



**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. 2012. hal-00720823v1

**HAL Id: hal-00720823**

**<https://hal.science/hal-00720823v1>**

Preprint submitted on 26 Jul 2012 (v1), 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 Maximalordnungen rationaler Quaternionenalgebren, und die nichtzyklischen endlichen Untergruppen der Bianchi-Gruppen

Norbert Krämer

26. Juli 2012

## Zusammenfassung

Sei  $F$  eine rationale Quaternionenalgebra, und sei  $k$  ein imaginärquadratischer Zerfällungskörper von  $F$ . Erweitert man  $F$  zur  $2 \times 2$ -Matrixalgebra über  $k$ , dann lässt sich jede  $F$ -Maximalordnung in eine Maximalordnung dieser Erweiterung einbetten. Wir zeigen, dass alle einbettenden Maximalordnungen isomorph zueinander sind, und dass und wie ihr Isomorphietyp (in Relation zur  $2 \times 2$ -Matrixalgebra über der Hauptordnung von  $k$ ) nur vom Verzweigungsverhalten von  $F$  abhängt (Satz 6.2). Damit können wir ermitteln, ob die Bianchi-Gruppe über der Hauptordnung von  $k$  3-Dieder-, Tetraeder- oder maximalendliche 2-Diedergruppen enthält (Satz 7.1).

## Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>2</b>
<b>2</b>	<b>Bezeichnungen</b>	<b>3</b>
<b>3</b>	<b>Grundlagen</b>	<b>4</b>
<b>4</b>	<b>Spezielle Einbettung rationaler Quaternionenalgebren</b>	<b>7</b>
<b>5</b>	<b>Spezielle Einbettung von Maximalordnungen</b>	<b>8</b>
<b>6</b>	<b>Typisierung der einbettenden Maximalordnungen</b>	<b>11</b>
<b>7</b>	<b>Die endlichen Untergruppen der Bianchi-Gruppen</b>	<b>13</b>

---

*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  $\mathfrak{o}$  die Hauptordnung des imaginärquadratischen Zahlkörpers  $k = \mathbb{Q}(i\sqrt{d})$ . Sei  $F$  eine  $\mathbb{Q}$ -Quaternionenalgebra mit Zerfällungskörper  $k$ . Wir untersuchen die Einbettungen  $F \hookrightarrow M_2(k)$  und klären, welche  $M_2(k)$ -Maximalordnungen  $\mathfrak{M}$  dabei als Erweiterung einer  $F$ -Maximalordnung auftreten können: Der Isomorphietyp von  $\mathfrak{M}$  in Relation zu  $M_2(\mathfrak{o})$  hängt nur vom Verzweigungsverhalten von  $F$  ab.

Unser Hauptergebnis ist der nachstehende Satz 6.2. Darin verwenden wir die folgenden Notationen: Für eine Stelle  $p$  von  $\mathbb{Q}$  und  $a, b \in \mathbb{Q}^\times$  bezeichne  $\left(\frac{a, b}{p}\right)$  das Hilbert-Symbol.

Sei  $\left(\frac{F}{p}\right) := +1$  oder  $-1$ , je nachdem, ob  $F$  an der Stelle  $p$  zerlegt oder verzweigt ist.

Sei  $v(F)$  das Produkt der endlichen Verzweigungsstellen von  $F$ , multipliziert mit  $-1$ , falls  $F$  an der Stelle  $\infty$  verzweigt ist.

Schließlich sei  $n(\mathfrak{M}) := N_{k|\mathbb{Q}}(N(\mathfrak{M}M_2(\mathfrak{o})))^{-1}$ . Hierbei ist  $N(\mathfrak{M}M_2(\mathfrak{o}))$  die Norm des Ideals  $\mathfrak{M}M_2(\mathfrak{o})$  und  $N_{k|\mathbb{Q}}(N(\mathfrak{M}M_2(\mathfrak{o})))$  die Absolutnorm des  $\mathfrak{o}$ -Ideals  $N(\mathfrak{M}M_2(\mathfrak{o}))$ .

**Satz 6.2.** *Sei  $d \in \mathbb{N}$  quadratfrei, und sei  $k = \mathbb{Q}(i\sqrt{d})$ . Sei  $F$  eine  $\mathbb{Q}$ -Quaternionenalgebra. Sei  $\mathfrak{F}$  eine  $F$ -Maximalordnung, und sei  $\mathfrak{M}$  eine  $M_2(k)$ -Maximalordnung.*

*Genau dann gibt es eine Einbettung  $f : F \hookrightarrow M_2(k)$  mit  $f(\mathfrak{F}) \subset \mathfrak{M}$ ,*

*wenn  $\left(\frac{v(F)n(\mathfrak{M}), -d}{p}\right) = \left(\frac{F}{p}\right)$  für alle Stellen  $p$  von  $\mathbb{Q}$ .*

Bemerkung: Der Isomorphietyp von  $\mathfrak{M}$  in Relation zu  $M_2(\mathfrak{o})$  wird bekanntlich durch die Gesamtheit der Hilbertsymbole  $\left(\frac{n(\mathfrak{M}), -d}{p}\right)$  charakterisiert (Lemmata 3.3 und 3.4).

Zum Beweis von Satz 6.2 konstruieren wir zuerst spezielle Einbettungen von  $F$  und  $\mathfrak{F}$  (Sätze 4.1 und 5.2). Die generelle Aussage folgt durch Vergleich mit diesen Einbettungen.

Als Anwendung von Satz 6.2 können wir dann klären, welche nichtzyklischen endlichen Untergruppen die Bianchi-Gruppe  $PSL_2(\mathfrak{o}) = SL_2(\mathfrak{o})/\{\pm 1\}$  enthält:

**Satz 7.1.** *Sei  $d \in \mathbb{N}$  quadratfrei, und sei  $k = \mathbb{Q}(i\sqrt{d})$  mit Hauptordnung  $\mathfrak{o}$ .*

(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  $d$ .*

Es ist bekannt, welche endlichen Untergruppen die Gruppe  $PSL_2(k)$  enthält, und dass es bis auf Isomorphie jeweils höchstens eine  $M_2(k)$ -Maximalordnung gibt, deren projektive Norm-Eins-Gruppe Untergruppen vom Isomorphietyp  $\mathcal{D}_3$ ,  $\mathcal{T}$  oder (maximalendlich)  $\mathcal{D}_2$  enthält (Lemma 3.5 und [5, Sätze 20.39, 20.41, 26.12 und 26.14]).

Aber die Frage, ob die Bianchi-Gruppe  $PSL_2(\mathfrak{o})$  Untergruppen vom Isomorphietyp  $\mathcal{D}_3$ ,  $\mathcal{T}$  oder (maximalendlich)  $\mathcal{D}_2$  enthält, wurde in [5] nur für spezielle  $d$  beantwortet.

Unter Verwendung der Ergebnisse von [5] 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 beweisen Satz 7.1 durch Zurückführung auf Satz 6.2:

Enthält  $PSL_2(k)$  eine Untergruppe vom Isomorphietyp  $\mathcal{D}_3$  oder  $\mathcal{T}$ , dann erzeugt deren Urbild in  $SL_2(k)$  über  $\mathbb{Q}$  eine Quaternionenalgebra  $F \subset M_2(k)$  und über  $\mathbb{Z}$  eine  $F$ -Maximalordnung  $\mathfrak{F}$ , die sich natürlich in eine  $M_2(k)$ -Maximalordnung  $\mathfrak{M}$  einbetten lässt. Daher führt die Frage  $\mathcal{D}_3 \subset PSL_2(\mathfrak{o})$  bzw.  $\mathcal{T} \subset PSL_2(\mathfrak{o})$  zurück auf die Frage nach dem Isomorphietyp von  $\mathfrak{M}$ , die wir als Spezialfall von Satz 6.2 beantworten können.

Die vom Urbild einer Gruppe  $\mathcal{D}_2 \subset PSL_2(k)$  erzeugte  $F$ -Ordnung ist nicht maximal. Wir nehmen zum Beweis von 7.1.(iii) daher [5, Satz 26.12] zu Hilfe. Dort werden u. a. die Einbettungen von Tetraeder- und 2-Diedergruppen zueinander in Beziehung gesetzt.

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

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. Wenn  $R$  kommutativ ist, dann sei  $M_2(R)$  die  $R$ -Algebra der  $2 \times 2$ -Matrizen mit Koeffizienten aus  $R$ .

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,  $k = \mathbb{Q}(i\sqrt{d}) \subset \mathbb{C}$  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  $H$  die Untergruppe der Hauptideale. Für  $\mathfrak{a} \in I$  sei  $N_{k|\mathbb{Q}}(\mathfrak{a}) \in \mathbb{Q}^+$  die Absolutnorm bezüglich  $k/\mathbb{Q}$ . 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  $p \in \mathbb{N}$  Primzahl, dann ist  $k$  auf natürliche Weise eingebettet in die halbeinfache

quadratische Erweiterung  $k_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} k$  von  $\mathbb{Q}_p$ , mit 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  $\mathfrak{o}$  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  $\mathbb{Q}$  bzw.  $k$  ist  $\mathbb{Q}_{\infty} = \mathbb{R}$  bzw.  $k_{\infty} = \mathbb{C}$ .

