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

Norbert Krämer

▶ **To cite this version:**

Norbert Krämer. Imaginärquadratische Einbettung von Ordnungen rationaler Quaternionenalgebren, und die nichtzyklischen endlichen Untergruppen der Bianchi-Gruppen. 2014. hal-00720823v5

HAL Id: hal-00720823

https://hal.science/hal-00720823v5

Preprint submitted on 17 Mar 2015 (v5), 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

17. März 2015

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 als Durchschnitt einer M-Maximalordnung mit F auftreten. Wir zeigen, dass der Isomorphietyp einer M-Maximalordnung durch die Diskriminante ihres Durchschnitts mit F bestimmt ist. Wir setzen dann diesen Durchschnitt in Beziehung zum Durchschnitt einer zweiten M-Maximalordnung mit einer zweiten rationalen Quaternionenalgebra in M (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 6.8).
Zusätzlich bestimmen wir die Anzahl der M-Maximalordnungen, die mit F jeweils denselben Durchschnitt haben. Damit berechnen wir die Konjugationsklassenzahlen der nichtzyklischen maximalendlichen Untergruppen der Bianchi-Gruppe (Satz 7.5).
Im abschließenden Kapitel 8 untersuchen wir die nichttrivialen Durchschnitte der nichtzyklischen endlichen Untergruppen der Bianchi-Gruppen (wird fortgesetzt).

Inhaltsverzeichnis

1 Einleitung **2**

2 Bezeichnungen und Grundlagen **4**

3 Einbettung rationaler Quaternionenalgebren **6**

4 Einbettung p-adischer Quaternionenordnungen **10**

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

5 Einbettung rationaler Quaternionenordnungen **20**

6 Die nichtzyklischen endlichen Untergruppen **25**

7 Konjugationsklassenanzahlen **29**

8 Die Durchschnitte von nichtzyklischen endlichen Gruppen **34**

1 Einleitung

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 $M \cong k \otimes_{\mathbb{Q}} F$ eine Erweiterung von F zur k-Quaternionenalgebra.

Ist $\mathfrak{G}$ eine F-Ordnung und $n^2\mathbb{Z}$ die Diskriminante von $\mathfrak{G}$ mit $n \in \mathbb{N}$, dann sei $\Delta(\mathfrak{G}) := +n$ oder $-n$, je nachdem, ob F an der Stelle ∞ zerfällt oder verzweigt ist. Ist $\mathfrak{F}$ eine F-Maximalordnung mit $\mathfrak{G} \subset \mathfrak{F}$, so 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 $\mathfrak{o}_p$ isomorphe Ordnung enthält.

Wir untersuchen die Existenz und die Struktur der $\mathfrak{o}$-kompatiblen F-Ordnungen (Satz 5.3 mit den Sätzen 4.1, 4.2 und 4.4), und wir zeigen, dass eine F-Ordnung $\mathfrak{G}$ genau dann $\mathfrak{o}$-kompatibel ist, wenn es eine M-Maximalordnung $\mathfrak{M}$ mit $\mathfrak{G} = F \cap \mathfrak{M}$ gibt (Satz 5.5), und dass der Isomorphietyp von $\mathfrak{M}$ dann nur von $\Delta(\mathfrak{G})$ abhängt (Satz 5.6).

Unser Hauptergebnis ist der nachstehende Satz 5.8, der die Durchschnitte $F \cap \mathfrak{M}$ und $F' \cap \mathfrak{M}'$ zweier $\mathbb{Q}$-Quaternionenalgebren F, F' mit zwei M-Maximalordnungen $\mathfrak{M}, \mathfrak{M}'$ 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 $\Sigma_k(F)$ das Produkt der Verzweigungsstellen von F, die in k zerlegt sind. Und sei $\Lambda(\mathfrak{M} \cap \mathfrak{M}') := [\mathfrak{M} : (\mathfrak{M} \cap \mathfrak{M}')]$. *Bemerkung*: Der Isomorphietyp von $\mathfrak{M}$ relativ zu $\mathfrak{M}'$ hängt nur von der Gesamtheit der Hilbertsymbole $\left(\frac{\Lambda(\mathfrak{M} \cap \mathfrak{M}'), -d}{p}\right)$ ab. $\mathfrak{M}$, $\mathfrak{M}'$ sind genau dann isomorph, wenn es ein $f \in \mathbb{N}$ gibt mit: $f \mid \Sigma_k(F)$ und $\left(\frac{f\Lambda(\mathfrak{M} \cap \mathfrak{M}'), -d}{p}\right) = 1$ 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 dasss für alle Stellen p von $\mathbb{Q}$ gilt:
$$\left(\frac{\Delta(F \cap \mathfrak{M}) f \Lambda(\mathfrak{M} \cap \mathfrak{M}') \Delta(F' \cap \mathfrak{M}'), -d}{p}\right) = \left(\frac{F}{p}\right)\left(\frac{F'}{p}\right).$$

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.

Für eine $\mathfrak{o}$-kompatible F-Ordnung $\mathfrak{G}$ bestimmen wir zusätzlich die Anzahl der M-Maximalordnungen $\mathfrak{N}$ mit $\mathfrak{G} = F \cap \mathfrak{N}$ und jeweils die Anzahl der $\mathfrak{N}^\times$-Konjugationsklassen von Einbettungen $j : \mathfrak{G} \hookrightarrow \mathfrak{N}$ mit $j(\mathfrak{G}) = j(F) \cap \mathfrak{N}$ (Satz 7.3 mit Satz 4.8).

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 6.8. *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 maximalendliche* 2*-Diedergruppe* $\mathcal{D}_2$*,*
wenn $p \equiv 1 \pmod 4$ *für alle Primteiler* $p \neq 2$ *von* d*.*

Und mit Satz 7.3 bestimmen wir zusätzlich unter anderem die Konjugationsklassenanzahlen der nichtzyklischen maximalendlichen Untergruppen von $PSL_2(\mathfrak{o})$ (Satz 7.5).

Unter Verwendung der Ergebnisse von [4] lassen sich nun auch die Konjugationsklassenanzahlen der zyklischen Untergruppen einer 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 6.8 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 6.4.(i), 6.4.(ii) und 6.6, sowie Satz 6.7 mit dem Spezialfall Satz 6.8.

Im abschließenden Kapitel 8 untersuchen wir die nichttrivialen Durchschnitte der nichtzyklischen maximalendlichen Untergruppen der (unter anderem) Bianchi-Gruppen.
Wir zeigen für $m = 2, 3$, wie sich m-Diedergruppen in Gruppen der Ordnung m schneiden (Sätze 8.3, 8.4, 8.5). Wir ermitteln so neu die bekannte Anzahl der Konjugationsklasssenanzahlen von Gruppen der Ordnung m, die in m-Diedergruppen enthalten sind (Satz 8.6).

Ich danke Alexander D. Rahm für seine Ratschläge und die technische Unterstützung, und Jürgen Rohlfs 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 $z \mapsto \overline{z}$ die komplexe Konjugation und $|z| = \sqrt{z\overline{z}}$ 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.

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 $a \mapsto \overline{a}$ 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 gilt: $\mathbb{Q}_\infty = \mathbb{R}$, $k_\infty = \mathbb{C}$.
Ist p zerlegt in k mit den Primteilern $\mathfrak{p}$ und $\overline{\mathfrak{p}}$, dann ist $k_p \cong k_\mathfrak{p} \times k_{\overline{\mathfrak{p}}}$ und $\mathfrak{o}_p \cong \mathfrak{o}_\mathfrak{p} \times \mathfrak{o}_{\overline{\mathfrak{p}}}$.

Für eine Stelle p von $\mathbb{Q}$ und $a, b \in \mathbb{Q}_p^\times$ sei $\left(\dfrac{a,b}{p}\right)$ das Hilbert-Symbol.
Für Rechenregeln zum Hilbert-Symbol siehe [1, Kapitel I, § 6, Formeln (9)-(13), Satz 7].

Eine $\mathbb{Q}$-Quaternionenalgebra F ist auf natürliche Weise eingebettet in ihre p-Komponente $F_p \cong \mathbb{Q}_p \otimes_{\mathbb{Q}} F$. 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 k-Quaternionenalgebra M ist analog $k \subset M \subset M_\mathfrak{p} \cong k_\mathfrak{p} \otimes_k M$ und $k_\mathfrak{p} \subset M_\mathfrak{p}$. Ist $\mathfrak{p}$ endlich und $\mathfrak{M} \subset M$ ein $\mathfrak{o}$-Modul, so ist $\mathfrak{M}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}\mathfrak{M}$. Wir identifizieren M_∞ mit $M_2(\mathbb{C})$.

Definition 2.1. *Sei F eine $\mathbb{Q}$-Quaternionenalgebra, und sei $\mathfrak{G}$ eine F-Ordnung.*
Ist $n^2\mathbb{Z}$ die Diskriminante von $\mathfrak{G}$ mit $n \in \mathbb{N}$, dann sei $\Delta(\mathfrak{G}) := +n$ oder $-n$,
je nachdem, ob F an der Stelle ∞ zerfällt oder verzweigt ist.

Bemerkung: Das $\mathbb{Z}$-Ideal $\Delta(\mathfrak{G})\mathbb{Z}$ wird in [2, § 2] als Stufe von $\mathfrak{G}$ bezeichnet, Auch eine Bezeichnung als reduzierte Diskriminante von $\mathfrak{G}$ liegt nahe, siehe [5, Definition 2.7.4].

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 k_p das Zentrum von M_p. Ist p verzweigt oder träge in k mit Primteiler $\mathfrak{p}$, so ist auf natürliche Weise $M_p = M_\mathfrak{p}$, und für einen $\mathfrak{o}$-Modul $\mathfrak{M} \subset M$ ist $\mathfrak{M}_p = \mathfrak{M}_\mathfrak{p}$.
Ist p zerlegt in k mit den Primteilern $\mathfrak{p}$ und $\overline{\mathfrak{p}}$, dann ist $M_p \cong M_\mathfrak{p} \times M_{\overline{\mathfrak{p}}} \cong F_p \times F_p$. Wir nennen dann M_p eine k_p-Quaternionenalgebra (obwohl $k_p \cong k_\mathfrak{p} \times k_{\overline{\mathfrak{p}}}$ kein Körper ist). Ist $\mathfrak{M}$ eine M-Ordnung, dann nennen wir $\mathfrak{M}_p = \mathfrak{o}_p\mathfrak{M} \cong \mathfrak{M}_\mathfrak{p} \times \mathfrak{M}_{\overline{\mathfrak{p}}}$ eine M_p-Ordnung. Diese Benennungen ermöglichen uns einheitliche und unkomplizierte Formulierungen von Sätzen und Lemmata in Kapitel 4. Die Aussagen über M_p und $\mathfrak{M}_p$ leiten sich natürlich jeweils aus ihren Eigenschaften als direktes Produkt von Algebren bzw. Ordnungen her.

Eine F-Ordnung $\mathfrak{G}$ heißt in eine M-Maximalordnung $\mathfrak{N}$ optimal eingebettet, wenn $\mathfrak{G} = F \cap \mathfrak{N}$ gilt. Eine F-Maximalordnung $\mathfrak{F} \subset \mathfrak{M}$ ist stets optimal in $\mathfrak{M}$ eingebettet.

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, $U_{11}, U_{12}, U_{21}, U_{22} \in Q$ Matrizeseinheiten 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 Matrizeseinheiten die Gleichung (oder Darstellung) $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Für eine Darstellung bezüglich Matrizeseinheiten gelten die bekannten Matrix-Rechenregeln.

Lemma 2.2. *Sei K algebraischer oder $\mathfrak{p}$-adischer Zahlkörper, und sei Q eine K-Quaternionenalgebra. Seien $A, B \in Q$ mit $N(A) = N(B)$, $S(A) = S(B)$ und $S(A)^2 \neq 4N(A)$. Dann gibt es ein $J \in Q^\times$ mit $JAJ^{-1} = B$.*

Beweis. 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 $J := Y^{-1}X$.

□

Ist K ein algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{O}$, und ist $\mathfrak{A}$ ein $\mathfrak{O}$-Ideal, dann bezeichne $N_{abs}(\mathfrak{A}) \in \mathbb{Q}^+$ die Absolutnorm von $\mathfrak{A}$, und für $A \in K^\times$ sei $N_{abs}(A) := N_{abs}(A\mathfrak{O})$. Falls $\mathfrak{A} \subset \mathfrak{O}$, ist $N_{abs}(\mathfrak{A}) = [\mathfrak{O} : \mathfrak{A}]$.

Lemma 2.3. *Sei K ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{O}$ und Primelement Π. Seien $Q \cong M_2(K)$ eine K-Quaternionenalgebra und $\mathfrak{M}, \mathfrak{M}'$ zwei Q-Maximalordnungen. Dann gibt es genau ein $r \in \mathbb{N}_0$ mit den folgenden Eigenschaften.*

(i) Es gibt Matrizeseinheiten in Q, bezüglich derer gilt:
$$\mathfrak{M} = \begin{pmatrix} \mathfrak{O} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{O} \end{pmatrix} \text{ und } \mathfrak{M}' = \begin{pmatrix} \mathfrak{O} & \Pi^{-r}\mathfrak{O} \\ \Pi^r\mathfrak{O} & \mathfrak{O} \end{pmatrix} = J\mathfrak{M}J^{-1} \text{ mit } J = \begin{pmatrix} 1 & 0 \\ 0 & \Pi^r \end{pmatrix}.$$

(ii) $N(\mathfrak{M}'\mathfrak{M})^{-1} = N(\mathfrak{M}\mathfrak{M}')^{-1} = \Pi^r\mathfrak{O}$.

(iii) *Sei* $J' \in \mathfrak{M} \setminus \Pi\mathfrak{M}$ *mit* $\mathfrak{M}' = J'\mathfrak{M}J'^{-1}$. *Dann ist* $N(J') \in \Pi^r\mathfrak{O}^\times$.

(iv) $\mathfrak{M} \cap \mathfrak{M}'$ *hat die Diskriminante* $\Pi^{2r}\mathfrak{O}$, *und es gilt* $[\mathfrak{M} : (\mathfrak{M} \cap \mathfrak{M}')] = N_{abs}(\Pi\mathfrak{O})^r$.

Beweis. Wir zeigen die Existenz von r. Die Eindeutigkeit folgt dann sofort, etwa mit (ii).

(i) Für einen kurzen Beweis siehe [2, Beweis von Satz 7, Fall b)].

(ii) Man prüft leicht nach, dass $\mathfrak{M}\mathfrak{M}' = \mathfrak{M}J^{-1}$. Also gilt $N(\mathfrak{M}\mathfrak{M}')^{-1} = N(J)\mathfrak{O} = \Pi^r\mathfrak{O}$.

(iii) Wegen $\mathfrak{M}' = J'\mathfrak{M}J'^{-1} = J\mathfrak{M}J^{-1}$ ist $J^{-1}J'\mathfrak{M} = \mathfrak{M}J^{-1}J'$ ein zweiseitiges $\mathfrak{M}$-Ideal. Mit [5, Theorem 6.5.3.2] folgt $J' = \Pi^e JY$ für ein $e \in \mathbb{Z}$ und ein $Y \in \mathfrak{M}^\times$. Wegen $J, J' \in \mathfrak{M}$ und $J, J' \notin \Pi\mathfrak{M}$ ist $e = 0$. Also gilt $N(J')\mathfrak{O} = N(J)\mathfrak{O} = \Pi^r\mathfrak{O}$.

(iv) Nach (i) hat $\mathfrak{M}\cap\mathfrak{M}'$ die Diskriminante $\Pi^{2r}\mathfrak{O}$, und es ist $[\mathfrak{M} : (\mathfrak{M}\cap\mathfrak{M}')] = [\mathfrak{O} : \Pi^r\mathfrak{O}]$.

□

Lemma 2.4. *Sei* K *ein* $\mathfrak{p}$*-adischer Zahlkörper, und sei* Q *eine* K*-Quaternionenalgebra. Sei* $L \subset Q$ *eine halbeinfache quadratische Erweiterung von* K, *und seien* $\mathfrak{M}, \mathfrak{M}'$ *zwei* Q*-Maximalordnungen mit* $L \cap \mathfrak{M} = L \cap \mathfrak{M}'$. *Dann gibt es ein* $J \in L^\times$ *mit* $\mathfrak{M}' = J\mathfrak{M}J^{-1}$.

Beweis. Spezialfall einer lokalen Version von [2, Satz 7], Beweis siehe dort, 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) *Für eine Stelle* p *von* $\mathbb{Q}$ *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* $\Phi_F : M \to M$ *die Abbildung mit* $\Phi_F(A + i\sqrt{d}B) := A - i\sqrt{d}B$ *für* $A, B \in F$.

(v) *Für* $T \in M^\times$ *mit* $\Phi_F(T) = T^*$ *sei* $F(F,T) := \{A \in M \mid T\Phi_F(A)T^{-1} = A\}$.

Bemerkung: Für eine F-Maximalordnung $\mathfrak{F}$ gilt offenbar $\Delta(\mathfrak{F}) = \Sigma(F)$.

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 ist an einer Stelle $\mathfrak{p}$ von k genau dann verzweigt, wenn $\Sigma_k(F) \in \mathfrak{p}$ 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 $|\Sigma(E)| = \Sigma_k(E) = \Sigma_k(F)$.*

Beweis.

(i) Ist $p \neq \infty$ in k nicht zerlegt, dann zerfällt M_p, siehe [5, Theorem 2.6.5], und es gilt $M_\infty = M_2(\mathbb{C})$. Ist $p \neq \infty$ in k zerlegt, $p\mathfrak{o} = \mathfrak{p}\overline{\mathfrak{p}}$, dann gilt $M_p \cong M_\mathfrak{p} \times M_{\overline{\mathfrak{p}}} \cong F_p \times F_p$.

(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 $\tau := \Sigma(E)$. Nachfolgend 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 $\mathbb{Q}$-Algebrenautomorphismus von M mit $\Phi_E(\lambda A) = \overline{\lambda}\Phi_E(A)$ und $\Phi_E^2(A) = A$ und $\Phi_E(A^*) = \Phi_E(A)^*$ für alle $\lambda \in k$, $A \in M$. Es gilt $E = \{A \in M \mid \Phi_E(A) = A\}$.*

(ii) *Sei $T \in M^\times$ mit $\Phi_E(T) = T^*$. Dann gilt:*
$F(E,T)$ ist $\mathbb{Q}$-Quaternionenalgebra mit $\Phi_{F(E,T)}(A) = T\Phi_E(A)T^{-1}$ für $A \in M$, und $N(T) \in \mathbb{Q}^\times$ sowie $\left(\frac{N(T),-d}{p}\right) = \left(\frac{E}{p}\right)\left(\frac{F(E,T)}{p}\right)$ für alle Stellen p von $\mathbb{Q}$.

(iii) *Sei $F \subset M$ eine $\mathbb{Q}$-Quaternionenalgebra. Dann ist $F = F(E,T)$ mit $T \in M^\times$ und $\Phi_E(T) = T^*$, und T ist bis auf einen Faktor aus $\mathbb{Q}^\times$ eindeutig. Falls $S(T)^2 \neq 4N(T)$, ist $E \cap F = \mathbb{Q}[i\sqrt{d}(T - T^*)]$ eine halbeinfache quadratische Erweiterung von $\mathbb{Q}$.*

Bemerkung: Für jede Stelle p von $\mathbb{Q}$ ist Φ_E auf natürliche Weise zu einem $\mathbb{Q}_p$-Algebrenautomorphismus von M_p mit Fixalgebra E_p fortsetzbar, den wir auch mit Φ_E bezeichnen.

Beweis. Wir kürzen $\Phi := \Phi_E$ und $F(T) := F(E,T)$ 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. Wegen $i\sqrt{d} \notin F(T)$ ist $F(T)$ eine zentrale $\mathbb{Q}$-Algebra, und wegen $M \cong k \otimes_{\mathbb{Q}} F(T)$ auch einfache $\mathbb{Q}$-Algebra. Sei $A \in M$. Dann gibt es $A', A'' \in F(T)$ mit $A = A' + i\sqrt{d}A''$, und damit gilt: $\Phi_{F(T)}(A) = A' - i\sqrt{d}A'' = T\Phi(A')T^{-1} - i\sqrt{d}T\Phi(A'')T^{-1} = T\Phi(A' + i\sqrt{d}A'')T^{-1}$.
Sei p eine Stelle von $\mathbb{Q}$. Ist p in k zerlegt, so ist $\left(\frac{N(T),-d}{p}\right) = 1 = \left(\frac{E}{p}\right)\left(\frac{F(T)}{p}\right)$, siehe Lemma 3.2.(ii). Wir können nun also p als nicht zerlegt in k annehmen.

- Im Fall $\left(\frac{E}{p}\right)\left(\frac{F(T)}{p}\right) = 1$, ist E_p isomorph zu $F(T)_p$. Einen Isomorphismus $E_p \to F(T)_p$ können wir zu einem k_p-Algebrenautomorhismus 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 $N(T) = T\Phi(T) = \lambda\overline{\lambda}$.

Sei τ wie in Lemma 3.3. Es gibt ein $U \in E^\times$ mit $U^2 = \tau$. Sei $T' := i\sqrt{d}U$. Dann gilt $\Phi(T') = T'^*$. Aus $N(T') = d\tau$ folgt $\left(\frac{N(T'),-d}{p}\right) = -1$ und $\left(\frac{E}{p}\right)\left(\frac{F(T')}{p}\right) = -1$.

- 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 $N(T) = T\Phi(T) = \lambda\overline{\lambda}N(T')$.

(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 $T = \Phi(\lambda T^*) = \overline{\lambda}\lambda T$, und daher gilt $\overline{\lambda}\lambda = 1$. Also gibt es ein $\mu \in k^\times$ mit $\lambda = \mu\overline{\mu}^{-1}$. Wir ersetzen T durch μT.
Dann ist $\Phi(T) = T^*$, und offensichtlich gilt $\Phi_F = \Phi_{F(T)}$, also $F = F(T)$.
Für $S(T)^2 \neq 4N(T)$ sei $X \in E \cap F$. Dann gilt $X = \Phi_F(X) = T\Phi(X)T^{-1} = TXT^{-1}$, also $X \in k[T]$. Mit $i\sqrt{d}(T - T^*) \in E \cap F$ folgt die Behauptung $X \in \mathbb{Q}[i\sqrt{d}(T - T^*)]$.

□

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 $F(\tau) := \left\{ \begin{pmatrix} a & b \\ \tau\overline{b} & \overline{a} \end{pmatrix} \middle| a, b \in k \right\}$.
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 $2 \mid d$.
Dann hat die $F(\tau)$-Ordnung $\mathfrak{F}(\tau) := F(\tau) \cap M_2(\mathfrak{o})$ die Diskriminante $t^2D^2\mathbb{Z}$. Falls $\tau \neq 1$, gilt dann außerdem $F(\tau) \cap M_2(\mathbb{Q}) \cong \mathbb{Q}(\sqrt{\tau})$ und $\mathfrak{F}(\tau) \cap M_2(\mathbb{Z}) = F(\tau) \cap M_2(\mathbb{Z}) \cong \mathbb{Z}[\sqrt{\tau}]$.

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 $F(E, T)$. 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 $F(E, T) = F(\tau)$ 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 $\tau(d + 1)$.
Die Diskriminante von $\mathfrak{F}(\tau)$ kann man leicht elementar berechnen. Die letzte Behauptung folgt aus $F(\tau) \cap M_2(\mathbb{Q}) = \left\{ \begin{pmatrix} a & b \\ \tau b & a \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\} = \mathbb{Q}\left[\begin{pmatrix} 0 & 1 \\ \tau & 0 \end{pmatrix}\right]$ sowie $\begin{pmatrix} 0 & 1 \\ \tau & 0 \end{pmatrix}^2 = \tau$.

□

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 $\mathfrak{O}_p, \mathfrak{O}_p' \subset \mathfrak{F}_p$.
Sei p verzweigt in K_p und träge in K_p'. Sei $\Pi \in \mathfrak{O}_p$ Primelement, und sei $\mathfrak{O}_p' = \mathbb{Z}_p[\Omega]$.

(i) Sei $\mathfrak{G}_p$ eine F_p-Ordnung mit $\mathfrak{O}_p \subset \mathfrak{G}_p \subset \mathfrak{F}_p$.
Dann gibt es ein $r \in \mathbb{N}_0$ mit $\mathfrak{G}_p = \mathfrak{O}_p + \mathfrak{O}_p\Pi^r\Omega$ und $[\mathfrak{F}_p : \mathfrak{G}_p] = [\mathfrak{O}_p : \mathfrak{O}_p\Pi^r] = p^r$.

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

(iii) Sei $r \in \mathbb{N}_0$. Dann sind $\mathfrak{O}_p + \mathfrak{O}_p\Pi^r\Omega$ und $\mathfrak{O}_p' + p^r\mathfrak{O}_p'\Pi$ jeweils F_p-Ordnungen.

(iv) Sei $F_p \cong M_2(\mathbb{Q}_p)$, und sei $\mathfrak{G}_p$ eine F_p-Ordnung mit $\mathfrak{O}_p \subset \mathfrak{G}_p$.
Dann ist $\Pi\mathfrak{F}_p\Pi^{-1}$ eine F_p-Maximalordnung mit $\mathfrak{O}_p \subset \Pi\mathfrak{F}_p\Pi^{-1} \neq \mathfrak{F}_p$,
und es gilt entweder $\mathfrak{G}_p \subset \mathfrak{F}_p$ oder $\mathfrak{G}_p = \Pi\mathfrak{F}_p\Pi^{-1}$.

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 $\alpha + \gamma\Omega \in p\mathfrak{O}_p'$, 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 $\mathfrak{O}_p$-Basis des Linksmoduls $\mathfrak{F}_p$.

Sei $\mathfrak{B}_p = \{B \in K_p \mid B\Omega \in \mathfrak{G}_p\}$.
Wegen $\mathfrak{O}_p \subset \mathfrak{G}_p \subset \mathfrak{F}_p$ ist $\mathfrak{B}_p$ ein ganzes $\mathfrak{O}_p$-Ideal, also gilt $\mathfrak{B}_p = \mathfrak{O}_p\Pi^r$ mit $r \in \mathbb{N}_0$.
Nach Konstruktion gilt $\mathfrak{B}_p\Omega \subset \mathfrak{G}_p$, wegen $\mathfrak{O}_p \subset \mathfrak{G}_p$ also $\mathfrak{O}_p + \mathfrak{B}_p\Omega \subset \mathfrak{G}_p$.
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 $A, B \in \mathfrak{O}_p$, und wegen $\mathfrak{O}_p \subset \mathfrak{G}_p$ ist $B\Omega \in \mathfrak{G}_p$, also $B \in \mathfrak{B}_p$.
Da p in K_p verzweigt ist, gilt $[\mathfrak{O}_p : \mathfrak{O}_p\Pi] = p$ und $[\mathfrak{F}_p : \mathfrak{G}_p] = [\mathfrak{O}_p : \mathfrak{B}_p] = p^r$.

(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 $\mathfrak{O}_p'$-Basis des Linksmoduls $\mathfrak{F}_p$ ist, und dass $\mathfrak{G}_p = \mathfrak{O}_p' + \mathfrak{B}_p'\Pi$ für ein ganzes $\mathfrak{O}_p'$-Ideal $\mathfrak{B}_p' = p^r\mathfrak{O}_p'$ ist, mit $r \in \mathbb{N}_0$. Wegen $[\mathfrak{O}_p' : p\mathfrak{O}_p'] = p^2$ ist dann $[\mathfrak{F}_p : \mathfrak{G}_p] = [\mathfrak{O}_p' : \mathfrak{B}_p'] = p^{2r}$.

(iii) Zum Beweis, dass $\mathfrak{G}_p := \mathfrak{O}_p + \mathfrak{O}_p\Pi^r\Omega$ eine F_p-Ordnung ist, müssen wir nur zeigen, dass $\mathfrak{G}_p$ multiplikativ abgeschlossen ist. Seien also $A_1, A_2 \in \mathfrak{O}_p$ und $B_1, B_2 \in \mathfrak{O}_p\Pi^r$.
Da $\mathfrak{F}_p$ multiplikativ abgeschlossen ist, ist $\Omega(A_2 + B_2\Omega) = A' + B'\Omega$ mit $A', B' \in \mathfrak{O}_p$.

Dann ist $(A_1 + B_1\Omega)(A_2 + B_2\Omega) = A'' + B''\Omega$ mit $A'' = A_1A_2 + B_1A' \in \mathfrak{O}_p$ und $B'' = A_1B_2 + B_1B' \in \mathfrak{O}_p\Pi^r$. Genauso folgt, dass $\mathfrak{O}'_p + p^r\mathfrak{O}'_p\Pi$ eine F_p-Ordnung ist.

(iv) Sei $\mathfrak{F}'_p$ eine F_p-Maximalordnung mit $\mathfrak{O}_p \subset \mathfrak{F}'_p$. Dann gilt $\mathfrak{O}_p = K_p \cap \mathfrak{F}_p = K_p \cap \mathfrak{F}'_p$. Daher gibt es nach Lemma 2.4 ein $X \in K_p^\times$ mit $\mathfrak{F}'_p = X\mathfrak{F}_pX^{-1}$.
Wegen $\Pi^2p^{-1} \in \mathfrak{O}_p^\times$ gibt es ein $r \in \mathbb{Z}$ und $Y \in \mathfrak{O}_p^\times$ mit $X = p^rY$ oder $X = \Pi p^rY$. Also ist $\mathfrak{F}'_p = \mathfrak{F}_p$ oder $\mathfrak{F}'_p = \Pi\mathfrak{F}_p\Pi^{-1}$, und wegen $\Pi \notin \mathbb{Q}_p^\times\mathfrak{F}_p^\times$ gilt $\Pi\mathfrak{F}_p\Pi^{-1} \neq \mathfrak{F}_p$, siehe [5, Theorem 6.5.3.2]. Damit folgt $\mathfrak{G}_p \subset \mathfrak{F}_p$ oder $\mathfrak{G}_p \subset \Pi\mathfrak{F}_p\Pi^{-1}$. Falls $\mathfrak{G}_p \subsetneq \Pi\mathfrak{F}_p\Pi^{-1}$, gibt es nach (i) ein $r \in \mathbb{N}$ mit $\mathfrak{G}_p = \mathfrak{O}_p + \mathfrak{O}_p\Pi^r\Pi\Omega\Pi^{-1} = \mathfrak{O}_pN(\Pi)^{-1}\Pi^{r+1}\Omega\Pi^* \subset \mathfrak{F}_p$.

□

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 $\mathfrak{O}_p \subset \mathfrak{F}_p$. Sei p zerlegt in K_p, sei also K_p kein Körper.

