}') \in \mathbb{Q}^{\times(2)}$, und miteinander multipliziert folgt: $\Lambda(F \cap \mathfrak{N})\Lambda(\mathfrak{N} \cap \mathfrak{N}')\Lambda(F \cap \mathfrak{N}')\Lambda(\mathfrak{M} \cap \mathfrak{M}') \in \mathbb{Q}^{\times(2)}$. Es genügt also zu zeigen, dass $\Lambda(\mathfrak{M} \cap \mathfrak{M}') \in \mathbb{Q}^{\times(2)}$. Die Behauptung folgt sofort durch globale Synthese der folgenden lokalen Resultate.

- Falls F an der Stelle p verzweigt ist und p in k zerlegt ist, ist M an den Primteilern von p verzweigt, Lemma 3.2.(i). Daher gilt $\mathfrak{F}_p = \mathfrak{F}'_p$ und $\mathfrak{M}_p = \mathfrak{M}'_p$.
- Falls F an der Stelle p verzweigt ist und p in k verzweigt ist, ist $\mathfrak{F}_p = \mathfrak{F}'_p$ die einzige F_p -Maximalordnung, und nach Lemma 4.5 ist $\mathfrak{M}_p = \mathfrak{M}'_p$.
- Falls p in k träge ist, zerfällt die k_p -Quaternionenalgebra M_p .
Nach Lemma 2.1.(ii) gibt es ein $r \in \mathbb{N}_0$ und Matrizeseinheiten in M_p , bezüglich derer $\mathfrak{M}_p = \begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$, $\mathfrak{M}'_p = \begin{pmatrix} \mathfrak{o}_p & p^{-r}\mathfrak{o}_p \\ p^r\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ und $[\mathfrak{M}_p : (\mathfrak{M} \cap \mathfrak{M}')_p] = p^{2r}$.
- Falls F an der Stelle p zerfällt, gibt es nach Lemma 2.1.(ii) ein $r \in \mathbb{N}_0$ und Matrizeseinheiten in F_p , bezüglich derer $\mathfrak{F}_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$, $\mathfrak{F}'_p = \begin{pmatrix} \mathbb{Z}_p & p^{-r}\mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$.
Also gilt $\mathfrak{M}_p = \begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$, $\mathfrak{M}'_p = \begin{pmatrix} \mathfrak{o}_p & p^{-r}\mathfrak{o}_p \\ p^r\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ und $[\mathfrak{M}_p : (\mathfrak{M} \cap \mathfrak{M}')_p] = p^{2r}$.

□

Satz 5.6. Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.

Seien F, F' isomorphe \mathbb{Q} -Quaternionenalgebren, sei M eine gemeinsame Erweiterung von F und F' zur k -Quaternionenalgebra, und seien $\mathfrak{N}, \mathfrak{N}'$ zwei M -Maximalordnungen.

Dann gibt es ein $f \in \mathbb{N}$ mit $f \mid \Sigma_k(F)$, so dass für alle Stellen p von \mathbb{Q} gilt:

$$\left(\frac{\Lambda(F \cap \mathfrak{N})f\Lambda(\mathfrak{N} \cap \mathfrak{N}')\Lambda(F' \cap \mathfrak{N}'), -d}{p} \right) = 1.$$

Insbesondere gilt: \mathfrak{N} ist isomorph zu \mathfrak{N}' , falls $\Lambda(F \cap \mathfrak{N}) = \Lambda(F' \cap \mathfrak{N}')$.

Beweis. Ein Isomorphismus: $j : F' \rightarrow F$ ist zu einem Automorphismus von M fortsetzbar.

Nach Lemma 5.4.(iii) gibt es ein $f \in \mathbb{N}$ mit $f \mid \Sigma_k(F)$ und $\left(\frac{f\Lambda(j(\mathfrak{N}') \cap \mathfrak{N}'), -d}{p} \right) = 1$

für alle Stellen p von \mathbb{Q} . Mit $\Lambda(F \cap j(\mathfrak{N}')) = \Lambda(F' \cap \mathfrak{N}')$ folgt daraus die Behauptung,

denn nach Lemma 5.4.(ii) gilt: $\Lambda(\mathfrak{N} \cap \mathfrak{N}')\Lambda(\mathfrak{N} \cap j(\mathfrak{N}'))\Lambda(j(\mathfrak{N}') \cap \mathfrak{N}') \in \mathbb{Q}^{\times(2)}$,

und nach Lemma 5.5.(iv) gilt: $\Lambda(F \cap \mathfrak{N})\Lambda(\mathfrak{N} \cap j(\mathfrak{N}'))\Lambda(F \cap j(\mathfrak{N}')) \in \mathbb{Q}^{\times(2)}$.

□

Lemma 5.7. Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.