Für eine  $\mathbb{Q}$ -Quaternionenalgebra  $F$  sei  $F_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} F$ . Auf natürliche Weise sei  $F$  eingebettet in  $F_p$ . Sei  $\mathbb{Q}$  mit dem Zentrum von  $F$  und  $\mathbb{Q}_p$  mit dem Zentrum von  $F_p$  identifiziert. Für eine Stelle  $\mathfrak{p}$  von  $k$  sei analog  $k \subset M_2(k) \subset M_2(k)_{\mathfrak{p}} = M_2(k_{\mathfrak{p}})$  und  $k_{\mathfrak{p}} \subset M_2(k_{\mathfrak{p}})$ . Betrachte  $p \in \mathbb{N}$ : Für einen  $\mathbb{Z}$ -Modul  $\mathfrak{F} \subset F$  ist dann  $\mathfrak{F}_p = \mathbb{Z}_p \mathfrak{F}$  die lokale Komponente. Für eine endliche Stelle  $\mathfrak{p}$  von  $k$  und einen  $\mathfrak{o}$ -Modul  $\mathfrak{M} \subset M_2(k)$  ist analog  $\mathfrak{M}_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}} \mathfrak{M}$ .

Für ein Element  $M$  einer Quaternionenalgebra  $Q$  bezeichne  $M^*$  das konjugierte Element.  $N(M) = MM^*$  und  $S(M) = M + M^*$  sind dann die Norm und die Spur von  $M$ . In  $Q$  bzw. einer  $Q$ -Maximalordnung  $\mathfrak{M}$  sei  $\Gamma(Q)$  bzw.  $\Gamma(\mathfrak{M})$  die Norm-Eins-Gruppe, und sei  $P\Gamma(Q) = \Gamma(Q)/\{\pm 1\}$  bzw.  $P\Gamma(\mathfrak{M}) = \Gamma(\mathfrak{M})/\{\pm 1\}$  die projektive Norm-Eins-Gruppe. Speziell ist dann  $PSL_2(\mathfrak{o}) = P\Gamma(M_2(\mathfrak{o}))$  die Bianchi-Gruppe.

Ist  $K$  ein algebraischer oder  $\mathfrak{p}$ -adischer Zahlkörper, dann heißen (in dieser Reihenfolge)  $M_{11}, M_{12}, M_{21}, M_{22} \in M_2(K) \setminus \{0\}$  Matrizeseinheiten, wenn für alle  $r, s \in \{1, 2\}$  gilt:  $M_{r1}M_{1s} = M_{r2}M_{2s} = M_{rs}$  und  $M_{r1}M_{2s} = M_{r2}M_{1s} = 0$ . Dann ist  $\{M_{11}, M_{12}, M_{21}, M_{22}\}$  eine Basis von  $M_2(K)$ , und  $\alpha M_{11} + \beta M_{12} + \gamma M_{21} + \delta M_{22}$  mit  $\alpha, \beta, \gamma, \delta \in K$  hat bezüglich der Matrizeseinheiten die Darstellung  $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ , mit den bekannten Matrix-Rechenregeln.

Ist  $p \neq 2$  Primzahl und  $a \in \mathbb{Z}$  teilerfremd zu  $p$ , dann sei  $\left(\frac{a}{p}\right)$  das Legendre-Symbol.

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

Für  $m \in \mathbb{N}$  sei  $\mathcal{D}_m$  stets eine  $m$ -Diedergruppe.  $\mathcal{T}$  bezeichne stets eine Tetraedergruppe.  $\mathcal{D}_3$  und  $\mathcal{T}$  sind isomorph zur symmetrischen Gruppe  $\mathcal{S}_3$  bzw. alternierenden Gruppe  $\mathcal{A}_4$ .  $\mathcal{D}_2$  ist Normalteiler in  $\mathcal{T}$  und isomorph zur Kleinschen Vierergruppe  $\mathcal{V}_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

### 3 Grundlagen

**Lemma 3.1.** *Sei  $K$  algebraischer oder  $\mathfrak{p}$ -adischer Zahlkörper.*

*Sei  $Q$  eine  $K$ -Quaternionenalgebra.*

a) *Seien  $A, B \in Q$  mit  $N(A) = N(B)$ ,  $S(A) = S(B)$  und  $S(A)^2 \neq 4N(A)$ .*

*Dann gibt es einen Automorphismus  $j$  von  $Q$  mit  $j(A) = B$ .*

b) *Sei  $j$  ein Automorphismus von  $Q$ .*

*Dann gibt es  $J \in Q^{\times}$  mit  $j(q) = JqJ^{-1}$  für alle  $q \in Q$ .*

c) *Sei  $L$  ein quadratischer Erweiterungskörper von  $K$ .*

*Genau dann ist  $L$  Zerfällungskörper von  $Q$ , wenn es eine Einbettung  $e : L \hookrightarrow Q$  gibt.*

*Beweis.*

- a) Falls  $K[A]$  Körper ist, siehe [2, Teil IV, § 4, Satz 3].  
 Sei also  $K[A]$  kein Körper. Dann zerfällt  $Q$ , lässt sich also als Matrixalgebra  $M_2(K)$  darstellen, und das charakteristische Polynom von  $A$  hat in  $K$  zwei Nullstellen  $a \neq b$ .  
 Nun folgt leicht, dass es  $X, Y \in Q^\times$  gibt mit  $XAX^{-1} = YBY^{-1} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ .  
 Mit  $j(q) := Y^{-1}XqX^{-1}Y$  für  $q \in Q$  folgt die Behauptung.
- b) Siehe [2, Teil IV, § 4, Satz 5].
- c) Siehe [2, Teil IV, § 4, Sätze 13 und 17].

□

**Lemma 3.2.** *Sei  $K$  ein  $\mathfrak{p}$ -adischer Zahlkörper mit Hauptordnung  $\mathfrak{D}$ , und sei  $\pi \in \mathfrak{D}$  ein Primelement. Seien  $\mathfrak{M}$  und  $\mathfrak{M}'$  zwei  $M_2(K)$ -Maximalordnungen.*

- a) *Dann gibt es Matrizeeinheiten in  $M_2(K)$ , bezüglich derer  $\mathfrak{M}$  und  $\mathfrak{M}'$  die Darstellungen  $\begin{pmatrix} \mathfrak{D} & \mathfrak{D} \\ \mathfrak{D} & \mathfrak{D} \end{pmatrix}$  und  $\begin{pmatrix} \mathfrak{D} & \pi^{-r}\mathfrak{D} \\ \pi^r\mathfrak{D} & \mathfrak{D} \end{pmatrix}$  haben, mit  $r \in \mathbb{N}_0$ .*
- b) *Sei  $M\mathfrak{M}'M^{-1} \subset \mathfrak{M}$  für ein  $M \in \mathfrak{M}$ ,  $M \notin \pi\mathfrak{M}$ .  
 Dann ist  $N(\mathfrak{M}'\mathfrak{M}) = N(M)^{-1}\mathfrak{D}$ .*

*Beweis.*

- a) Siehe [4, Seite 135, im Beweis von Satz 7].
- b) Da  $M\mathfrak{M}'M^{-1}$  eine  $M_2(K)$ -Maximalordnung ist, gilt  $M\mathfrak{M}'M^{-1} = \mathfrak{M}$ .  
 Bezüglich der Matrizeeinheiten in a) sei  $M' = \begin{pmatrix} \pi^r & 0 \\ 0 & 1 \end{pmatrix}$ . Dann ist  $M'\mathfrak{M}'M'^{-1} = \mathfrak{M}$  und  $N(\mathfrak{M}'\mathfrak{M}) = \pi^{-r}\mathfrak{D} = N(M')^{-1}\mathfrak{D}$ . Also ist  $MM'M'^{-1}\mathfrak{M} = \mathfrak{M}MM'^{-1}$  ein zweiseitiges  $\mathfrak{M}$ -Ideal. Mit [2, Teil VI, § 11, Satz 13] folgt  $M = \pi^s M'E$  für ein  $s \in \mathbb{Z}$  und  $E \in \mathfrak{M}^\times$ .  
 Wegen  $M, M' \in \mathfrak{M}$  und  $M, M' \notin \pi\mathfrak{M}$  ist  $s = 0$ . Also gilt  $N(M)^{-1}\mathfrak{D} = N(M')^{-1}\mathfrak{D}$ .

□

**Lemma 3.3.** *Sei  $d \in \mathbb{N}$  quadratfrei, und sei  $k = \mathbb{Q}(i\sqrt{d})$  mit Hauptordnung  $\mathfrak{o}$ , Idealgruppe  $I$  und Hauptidealgruppe  $H$ . Seien  $\mathfrak{M}$  und  $\mathfrak{M}'$  zwei  $M_2(k)$ -Maximalordnungen.*

- a) *Dann gilt stets  $N(\mathfrak{M}\mathfrak{M}')N(\mathfrak{M}M_2(\mathfrak{o}))N(\mathfrak{M}'M_2(\mathfrak{o})) \in I^{(2)}$ .*
- b) *Genau dann sind  $\mathfrak{M}$  und  $\mathfrak{M}'$  isomorph, wenn  $N(\mathfrak{M}\mathfrak{M}') \in I^{(2)}H$ .*

Bemerkung: Lemma 3.3 ist Spezialfall eines allgemeinen Satzes, siehe etwa [5, Satz 10.9].