(i) Sei $\mathfrak{G}_p$ eine F_p-Ordnung mit $\mathfrak{O}_p \subset \mathfrak{G}_p \subset \mathfrak{F}_p$.
Dann gibt es Matrizeseinheiten in F_p, bezüglich derer $\mathfrak{O}_p = \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$ 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) Seien $r, s \in \mathbb{Z}$ mit $r + s \geq 0$, und seien (beliebige) Matrizeseinheiten in F_p gegeben.
Bezüglich dieser Matrizeseinheiten ist dann $\begin{pmatrix} \mathbb{Z}_p & p^s\mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ eine F_p-Ordnung.

Beweis.

(i) Je zwei zerfallende halbeinfache quadratische Erweiterungen von $\mathbb{Q}_p$ sind isomorph zueinander. Nach Lemma 2.2 gibt es also Matrizeseinheiten $U_{11}, U_{12}, U_{21}, U_{22} \in F_p$, bezüglich derer $\mathfrak{O}_p = \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$ 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 $\beta U_{12} = U_{11}AU_{22} \in \mathfrak{G}_p$ und $\gamma U_{21} = U_{22}AU_{11} \in \mathfrak{G}_p$ sowie $\alpha, \delta \in \mathbb{Z}_p$. Also ist $\{U_{11}, p^sU_{12}, p^rU_{21}, U_{22}\}$ 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 Matrizeseinheiten $U_{11}, p^sU_{12}, p^{-s}U_{21}, U_{22}$ gilt schließlich $\mathfrak{O}_p = \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$ und $\mathfrak{G}_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^{r+s}\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$.

(ii) leicht nachzurechnen

□

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 $\mathfrak{O}_p \subset \mathfrak{F}_p$, $\mathfrak{O}'_p \subset \mathfrak{F}'_p$. Seien $\mathfrak{G}_p, \mathfrak{G}'_p$ zwei F_p-Ordnungen mit $\mathfrak{O}_p \subset \mathfrak{G}_p \subset \mathfrak{F}_p$, $\mathfrak{O}'_p \subset \mathfrak{G}'_p \subset \mathfrak{F}'_p$ und $[\mathfrak{F}_p : \mathfrak{G}_p] = [\mathfrak{F}'_p : \mathfrak{G}'_p]$. Dann gilt: Ein Isomorphismus $\mathfrak{O}_p \to \mathfrak{O}'_p$ lässt sich zu einem Isomorphismus $\mathfrak{G}_p \to \mathfrak{G}'_p$ fortsetzen.*

Beweis. Ein Isomorphismus $\mathfrak{O}_p \to \mathfrak{O}'_p$ ist nach Lemma 2.2 zu einem Automorphismus $j : F_p \to F_p$ fortsetzbar. Wegen $K'_p \cap j(\mathfrak{F}_p) = j(\mathfrak{O}_p) = \mathfrak{O}'_p = K'_p \cap \mathfrak{F}'_p$ gibt es nach Lemma 2.4 ein $X \in K'^{\times}_p$ mit $\mathfrak{F}'_p = Xj(\mathfrak{F}_p)X^{-1}$, und es gilt $\mathfrak{O}'_p \subset Xj(\mathfrak{G}_p)X^{-1} \subset \mathfrak{F}'_p$.
Falls K_p Körper ist, folgt mit Satz 4.1.(i) bzw. 4.1.(ii), dass $Xj(\mathfrak{G}_p)X^{-1} = \mathfrak{G}'_p$.
Falls K_p zerfällt, gibt es nach Satz 4.2.(i) Matrizeseinheiten in F_p und $r, s, r', s' \in \mathbb{Z}$ mit $r + s = r' + s'$, bezüglich derer gilt: $\mathfrak{O}'_p = \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$, $Xj(\mathfrak{G}_p)X^{-1} = \begin{pmatrix} \mathbb{Z}_p & p^s\mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ 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 $Y := \begin{pmatrix} p^r & 0 \\ 0 & p^{r'} \end{pmatrix} \in K'^{\times}_p$ 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 Matrizeseinheiten 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 $\mathfrak{O}_p, \mathfrak{O}'_p$. Sei p verzweigt in K_p und träge in K'_p. Sei $\Pi \in \mathfrak{O}_p$ Primelement, und sei $\mathfrak{O}'_p = \mathbb{Z}_p[\Omega]$. Da $\mathfrak{F}_p$ die einzige F_p-Maximalordnung ist, gilt $K_p \cap \mathfrak{F}_p = \mathfrak{O}_p$ und $K'_p \cap \mathfrak{F}_p = \mathfrak{O}'_p$. 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 $\mathfrak{G}_p = \mathfrak{O}_p + \mathfrak{O}_p\Pi\Omega$, und $\{1, \Pi, p\Omega, \Pi\Omega\}$ ist eine $\mathbb{Z}_p$-Basis von $\mathfrak{G}_p$. Damit folgt, dass $K_p \cap \mathfrak{G}_p = \mathfrak{O}_p = \{A \in K_p \cap \mathfrak{F}_p \mid (S(A)^2 - 4N(A)) \in p\mathbb{Z}_p\}$ 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 [2, 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 und M eine Erweiterung von F zur k-Quaternionenalgebra. Seien $\mathfrak{F}$ eine F-Maximalordnung und p eine endliche Verzweigungsstelle von F.

(i) *Falls p in k verzweigt ist, gibt es genau eine M_p-Maximalordnung $\mathfrak{M}_p$ mit $\mathfrak{F}_p \subset \mathfrak{M}_p$.*

(ii) *Falls p in k träge ist, gibt es genau zwei M_p-Maximalordnungen $\mathfrak{M}_p \neq \mathfrak{M}'_p$ mit $\mathfrak{F}_p \subset \mathfrak{M}_p$ und $\mathfrak{F}_p \subset \mathfrak{M}'_p$. Es gilt $[\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{M}'_p)] = p^2$ und $\Phi_F(\mathfrak{M}_p) = \mathfrak{M}'_p$.*

Beweis. Sei $K_p \subset F_p$ quadratische Körpererweiterung von $\mathbb{Q}_p$ mit Hauptordnung $\mathfrak{O}_p$. Falls p verzweigt in k ist, sei p träge in K_p. Falls p träge in k ist, sei p verzweigt in K_p. $L_p := k_p K_p$ ist quadratische Körpererweiterung von k_p mit Hauptordnung $\mathfrak{L}_p = \mathfrak{o}_p\mathfrak{O}_p$. Seien $\mathfrak{M}_p$ und $\mathfrak{M}'_p$ zwei M_p-Maximalordnungen mit $\mathfrak{F}_p \subset \mathfrak{M}_p$ und $\mathfrak{F}_p \subset \mathfrak{M}'_p$. Dann gilt $\mathfrak{L}_p = \mathfrak{o}_p\mathfrak{O}_p = \mathfrak{o}_p(K_p \cap \mathfrak{M}_p) \subset L_p \cap \mathfrak{M}_p \subset \mathfrak{L}_p$, also gilt $\mathfrak{L}_p = L_p \cap \mathfrak{M}_p$ und genauso $\mathfrak{L}_p = L_p \cap \mathfrak{M}'_p$. Daher gibt es nach Lemma 2.4 ein $X \in L_p^\times$ mit $\mathfrak{M}'_p = X\mathfrak{M}_pX^{-1}$.

(i) Sei $\pi \in \mathfrak{o}_p$ Primelement. Dann ist π auch Primelement in $\mathfrak{L}_p$. Daher gibt es $r \in \mathbb{Z}$ und $Y \in \mathfrak{L}_p^\times \subset \mathfrak{M}_p^\times$ mit $X = \pi^r Y$. Also gilt $\mathfrak{M}'_p = \pi^r Y\mathfrak{M}_pY^{-1}\pi^{-r} = \mathfrak{M}_p$.

(ii) Sei $\Pi \in \mathfrak{O}_p$ Primelement, also auch Primelement in $\mathfrak{L}_p$. Es gilt $\Pi^2 p^{-1} \in \mathfrak{O}_p^\times$. Daher gibt es $r \in \mathbb{Z}$ und $Y \in \mathfrak{L}_p^\times \subset \mathfrak{M}_p^\times$ mit $X = p^rY$ oder $X = \Pi p^rY$. Also gilt $\mathfrak{M}'_p = \mathfrak{M}_p$ oder $\mathfrak{M}'_p = \Pi\mathfrak{M}_p\Pi^{-1}$. Sei nun $\mathfrak{M}'_p = \Pi\mathfrak{M}_p\Pi^{-1}$. Die k_p-Algebra M_p zerfällt, siehe Lemma 3.2.(i). Wegen $\Pi \notin k_p^\times\mathfrak{M}_p^\times$ gilt daher $\mathfrak{M}'_p \neq \mathfrak{M}_p$, siehe [5, Theorem 6.5.3.2]. Aus $N(\Pi) \in p^1\mathfrak{O}_p^\times$ folgt mit Lemma 2.3, dass $[\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{M}'_p)] = N_{abs}(p\mathfrak{O}_p)^1 = p^2$. Da F_p bis auf Isomorphie eindeutig ist, gibt es (vergleiche Satz 3.5) Matrizeseinheiten in M_p, bezüglich derer $\mathfrak{F}_p = \left\{ \begin{pmatrix} a & b \\ p\overline{b} & \overline{a} \end{pmatrix} \middle| a, b \in \mathfrak{o}_p \right\}$ und o.b.d.A. $\mathfrak{M}_p = M_2(\mathfrak{o}_p)$, $\mathfrak{M}'_p = \begin{pmatrix} \mathfrak{o}_p & p^{-1}\mathfrak{o}_p \\ p\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ gilt. Mit $2pi\sqrt{d}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = i\sqrt{d}\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} - \begin{pmatrix} 0 & i\sqrt{d} \\ -pi\sqrt{d} & 0 \end{pmatrix}$ folgt $\Phi_F\left(\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right) = \begin{pmatrix} 0 & p^{-1} \\ 0 & 0 \end{pmatrix}$, also $\Phi_F(\mathfrak{M}_p) \neq \mathfrak{M}_p$, das heißt $\Phi_F(\mathfrak{M}_p) = \mathfrak{M}'_p$.

□

Lemma 4.6. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Seien F eine $\mathbb{Q}$-Quaternionenalgebra und M eine Erweiterung von F zur k-Quaternionenalgebra. Seien $\mathfrak{F}$ eine F-Maximalordnung und p eine endliche Stelle von $\mathbb{Q}$. Falls F_p zerfällt oder p in k zerlegt ist, gibt es genau eine M_p-Maximalordnung $\mathfrak{M}_p$ mit $\mathfrak{F}_p \subset \mathfrak{M}_p$.

Beweis. Sei $\mathfrak{p} \subset \mathfrak{o}$ ein Primteiler von p.
Falls F_p zerfällt, hat $\mathfrak{F}_p$ die Diskriminante $\mathbb{Z}_p$. Dann hat $\mathfrak{M}_\mathfrak{p} := \mathfrak{o}_\mathfrak{p}\mathfrak{F}_p$ die Diskriminante $\mathfrak{o}_\mathfrak{p}$, ist also die einzige $M_\mathfrak{p}$-Maximalordnung $\mathfrak{M}_\mathfrak{p}$ mit $\mathfrak{F}_p \subset \mathfrak{M}_\mathfrak{p}$. Ist p in k verzweigt oder träge, bleibt nichts zu zeigen. Ist p in k zerlegt, folgt die Behauptung mit $\mathfrak{M}_p :\cong \mathfrak{M}_\mathfrak{p} \times \mathfrak{M}_{\overline{\mathfrak{p}}}$.
Falls F_p Divisionsalgebra ist und p in k zerlegt ist, gilt $M_p \cong M_\mathfrak{p} \times M_{\overline{\mathfrak{p}}} \cong F_p \times F_p$, und $\mathfrak{M}_p :\cong \mathfrak{F}_p \times \mathfrak{F}_p$ ist die einzige M_p-Maximalordnung. ($\mathfrak{F}_p$ ist darin diagonal eingebettet.)
□

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, 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 $\mathfrak{F}_p$ eine F_p-Maximalordnung mit $F_p \cap \mathfrak{N}_p \subset \mathfrak{F}_p$. Dann gibt es genau eine M_p-Maximalordnung $\mathfrak{M}_p$ mit $\mathfrak{F}_p \subset \mathfrak{M}_p$ und $[\mathfrak{F}_p : (F_p \cap \mathfrak{N}_p)] = [\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)]$. Die Inklusion $\mathfrak{F}_p \hookrightarrow \mathfrak{M}_p$ induziert einen Isomorphismus $\mathfrak{F}_p/(F_p \cap \mathfrak{N}_p) \to \mathfrak{M}_p/(\mathfrak{M}_p \cap \mathfrak{N}_p)$.*

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

• Sei zunächst p zerlegt in k.
Wegen $p \nmid \Sigma_k(F)$ gilt $F_p \cong M_2(\mathbb{Q}_p)$. Sei $p\mathfrak{o} = \mathfrak{p}\overline{\mathfrak{p}}$. Dann gilt $\mathfrak{N}_p \cong \mathfrak{N}_\mathfrak{p} \times \mathfrak{N}_{\overline{\mathfrak{p}}}$. Wegen $F_p \cong M_\mathfrak{p} \cong M_{\overline{\mathfrak{p}}}$ gibt es F_p-Maximalordnungen $\mathfrak{F}'_p$, $\mathfrak{F}''_p$ mit $\mathfrak{N}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}\mathfrak{F}'_p$ und $\mathfrak{N}_{\overline{\mathfrak{p}}} = \mathfrak{o}_{\overline{\mathfrak{p}}}\mathfrak{F}''_p$. Es gibt ein $r \in \mathbb{N}_0$ und Matrizeseinheiten in F_p, bezüglich derer $\mathfrak{F}'_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ 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 $\mathfrak{N}_p \cong \begin{pmatrix} \mathfrak{o}_\mathfrak{p} & \mathfrak{o}_\mathfrak{p} \\ \mathfrak{o}_\mathfrak{p} & \mathfrak{o}_\mathfrak{p} \end{pmatrix} \times \begin{pmatrix} \mathfrak{o}_{\overline{\mathfrak{p}}} & p^{-r}\mathfrak{o}_{\overline{\mathfrak{p}}} \\ p^r\mathfrak{o}_{\overline{\mathfrak{p}}} & \mathfrak{o}_{\overline{\mathfrak{p}}} \end{pmatrix}$. 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 gilt $\mathfrak{o}_p \cong \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix} \subset \mathfrak{G}_p$. Nach Satz 4.2.(i) gilt $\mathfrak{F}_p = \begin{pmatrix} \mathbb{Z}_p & p^{-s}\mathbb{Z}_p \\ p^s\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ mit $s \in \mathbb{Z}$. Wegen $\mathfrak{G}_p \subset \mathfrak{F}_p$ gilt $0 \le s \le r$ und $[\mathfrak{F}_p : \mathfrak{G}_p)] = p^r$. Nach Lemma 4.6 gibt es genau eine M_p-Maximalordnung $\mathfrak{M}_p$ mit $\mathfrak{F}_p \subset \mathfrak{M}_p$. Dann gilt $\mathfrak{M}_p \cong \begin{pmatrix} \mathfrak{o}_\mathfrak{p} & p^{-s}\mathfrak{o}_\mathfrak{p} \\ p^s\mathfrak{o}_\mathfrak{p} & \mathfrak{o}_\mathfrak{p} \end{pmatrix} \times \begin{pmatrix} \mathfrak{o}_{\overline{\mathfrak{p}}} & p^{-s}\mathfrak{o}_{\overline{\mathfrak{p}}} \\ p^s\mathfrak{o}_{\overline{\mathfrak{p}}} & \mathfrak{o}_{\overline{\mathfrak{p}}} \end{pmatrix}$, und aus $\mathfrak{M}_p \cap \mathfrak{N}_p \cong \begin{pmatrix} \mathfrak{o}_\mathfrak{p} & \mathfrak{o}_\mathfrak{p} \\ p^s\mathfrak{o}_\mathfrak{p} & \mathfrak{o}_\mathfrak{p} \end{pmatrix} \times \begin{pmatrix} \mathfrak{o}_{\overline{\mathfrak{p}}} & p^{-s}\mathfrak{o}_{\overline{\mathfrak{p}}} \\ p^r\mathfrak{o}_{\overline{\mathfrak{p}}} & \mathfrak{o}_{\overline{\mathfrak{p}}} \end{pmatrix}$ folgt $[\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)] = p^s p^{r-s} = p^r$, und $\mathfrak{F}_p/\mathfrak{G}_p \to \mathfrak{M}_p/(\mathfrak{M}_p \cap \mathfrak{N}_p)$ ist Isomorphismus.

• Sei nun p verzweigt oder träge in k.
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 $\mathfrak{M}_p$ eine M_p-Maximalordnung mit $\mathfrak{F}_p \subset \mathfrak{M}_p$. Nur falls p in k träge ist, müssen wir $\mathfrak{M}_p$ im Beweisverlauf eventuell ersetzen, siehe Lemma 4.5. Die induzierte Abbildung $\mathfrak{F}_p/\mathfrak{G}_p \to \mathfrak{M}_p/(\mathfrak{M}_p \cap \mathfrak{N}_p)$ ist injektiv. Es gibt ein $r \in \mathbb{N}_0$ und Matrizeseinheiten $U_{11}, U_{12}, U_{21}, U_{22} \in M_p$, bezüglich derer $\mathfrak{M}_p = \begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ und $\mathfrak{N}_p = \begin{pmatrix} \mathfrak{o}_p & \pi^{-r}\mathfrak{o}_p \\ \pi^r\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ gilt. Wir zeigen (i) und (ii) zuerst für den Fall, dass $\pi^r \notin p\mathfrak{o}_p$.

- Dann ist entweder $r = 0$, also $\mathfrak{M}_p = \mathfrak{N}_p$ und $\mathfrak{G}_p = \mathfrak{F}_p$, also nichts weiter zu zeigen.
- Oder es ist $r = 1$ und p ist verzweigt in k. Dann ist $[\mathfrak{F}_p : \mathfrak{G}_p] \le [\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)] = p$. Falls $\mathfrak{G}_p = \mathfrak{F}_p$, wäre $\mathfrak{M}_p = \mathfrak{N}_p$, also doch $r = 0$. Also ist $[\mathfrak{F}_p : \mathfrak{G}_p] = p$, und nach Satz 4.4 ist $\mathfrak{G}_p$ bis auf Isomorphie eindeutig bestimmt, enthält nach Satz 4.1.(i) also eine zu $\mathfrak{o}_p$ isomorphe Ordnung, und $\mathfrak{F}_p/\mathfrak{G}_p \to \mathfrak{M}_p/(\mathfrak{M}_p \cap \mathfrak{N}_p)$ ist surjektiv.

Wir können nun also annehmen, dass $\pi^r \in p\mathfrak{o}_p$ oder gleichwertig $[\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)] \ge p^2$.

(i) Wir konstuieren (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 $U := \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in F_p \smallsetminus \mathbb{Q}_p$.

Wir zeigen zunächst, dass wir $c = \overline{a}$ annehmen können.
Falls $c \neq \overline{a}$, gilt $c - \overline{a} = S(U) - (a + \overline{a}) \in \mathbb{Q}_p^\times$, und wegen $a(c - \overline{a}) = N(U) - a\overline{a} \in \mathbb{Q}_p$ 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 $c = \overline{a} = 0$.
Wir können also $U = \begin{pmatrix} a & b \\ 0 & \overline{a} \end{pmatrix}$ 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 $U = \begin{pmatrix} \omega & b \\ 0 & \overline{\omega} \end{pmatrix}$ annehmen, mit $b \in \mathfrak{o}_p$.

(ii) Wir wollen zeigen, dass $\mathfrak{F}_p/\mathfrak{G}_p \to \mathfrak{M}_p/(\mathfrak{M}_p \cap \mathfrak{N}_p)$ surjektiv ist. Dazu genügt es, die Surjektivität von $f_{21} : \mathfrak{F}_p \to \mathfrak{o}_p$ mit Zuordnungsvorschrift $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \gamma$ zu zeigen.

- Falls p in k verzweigt ist, sei $K_p \subset F_p$ eine quadratische Körpererweiterung von $\mathbb{Q}_p$ mit Hauptordnung $\mathfrak{O}_p \subset \mathfrak{F}_p$. Sei p träge in K_p, und sei $\mathfrak{O}_p = \mathbb{Z}_p[\Omega]$. Es gibt $\alpha, \beta, \gamma, \delta \in \mathfrak{o}_p$ mit $\Omega = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ und $\Omega U = \begin{pmatrix} \alpha\omega & \alpha b + \beta\overline{\omega} \\ \gamma\omega & \gamma b + \delta\overline{\omega} \end{pmatrix}$. Nach Lemma 4.5.(i) und Lemma 4.6 gilt $\mathfrak{F}_p \not\subset \begin{pmatrix} \mathfrak{o}_p & \pi^{-1}\mathfrak{o}_p \\ \pi\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$. Also gilt: $\gamma \in \mathfrak{o}_p^\times$, $\{\gamma, \gamma\omega\}$ ist $\mathbb{Z}_p$-Basis von $\mathfrak{o}_p$, und $f_{21} : \mathfrak{F}_p \to \mathfrak{o}_p$ ist surjektiv.
- Falls p in k träge ist, sei $K_p \subset F_p$ quadratische Körpererweiterung von $\mathbb{Q}_p$ mit Hauptordnung $\mathfrak{O}_p \subset \mathfrak{F}_p$. Sei p verzweigt in K_p, und sei $\Pi \in \mathfrak{O}_p$ Primelement. Es gibt $\alpha, \beta, \gamma, \delta \in \mathfrak{o}_p$ mit $\Pi = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Falls $\gamma \in \mathfrak{o}_p^\times$, folgt wie in (i), dass f_{21} surjektiv ist. Wir dürfen also $\gamma = \gamma' p^s$ mit $\gamma' \in \mathfrak{o}_p^\times$ und $s \in \mathbb{N}$ annehmen. Bezüglich der Matrizeseinheiten $U_{11}, p^{-s}U_{12}, p^sU_{21}, U_{22} \in M_p$ gilt dann:
  $U = \begin{pmatrix} \omega & p^s b \\ 0 & \overline{\omega} \end{pmatrix}$, $\Pi = \begin{pmatrix} \alpha & p^s\beta \\ \gamma' & \delta \end{pmatrix}$, $\Pi U = \begin{pmatrix} \alpha\omega & p^s(\alpha b + \beta\overline{\omega}) \\ \gamma'\omega & p^s\gamma' b + \delta\overline{\omega} \end{pmatrix}$. Speziell gilt $\mathfrak{F}_p \subset \begin{pmatrix} \mathfrak{o}_p & p^s\mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$. Also ist F_p Divisionsalgebra, $\mathfrak{F}_p$ hat die Diskriminante $p^2\mathbb{Z}_p$,

und es gilt $s = 1$, 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 $\mathfrak{M}_p$ 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.
Falls p Verzweigungsstelle von F ist, müssen wir noch die Eindeutigkeit von $\mathfrak{M}_p$ zeigen. Das verschieben wir als Anhang auf den Beweis von Satz 4.8.(ii).

□

Satz 4.8. *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 $\mathbb{Q}$ mit $p \nmid \Sigma_k(F)$. Seien $\mathfrak{F}_p$ eine F_p-Maximalordnung, $\mathfrak{O}_p \subset \mathfrak{F}_p$ eine zu $\mathfrak{o}_p$ isomorphe Ordnung und $\mathfrak{G}_p$ eine F_p-Ordnung mit $\mathfrak{O}_p \subset \mathfrak{G}_p \subset \mathfrak{F}_p$. Bezeichne $C(\mathfrak{G}_p)$ die Anzahl der M_p-Maximalordnungen $\mathfrak{N}_p$ mit $\mathfrak{G}_p = F_p \cap \mathfrak{N}_p$.

(i) Sei p zerlegt in k.
Es ist $C(\mathfrak{F}_p) = 1$. Für $\mathfrak{G}_p \neq \mathfrak{F}_p$ ist $C(\mathfrak{G}_p) = 2$.

(ii) Sei p träge in k.
Falls $F_p \cong M_2(\mathbb{Q}_p)$, ist $C(\mathfrak{F}_p) = 1$. Falls $F_p \ncong M_2(\mathbb{Q}_p)$ oder $\mathfrak{G}_p \neq \mathfrak{F}_p$, ist $C(\mathfrak{G}_p) = 2$.

(iii) Sei p verzweigt in k.
Es ist $C(\mathfrak{F}_p) = 1$. Für $\mathfrak{G}_p \neq \mathfrak{F}_p$ wird $C(\mathfrak{G}_p)$ durch die folgenden Tabellen dargestellt.

$[\mathfrak{F}_p : \mathfrak{G}_p]$	$C(\mathfrak{G}_p)$, *falls* $p \neq 2$	
	$F_p \cong M_2(\mathbb{Q}_p)$	$F_p \ncong M_2(\mathbb{Q}_p)$
p	1	$p+1$
p^2	$p-1$	$2p$
$\geq p^3$	$2p$	$2p$

$[\mathfrak{F}_p : \mathfrak{G}_p]$	$C(\mathfrak{G}_p)$, *falls* $p = 2$			
	$d \equiv 1 \pmod 4$		$d \equiv 2 \pmod 4$	
	$F_p \cong M_2(\mathbb{Q}_p)$	$F_p \ncong M_2(\mathbb{Q}_p)$	$F_p \cong M_2(\mathbb{Q}_p)$	$F_p \ncong M_2(\mathbb{Q}_p)$
2	1	3	1	3
4	1	2	1	2
8	2	4	2	4
16	4	8	4	4
32	8	8	4	8
64	8	8	8	16
≥ 128	8	8	16	16

Beweis. Die Behauptungen für $\mathfrak{F}_p$, folgen mit den Lemmata 4.5 und 4.6. Sei nun $\mathfrak{G}_p \neq \mathfrak{F}_p$.

(i) Sei $p\mathfrak{o} = \mathfrak{p}\overline{\mathfrak{p}}$. Nach Satz 4.2.(i) gibt es $r \in \mathbb{N}$ und Matrizeseinheiten in F_p, bezüglich derer $\mathfrak{O}_p = \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$ und $\mathfrak{G}_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ gilt. $\mathfrak{G}_p$ ist diagonal in $\mathfrak{N}_\mathfrak{p} \times \mathfrak{N}_{\overline{\mathfrak{p}}}$

eingebettet. Wegen $\mathfrak{O}_p \subset \mathfrak{G}_p$ gilt $\begin{pmatrix} \mathfrak{o}_\mathfrak{p} & 0 \\ 0 & \mathfrak{o}_\mathfrak{p} \end{pmatrix} \times \begin{pmatrix} \mathfrak{o}_{\overline{\mathfrak{p}}} & 0 \\ 0 & \mathfrak{o}_{\overline{\mathfrak{p}}} \end{pmatrix} \subset \mathfrak{N}_\mathfrak{p} \times \mathfrak{N}_{\overline{\mathfrak{p}}}$. Mit Satz 4.2.(i) folgt aus $\mathfrak{o}_\mathfrak{p} \cong \mathfrak{o}_{\overline{\mathfrak{p}}} \cong \mathbb{Z}_p$, dass $\mathfrak{N}_p \cong \mathfrak{N}_\mathfrak{p} \times \mathfrak{N}_{\overline{\mathfrak{p}}} = \begin{pmatrix} \mathfrak{o}_\mathfrak{p} & p^{-s}\mathfrak{o}_\mathfrak{p} \\ p^s\mathfrak{o}_\mathfrak{p} & \mathfrak{o}_\mathfrak{p} \end{pmatrix} \times \begin{pmatrix} \mathfrak{o}_{\overline{\mathfrak{p}}} & p^{-s'}\mathfrak{o}_{\overline{\mathfrak{p}}} \\ p^{s'}\mathfrak{o}_{\overline{\mathfrak{p}}} & \mathfrak{o}_{\overline{\mathfrak{p}}} \end{pmatrix}$ mit $s, s' \in \mathbb{Z}$. Wegen $\mathfrak{G}_p \subset \mathfrak{N}_p$ gilt $0 \leq s, s' \leq r$. Man erkennt dann leicht, dass $\mathfrak{G}_p = F_p \cap \mathfrak{N}_p$ genau dann, wenn entweder $s = 0$ und $s' = r$ oder $s' = 0$ und $s = r$.

(ii) 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 $F_p = \left\{ \begin{pmatrix} a & b \\ \tau\overline{b} & \overline{a} \end{pmatrix} \middle| a, b \in k_p \right\}$ gilt.
F_p zerfällt genau dann, wenn $\left(\frac{\tau, -d}{p}\right) = 1$, also wenn $p \nmid \tau$ gilt. Die F_p-Ordnung $\mathfrak{F}_p := \left\{ \begin{pmatrix} a & b \\ \tau\overline{b} & \overline{a} \end{pmatrix} \middle| a, b \in \mathfrak{o}_p \right\}$ hat die Diskriminante $\tau^2\mathbb{Z}_p$, ist also Maximalordnung.
Für $r \in \mathbb{N}$ sei $\mathfrak{G}(r)_p := \left\{ \begin{pmatrix} a & p^r b \\ p^r\tau\overline{b} & \overline{a} \end{pmatrix} \middle| a, b \in \mathfrak{o}_p \right\}$. Dann ist $\mathfrak{G}(r)_p$ eine F_p-Ordnung mit $\mathfrak{G}(r)_p \subset \mathfrak{F}_p$. Es gilt $[\mathfrak{F}_p : \mathfrak{G}(r)_p] = p^{2r}$, und $\mathfrak{G}(r)_p$ enthält die zu $\mathfrak{o}_p$ isomorphe Ordnung $\mathfrak{O}_p := \left\{ \begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix} \middle| a \in \mathfrak{o}_p \right\}$. Wegen $\mathfrak{G}_p \cong \mathfrak{G}(r)_p$ für ein $r \in \mathbb{N}$ genügt es, die Behauptung für $\mathfrak{G}_p = \mathfrak{G}(r)_p$ zu zeigen. Seien $\mathfrak{N}(r)_p := \begin{pmatrix} \mathfrak{o}_p & p^r\mathfrak{o}_p \\ p^{-r}\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ und $\mathfrak{N}(-r)_p := \begin{pmatrix} \mathfrak{o}_p & (p^r\tau)^{-1}\mathfrak{o}_p \\ p^r\tau\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$. Dann gilt $F_p \cap \mathfrak{N}(r)_p = F_p \cap \mathfrak{N}(-r)_p = \mathfrak{G}(r)_p$.
Sei umgekehrt $\mathfrak{N}_p$ eine M_p-Ordnung mit $F_p \cap \mathfrak{N}_p = \mathfrak{G}(r)_p$. Es genügt zu zeigen, dass $\mathfrak{N}_p = \begin{pmatrix} \mathfrak{o}_p & p^s\mathfrak{o}_p \\ p^{-s}\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ mit $s \in \mathbb{Z}$. Da p im Quotientenkörper K_p von $\mathfrak{O}_p$ träge ist, gilt $\mathfrak{L}_p := \begin{pmatrix} \mathfrak{o}_p & 0 \\ 0 & \mathfrak{o}_p \end{pmatrix} \subset \mathfrak{N}_p$. Sei $L_p := \begin{pmatrix} k_p & 0 \\ 0 & k_p \end{pmatrix}$. Dann gilt $L_p \cap \mathfrak{N}_p = L_p \cap M_2(\mathfrak{o}_p) = \mathfrak{L}_p$. Also gibt es nach Lemma 2.4 ein $X \in L_p^\times$ mit $\mathfrak{N}_p = XM_2(\mathfrak{o}_p)X^{-1}$. Es gibt dann $s, t \in \mathbb{Z}$ und ein $Y \in \mathfrak{L}_p^\times$ mit $X = p^t \begin{pmatrix} p^s & 0 \\ 0 & 1 \end{pmatrix} Y$. Damit folgt die Behauptung.