Sei E eine \mathbb{Q} -Quaternionenalgebra mit $|\Sigma(E)| = \Sigma_k(E)$, sei M eine Erweiterung von E zur k -Quaternionenalgebra, und sei F eine weitere \mathbb{Q} -Quaternionenalgebra mit $F \subset M$.

Dann gibt es ein $e \in \mathbb{N}$ mit $e \mid \Sigma_k(E)$, eine E -Maximalordnung \mathfrak{E} und eine F -Maximalordnung \mathfrak{F} , sowie M -Maximalordnungen \mathfrak{N} und \mathfrak{L} mit $\mathfrak{E} \subset \mathfrak{N}$ und $\mathfrak{F} \subset \mathfrak{L}$, so dass gilt:

$$\left(\frac{\Sigma(F)e\Lambda(\mathfrak{L} \cap \mathfrak{N})\Sigma(E), -d}{p} \right) = \left(\frac{E}{p} \right) \left(\frac{F}{p} \right) \text{ für alle Stellen } p \text{ von } \mathbb{Q}.$$

Beweis. Nach Satz 3.4.(iii) gibt es ein $T \in M^\times$ mit $\Phi_E(T) = T^*$, so dass $F = F(T)$ für $F(T) := \{A \in M \mid T\Phi_E(A)T^{-1} = A\}$. O.B.d.A. sei $N(T) \in \mathbb{Z}$ und $S(T) \in 4\mathbb{Z}$.

- Falls $S(T)^2 = 4N(T)$, gilt $N(T) \in \mathbb{Q}^{\times(2)}$, und nach Satz 3.4.(ii) ist F isomorph zu E . Sei $J \in M^\times$ mit $F = JEJ^{-1}$. Seien \mathfrak{E} eine E -Maximalordnung und \mathfrak{N} eine M -Maximalordnung mit $\mathfrak{E} \subset \mathfrak{N}$. Dann sind $\mathfrak{F} := JEJ^{-1}$ eine F -Maximalordnung und $\mathfrak{L} := J\mathfrak{N}J^{-1}$

eine M -Maximalordnung mit $\mathfrak{F} \subset \mathfrak{L}$. Es gilt $\Sigma(F) = \Sigma(E)$, und nach Lemma 5.4.(iii) gibt es ein $e \in \mathbb{N}$ mit $e \mid \Sigma_k(E)$, so dass $\left(\frac{e\Lambda(\mathfrak{L} \cap \mathfrak{N}), -d}{p}\right) = 1 = \left(\frac{E}{p}\right) \left(\frac{F}{p}\right)$ für alle p .

• Wir können nun also annehmen, dass $S(T)^2 \neq 4N(T)$ gilt. An den Stellen p von \mathbb{Q} mit $p \mid \Sigma_k(E)$ ist $F_p \cap \mathfrak{N}_p$ die F_p -Maximalordnung, hat also die Diskriminante $p^2\mathbb{Z}_p$. Sei $DdN(T) = tg$ mit $t \in \mathbb{Z}$ und $g \in \mathbb{N}$, so dass t teilerfremd zu $\Sigma_k(E)$ ist und alle Primteiler von g auch Teiler von $\Sigma_k(E)$ sind. Nach Voraussetzung und nach Lemma 4.8 gibt es eine E -Maximalordnung \mathfrak{E} und eine M -Maximalordnung \mathfrak{N} mit $\mathfrak{E} \subset \mathfrak{N}$, so dass an allen endlichen Stellen p von \mathbb{Q} mit $p \nmid \Sigma_k(E)$ gilt: Die F_p -Ordnung $F_p \cap \mathfrak{N}_p$ hat die Diskriminante $D^2d^2N(T)^2\mathbb{Z}_p$. (Wir gehen von beliebigen $\mathfrak{E} \subset \mathfrak{N}$ aus und wenden Lemma 4.8 an den Stellen p von \mathbb{Q} an, für die $p \mid t$ gilt oder an denen $F_p \cap \mathfrak{N}_p$ nicht maximal ist.) Dann hat $F \cap \mathfrak{N}$ also die Diskriminante $(DdN(T)\Sigma_k(E)/g)^2\mathbb{Z}$. Andererseits hat $F \cap \mathfrak{N}$ die Diskriminante $(\Sigma(F)\Lambda(F \cap \mathfrak{N}))^2\mathbb{Z}$. Unter Beachtung des Vorzeichens (Satz 3.4.(ii) für $p = \infty$) gilt also $|D|dN(T)\Sigma(E) = g\Sigma(F)\Lambda(F \cap \mathfrak{N})$. Sei nun \mathfrak{F} eine F -Maximalordnung mit $F \cap \mathfrak{N} \subset \mathfrak{F}$. Nach Satz 5.5.(iii) gibt es eine M -Maximalordnung \mathfrak{L} mit $\mathfrak{F} \subset \mathfrak{L}$ und $\Lambda(F \cap \mathfrak{N}) = \Lambda(\mathfrak{L} \cap \mathfrak{N})$. Sei $e \in \mathbb{N}$ der quadratfreie Anteil von g . Die Behauptung folgt dann, weil nach Satz 3.4.(ii) gilt: $\left(\frac{N(T), -d}{p}\right) = \left(\frac{E}{p}\right) \left(\frac{F}{p}\right)$ für alle Stellen p von \mathbb{Q} . \square

Satz 5.8. Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.