*Beweis.* Ist  $\mathfrak{a} \in I$ , dann ist  $\mathfrak{M}\mathfrak{a}$  ein zweiseitiges  $\mathfrak{M}$ -Ideal und  $N(\mathfrak{M}\mathfrak{a}) = \mathfrak{a}^2$ . Ist umgekehrt  $\mathfrak{A}$  ein zweiseitiges  $\mathfrak{M}$ -Ideal, dann ist  $\mathfrak{A} = \mathfrak{M}\mathfrak{a}$  mit  $\mathfrak{a} \in I$ , siehe [2, Teil VI, § 11, Satz 13].

- a)  $\mathfrak{A} = \mathfrak{M}\mathfrak{M}'M_2(\mathfrak{o})(\mathfrak{M}M_2(\mathfrak{o}))^{-1}$  ist ein zweiseitiges  $\mathfrak{M}$ -Ideal.  
 Nach [2, Teil VI, § 4, Satz 3 (Normenmultiplikationssatz)] gilt:  
 $N(\mathfrak{M}\mathfrak{M}')N(\mathfrak{M}'M_2(\mathfrak{o})) = N(\mathfrak{M}\mathfrak{M}'M_2(\mathfrak{o})) = N(\mathfrak{A})N(\mathfrak{M}M_2(\mathfrak{o}))$ , also  
 $N(\mathfrak{M}\mathfrak{M}')N(\mathfrak{M}M_2(\mathfrak{o}))N(\mathfrak{M}'M_2(\mathfrak{o})) = N(\mathfrak{A})N(\mathfrak{M}M_2(\mathfrak{o}))^2 \in I^{(2)}$ .
- b) Falls  $\mathfrak{M}$  und  $\mathfrak{M}'$  isomorph sind, gibt es ein  $M \in GL_2(k)$  mit  $\mathfrak{M} = M\mathfrak{M}'M^{-1}$ .  
 Dann ist  $\mathfrak{M}M = M\mathfrak{M}'$ , und  $\mathfrak{A} = (\mathfrak{M}\mathfrak{M}')^{-1}M\mathfrak{M}'$  ist ein zweiseitiges  $\mathfrak{M}'$ -Ideal.  
 Also ist dann  $N(\mathfrak{M}\mathfrak{M}') = N(M\mathfrak{M}')N(\mathfrak{A})^{-1} \in I^{(2)}H$ .  
 Falls umgekehrt  $N(\mathfrak{M}\mathfrak{M}') \in I^{(2)}H$ , gibt es ein zweiseitiges  $\mathfrak{M}$ -Ideal  $\mathfrak{A}$  mit  
 $N(\mathfrak{A}\mathfrak{M}\mathfrak{M}') = N(\mathfrak{A})N(\mathfrak{M}\mathfrak{M}') \in H$ . Nach [3, Satz 1] gibt es ein  $M \in GL_2(k)$  mit  
 $\mathfrak{A}\mathfrak{M}\mathfrak{M}' = \mathfrak{M}M$ . Die Rechtsordnung dieses Ideals ist  $\mathfrak{M}' = M^{-1}\mathfrak{M}M$ .

□

**Lemma 3.4.** Sei  $d \in \mathbb{N}$  quadratfrei, und sei  $k = \mathbb{Q}(i\sqrt{d})$  mit Hauptordnung  $\mathfrak{o}$ , Idealgruppe  $I$  und Hauptidealgruppe  $H$ . Sei  $\mathfrak{a} \in I$ . Dann sind die folgenden Aussagen äquivalent:

- (i)  $\mathfrak{a} \in I^{(2)}H$ .
- (ii) Es gibt  $a \in k^\times$  mit  $N_{k|\mathbb{Q}}(\mathfrak{a}) = N_{k|\mathbb{Q}}(a)$ .
- (iii)  $\left( \frac{N_{k|\mathbb{Q}}(\mathfrak{a}), -d}{p} \right) = 1$  für alle Stellen  $p$  von  $\mathbb{Q}$ .

*Beweis.*

- (i)  $\Leftrightarrow$  (ii): Siehe [1, Kapitel III, § 8, Sätze 6 und 7].
- (ii)  $\Leftrightarrow$  (iii): Siehe [1, Kapitel I, § 7, Satz 1 (Minkowski-Hasse)].

□

Für Rechenregeln zum Hilbert-Symbol siehe [1, Kapitel I, § 5, Formeln (9)-(13), Satz 7].

**Lemma 3.5.** Sei  $d \in \mathbb{N}$  quadratfrei, und sei  $k = \mathbb{Q}(i\sqrt{d})$ .  
 Jede endliche nichttriviale Untergruppe von  $PSL_2(k)$  ist vom Isomorphietyp  
 $\mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/3\mathbb{Z}$ ,  $\mathcal{D}_3$  (3-Diedergruppe),  $\mathcal{T}$  (Tetraedergruppe) oder  $\mathcal{D}_2$  (2-Diedergruppe).

*Beweis.* Sei  $G \subset SL_2(k)$  Urbild einer endlichen, nichttrivialen Untergruppe von  $PSL_2(k)$ .  
 Das Urbild  $M \in G$  eines Elements der Ordnung  $m > 1$  hat die Ordnung  $2m$ . Ist  $\zeta \in \mathbb{C}$   
 eine primitive  $2m$ -te Einheitswurzel, dann ist  $S(M) = \zeta + \bar{\zeta} \in \mathfrak{o} \cap \mathbb{R} = \mathbb{Z}$ . Daher muss  
 $m = 2$  oder  $m = 3$  sein. Gemäß [7, Chapter 4.4] ist  $G$  also eine zyklische Gruppe der  
 Ordnung 4 oder 6, oder eine binäre 3-Dieder-, Tetraeder- oder 2-Diedergruppe.

□

## 4 Spezielle Einbettung rationaler Quaternionenalgebren

**Satz 4.1.** Sei  $d \in \mathbb{N}$  quadratfrei, und sei  $k = \mathbb{Q}(i\sqrt{d})$  mit Hauptordnung  $\mathfrak{o}$  und Diskriminante  $D$ . Sei  $F$  eine  $\mathbb{Q}$ -Quaternionenalgebra mit Zerfällungskörper  $k$ .

a) Es gibt  $t \in \mathbb{Q}^\times$ , so dass  $F$  isomorph ist zur  $\mathbb{Q}$ -Algebra  $F(t) := \left\{ \begin{pmatrix} a & b \\ t\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in k \right\}$  mit Basis  $\left\{ 1, U := \begin{pmatrix} i\sqrt{d} & 0 \\ 0 & -i\sqrt{d} \end{pmatrix}, V(t) := \begin{pmatrix} 0 & 1 \\ t & 0 \end{pmatrix}, W(t) := \begin{pmatrix} 0 & i\sqrt{d} \\ -ti\sqrt{d} & 0 \end{pmatrix} \right\}$ .

b)  $F$  und  $F(t)$  sind genau an den Stellen  $p$  von  $\mathbb{Q}$  verzweigt, wo  $\left(\frac{t, -d}{p}\right) = -1$  ist.

c) Man kann o.B.d.A. annehmen, dass  $t \in \mathbb{Z}$  und quadratfrei ist, dass  $t$  teilerfremd zu  $D$  ist, und dass  $t \equiv 1 \pmod{4}$ , falls  $2 \mid d$ .

d)  $F(t) \cap M_2(\mathfrak{o}) = \left\{ \begin{pmatrix} a & b \\ t\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathfrak{o} \right\}$  ist eine  $F(t)$ -Ordnung mit Diskriminante  $t^2 D^2 \mathbb{Z}$ .

*Beweis.* Aus  $U^2 = -d$ ,  $V(t)^2 = t$  und  $W(t) = UV(t) = -V(t)U$  folgt zunächst leicht, dass  $F(t)$  eine  $\mathbb{Q}$ -Quaternionenalgebra ist, falls  $t \in \mathbb{Q}^\times$ .

a) Da  $k$  Zerfällungskörper von  $F$  ist, kann man  $F$  in  $M_2(k)$  und nach Lemma 3.1.c) auch  $k$  in  $F$  (als  $\mathbb{Q}$ -Algebren) einbetten. Nach Lemma 3.1.a) kann man die Einbettungen  $e : k \hookrightarrow F$  und  $f : F \hookrightarrow M_2(k)$  so annehmen, dass  $f(e(a)) = \begin{pmatrix} a & 0 \\ 0 & \bar{a} \end{pmatrix}$  für  $a \in k$ .

Speziell ist dann  $U = f(e(i\sqrt{d})) \in f(F)$ .