Anhang zum Beweis von Lemma 4.7.(ii): Sei p träge in k und Verzweigungsstelle von F. Nach Lemma 4.5.(ii) sind $\mathfrak{M}(+)_p := \begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ und $\mathfrak{M}(-)_p := \begin{pmatrix} \mathfrak{o}_p & p^{-1}\mathfrak{o}_p \\ p\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ die beiden einzigen M_p-Maximalordnungen mit $\mathfrak{F}_p \subset \mathfrak{M}(+)_p$ und $\mathfrak{F}_p \subset \mathfrak{M}(-)_p$.
Es gilt $[\mathfrak{M}(+)_p : (\mathfrak{M}(+)_p \cap \mathfrak{N}(r)_p)] = [\mathfrak{M}(-)_p : (\mathfrak{M}(-)_p \cap \mathfrak{N}(-r)_p)] = p^{2r}$ und $[\mathfrak{M}(+)_p : (\mathfrak{M}(+)_p \cap \mathfrak{N}(-r)_p)] = [\mathfrak{M}(-)_p : (\mathfrak{M}(-)_p \cap \mathfrak{N}(r)_p)] = p^{2r+2}$. Die in Lemma 4.7.(ii) angegebene Zuordnung $\mathfrak{N}_p \mapsto \mathfrak{M}_p$ ist wegen $[\mathfrak{F}_p : \mathfrak{G}(r)_p] = p^{2r}$ also eindeutig.

(iii) Wie in (ii) gibt es ein $\tau \in \mathbb{Z}$ mit den Eigenschaften laut Satz 3.5 und Matrizeseinheiten in M_p, bezüglich derer $F_p = \left\{ \begin{pmatrix} a & b \\ \tau\overline{b} & \overline{a} \end{pmatrix} \middle| a, b \in k_p \right\}$ gilt. Diesbezüglich

sei $\mathfrak{N}'_p := \begin{pmatrix} \mathfrak{o}_p & p\mathfrak{o}_p \\ p^{-1}\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$. Dann ist $\mathfrak{G}'_p := F_p \cap \mathfrak{N}'_p = \left\{ \begin{pmatrix} a & pb \\ p\tau\overline{b} & \overline{a} \end{pmatrix} \middle| a, b \in \mathfrak{o}_p \right\}$ eine F_p-Ordnung mit Diskriminante $p^4 D^2 \mathbb{Z}_p$. Seien $\mathfrak{F}_p$ eine F_p-Maximalordnung mit $\mathfrak{G}'_p \subset \mathfrak{F}_p$ und $\mathfrak{M}_p$ die M_p-Maximalordnung mit $\mathfrak{F}_p \subset \mathfrak{M}_p$. Dann gilt $[\mathfrak{F}_p : \mathfrak{G}'_p] \geq p^2$. Sei $\pi \in \mathfrak{o}_p$ ein Primelement. Wie im Beweis von Lemma 4.7 folgt nun, dass es $b, \alpha, \beta, \delta \in \mathfrak{o}_p$, $\gamma \in \mathfrak{o}_p^\times$ und Matrizeseinheiten in M_p gibt, bezüglich derer gilt: $\mathfrak{M}_p = \begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$, und $\left\{ 1, \Pi := \begin{pmatrix} \pi & b \\ 0 & \overline{\pi} \end{pmatrix}, \Omega := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \Pi\Omega \right\}$ ist $\mathbb{Z}_p$-Basis von $\mathfrak{F}_p$, und p ist träge in $K'_p = \mathbb{Q}_p(\Omega)$ mit Hauptordnung $\mathfrak{O}'_p = \mathbb{Z}_p[\Omega]$. Sei $\mathfrak{O}_p := \mathbb{Z}_p[\Pi]$ und $\mathfrak{G}(r)_p := \mathfrak{O}_p + \mathfrak{O}_p \Pi^r \Omega$ für $r \in \mathbb{N}$. Es genügt, die Anzahl der M_p-Maximalordnungen $\mathfrak{N}_p$ mit $\mathfrak{G}(r)_p = F_p \cap \mathfrak{N}_p$ zu berechnen, siehe die Lemmata 4.1.(i) und 4.3.

Sei zunächst $\mathfrak{N}_p$ eine M_p-Maximalordnung mit $\mathfrak{G}(r)_p = F_p \cap \mathfrak{N}_p$. Nach Lemma 4.7.(ii) und den Lemmata 4.5.(i), 4.6 ist dann $[\mathfrak{F}_p : \mathfrak{G}(r)_p] = [\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)] = p^r$. Nach Lemma 2.3.(i) gibt es $J \in \mathfrak{M}_p \smallsetminus \pi\mathfrak{M}_p$ mit $J\mathfrak{M}_p J^{-1} = \mathfrak{N}_p$ und $N(J) \in \pi^r \mathfrak{o}_p^\times$. Für jedes $m \in \mathbb{N}_0$ wählen wir eine Repräsentantenmenge $\mathfrak{r}_p(m) \subset \mathfrak{o}_p$ von $\mathfrak{o}_p / \pi^m \mathfrak{o}_p$. Mit [5, Theorem 6.5.3.3] folgt dann leicht, dass wir $J = J(m,n,c) := \begin{pmatrix} \pi^m & c \\ 0 & \overline{\pi}^n \end{pmatrix}$ annehmen können, mit $m, n \in \mathbb{N}_0$, $m + n = r$, $c \in \mathfrak{o}_p$, für die darüberhinaus gilt:

(C1) $c \in \mathfrak{r}_p(m)$, und $c \in \mathfrak{o}_p^\times$, falls $mn > 0$.

Die Abbildung mit Zuordnungsvorschrift $\mathfrak{N}_p \mapsto (m,n,c)$ ist wohldefiniert und injektiv, und man überprüft leicht, dass $\Pi \in \mathfrak{N}_p$ oder $J^{-1}\Pi J \in \mathfrak{M}_p$ äquivalent ist zu:

(C2) $(\pi - \overline{\pi})c + \overline{\pi}^n b \in \pi^m \mathfrak{o}_p$.

Wir berechnen für jedes $(m,n) \in \mathbb{N}_0 \times \mathbb{N}_0$ die Anzahl C(m,n) der $c \in \mathfrak{o}_p$, die die Bedingungen (C1) und (C2) erfüllen. Dazu benötigen wir zwei Vorbemerkungen:

- Falls $p \neq 2$, gilt $(\pi - \overline{\pi}) \in \pi\mathfrak{o}_p^\times$.
  Falls $p = 2$ und $d \equiv 1 \pmod 4$, gilt $(\pi - \overline{\pi}) \in \pi^2 \mathfrak{o}_p^\times$.
  Falls $p = 2$ und $d \equiv 2 \pmod 4$, gilt $(\pi - \overline{\pi}) \in \pi^3 \mathfrak{o}_p^\times$.
  Zum Beweis ist nur zu beachten, dass wir $\pi - \overline{\pi} = 2i\sqrt{d}$ annehmen können.
- Genau dann gilt $b \in \mathfrak{o}_p^\times$, wenn F_p zerfällt. Falls $p = 2$, gilt stets $b \notin \pi^2 \mathfrak{o}_p$.
  Zum Beweis der ersten Behauptung sei zunächst $b \in \pi\mathfrak{o}_p$. Dann ist $\Pi/\pi \in \mathfrak{M}_p$, also $\mathfrak{o}_p \mathfrak{F}_p \subsetneq \mathfrak{M}_p$. Also hat $\mathfrak{F}_p$ die Diskriminante $p^2\mathbb{Z}_p$.
  Sei umgekehrt F_p eine $\mathbb{Q}_p$-Divisionsalgebra. Wir zeigen, dass der $\mathfrak{o}_p$-Modul $\mathfrak{M}'_p$ mit Basis $\{1, \Pi/\pi, \Omega, \Pi\Omega/\pi\}$ multiplikativ abgeschlossen, also M_p-Ordnung ist: ($\mathfrak{M}'_p$ ist dann Maximalordnung, nach Lemma 4.5.(i) also $\mathfrak{M}'_p = \mathfrak{M}_p$, $b \in \pi\mathfrak{o}_p$.) Multiplikation von links mit (Π/π) oder von rechts mit Ω überführt $\mathfrak{M}'_p$ in sich. Die Behauptung folgt nun mit $\Omega\Pi/\pi = (\Pi/\pi)(\Pi^{-1}\Omega\Pi) \in (\Pi/\pi)\mathfrak{F}_p \subset \mathfrak{M}'_p$.
  Zum Beweis der zweiten Behauptung nehmen wir $b = \pi^2 b'$ mit $b' \in \mathfrak{o}_p$ an.
  Es gibt $x, u, v, w \in \mathfrak{o}_p$ mit $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = x + u\Pi/\pi + v\Omega + w\Pi\Omega/\pi$. Daraus folgt $0 = v\gamma + w\gamma\overline{\pi}/\pi$, also $v + w \in \pi\mathfrak{o}_p$, und $1 = (u + w\delta)\pi b' + (v + w)\beta$, Widerspruch.

Nun können wir die $C(m,n)$ elementar berechnen. Wir führen die Details hier nicht aus, sondern fassen nur die Ergebnisse in den beiden folgenden Tabellen zusammen.

m,n	$C(m,n)$, falls $p \neq 2$	
	$F_p \cong M_2(\mathbb{Q}_p)$	$F_p \ncong M_2(\mathbb{Q}_p)$
$m=0, n\geq 0$	1	1
$m\geq 1, n=0$	0	p
$m=1, n\geq 1$	$p-1$	$p-1$
$m\geq 2, n=1$	p	0
$m\geq 2, n\geq 2$	0	0

m,n	$C(m,n)$, falls $p=2$			
	$d\equiv 1 \pmod 4$		$d\equiv 2 \pmod 4$	
	$F_p \cong M_2(\mathbb{Q}_p)$	$F_p \ncong M_2(\mathbb{Q}_p)$	$F_p \cong M_2(\mathbb{Q}_p)$	$F_p \ncong M_2(\mathbb{Q}_p)$
$m=0, n\geq 0$	1	1	1	1
$m=1, n=0$	0	$p=2$	0	$p=2$
$m=1, n\geq 1$	$p-1=1$	$p-1=1$	$p-1=1$	$p-1=1$
$m\geq 2, n=0$	0	0	0	0
$m=2, n=1$	0	$p^2-p=2$	0	$p^2-p=2$
$m=2, n\geq 2$	$p^2-p=2$	$p^2-p=2$	$p^2-p=2$	$p^2-p=2$
$m\geq 3, n=1$	0	$p^2=4$	0	0
$m=3, n=2$	$p^2=4$	0	0	$p^3-p^2=4$
$m=3, n\geq 3$	0	0	$p^3-p^2=4$	$p^3-p^2=4$
$m\geq 4, n=2$	$p^2=4$	0	0	$p^3=8$
$m\geq 4, n=3$	0	0	$p^3=8$	0
$m\geq 4, n\geq 4$	0	0	0	0

Seien nun umgekehrt $m,n\in\mathbb{N}_0$, $m+n=r$, $c\in\mathfrak{o}_p$, für die (C1) und (C2) gelten, und seien $\mathfrak{N}_p := J(m,n,c)\mathfrak{M}_p J(m,n,c)^{-1}$ und $\mathfrak{H}_p := F_p\cap\mathfrak{N}_p$. Dann gilt $\mathfrak{O}_p\subset\mathfrak{H}_p$. Falls $\mathfrak{H}_p\subset\mathfrak{F}_p$, folgt mit den Lemmata 4.7.(ii) (sowie 4.5.(i) und 4.6) und 2.3.(iii)(iv): $[\mathfrak{F}_p:\mathfrak{H}_p]=[\mathfrak{M}_p:(\mathfrak{M}_p\cap\mathfrak{N}_p)]=p^r$, mit Lemma 4.1.(i) also $\mathfrak{H}_p=\mathfrak{G}(r)_p$. Ist $\mathfrak{H}_p\not\subset\mathfrak{F}_p$, folgt mit den Lemmata 4.1.(iv) und 4.5.(i): $\mathfrak{H}_p=\Pi\mathfrak{F}_p\Pi^{-1}$ und $\mathfrak{N}_p=\Pi\mathfrak{M}_p\Pi^{-1}$. O.B.d.A. sei $b\in\mathfrak{r}_p(1)$. Wegen $\Pi=J(1,1,b)$ können wir zusammenfassen:

Sei $[\mathfrak{F}_p:\mathfrak{G}_p]=p^r$. Dann ist $C(\mathfrak{G}_p)$ gleich der Summe der $C(m,n)$ mit $m,n\in\mathbb{N}_0$ und $m+n=r$, vermindert um 1, falls F_p zerfällt und $r=2$ ist.

□

Lemma 4.9. *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. Dann gilt:
Es gibt eine E_p-Maximalordnung $\mathfrak{E}_p$ und eine M_p-Maximalordnung $\mathfrak{N}_p$ mit $\mathfrak{E}_p\subset\mathfrak{N}_p$, so dass die $F(E,T)_p$-Ordnung $F(E,T)_p\cap\mathfrak{N}_p$ die Diskriminante $D^2d^2N(T)^2\mathbb{Z}_p$ hat.

Beweis. Wegen $\Phi_E(T) = T^*$ gibt es $\sigma, \alpha, \beta, \gamma \in \mathbb{Q}_p$ und Matrizeseinheiten 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 Matrizeseinheiten 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 $\left\{1, U := \begin{pmatrix} 0 & 1 \\ \tau d & 0 \end{pmatrix}, V := \begin{pmatrix} \sigma d & -i\sqrt{d} \\ \tau d i\sqrt{d} & -\sigma d \end{pmatrix}, W := \begin{pmatrix} i\sqrt{d} & 0 \\ 2\sigma d & -i\sqrt{d} \end{pmatrix} = (\sigma U + UV/d)/\tau\right\}$ eine $\mathbb{Z}_p$-Basis einer $F(E,T)_p$-Ordnung $\mathfrak{G}_p \subset \mathfrak{N}_p$ mit Diskriminante $16d^4N(T)^2\mathbb{Z}_p$ ist.
Falls $p = 2$ in k verzweigt oder $p \neq 2$ ist, sieht man leicht, dass $\mathfrak{G}_p = F(E,T)_p \cap \mathfrak{N}_p$ 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 $F(E,T)_p$-Ordnung $F(E,T)_p \cap \mathfrak{N}_p$, Die Diskriminante ist in diesem Fall also $d^4N(T)^2\mathbb{Z}_p$. □

5 Einbettung rationaler Quaternionenordnungen

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

Bemerkung: Sei F eine $\mathbb{Q}$-Quaternionenalgebra, und sei $\mathfrak{G}$ eine F-Ordnung. Dann gilt offenbar $\Delta(\mathfrak{G}) = \Sigma(F)\Lambda(\mathfrak{G})$, siehe auch die Bemerkungen zu den Definitionen 2.1, 3.1.

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 $\Lambda(\mathfrak{G}) \in N_{abs}(I)$.

(ii) Sei $\lambda \in \mathbb{N}$ teilerfremd zu $\Sigma_k(F)$, und sei $\lambda \in N_{abs}(I)$.
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 $\mathfrak{O}_p$. Nach den Sätzen 4.1, 4.2 gibt es eine F_p-Ordnung $\mathfrak{G}_p$ mit $\mathfrak{O}_p \subset \mathfrak{G}_p \subset \mathfrak{F}_p$ 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 $\mathfrak{G}_p \to \mathfrak{G}'_p$.

□

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) $\Lambda(\mathfrak{N} \cap \mathfrak{N}') = N_{abs}(N(\mathfrak{N}\mathfrak{N}'))^{-1}$.

(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 $\left(\dfrac{f\Lambda(\mathfrak{N} \cap \mathfrak{N}'), -d}{p}\right) = 1$ *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, und sei π ein Primelement in $\mathfrak{o}_\mathfrak{p}$.
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 2.3.(iv) und 2.3.(ii) ein $r \in \mathbb{N}_0$, so dass gilt: $[\mathfrak{N}_\mathfrak{p} : (\mathfrak{N} \cap \mathfrak{N}')_\mathfrak{p}] = N_{abs}(\pi\mathfrak{o}_\mathfrak{p})^r = N_{abs}(N(\mathfrak{N}\mathfrak{N}')_\mathfrak{p})^{-1}$.

(ii) $\mathfrak{A} := (\mathfrak{N}\mathfrak{M}\mathfrak{N}'\mathfrak{N})^{-1} = (\mathfrak{N}\mathfrak{M}\mathfrak{M}\mathfrak{N}'\mathfrak{N}'\mathfrak{N})^{-1}$ ist ein zweiseitiges ganzes $\mathfrak{N}$-Ideal und teilerfremd zu $\Sigma_k(F)$. Daher gibt es ein ganzes $\mathfrak{o}$-Ideal $\mathfrak{a}$ mit $\mathfrak{A} = \mathfrak{N}\mathfrak{a}$, siehe dazu etwa [5, Lemma 6.7.5]. Dann gilt $\mathfrak{a}^2 = N(\mathfrak{A}) = N(\mathfrak{N}'\mathfrak{N})^{-1}N(\mathfrak{M}\mathfrak{N}')^{-1}N(\mathfrak{N}\mathfrak{M})^{-1}$.
Nach (i) gilt also $\Lambda(\mathfrak{N}' \cap \mathfrak{N})\Lambda(\mathfrak{M} \cap \mathfrak{N}')\Lambda(\mathfrak{N} \cap \mathfrak{M}) = N_{abs}(\mathfrak{a})^2 \in \mathbb{Q}^{\times(2)}$.

(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 $\mathfrak{f} \in R$ gibt mit $\mathfrak{f}N(\mathfrak{N}\mathfrak{N}')^{-1} \in I^{(2)}H$.
Nach [1, Kapitel III, § 8, Sätze 6 und 7] gilt $\mathfrak{f}N(\mathfrak{N}\mathfrak{N}')^{-1} \in I^{(2)}H$ genau dann, wenn $N_{abs}(\mathfrak{f})\Lambda(\mathfrak{N} \cap \mathfrak{N}') = N_{abs}(\mathfrak{f}N(\mathfrak{N}\mathfrak{N}')^{-1}) \in N_{abs}(k^\times)$, nach [1, Kapitel I, § 7, Satz 1] (Minkowski-Hasse) also genau dann, wenn $\left(\dfrac{N_{abs}(\mathfrak{f})\Lambda(\mathfrak{N} \cap \mathfrak{N}'), -d}{p}\right) = 1$ für alle p.

Falls $\mathfrak{N}$ isomorph zu $\mathfrak{N}'$ ist, sei f der quadratfreie Anteil von $N_{abs}(\mathfrak{f})$. 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 $\mathfrak{f} \in R$ mit $f = N_{abs}(\mathfrak{f})$.

□

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) Sind $\mathfrak{N}$ eine M-Maximalordnung und $\mathfrak{F}$ eine F-Maximalordnung mit $F \cap \mathfrak{N} \subset \mathfrak{F}$, so gibt es genau eine M-Maximalordnung $\mathfrak{M}$ mit $\mathfrak{F} \subset \mathfrak{M}$ und $\Lambda(F \cap \mathfrak{N}) = \Lambda(\mathfrak{M} \cap \mathfrak{N})$.
Die Inklusion $\mathfrak{F} \hookrightarrow \mathfrak{M}$ induziert einen Isomorphismus $\mathfrak{F}/(F \cap \mathfrak{N}) \to \mathfrak{M}/(\mathfrak{M} \cap \mathfrak{N})$.

(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 4.7.(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 Satz 4.8.
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 4.7.(ii) genau eine M_p-Maximalordnung $\mathfrak{M}_p$ mit $\mathfrak{F}_p \subset \mathfrak{M}_p$ und $[\mathfrak{F}_p : (F_p \cap \mathfrak{N}_p)] = [\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)]$.
$\mathfrak{M}$ setzt sich eindeutig aus den lokalen Komponenten zusammen. Die Abbildung $\mathfrak{F}/(F \cap \mathfrak{N}) \to \mathfrak{M}/(\mathfrak{M} \cap \mathfrak{N})$ ist Isomorphismus, da für alle $p \neq \infty$ ein Isomorphismus.

(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 verzweigt oder zerlegt ist, dann ist $\mathfrak{F}_p = \mathfrak{F}'_p$, und nach Lemma 4.5.(ii) bzw. Lemma 4.6 gilt $\mathfrak{M}_p = \mathfrak{M}'_p$.
- Falls F an der Stelle p verzweigt ist und p in k träge ist, dann ist $\mathfrak{F}_p = \mathfrak{F}'_p$, und nach Lemma 4.5.(ii) gilt entweder $\mathfrak{M}_p = \mathfrak{M}'_p$ oder $[\mathfrak{M}_p : (\mathfrak{M} \cap \mathfrak{M}')_p] = p^2$.
- Falls F an der Stelle p zerfällt, gibt es nach Lemma 2.3.(i) 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 $[\mathfrak{M}_p : (\mathfrak{M} \cap \mathfrak{M}')_p] = p^{2r}$. (Falls $p\mathfrak{o} = \mathfrak{p}\overline{\mathfrak{p}}$, ist $[\mathfrak{M}_p : (\mathfrak{M} \cap \mathfrak{M}')_p] = [\mathfrak{M}_\mathfrak{p} : (\mathfrak{M} \cap \mathfrak{M}')_\mathfrak{p}][\mathfrak{M}_{\overline{\mathfrak{p}}} : (\mathfrak{M} \cap \mathfrak{M}')_{\overline{\mathfrak{p}}}] = p^{2r}$.)

□

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:
$\left(\dfrac{\Lambda(F \cap \mathfrak{N}) f \Lambda(\mathfrak{N} \cap \mathfrak{N}')\Lambda(F' \cap \mathfrak{N}'), -d}{p}\right) = 1.$
Insbesondere gilt: $\mathfrak{N}$ ist isomorph zu $\mathfrak{N}'$, falls $\Lambda(F \cap \mathfrak{N}) = \Lambda(F' \cap \mathfrak{N}')$.

Beweis. Ein Isomorphismus: $j : F' \to F$ 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 $\left(\dfrac{f\Lambda(j(\mathfrak{N}') \cap \mathfrak{N}'), -d}{p}\right) = 1$ 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:
$\left(\dfrac{\Sigma(F) e \Lambda(\mathfrak{L} \cap \mathfrak{N})\Sigma(E), -d}{p}\right) = \left(\dfrac{E}{p}\right)\left(\dfrac{F}{p}\right)$ *für alle Stellen p von $\mathbb{Q}$.*

Beweis. Nach Satz 3.4.(iii) gibt es ein $T \in M^\times$ mit $\Phi_E(T) = T^*$, so dass $F = F(E, T)$. O.B.d.A. sei $N(T) \in \mathbb{Z}$ und $S(T) \in 4\mathbb{Z}$.
Falls $S(T)^2 = 4N(T)$, gilt $N(T) \in \mathbb{Q}^{\times(2)}$. Nach Satz 3.4.(ii) ist F isomorph zu E, also $\Sigma(F) = \Sigma(E)$. 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 ist $\mathfrak{F} := J\mathfrak{E}J^{-1}$ eine F-Maximalordnung und $\mathfrak{L} := J\mathfrak{N}J^{-1}$ eine M-Maximalordnung mit $\mathfrak{F} \subset \mathfrak{L}$. Nach Lemma 5.4.(iii) gibt es ein $e \in \mathbb{N}$ mit $e \mid \Sigma_k(E)$ und $\left(\dfrac{e\Lambda(\mathfrak{L} \cap \mathfrak{N}), -d}{p}\right) = 1 = \left(\dfrac{E}{p}\right)\left(\dfrac{F}{p}\right)$ 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 Lemma 4.9 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 $D^2d^2N(T)^2\mathbb{Z}_p$.
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 $\mathbb{Q}$.
□

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 dasss für alle Stellen p von $\mathbb{Q}$ gilt:
$\left(\frac{\Delta(F \cap \mathfrak{M})f\Lambda(\mathfrak{M} \cap \mathfrak{M}')\Delta(F' \cap \mathfrak{M}'), -d}{p}\right) = \left(\frac{F}{p}\right)\left(\frac{F'}{p}\right)$.

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 $\Lambda(F \cap \mathfrak{M}) = \Lambda(\mathfrak{L}' \cap \mathfrak{M})$, und 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 $\Lambda(\mathfrak{L} \cap \mathfrak{N})\Lambda(\mathfrak{L} \cap \mathfrak{L}')\Lambda(\mathfrak{L}' \cap \mathfrak{M})\Lambda(\mathfrak{M} \cap \mathfrak{N}) \in \mathbb{Q}^{\times(2)}$, und 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 $\mathbb{Q}$, also $\left(\frac{\Delta(F \cap \mathfrak{M})e\Lambda(\mathfrak{M} \cap \mathfrak{N})\Sigma(E), -d}{p}\right) = \left(\frac{E}{p}\right)\left(\frac{F}{p}\right)$ für alle Stellen p von $\mathbb{Q}$. Entsprechend gibt es ein $e' \in \mathbb{N}$ mit $e' \mid \Sigma_k(E)$ und eine E-Maximalordnung $\mathfrak{E}'$, sowie eine M-Maximalordnung $\mathfrak{N}'$ mit $\mathfrak{E}' \subset \mathfrak{N}'$, so dass für alle Stellen p von $\mathbb{Q}$ gilt: $\left(\frac{\Delta(F' \cap \mathfrak{M}')e'\Lambda(\mathfrak{M}' \cap \mathfrak{N}')\Sigma(E), -d}{p}\right) = \left(\frac{E}{p}\right)\left(\frac{F'}{p}\right)$. Bezeichne f den quadratfreien Anteil von ee'. Die Behauptung folgt dann durch Multiplikation der beiden Gleichungen, denn nach Lemma 5.5.(iv) gilt $\Lambda(\mathfrak{N} \cap \mathfrak{N}') = \Lambda(E \cap \mathfrak{N})\Lambda(\mathfrak{N} \cap \mathfrak{N}')\Lambda(E \cap \mathfrak{N}') \in \mathbb{Q}^{\times(2)}$, und mit Lemma 5.4.(ii) folgt daraus $\Lambda(\mathfrak{M} \cap \mathfrak{M}')\Lambda(\mathfrak{M} \cap \mathfrak{N})\Lambda(\mathfrak{N} \cap \mathfrak{N}')\Lambda(\mathfrak{N}' \cap \mathfrak{M}') \in \mathbb{Q}^{\times(2)}$.
□

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 $\left(\frac{\Delta(F \cap \mathfrak{M})\Lambda(\mathfrak{M} \cap M_2(\mathfrak{o})), -d}{p}\right) = \left(\frac{F}{p}\right)$.

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

Beweis. Seien $F' = M_2(\mathbb{Q})$, $M = M_2(k)$ und $\mathfrak{M}' = M_2(\mathfrak{o})$. Damit gilt $\Sigma_k(F) = 1$ und $\Delta(F' \cap \mathfrak{M}') = 1$ sowie $\left(\frac{F'}{p}\right) = 1$ für alle Stellen p. Die Behauptung folgt mit Satz 5.8. □

6 Die nichtzyklischen endlichen Untergruppen

Definition 6.1.

(i) Bezeichne $P : SL_2(\mathbb{C}) \to PSL_2(\mathbb{C})$ *die kanonische Projektion. Für Untergruppen* $\Gamma \subset SL_2(\mathbb{C})$ *mit* $\{\pm 1\} \subset \Gamma$ *kürzen wir* $P\Gamma := P(\Gamma) = \Gamma/\{\pm 1\}$ *ab.*

(ii) Für einen Ring $R \subset M_2(\mathbb{C})$ *mit Eins sei* $\Gamma(R) := \{A \in R \mid N(A) = 1\}$

(iii) Für eine endliche Menge $\mathcal{G} \subset PSL_2(\mathbb{C})$ *seien* $F(\mathcal{G}) \subset M_2(\mathbb{C})$ *der von* $P^{-1}(\mathcal{G})$ *erzeugte* $\mathbb{Q}$*-Vektorraum und* $\mathfrak{F}(\mathcal{G})$ *der von* $P^{-1}(\mathcal{G})$ *erzeugte* $\mathbb{Z}$*-Modul.*

Bemerkung: Speziell ist $P\Gamma(M_2(\mathfrak{o})) = PSL_2(\mathfrak{o})$ eine Bianchi-Gruppe.

Für $2 \leq m \in \mathbb{N}$ bezeichne $\mathcal{D}_m \subset PSL_2(\mathbb{C})$ stets eine (projektive) m-Diedergruppe, und $\mathcal{T} \subset PSL_2(\mathbb{C})$ bezeichne stets eine (projektive) Tetraedergruppe. Dann ist $P^{-1}(\mathcal{D}_m)$ 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 Tetraedergruppe $\mathcal{T}$ enthält genau eine 2-Diedergruppe $\mathcal{D}_2$, und umgekehrt ist eine 2-Diedergruppe $\mathcal{D}_2$ Normalteiler in genau einer Tetraedergruppe $\mathcal{T}$. Wir fassen die bekannten Grundlagen in den Lemmata 6.2 und 6.3 zusammen:

Lemma 6.2. *Sei* $d \in \mathbb{N}$ *quadratfrei, und sei* $k = \mathbb{Q}(i\sqrt{d})$.
Sei M *eine* $\mathbb{Q}$*-Quaternionenalgebra oder eine* k*-Quaternionenalgebra.*
Ist $\mathcal{G} \subset P\Gamma(M)$ *eine nichttriviale endliche Gruppe, dann hat* $\mathcal{G}$ *die Ordnung* 2 *oder* 3*, oder* $\mathcal{G}$ *ist eine* 3*-Diedergruppe, Tetraedergruppe oder* 2*-Diedergruppe.*

Beweis. Sei $\mathcal{G}$ eine nichttriviale endliche Untergruppe von $P\Gamma(M)$, und sei $\mathcal{C}_m \subset \mathcal{G}$ eine zyklische Untergruppe der Ordnung $m > 1$. Dann ist $P^{-1}(\mathcal{C}_m)$ zyklisch und hat die Ordnung $2m$. Sei U ein erzeugendes Element von $P^{-1}(\mathcal{C}_m)$, und sei $\zeta \in \mathbb{C}$ eine primitive $2m$-te Einheitswurzel. Dann ist $S(U) = \zeta + \overline{\zeta} \in \mathfrak{o} \cap \mathbb{R} = \mathbb{Z}$. Daher muss $m = 2$ oder $m = 3$ sein. Nach [7, Chapter 4.4] ist $P^{-1}(\mathcal{G})$ also eine zyklische Gruppe der Ordnung 4 oder 6, oder eine binäre 3-Diedergruppe, binäre Tetraedergruppe oder binäre 2-Diedergruppe. □

Lemma 6.3. *Sei* $\mathcal{G}$ *eine* 3*-Diedergruppe* $\mathcal{D}_3$*, Tetraedergruppe* $\mathcal{T}$ *oder* 2*-Diedergruppe* $\mathcal{D}_2$*. Dann ist* $F(\mathcal{G})$ *eine* $\mathbb{Q}$*-Quaternionenalgebra,* $\mathfrak{F}(\mathcal{G})$ *ist eine* $F(\mathcal{G})$*-Ordnung, und es gilt* $P^{-1}(\mathcal{G}) = \Gamma(\mathfrak{F}(\mathcal{G})) = \mathfrak{F}(\mathcal{G})^\times$*. Im Einzelnen gilt:*

(i) $P^{-1}(\mathcal{D}_3)$ *wird von zwei Elementen* U, V *erzeugt, mit* $U^3 = -1$ *und* $VUV^{-1} = U^{-1}$. $\Sigma(F(\mathcal{D}_3)) = -3$ *und* $\Lambda(\mathfrak{F}(\mathcal{D}_3)) = 1$, *also* $\Delta(\mathfrak{F}(\mathcal{D}_3)) = -3$.