Seien F, F' zwei \mathbb{Q} -Quaternionenalgebren, sei M eine gemeinsame Erweiterung von F und F' zur k -Quaternionenalgebra, und seien $\mathfrak{M}, \mathfrak{M}'$ zwei M -Maximalordnungen.

Dann gibt es ein $f \in \mathbb{N}$ mit $f \mid \Sigma_k(F)$, so dass für alle Stellen p von \mathbb{Q} gilt:

$$\left(\frac{\Sigma(F)\Lambda(F \cap \mathfrak{M})f\Lambda(\mathfrak{M} \cap \mathfrak{M}')\Sigma(F')\Lambda(F' \cap \mathfrak{M}'), -d}{p}\right) = \left(\frac{F}{p}\right) \left(\frac{F'}{p}\right).$$

Beweis. Sei \mathfrak{F}' eine F -Maximalordnung mit $F \cap \mathfrak{M} \subset \mathfrak{F}'$. Nach Satz 5.5.(iii) gibt es eine M -Maximalordnung \mathfrak{L}' mit $\mathfrak{F}' \subset \mathfrak{L}'$ und $\Lambda(F \cap \mathfrak{M}) = \Lambda(\mathfrak{L}' \cap \mathfrak{M})$. Nach Lemma 3.2 gibt es eine \mathbb{Q} -Quaternionenalgebra $E \subset M$ mit $|\Sigma(E)| = \Sigma_k(E)$. Seien $e, \mathfrak{E}, \mathfrak{F}, \mathfrak{N}$ und \mathfrak{L} wie in Lemma 5.7. Nach Lemma 5.4.(ii) gilt $\Lambda(\mathfrak{L} \cap \mathfrak{N})\Lambda(\mathfrak{L} \cap \mathfrak{L}')\Lambda(\mathfrak{L}' \cap \mathfrak{M})\Lambda(\mathfrak{M} \cap \mathfrak{N}) \in \mathbb{Q}^{\times(2)}$. Nach Lemma 5.5.(iv) gilt $\Lambda(\mathfrak{L} \cap \mathfrak{L}') = \Lambda(F \cap \mathfrak{L})\Lambda(\mathfrak{L} \cap \mathfrak{L}')\Lambda(F \cap \mathfrak{L}') \in \mathbb{Q}^{\times(2)}$. Mit Lemma 5.7 folgt $\left(\frac{\Sigma(F)e\Lambda(F \cap \mathfrak{M})\Lambda(\mathfrak{M} \cap \mathfrak{N})\Sigma(E), -d}{p}\right) = \left(\frac{E}{p}\right) \left(\frac{F}{p}\right)$ für alle Stellen p von \mathbb{Q} .

Entsprechend gibt es ein $e' \in \mathbb{N}$ mit $e' \mid \Sigma_k(E)$, so dass für alle Stellen p von \mathbb{Q} gilt: $\left(\frac{\Sigma(F')e'\Lambda(F' \cap \mathfrak{M}')\Lambda(\mathfrak{M}' \cap \mathfrak{N})\Sigma(E), -d}{p}\right) = \left(\frac{E}{p}\right) \left(\frac{F'}{p}\right)$.

Nach Lemma 5.4.(ii) gilt $\Lambda(\mathfrak{M} \cap \mathfrak{M}')\Lambda(\mathfrak{M} \cap \mathfrak{N})\Lambda(\mathfrak{N} \cap \mathfrak{M}') \in \mathbb{Q}^{\times(2)}$. Sei f der quadratfreie Anteil von ee' . Die Behauptung folgt dann durch Multiplikation der beiden Gleichungen. \square

Satz 5.9. Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung \mathfrak{o} .

Sei $F \subset M_2(k)$ eine \mathbb{Q} -Quaternionenalgebra, und sei \mathfrak{M} eine $M_2(k)$ -Maximalordnung.

Für alle Stellen p von \mathbb{Q} gilt dann $\left(\frac{\Sigma(F)\Lambda(F \cap \mathfrak{M})\Lambda(\mathfrak{M} \cap M_2(\mathfrak{o})), -d}{p}\right) = \left(\frac{F}{p}\right)$.