Nach Lemma 3.1.a) kann man den Automorphismus  $\begin{pmatrix} a & 0 \\ 0 & \bar{a} \end{pmatrix} \mapsto \begin{pmatrix} \bar{a} & 0 \\ 0 & a \end{pmatrix}$  von  $f(e(k))$  zu einem Automorphismus von  $f(F)$  fortsetzen. Nach Lemma 3.1.b) gibt es also ein  $T \in f(F)^\times$  mit  $TUT^{-1} = -U$ . Man rechnet leicht nach, dass  $T = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$  mit  $b, c \in k^\times$ . Wegen  $bc = -N(T) \in \mathbb{Q}^\times$  gibt es  $t \in \mathbb{Q}^\times$  mit  $c = t\bar{b}$ . Sei  $b = \alpha + \beta i\sqrt{d}$  mit  $\alpha, \beta \in \mathbb{Q}$ . Aus  $\begin{pmatrix} 0 & b\bar{b} \\ t\bar{b} & 0 \end{pmatrix} = \begin{pmatrix} \bar{b} & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & b \\ t\bar{b} & 0 \end{pmatrix} = (\alpha - \beta U)T \in f(F)$  folgt  $V(t) \in f(F)$ . Da  $U$  und  $V(t)$  die  $\mathbb{Q}$ -Algebra  $F(t)$  erzeugen, ist also  $f(F) = F(t)$ .

b) Ist eine Primzahl  $p$  in  $\mathfrak{o}$  zerlegt, dann ist  $F$  unverzweigt an der Stelle  $p$ , da  $k$  Zerfällungskörper von  $F$  ist, und man prüft leicht nach, dass  $\left(\frac{t, -d}{p}\right) = 1$  für alle  $t \in \mathbb{Q}^\times$ .

Betrachte nun den Fall, dass  $p$  verzweigt oder träge in  $\mathfrak{o}$  ist, mit Primteiler  $\mathfrak{p} \subset \mathfrak{o}$ .

Da  $N(U + W(1)) = 0$ , ist  $F(1)$  keine Divisionsalgebra, also speziell auch unverzweigt an der Stelle  $p$ . Daher ist  $F(t)$  genau dann unverzweigt an der Stelle  $p$ , wenn  $F(t)_p$  und  $F(1)_p$  isomorph sind. Man kann einen Isomorphismus  $j: F(t)_p \rightarrow F(1)_p$  dann so wählen, dass  $j(U) = U$ . Und man kann  $j$  zu einem Automorphismus von  $M_2(k_{\mathfrak{p}})$  fortsetzen, denn eine  $\mathbb{Q}_p$ -Basis von  $F(t)_p$  oder  $F(1)_p$  ist auch  $k_{\mathfrak{p}}$ -Basis von  $M_2(k_{\mathfrak{p}})$ .



$F$  ist also unverzweigt an der Stelle  $p$  genau dann, wenn es  $J \in k_p[U]^\times$  gibt mit  $JV(t)J^{-1} = j(V(t)) \in F(1)_p$ . Das ist genau dann der Fall, wenn es  $a, b \in k_p^\times$  gibt mit  $\begin{pmatrix} 0 & ab^{-1} \\ tba^{-1} & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ t & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{-1} \in F(1)_p$ , d.h. mit  $tba^{-1} = \overline{ab^{-1}}$  oder gleichwertig  $t = ab^{-1}\overline{ab^{-1}}$ . Das ist genau dann der Fall, wenn  $\left(\frac{t, -d}{p}\right) = 1$ .

Diese Argumentation ist auch für die unendliche Stelle von  $\mathbb{Q}$  gültig.

- c) Es gibt  $r \in \mathbb{Q}^+$ , so dass  $tr^2 \in \mathbb{Z}$  quadratfrei ist. Wegen  $\left(\frac{tr^2, -d}{p}\right) = \left(\frac{t, -d}{p}\right)$  für alle Stellen  $p$  von  $\mathbb{Q}$ , haben  $F(tr^2)$  und  $F(t)$  dieselben Verzweigungsstellen, sind also isomorph. Man kann daher  $t \in \mathbb{Z}$  und quadratfrei annehmen. (Ersetze  $t$  durch  $tr^2$ .)

Sei  $g$  der größte gemeinsame Teiler von  $t$  und  $d$ , und sei  $t = gt'$  und  $d = gd'$ . Wegen  $\left(\frac{d + g^2, -d}{p}\right) = 1$  ist  $\left(\frac{t, -d}{p}\right) = \left(\frac{g^2t'(d' + g), -d}{p}\right)$ . Falls  $g > 1$  ist, ersetze man  $t$  durch den quadratfreien Anteil von  $t'(d' + g)$ . Dann ist  $t$  teilerfremd zu  $d$ . Falls  $t$  und  $D$  einen gemeinsamen Teiler  $g' > 1$  haben, ist  $g' = 2$  und  $d \equiv 1 \pmod{4}$ , und man ersetze  $t$  durch den quadratfreien Anteil von  $t(d + 1)/4$ . Dann ist  $t$  teilerfremd zu  $D$ .

Falls  $2 \mid d$  und  $t \not\equiv 1 \pmod{4}$ , ist  $d \equiv 2 \pmod{4}$  und  $t \equiv 3 \pmod{4}$ .

In diesem Fall ersetze man schließlich  $t$  durch den quadratfreien Anteil von  $t(d + 1)$ .

- d) rechnet man leicht nach.

□

## 5 Spezielle Einbettung von Maximalordnungen

**Definition 5.1.** 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  $\mathfrak{M}$  eine  $M_2(k)$ -Maximalordnung.

- a) Für eine Stelle  $p$  von  $\mathbb{Q}$  sei  $\left(\frac{F}{p}\right) := +1$  oder  $-1$ , je nachdem, ob  $F$  an der Stelle  $p$  zerlegt oder verzweigt ist.

- b) Sei  $v(F)$  das Produkt der endlichen Verzweigungsstellen von  $F$ , multipliziert mit  $-1$ , falls  $F$  an der Stelle  $\infty$  verzweigt ist.

- c) Sei  $n(\mathfrak{M}) := N_{k|\mathbb{Q}}(N(\mathfrak{M}M_2(\mathfrak{o})))^{-1}$ .

**Satz 5.2.** Sei  $d \in \mathbb{N}$  quadratfrei, und sei  $k = \mathbb{Q}(i\sqrt{d})$  mit Hauptordnung  $\mathfrak{o}$  und Diskriminante  $D$ . Seien  $t, F(t), U, V(t), W(t)$  wie in Satz 4.1.

Dann gibt es eine  $F(t)$ -Maximalordnung  $\mathfrak{F}(t)$  und eine  $M_2(k)$ -Maximalordnung  $\mathfrak{M}(t)$  mit  $\mathfrak{F}(t) \subset \mathfrak{M}(t)$ , so dass  $v(F(t))n(\mathfrak{M}(t)) = t|D|$ .

*Beweis.* Man rechnet elementar nach, dass die unten in (i) - (v) definierten  $\mathbb{Z}_p$ -Moduln  $\mathfrak{F}(t)_p$  und  $\mathfrak{o}_p$ -Moduln  $\mathfrak{M}(t)_p$  multiplikativ abgeschlossen sind mit  $\mathfrak{F}(t)_p \subset \mathfrak{M}(t)_p$  für  $\mathfrak{p} \mid p$ . Man rechnet auch elementar nach, dass  $\mathfrak{F}(t)_p$  die Diskriminante  $\mathbb{Z}_p$  oder  $p^2\mathbb{Z}_p$  hat, je nachdem, ob  $F(t)$  an der Stelle  $\mathfrak{p}$  zerlegt oder verzweigt ist. An allen endlichen Stellen  $\mathfrak{p}$  von  $k$  hat  $\mathfrak{M}(t)_p$  die Diskriminante  $\mathfrak{o}_p$ . Also sind  $\mathfrak{F}(t)_p$  und  $\mathfrak{M}(t)_p$  stets Maximalordnungen. Da  $\mathfrak{F}(t)_p = (F(t) \cap M_2(\mathfrak{o}))_p$  bzw.  $\mathfrak{M}(t)_p = M_2(\mathfrak{o})_p$  an fast allen endlichen Stellen, sind  $\mathfrak{F}(t)$  und  $\mathfrak{M}(t)$  wohldefinierte Maximalordnungen mit  $\mathfrak{F}(t) \subset \mathfrak{M}(t)$ , siehe [2, Teil VI, § 11, Satz 23]. Im Folgenden kürzen wir  $v(t) = v(F(t))$  und  $n(t) = n(\mathfrak{M}(t))$  ab. Wir zeigen  $t|D| = v(t)n(t)$  lokal durch Abgleich der Vielfachheit der Primzahl  $p$  in den Termen  $tD$ ,  $v(t)$ ,  $n(t)$ . Schließlich ist  $t|D| < 0$  genau dann, wenn  $t < 0$ , also wenn  $\left(\frac{t, -d}{\infty}\right) = -1$ , d.h. wenn  $F(t)$  an der Stelle  $\infty$  verzweigt ist. Genau dann ist auch  $v(t) < 0$  und  $v(t)n(t) < 0$ .

(i) Falls  $p \neq \infty$  und  $p \nmid tD$ , ist  $\left(\frac{t, -d}{p}\right) = 1$ .