(ii) $P^{-1}(\mathcal{D}_2)$ *wird von zwei Elementen* U, V *erzeugt, mit* $U^2 = -1$ *und* $VUV^{-1} = U^{-1}$. *Falls* $\mathcal{D}_2 \subset \mathcal{T}$, *wird* $P^{-1}(\mathcal{T})$ *von* U, V *und* $W := (1 - U - V - UV)/2$ *erzeugt. Dann gilt* $F(\mathcal{D}_2) = F(\mathcal{T})$, $\Sigma(F(\mathcal{D}_2)) = \Sigma(F(\mathcal{T})) = -2$ *und* $\mathfrak{F}(\mathcal{D}_2) \subset \mathfrak{F}(\mathcal{T})$, $\Lambda(\mathfrak{F}(\mathcal{T})) = 1$, *also* $\Delta(\mathfrak{F}(\mathcal{T})) = -2$, *und* $\Lambda(\mathfrak{F}(\mathcal{D}_2)) = 2$, *also* $\Delta(\mathfrak{F}(\mathcal{D}_2)) = -4$.

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 $WV = UW$. Eine elementare Rechnung zeigt, dass $W = (1 - U - V - UV)/2$ gilt, 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.

Bei den Erzeugendenrelationen für $P^{-1}(\mathcal{D}_3)$ und $P^{-1}(\mathcal{D}_2)$ können wir die Gleichung $V^2 = -1$ weglassen, denn aus $V^2UV^{-2} = VU^{-1}V^{-1} = (VUV^{-1})^{-1} = U$ erhalten wir $V^2 \in \mathbb{C}[U] \cap \mathbb{C}[V] = \mathbb{C}$, wegen $V \notin \mathbb{C}$ also $S(V) = 0$ und $V^2 = -N(V) = -1$.
Wegen $N(F(\mathcal{G})^\times) \subset \mathbb{Q}^+$ ist $\mathfrak{F}(\mathcal{G})^\times = \Gamma(\mathfrak{F}(\mathcal{G}))$ endlich. Wegen $\mathcal{G} \subset P\Gamma(\mathfrak{F}(\mathcal{G}))$ folgt mit Lemma 6.2, dass $P\Gamma(\mathfrak{F}(\mathcal{G})) \in \{\mathcal{D}_3, \mathcal{T}, \mathcal{D}_2\}$. Falls $\mathcal{G} \in \{\mathcal{D}_3, \mathcal{T}\}$, ist also $\mathcal{G} = P\Gamma(\mathfrak{F}(\mathcal{G}))$. Falls $\mathcal{G} = \mathcal{D}_2$, gilt $W \notin \mathfrak{F}(\mathcal{D}_2)$, also $P\Gamma(\mathfrak{F}(\mathcal{D}_2)) \subsetneq P\Gamma(\mathfrak{F}(\mathcal{T})) = \mathcal{T}$ und $P\Gamma(\mathfrak{F}(\mathcal{D}_2)) = \mathcal{D}_2$. □

Satz 6.4. *Sei* $d \in \mathbb{N}$ *quadratfrei, und sei* $k = \mathbb{Q}(i\sqrt{d})$.
Seien $\mathcal{D}_3$ *eine* 3*-Diedergruppe und* $\mathcal{T}$ *eine Tetraedergruppe. Dann gilt:*

(i) Es gibt bis auf Isomorphie genau eine k*-Quaternionenalgebra* M *mit* $\mathcal{D}_3 \subset P\Gamma(M)$ *und bis auf Isomorphie genau eine* M*-Maximalordnung* $\mathfrak{M}$ *mit* $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$. *Genau dann gilt* $M \cong M_2(k)$, *wenn* $d \not\equiv 2 \pmod 3$.

(ii) Es gibt bis auf Isomorphie genau eine k-Quaternionenalgebra M mit $\mathcal{T} \subset P\Gamma(M)$ und bis auf Isomorphie genau eine M-Maximalordnung $\mathfrak{M}$ mit $\mathcal{T} \subset P\Gamma(\mathfrak{M})$. Genau dann gilt $M \cong M_2(k)$, wenn $d \not\equiv 7 \pmod 8$.

Bemerkung: Im Fall $M \cong M_2(k)$ leistet Satz 6.7 die genaue Typisierung von $\mathfrak{M}$.

Beweis. Sei M eine k-Quaternionenalgebra, und sei $\mathcal{G} = \mathcal{D}_3$ oder $\mathcal{G} = \mathcal{T}$.
$\mathcal{G} \subset P\Gamma(M)$ gilt genau dann, wenn M eine Erweiterung von $F(\mathcal{G})$ zur k-Algebra ist, was den Isomorphietyp von M festlegt. Der Isomorphietyp von $\mathfrak{M}$ ist eindeutig nach Satz 5.6. Nach Lemma 3.2.(ii) ist $M \cong M_2(k)$ genau dann, wenn $\Sigma_k(F(\mathcal{G})) = \Sigma_k(M_2(\mathbb{Q})) = 1$ gilt, also wenn die einzige endliche Verzweigungsstelle p von $F(\mathcal{G})$ in k nicht zerlegt ist,

(i) also wenn 3 in k nicht zerlegt ist, also wenn $-d \not\equiv 1 \pmod 3$.

(ii) also wenn 2 in k nicht zerlegt ist, also wenn $-d \not\equiv 1 \pmod 8$.

□

Wir behandeln in den Kapiteln 6 und 7 die maximalendlichen Untergruppen von $P\Gamma(\mathfrak{M})$. $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$ bzw. $\mathcal{T} \subset P\Gamma(\mathfrak{M})$ ist stets eine maximalendliche Untergruppe von $P\Gamma(\mathfrak{M})$. Ist aber $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$, so gibt es (genau) eine Tetraedergruppe $\mathcal{T}$ mit $\mathcal{D}_2 \subset \mathcal{T} \subset P\Gamma(M)$, und $\mathcal{D}_2$ ist genau dann maximalendliche Untergruppe von $P\Gamma(\mathfrak{M})$, wenn $\mathcal{T} \not\subset P\Gamma(\mathfrak{M})$.

Lemma 6.5. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung $\mathfrak{o}$.*
Sei $\mathcal{D}_2$ eine 2-Diedergruppe, und sei M eine k-Quaternionenalgebra mit $\mathcal{D}_2 \subset P\Gamma(M)$.

(i) Ist $\mathfrak{M}$ eine M-Maximalordnung, so gilt: Genau dann ist $\mathcal{D}_2$ eine maximalendliche Untergruppe von $P\Gamma(\mathfrak{M})$, 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-Ordnung, wenn $d \not\equiv 3 \pmod 4$.

Beweis. Wir kürzen $F := F(\mathcal{D}_2) = F(\mathcal{T})$ 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 $2 \in N_{abs}(I)$ gilt, also wenn 2 in k nicht zerlegt und nicht träge ist, also wenn $-d \not\equiv 1 \pmod 4$ gilt.

□

Satz 6.6. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Genau dann gibt es eine k-Quaternionenalgebra M und eine M-Maximalordnung $\mathfrak{M}$ mit einer maximalendlichen 2-Diedergruppe $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$, wenn $d \not\equiv 3 \pmod 4$.
In diesem Fall gilt $M \cong M_2(k)$, und $\mathfrak{M}$ ist bis auf Isomorphie eindeutig.

Beweis. Die erste Behauptung folgt mit Lemma 6.5.(i), Satz 5.5.(i) und Lemma 6.5.(ii), beziehungsweise umgekehrt mit Lemma 6.5.(ii), Satz 5.5.(ii) und Lemma 6.5.(i).
Die zweite Behauptung folgt wegen $d \not\equiv 7 \pmod 8$ mit Satz 6.4.(ii) und mit Satz 6.5. □

Satz 6.7. *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: $\left(\dfrac{-3\Lambda(\mathfrak{M} \cap M_2(\mathfrak{o})), -d}{p}\right) = 1.$

(ii) $P\Gamma(\mathfrak{M})$ *enthält genau dann eine Tetraedergruppe $\mathcal{T}$,*
wenn für alle Stellen $p \neq 2, \infty$ von $\mathbb{Q}$ gilt: $\left(\dfrac{-2\Lambda(\mathfrak{M} \cap M_2(\mathfrak{o})), -d}{p}\right) = 1.$

(iii) $P\Gamma(\mathfrak{M})$ *enthält genau dann eine maximalendliche 2-Diedergruppe $\mathcal{D}_2$,*
wenn für alle Stellen $p \neq 2, \infty$ von $\mathbb{Q}$ gilt: $\left(\dfrac{-\Lambda(\mathfrak{M} \cap M_2(\mathfrak{o})), -d}{p}\right) = 1.$

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 6.3.(i) ist dann $\left(\dfrac{-3\lambda, -d}{p}\right) = 1$ für alle $p \neq 3, \infty$.

Sei nun umgekehrt $\left(\dfrac{-3\lambda, -d}{p}\right) = 1$ für alle $p \neq 3, \infty$. Die Anzahl der Stellen p mit $\left(\dfrac{-3\lambda, -d}{p}\right) = -1$ ist gerade. Also ist $\left(\dfrac{-3\lambda, -d}{3}\right) = -1$, speziell $d \not\equiv 2 \pmod 3$.
Sei $\mathcal{D}_3'$ eine 3-Diedergruppe. Nach Satz 6.4.(i) gibt es eine $M_2(k)$-Maximalordnung $\mathfrak{M}'$ mit $\mathcal{D}_3' \subset P\Gamma(\mathfrak{M}')$ oder äquivalent mit $\mathfrak{F}(\mathcal{D}_3') = F(\mathcal{D}_3') \cap \mathfrak{M}'$. Dann gilt $\left(\dfrac{-3\Lambda(\mathfrak{M}' \cap M_2(\mathfrak{o})), -d}{p}\right) = 1$ für alle $p \neq 3, \infty$, also $= \left(\dfrac{-3\lambda, -d}{p}\right)$ für alle 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 also $\mathfrak{M}$ isomorph zu $\mathfrak{M}'$. Daher gibt es eine 3-Diedergruppe $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$.

(ii) folgt mit Lemma 6.3.(ii) und umgekehrt mit Satz 6.4.(ii) 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 Lemma 6.5.(i), Satz 5.9 und Lemma 6.3.(ii) ist dann $\left(\dfrac{-\lambda, -d}{p}\right) = 1$ für alle $p \neq 2, \infty$.

Sei nun umgekehrt $\left(\dfrac{-\lambda, -d}{p}\right) = 1$ für alle $p \neq 2, \infty$. Die Anzahl der Stellen p mit $\left(\dfrac{-\lambda, -d}{p}\right) = -1$ ist gerade. Also ist $\left(\dfrac{-\lambda, -d}{2}\right) = -1$ und speziell $d \not\equiv 7 \pmod 8$.
Falls $d \equiv 3 \pmod 8$, wäre 2 in k träge. Nach Lemma 5.4.(i) gilt $\lambda \in N_{abs}(I)$. Daher

wäre der quadratfreie Anteil von λ ungerade, Widerspruch. Also ist $d \not\equiv 3 \pmod 4$. Nach Satz 6.6 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 6.8. *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 maximalendliche 2-Diedergruppe $\mathcal{D}_2$, wenn $p \equiv 1 \pmod 4$ für alle Primteiler $p \neq 2$ von d.

Beweis. Nach Satz 6.7 gilt:

(i) $PSL_2(\mathfrak{o})$ enthält genau dann eine 3-Diedergruppe $\mathcal{D}_3$, wenn für alle Stellen $p \neq 3, \infty$ von $\mathbb{Q}$ gilt: $\left(\frac{-3, -d}{p}\right) = 1$.

(ii) $PSL_2(\mathfrak{o})$ enthält genau dann eine Tetraedergruppe $\mathcal{T}$, wenn für alle Stellen $p \neq 2, \infty$ von $\mathbb{Q}$ gilt: $\left(\frac{-2, -d}{p}\right) = 1$.

(iii) $PSL_2(\mathfrak{o})$ enthält genau dann eine maximalendliche 2-Diedergruppe $\mathcal{D}_2$, wenn für alle $p \neq 2, \infty$ gilt: $\left(\frac{-1, -d}{p}\right) = 1$.

Die Behauptung folgt dann jeweils durch Auswertung der Hilbertsymbole.

□

7 Konjugationsklassenanzahlen

Definition 7.1. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$. Sei $\mathcal{G}$ eine endliche Gruppe. Seien F eine $\mathbb{Q}$-Quaternionenalgebra und M eine Erweiterung von F zur k-Quaternionenalgebra. Seien $\mathfrak{G}$ eine F-Ordnung und $\mathfrak{N}$ eine M-Maximalordnung.*

(i) Bezeichne $\mu(\mathcal{G}, \mathfrak{N})$ die Anzahl der $P\Gamma(\mathfrak{N})$-Konjugationsklassen maximalendlicher Untergruppen $\mathcal{G}' \subset P\Gamma(\mathfrak{N})$ vom Isomorphietyp $\mathcal{G}$.

(ii) Bezeichne $B(\mathfrak{G}, \mathfrak{N})$ die Anzahl der $\mathfrak{N}^\times$-Konjugationsklassen optimaler Einbettungen $j : \mathfrak{G} \hookrightarrow \mathfrak{N}$, und $B_1(\mathfrak{G}, \mathfrak{N})$ die entsprechende Anzahl der $\Gamma(\mathfrak{N})$-Konjugationsklassen.

(iii) Für $\mathfrak{O} = \mathfrak{G}$ oder $\mathfrak{O} = \mathfrak{N}$ bezeichne $\mathcal{A}(\mathfrak{O})$ die Gruppe der Automorphismen von $\mathfrak{O}$ und $\mathcal{I}(\mathfrak{O}) \subset \mathcal{A}(\mathfrak{O})$ die Untergruppe der Konjugationen mit Elementen aus $\mathfrak{O}^\times$.

Bemerkung: Die Bezeichnungen $\mu(\mathcal{D}_3, \mathfrak{N})$, $\mu(\mathcal{T}, \mathfrak{N})$ und $\mu(\mathcal{D}_2, \mathfrak{N})$ entsprechen den in [4, § 22 und § 24] definierten Bezeichnungen $\mu_3(\mathfrak{N})$, $\mu_{\mathcal{T}}(\mathfrak{N}) = \mu_2^{\mathcal{T}}(\mathfrak{N})$ und $\mu_2^-(\mathfrak{N})$.

Lemma 7.2. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Diskriminante D. Seien F eine $\mathbb{Q}$-Quaternionenalgebra und M eine Erweiterung von F zur k-Quaternionenalgebra. Bezeichne t die Anzahl der verschiedenen Primteiler von D, bezeichne r die Anzahl der Primteiler von $\Sigma_k(F)$, und bezeichne S die Anzahl der $f \in \mathbb{N}$ mit $f \mid \Sigma_k(F)$, für die an allen Stellen p von $\mathbb{Q}$ gilt: $\left(\frac{f, -d}{p}\right) = 1$. Dann ist $S = 2^s$ für ein $s \in \mathbb{N}_0$ mit $s \leq r$.*
Ist $\mathfrak{M}$ eine M-Maximalordnung, dann gilt $[\mathcal{A}(\mathfrak{M}) : \mathcal{I}(\mathfrak{M})] = 2^{t+r+s-1}$.

Bemerkung: $(r - s)$ ist der Rang der $t \times r$-Matrix (h_{pq}) mit $h_{pq} := 1 - \left(\frac{q, -d}{p}\right)$,
wo p die verschiedenen Primteiler von D und q die Primteiler von $\Sigma_k(F)$ durchläuft.

Beweis. Bezeichne R die von den Verzweigungsstellen von M erzeugte $\mathfrak{o}$-Idealgruppe. Sei $j \in \mathcal{A}(\mathfrak{M})$. Dann gibt es ein $J \in M^\times$ mit $j(A) = JAJ^{-1}$ für alle $A \in \mathfrak{M}$. Dann ist $\mathfrak{J} := \mathfrak{M}J$ ein zweiseitiges $\mathfrak{M}$-Ideal ist mit $\mathfrak{j} := N(\mathfrak{J}) \in RI^{(2)} \cap H$. Ist umgekehrt $\mathfrak{j} \in RI^{(2)} \cap H$, dann gibt es genau ein zweiseitiges $\mathfrak{M}$-Ideal $\mathfrak{J}$ mit $N(\mathfrak{J}) = \mathfrak{j}$ und ein $J \in M^\times$ mit $\mathfrak{J} = \mathfrak{M}J$. Die Zuordnungsvorschrift $j : A \mapsto JAJ^{-1}$ definiert dann ein $j \in \mathcal{A}(\mathfrak{M})$. Zum Beweis siehe [5, Corollary 2.9.9, Lemma 6.7.5 und Theorem 7.7.7].
Die Zuordnungsvorschrift $j \mapsto J$ bestimmt J eindeutig bis auf einen Faktor $a \in k^\times$.
Wegen $N(a) = a^2$ induziert die Zuordnungsvorschrift $j \mapsto \mathfrak{j}$ also einen surjektiven Homomorphismus $\mathcal{A}(\mathfrak{M}) \to (RI^{(2)} \cap H)/H^{(2)}$, und mit [5, Lemma 6.7.5] sieht man leicht ein, dass der Kern der Abbildung gleich $\mathcal{I}(\mathfrak{M})$ ist. Also gilt $[\mathcal{A}(\mathfrak{M}) : \mathcal{I}(\mathfrak{M})] = [(RI^{(2)} \cap H) : H^{(2)}]$.
Wir formen die Terme in $[\mathcal{A}(\mathfrak{M}) : \mathcal{I}(\mathfrak{M})] = [(RI^{(2)} \cap H) : (I^{(2)} \cap H)][(I^{(2)} \cap H) : H^{(2)}]$ um.
Die Einbettung $I^{(2)} \hookrightarrow I^{(2)}H$ induziert einen Isomorphismus $I^{(2)}/(I^{(2)} \cap H) \to I^{(2)}H/H$. Also gilt $[I^{(2)} : (I^{(2)} \cap H)] = [I^{(2)}H : H]$ und ebenso $[RI^{(2)} : (RI^{(2)} \cap H)] = [RI^{(2)}H : H]$. Daraus folgt $[RI^{(2)} : (RI^{(2)} \cap H)] = [RI^{(2)}H : I^{(2)}H][(I^{(2)} : (I^{(2)} \cap H)]$.
Wegen $[RI^{(2)} : I^{(2)}][(I^{(2)} : (I^{(2)} \cap H)] = [RI^{(2)} : (RI^{(2)} \cap H)][(RI^{(2)} \cap H) : (I^{(2)} \cap H)]$ gilt also $[(RI^{(2)} \cap H) : (I^{(2)} \cap H)] = [RI^{(2)} : I^{(2)}][RI^{(2)}H : I^{(2)}H]^{-1} = 2^{2r}[RI^{(2)}H : I^{(2)}H]^{-1}$.
Für die Umformung des Terms $[(I^{(2)} \cap H) : H^{(2)}]$ bemerken wir, dass die Zuordnungsvorschrift $\mathfrak{a} \mapsto \mathfrak{a}^2$ für $\mathfrak{a} \in I$ einen Isomorphismus $I/H \to I^{(2)}/H^{(2)}$ induziert. Also gilt $[I : H] = [I^{(2)} : H^{(2)}]$ und $[I : I^{(2)}H][I^{(2)}H : H] = [I^{(2)} : (I^{(2)} \cap H)][(I^{(2)} \cap H) : H^{(2)}]$.
Wegen $[I^{(2)} : (I^{(2)} \cap H)] = [I^{(2)}H : H]$ gilt also $[(I^{(2)} \cap H) : H^{(2)}] = [I : I^{(2)}H] = 2^{t-1}$.
Wir müssen jetzt also noch zeigen, dass $2^r = S[RI^{(2)}H : I^{(2)}H]$ gilt.
Wir wählen ein ganzes $\mathfrak{r} \in I$ mit $N_{abs}(\mathfrak{r}) = \Sigma_k(F)$. Sei $\mathcal{R}$ die Menge der ganzen $\mathfrak{a} \in I$ mit $\mathfrak{a} \mid \mathfrak{r}$. Für $\mathfrak{a}, \mathfrak{a}' \in \mathcal{R}$ bezeichne $ggT(\mathfrak{a}, \mathfrak{a}') \in I$ den größten gemeinsamen Teiler. Die Verknüpfungsvorschrift $\mathfrak{a} \times \mathfrak{a}' := \mathfrak{a}\mathfrak{a}'ggT(\mathfrak{a}, \mathfrak{a}')^{-2}$ definiert eine Gruppenstruktur auf $\mathcal{R}$, und die Einbettung $\mathcal{R} \hookrightarrow RI^{(2)}H$ erzeugt einen surjektiven Homomorphismus $\mathcal{R} \to RI^{(2)}H/I^{(2)}H$, denn für alle Primteiler $\mathfrak{p} \in I$ von $\Sigma_k(F)$ gilt $\mathfrak{p}^2 \in I^{(2)}$ und $\mathfrak{p}\overline{\mathfrak{p}} \in H$.
$\mathcal{R}$ enthält 2^r Elemente. Wir müssen zeigen, dass $\mathcal{R} \cap I^{(2)}H$ genau S Elemente enthält.

Die Zuordnungsvorschrift $\mathfrak{f} \mapsto N_{abs}(\mathfrak{f})$ induziert eine Bijektion zwischen $\mathcal{R}$ und der Menge der $f \in \mathbb{N}$ mit $f \mid \Sigma_k(F)$. Nach [1, Kapitel III, § 8, Sätze 6, 7 und Kapitel I, § 7, Satz 1] gilt $\mathfrak{f} \in I^{(2)}H$ genau dann, wenn $\left(\frac{N_{abs}(\mathfrak{f}), -d}{p}\right) = 1$ an allen Stellen p von $\mathbb{Q}$.

□

Satz 7.3. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Seien F eine $\mathbb{Q}$-Quaternionenalgebra und M eine Erweiterung von F zur k-Quaternionenalgebra. Seien $\mathfrak{G}$ eine F-Ordnung und $\mathfrak{N}$ eine M-Maximalordnung mit $\mathfrak{G} = F \cap \mathfrak{N}$. Bezeichne $C(\mathfrak{G})$ die Anzahl der M-Maximalordnungen $\mathfrak{N}'$ mit $\mathfrak{G} = F \cap \mathfrak{N}'$. Dann gilt:

(i) *$C(\mathfrak{G})$ ist das Produkt der in Satz 4.8 angegebenen $C(\mathfrak{G}_p)$, wobei p die Primteiler von $\Lambda(\mathfrak{G})$ mitsamt der in k trägen Verzweigungsstellen von F durchläuft.*
Ist $\mathfrak{L}$ eine M-Maximalordnung mit $\mathfrak{G} = F \cap \mathfrak{L}$, dann ist $\mathfrak{L}$ isomorph zu $\mathfrak{N}$.

(ii) $B(\mathfrak{G}, \mathfrak{N}) = C(\mathfrak{G})[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})]$

(iii) $B_1(\mathfrak{G}, \mathfrak{N}) = 2B(\mathfrak{G}, \mathfrak{N})$

Beweis.

(i) klar, bzw. siehe Satz 5.6.

(ii) Ist $\mathfrak{L}$ eine M-Maximalordnung mit $\mathfrak{G} = F \cap \mathfrak{L}$, so gibt es einen Automorphismus j von M mit $\mathfrak{N} = j(\mathfrak{L})$. Dann gilt $j(\mathfrak{G}) = j(F) \cap \mathfrak{N}$. Für jede M-Maximalordnung $\mathfrak{L}$ mit $\mathfrak{G} = F \cap \mathfrak{L}$ wählen wir einen Automorphismus $j_{\mathfrak{L}}$ von M mit $\mathfrak{N} = j_{\mathfrak{L}}(\mathfrak{L})$.
Eine Einbettung $j : \mathfrak{G} \hookrightarrow \mathfrak{N}$ mit $j(\mathfrak{G}) = j(F) \cap \mathfrak{N}$ ist zu einem Automorphismus von M fortsetzbar. Mit $\mathfrak{L} := j^{-1}(\mathfrak{N})$ gilt $\mathfrak{G} = F \cap \mathfrak{L}$ und $a(j) := j \circ j_{\mathfrak{L}}^{-1} \in \mathcal{A}(\mathfrak{N})$.
Die Abbildung mit Zuordnungsvorschrift $j \mapsto (\mathfrak{L}, a(j))$ ist injektiv. Sind umgekehrt eine M-Maximalordnung $\mathfrak{L}$ mit $\mathfrak{G} = F \cap \mathfrak{L}$ und ein $a \in \mathcal{A}(\mathfrak{N})$ gegeben, dann ist $j := a \circ j_{\mathfrak{L}}$ ein Automorphismus von M, und seine Einschränkung auf $\mathfrak{G}$ induziert eine Einbettung $j : \mathfrak{G} \hookrightarrow \mathfrak{N}$ mit $j(\mathfrak{G}) = j(F) \cap \mathfrak{N}$.
Zwei Einbettungen $j, j' : \mathfrak{G} \hookrightarrow \mathfrak{N}$ mit $j(\mathfrak{G}) = j(F) \cap \mathfrak{N}$ und $j'(\mathfrak{G}) = j'(F) \cap \mathfrak{N}$ sind genau dann $\mathfrak{N}^\times$-konjugiert, wenn $j' = a \circ j$ für ein $a \in \mathcal{I}(\mathfrak{N})$, also genau dann, wenn $j'^{-1}(\mathfrak{N}) = j^{-1}(\mathfrak{N})$ und $a(j') \circ a(j)^{-1} \in \mathcal{I}(\mathfrak{N})$. Damit folgt die Behauptung.

(iii) Sei $\mathcal{I}_1(\mathfrak{N})$ die Gruppe der Konjugationen von $\mathfrak{N}$ mit Elementen aus $\Gamma(\mathfrak{N})$. Wie in (ii) folgt $B_1(\mathfrak{G}, \mathfrak{N}) = C(\mathfrak{G})[\mathcal{A}(\mathfrak{N}) : \mathcal{I}_1(\mathfrak{N})]$. Also ist zu zeigen: $[\mathcal{I}(\mathfrak{N}) : \mathcal{I}_1(\mathfrak{N})] = 2$.
Ist $a \in \mathcal{I}(\mathfrak{N})$, so gibt es ein $X \in \mathfrak{N}^\times$ mit $a(A) = XAX^{-1}$ für alle $A \in \mathfrak{N}$. Die Zuordnungsvorschrift $a \mapsto X$ induziert Isomorphismen $\mathcal{I}(\mathfrak{N}) \to \mathfrak{N}^\times/\mathfrak{o}^\times$ und $\mathcal{I}_1(\mathfrak{N}) \to \Gamma(\mathfrak{N})/\{\pm 1\}$. Nach [5, Theorem 11.6.1] gilt $N(\mathfrak{N}^\times) = \mathfrak{o}^\times$, also induziert die Norm eine exakte Sequenz $\{1\} \to \Gamma(\mathfrak{N})/\{\pm 1\} \to \mathfrak{N}^\times/\mathfrak{o}^\times \to \mathfrak{o}^\times/\mathfrak{o}^{\times(2)} \to \{1\}$.

□

Lemma 7.4. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Sei M eine k-Quaternionenalgebra, und sei $\mathfrak{N}$ eine M-Maximalordnung.
Sei $\mathcal{G} \subset P\Gamma(\mathfrak{N})$ eine nichtzyklische maximalendliche Untergruppe.

(i) Dann ist $\mu(\mathcal{G},\mathfrak{N}) = B_1(\mathfrak{F}(\mathcal{G}),\mathfrak{N})[\mathcal{A}(\mathfrak{F}(\mathcal{G})) : \mathcal{I}(\mathfrak{F}(\mathcal{G}))]^{-1}$

(ii) Ist $\mathcal{G}$ *eine* 3*-Diedergruppe oder Tetraedergruppe, dann ist* $[\mathcal{A}(\mathfrak{F}(\mathcal{G})) : \mathcal{I}(\mathfrak{F}(\mathcal{G}))] = 2$. *Ist* $\mathcal{G}$ *eine* 2*-Diedergruppe, dann ist* $[\mathcal{A}(\mathfrak{F}(\mathcal{G})) : \mathcal{I}(\mathfrak{F}(\mathcal{G}))] = 6$.

Beweis. Nach Lemma 6.3 gilt $\mathfrak{F}(\mathcal{G})^\times = \Gamma(\mathfrak{F}(\mathcal{G})) = P^{-1}(\mathcal{G})$.

(i) Wegen $P^{-1}(\mathcal{G}) = \mathfrak{F}(\mathcal{G})^\times$ induziert die Zuordnungsvorschrift $\mathcal{G}' \mapsto \mathfrak{F}(\mathcal{G}')$ eine Bijektion zwischen den maximalendlichen Untergruppen $\mathcal{G}' \subset P\Gamma(\mathfrak{N})$ vom Isomorphietyp $\mathcal{G}$ und den optimal eingebetteten Ordnungen $\mathfrak{F}' \subset \mathfrak{N}$ vom Isomorphietyp $\mathfrak{F}(\mathcal{G})$.
Zwei solche Gruppen $\mathcal{G}'$, $\mathcal{G}''$ sind genau dann $P\Gamma(\mathfrak{N})$-konjugiert, wenn $P^{-1}(\mathcal{G}')$ und $P^{-1}(\mathcal{G}'')$ $\Gamma(\mathfrak{N})$-konjugiert sind, also wenn $\mathfrak{F}(\mathcal{G}')$ und $\mathfrak{F}(\mathcal{G}'')$ $\Gamma(\mathfrak{N})$-konjugiert sind.