Speziell gilt $\left(\frac{\Sigma(F)\Lambda(F \cap M_2(\mathfrak{o})), -d}{p}\right) = \left(\frac{F}{p}\right)$ für alle Stellen p von \mathbb{Q} .

Beweis. Sei $F' = M_2(\mathbb{Q})$, sei $M = M_2(k)$, und sei $\mathfrak{M}' = M_2(\mathfrak{o})$. Wegen $F' \cap \mathfrak{M}' = M_2(\mathbb{Z})$ gilt $\Lambda(F' \cap \mathfrak{M}') = 1$. Außerdem gilt $\Sigma(F') = 1$ und $\left(\frac{F'}{p}\right) = 1$ für alle Stellen p von \mathbb{Q} . Die Voraussetzungen von Satz 5.8 sind gegeben, die Behauptung folgt jetzt unmittelbar. \square

6 Die endlichen Untergruppen der Bianchi-Gruppen

Für eine $M_2(k)$ -Maximalordnung \mathfrak{M} seien $\Gamma(\mathfrak{M}) := \{A \in \mathfrak{M} \mid N(A) = 1\} \subset \mathfrak{M}^\times$ und $PT(\mathfrak{M}) := \Gamma(\mathfrak{M})/\{\pm 1\}$. Speziell ist dann $PT(M_2(\mathfrak{o})) = PSL_2(\mathfrak{o})$ die Bianchi-Gruppe.

Bezeichne $P : SL_2(\mathbb{C}) \rightarrow PSL_2(\mathbb{C})$ die kanonische Projektion.

Für $2 \leq m \in \mathbb{N}$ bezeichne \mathcal{D}_m stets eine (projektive) m -Diedergruppe, und \mathcal{T} bezeichne stets eine (projektive) Tetraedergruppe. Für $\mathcal{D}_m \subset PSL_2(\mathbb{C})$ bzw. $\mathcal{T} \subset PSL_2(\mathbb{C})$ ist dann $P^{-1}(\mathcal{D}_m)$ bzw. $P^{-1}(\mathcal{T})$ eine binäre m -Diedergruppe bzw. binäre Tetraedergruppe. \mathcal{D}_3 , \mathcal{T} bzw. \mathcal{D}_2 sind isomorph zur symmetrischen Gruppe \mathcal{S}_3 , alternierenden Gruppe \mathcal{A}_4 bzw. Kleinschen Vierergruppe \mathcal{V}_4 . Eine Gruppe \mathcal{T} enthält genau einen Normalteiler \mathcal{D}_2 , und umgekehrt ist $\mathcal{D}_2 \subset PSL_2(\mathbb{C})$ Untergruppe genau einer Gruppe $\mathcal{T} \subset PSL_2(\mathbb{C})$.

Wir fassen die bekannten Grundlagen in Lemma 6.1 und Satz 6.2 zusammen.

Lemma 6.1. *Sei $\mathcal{G} \subset PSL_2(\mathbb{C})$ eine 3-Diedergruppe \mathcal{D}_3 , eine Tetraedergruppe \mathcal{T} oder eine 2-Diedergruppe $\mathcal{D}_2 \subset \mathcal{T}$. Dann erzeugen die Elemente von $P^{-1}(\mathcal{G})$ über \mathbb{Q} eine Quaternionenalgebra $F(\mathcal{G})$ und über \mathbb{Z} eine $F(\mathcal{G})$ -Ordnung $\mathfrak{F}(\mathcal{G})$. Im Einzelnen gilt:*

$$(i) \quad \Sigma(F(\mathcal{D}_3)) = -3 \text{ und } \Lambda(\mathfrak{F}(\mathcal{D}_3)) = 1.$$

$$(ii) \quad F(\mathcal{D}_2) = F(\mathcal{T}), \quad \Sigma(F(\mathcal{T})) = -2, \quad \mathfrak{F}(\mathcal{D}_2) \subset \mathfrak{F}(\mathcal{T}), \quad \Lambda(\mathfrak{F}(\mathcal{T})) = 1 \text{ und } \Lambda(\mathfrak{F}(\mathcal{D}_2)) = 2.$$

Beweis.