Sei  $\mathfrak{F}(t)_p := (F(t) \cap M_2(\mathfrak{o}))_p$ , und sei  $\mathfrak{M}(t)_p := M_2(\mathfrak{o})_p$  für alle Primteiler  $\mathfrak{p}$  von  $p$ . Es gilt  $p \nmid tD$  und  $p \nmid v(t)$ . Aus  $N(\mathfrak{M}(t)M_2(\mathfrak{o}))_p = \mathfrak{o}_p$  für alle  $\mathfrak{p} \mid p$  folgt  $p \nmid n(t)$ .

(ii) Falls  $\left(\frac{t, -d}{p}\right) = 1$  und  $p \mid t$ , ist  $p$  zerlegt in  $\mathfrak{o}$ ,  $p\mathfrak{o} = \mathfrak{p}\bar{\mathfrak{p}}$ .

- Falls  $p \neq 2$ , sei  $\alpha \in \mathbb{N}$  minimal mit der Eigenschaft  $\alpha^2 \equiv -d \pmod{p}$ , und sei  $\mathfrak{p}$  das von  $p$  und  $\alpha + i\sqrt{d}$  erzeugte Primideal. Sei  $\mathfrak{F}(t)_p$  der  $\mathbb{Z}_p$ -Modul mit Basis  $\{1, U, V(t), (\alpha V(t) + W(t))/p\}$ .
- Falls  $p = 2$ , ist  $d \equiv 7 \pmod{8}$ . Sei  $\mathfrak{p}$  das von 2 und  $(1 + i\sqrt{d})/2$  erzeugte Primideal. Sei  $\mathfrak{F}(t)_p$  der  $\mathbb{Z}_p$ -Modul mit Basis  $\{1, (1 + U)/2, V(t), (V(t) + W(t))/4\}$ .

Sei  $\mathfrak{M}(t)_p := M_2(\mathfrak{o})_p$  und  $\mathfrak{M}(t)_{\bar{\mathfrak{p}}} := \begin{pmatrix} \mathfrak{o} & \bar{\mathfrak{p}}^{-1} \\ \bar{\mathfrak{p}} & \mathfrak{o} \end{pmatrix}_{\bar{\mathfrak{p}}}$ .

Es gilt  $p \mid tD$ , aber  $p^2 \nmid tD$  und  $p \nmid v(t)$ .

$N(\mathfrak{M}(t)M_2(\mathfrak{o}))_p = \mathfrak{o}_p$  und  $N(\mathfrak{M}(t)M_2(\mathfrak{o}))_{\bar{\mathfrak{p}}} = \bar{\mathfrak{p}}^{-1}\mathfrak{o}_{\bar{\mathfrak{p}}}$ .

Mit  $N_{k|\mathbb{Q}}(\bar{\mathfrak{p}}) = p$  folgt  $p \mid n(t)$ , aber  $p^2 \nmid n(t)$ .

(iii) Falls  $\left(\frac{t, -d}{p}\right) = 1$  und  $p \mid D$ , ist  $p$  verzweigt in  $\mathfrak{o}$ ,  $p\mathfrak{o} = \mathfrak{p}^2$ .

- Falls  $p \neq 2$ , sei  $\beta \in \mathbb{N}$  minimal mit der Eigenschaft  $\beta^2 \equiv t \pmod{p}$ . Sei  $\mathfrak{F}(t)_p$  der  $\mathbb{Z}_p$ -Modul mit Basis  $\{1, U, V(t), (\beta U + W(t))/p\}$ , und sei  $\mathfrak{M}(t)_p$  der  $\mathfrak{o}_p$ -Modul mit Basis  $\{1, U, V(t), (\beta U + W(t))/p\}$ . Es gilt  $p \mid tD$ , aber  $p^2 \nmid tD$  und  $p \nmid v(t)$ . Mit  $M = \begin{pmatrix} \beta & 1 \\ 0 & i\sqrt{d} \end{pmatrix}$  rechnet man leicht nach, dass  $M\mathfrak{M}(t)_pM^{-1} \subset M_2(\mathfrak{o})_p$ . Nach Lemma 3.2.b) ist  $N(\mathfrak{M}(t)M_2(\mathfrak{o}))_p = N(M)^{-1}\mathfrak{o}_p = (\beta i\sqrt{d})^{-1}\mathfrak{o}_p = \mathfrak{p}^{-1}\mathfrak{o}_p$ . Mit  $N_{k|\mathbb{Q}}(\mathfrak{p}) = p$  folgt  $p \mid n(t)$ , aber  $p^2 \nmid n(t)$ .

- Falls  $p = 2$  und  $2 \mid d$ , gilt  $t \equiv 1 \pmod{4}$  (Satz 4.1.c), also  $t \equiv 1 \pmod{8}$ . Sei  $\mathfrak{F}(t)_p$  der  $\mathbb{Z}_p$ -Modul mit Basis  $\{1, U, (1 + V(t))/2, (U + W(t))/4\}$ , und sei  $\mathfrak{M}(t)_p$  der  $\mathfrak{o}_p$ -Modul mit Basis  $\{1, U, (1 + V(t))/2, (U + W(t))/4\}$ . Es gilt  $p^3 \mid tD$ , aber  $p^4 \nmid tD$  und  $p \nmid v(t)$ .

Mit  $M = \begin{pmatrix} 1 + 2i\sqrt{d} & 1 \\ 1 & 1 \end{pmatrix}$  gilt  $M\mathfrak{M}(t)_p M^{-1} \subset M_2(\mathfrak{o})_p$ .

Nach Lemma 3.2.b) ist  $N(\mathfrak{M}(t)M_2(\mathfrak{o}))_p = N(M)^{-1}\mathfrak{o}_p = (2i\sqrt{d})^{-1}\mathfrak{o}_p = \mathfrak{p}^{-3}\mathfrak{o}_p$ , also  $p^3 \mid n(t)$ , aber  $p^4 \nmid n(t)$ .

- Falls  $p = 2$  und  $d \equiv 1 \pmod{4}$ , ist  $t \equiv 1 \pmod{4}$ . Sei  $\mathfrak{F}(t)_p$  der  $\mathbb{Z}_p$ -Modul mit Basis  $\{1, U, (1 + V(t))/2, (U + W(t))/2\}$ , und sei  $\mathfrak{M}(t)_p$  der  $\mathfrak{o}_p$ -Modul mit Basis  $\{1, U, (1 + V(t))/2, (U + W(t))/2\}$ . Es gilt  $p^2 \mid tD$ , aber  $p^3 \nmid tD$  und  $p \nmid v(t)$ .

Mit  $M = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$  gilt  $M\mathfrak{M}(t)_p M^{-1} \subset M_2(\mathfrak{o})_p$ .

Nach Lemma 3.2.b) ist  $N(\mathfrak{M}(t)M_2(\mathfrak{o}))_p = N(M)^{-1}\mathfrak{o}_p = 2^{-1}\mathfrak{o}_p = \mathfrak{p}^{-2}\mathfrak{o}_p$ , also  $p^2 \mid n(t)$ , aber  $p^3 \nmid n(t)$ .

- (iv) Falls  $\left(\frac{t, -d}{p}\right) = -1$  und  $p \mid t$ , ist  $p$  träge in  $\mathfrak{o}$ ,  $p\mathfrak{o} = \mathfrak{p}$ .

Sei  $\mathfrak{F}(t)_p := (F(t) \cap M_2(\mathfrak{o}))_p$ , und sei  $\mathfrak{M}(t)_p := M_2(\mathfrak{o})_p$ .

Es gilt  $p \mid tD$  und  $p \mid v(t)$ , aber  $p^2 \nmid tD$  und  $p^2 \nmid v(t)$ . Wie in (i) folgt  $p \nmid n(t)$ .

- (v) Falls  $\left(\frac{t, -d}{p}\right) = -1$  und  $p \mid D$ , ist  $p$  verzweigt in  $\mathfrak{o}$ ,  $p\mathfrak{o} = \mathfrak{p}^2$ .

- Falls  $p \neq 2$ , sei  $\mathfrak{F}(t)_p := (F(t) \cap M_2(\mathfrak{o}))_p$ , und sei  $\mathfrak{M}(t)_p := M_2(\mathfrak{o})_p$ . Es gilt  $p \mid tD$  und  $p \mid v(t)$ , aber  $p^2 \nmid tD$  und  $p^2 \nmid v(t)$ . Wie in (i) folgt  $p \nmid n(t)$ .
- Falls  $p = 2$  und  $2 \mid d$ , gilt  $t \equiv 1 \pmod{4}$  (Satz 4.1.c), also  $t \equiv 5 \pmod{8}$ . Sei  $\mathfrak{F}(t)_p$  der  $\mathbb{Z}_p$ -Modul mit Basis  $\{1, U, (1 + V(t))/2, (U + W(t))/2\}$ , und sei  $\mathfrak{M}(t)_p$  der  $\mathfrak{o}_p$ -Modul mit Basis  $\{1, U/i\sqrt{d}, (1 + V(t))/2, (U + W(t))/2i\sqrt{d}\}$ . Es gilt  $p^3 \mid tD$  und  $p \mid v(t)$ , aber  $p^4 \nmid tD$  und  $p^2 \nmid v(t)$ .