Also ist $\mu(\mathcal{G},\mathfrak{N}) = B(\mathfrak{F}(\mathcal{G}),\mathfrak{N}))[\mathcal{A}'(\mathcal{G}) : \mathcal{I}'(\mathcal{G})]^{-1}$, wo $\mathcal{A}'(\mathcal{G})$ die Gruppe der Einbettungen $j : \mathfrak{F}(\mathcal{G}) \hookrightarrow \mathfrak{N}$ mit $j(\mathfrak{F}(\mathcal{G})) = \mathfrak{F}(\mathcal{G})$ ist, und $\mathcal{I}'(\mathcal{G})$ die Untergruppe der $j \in \mathcal{A}'(\mathcal{G})$, die durch Konjugation mit einem Element aus $\Gamma(\mathfrak{N})$ erzeugt werden.

Offenbar gilt $\mathcal{A}'(\mathcal{G}) \subset \mathcal{A}(\mathfrak{F}(\mathcal{G}))$ und $\mathcal{I}(\mathfrak{F}(\mathcal{G})) \subset \mathcal{I}'(\mathcal{G})$. Ein $j \in \mathcal{A}(\mathfrak{F}(\mathcal{G}))$ induziert genau einen Automorphismus von M mit $j(\mathfrak{F}(\mathcal{G})) = \mathfrak{F}(\mathcal{G})$, also gilt $\mathcal{A}'(\mathcal{G}) = \mathcal{A}(\mathfrak{F}(\mathcal{G}))$. Falls $J \in \Gamma(\mathfrak{N})$ mit $J\mathfrak{F}(\mathcal{G})J^{-1} = \mathfrak{F}(\mathcal{G})$, so ist wegen $P^{-1}(\mathcal{G}) = \Gamma(\mathfrak{F}(\mathcal{G}))$ auch $JP^{-1}(\mathcal{G})J^{-1} = P^{-1}(\mathcal{G})$. Weil $P^{-1}(\mathcal{G}) \subset \Gamma(\mathfrak{N})$ maximalendlich, also sein eigener Normalisator in $\Gamma(\mathfrak{N})$ ist, folgt $J \in P^{-1}(\mathcal{G}) = \mathfrak{F}(\mathcal{G})^\times$. Daher gilt $\mathcal{I}'(\mathcal{G}) = \mathcal{I}(\mathfrak{F}(\mathcal{G}))$.

(ii) $\mathfrak{F}(\mathcal{G})^\times$ hat das Zentrum $\{\pm 1\}$, also ist $\mathcal{I}(\mathfrak{F}(\mathcal{G})) \cong \mathfrak{F}(\mathcal{G})^\times/\{\pm 1\} \cong \mathcal{G}$.

$\mathfrak{F}(\mathcal{D}_3)^\times = P^{-1}(\mathcal{D}_3)$ wird erzeugt von U und V mit $U^3 = -1$ und $VUV^{-1} = U^{-1}$.
$j \in \mathcal{A}(\mathfrak{F}(\mathcal{D}_3))$ ist durch $j(U) \in \{U, U^{-1}\}$, $j(V) \in \{\pm V, \pm UV, \pm U^{-1}V\}$ definierbar.
$\mathcal{A}(\mathfrak{F}(\mathcal{D}_3))$ enthält also 12 Elemente, und $\mathcal{I}(\mathfrak{F}(\mathcal{D}_3)) \cong \mathcal{D}_3 \cong \mathcal{S}_3$ enthält 6 Elemente.

$\mathfrak{F}(\mathcal{D}_2)^\times = P^{-1}(\mathcal{D}_2)$ wird erzeugt von U und V mit $U^2 = -1$ und $VUV^{-1} = U^{-1}$.
$j \in \mathcal{A}(\mathfrak{F}(\mathcal{D}_2))$ ist durch $j(U)$ und $j(V)$ definierbar. Dafür gibt es 6×4 Möglichkeiten.
$\mathcal{A}(\mathfrak{F}(\mathcal{D}_2))$ enthält also 24 Elemente, und $\mathcal{I}(\mathfrak{F}(\mathcal{D}_2)) \cong \mathcal{D}_2 \cong \mathcal{V}_4$ enthält 4 Elemente.

$\mathfrak{F}(\mathcal{T})^\times = P^{-1}(\mathcal{T}) \supset P^{-1}(\mathcal{D}_2)$ wird erzeugt von U, V, und $W = (1 - U - V - UV)$.
$j \in \mathcal{A}(\mathfrak{F}(\mathcal{T}))$ ist durch $j(U)$ und $j(V)$ definierbar. Dafür gibt es 6×4 Möglichkeiten.
$\mathcal{A}(\mathfrak{F}(\mathcal{T}))$ enthält also 24 Elemente, und $\mathcal{I}(\mathfrak{F}(\mathcal{T})) \cong \mathcal{T} \cong \mathcal{A}_4$ enthält 12 Elemente.

□

Satz 7.5. *Sei* $d \in \mathbb{N}$ *quadratfrei, sei* $k = \mathbb{Q}(i\sqrt{d})$ *mit Diskriminante* D*, und bezeichne* t *die Anzahl der verschiedenen Primteiler von* D.
Sei M *eine* k*-Quaternionenalgebra, und sei* $\mathfrak{N}$ *eine* M*-Maximalordnung.*

(i) Sei $\mathcal{D}_3 \subset P\Gamma(\mathfrak{N})$ *eine* 3*-Diedergruppe. Dann gilt:*

- *Falls* $d \equiv 0 \pmod 3$*, ist* $\mu(\mathcal{D}_3,\mathfrak{N}) = 2^{t-1}$.
- *Falls* $d \equiv 1 \pmod 3$*, ist* $\mu(\mathcal{D}_3,\mathfrak{N}) = 2^t$.
- *Falls* $d \equiv 2 \pmod 3$*, ist*
  - $\mu(\mathcal{D}_3,\mathfrak{N}) = 2^t$*, falls* d *einen Primteiler* $p \equiv \pm 5 \pmod{12}$ *hat*

– $\mu(\mathcal{D}_3, \mathfrak{N}) = 2^{t+1}$, *falls* $p \equiv \pm 1 \pmod{12}$ *für alle Primteiler* $p \neq 2$ *von* d

(ii) Sei $\mathcal{T} \subset P\Gamma(\mathfrak{N})$ *eine Tetraedergruppe. Dann gilt:*

- *Falls* $d \not\equiv 3 \pmod 4$, *ist* $\mu(\mathcal{T}, \mathfrak{N}) = 2^{t-1}$.
- *Falls* $d \equiv 3 \pmod 8$, *ist* $\mu(\mathcal{T}, \mathfrak{N}) = 2^t$.
- *Falls* $d \equiv 7 \pmod 8$, *ist*
  - $\mu(\mathcal{T}, \mathfrak{N}) = 2^t$, *falls* d *einen Primteiler* $p \equiv \pm 3 \pmod 8$ *hat*
  - $\mu(\mathcal{T}, \mathfrak{N}) = 2^{t+1}$, *falls* $p \equiv \pm 1 \pmod 8$ *für alle Primteiler* p *von* d

(iii) Sei $\mathcal{D}_2 \subset P\Gamma(\mathfrak{N})$ *eine maximalendliche* 2*-Diedergruppe. Dann ist* $d \not\equiv 3 \pmod 4$ *und* $\mu(\mathcal{D}_2, \mathfrak{N}) = 2^{t-1}$.

Bemerkung: Satz 7.5 geht schon aus [4, Sätze 20.39 und 26.12] hervor, wird dort allerdings unter Rückgriff auf $P\Gamma(\mathfrak{N})$-Konjugationsklassen zyklischer Untergruppen bewiesen.

Beweis. Wir berechnen $\mu(\mathcal{G}, \mathfrak{N})$ mit Lemma 7.4 mithilfe von Satz 7.3. Zur Berechnung der Faktoren $C(\mathfrak{F}(\mathcal{G}))$ und $[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})]$ greifen wir auf Satz 4.8 und Lemma 7.2 zurück.

(i) $\mu(\mathcal{D}_3, \mathfrak{N}) = C(\mathfrak{F}(\mathcal{D}_3))[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})]$. Es ist $\Lambda(\mathfrak{F}(\mathcal{D}_3)) = 1$ und $F(\mathcal{D}_3)_3 \ncong M_2(\mathbb{Q}_3)$.
Falls $d \equiv 1 \pmod 3$, ist 3 träge in k, also $C(\mathfrak{F}(\mathcal{D}_3)) = 2$. Sonst ist $C(\mathfrak{F}(\mathcal{D}_3)) = 1$.
Falls $d \not\equiv 2 \pmod 3$, ist $\Sigma_k(F(\mathcal{D}_3)) = 1$. Daher gilt dann $[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})] = 2^{t-1}$.
Falls $d \equiv 2 \pmod 3$, ist $\Sigma_k(F(\mathcal{D}_3)) = 3$. Gilt in diesem Fall $\left(\frac{3, -d}{p}\right) = 1$ an allen Stellen p von $\mathbb{Q}$, dann ist $[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})] = 2^{t+1}$, sonst ist $[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})] = 2^t$. Die Auswertung der Hilbertsymbole liefert hier: $\left(\frac{3, -d}{p}\right) = 1$ an allen Stellen p von $\mathbb{Q}$ ist äquivalent zu $p \equiv \pm 1 \pmod{12}$ für alle Primteiler $p \neq 2$ von d.

(ii) $\mu(\mathcal{T}, \mathfrak{N}) = C(\mathfrak{F}(\mathcal{T}))[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})]$. Es ist $\Lambda(\mathfrak{F}(\mathcal{T})) = 1$ und $F(\mathcal{T})_2 \ncong M_2(\mathbb{Q}_2)$.
Falls $d \equiv 3 \pmod 8$, ist 2 träge in k, also $C(\mathfrak{F}(\mathcal{T})) = 2$. Sonst ist $C(\mathfrak{F}(\mathcal{T})) = 1$.
Falls $d \not\equiv 7 \pmod 8$, ist $\Sigma_k(F(\mathcal{T})) = 1$. Daher gilt dann $[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})] = 2^{t-1}$.
Falls $d \equiv 7 \pmod 8$, ist $\Sigma_k(F(\mathcal{T})) = 2$. Gilt in diesem Fall $\left(\frac{2, -d}{p}\right) = 1$ an allen Stellen p von $\mathbb{Q}$, dann ist $[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})] = 2^{t+1}$, sonst ist $[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})] = 2^t$. Die Auswertung der Hilbertsymbole liefert hier: $\left(\frac{2, -d}{p}\right) = 1$ an allen Stellen p von $\mathbb{Q}$ ist äquivalent zu $p \equiv \pm 1 \pmod 8$ für alle Primteiler p von d.

(iii) $\mu(\mathcal{D}_2, \mathfrak{N}) = C(\mathfrak{F}(\mathcal{D}_2))[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})]/3$. Es ist $\Lambda(\mathfrak{F}(\mathcal{D}_2)) = 2$ und $F(\mathcal{D}_2)_2 \ncong M_2(\mathbb{Q}_2)$.
Nach Satz 6.6 ist $d \not\equiv 3 \pmod 4$, also ist 2 verzweigt in k, also gilt $C(\mathfrak{F}(\mathcal{D}_2)) = 3$ und $\Sigma_k(F(\mathcal{D}_2)) = 1$. Daher gilt $[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})] = 2^{t-1}$.

□

8 Die Durchschnitte von nichtzyklischen endlichen Gruppen

Lemma 8.1. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung $\mathfrak{o}$.*
Sei $d \not\equiv 3 \pmod 4$ und sei $d \neq 1$. Dann ist 2 verzweigt in k. Sei $\pi \in \mathfrak{o}_2$ ein Primelement.
Sei M eine k-Quaternionenalgebra, und sei $\mathcal{D}_2 \subset P\Gamma(M)$ eine 2-Diedergruppe.
Seien U, V Erzeugende von $P^{-1}(\mathcal{D}_2)$ mit $U^2 = -1$ und $VUV^{-1} = U^{-1}$. Dann gilt:

(i) Seien $\mathcal{T} \subset P\Gamma(M)$ die Tetraedergruppe mit $\mathcal{D}_2 \subset \mathcal{T}$ und $\mathfrak{M}$ die M-Maximalordnung mit $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{M}$. Für alle $X \in \{U, V, UV\}$ gilt dann $k(X)_2 \cap \mathfrak{M}_2 = \mathfrak{o}_2[(1+X)/\pi]$.

(ii) Sei $\mathfrak{N}$ eine M-Maximalordnung. Sei $\mathcal{D}_2 \subset P\Gamma(\mathfrak{N})$ maximalendliche Untergruppe. Für genau ein $X \in \{U, V, UV\}$ ist dann $k(X) \cap \mathfrak{N}$ die Hauptordnung von $k(X)$.

(a) $k(X) \cap \mathfrak{N} = \mathfrak{o}[(i\sqrt{d} + X)/2]$, falls $d \equiv 1 \pmod 4$.
(b) $(k(X) \cap \mathfrak{N})_2 = \mathfrak{o}_2[(1+X)/\pi]$, falls $d \equiv 2 \pmod 4$.

Für $Y \in \{U, V, UV\}$ mit $Y \neq X$ gilt dann $k(Y) \cap \mathfrak{N} = \mathfrak{o}[Y]$.

(iii) Es gibt genau eine M-Maximalordnung $\mathfrak{N}$ mit $\mathcal{D}_2 \subset P\Gamma(\mathfrak{N})$, für die $k(U) \cap \mathfrak{N} = \mathfrak{o}[U]$ und $k(V) \cap \mathfrak{N} = \mathfrak{o}[V]$ gilt. $\mathcal{D}_2$ ist dann maximalendliche Untergruppe von $P\Gamma(\mathfrak{N})$.

Beweis. Nach Satz 4.8 gibt es genau eine M-Maximalordnung $\mathfrak{M}$ mit $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{M}$ und genau drei M-Maximalordnungen $\mathfrak{N}$ mit $\mathfrak{F}(\mathcal{D}_2) = F(\mathcal{D}_2) \cap \mathfrak{N}$.

(i) Sei $W = (1 - U - V - UV) \in P^{-1}(\mathcal{T})$. Wir definieren einen $\mathfrak{o}$-Modul $\mathfrak{M}$ wie folgt: Sei $\{1, (1+U)/\pi, (1+V)/\pi, W\}$ eine $\mathfrak{o}_2$-Basis von $\mathfrak{M}_2$, und für alle endlichen Stellen $p \neq 2$ von $\mathbb{Q}$ sei $\{1, U, V, W\}$ eine $\mathfrak{o}_p$-Basis von $\mathfrak{M}_p$. Man prüft elementar nach, dass $\mathfrak{M}$ eine M-Maximalordnung mit $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{M}$ ist und die angegebene Gleichung gilt.

Zum Beweis von (ii) und (iii) sei $\mathfrak{N}$ der $\mathfrak{o}$-Modul mit $\mathfrak{o}$-Basis:

(a) entweder $\{1, U, (i\sqrt{d}U + V)/2, (i\sqrt{d} + UV)/2\}$
oder $\{1, V, (i\sqrt{d}V + UV)/2, (i\sqrt{d} + U)/2\}$
oder $\{1, UV, (i\sqrt{d}UV + U)/2, (i\sqrt{d} + V)/2\}$.

(b) entweder $\{1, U, (i\sqrt{d} + U + V)/2, (1 + i\sqrt{d}U + UV)/2\}$
oder $\{1, V, (i\sqrt{d} + V + UV)/2, (1 + i\sqrt{d}V + U)/2\}$
oder $\{1, UV, (i\sqrt{d} + UV + U)/2, (1 + i\sqrt{d}UV + V)/2\}$.

Man prüft elementar, dass $\mathfrak{N}$ eine M-Maximalordnung mit $\mathfrak{F}(\mathcal{D}_2) = F(\mathcal{D}_2) \cap \mathfrak{N}$ ist. Existenz und Eindeutigkeit von X bzw. $\mathfrak{N}$ sowie die Aussage für Y folgen dann leicht. □

Lemma 8.2. *Sei $d \in \mathbb{N}$ quadratfrei, $d \neq 1$, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung $\mathfrak{o}$.*
Sei $U \in SL_2(\mathbb{C})$ mit $U^2 = -1$, und sei $K := k(U)$ mit Hauptordnung $\mathfrak{O}$.

(i) Sei $k_+ := \mathbb{Q}(i\sqrt{d}U)$ mit Hauptordnung $\mathfrak{o}_+$, und sei $\mathcal{U} \subset \Gamma(\mathfrak{o}[U])$ die von U erzeugte Untergruppe. Dann ist $\mathcal{U}$ ist die Gruppe der Einheitswurzeln in K mit Norm 1, und es gilt $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] \leq 2$. Weiterhin gilt $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] = 2$ genau dann, wenn es $x, y \in \mathbb{Z}$ gibt mit $x^2 - dy^2 = 2$.

(ii) $\Gamma_2(\mathfrak{o}[U]) := \{A \in \Gamma(\mathfrak{o}[U]) \mid (A-1) \in 2\mathfrak{o}[U]\}$ *ist Gruppe mit* $\Gamma(\mathfrak{o}[U])^{(2)} \subset \Gamma_2(\mathfrak{o}[U])$ *und* $[\Gamma_2(\mathfrak{o}[U]) : \Gamma(\mathfrak{o}[U])^{(2)}] \leq 2$. *Genau dann gilt* $[\Gamma_2(\mathfrak{o}[U]) : \Gamma(\mathfrak{o}[U])^{(2)}] = 1$, *wenn* $d \equiv 7 \pmod 8$ *gilt und es* $x, y \in \mathbb{Z}$ *gibt mit* $x^2 - dy^2 = 2$.

(iii) *Falls* $d \equiv 1 \pmod 4$, *gilt* $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] = 1$ *oder* $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] = 3$.

(iv) *Falls* $d \equiv 2 \pmod 4$, *gilt* $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] \leq 2$, *speziell also* $\Gamma(\mathfrak{O})^{(2)} \subset \Gamma(\mathfrak{o}[U])$. *Genau dann gilt* $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] = 2$, *wenn es* $x, y \in \mathbb{Z}$ *gibt mit* $x^2 - dy^2 = 2$.

(v) *Falls* $d \equiv 3 \pmod 4$, *gilt* $\mathfrak{O} = \mathfrak{o}[U]$, *speziell also* $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] = 1$.

Bemerkung: Aus $x^2 - dy^2 \equiv 2 \pmod 8$ folgt leicht $d \equiv 2 \pmod 4$ oder $d \equiv 7 \pmod 8$.

Beweis. Man sieht leicht ein (siehe Lemma 6.2), dass U die Gruppe der Einheitswurzeln von K mit Norm 1 erzeugt. K ist ein algebraischer Zahlkörper mit zwei komplexen Stellen. Also ist $\Gamma(\mathfrak{O})$ direktes Produkt von $\mathcal{U}$ und einer zyklischen unendlichen Gruppe. Wegen $U \notin \mathcal{U}^{(2)} = \{\pm 1\}$ folgt daraus $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{O})^{(2)}] = [\Gamma(\mathfrak{o}[U]) : \Gamma(\mathfrak{o}[U])^{(2)}] = 4$.
Sei $\mathcal{U}'$ die Gruppe aller Einheitswurzeln von K, und sei ϵ eine Grundeinheit von K.

(i) Sei ϵ_+ eine Grundeinheit von k_+.
Falls $d = 2$, wird $\mathcal{U}'$ von $U' := i\sqrt{2}(1-U)/2$ erzeugt. Wir können $\epsilon_+ = 1 + i\sqrt{2}U$ annehmen, und wegen $N(U') = N(\epsilon_+) = -1$ können wir $\epsilon = \epsilon_+$ annehmen, siehe [3, § 26 (9)]. Daher wird $\Gamma(\mathfrak{O})$ von $U = U'^2$ und $U'\epsilon_+$ erzeugt. Wegen $U'\epsilon_+ \notin \mathcal{U}\Gamma(\mathfrak{o}_+)$, aber $(U'\epsilon_+)^2 \in \mathcal{U}\Gamma(\mathfrak{o}_+)$ gilt also $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] = 2$, und die Gleichung $x^2 - 2y^2 = 2$ ist mit $x = 2$, $y = 1$ lösbar. Wir können also ab hier $d \neq 2$ annehmen. Für $d = 3$ sieht man leicht ein, dass $\Gamma(\mathfrak{O}) \cap \mathcal{U}'\mathfrak{o}_+^\times = \mathcal{U}\Gamma(\mathfrak{o}_+)$ gilt. Für $d > 3$ gilt sogar $\mathcal{U}' = \mathcal{U}$. Nach [3, § 20, Satz 14] gilt also $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] \leq [\mathfrak{O}^\times : \mathcal{U}'\mathfrak{o}_+^\times] \leq 2$.

Für $d \equiv 1 \pmod 4$ ist $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] = [\mathfrak{O}^\times : \mathcal{U}'\mathfrak{o}_+^\times] = 1$, siehe [3, § 26 (10_{II})], und $x^2 - dy^2 = 2$ ist $\pmod 4$ unlösbar. Wir können also $d \not\equiv 1 \pmod 4$ annehmen. Es ist $\epsilon = (a + bU)/2$ mit $a, b \in \mathfrak{o}$ und $a = \alpha + \alpha' i\sqrt{d}$, $\epsilon_+ = (\gamma + \gamma' i\sqrt{d}U)/2$ mit $\alpha, \alpha', \gamma, \gamma' \in \mathbb{Z}$. Falls $[\mathfrak{O}^\times : \mathcal{U}'\mathfrak{o}_+^\times] = 2$, können wir $\epsilon_+ = \epsilon^2 U \in \Gamma(\mathfrak{o}_+)$ annehmen, siehe [3, § 26 (8)]. Dann folgt $2N(\epsilon) - \gamma' i\sqrt{d} - \gamma U = 2N(\epsilon) + 2\epsilon^2 = a^2 + abU$, also $2N(\epsilon) + \gamma' i\sqrt{d} = a^2 = (\alpha^2 - d\alpha'^2) + 2\alpha\alpha' i\sqrt{d}$, und speziell $\alpha^2 - d\alpha'^2 = 2N(\epsilon)$.

- Sei $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] = 2$. Dann gilt auch $[\mathfrak{O}^\times : \mathcal{U}'\mathfrak{o}_+^\times] = 2$. Wäre $N(\epsilon) = -1$, so würde $\Gamma(\mathfrak{O})$ von U und $\epsilon^2 = -\epsilon_+ U$ erzeugt, also wäre $\Gamma(\mathfrak{O}) = \mathcal{U}\Gamma(\mathfrak{o}_+)$, Widerspruch. Daher gilt $N(\epsilon) = 1$, also $\alpha^2 - d\alpha'^2 = 2$.
- Sei umgekehrt $N(x + yi\sqrt{d}U) = x^2 - dy^2 = 2$ mit $x, y \in \mathbb{Z}$. Nach [3, § 26 (12_{II})] gilt dann $[\mathfrak{O}^\times : \mathcal{U}'\mathfrak{o}_+^\times] = 2$. Aus $N(\epsilon) = -1$ folgt $N(\alpha + \alpha' i\sqrt{d}U)) = -2$, also $N(e_+) = -1$, Widerspruch zu [3, § 26 (9)]. Also gilt $\Gamma(\mathfrak{O}) = \mathfrak{O}^\times$, $\Gamma(\mathfrak{o}_+) = \mathfrak{o}_+^\times$.

(ii) Für $A = 1 + 2B \in \Gamma_2(\mathfrak{o}[U])$ gilt $A^{-1} = A^* = 1 + 2B^* \in \Gamma_2(\mathfrak{o}[U])$, und $\Gamma_2(\mathfrak{o}[U])$ ist multiplikativ abgeschlossen, also eine Gruppe. Für $A = a + bU \in \Gamma(\mathfrak{o}[U])$ mit $a, b \in \mathfrak{o}$ folgt mit $U^* = -U$, dass $A - A^* = 2bU$, also $A^2 = 1 + 2bAU \in \Gamma_2(\mathfrak{o}[U])$. Wegen $U \notin \Gamma_2(\mathfrak{o}[U])$ gilt $[\Gamma(\mathfrak{o}[U]) : \Gamma_2(\mathfrak{o}[U])] \geq 2$, also $[\Gamma_2(\mathfrak{o}[U]) : \Gamma(\mathfrak{o}[U])^{(2)}] \leq 2$.

Sei zunächst $d \not\equiv 7 \pmod 8$, also 2 in k verzweigt oder träge, $2\mathfrak{o} = \mathfrak{p}^2$ oder $2\mathfrak{o} = \mathfrak{p}$. Für $A = a + bU \in \Gamma(\mathfrak{o}[U])$ mit $a, b \in \mathfrak{o}$ gilt $N(A) = a^2 + b^2 = 1$ oder gleichwertig $(a-b-1)(a-b+1) = -2ab$. Falls $d \equiv 3 \pmod 8$, folgt daraus sofort $a - b \pm 1 \in 2\mathfrak{o}$. Falls $d \not\equiv 3 \pmod 4$, folgt $a - b \pm 1 \in \mathfrak{p}$, wegen $[\mathfrak{o} : \mathfrak{p}] = 2$ also $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Damit folgt $-2ab \in 2\mathfrak{p}$, also auch $(a-b\pm1) \in 2\mathfrak{o}$. In beiden Fallen folgt $-2ab \in 4\mathfrak{o}$, also $a \in 2\mathfrak{o}$, $(b+1) \in 2\mathfrak{o}$ oder $b \in 2\mathfrak{o}$, $(a-1) \in 2\mathfrak{o}$. Falls $a = 2a'$, $b = -1 + 2b'$ mit $a', b' \in \mathfrak{o}$, gilt $AU = 1 + 2(a' - b')U \in \Gamma_2(\mathfrak{o}[U])$. Falls $a = 1 + 2a'$, $b = 2b'$ mit $a', b' \in \mathfrak{o}$, gilt $A = 1 + 2(a' + b')U \in \Gamma_2(\mathfrak{o}[U])$. Daher gilt $A \in \Gamma_2(\mathfrak{o}[U])$ oder $AU \in \Gamma_2(\mathfrak{o}[U])$, also $[\Gamma(\mathfrak{o}[U]) : \Gamma_2(\mathfrak{o}[U])] = [\Gamma_2(\mathfrak{o}[U]) : \Gamma(\mathfrak{o}[U])^{(2)}] = 2$.

Sei nun $d \equiv 7 \pmod 8$ und $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] = 1$. Sei $A \in \Gamma(\mathfrak{o}[U]) = \Gamma(\mathfrak{O})$. Dann gilt $A = A'$ oder $A = UA'$ mit $A' = a' + b'i\sqrt{d}U$ und $a', b' \in \mathbb{Z}$ mit $a'^2 - db'^2 = 1$. Es gilt entweder $(a'-1) \in 2\mathbb{Z}$ und $b'i\sqrt{d} \in 2\mathfrak{o}$ oder $(b'i\sqrt{d}+1) \in 2\mathfrak{o}$ und $a' \in 2\mathbb{Z}$. Daher gilt $A' \in \Gamma_2(\mathfrak{O})$ oder $UA' = (-b'i\sqrt{d} + a'U) \in \Gamma_2(\mathfrak{O})$. Also ist $[\Gamma(\mathfrak{o}[U]) : \Gamma_2(\mathfrak{o}[U])] = 2$.

Sei schließlich $d \equiv 7 \pmod 8$ und $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] = 2$. Wie in (i) sei $\epsilon = (a+bU)/2$ mit $a, b \in \mathfrak{o}$ und $a = \alpha + \alpha' i\sqrt{d}$ mit $\alpha, \alpha' \in \mathbb{Z}$ und $\alpha^2 - d\alpha'^2 = 2$. Offenbar ist α ungerade, also $\epsilon \notin \Gamma_2(\mathfrak{o}[U])$. Analog ist $U\epsilon \notin \Gamma_2(\mathfrak{o}[U])$, also $[\Gamma(\mathfrak{o}[U]) : \Gamma_2(\mathfrak{o}[U])] = 4$.

(iii) Nach [3, § 26 (10_{II})] gilt hier $\mathfrak{O}^\times = \mathfrak{o}_+^\times \mathcal{U}$, also o.B.d.A. $\epsilon = \epsilon_+ = (\gamma + \gamma' i\sqrt{d}U)/2$ mit $\gamma, \gamma' \in \mathbb{Z}$ und $\gamma^2 - d\gamma'^2 = 4N(\epsilon) = \pm 4$, speziell also $\gamma \equiv \gamma' \pmod 2$. Damit gilt $(\gamma + \gamma' i\sqrt{d}U)^3 = 4\gamma(\pm 1 + d\gamma'^2) - 4\gamma'(\pm 1 - \gamma^2)i\sqrt{d}U \in 8\mathbb{Z}[i\sqrt{d}U]$, also $\epsilon^3 \in \mathfrak{o}[U]^\times$.

(iv) Offenbar gilt $\mathfrak{o}_+ = \mathbb{Z}[i\sqrt{d}U] \subset \mathfrak{o}[U]$, also $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] \le [\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] \le 2$. Falls $d = 2$ ist, seien U', ϵ_+ wie im Beweis von (i). Dann ist $U'\epsilon_+ \notin \Gamma(\mathfrak{o}[U])$, also gilt $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] = 2$, und mit $x = 2$, $y = 1$ ist $x^2 - 2y^2 = 2$. Sei ab hier $d \neq 2$. Falls $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] = 2$, so folgt mit (i), dass es $x, y \in \mathbb{Z}$ gibt mit $x^2 - dy^2 = 2$. Sei umgekehrt $x^2 - dy^2 = 2$ mit $x, y \in \mathbb{Z}$. Wie in (i) seien dann $\epsilon = (a + bU)/2$ mit $a, b \in \mathfrak{o}$ und $a = \alpha + \alpha' i\sqrt{d}$ mit $\alpha, \alpha' \in \mathbb{Z}$ und $\alpha^2 - d\alpha'^2 = 2$. Offenbar ist α' ungerade. Damit prüft man leicht nach, dass $\epsilon \notin \Gamma(\mathfrak{o}[U])$. Also ist $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] = 2$.

(v) klar

□

Satz 8.3. *Sei $d \in \mathbb{N}$ quadratfrei, sei $d \neq 1$, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Seien M eine k-Quaternionenalgebra und $\mathfrak{M}$ eine M-Maximalordnung.
Sei $\mathcal{T} \subset P\Gamma(\mathfrak{M})$ eine Tetraedergruppe. Die drei Untergruppen von $\mathcal{T}$ der Ordnung 2 sind paarweise zueinander $P\Gamma(\mathfrak{M})$-konjugiert. Sei $\mathcal{C}_2 \subset \mathcal{T}$ eine Untergruppe der Ordnung 2.

(i) Sei $d \equiv 2 \pmod 4$, und es gebe $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 2$. Dann gibt es eine maximalendliche 2-Diedergruppe $\mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2'$. Jede Tetraedergruppe $\mathcal{T}'' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{T}''$ ist $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{T}$. Jede maximalendliche 2-Diedergruppe $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2''$ ist $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{D}_2'$.