- (i) $P^{-1}(\mathcal{D}_3)$ wird von zwei Elementen U, V erzeugt, mit $U^3 = -1$ ($U^2 - U + 1 = 0$), $V^2 = -1$, $VUV^{-1} = U^{-1}$, siehe [7, 4.4.7]. U, V erzeugen über \mathbb{Q} eine Quaternionenalgebra $F(\mathcal{D}_3)$ und über \mathbb{Z} eine $F(\mathcal{D}_3)$ -Ordnung $\mathfrak{F}(\mathcal{D}_3)$ mit Diskriminante $9\mathbb{Z}$. Also zerfällt $F(\mathcal{D}_3)$ an allen Stellen $p \neq 3, \infty$ von \mathbb{Q} . Jedes $A \in F(\mathcal{D}_3)$ ist darstellbar als $A = \alpha + \beta U + \gamma V + \delta UV$ mit $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$. Falls $A \neq 0$ ist, ist $N(A) = \alpha^2 + \alpha\beta + \beta^2 + \gamma^2 + \gamma\delta + \delta^2 > 0$. Daher ist $F(\mathcal{D}_3)$ Divisionsalgebra. Die Anzahl der Verzweigungsstellen von $F(\mathcal{D}_3)$ ist gerade. Also ist $F(\mathcal{D}_3)$ genau an den Stellen 3 und ∞ verzweigt, und $\mathfrak{F}(\mathcal{D}_3)$ ist eine $F(\mathcal{D}_3)$ -Maximalordnung.

- (ii) Sei $\mathcal{D}_2 \subset \mathcal{T}$. Dann wird $P^{-1}(\mathcal{D}_2)$ von zwei Elementen U, V erzeugt, mit $U^2 = -1$, $V^2 = -1$, $VUV^{-1} = U^{-1}$, siehe [7, 4.4.7]. $P^{-1}(\mathcal{T})$ wird von U und V sowie von einem Element W erzeugt, mit $W^3 = -1$, $UWU^{-1} = VW$ und $WV = UW$; und eine elementare Rechnung zeigt, dass $W = (1 - U - V - UV)/2$, siehe [7, 4.4.10]. U, V, W erzeugen über \mathbb{Q} eine Quaternionenalgebra $F(\mathcal{T}) = F(\mathcal{D}_2)$ und über \mathbb{Z} eine Ordnung $\mathfrak{F}(\mathcal{T})$ mit Diskriminante $4\mathbb{Z}$. Also zerfällt $F(\mathcal{T})$ an allen Stellen $p \neq 2, \infty$. Jedes $A \in F(\mathcal{T})$ ist darstellbar als $A = \alpha + \beta U + \gamma V + \delta UV$ mit $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$. Falls $A \neq 0$, ist $N(A) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 > 0$. Daher ist $F(\mathcal{T})$ Divisionsalgebra. Die Anzahl der Verzweigungsstellen von $F(\mathcal{T})$ ist gerade. Also ist $F(\mathcal{T})$ genau an den Stellen 2 und ∞ verzweigt, und $\mathfrak{F}(\mathcal{T})$ ist eine $F(\mathcal{T})$ -Maximalordnung. Man rechnet nun leicht nach, dass $\mathfrak{F}(\mathcal{D}_2)$ die Diskriminante $16\mathbb{Z}$ hat, also $[\mathfrak{F}(\mathcal{T}) : \mathfrak{F}(\mathcal{D}_2)] = 2$ gilt.

□

Satz 6.2. Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$. Dann gilt:

- (i) Sei \mathcal{G} eine nichtzyklische endliche Untergruppe von $PSL_2(k)$.
Dann ist \mathcal{G} eine 3-Diedergruppe, Tetraedergruppe oder 2-Diedergruppe.
- (ii) $PSL_2(k)$ enthält genau dann eine 3-Diedergruppe \mathcal{D}_3 , wenn $d \not\equiv 2 \pmod{3}$.
- (iii) $PSL_2(k)$ enthält genau dann eine Tetraedergruppe \mathcal{T} , wenn $d \not\equiv 7 \pmod{8}$.

Bemerkung: $\mathcal{D}_3 \subset PSL_2(k)$ bzw. $\mathcal{T} \subset PSL_2(k)$ ist in $P\Gamma(\mathfrak{M})$ für eine $M_2(k)$ -Maximalordnung \mathfrak{M} enthalten. Nach Satz 5.6 ist der Isomorphietyp von \mathfrak{M} unabhängig von der konkreten Gruppe \mathcal{D}_3 bzw. \mathcal{T} . Die genaue Typisierung von \mathfrak{M} wird von Satz 6.4 geleistet.

Beweis.