Mit  $M = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$  gilt  $M\mathfrak{M}(t)_p M^{-1} \subset M_2(\mathfrak{o})_p$ .

Nach Lemma 3.2.b) ist  $N(\mathfrak{M}(t)M_2(\mathfrak{o}))_p = N(M)^{-1}\mathfrak{o}_p = 2^{-1}\mathfrak{o}_p = \mathfrak{p}^{-2}\mathfrak{o}_p$ , also  $p^2 \mid n(t)$ , aber  $p^3 \nmid n(t)$ .

- Falls  $p = 2$  und  $d \equiv 1 \pmod{4}$ , ist  $t \equiv 3 \pmod{4}$ . Sei  $\mathfrak{F}(t)_p$  der  $\mathbb{Z}_p$ -Modul mit Basis  $\{1, U, V(t), (1 + U + V(t) + W(t))/2\}$ , und sei  $\mathfrak{M}(t)_p$  der  $\mathfrak{o}_p$ -Modul mit Basis  $\{1, (1 + U)/(1 + i\sqrt{d}), (1 + V(t))/(1 + i\sqrt{d}), (1 + U + V(t) + W(t))/2\}$ . Es gilt  $p^2 \mid tD$  und  $p \mid v(t)$ , aber  $p^3 \nmid tD$  und  $p^2 \nmid v(t)$ .

Mit  $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 + i\sqrt{d} \end{pmatrix}$  gilt  $M\mathfrak{M}(t)_p M^{-1} \subset M_2(\mathfrak{o})_p$ . Nach Lemma 3.2.b) ist

$N(\mathfrak{M}(t)M_2(\mathfrak{o}))_p = N(M)^{-1}\mathfrak{o}_p = (1 + i\sqrt{d})^{-1}\mathfrak{o}_p = \mathfrak{p}^{-1}\mathfrak{o}_p$ ,

also  $p \mid n(t)$ , aber  $p^2 \nmid n(t)$ .

□

## 6 Typisierung der einbettenden Maximalordnungen

**Satz 6.1.** Sei  $d \in \mathbb{N}$  quadratfrei, und sei  $k = \mathbb{Q}(i\sqrt{d})$  mit Hauptordnung  $\mathfrak{o}$  und Diskriminante  $D$ . Sei  $F \subset M_2(k)$  eine  $\mathbb{Q}$ -Quaternionenalgebra, und seien  $\mathfrak{F}, \mathfrak{F}'$  zwei  $F$ -Maximalordnungen. Seien  $\mathfrak{M}, \mathfrak{M}'$  zwei  $M_2(k)$ -Maximalordnungen mit  $\mathfrak{F} \subset \mathfrak{M}, \mathfrak{F}' \subset \mathfrak{M}'$ . Dann gibt es  $m \in \mathbb{N}$ , so dass  $N(\mathfrak{M}\mathfrak{M}') = m^{-1}\mathfrak{o}$ .

*Beweis.* Die Behauptung folgt durch Zusammenfügen der folgenden lokalen Ergebnisse.

- (i) Sei  $p$  eine endliche Stelle von  $\mathbb{Q}$ , an der  $F$  zerfällt. Nach Lemma 3.2.a) gibt es Matrizeinheiten in  $F_p$ , bezüglich derer  $\mathfrak{F}_p$  und  $\mathfrak{F}'_p$  die Darstellungen  $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$  und  $\begin{pmatrix} \mathbb{Z}_p & p^{-r}\mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$  haben, mit  $r \in \mathbb{N}_0$ . Für  $\mathfrak{p} \mid p$  gilt dann offenbar  $\mathfrak{M}_{\mathfrak{p}} = \begin{pmatrix} \mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \\ \mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \end{pmatrix}$  und  $\mathfrak{M}'_{\mathfrak{p}} = \begin{pmatrix} \mathfrak{o}_{\mathfrak{p}} & p^{-r}\mathfrak{o}_{\mathfrak{p}} \\ p^r\mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \end{pmatrix}$ . Also gilt  $N(\mathfrak{M}\mathfrak{M}')_{\mathfrak{p}} = N(\mathfrak{M}_{\mathfrak{p}}\mathfrak{M}'_{\mathfrak{p}}) = p^{-r}\mathfrak{o}_{\mathfrak{p}}$ . (Ist  $p$  in  $\mathfrak{o}$  zerlegt, folgt das Ergebnis durch Zusammenfügen für die beiden Primteiler von  $p$ .)
- (ii) Sei  $p$  eine endliche Verzweigungsstelle von  $F$ , und sei  $p \nmid D$ . Dann ist  $p$  träge in  $\mathfrak{o}$ ,  $p\mathfrak{o} = \mathfrak{p}$ . Es gibt  $r \in \mathbb{N}_0$ , so dass  $N(\mathfrak{M}\mathfrak{M}')_{\mathfrak{p}} = N(\mathfrak{M}_{\mathfrak{p}}\mathfrak{M}'_{\mathfrak{p}}) = \mathfrak{p}^{-r}\mathfrak{o}_{\mathfrak{p}} = p^{-r}\mathfrak{o}_{\mathfrak{p}}$ .
- (iii) Sei  $p$  Verzweigungsstelle von  $F$  mit  $p \mid D$ ,  $p\mathfrak{o} = \mathfrak{p}^2$ . Sei  $\pi \in \mathfrak{o}_{\mathfrak{p}}$  Primelement.  $F_p$  ist Divisionsalgebra mit der einzigen Maximalordnung  $\mathfrak{F}_p = \mathfrak{F}'_p$ . Wir zeigen  $\mathfrak{M}_{\mathfrak{p}} = \mathfrak{M}'_{\mathfrak{p}}$ . Wir führen den Beweis durch Widerspruch. Wir nehmen also an, dass  $\mathfrak{M}_{\mathfrak{p}} \neq \mathfrak{M}'_{\mathfrak{p}}$ . Nach Lemma 3.2.a) gibt es dann Matrizeinheiten in  $M_2(k_{\mathfrak{p}})$ , bezüglich derer  $\mathfrak{M}_{\mathfrak{p}}$  und  $\mathfrak{M}'_{\mathfrak{p}}$  die Darstellungen  $\begin{pmatrix} \mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \\ \mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \end{pmatrix}$  und  $\begin{pmatrix} \mathfrak{o}_{\mathfrak{p}} & \pi^{-r}\mathfrak{o}_{\mathfrak{p}} \\ \pi^r\mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}} \end{pmatrix}$  haben, mit  $r \in \mathbb{N}$ .

- Sei  $p \neq 2$ .

Nach Satz 4.1 gibt es  $t \in \mathbb{Q}^{\times}$ , so dass 4.1.c) gilt und  $F$  isomorph zu  $F(t)$  ist. Entsprechend zu  $V(t) \in F(t)$  gibt es dann  $V \in \mathfrak{F}_p \subset \mathfrak{M}_{\mathfrak{p}} \cap \mathfrak{M}'_{\mathfrak{p}}$  mit  $V^2 = t$ .

Wegen  $S(V) = 0$  gibt es  $a, b, c \in \mathfrak{o}_{\mathfrak{p}}$  mit  $V = \begin{pmatrix} a & b \\ \pi c & -a \end{pmatrix}$ . Wegen  $N(V) = -t$  ist

$t = a^2 + \pi bc \equiv a^2 \pmod{\pi}$ . Daraus folgt  $t \in k_{\mathfrak{p}}^{\times(2)}$ . Aber wegen  $\left(\frac{t, -d}{p}\right) = -1$

(siehe Satz 4.1.b) ist  $t \notin \mathbb{Q}_p^{\times(2)}$ , und da  $p$  in  $\mathfrak{o}$  verzweigt ist, auch  $t \notin k_{\mathfrak{p}}^{\times(2)}$ .

- Sei  $p = 2$ .

$F_2$  ist eine (bis auf Isomorphie die einzige)  $\mathbb{Q}_2$ -Divisions-Quaternionenalgebra. Daher gibt es  $A, B \in F_2$  mit  $A^2 = -1$ ,  $B^2 = -1$ ,  $AB = -BA$ . Dann ist  $C = (1 - A - B - AB)/2 \in \mathfrak{F}_2 \subset \mathfrak{M}_{\mathfrak{p}} \cap \mathfrak{M}'_{\mathfrak{p}}$ . Wegen  $S(C) = 1$  gibt es  $a, b, c \in \mathfrak{o}_{\mathfrak{p}}$

mit  $C = \begin{pmatrix} a & b \\ \pi c & 1 - a \end{pmatrix}$ . Dann ist  $a(1 - a) = N(C) + \pi bc \equiv 1 \pmod{\pi}$ . Aber

da notwendig  $a \equiv 0 \pmod{\pi}$  oder  $a \equiv 1 \pmod{\pi}$ , ist  $a(1 - a) \equiv 0 \pmod{\pi}$ . □

**Satz 6.2.** Sei  $d \in \mathbb{N}$  quadratfrei, und sei  $k = \mathbb{Q}(i\sqrt{d})$ . Sei  $F$  eine  $\mathbb{Q}$ -Quaternionenalgebra. Sei  $\mathfrak{F}$  eine  $F$ -Maximalordnung, und sei  $\mathfrak{M}$  eine  $M_2(k)$ -Maximalordnung.