(ii) Sei $d \not\equiv 2 \pmod 4$, oder für alle $x, y \in \mathbb{Z}$ sei $x^2 - dy^2 \neq 2$. Dann gibt es eine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{T}'$, die nicht $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{T}$ ist.

Jede Tetraedergruppe $\mathcal{T}'' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{T}''$ ist $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{T}$ oder zu $\mathcal{T}'$. Es gibt keine maximalendliche 2-Diedergruppe $\mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2'$.

Bemerkung: Falls $d = 1$, ist $\mu(\mathcal{T}, \mathfrak{M}) = 1$ und $\mathfrak{M} \cong M_2(\mathfrak{o})$, siehe die Sätze 7.5, 6.7. Dann ist $\mathcal{C}_2$ also bis auf $P\Gamma(\mathfrak{M})$-Konjugation nur in einer Tetraedergruppe enthalten.

Beweis. Sei $\mathcal{D}_2$ die 2-Diedergruppe mit $\mathcal{C}_2 \subset \mathcal{D}_2 \subset \mathcal{T}$. Wir zeigen (a), dass es eine 2-Diedergruppe $\mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2'$ gibt, die nicht $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{D}_2$ ist, und dass jede 2-Diedergruppe $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2''$ dann $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{D}_2$ oder $\mathcal{D}_2'$ ist. Wir müssen danach nur noch klären (b), ob $\mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$ eine maximalendliche Untergruppe ist, oder ob es eine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{D}_2' \subset \mathcal{T}'$ gibt.

(a) $P^{-1}(\mathcal{D}_2)$ wird von $U \in P^{-1}(\mathcal{C}_2)$ und V mit $U^2 = -1$ und $VUV^{-1} = U^{-1}$ erzeugt. Ist $\mathcal{D}_2'$ eine 2-Diedergruppe mit $\mathcal{C}_2 \subset \mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$, dann wird $P^{-1}(\mathcal{D}_2')$ von U und V' mit $V'UV'^{-1} = U^{-1}$ erzeugt. Daraus folgt $X' := V^{-1}V' \in k(U) \cap \Gamma(\mathfrak{M})$.
V' und X' sind durch $\mathcal{D}_2'$ bis auf einen Faktor aus $P^{-1}(\mathcal{C}_2)$ eindeutig bestimmt.
Ist umgekehrt $X' \in k(U) \cap \Gamma(\mathfrak{M})$ und $V' := VX'$, so ist $V'UV'^{-1} = U^{-1}$, also sind U und V' Erzeugende von $P^{-1}(\mathcal{D}_2')$ für eine 2-Diedergruppe $\mathcal{D}_2'$ mit $\mathcal{C}_2 \subset \mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$.
$\mathcal{D}_2$ und $\mathcal{D}_2'$ sind genau dann $P\Gamma(\mathfrak{M})$-konjugiert, wenn es ein $U' \in P^{-1}(\mathcal{C}_2)$ und ein $J \in \Gamma(\mathfrak{M})$ gibt mit $JUJ^{-1} = U$ und $JV'J^{-1} = VU'$.
Zwischenbemerkung: Wir können o.B.d.A. $JUJ^{-1} = U$ annehmen, da die Elemente $X \in P^{-1}(\mathcal{D}_2)$ mit $X^2 = -1$ in $P^{-1}(\mathcal{T})$ jeweils paarweise zueinander konjugiert sind. Dann ist $J \in k(U) \cap \Gamma(\mathfrak{M})$, und $X' = V^{-1}V' = V^{-1}J^{-1}VU'J = (J^{-1})^*U'J = J^2U'$.
Ist umgekehrt $X' = J^2U'$ mit $U' \in P^{-1}(\mathcal{C}_2)$ und $J \in k(U) \cap \Gamma(\mathfrak{M})$, so ist $JUJ^{-1} = U$ und $JV'J^{-1} = JVX'J^{-1} = JVJ^2U'J^{-1} = VJ^*J^2U'J^{-1} = VU'$.
Wegen $d \neq 1$ ist $k(U)$ algebraischer Zahlkörper mit zwei komplexen Stellen, Nach dem Dirichletschen Einheitensatz ist $k(U) \cap \Gamma(\mathfrak{M})$ daher direktes Produkt einer zyklischen unendlichen Gruppe und der Untergruppe $P^{-1}(\mathcal{C}_2)$ der Einheitswurzeln von $k(U)$ mit Norm 1. Deshalb gilt $[(k(U) \cap \Gamma(\mathfrak{M})) : (k(U) \cap \Gamma(\mathfrak{M}))^{(2)} P^{-1}(\mathcal{C}_2)] = 2$. Sei jetzt $\mathcal{D}_2'$ eine 2-Diedergruppe mit $\mathcal{C}_2 \subset \mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$ und $X' \notin (k(U) \cap \Gamma(\mathfrak{M}))^{(2)} P^{-1}(\mathcal{C}_2)$. Dann ist $\mathcal{D}_2'$ nicht $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{D}_2$. Ist nun $\mathcal{D}_2''$ eine 2-Diedergruppe mit $\mathcal{C}_2 \subset \mathcal{D}_2'' \subset P\Gamma(\mathfrak{M})$, so wird $P^{-1}(\mathcal{D}_2'')$ von U und V'' mit $V''UV''^{-1} = U^{-1}$ erzeugt. Wegen $V'^{-1}V'' = (V^{-1}V')^{-1}V^{-1}V''$ gilt $V^{-1}V'' \in (k(U) \cap \Gamma(\mathfrak{M}))^{(2)} P^{-1}(\mathcal{C}_2)$ oder $V'^{-1}V'' \in (k(U) \cap \Gamma(\mathfrak{M}))^{(2)} P^{-1}(\mathcal{C}_2)$, und $\mathcal{D}_2''$ ist $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{D}_2$ oder $\mathcal{D}_2'$.

(b) Falls $d \equiv 3 \pmod 4$, gibt es nach Satz 6.6 keine maximalendliche 2-Diedergruppe $\mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$. Also gilt dann $\mathcal{D}_2' \subset \mathcal{T}'$ für eine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{M})$.
Falls $d \not\equiv 3 \pmod 4$, gilt nach Lemma 8.1.(i) dann $(k(U) \cap \mathfrak{M})_2 = \mathfrak{o}_2[(1+U)/\pi]$.
Falls $d \equiv 1 \pmod 4$, gibt es keine maximalendliche 2-Diedergruppe $\mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2'$, denn nach Lemma 8.1.(ii) wäre sonst $k(U) \cap \mathfrak{M} = \mathfrak{o}[(i\sqrt{d}+U)/2]$ oder $k(U) \cap \mathfrak{M} = \mathfrak{o}[U]$. Also gilt $\mathcal{D}_2' \subset \mathcal{T}'$ für eine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{M})$.

Sei nun $d \equiv 2 \pmod 4$. $P^{-1}(\mathcal{T})$ wird von U, V und $W := (1-U-V-UV)/2$ erzeugt. Wenn es eine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{D}_2' \subset \mathcal{T}'$ gibt, wird $P^{-1}(\mathcal{T}')$ von U, V' und $W' := (1-U-V'-UV')/2$ erzeugt. Aus $(1+U)V(1-X')/2 = W'-W \in \mathfrak{M}$ folgt dann $N(1-X') \in 2\mathfrak{o}$ oder gleichwertig $S(X') \in 2\mathfrak{o}$, und daher $X' \in \Gamma(\mathfrak{o}[U])$.

Sei umgekehrt $X' \in \Gamma(\mathfrak{o}[U])$. Dann sind U, $V' = VX'$ und $W' := (1-U-V'-UV')/2$ Erzeugende von $P^{-1}(\mathcal{T}')$ für eine Tetraedergruppe $\mathcal{T}'$ mit $\mathcal{C}_2 \subset \mathcal{T}'$. Wir wollen zeigen, dass $\mathcal{T}' \subset P\Gamma(\mathfrak{M})$ oder (hinreichend) $W' = W + (1+U)V(1-X')/2 \in \mathfrak{M}_2$ gilt. Es gilt $(1+U)/\pi \in \mathfrak{M}_2$. Sei $X' = a + bU$ mit $a, b \in \mathfrak{o}$. Wegen $N(X') = a^2 + b^2 = 1$ und $[\mathfrak{o}_2 : \pi\mathfrak{o}_2] = 2$ gilt $(1-a+b) \in \pi\mathfrak{o}_2$ und $(1-X')/\pi = (1-a+b)/\pi - b(1+U)/\pi \in \mathfrak{M}_2$.
Es ist $X' \in (k(U) \cap \Gamma(\mathfrak{M})) \smallsetminus (k(U) \cap \Gamma(\mathfrak{M}))^{(2)} P^{-1}(\mathcal{C}_2)$, und $k(U) \cap \mathfrak{M}$ ist die Hauptordnung von $k(U)$. Nach Lemma 8.2.(iv) gilt $(k(U) \cap \Gamma(\mathfrak{M}))^{(2)} P^{-1}(\mathcal{C}_2) \subset \Gamma(\mathfrak{o}[U])$.
$\mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$ ist genau dann eine maximalendliche 2-Diedergruppe,
wenn $X' \notin \Gamma(\mathfrak{o}[U])$, also genau dann, wenn $[(k(U) \cap \Gamma(\mathfrak{M})) : \Gamma(\mathfrak{o}[U])] = 2$,
nach Lemma 8.2.(iv) also genau dann, wenn es $x, y \in \mathbb{Z}$ gibt mit $x^2 - dy^2 = 2$.

□

Satz 8.4. *Sei $d \in \mathbb{N}$ quadratfrei, sei $d \neq 1$, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Seien M eine k-Quaternionenalgebra und $\mathfrak{N}$ eine M-Maximalordnung.
Sei $\mathcal{D}_2 \subset P\Gamma(\mathfrak{N})$ eine maximalendliche 2-Diedergruppe.

(i) Sei $d \equiv 2 \pmod 4$, und es gebe $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 2$.

- *(a) Dann gibt es eine Untergruppe $\mathcal{C}_2 \subset \mathcal{D}_2$ der Ordnung 2 und eine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{N})$ mit $\mathcal{C}_2 \subset \mathcal{T}'$. Die Zuordnung $\mathcal{D}_2 \mapsto \mathcal{C}_2$ ist eindeutig. Jede Tetraedergruppe $\mathcal{T}'' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{T}''$ ist $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{T}'$.*
- *(b) Seien $\mathcal{C}_2', \mathcal{C}_2'' \subset \mathcal{D}_2$ die beiden anderen Untergruppen der Ordnung 2. Dann sind $\mathcal{C}_2'$ und $\mathcal{C}_2''$ zueinander $P\Gamma(\mathfrak{N})$-konjugiert.*
- *(c) Jede maximalendliche 2-Diedergruppe $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{N})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2''$ ist $P\Gamma(\mathfrak{N})$-konjugiert zu $\mathcal{D}_2$.*
- *(d) Jede maximalendliche 2-Diedergruppe $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{N})$ mit $\mathcal{C}_2' \subset \mathcal{D}_2''$ oder $\mathcal{C}_2'' \subset \mathcal{D}_2''$ ist $P\Gamma(\mathfrak{N})$-konjugiert zu $\mathcal{D}_2$.*

(ii) Sei $d \not\equiv 2 \pmod 4$, oder für alle $x, y \in \mathbb{Z}$ sei $x^2 - dy^2 \neq 2$.

- *(a) Sei $\mathcal{C}_2 \subset \mathcal{D}_2$ eine Untergruppe der Ordnung 2. Dann gibt es keine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{N})$ mit $\mathcal{C}_2 \subset \mathcal{T}'$.*
- *(b) Seien $\mathcal{C}_2', \mathcal{C}_2'' \subset \mathcal{D}_2$ die beiden anderen Untergruppen der Ordnung 2. Dann sind $\mathcal{C}_2$, $\mathcal{C}_2'$ und $\mathcal{C}_2''$ paarweise nicht zueinander $P\Gamma(\mathfrak{N})$-konjugiert.*
- *(c) Es gibt eine maximalendliche 2-Diedergruppe $\mathcal{D}_2' \subset P\Gamma(\mathfrak{N})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2'$, die nicht $P\Gamma(\mathfrak{N})$-konjugiert zu $\mathcal{D}_2$ ist. Jede maximalendliche 2-Diedergruppe $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{N})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2''$ ist $P\Gamma(\mathfrak{N})$-konjugiert zu $\mathcal{D}_2$ oder $\mathcal{D}_2'$.*
- *(d) Jede maximalendliche 2-Diedergruppe $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{N})$ mit $\mathcal{C}_2' \subset \mathcal{D}_2''$ oder $\mathcal{C}_2'' \subset \mathcal{D}_2''$ ist $P\Gamma(\mathfrak{N})$-konjugiert zu $\mathcal{D}_2$ oder zu $\mathcal{D}_2'$.*

Bemerkung: Falls $d = 1$, ist $\mu(\mathcal{D}_2, \mathfrak{N}) = 1$ und $\mathfrak{N} \cong M_2(\mathfrak{o})$, siehe die Sätze 7.5, 6.6, 6.7. Dann ist $\mathcal{C}_2$ also bis auf $P\Gamma(\mathfrak{N})$-Konjugation nur in einer maximalendlichen 2-Diedergruppe enthalten. Weiter ist wohlbekannt, dass $\mathcal{C}_2, \mathcal{C}_2', \mathcal{C}_2''$ paarweise nicht zueinander $P\Gamma(\mathfrak{N})$-konjugiert sind, und dass es keine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{N})$ gibt mit $\mathcal{C}_2 \subset \mathcal{T}'$.

Beweis. Nach Satz 6.6 ist $d \not\equiv 3 \pmod 4$, also 2 verzweigt in k. Sei $\pi \in \mathfrak{o}_2$ Primelement. In den Beweisabschnitten (a) - (d) zeigen wir jeweils beide Teile (i) und (ii) des Satzes.

(a) Sei $d \equiv 2 \pmod 4$, und es gebe $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 2$.
Daraus folgt $\left(\frac{2,-d}{p}\right) = \left(\frac{2,d}{p}\right) = 1$ für alle Stellen $p \neq 2, \infty$ von $\mathbb{Q}$. Nach Satz 6.7 gibt es daher auch eine Tetraedergruppe $\mathcal{T} \subset P\Gamma(\mathfrak{N})$. Nach Satz 8.3 gibt es eine maximalendliche 2-Diedergruppe $\mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$, so dass $\mathcal{T} \cap \mathcal{D}_2'$ die Ordnung 2 hat. Die $P\Gamma(\mathfrak{N})$-Konjugationsklasse von $\mathcal{D}_2'$ ist durch die $P\Gamma(\mathfrak{N})$-Konjugationsklasse von $\mathcal{T}$ eineindeutig bestimmt. Nach Satz 7.5 gilt $\mu(\mathcal{D}_2, \mathfrak{N}) = \mu(\mathcal{T}, \mathfrak{N})$. Also gibt es auch eine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{N})$, so dass $\mathcal{C}_2 := \mathcal{T}' \cap \mathcal{D}_2$ die Ordnung 2 hat.
Sei $X \in P^{-1}(\mathcal{C}_2)$ mit $X^2 = -1$. Nach Lemma 8.1.(i) gilt $(k(X) \cap \mathfrak{N})_2 = \mathfrak{o}_2[(1+X)/\pi]$, Nach Lemma 8.1.(ii) ist dadurch X bis aufs Vorzeichen, also $\mathcal{C}_2$ eindeutig bestimmt.

Sei umgekehrt $\mathcal{T}' \subset P\Gamma(\mathfrak{N})$ eine Tetraedergruppe, so dass $\mathcal{T}' \cap \mathcal{D}_2$ die Ordnung 2 hat. Nach Satz 8.3 ist dann $d \equiv 2 \pmod 4$, und es gibt $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 2$.

(b) $P^{-1}(\mathcal{D}_2)$ wird von U und V mit $U^2 = -1$ und $VUV^{-1} = U^{-1}$ erzeugt.

Sei $d \equiv 2 \pmod 4$, und es gebe $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 2$. Dann ist x gerade.
Wir nehmen o.b.d. A. an, dass $U \in P^{-1}(\mathcal{C}_2')$, $V \in P^{-1}(\mathcal{C}_2'')$ und $UV \in P^{-1}(\mathcal{C}_2)$ gilt.
Gemäß Beweisabschnitt (a) gilt dann $(k(UV) \cap \mathfrak{N})_2 = \mathfrak{o}_2[(1+UV)/\pi]$.
Sei $\epsilon := (x + yi\sqrt{d}U + yi\sqrt{d}V - xUV)/2 = (1 - UV)x/2 + yU(1 - UV)i\sqrt{d}/2 \in \mathfrak{N}$
Man rechnet elementar nach, dass $N(\epsilon) = 1$ und $\epsilon V \epsilon^{-1} = U$ gilt.

Seien umgekehrt zwei Untergruppen von $\mathcal{D}_2$ der Ordnung 2 zueinander $P\Gamma(\mathfrak{N})$-konjugiert. Wir können o.B.d.A. annehmen, dass $\epsilon V \epsilon^{-1} = U$ gilt, mit $\epsilon \in \Gamma(\mathfrak{N})$. Dann gilt $k(V) \cap \mathfrak{N} \cong k(U) \cap \mathfrak{N}$, und nach Lemma 8.1 gilt $k(UV) \cap \mathfrak{N} = \mathfrak{o}[(i\sqrt{d} + UV)/2]$, falls $d \equiv 1 \pmod 4$, bzw. $(k(UV) \cap \mathfrak{N})_2 = \mathfrak{o}_2[(1+UV)/\pi]$, falls $d \equiv 2 \pmod 4$.
Aus $\epsilon V \epsilon^{-1} = U$ folgt $\epsilon = (a + bU + bV - aUV)/2$ mit $a, b \in \mathfrak{o}$ und $a^2 + b^2 = 2$. Sei $V' := \epsilon U \epsilon^{-1} = ((-a^2 + b^2)/2 - abU)V$ und sei $\mathcal{D}_2' \subset P\Gamma(\mathfrak{N})$ die von $P(U)$ und $P(V')$ erzeugte 2-Diedergruppe. Wir kürzen $F := F(\mathcal{D}_2)$ und $F' := F(\mathcal{D}_2') = \epsilon F \epsilon^{-1}$ ab.
Offenbar gilt $\Phi_F(\mathfrak{N}) = \mathfrak{N}$. Seien $T := \epsilon \Phi_F(\epsilon)^* = (a\overline{a} + b\overline{b})/2 + (-a\overline{b} + \overline{a}b)U/2$ und $\gamma := (a\overline{a} + b\overline{b})/2$, $\gamma' i\sqrt{d} := (-a\overline{b} + \overline{a}b)/2$. Wegen $T \in \Gamma(\mathfrak{N})$ ist $N(T) = \gamma^2 - d\gamma'^2 = 1$, und wegen $k(U) \cap \mathfrak{N} = \mathfrak{o}[U]$ sind $\gamma, \gamma' \in \mathbb{Z}$, und γ ist ungerade, γ' ist gerade.
Für alle $B \in F$ gilt $\epsilon B \epsilon^{-1} = T\Phi_F(\epsilon) B \Phi_F(\epsilon)^{-1} T^{-1} = T\Phi_F(\epsilon B \epsilon^{-1}) T^{-1}$. Also gilt $A = T\Phi_F(A)T^{-1}$ für alle $A \in F'$, und daher $\Phi_{F'}(A) = T\Phi_F(A)T^{-1}$ für alle $A \in M$. Also ist $\Phi_{F'}(TV) = TT^*VT^{-1} = TV$, und aus $T \in k(U)$ folgt $(TV)U(TV)^{-1} = U^{-1}$. Also erzeugen $P(U)$ und $P(TV)$ eine 2-Diedergruppe $\mathcal{D}_2''$ mit $P^{-1}(\mathcal{D}_2'') \subset F' \cap \mathfrak{N}$. Mit Lemma 6.3 folgt $P^{-1}(\mathcal{D}_2'') \subset \Gamma(F' \cap \mathfrak{N}) = \Gamma(\mathfrak{F}(\mathcal{D}_2')) = P^{-1}(\mathcal{D}_2')$, also $\mathcal{D}_2'' = \mathcal{D}_2'$.
Wegen $(1 + UTV)/\pi = (1 + \gamma UV)/\pi - \gamma' i\sqrt{d}V/\pi \in \mathfrak{N}_2$ ist notwendig $TV = \pm V'$, das heißt $\gamma + \gamma' i\sqrt{d}U = \pm((-a^2 + b^2)/2 - abU)$. Sei $a = \alpha + \alpha' i\sqrt{d}$ und $b = \beta + \beta' i\sqrt{d}$ mit $\alpha, \alpha', \beta, \beta' \in \mathbb{Z}$. Damit erhalten wir $-\alpha\alpha' + \beta\beta' = 0$ und $\alpha\beta - \alpha'\beta' d = 0$. Daraus folgt $\beta'(\beta^2 - d\alpha'^2) = \alpha(\beta^2 - d\alpha'^2) = 0$, wegen $d \neq 1$ also $\alpha = \beta' = 0$ oder $\alpha' = \beta = 0$. Dann ist $2 = a^2 + b^2 = \beta^2 - d\alpha'^2$ oder $2 = \alpha^2 - d\beta'^2$, und es folgt $d \not\equiv 1 \pmod 4$.

(c) Sei $d \equiv 2 \pmod 4$, und es gebe $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 2$.
Dann folgt die Behauptung mit Satz 8.4.(i)(a) und Satz 8.3.(i).

Sei $d \not\equiv 2 \pmod 4$, oder für alle $x, y \in \mathbb{Z}$ sei $x^2 - dy^2 \neq 2$.
Der Beweis erfolgt dann wie Abschnitt (a) im Beweis von Satz 8.3, wenn wir dort die Zwischenbemerkung wie folgt ersetzen:
Zwischenbemerkung: Wir können o.B.d.A. $JUJ^{-1} = U$ annehmen, da U in $P^{-1}(\mathcal{D}_2)$ zu U^{-1}, nach Satz 8.4.(ii)(b) aber nicht zu $V^{\pm 1}$ und $(UV)^{\pm 1}$ konjugiert ist.

(d) $P^{-1}(\mathcal{D}_2)$ wird von U, V mit $U^2 = -1$ und $VUV^{-1} = U^{-1}$ erzeugt. O.B.d.A. können wir $U \in P^{-1}(\mathcal{C}_2')$ mit $k(U) \cap \mathfrak{N} = \mathfrak{o}[U]$, $V \in P^{-1}(\mathcal{C}_2'')$ und $UV \in P^{-1}(\mathcal{C}_2)$ annehmen.

Sei $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{N})$ eine maximalendliche 2-Diedergruppe mit $\mathcal{C}_2' \subset \mathcal{D}_2''$. Wir zeigen, dass es eine 2-Diedergruppe $\mathcal{D}_2'$ mit $\mathcal{C}_2 \subset \mathcal{D}_2'$ gibt, die $P\Gamma(\mathfrak{N})$-konjugiert zu $\mathcal{D}_2''$ ist:
$P^{-1}(\mathcal{D}'')$ wird von U, V' mit $V'UV'^{-1} = U^{-1}$ erzeugt. Dann ist $V^{-1}V' \in \mathfrak{o}[U]$.
Sei $V' = V(a + bU)$ mit $a, b \in \mathfrak{o}$. Aus $a^2 + b^2 = 1$ folgt $a - b \notin \pi\mathfrak{o}_2$. Wir können V' durch $UV' = V(b - aU)$ ersetzen, o.B.d.A. also $b \in \pi\mathfrak{o}_2$ annehmen. Sei $a = \alpha + \alpha' i\sqrt{d}$, $b = \beta + \beta' i\sqrt{d}$ mit $\alpha, \alpha', \beta, \beta' \in \mathbb{Z}$. Dann ist $\alpha^2 - d\alpha'^2 + \beta^2 - d\beta'^2 = 1$ und $\alpha\alpha' + \beta\beta' = 0$.
Falls $d \equiv 2 \pmod 4$, ist $\beta \equiv 0 \pmod 2$. Falls $d \equiv 1 \pmod 4$, ist $\beta \equiv \beta' \pmod 2$. In jedem Fall folgt $\alpha - 1 \equiv \alpha' \equiv 0 \pmod 2$. Falls $d \equiv 2 \pmod 4$, ist $d\beta'^2 \equiv 0 \pmod 4$, also $\beta' \equiv 0 \pmod 2$. Falls $d \equiv 1 \pmod 4$, ist $\beta \equiv \beta' \equiv \beta\beta' \equiv 0 \pmod 2$.
Daher gilt $\epsilon := ((a+1) + bU + (a-1)V - bUV)/2 \in \mathfrak{N}$. Aus $N(\epsilon) = 1$ folgt $\epsilon \in \Gamma(\mathfrak{N})$.
Weiter gilt $\epsilon U \epsilon^{-1} = U(a + bUV)$ und $\epsilon V' \epsilon^{-1} = V(a + bUV)$, sowie $\epsilon UV' \epsilon^{-1} = UV$.
Sei $\mathcal{D}' \subset P\Gamma(\mathfrak{N})$ die von $P(\epsilon U \epsilon^{-1})$ und $P(\epsilon V' \epsilon^{-1})$ erzeugte 2-Diedergruppe.

Es bleibt zu zeigen, dass es zu jeder maximalendlichen 2-Diedergruppe $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{N})$ mit $\mathcal{C}_2'' \subset \mathcal{D}_2''$ eine 2-Diedergruppe $\mathcal{D}_2'$ mit $\mathcal{C}_2 \subset \mathcal{D}_2'$ gibt, die $P\Gamma(\mathfrak{N})$-konjugiert zu $\mathcal{D}_2''$ ist. Falls $k(V) \cap \mathfrak{N} = \mathfrak{o}[V]$, verläuft der Beweis analog zum Fall $\mathcal{C}_2' \subset \mathcal{D}_2''$.
Sei also $k(V) \cap \mathfrak{N} \neq \mathfrak{o}[V]$, nach Lemma 8.1 also $k(UV) \cap \mathfrak{N} = \mathfrak{o}[UV]$.
Gemäß Beweisabschnitt (b) gilt dann $d \not\equiv 2 \pmod 4$ oder $x^2 - dy^2 \neq 2$ für alle $x, y \in \mathbb{Z}$. Mit Lemma 8.2.(iii) folgt $d \equiv 1 \pmod 4$ und $[\Gamma(k(V) \cap \mathfrak{N}) : \Gamma(\mathfrak{o}[V])] = 3$.
$P^{-1}(\mathcal{D}'')$ wird von V, U' mit $U'VU'^{-1} = V^{-1}$ erzeugt. Sei $X := U^{-1}U'$. Dann gilt $X \in k(V) \cap \Gamma(\mathfrak{N})$. Sei $U'' := UX^3 = U'X^2$, und sei $\mathcal{D}'''$ die von $P(V)$ und $P(U'')$ erzeugte 2-Diedergruppe. Wegen $XU''X^{-1} = U''X^*X^{-1} = U'$ sind $\mathcal{D}'', \mathcal{D}'''$ zueinander $P\Gamma(\mathfrak{N})$ konjugiert, und mit $U^{-1}U'' = X^3 \in \Gamma(\mathfrak{o}[V])$ folgt analog zum Fall $\mathcal{C}_2' \subset \mathcal{D}_2''$, dass es eine 2-Diedergruppe $\mathcal{D}_2'$ mit $\mathcal{C}_2 \subset \mathcal{D}_2'$ gibt, die $P\Gamma(\mathfrak{N})$-konjugiert zu $\mathcal{D}_2'''$ ist.

□

Satz 8.5. *Sei $d \in \mathbb{N}$ quadratfrei, sei $d \neq 3$, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Seien M eine k-Quaternionenalgebra und $\mathfrak{M}$ eine M-Maximalordnung. Sei $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$ eine 3-Diedergruppe, und sei $\mathcal{C}_3 \subset \mathcal{D}_3$ deren Untergruppe der Ordnung 3. Dann gibt es eine 3-Diedergruppe $\mathcal{D}_3' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_3 \subset \mathcal{D}_3'$, die nicht $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{D}_3$ ist. Jede 3-Diedergruppe $\mathcal{D}_3'' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_3 \subset \mathcal{D}_3''$ ist $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{D}_3$ oder zu $\mathcal{D}_3'$.

Bemerkung: Falls $d = 3$, ist $\mu(\mathcal{D}_3, \mathfrak{M}) = 1$ und $\mathfrak{M} \cong M_2(\mathfrak{o})$, siehe die Sätze 7.5, 6.7.
Dann ist $\mathcal{C}_3$ also bis auf $P\Gamma(\mathfrak{M})$-Konjugation nur in einer 3-Diedergruppe enthalten.

Beweis. wie Abschnitt (a) im Beweis von Satz 8.3, wenn wir dort $\mathcal{D}_2$, $\mathcal{C}_2$, $U^2 = -1, d \neq 1$ durch $\mathcal{D}_3$, $\mathcal{C}_3$, $U^3 = -1, d \neq 3$ ersetzen, sowie die Zwischenbemerkung wie folgt ersetzen: *Zwischenbemerkung*: Wir können o.B.d.A. $JUJ^{-1} = U$ annehmen, da die beiden Elemente $X = U^{\pm 1} \in P^{-1}(\mathcal{D}_3) \smallsetminus \mathfrak{o}^\times$ mit $X^3 = -1$ in $P^{-1}(\mathcal{D}_3)$ zueinander konjugiert sind. □

Satz 8.6. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Seien M eine k-Quaternionenalgebra und $\mathfrak{N}$ eine M-Maximalordnung.
Für $m = 3$ oder $m = 2$ bezeichne $\lambda_m^*(\mathfrak{N})$ die Anzahl der $P\Gamma(\mathfrak{N})$-Konjugationsklassen von Gruppen der Ordnung m, die in einer m-Diedergruppe $\mathcal{D}_m \subset P\Gamma(\mathfrak{N})$ enthalten sind.
Für $d \neq 3$ ist dann $2\lambda_3^*(\mathfrak{N}) = \mu(\mathcal{D}_3, \mathfrak{N})$, und für $d \neq 1$ ist $2\lambda_2^*(\mathfrak{N}) = \mu(\mathcal{T}, \mathfrak{N}) + 3\mu(\mathcal{D}_2, \mathfrak{N})$.

Bemerkung: $\lambda_m^*(\mathfrak{N})$ entspricht der in [4, § 15] definierten Bezeichnung $\lambda_{2m}^*(\mathfrak{N})$.
Satz 8.6 geht schon aus [4, Sätze 20.39 und 26.12, Tabellen 20.40 und 26.13] hervor. Erstmals explizit formuliert und auf andere Art bewiesen wurde er in [6, Corollary 23].