- (i) Sei \mathcal{G} eine nichttriviale endliche Untergruppe von $PSL_2(k)$, und sei $\mathcal{U} \subset \mathcal{G}$ eine zyklische Untergruppe der Ordnung $u > 1$. Dann ist $P^{-1}(\mathcal{U})$ zyklisch und hat die Ordnung $2u$. Sei U ein erzeugendes Element von $P^{-1}(\mathcal{U})$, und sei $\zeta \in \mathbb{C}$ eine primitive $2u$ -te Einheitswurzel. Dann ist $S(U) = \zeta + \bar{\zeta} \in \mathfrak{o} \cap \mathbb{R} = \mathbb{Z}$. Daher muss $u = 2$ oder $u = 3$ sein. Nach [7, Chapter 4.4] ist $P^{-1}(\mathcal{G})$ also eine zyklische Gruppe der Ordnung 4 oder 6, oder eine binäre 3-Dieder-, Tetraeder- oder 2-Diedergruppe.
- (ii) Sei $\mathcal{D}_3 \subset PSL_2(\mathbb{C})$. Genau dann enthält $PSL_2(k)$ eine 3-Diedergruppe, wenn es eine Einbettung $\mathcal{D}_3 \hookrightarrow PSL_2(k)$ gibt. Dies ist genau dann der Fall, wenn es eine Einbettung $F(\mathcal{D}_3) \hookrightarrow M_2(k)$ gibt. Nach Lemma 3.2.(ii) trifft dies genau dann zu, wenn $\Sigma_k(F(\mathcal{D}_3)) = \Sigma_k(M_2(\mathbb{Q})) = 1$ gilt, also genau dann, wenn die einzige endliche Verzweigungsstelle 3 von $F(\mathcal{D}_3)$ in k nicht zerlegt ist, also wenn $-d \not\equiv 1 \pmod{3}$.
- (iii) Sei $\mathcal{D}_2 \subset \mathcal{T} \subset PSL_2(\mathbb{C})$. Genau dann enthält $PSL_2(k)$ eine Tetraedergruppe und eine 2-Diedergruppe, wenn es eine Einbettung $\mathcal{D}_2 \subset \mathcal{T} \hookrightarrow PSL_2(k)$ gibt. Wie in (ii) zeigt man, dass dies genau dann zutrifft, wenn die einzige endliche Verzweigungsstelle 2 von $F(\mathcal{T}) = F(\mathcal{D}_2)$ in k nicht zerlegt ist, also wenn $-d \not\equiv 1 \pmod{8}$.

□

Satz 6.3. Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung \mathfrak{o} .
Seien \mathcal{D}_2 eine 2-Diedergruppe und \mathcal{T} eine Tetraedergruppe mit $\mathcal{D}_2 \subset \mathcal{T} \subset PSL_2(k)$.

- (i) Sei \mathfrak{M} eine $M_2(k)$ -Maximalordnung.
Genau dann gilt $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$ und $\mathcal{T} \not\subset P\Gamma(\mathfrak{M})$, wenn $F(\mathcal{D}_2) \cap \mathfrak{M} = \mathfrak{F}(\mathcal{D}_2)$.
- (ii) Genau dann ist $\mathfrak{F}(\mathcal{D}_2)$ eine \mathfrak{o} -kompatible $M_2(k)$ -Ordnung, wenn $d \not\equiv 3 \pmod{4}$.
- (iii) Genau dann gibt es eine $M_2(k)$ -Maximalordnung \mathfrak{M} mit
 $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$ und $\mathcal{T} \not\subset P\Gamma(\mathfrak{M})$, wenn $d \not\equiv 3 \pmod{4}$.
Der Isomorphietyp von \mathfrak{M} ist unabhängig von der konkreten Gruppe \mathcal{D}_2 .

Beweis. Wir kürzen $F := F(\mathcal{T}) = F(\mathcal{D}_2)$ ab.

- (i) Genau dann gilt $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$ und $\mathcal{T} \not\subset P\Gamma(\mathfrak{M})$, wenn $\mathfrak{F}(\mathcal{D}_2) \subset \mathfrak{M}$ und $\mathfrak{F}(\mathcal{T}) \not\subset \mathfrak{M}$.
Wir zeigen die Äquivalenz zu $F \cap \mathfrak{M} = \mathfrak{F}(\mathcal{D}_2)$ durch Widerspruch. Wir nehmen also $\mathfrak{F}(\mathcal{D}_2) \subsetneq F \cap \mathfrak{M}$ an. Wegen $\Lambda(\mathfrak{F}(\mathcal{D}_2)) = 2$ ist dann $F \cap \mathfrak{M}$ eine F -Maximalordnung. Da F an der Stelle 2 verzweigt ist, ist $\mathfrak{F}(\mathcal{T})_2$ die F_2 -Maximalordnung und $\mathfrak{F}(\mathcal{T})$ die einzige F -Maximalordnung, die $\mathfrak{F}(\mathcal{D}_2)$ enthält. Also ist $F \cap \mathfrak{M} = \mathfrak{F}(\mathcal{T})$, Widerspruch.
- (ii) Nach Satz 4.4.(i) gibt es genau eine F_2 -Ordnung $\mathfrak{G}_2 \subset \mathfrak{F}(\mathcal{T})_2$ mit $[\mathfrak{F}(\mathcal{T})_2 : \mathfrak{G}_2] = 2$, also genau eine F -Ordnung $\mathfrak{G} \subset \mathfrak{F}(\mathcal{T})$ mit $\Lambda(\mathfrak{G}) = 2$. Nach Satz 5.3 ist $\mathfrak{F}(\mathcal{D}_2)$ also genau dann eine \mathfrak{o} -kompatible F -Ordnung, wenn $2 \nmid \Sigma_k(F)$ und $2 \in N_{k|\mathbb{Q}}(I)$ gilt, also wenn 2 in k nicht zerlegt und nicht träge ist, also wenn $-d \not\equiv 1 \pmod{4}$ gilt.
- (iii) Die erste Behauptung folgt mit (i), Satz 5.5.(i) und (ii), beziehungsweise umgekehrt mit (ii), Satz 5.5.(ii) und (i). Die zweite Behauptung folgt mit Satz 5.6.