Genau dann gibt es eine Einbettung  $f : F \hookrightarrow M_2(k)$  mit  $f(\mathfrak{F}) \subset \mathfrak{M}$ ,

wenn  $\left(\frac{v(F)n(\mathfrak{M}), -d}{p}\right) = \left(\frac{F}{p}\right)$  für alle Stellen  $p$  von  $\mathbb{Q}$ .

*Beweis.*

(i) Sei  $f : F \hookrightarrow M_2(k)$  eine Einbettung mit  $f(\mathfrak{F}) \subset \mathfrak{M}$ .

Nach Satz 4.1 gibt es  $t \in \mathbb{Q}^\times$ , so dass 4.1.c) gilt und  $F$  isomorph zu  $F(t)$  ist. Nach Satz 5.2 und Satz 4.1.b) ist  $\left(\frac{v(F)n(\mathfrak{M}(t)), -d}{p}\right) = \left(\frac{t|D|, -d}{p}\right) = \left(\frac{F}{p}\right)$  für alle  $p$ .

Ein Isomorphismus  $j : f(F) \rightarrow F(t)$  lässt sich zu einem Automorphismus von  $M_2(k)$  fortsetzen, denn eine  $\mathbb{Q}$ -Basis von  $f(F)$  oder  $F(t)$  ist auch  $k$ -Basis von  $M_2(k)$ .

Mit den Lemmata 3.3.b) und 3.3.a) folgt  $N(\mathfrak{M}M_2(\mathfrak{o}))N(j(\mathfrak{M})M_2(\mathfrak{o})) \in I^{(2)}H$ .

$j(f(\mathfrak{F}))$  ist  $F(t)$ -Maximalordnung mit  $j(f(\mathfrak{F})) \subset j(\mathfrak{M})$ . Nach Satz 6.1 gibt es  $m \in \mathbb{N}$ , so dass  $N(j(\mathfrak{M})\mathfrak{M}(t)) = m^{-1}\mathfrak{o} \in I^{(2)}H$ . Mit Lemma 3.3.a) folgt

$N(j(\mathfrak{M})M_2(\mathfrak{o}))N(\mathfrak{M}(t)M_2(\mathfrak{o})) \in I^{(2)}H$ , also  $N(\mathfrak{M}M_2(\mathfrak{o}))N(\mathfrak{M}(t)M_2(\mathfrak{o})) \in I^{(2)}H$ .

Mit Lemma 3.4 folgt  $\left(\frac{n(\mathfrak{M})n(\mathfrak{M}(t)), -d}{p}\right) = 1$  für alle  $p$ , und also die Behauptung.

(ii) Sei  $\left(\frac{v(F)n(\mathfrak{M}), -d}{p}\right) = \left(\frac{F}{p}\right)$  für alle Stellen  $p$  von  $\mathbb{Q}$ .

$F$  ist genau an den Stellen  $p$  von  $\mathbb{Q}$  verzweigt, wo  $\left(\frac{v(F)n(\mathfrak{M}), -d}{p}\right) = -1$  ist. Daher

haben  $F$  und  $F(v(F)n(\mathfrak{M}))$  die gleichen Verzweigungsstellen, sind also isomorph, siehe Satz 4.1.b) und [2, Teil VII, § 5, Satz 8]. Speziell ist  $k$  Zerfällungskörper von  $F$ . Nach Satz 4.1 gibt es  $t \in \mathbb{Q}^\times$ , so dass 4.1.c) gilt und  $F$  isomorph zu  $F(t)$  ist.

Nach Satz 5.2 ist  $\left(\frac{v(F)n(\mathfrak{M}(t)), -d}{p}\right) = \left(\frac{t|D|, -d}{p}\right) = \left(\frac{F}{p}\right)$  für alle  $p$ .

Mit den Lemmata 3.4, 3.3.a) und 3.3.b) folgt, dass  $\mathfrak{M}$  und  $\mathfrak{M}(t)$  isomorph sind.

Sei  $e : F \hookrightarrow M_2(k)$  eine Einbettung mit  $e(F) = F(t)$ ,

und sei  $\mathfrak{M}'$  eine  $M_2(k)$ -Maximalordnung mit  $e(\mathfrak{F}) \subset \mathfrak{M}'$ . Nach Satz 6.1 gibt es  $m \in \mathbb{N}$ , so dass  $N(\mathfrak{M}'\mathfrak{M}(t)) = m^{-1}\mathfrak{o} \in I^{(2)}H$ . Mit Lemma 3.3.b) folgt, dass  $\mathfrak{M}'$  und  $\mathfrak{M}(t)$ , also auch  $\mathfrak{M}'$  und  $\mathfrak{M}$  isomorph sind. Ein Isomorphismus  $j : \mathfrak{M}' \rightarrow \mathfrak{M}$  lässt sich auf natürliche Weise zu einem Automorphismus von  $M_2(k)$  fortsetzen.

Sei  $f = joe$ . Dann ist  $f : F \hookrightarrow M_2(k)$  Einbettung mit  $f(\mathfrak{F}) = j(e(\mathfrak{F})) \subset j(\mathfrak{M}') = \mathfrak{M}$ .

□

## 7 Die endlichen Untergruppen der Bianchi-Gruppen

**Satz 7.1.** Sei  $d \in \mathbb{N}$  quadratfrei, und sei  $k = \mathbb{Q}(i\sqrt{d})$  mit Hauptordnung  $\mathfrak{o}$ .

- (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.* Für eine  $\mathbb{Q}$ -Quaternionenalgebra  $F$  bezeichne  $\pi : \Gamma(F) \rightarrow P\Gamma(F)$  die kanonische Projektion. Und bezeichne  $\pi : SL_2(\mathbb{C}) \rightarrow PSL_2(\mathbb{C})$  ebenfalls die kanonische Projektion.

- (i) Betrachte zunächst eine 3-Diedergruppe  $\mathcal{D}_3 \subset PSL_2(\mathbb{C})$ .

Dann ist  $\pi^{-1}(\mathcal{D}_3)$  eine binäre 3-Diedergruppe. Sie wird von zwei Elementen  $A, B$  erzeugt, mit  $A^3 = -1$  ( $A^2 - A + 1 = 0$ ),  $B^2 = -1$ ,  $BAB^{-1} = A^{-1}$ , siehe [7, 4.4.7].  $A, B$  erzeugen über  $\mathbb{Q}$  eine Quaternionenalgebra  $F(\mathcal{D}_3)$ , und über  $\mathbb{Z}$  eine 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  $M \in F(\mathcal{D}_3)$  ist darstellbar als  $M = \alpha + \beta A + \gamma B + \delta AB$  mit  $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$ . Falls  $M \neq 0$ , ist  $N(M) = \alpha^2 + \alpha\beta + \beta^2 + \gamma^2 + \gamma\delta + \delta^2 > 0$ . Daher ist  $F(\mathcal{D}_3)$  Divisionsalgebra. Die Anzahl der Verzweigungsstellen von  $F(\mathcal{D}_3)$  ist gerade (siehe [2, Teil VII, § 5, Satz 9]) und  $> 0$ . Daher ist  $F(\mathcal{D}_3)$  genau an den Stellen 3 und  $\infty$  verzweigt, und  $\mathfrak{F}(\mathcal{D}_3)$  ist eine  $F(\mathcal{D}_3)$ -Maximalordnung.

Sei nun  $F$  eine  $\mathbb{Q}$ -Quaternionenalgebra, die genau an den Stellen 3,  $\infty$  verzweigt ist. Dadurch ist der Isomorphietyp von  $F$  eindeutig bestimmt. Also gibt es eine 3-Diedergruppe  $\mathcal{D}_3 \subset P\Gamma(F)$ . Sei  $\mathfrak{F}(\mathcal{D}_3)$  die von  $\pi^{-1}(\mathcal{D}_3)$  erzeugte  $F$ -Maximalordnung. Offenbar gibt es genau dann eine Einbettung  $\mathcal{D}_3 \hookrightarrow PSL_2(\mathfrak{o})$ , d.h. eine Einbettung  $\pi^{-1}(\mathcal{D}_3) \hookrightarrow SL_2(\mathfrak{o})$ , wenn es eine Einbettung  $F \hookrightarrow M_2(k)$  gibt mit  $\mathfrak{F}(\mathcal{D}_3) \hookrightarrow M_2(\mathfrak{o})$ . Nach Satz 6.2 ist das wegen  $v(F) = -3$  und  $n(M_2(\mathfrak{o})) = 1$  genau dann möglich, wenn  $\left(\frac{-3, -d}{p}\right) = 1$  für  $p \neq 3, \infty$  und  $\left(\frac{-3, -d}{p}\right) = -1$  für  $p = 3, \infty$ .