Beweis. Für $d \neq 3$ geht die Behauptung $2\lambda_3^*(\mathfrak{N}) = \mu(\mathcal{D}_3, \mathfrak{N})$ direkt aus Satz 8.5 hervor. Sei nun zunächst $d \equiv 2 \pmod 4$, und es gebe $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 2$. Dann gibt es zu jeder Tetraedergruppe $\mathcal{T} \subset P\Gamma(\mathfrak{N})$ eine 2-Diedergruppe $\mathcal{D}_2 \subset P\Gamma(\mathfrak{N})$ und zu jeder 2-Diedergruppe $\mathcal{D}_2 \subset P\Gamma(\mathfrak{N})$ eine Tetraedergruppe $\mathcal{T} \subset P\Gamma(\mathfrak{N})$, so dass $\mathcal{T} \cap \mathcal{D}_2$ die Ordnung 2 hat. $\mathcal{T}$ und $\mathcal{D}_2$ sind bis auf $P\Gamma(\mathfrak{N})$-Konjugation durch $\mathcal{T} \cap \mathcal{D}_2$ eindeutig bestimmt, und $\mathcal{T} \cup \mathcal{D}_2$ enthält bis auf $P\Gamma(\mathfrak{N})$-Konjugation genau zwei Gruppen der Ordnung 2, siehe Satz 8.3.(i) und 8.4.(i)(b)-(d).
Sei schließlich $d \neq 1$, und sei $d \not\equiv 2 \pmod 4$, oder für alle $x, y \in \mathbb{Z}$ sei $x^2 - dy^2 \neq 2$.
Der Durchschnitt $\mathcal{T} \cap \mathcal{D}_2$ einer Tetraedergruppe $\mathcal{T} \subset P\Gamma(\mathfrak{N})$ und einer 2-Diedergruppe $\mathcal{D}_2 \subset P\Gamma(\mathfrak{N})$ ist dann stets trivial, siehe Satz 8.3.(ii) oder 8.4.(ii)(a). Die Behauptung folgt für Tetraedergruppen mit Satz 8.3.(ii) und für 2-Diedergruppen mit 8.4.(ii)(b)-(d). □

Lemma 8.7. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Seien M eine k-Quaternionenalgebra und $\mathfrak{M}$ eine M-Maximalordnung.
Sei $d' \in \mathbb{N}$ quadratfrei mit $d' \neq d$. Sei $X \in M$ mit $X^2 = -d'$, und sei $K := \mathbb{Q}(X)$ mit Hauptordnung $\mathfrak{O}$. Seien $F, F' \subset M$ zwei $\mathbb{Q}$-Quaternionenalgebren, und seien $\mathfrak{F} := F \cap \mathfrak{M}$ und $\mathfrak{F}' := F' \cap \mathfrak{M}$. Sei $\Delta(\mathfrak{F})$ teilerfremd zu $\Delta(\mathfrak{F}')$, und sei $\mathfrak{F} \cap \mathfrak{F}' = \mathfrak{O}$.
Dann zerfällt M, und es gibt teilerfremde $x, y \in \mathbb{Z}$, so dass eine derAussagen (i)-(vi) gilt:

(i) $d' \not\equiv 3 \pmod 4$, *y ist gerade,*
$\Delta(\mathfrak{F})\Delta(\mathfrak{F}') = x^2 - dd'y^2 \equiv 1 \pmod 4$.

(ii) $d' \not\equiv 3 \pmod 4$, *y ist ungerade,* $d \not\equiv 3 \pmod 4$,
$\Delta(\mathfrak{F})\Delta(\mathfrak{F}') = 4(x^2 - dd'y^2) \equiv 0 \pmod 4$.

(iii) $d' \not\equiv 3 \pmod 4$, *y ist ungerade,* $d \equiv 3 \pmod 4$,
$\Delta(\mathfrak{F})\Delta(\mathfrak{F}') = x^2 - dd'y^2 \not\equiv 0 \pmod 4$.

(iv) $d' \equiv 3 \pmod 4$, $d \not\equiv 3 \pmod 4$,
$\Delta(\mathfrak{F})\Delta(\mathfrak{F}') = x^2 - dd'y^2$.

(v) $d' \equiv 3 \pmod 4$, $d \equiv 3 \pmod 4$, *x oder y sind gerade,*
$\Delta(\mathfrak{F})\Delta(\mathfrak{F}') = x^2 - dd'y^2$ *ist ungerade.*

(vi) $d' \equiv 3 \pmod 4$, $d \equiv 3 \pmod 4$, *x und y sind ungerade,*
$4\Delta(\mathfrak{F})\Delta(\mathfrak{F}') = x^2 - dd'y^2$.

Beweis. $\Sigma_k(F)$ und $\Sigma_k(F')$ sind als Teiler von $\Delta(\mathfrak{F})$ und $\Delta(\mathfrak{F}')$ teilerfremd. Wegen $F, F' \subset M$ gilt also $\Sigma_k(F) = \Sigma_k(F') = 1$, und M zerfällt Sei $\mathfrak{O} = \mathbb{Z}[\Omega]$. Wir können o.B.d.A. $\Omega = X$ bzw. $\Omega = (1+X)/2$ annehmen. Sei $L := k(X)$, und sei $\mathfrak{L} = L \cap \mathfrak{M}$. Wir zeigen, dass $\mathfrak{L}_p = \mathfrak{o}_p[\Omega]$ für alle endlichen Stellen p von $\mathbb{Q}$, also $\mathfrak{L} = \mathfrak{o}[\Omega]$: O.b.d.A. sei $p \nmid \Delta(\mathfrak{F})$. Dann zerfällt$F_p$, und $\mathfrak{F}_p$ ist eine F_p-Maximalordnung. Daher lässt sich $\{1, \Omega\}$ zu einer $\mathbb{Z}_p$-Basis von $\mathfrak{F}_p$ fortsetzen. Diese ist dann auch $\mathfrak{o}_p$-Basis von $\mathfrak{M}_p$.
Nach Satz 3.4 gibt es ein $T \in M^\times$ mit $\Phi_F(T) = T^*$ und $\Phi_{F'}(A) = T\Phi_F(A)T^{-1}$ für alle $A \in M$. Offenbar gilt $\sqrt{d}(T - T^*) \in F \cap F' = K$, also ist $T = \alpha + \beta i\sqrt{d}X$ mit $\alpha, \beta \in \mathbb{Q}$ und $N(T) = \alpha^2 - dd'\beta^2$. O.B.d.A. sei $T \in \mathfrak{M}$, aber $T \notin n\mathfrak{M}$ für alle $n \in \mathbb{N}$ mit $n > 1$. Dann ist T bis aufs Vorzeichen eindeutig bestimmt, und es gilt $T \in \mathfrak{L}$.
Sei nun p eine endliche Stelle von $\mathbb{Q}$, zunächst mit $p \nmid \Delta(\mathfrak{F})$.
Dann gibt es Matrizeseinheiten in F_p, bezüglich derer $\mathfrak{F}_p = M_2(\mathbb{Z}_p)$, $\mathfrak{M}_p = M_2(\mathfrak{o}_p)$ und $\Phi_F\left(\begin{pmatrix} t & u \\ v & w \end{pmatrix}\right) = \begin{pmatrix} \overline{t} & \overline{u} \\ \overline{v} & \overline{w} \end{pmatrix}$ für $t, u, v, w \in k_p$. Nach Lemma 4.3 können wir diese Matrizeseinheiten so wählen, dass $X = \Omega = \begin{pmatrix} 0 & 1 \\ -d' & 0 \end{pmatrix}$, falls $d' \not\equiv 3 \pmod 4$ oder $p \neq 2$, und $\Omega = \begin{pmatrix} 1 & 1 \\ -(1+d')/4 & 0 \end{pmatrix}$, $X = \begin{pmatrix} 1 & 2 \\ -(1+d')/2 & -1 \end{pmatrix}$, falls $d' \equiv 3 \pmod 4$ und $p = 2$. Wir betrachten zuerst den Fall $d' \not\equiv 3 \pmod 4$ oder $p \neq 2$. Dann ist $T = \begin{pmatrix} \alpha & \beta i\sqrt{d} \\ -\beta d' i\sqrt{d} & \alpha \end{pmatrix}$, und es gilt $\alpha, \beta \in \mathbb{Z}_p$, nicht beide durch p teilbar. Damit prüft man elementar nach, dass $\left\{1, X, Y := \begin{pmatrix} -\alpha & \beta i\sqrt{d} \\ \beta d' i\sqrt{d} & \alpha \end{pmatrix}, Z := (XY - \alpha X)/d' = \begin{pmatrix} \beta i\sqrt{d} & 0 \\ 2\alpha & -\beta i\sqrt{d} \end{pmatrix}\right\}$ eine $\mathbb{Z}_p$-Basis einer F_p'-Ordnung $\mathfrak{G}_p \subset \mathfrak{F}_p'$ mit Diskriminante $16(\alpha^2 - dd'\beta^2)^2\mathbb{Z}_p$ ist.
Für $p \neq 2$ prüft man leicht nach, dass $\mathfrak{G}_p = \mathfrak{F}_p'$ gilt. (Man setzt $A = t + uX + vY + wZ \in \mathfrak{F}_p'$ mit $t, u, v, w \in \mathbb{Q}_p$ an, und zeigt $t, u, v, w \in \mathbb{Z}_p$.) Für $p = 2$ prüft man genauso, dass gilt:

(i) Falls $\beta \equiv 0 \pmod 2$, ist $\{1, X, (Y-1)/2, Z/2\}$ eine $\mathbb{Z}_p$-Basis von $\mathfrak{F}_p'$,
und $\mathfrak{F}_p'$ hat die Diskriminante $(\alpha^2 - dd'\beta^2)^2\mathbb{Z}_p$.

(ii) Falls $\beta \equiv 1 \pmod 2$ und $d \not\equiv 3 \pmod 4$, ist $\mathfrak{F}_p' = \mathfrak{G}_p$.

(iii) Falls $\beta \equiv 1 \pmod 2$ und $d \equiv 3 \pmod 4$, ist $\{1, X, (\alpha + X + Y)/2, (1+Z)/2\}$ eine $\mathbb{Z}_p$-Basis von $\mathfrak{F}_p'$, und $\mathfrak{F}_p'$ hat die Diskriminante $(\alpha^2 - dd'\beta^2)^2\mathbb{Z}_p$.

Wir betrachten nun den verbleibenden Fall, dass $d' \equiv 3 \pmod 4$ und $p = 2$. Dann ist $T = \begin{pmatrix} \alpha + \beta i\sqrt{d} & 2\beta i\sqrt{d} \\ -\beta(1+d')i\sqrt{d}/2 & \alpha - \beta i\sqrt{d} \end{pmatrix}$. Sei in diesem Fall $\mathfrak{G}_p$ der $\mathbb{Z}_p$-Modul mit Basis

$\left\{1, \Omega, Y := \begin{pmatrix} -\alpha & \beta i\sqrt{d} \\ \beta(1+d')i\sqrt{d}/4 & 0 \end{pmatrix}, Z := \begin{pmatrix} \beta i\sqrt{d} & 0 \\ \alpha - \beta i\sqrt{d} & -\beta i\sqrt{d} \end{pmatrix}\right\}$. Dann hat $\mathfrak{G}_p$ die Diskriminante $(\alpha^2 - dd'\beta^2)^2\mathbb{Z}_p$, und man prüft im Einzelnen nach, dass gilt:

(iv) Falls $d \not\equiv 3 \pmod 4$, folgt aus $T \in \mathfrak{M}_p \smallsetminus 2\mathfrak{M}_p$, dass $\alpha, \beta \in \mathbb{Z}_p$, nicht beide durch 2 teilbar sind. Nun prüft man leicht, dass $\mathfrak{G}_p = F'_p \cap \mathfrak{M}_p$, also $\mathfrak{F}'_p = \mathfrak{G}_p$ gilt.

(v) Falls $d \equiv 3 \pmod 4$ und $\alpha, \beta \in \mathbb{Z}_p$, gilt $\alpha \equiv 0 \pmod 2$ oder $\beta \equiv 0 \pmod 2$. Auch in diesen Fällen prüft man leicht, dass $\mathfrak{F}'_p = \mathfrak{G}_p$ gilt.

(vi) Falls schließlich $d \equiv 3 \pmod 4$ und $\alpha, \beta \notin \mathbb{Z}_p$, gilt $\alpha' := 2\alpha \in \mathbb{Z}_p$, $\beta' := 2\beta \in \mathbb{Z}_p$ und $\alpha' \equiv \beta' \equiv 1 \pmod 2$. Dann ist $\{1, \Omega, (2Y - \Omega)/2, (2Z - 1)/2\}$ eine $\mathbb{Z}_p$-Basis von $\mathfrak{F}'_p$, und $\mathfrak{F}'_p$ hat die Diskriminante $16^{-1}(\alpha'^2 - dd'\beta'^2)^2\mathbb{Z}_p$.

Sei nun p eine endliche Stelle von $\mathbb{Q}$ mit $p \nmid \Delta(\mathfrak{F}')$ und o.B.d.A. $p \neq 2$.
Es gilt $\Phi_{F'}(T^*) = (T^*)^*$, $\Phi_F(A) = T^*\Phi_{F'}(A)(T^*)^{-1}$ für $A \in M$, und $T^* = \alpha - \beta i\sqrt{d}X$.
F'_p zerfällt und $\mathfrak{F}'_p$ ist eine F'_p-Maximalordnung. Wie oben im Fall $p \nmid \Delta(\mathfrak{F})$ folgt, dass es Matrizeseinheiten in F'_p gibt, bezüglich derer $\mathfrak{F}'_p = M_2(\mathbb{Z}_p)$ und $X = \Omega = \begin{pmatrix} 0 & 1 \\ -d' & 0 \end{pmatrix}$ gilt.
Dann ist $T^* = \begin{pmatrix} \alpha & -\beta i\sqrt{d} \\ \beta d' i\sqrt{d} & \alpha \end{pmatrix}$, und es gilt $\alpha, \beta \in \mathbb{Z}_p$, nicht beide durch p teilbar, und wie oben folgt, dass $\left\{1, X, \begin{pmatrix} -\alpha & -\beta i\sqrt{d} \\ -\beta d' i\sqrt{d} & \alpha \end{pmatrix}, \begin{pmatrix} -\beta i\sqrt{d} & 0 \\ 2\alpha & \beta i\sqrt{d} \end{pmatrix}\right\}$ eine $\mathbb{Z}_p$-Basis von $\mathfrak{F}_p$ mit Diskriminante $16(\alpha^2 - dd'\beta^2)^2\mathbb{Z}_p = (\alpha^2 - dd'\beta^2)^2\mathbb{Z}_p$ ist.
Wir beachten noch, dass $\mathfrak{F}_p$ und $\mathfrak{F}'_p$ im Fall $p \nmid \Delta(\mathfrak{F})\Delta(\mathfrak{F}')$ die Diskriminante $\mathbb{Z}_p$ haben, und fügen nun die lokalen Ergebnisse zusammen:
Das Produkt der Diskriminanten von $\mathfrak{F}$ und $\mathfrak{F}'$ ist $= (\alpha^2 - dd'\beta^2)^2\mathbb{Z}$ in den Fällen (i), (iii), (iv), (v) bzw. $16(\alpha^2 - dd'\beta^2)^2\mathbb{Z}$ im Fall (ii) bzw. $16^{-1}(\alpha'^2 - dd'\beta'^2)^2\mathbb{Z}$ im Fall (vi).
Also gilt $\Delta(\mathfrak{F})\Delta(\mathfrak{F}') = \pm(\alpha^2 - dd'\beta^2)$ bzw. $\pm 4(\alpha^2 - dd'\beta^2)$ bzw. $\pm(\alpha'^2 - dd'\beta'^2)/4$.
Nach Satz 3.4.(ii) ist $\alpha^2 - dd'\beta^2 = N(T) > 0$ genau dann, wenn F, F' an der Stelle ∞ das gleiche Verzweigungsverhalten haben, also $\Delta(\mathfrak{F})$ und $\Delta(\mathfrak{F}')$ gleiches Vorzeichen haben.
Wir setzen schließlich $x = \alpha$, $y = \beta$ in den Fällen (i)- (v) und $x = \alpha'$, $y = \beta'$ im Fall (vi). □

Satz 8.8. *Sei $d \in \mathbb{N}$ quadratfrei, sei $d \neq 1$, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Sei M eine k-Quaternionenalgebra.

(i) Seien $\mathfrak{M}$ eine M-Maximalordnung, $\mathcal{T} \subset P\Gamma(\mathfrak{M})$ eine Tetraedergruppe und $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$ eine 3-Diedergruppe. Sei $\mathcal{T} \cap \mathcal{D}_3$ eine Gruppe der Ordnung 2. Dann gilt $M \cong M_2(k)$ und $d \equiv 3 \pmod 8$, und es gibt $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 6$.

(ii) Sei umgekehrt $M \cong M_2(k)$ und $d \equiv 3 \pmod 8$, und seien $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 6$. Dann gibt es eine M-Maximalordnung $\mathfrak{M}$, so dass $P\Gamma(\mathfrak{M})$ Tetraedergruppen und 3-Diedergruppen enthält. Sei $\mathcal{C}_2 \subset P\Gamma(\mathfrak{M})$ eine Gruppe der Ordnung 2. Dann gilt:

(a) *Ist* $\mathcal{T} \subset P\Gamma(\mathfrak{M})$ *eine Tetraedergruppe mit* $\mathcal{C}_2 \subset \mathcal{T}$,
dann enthält $P\Gamma(\mathfrak{M})$ *bis auf* $P\Gamma(\mathfrak{M})$*-Konjugation genau*

- *eine 3-Diedergruppe* $\mathcal{D}_3$ *mit* $\mathcal{C}_2 \subset \mathcal{D}_3$, *falls* $d \equiv 0 \pmod 3$ *gilt*
- *zwei 3-Diedergruppen* $\mathcal{D}_3, \mathcal{D}_3'$ *mit* $\mathcal{C}_2 \subset \mathcal{D}_3, \mathcal{D}_3'$, *falls* $d \equiv 1 \pmod 3$ *gilt*

(b) *Ist* $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$ *eine 3-Diedergruppe mit* $\mathcal{C}_2 \subset \mathcal{D}_3$,
dann enthält $P\Gamma(\mathfrak{M})$ *bis auf* $P\Gamma(\mathfrak{M})$*-Konjugation genau*
zwei Tetraedergruppen $\mathcal{T}, \mathcal{T}'$ *mit* $\mathcal{C}_2 \subset \mathcal{T}, \mathcal{T}'$.

Beweis.

(i) Sei $F := F(\mathcal{T})$, und sei $\mathfrak{F} := \mathfrak{F}(\mathcal{T}) = F \cap \mathfrak{M}$. Dann gilt $\Delta(\mathfrak{F}) = -2$.
Sei $F' := F(\mathcal{D}_3)$, und sei $\mathfrak{F}' := \mathfrak{F}(\mathcal{D}_3) = F' \cap \mathfrak{M}$. Dann gilt $\Delta(\mathfrak{F}') = -3$.
Sei $d' := 1$, und sei X ein erzeugendes Element von $P^{-1}(\mathcal{T} \cap \mathcal{D}_3)$.
Dann gilt $X^2 = -d'$, und $\mathfrak{F} \cap \mathfrak{F}' = \mathbb{Z}[X]$ ist die Hauptordnung von $\mathbb{Q}(X)$.
Damit sind die Voraussetzungen von Lemma 8.7 gegeben, also gilt $M \cong M_2(k)$.
Wegen $\Delta(\mathfrak{F})\Delta(\mathfrak{F}') = 6$ und $d' \not\equiv 3 \pmod 4$ trifft notwendig Aussage 8.7.(iii) zu:
Es gibt $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 6$. Mit $d \equiv 3 \pmod 4$ folgt daraus $d \equiv 3 \pmod 8$.

(ii) Aus $x^2 - dy^2 = 6$ folgt $x \equiv y \equiv 1 \pmod 2$ und $d \not\equiv 2 \pmod 3$. Nach Satz 6.4.(ii) gibt es wegen $d \equiv 3 \pmod 8$ eine M-Maximalordnung $\mathfrak{M}$, so dass $P\Gamma(\mathfrak{M})$ Tetraedergruppen enthält. Mit (a) folgt, dass $P\Gamma(\mathfrak{M})$ auch 3-Diedergruppen enthält.

(a) Seien U, V, W Erzeugende von $P^{-1}(\mathcal{T})$ mit $U^2 = -1$, $VUV^{-1} = U^{-1}$ und $W = (1-U-V-UV)/2$, und o.B.d.A. sei V erzeugendes Element von $P^{-1}(\mathcal{C}_2)$.
Seien $a := (x + yi\sqrt{d})/2$ und $b := \overline{a}$. Dann gilt $a, b \in \mathfrak{o}$ und $a^2 + b^2 = 3$.
$U_3 := (1+aU+bUV)/2$ und V sind Erzeugende von $P^{-1}(\mathcal{D}_3)$ für eine 3-Diedergruppe $\mathcal{D}_3$ mit $\mathcal{C}_2 \subset \mathcal{D}_3$, und es gilt $U_3 \in \mathfrak{M}_p$ für alle endlichen Stellen $p \neq 2$.
$F(\mathcal{D}_3)$ zerfällt an der Stelle 2. Daher gibt es genau eine M_2-Maximalordnung $\mathfrak{M}_2'$ mit $\mathfrak{F}(\mathcal{D}_3) \subset \mathfrak{M}_2'$, und es gilt $k(V)_2 \cap \mathfrak{M}_2' = \mathfrak{o}_2[V]$. Man prüft elementar, dass $3W = (a+b+3)/2 - (a+b)U_3 + (a-b-3)V/2 - (a-b)U_3V$ und $3U = -a + bV + 2aU_3 - 2bU_3V$ gilt. Daraus folgt $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{M}_2'$. Nach Lemma 4.5.(ii) gilt also $\mathfrak{M}_2 = \mathfrak{M}_2'$ oder $\mathfrak{M}_2 = \Phi_{F(\mathcal{T})}(\mathfrak{M}_2')$. Wir ersetzen ggf. y durch $-y$ oder U_3 durch $\Phi_{F(\mathcal{T})}(U_3)$, können o.B.d.A. also $\mathfrak{M}_2 = \mathfrak{M}_2'$ annehmen.
Also gilt $k(V) \cap \mathfrak{M} = \mathfrak{o}[V]$, und es gilt $\mathfrak{F}(\mathcal{D}_3) \subset \mathfrak{M}$ oder äquivalent $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$.
Sei $\mathfrak{O}$ die Hauptordnung von $k(V)$. Wegen $d \equiv 3 \pmod 8$ gilt $\mathfrak{O} = \mathfrak{o}[V]$.
Sei $U_{-3} := (1+aU-bUV)/2$. Denn sind U_{-3} und V Erzeugende von $P^{-1}(\mathcal{D}_{-3})$ für eine 3-Diedergruppe $\mathcal{D}_{-3} \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{D}_{-3}$. Mit $UU_3U^{-1} = U_{-3}$ und $UVU^{-1} = V^{-1}$ folgt, dass $\mathcal{D}_3$ und $\mathcal{D}_{-3}$ zueinander $P\Gamma(\mathfrak{M})$-kongugiert sind.
Ist $\mathcal{D}_3' \subset P\Gamma(\mathfrak{M})$ eine 3-Diedergruppe mit $\mathcal{C}_2 \subset \mathcal{D}_3'$, so wird $P^{-1}(\mathcal{D}_3')$ von U_3', V erzeugt mit ${U_3'}^3 = -1$, $VU_3'V^{-1} = {U_3'}^{-1}$. Damit folgt $U_3' = (1 + a'U + b'UV)/2$ mit $a', b' \in k$ und $a'^2 + b'^2 = 3$, sowie $a' = -S(UU_3) \in \mathfrak{o}$ und $b' = S(VUU_3) \in \mathfrak{o}$.
Wegen $U^{-1}(U_3' - U_3) \in k(V) \cap \mathfrak{M} = \mathfrak{o}[V]$ gilt weiter $(a'-a) \in 2\mathfrak{o}$ und $(b'-b) \in 2\mathfrak{o}$.
$a' + b'V = U^{-1}(U_3' - U_3'^*)$ ist durch $\mathcal{D}_3'$ bis aufs Vorzeichen eindeutig bestimmt.
Sind umgekehrt $a', b' \in \mathfrak{o}$ mit $a'^2 + b'^2 = 3$ sowie $(a' - a) \in 2\mathfrak{o}$ und $(b' - b) \in 2\mathfrak{o}$,

so sind $U_3' := (1 + a'U + b'UV)/2$ und V Erzeugende von $P^{-1}(\mathcal{D}_3')$ für eine 3-Diedergruppe $\mathcal{D}_3' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{D}_3'$.

Sind $\mathcal{D}_3$ und $\mathcal{D}_3'$ zueinander $P\Gamma(\mathfrak{M})$-kongugiert, so gibt es ein $J' \in \Gamma(\mathfrak{M})$ mit $J'VJ'^{-1} = V^{\pm 1}$ sowie $J'U_3'J'^{-1} = U_3$, also (ersetze ggf. J' durch UJ') gibt es ein $J' \in \Gamma(\mathfrak{M})$ mit $J'VJ'^{-1} = V$ sowie $J'U_3'J'^{-1} = U_3$ oder $J'U_3'J'^{-1} = U_{-3}$. Dann ist $J' \in \Gamma(\mathfrak{o}[V])$. Mit $J'U = UJ'^*$ und $J'^* = J'^{-1}$ prüft man elementar nach, dass $a' + b'V = (a \pm bV)J'^2$, also $J'^2 = (a \pm bV)^{-1}(a' + b'V)$ gilt.
Gibt es umgekehrt ein $J' \in \Gamma(\mathfrak{o}[V])$ mit $J'^2 = (a \pm bV)^{-1}(a' + b'V)$, so prüft man ebenso elementar nach, dass $J'U_3'J'^{-1} = U_3$ bzw. $J'U_3'J'^{-1} = U_{-3}$ gilt, dass also $\mathcal{D}_3$ und $\mathcal{D}_3'$ zueinander $P\Gamma(\mathfrak{M})$-kongugiert sind.

Falls allgemeiner $X_\pm' := (a \pm bV)^{-1}(a' + b'V) \in \mathfrak{O}$ gilt, so kann man elementar nachrechnen, dass $X_\pm' \in \Gamma_2(\mathfrak{o}[V]) := \{X \in \Gamma(\mathfrak{o}[V]) \mid (X-1) \in 2\mathfrak{o}[V]\}$ gilt.
Ist umgekehrt ein $X' \in \Gamma_2(\mathfrak{o}[V])$ gegeben, so gilt $(a \pm bV)X' = a' + b'V$ mit $a', b' \in \mathfrak{o}$ und $a'^2 + b'^2 = 3$ sowie $(a' - a) \in 2\mathfrak{o}$ und $(b' - b) \in 2\mathfrak{o}$.

- Falls $d \equiv 0 \pmod 3$, ist 3 in k verzweigt. Sei $3\mathfrak{o} = \mathfrak{p}^2$. Da 3 in $\mathbb{Q}(V)$ träge ist, ist $\mathfrak{p}$ in $k(V)$ träge. Sei $\mathfrak{p}\mathfrak{O} = \mathfrak{P}$. Wegen $N(a \pm bV) = N(a' + b'V) = 3$ ist dann notwendig $(a \pm bV)\mathfrak{O} = (a' + b'V)\mathfrak{O} = \mathfrak{P}$, also $X_\pm' \in \Gamma_2(\mathfrak{o}[V])$.
  Wären $\mathcal{D}_3$ und $\mathcal{D}_3'$ nicht $P\Gamma(\mathfrak{M})$-kongugiert, so wäre weder $X_+' \in \Gamma(\mathfrak{o}[V])^{(2)}$ noch $X_-' \in \Gamma(\mathfrak{o}[V])^{(2)}$. Nach Lemma 8.2.(ii) gilt $[\Gamma_2(\mathfrak{o}[V]) : \Gamma(\mathfrak{o}[V])^{(2)}] = 2$. Also wäre ${X_+'}^{-1}X_-' \in \Gamma(\mathfrak{o}[V])^{(2)}$, das heißt es gäbe ein $J \in \Gamma(\mathfrak{o}[V])$ mit $(a + bV)(a - bV)^{-1} = J^2$. Sei $J = \alpha + \beta V$ mit $\alpha, \beta \in k$. Damit folgt $(\alpha - \beta V)(a + bV) = (\alpha + \beta V)(a - bV)$, und daraus folgt $\alpha b = \beta a$. Mit $1 = N(J) = \alpha^2 + \beta^2$ und $a^2 + b^2 = 3$ folgt $(a/\alpha)^2 = 3$, Widerspruch.
- Falls $d \equiv 1 \pmod 3$, ist 3 in k träge und in $\mathbb{Q}(i\sqrt{d}V)$ zerlegt. Also ist $3\mathfrak{o}$ in $k(V)$ zerlegt. Sei $3\mathfrak{O} = \mathfrak{P}\mathfrak{P}^*$ und $(a+bV)\mathfrak{O} = \mathfrak{P}$, also $(a-bV)\mathfrak{O} = \mathfrak{P}^*$. Mit $(a' + b'V)\mathfrak{O} \in \{\mathfrak{P}, \mathfrak{P}^*\}$ folgt entweder $X_+' \in \Gamma_2(\mathfrak{o}[V])$ oder $X_-' \in \Gamma_2(\mathfrak{o}[V])$. Wir wählen $\mathcal{D}_3'$ so, dass $X_+' \in \Gamma_2(\mathfrak{o}[V]) \setminus \Gamma(\mathfrak{o}[V])^{(2)}$. Dann sind $\mathcal{D}_3, \mathcal{D}_3'$ nicht $P\Gamma(\mathfrak{M})$-kongugiert, weil weder $X_+' \in \Gamma(\mathfrak{o}[V])^{(2)}$ noch $X_-' \in \Gamma(\mathfrak{o}[V])^{(2)}$ gilt.
  Wir prüfen nun die $P\Gamma(\mathfrak{M})$-Konjugationsklasse einer (beliebigen) 3-Diedergruppe $\mathcal{D}_3'' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{D}_3''$. Es gibt $a'', b'' \in \mathfrak{o}$ mit $a''^2 + b''^2 = 3$ und $(a'' - a) \in 2\mathfrak{o}$, $(b'' - b) \in 2\mathfrak{o}$, so dass $U_3'' := (1 + a''U + b''UV)/2$, V Erzeugende von $P^{-1}(\mathcal{D}_3'')$ sind. Wegen $UU_3''U^{-1} = (1 + a''U - b''UV)/2$ können wir o.B.d.A. $X_+'' := (a + bV)^{-1}(a'' + b''V) \in \Gamma_2(\mathfrak{o}[V])$ annehmen. Ist $\mathcal{D}_3''$ nicht $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{D}_3$, so ist $X_+'' \notin \Gamma(\mathfrak{o}[V])^{(2)}$. Also gibt es ein $J \in \Gamma(\mathfrak{o}[V])$ mit $(a' + b'V)^{-1}(a'' + b''V) = {X_+'}^{-1}X_+'' = J^2$. Damit folgt elementar $JU_3''J^{-1} = U_3'$, also ist $\mathcal{D}_3''$ dann $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{D}_3'$.