□

Satz 6.4. Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.
Sei \mathfrak{M} eine $M_2(k)$ -Maximalordnung. Dann gilt:

- (i) $P\Gamma(\mathfrak{M})$ enthält genau dann eine 3-Diedergruppe \mathcal{D}_3 ,
wenn für alle Stellen $p \neq 3, \infty$ von \mathbb{Q} gilt: $\left(\frac{-3\Lambda(\mathfrak{M} \cap M_2(\mathfrak{o})), -d}{p} \right) = 1$.
- (ii) $P\Gamma(\mathfrak{M})$ enthält genau dann eine Tetraedergruppe \mathcal{T} ,
wenn für alle Stellen $p \neq 2, \infty$ von \mathbb{Q} gilt: $\left(\frac{-2\Lambda(\mathfrak{M} \cap M_2(\mathfrak{o})), -d}{p} \right) = 1$.
- (iii) $P\Gamma(\mathfrak{M})$ enthält genau dann eine 2-Diedergruppe \mathcal{D}_2 ,
aber nicht die Tetraedergruppe \mathcal{T} mit $\mathcal{D}_2 \subset \mathcal{T} \subset PSL_2(k)$,
wenn für alle Stellen $p \neq 2, \infty$ von \mathbb{Q} gilt: $\left(\frac{-\Lambda(\mathfrak{M} \cap M_2(\mathfrak{o})), -d}{p} \right) = 1$.

Beweis. Wir kürzen $\lambda := \Lambda(\mathfrak{M} \cap M_2(\mathfrak{o}))$ ab.

(i) Sei $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$, oder äquivalent $\mathfrak{F}(\mathcal{D}_3) \subset \mathfrak{M}$, oder äquivalent $\mathfrak{F}(\mathcal{D}_3) = F(\mathcal{D}_3) \cap \mathfrak{M}$.
Nach Satz 5.9 und Lemma 6.1.(i) ist dann $\left(\frac{-3\lambda, -d}{p}\right) = 1$ für alle $p \neq 3, \infty$.

Sei nun umgekehrt $\left(\frac{-3\lambda, -d}{p}\right) = 1$ für alle $p \neq 3, \infty$. Die Anzahl der Stellen p von

\mathbb{Q} mit $\left(\frac{-3\lambda, -d}{p}\right) = -1$ ist gerade. Also gilt $\left(\frac{-3\lambda, -d}{3}\right) = -1$, und speziell gilt

$d \not\equiv 2 \pmod{3}$. Nach Satz 6.2.(ii) gibt es eine 3-Diedergruppe $\mathcal{D}'_3 \subset PSL_2(k)$.

Es gibt eine $M_2(k)$ -Maximalordnung \mathfrak{M}' mit $\mathfrak{F}(\mathcal{D}'_3) \subset \mathfrak{M}'$, oder äquivalent mit

$\mathfrak{F}(\mathcal{D}'_3) = F(\mathcal{D}'_3) \cap \mathfrak{M}'$. Dann gilt $\left(\frac{-3\Lambda(\mathfrak{M}' \cap M_2(\mathfrak{o})), -d}{p}\right) = \left(\frac{-3\lambda, -d}{p}\right)$ für alle

Stellen p . Nach Lemma 5.4.(ii) gilt $\Lambda(\mathfrak{M} \cap \mathfrak{M}') \lambda \Lambda(M_2(\mathfrak{o}) \cap \mathfrak{M}') \in \mathbb{Q}^{\times(2)}$. Nach Lemma 5.4.(iii) ist \mathfrak{M} isomorph zu \mathfrak{M}' , also gibt es eine 3-Diedergruppe $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$.

(ii) folgt mit Lemma 6.1.(ii) und umgekehrt mit Satz 6.2.(iii) wie im Beweis von (i).

(iii) Sei $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$ und $\mathcal{T} \not\subset P\Gamma(\mathfrak{M})$.

Nach Satz 6.3.(i), Satz 5.9 und Lemma 6.1.(ii) ist dann $\left(\frac{-\lambda, -d}{p}\right) = 1$ für $p \neq 2, \infty$.