Falls  $p \neq 3, \infty$  und  $p \nmid d$ , ist  $\left(\frac{-3, -d}{p}\right) = 1$ . Betrachte nun den Fall  $p \mid d$ ,  $p \neq 3$ :

Für  $p \neq 2$  ist  $\left(\frac{-3, -d}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$  genau dann, wenn  $p \equiv 1 \pmod{3}$ .

Für  $p = 2$  ist  $\left(\frac{-3, -d}{p}\right) = \left(\frac{-3, 2}{2}\right) \left(\frac{-3, -d/2}{2}\right) = -1$ .

Die Gleichung für  $p = \infty$  gilt stets, die für  $p = 3$  folgt aus den anderen Gleichungen.

- (ii) Betrachte zunächst eine 2-Diedergruppe  $\mathcal{D}_2 \subset PSL_2(\mathbb{C})$ .

Dann ist  $\pi^{-1}(\mathcal{D}_2)$  eine binäre 2-Diedergruppe. Sie wird von zwei Elementen  $A, B$  erzeugt, mit  $A^2 = -1$ ,  $B^2 = -1$ ,  $BAB^{-1} = A^{-1}$ , siehe [7, 4.4.7].

$\mathcal{D}_2$  ist in genau einer Tetraedergruppe  $\mathcal{T} \subset PSL_2(\mathbb{C})$  enthalten.

Dann ist  $\pi^{-1}(\mathcal{T})$  eine binäre Tetraedergruppe. Sie wird von  $A, B$  wie oben, sowie von einem Element  $C$  erzeugt, mit  $C^3 = -1$ ,  $ACA^{-1} = BC$  und  $CB = AC$ ; und eine elementare Rechnung zeigt, dass  $C = (1 - A - B - AB)/2$ , siehe [7, 4.4.10].

$A, B, C$  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  $M \in F(\mathcal{T})$  ist darstellbar als  $M = \alpha + \beta A + \gamma B + \delta AB$  mit  $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$ . Falls  $M \neq 0$ , ist  $N(M) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 > 0$ . Daher ist  $F(\mathcal{T})$  Divisionsalgebra. Die Anzahl der Verzweigungsstellen von  $F(\mathcal{T})$  ist gerade und  $> 0$ . Daher ist  $F(\mathcal{T})$  genau an den Stellen 2 und  $\infty$  verzweigt, und  $\mathfrak{F}(\mathcal{T})$  ist eine  $F(\mathcal{T})$ -Maximalordnung.

Sei nun  $F$  eine  $\mathbb{Q}$ -Quaternionenalgebra, die genau an den Stellen 2,  $\infty$  verzweigt ist. Dadurch ist der Isomorphietyp von  $F$  eindeutig bestimmt. Also gibt es eine Tetraedergruppe  $\mathcal{T} \subset P\Gamma(F)$ . Sei  $\mathfrak{F}(\mathcal{T})$  die von  $\pi^{-1}(\mathcal{T})$  erzeugte  $F$ -Maximalordnung. Offenbar gibt es genau dann eine Einbettung  $\mathcal{T} \hookrightarrow PSL_2(\mathfrak{o})$ , d.h. eine Einbettung  $\pi^{-1}(\mathcal{T}) \hookrightarrow SL_2(\mathfrak{o})$ , wenn es eine Einbettung  $F \hookrightarrow M_2(k)$  gibt mit  $\mathfrak{F}(\mathcal{T}) \hookrightarrow M_2(\mathfrak{o})$ . Nach Satz 6.2 ist das wegen  $v(F) = -2$  und  $n(M_2(\mathfrak{o})) = 1$  genau dann möglich, wenn  $\left(\frac{-2, -d}{p}\right) = 1$  für  $p \neq 2, \infty$  und  $\left(\frac{-2, -d}{p}\right) = -1$  für  $p = 2, \infty$ .

Falls  $p \neq 2, \infty$  und  $p \nmid d$ , ist  $\left(\frac{-2, -d}{p}\right) = 1$ . Betrachte nun den Fall  $p \mid d$ ,  $p \neq 2$ :

$\left(\frac{-2, -d}{p}\right) = \left(\frac{-2}{p}\right) = 1$  genau dann, wenn  $p \equiv 1$  oder  $p \equiv 3 \pmod{8}$ .

Die Gleichung für  $p = \infty$  gilt stets, die für  $p = 2$  folgt aus den anderen Gleichungen.

- (iii) Wie in (ii) sei  $F$  eine  $\mathbb{Q}$ -Quaternionenalgebra, die genau an den Stellen 2 und  $\infty$  verzweigt ist, Sei  $\mathcal{D}_2 \subset P\Gamma(F)$  eine 2-Diedergruppe, und sei  $\mathcal{T} \subset P\Gamma(F)$  die Tetraedergruppe mit  $\mathcal{D}_2 \subset \mathcal{T}$ .

Betrachte eine  $M_2(k)$ -Maximalordnung  $\mathfrak{M}'$ , für die es eine Einbettung  $\mathcal{D}_2 \hookrightarrow P\Gamma(\mathfrak{M}')$  mit  $\mathcal{T} \not\hookrightarrow P\Gamma(\mathfrak{M}')$ , d.h. eine Einbettung  $\pi^{-1}(\mathcal{D}_2) \hookrightarrow \Gamma(\mathfrak{M}')$  mit  $\pi^{-1}(\mathcal{T}) \not\hookrightarrow \Gamma(\mathfrak{M}')$  gibt. In der Schreibweise der Arbeit [5] ist dies gleichwertig zu  $\mu_2^-(\mathfrak{M}') > 0$ , siehe [5, Definitionen 15.5, 22.2, 24.2]. Nach [5, Satz 26.12] gibt es genau dann eine solche Maximalordnung  $\mathfrak{M}'$ , wenn 2 in  $\mathfrak{o}$  verzweigt ist. Sei im Folgenden also  $2\mathfrak{o} = \mathfrak{p}^2$ .

Sei  $f : F \hookrightarrow M_2(k)$  eine Einbettung. Sei  $\mathfrak{M}$  eine  $M_2(k)$ -Maximalordnung mit  $f(\pi^{-1}(\mathcal{T})) \subset \Gamma(\mathfrak{M})$ , also auch  $f(\mathfrak{F}(\mathcal{T})) \subset \mathfrak{M}$ . Sei  $\mathfrak{M}'$  eine  $M_2(k)$ -Maximalordnung mit  $f(\pi^{-1}(\mathcal{D}_2)) \subset \Gamma(\mathfrak{M}')$ , aber  $f(\pi^{-1}(\mathcal{T})) \not\subset \Gamma(\mathfrak{M}')$ . Nach [5, Satz 26.12] gilt:

- Wenn  $p \equiv \pm 1 \pmod{8}$  für alle Primteiler  $p \neq 2$  von  $d$ , dann sind  $\mathfrak{M}$  und  $\mathfrak{M}'$  isomorph (vom gleichen Maximalordnungstyp).
- Wenn  $p \equiv \pm 3 \pmod{8}$  für einen Primteiler  $p$  von  $d$ , dann ist  $N(\mathfrak{M}\mathfrak{M}')_{\mathfrak{p}} \in I^{(2)}H$ .

Nach Lemma 3.4 ist  $\mathfrak{p} \in I^{(2)}H$  äquivalent zu  $\left(\frac{2, -d}{p}\right) = 1$  für alle  $p$ .

Dies ist äquivalent zu  $\left(\frac{2}{p}\right) = 1$ , also zu  $p \equiv \pm 1 \pmod{8}$  für  $p \neq 2, p \mid d$ .

Daher ist stets  $N(\mathfrak{M}\mathfrak{M}')_{\mathfrak{p}} \in I^{(2)}H$ . Mit den Lemmata 3.3.a) und 3.4 folgt daraus, dass  $\left(\frac{2n(\mathfrak{M})n(\mathfrak{M}'), -d}{p}\right) = 1$  für alle  $p$ . Wegen  $f(\mathfrak{F}(\mathcal{T})) \subset \mathfrak{M}$  gilt andererseits

nach Satz 6.2, dass  $\left(\frac{-2n(\mathfrak{M}), -d}{p}\right) = 1$  für  $p \neq 2, \infty$  und  $= -1$  für  $p = 2, \infty$ .

Also ist  $\mathcal{D}_2 \hookrightarrow PSL_2(\mathfrak{o})$  mit  $\mathcal{T} \not\hookrightarrow PSL_2(\mathfrak{o})$ , oder gleichwertig dazu  $\mathfrak{M}' = M_2(\mathfrak{o})$  genau dann möglich, wenn  $\left(\frac{-1, -d}{p}\right) = 1$  für  $p \neq 2, \infty$  und  $= -1$  für  $p = 2, \infty$ .

Dies ist äquivalent zu  $\left(\frac{-1}{p}\right) = 1$ , also zu  $p \equiv 1 \pmod{4}$  für  $p \neq 2, p \mid d$ .

□

## 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, *Über die Idealklassenzahl hyperkomplexer Systeme*, Math. Z. **43** (1938), no. 1, 481–494, DOI 10.1007/BF01181104. MR1545733
- [4] ———, *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. **195** (1955), 127–151 (1956). MR0080767 (18,297c)
- [5] 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/>.
- [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