Sei nun umgekehrt $\left(\frac{-\lambda, -d}{p}\right) = 1$ für alle $p \neq 2, \infty$. Die Anzahl der Stellen p mit

$\left(\frac{-\lambda, -d}{p}\right) = -1$ ist gerade. Also ist $\left(\frac{-\lambda, -d}{2}\right) = -1$ und speziell $d \not\equiv 7 \pmod{8}$.

Falls $d \equiv 3 \pmod{8}$, ist 2 in k träge. Nach Lemma 5.4.(i) gilt $\lambda \in N_{k|\mathbb{Q}}(I)$. Deshalb wäre der quadratfreie Anteil von λ ungerade, Widerspruch. Also ist $d \not\equiv 3 \pmod{4}$.

Nach Satz 6.2.(iii) gibt es eine 2-Diedergruppe \mathcal{D}'_2 und eine Tetraedergruppe \mathcal{T}' mit $\mathcal{D}'_2 \subset \mathcal{T}' \subset PSL_2(k)$. Nach Satz 6.3.(iii) gibt es eine $M_2(k)$ -Maximalordnung \mathfrak{M}' mit

$\mathcal{D}'_2 \subset P\Gamma(\mathfrak{M}')$ und $\mathcal{T}' \not\subset P\Gamma(\mathfrak{M}')$. Dann gilt $\left(\frac{-\Lambda(\mathfrak{M}' \cap M_2(\mathfrak{o})), -d}{p}\right) = \left(\frac{-\lambda, -d}{p}\right)$

für alle Stellen p , und nach den Lemmata 5.4.(ii), 5.4.(iii) ist \mathfrak{M}' isomorph zu \mathfrak{M} . □

Satz 6.5. Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung \mathfrak{o} . Dann gilt:

(i) $PSL_2(\mathfrak{o})$ enthält genau dann eine 3-Diedergruppe \mathcal{D}_3 ,
wenn $p \equiv 1 \pmod{3}$ für alle Primteiler $p \neq 3$ von d .

(ii) $PSL_2(\mathfrak{o})$ enthält genau dann eine Tetraedergruppe \mathcal{T} ,
wenn $p \equiv 1$ oder $p \equiv 3 \pmod{8}$ für alle Primteiler $p \neq 2$ von d .

(iii) $PSL_2(\mathfrak{o})$ enthält genau dann eine 2-Diedergruppe \mathcal{D}_2 ,
aber nicht die Tetraedergruppe \mathcal{T} mit $\mathcal{D}_2 \subset \mathcal{T} \subset PSL_2(k)$,
wenn $p \equiv 1 \pmod{4}$ für alle Primteiler $p \neq 2$ von d .

Beweis.

- (i) Nach Satz 6.4.(i) enthält $PSL_2(\mathfrak{o})$ genau dann eine 3-Diedergruppe \mathcal{D}_3 , wenn für alle Stellen $p \neq 3, \infty$ von \mathbb{Q} gilt: $\left(\frac{-3, -d}{p}\right) = 1$.
Die Behauptung folgt durch Auswertung der Hilbertsymbole.
- (ii) folgt mit Satz 6.4.(ii) wie im Beweis von (i) durch Auswertung der Hilbertsymbole.
- (iii) folgt mit Satz 6.4.(iii) wie im Beweis von (i) durch Auswertung der Hilbertsymbole.

□

Literatur

- [1] Senon I. Borewicz und Igor R. Šafarevič, *Zahlentheorie*, Aus dem Russischen übersetzt von Helmut Koch. Lehrbücher und Monographien aus dem Gebiete der Exakten Wissenschaften, Mathematische Reihe, Band 32, Birkhäuser Verlag, Basel, 1966. MR0195802 (33 #4000)
- [2] Max Deuring, *Algebren.*, Ergebnisse der Math. 4, Nr. 1, VI + 143 S, 1935.
- [3] Martin Eichler, *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. **195** (1955), 127–151 (1956). MR0080767 (18,297c)
- [4] Norbert Krämer, *Die Konjugationsklassenzahlen der endlichen Untergruppen in der Norm-Eins-Gruppe von Maximalordnungen in Quaternionenalgebren*, Diplomarbeit, Mathematisches Institut, Universität Bonn, 1980. <http://tel.archives-ouvertes.fr/tel-00628809/>.
- [5] Colin Maclachlan and Alan W. Reid, *The arithmetic of hyperbolic 3-manifolds*, Graduate texts in mathematics. 219, Springer-Verlag, New York, 2003.
- [6] Alexander D. Rahm, *Accessing the Farrell-Tate cohomology of discrete groups* (preprint, arXiv : 1112.4262, HAL : 00618167, 2012).
- [7] Tonny A. Springer, *Invariant theory*, Lecture Notes in Mathematics, Vol. 585, Springer-Verlag, Berlin, 1977. MR0447428 (56 #5740)

E-Mail: kraemer_norbert@t-online.de