(b) Sei t die Anzahl der Primteiler von D. Nach Satz 7.5.(ii) gibt es bis auf $P\Gamma(\mathfrak{M})$-Konjugation genau 2^t Tetraedergruppen $\mathcal{T}$ in $P\Gamma(\mathfrak{M})$. Nach Satz 8.3.(ii) gibt es daher bis auf $P\Gamma(\mathfrak{M})$-Konjugation genau 2^{t-1} Gruppen $\mathcal{C}_2' \subset P\Gamma(\mathfrak{M})$ der Ordnung 2, die in einer Tetraedergruppe $\mathcal{T}$ in $P\Gamma(\mathfrak{M})$ enthalten sind.
Nach (a) ist die Anzahl der 3-Diedergruppen $\mathcal{D}_3$ in $P\Gamma(\mathfrak{M})$, die eine solche Gruppe $\mathcal{C}_2'$ enthalten, bis auf $P\Gamma(\mathfrak{M})$-Konjugation gleich

- 2^{t-1}, falls $d \equiv 0 \pmod 3$
- 2^t, falls $d \equiv 1 \pmod 3$

Nach Satz 7.5.(i) ist diese Anzahl gleich der Anzahl aller $P\Gamma(\mathfrak{M})$-Konjugationsklassen von 3-Diedergruppen $\mathcal{D}_3$ in $P\Gamma(\mathfrak{M})$. Also enthält jede 3-Diedergruppe $\mathcal{D}_3$ in $P\Gamma(\mathfrak{M})$ eine solche Gruppe $\mathcal{C}_2'$. Die Behauptung folgt nun mit Satz 8.3.(ii).

□

Satz 8.9. *Sei $d \in \mathbb{N}$ quadratfrei, sei $d \neq 1$, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Sei M eine k-Quaternionenalgebra.

(i) Seien $\mathfrak{M}$ eine M-Maximalordnung, $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$ maximalendliche 2-Diedergruppe und $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$ eine 3-Diedergruppe. Sei $\mathcal{D}_2 \cap \mathcal{D}_3$ eine Gruppe der Ordnung 2. Dann gilt $M \cong M_2(k)$, und es gibt $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 3$.
Ist V ein erzeugendes Element von $P^{-1}(\mathcal{D}_2 \cap \mathcal{D}_3)$, dann gilt $k(V) \cap \mathfrak{M} = \mathfrak{o}[V]$.

(ii) Sei umgekehrt $M \cong M_2(k)$, und seien $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 3$. Dann gibt es eine M-Maximalordnung $\mathfrak{M}$, so dass $P\Gamma(\mathfrak{M})$ maximalendliche 2-Diedergruppen und 3-Diedergruppen enthält. Sei $\mathcal{C}_2 \subset P\Gamma(\mathfrak{M})$ eine Gruppe der Ordnung 2. Dann gilt:

(a) Ist $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$ eine maximalendliche 2-Diedergruppe mit $\mathcal{C}_2 \subset \mathcal{D}_2$ und $k(V) \cap \mathfrak{M} = \mathfrak{o}[V]$ für ein erzeugendes Element V von $P^{-1}(\mathcal{C}_2)$, dann enthält $P\Gamma(\mathfrak{M})$ bis auf $P\Gamma(\mathfrak{M})$-Konjugation genau

- *eine 3-Diedergruppe $\mathcal{D}_3$ mit $\mathcal{C}_2 \subset \mathcal{D}_3$, falls $d \equiv 0 \pmod 3$ gilt*
- *zwei 3-Diedergruppen $\mathcal{D}_3, \mathcal{D}_3'$ mit $\mathcal{C}_2 \subset \mathcal{D}_3, \mathcal{D}_3'$, falls $d \equiv 1 \pmod 3$ gilt*

(b) Ist $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$ eine 3-Diedergruppe mit $\mathcal{C}_2 \subset \mathcal{D}_3$, dann enthält $P\Gamma(\mathfrak{M})$ bis auf $P\Gamma(\mathfrak{M})$-Konjugation genau

- *eine maximalendliche 2-Diedergruppe $\mathcal{D}_2$ mit $\mathcal{C}_2 \subset \mathcal{D}_2$, falls $d \equiv 2 \pmod 4$ gilt und es $x', y' \in \mathbb{Z}$ mit $x'^2 - dy'^2 = 2$ gibt*
- *zwei maximalendliche 2-Diedergruppen $\mathcal{D}_2, \mathcal{D}_2'$ mit $\mathcal{C}_2 \subset \mathcal{D}_2, \mathcal{D}_2'$, falls $d \not\equiv 2 \pmod 4$ gilt oder $x'^2 - dy'^2 \neq 2$ für alle $x', y' \in \mathbb{Z}$ gilt*

Beweis.

(i) Sei $F := F(\mathcal{D}_2)$ und $\mathfrak{F} := \mathfrak{F}(\mathcal{D}_2) = F \cap \mathfrak{M}$. Dann gilt $\Delta(\mathfrak{F}) = -4$.
Sei $F' := F(\mathcal{D}_3)$, und sei $\mathfrak{F}' := \mathfrak{F}(\mathcal{D}_3) = F' \cap \mathfrak{M}$. Dann gilt $\Delta(\mathfrak{F}') = -3$.
Sei $d' := 1$, und sei X ein erzeugendes Element von $P^{-1}(\mathcal{D}_2 \cap \mathcal{D}_3)$.
Dann gilt $X^2 = -d'$, und $\mathfrak{F} \cap \mathfrak{F}' = \mathbb{Z}[X]$ ist die Hauptordnung von $\mathbb{Q}(X)$.
Damit sind die Voraussetzungen von Lemma 8.7 gegeben, also gilt $M \cong M_2(k)$.
Wegen $\Delta(\mathfrak{F})\Delta(\mathfrak{F}') = 12$ und $d' \not\equiv 3 \pmod 4$ trifft notwendig Aussage 8.7.(ii) zu:
Es gibt $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 3$.

(ii) Aus $x^2 - dy^2 = 3$ folgt $d \not\equiv 3 \pmod 4$, $y \equiv 1 \pmod 2$ und $d \not\equiv 2 \pmod 3$.
Nach Satz 6.6 gibt es eine M-Maximalordnung $\mathfrak{M}$, so dass $P\Gamma(\mathfrak{M})$ maximalendliche 2-Diedergruppen enthält. Mit (a) folgt, dass $P\Gamma(\mathfrak{M})$ auch 3-Diedergruppen enthält.

(a) Seien U, V Erzeugende von $P^{-1}(\mathcal{D}_2)$ mit $U^2 = -1$, $VUV^{-1} = U^{-1}$. Wir ersetzen ggf. U durch UV, können nach Lemma 8.1.(ii) also $k(U) \cap \mathfrak{M} = \mathfrak{o}[U]$ annehmen. Seien $a := x$ und $b := yi\sqrt{d}$, falls $d \equiv 1 \pmod 4$, bzw. $a := yi\sqrt{d}$ und $b := x$, falls $d \equiv 2 \pmod 4$. Dann gilt $a, b \in \mathfrak{o}$ und $a^2 + b^2 = 3$ sowie $b \in \mathfrak{o}_2^\times$. $U_3 := (1 + aU + bUV)/2$ und V sind Erzeugende von $P^{-1}(\mathcal{D}_3)$ für eine 3-Diedergruppe $\mathcal{D}_3$ mit $\mathcal{C}_2 \subset \mathcal{D}_3$, und es gilt $U_3 \in \mathfrak{M}_p$ für alle endlichen Stellen $p \neq 2$. $F(\mathcal{D}_3)$ zerfällt an der Stelle 2. Daher gibt es genau eine M_2-Maximalordnung $\mathfrak{M}_2'$ mit $\mathfrak{F}(\mathcal{D}_3) \subset \mathfrak{M}_2'$, und es gilt $k(V)_2 \cap \mathfrak{M}_2' = \mathfrak{o}_2[V]$. Man prüft elementar, dass $3U = -a + bV + 2aU_3 - 2bU_3V$ gilt. Daraus folgt $\mathfrak{F}(\mathcal{D}_2) \subset \mathfrak{M}_2'$, und wegen $b \in \mathfrak{o}_2^\times$ gilt $k(U)_2 \cap \mathfrak{M}_2' = \mathfrak{o}_2[U]$. Mit Lemma 8.1.(iii) folgt daraus $\mathfrak{M}_2' = \mathfrak{M}_2$. Also gilt $k(V) \cap \mathfrak{M} = \mathfrak{o}[V]$, und es gilt $\mathfrak{F}(\mathcal{D}_3) \subset \mathfrak{M}$ oder äquivalent $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$. Sei $\mathfrak{O}$ die Hauptordnung von $k(V)$. Wegen $d \not\equiv 3 \pmod 4$ gilt $\mathfrak{O} \neq \mathfrak{o}[V]$. Trotzdem können wir ab hier den Beweis von Satz 8.8.(ii)(a) wörtlich übernehmen,

(b) Sei t die Anzahl der verschiedenen Primteiler von D. Nach Satz 7.5.(iii) gibt es bis auf $P\Gamma(\mathfrak{M})$-Konjugation genau 2^{t-1} maximalendliche 2-Diedergruppen $\mathcal{D}_2$ in $P\Gamma(\mathfrak{M})$. Nach Satz 8.4.(i) bzw. nach Satz 8.4.(ii) gibt es daher bis auf $P\Gamma(\mathfrak{M})$-Konjugation genau 2^{t-1} Gruppen $\mathcal{C}_2' \subset P\Gamma(\mathfrak{M})$ der Ordnung 2, die in einer maximalendlichen 2-Diedergruppe $\mathcal{D}_2$ in $P\Gamma(\mathfrak{M})$ enthalten sind, und für die $k(V') \cap \mathfrak{M} = \mathfrak{o}[V']$ gilt, falls V' ein erzeugendes Element von $P^{-1}(\mathcal{C}_2')$ ist. Nach (a) ist die Anzahl der 3-Diedergruppen $\mathcal{D}_3$ in $P\Gamma(\mathfrak{M})$, die eine solche Gruppe $\mathcal{C}_2'$ enthalten, bis auf $P\Gamma(\mathfrak{M})$-Konjugation gleich

- 2^{t-1}, falls $d \equiv 0 \pmod 3$
- 2^t, falls $d \equiv 1 \pmod 3$

Nach Satz 7.5.(i) ist diese Anzahl gleich der Anzahl aller $P\Gamma(\mathfrak{M})$-Konjugationsklassen von 3-Diedergruppen $\mathcal{D}_3$ in $P\Gamma(\mathfrak{M})$. Also enthält jede 3-Diedergruppe $\mathcal{D}_3$ in $P\Gamma(\mathfrak{M})$ eine solche Gruppe $\mathcal{C}_2'$. Die Behauptung folgt nun mit Satz 8.4.

□

Lemma 8.10. *Sei $d \in \mathbb{N}$ quadratfrei, $d \neq 3$, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung $\mathfrak{o}$. Sei $U \in SL_2(\mathbb{C})$, $U \neq -1$, mit $U^3 = -1$, und sei $Y := U - U^*$, also $Y^2 = -3$.*

(i) Sei $K := k(U)$ mit Hauptordnung $\mathfrak{O}$, sei $k_+ := \mathbb{Q}(i\sqrt{d}Y)$ mit Hauptordnung $\mathfrak{o}_+$, und sei $\mathcal{U} \subset \Gamma(\mathfrak{o}[U])$ die von U erzeugte Untergruppe. Dann ist $\mathcal{U}$ die Gruppe der Einheitswurzeln in K mit Norm 1, und es gilt $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] \leq 2$. Weiterhin gilt $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] = 2$ genau dann, wenn es $x, y \in \mathbb{Z}$ gibt mit $x^2 - 3dy^2 = 12$.

(ii) $\Gamma_3(\mathfrak{o}[U]) := \{A \in \Gamma(\mathfrak{o}[U]) \mid (A - 1) \in Y\mathfrak{o}[U]\}$ ist Gruppe mit $\Gamma(\mathfrak{o}[U])^{(2)} \subset \Gamma_3(\mathfrak{o}[U])$ und $[\Gamma_3(\mathfrak{o}[U]) : \Gamma(\mathfrak{o}[U])^{(2)}] \leq 2$. Genau dann gilt $[\Gamma_3(\mathfrak{o}[U]) : \Gamma(\mathfrak{o}[U])^{(2)}] = 1$, wenn $d \equiv 2 \pmod 3$ gilt und es $x, y \in \mathbb{Z}$ gibt mit $x^2 - 3dy^2 = 12$.

Bemerkung: Aus $x^2 - 3dy^2 \equiv 12 \pmod 9$ folgt leicht $d \equiv 2 \pmod 3$.

Beweis. Man sieht leicht ein (siehe Lemma 6.2), dass U die Gruppe der Einheitswurzeln von K mit Norm 1 erzeugt. K ist ein algebraischer Zahlkörper mit zwei komplexen

Stellen. Also ist $\Gamma(\mathfrak{O})$ direktes Produkt von $\mathcal{U}$ und einer zyklischen unendlichen Gruppe. Wegen $U \notin \mathcal{U}^{(2)} = \{1, U^2, U^4\}$ folgt daraus $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{O})^{(2)}] = [\Gamma(\mathfrak{o}[U]) : \Gamma(\mathfrak{o}[U])^{(2)}] = 4$. Sei $\mathcal{U}'$ die Gruppe aller Einheitswurzeln von K, und sei ϵ eine Grundeinheit von K.

(i) Sei ϵ_+ eine Grundeinheit von k_+. Falls $d = 1$, wird $\mathcal{U}'$ von iU mit $N(iU) = -1$ erzeugt, und wir können $\epsilon_+ = 2+iY$ mit $N(\epsilon_+) = 1$ sowie $\epsilon = ((1-i)+(1+i)Y)/2$ mit $N(\epsilon) = i$ und $\epsilon_+ = i\epsilon^2$ annehmen, siehe [3, § 26 (8)]. $\Gamma(\mathfrak{O})$ wird von $U = -(iU)^2$ und $\epsilon_+ = U^{-1}(iU)\epsilon^2$ erzeugt. Also ist $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] = 1$, und die Gleichung $x^2 - 3y^2 = 12$ ist ganzzahlig nicht lösbar. Wir können ab hier also $d \neq 1$ annehmen. Dann gilt $\mathcal{U}' = \mathcal{U}$, nach [3, § 20, Satz 14] also $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] \leq [\mathfrak{O}^\times : \mathcal{U}'\mathfrak{o}_+^\times] \leq 2$.

Für $d \equiv 0 \pmod 3$ ist $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] = [\mathfrak{O}^\times : \mathcal{U}'\mathfrak{o}_+^\times] = 1$, siehe [3, § 26 ($10_\mathrm{I}$)], und $x^2 - 3dy^2 = 12$ ist $\pmod 9$ unlösbar. Wir können also $d \not\equiv 0 \pmod 3$ annehmen. Es ist $\epsilon = (a + bY)/2$ mit $a, b \in \mathfrak{o}$ und $a = \alpha + \alpha' i\sqrt{d}$, $b = \beta + \beta' i\sqrt{d}$ und $\epsilon_+ = (\gamma + \gamma' i\sqrt{d}Y)/2$ mit $\alpha, \alpha', \beta, \beta', \gamma, \gamma' \in \mathbb{Z}$. Falls $[\mathfrak{O}^\times : \mathcal{U}'\mathfrak{o}_+^\times] = 2$, können wir $\epsilon_+ = -\epsilon^2 \in \Gamma(\mathfrak{o}_+)$ annehmen, siehe [3, § 26 (8)]. Dann folgt $2N(\epsilon) - 2\epsilon_+ = a^2 + abY$, also speziell $2N(\epsilon) - \gamma = \alpha^2 - d\alpha'^2$, $0 = \alpha\alpha'$, $0 = \alpha\beta - d\alpha'\beta'$ und $-\gamma' = \alpha\beta' + \alpha'\beta$. Wäre $\alpha' = 0$, so wäre auch $\beta = 0$ und $\epsilon = (\alpha + \beta' i\sqrt{d}Y)/2 \in k_+$, Widerspruch. Also ist $\alpha = \beta' = 0$ und $\epsilon = (\alpha' i\sqrt{d} + \beta Y)/2$ und $4N(\epsilon) = -d\alpha'^2 + 3\beta^2$.

- Sei $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] = 2$. Dann gilt auch $[\mathfrak{O}^\times : \mathcal{U}'\mathfrak{o}_+^\times] = 2$. Wäre $N(\epsilon) = -1$, so würde $\Gamma(\mathfrak{O})$ von U und $\epsilon^2 = -\epsilon_+ U$ erzeugt, also wäre $\Gamma(\mathfrak{O}) = \mathcal{U}\Gamma(\mathfrak{o}_+)$, Widerspruch. Daher gilt $N(\epsilon) = 1$, also $x^2 - 3dy^2 = 12$ mit $x = 3\beta$, $y = \alpha'$.
- Sei umgekehrt $x^2 - 3dy^2 = 12$ mit $x, y \in \mathbb{Z}$. Dann gilt $\pi := (x + yi\sqrt{d}Y)/2 \in \mathfrak{o}_+$ mit $N(\pi) = 3$, und nach [3, § 26 (12_I)] ist $[\mathfrak{O}^\times : \mathcal{U}'\mathfrak{o}_+^\times] = 2$. Aus $N(\epsilon) = -1$ folgt $N(\pi') = -3$ für $\pi' := (3\beta + \alpha' i\sqrt{d}Y)/2 \in \mathfrak{o}_+$, also $N(e_+) = -1$, Widerspruch zu [3, § 26 (9)]. Also gilt $N(\epsilon) = N(\epsilon_+) = 1$ und $\Gamma(\mathfrak{O}) = \mathfrak{O}^\times$, $\Gamma(\mathfrak{o}_+) = \mathfrak{o}_+^\times$.

(ii) Es gilt $U^* = 1 - U$ und $UU^* = 1$ sowie $Y^* = -Y$ und $Y = 2U - 1 = U(1 + U)$. Für $A = 1 + YB \in \Gamma_3(\mathfrak{o}[U])$ gilt $A^{-1} = A^* = 1 - YB^* \in \Gamma_3(\mathfrak{o}[U])$, und $\Gamma_3(\mathfrak{o}[U])$ ist multiplikativ abgeschlossen, also eine Gruppe. Für $A = a + bU \in \Gamma(\mathfrak{o}[U])$ mit $a, b \in \mathfrak{o}$ gilt $A - A^* = bY$ und $A^2 = 1 + bAY \in \Gamma_3(\mathfrak{o}[U])$, also gilt $\Gamma(\mathfrak{o}[U])^{(2)} \subset \Gamma_3(\mathfrak{o}[U])$. Wegen $U \notin \Gamma_3(\mathfrak{o}[U])$ gilt $[\Gamma(\mathfrak{o}[U]) : \Gamma_3(\mathfrak{o}[U])] \geq 2$, also $[\Gamma_3(\mathfrak{o}[U]) : \Gamma(\mathfrak{o}[U])^{(2)}] \leq 2$.

Sei zunächst $d \not\equiv 2 \pmod 3$. also 3 in k verzweigt oder träge, $3\mathfrak{o} = \mathfrak{p}^2$ oder $3\mathfrak{o} = \mathfrak{p}$. Für $A = a + bU \in \Gamma(\mathfrak{o}[U])$ mit $a, b \in \mathfrak{o}$. gilt $a^2 + ab + b^2 = 1$ oder gleichwertig $(a - b - 1)(a - b + 1) = -3ab$. Also gilt $a - b - 1 = 3c$ oder $a - b + 1 = 3c$ mit $c \in \mathfrak{o}$. Falls $a - b - 1 = 3c$, folgt mit $YY^* = 3$, dass $A = 1 + Y(cY^* + bU^*) \in \Gamma_3(\mathfrak{o}[U])$. Falls $a - b + 1 = 3c$, sei $a' = -b$ und $b' = a + b$, also $a' - b' - 1 = 3c'$ mit $c' = -c - b$. Dann gilt $AU = a' + b'U = 1 + Y(c'Y^* + b'U^*) \in \Gamma_3(\mathfrak{o}[U])$. Daher gilt $A \in \Gamma_3(\mathfrak{o}[U])$ oder $AU \in \Gamma_3(\mathfrak{o}[U])$, also $[\Gamma(\mathfrak{o}[U]) : \Gamma_3(\mathfrak{o}[U])] = [\Gamma_3(\mathfrak{o}[U]) : \Gamma(\mathfrak{o}[U])^{(2)}] = 2$.

Sei nun $d \equiv 2 \pmod 3$ und zunächst $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] = 1$. Sei $A \in \Gamma(\mathfrak{o}[U]) = \Gamma(\mathfrak{O})$. Dann gilt $A = A'$ oder $A = UA'$ mit $A' = (a' + b' i\sqrt{d}Y)/2$ und $a', b' \in \mathbb{Z}$ mit $a'^2 - 3db'^2 = 4$. Es gilt $(a' - 2) \in 3\mathbb{Z}$ oder $(a' - 4) \in 3\mathbb{Z}$, somit $A' \in \Gamma_3(\mathfrak{o}[U])$ oder $UA' = ((a' - 3b' i\sqrt{d}) + (a' + b' i\sqrt{d})Y)/4 \in \Gamma_3(\mathfrak{o}[U])$. Also ist $[\Gamma(\mathfrak{o}[U]) : \Gamma_3(\mathfrak{o}[U])] = 2$.

Sei nun $d \equiv 2 \pmod 3$ und $[\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] = 2$. Wie in (i) sei $\epsilon = (\alpha' i\sqrt{d} + \beta Y)/2$ mit $\alpha', \beta \in \mathbb{Z}$ und $3\beta^2 - d\alpha'^2 = 4$. Dann ist $U\epsilon = ((\alpha' i\sqrt{d} - 3\beta) + (\alpha' i\sqrt{d} + \beta)Y)/4$. Mit $\alpha' i\sqrt{d} \pm 1 \notin 3\mathfrak{o}$ folgt leicht, dass $\epsilon, U\epsilon \notin \Gamma_2(\mathfrak{o}[U])$, also $[\Gamma(\mathfrak{o}[U]) : \Gamma_3(\mathfrak{o}[U])] = 4$.

□

Satz 8.11. *Sei $d \in \mathbb{N}$ quadratfrei, sei $d \neq 3$, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Sei M eine k-Quaternionenalgebra.

(i) Seien $\mathfrak{M}$ eine M-Maximalordnung, $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$ eine 3-Diedergruppe und $\mathcal{T} \subset P\Gamma(\mathfrak{M})$ eine Tetraedergruppe. Sei $\mathcal{D}_3 \cap \mathcal{T}$ eine Gruppe der Ordnung 3. Dann gilt $M \cong M_2(k)$, und es gibt $x, y \in \mathbb{Z}$ mit $x^2 - 3dy^2 = 24$.

(ii) Sei umgekehrt $M \cong M_2(k)$ und seien $x, y \in \mathbb{Z}$ mit $x^2 - 3dy^2 = 24$. Dann gibt es eine M-Maximalordnung $\mathfrak{M}$, so dass $P\Gamma(\mathfrak{M})$ sowohl 3-Diedergruppen als auch Tetraedergruppen enthält. Sei $\mathcal{C}_3 \subset P\Gamma(\mathfrak{M})$ eine Gruppe der Ordnung 3. Dann gilt:

(a) Sei $\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$ eine 3-Diedergruppe mit $\mathcal{C}_3 \subset \mathcal{D}_3$.
Dann enthält $P\Gamma(\mathfrak{M})$ bis auf $P\Gamma(\mathfrak{M})$-Konjugation genau
- *eine Tetraedergruppe $\mathcal{T}$ mit $\mathcal{C}_3 \subset \mathcal{T}$, falls $d \not\equiv 3 \pmod 4$*
- *zwei Tetraedergruppen $\mathcal{T}, \mathcal{T}'$ mit $\mathcal{C}_3 \subset \mathcal{T}$, $\mathcal{C}_3 \subset \mathcal{T}'$, falls $d \equiv 3 \pmod 8$.*

(b) Sei $\mathcal{T} \subset P\Gamma(\mathfrak{M})$ eine Tetraedergruppe mit $\mathcal{C}_3 \subset \mathcal{T}$.
Dann enthält $P\Gamma(\mathfrak{M})$ bis auf $P\Gamma(\mathfrak{M})$-Konjugation genau zwei 3-Diedergruppen $\mathcal{D}_3, \mathcal{D}_3'$ mit $\mathcal{C}_3 \subset \mathcal{D}_3$, $\mathcal{C}_3 \subset \mathcal{D}_3'$.

Beweis.

(i) Sei $F := F(\mathcal{D}_3)$, und sei $\mathfrak{F} := \mathfrak{F}(\mathcal{D}_3) = F \cap \mathfrak{M}$. Dann ist $\Delta(\mathfrak{F}) = -3$.
Sei $F' := F(\mathcal{T})$, und sei $\mathfrak{F}' := \mathfrak{F}(\mathcal{T}) = F' \cap \mathfrak{M}$. Dann gilt $\Delta(\mathfrak{F}') = -2$.
Sei $d' := 3$, sei U ein erzeugendes Element von $P^{-1}(\mathcal{D}_3 \cap \mathcal{T})$, und sei $X := U - U^*$.
Dann gilt $X^2 = -d'$, und $\mathfrak{F} \cap \mathfrak{F}' = \mathbb{Z}[U]$ ist die Hauptordnung von $\mathbb{Q}(X) = \mathbb{Q}(U)$.
Damit sind die Voraussetzungen von Lemma 8.7 gegeben, also gilt $M \cong M_2(k)$.
Wegen $d' \equiv 3 \pmod 4$ trifft notwendig eine der Aussagen 8.7.(iv)-(vi) zu,
die wir zusammenfassen: Es gibt $x, y \in \mathbb{Z}$ mit $x^2 - 3dy^2 = 4\Delta(\mathfrak{F})\Delta(\mathfrak{F}') = 24$.

(ii) Aus $x^2 - 3dy^2 = 24$ folgt $d \equiv 1 \pmod 3$ sowie entweder $d \not\equiv 3 \pmod 4$ und $x \equiv y \equiv 0 \pmod 2$ oder $d \equiv 3 \pmod 8$ und $x \equiv y \equiv 1 \pmod 2$. Nach Satz 6.4.(i) gibt es wegen $d \equiv 1 \pmod 3$ eine M-Maximalordnung $\mathfrak{M}$, so dass $P\Gamma(\mathfrak{M})$ 3-Diedergruppen enthält. Mit (a) folgt, dass $P\Gamma(\mathfrak{M})$ auch Tetraedergruppen enthält.
3 ist träge in k, und $3\mathfrak{o}$ ist verzweigt in $k(U)$ mit Hauptordnung $\mathfrak{o}[U]$. Sei $3\mathfrak{o}[U] = \mathfrak{R}^2$.

(a) Seien U, V Erzeugende von $P^{-1}(\mathcal{D}_3)$ mit $U^3 = -1$, $VUV^{-1} = U^{-1}$. Dann wird $P^{-1}(\mathcal{C}_3)$ von U erzeugt, und es gilt $k(U) \cap \mathfrak{M} = \mathfrak{o}[U]$. Seien $a := (x + 3yi\sqrt{d})/2$ und $b := (x - yi\sqrt{d})/2$. Dann gilt $a, b \in \mathfrak{o}$ und $a^2 + 3b^2 = 24$. Seien $Y := U - U^*$ sowie $U_t := (-2Y + xV - yi\sqrt{d}YV)/6$, $V_t := (-2Y - aV - bYV)/6$ und $W_t := U$.

Dann gilt $U_t^2 = -1$, $V_t U_t V_t^{-1} = U_t^{-1}$ und $W_t = (1 - U_t - V_t - U_t V_t)/2$.
Sei $\mathcal{T}$ die von $P(U_t)$, $P(V_t)$ und $P(W_t)$ erzeugte Tetraedergruppe. Dann gilt offenbar $\mathcal{C}_3 \subset \mathcal{T}$, und es gilt $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{M}_p$ für alle endlichen Stellen $p \neq 2, 3$, und mit $Y = 2U - 1$ sowie $(x + yi\sqrt{d}) \in 2\mathfrak{o}$ und $(a - b) \in 2\mathfrak{o}$ folgt auch $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{M}_2$. $F(\mathcal{T})$ zerfällt an der Stelle 3. Daher gibt es genau eine M_3-Maximalordnung $\mathfrak{M}_3'$ mit $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{M}_3'$. Man prüft elementar, dass $6V = xU_t - aV_t - \overline{a}U_t V_t$ gilt. Mit $x \in 3\mathbb{Z}$ und $a \in 3\mathfrak{o}$ folgt daraus $\mathfrak{F}(\mathcal{D}_3) \subset \mathfrak{M}_3'$. Nach Lemma 4.5.(ii) gilt also $\mathfrak{M}_3 = \mathfrak{M}_3'$ oder $\mathfrak{M}_3 = \Phi_{F(\mathcal{D}_3)}(\mathfrak{M}_3')$. Wir ersetzen ggf. y durch $-y$ oder U_t und V_t durch $\Phi_{F(\mathcal{D}_3)}(U_t)$ und $\Phi_{F(\mathcal{D}_3)}(V_t)$, können o.B.d.A. also $\mathfrak{M}_3 = \mathfrak{M}_3'$ annehmen. Also gilt $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{M}$ oder äquivalent $\mathcal{T} \subset P\Gamma(\mathfrak{M})$.
Seien $U_{-t} := -VV_tV^{-1}$, $V_{-t} := -VU_tV^{-1}$, $W_{-t} := (1 - U_{-t} - V_{-t} - U_{-t}V_{-t})/2$. Dann sind $U_{-t} = (-2Y + aV - bYV)/6$, $V_{-t} = (-2Y - xV - yi\sqrt{d}YV)/6$ und $W_{-t} = VW_tV^{-1} = U^{-1}$ Erzeugende von $P^{-1}(\mathcal{T}_-)$ für eine Tetraedergruppe $\mathcal{T}_- \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_3 \subset \mathcal{T}_-$. Und $\mathcal{T}$ und $\mathcal{T}_-$ sind zueinander $P\Gamma(\mathfrak{M})$-kongugiert.
Ist $\mathcal{T}' \subset P\Gamma(\mathfrak{M})$ eine Tetraedergruppe mit $\mathcal{C}_3 \subset \mathcal{T}'$, so wird $P^{-1}(\mathcal{T}')$ von U_t', V_t' und U erzeugt mit $U_t'^2 = -1$, $V_t'U_t'V_t'^{-1} = U_t'^{-1}$ und $U = (1 - U_t' - V_t' - U_t'V_t')/2$. Es gibt $a', b', c' \in \mathfrak{o}$ mit $V_t' = (-c'Y - a'V - b'YV)/6$. Mit $UV_t'U^{-1} = U_t'$ folgt $U_t' = (-c'Y + (a' + 3b')V/2 - (a' - b')YV/2)/6$ sowie $a'^2 + 3b'^2 = 24$ und $c' = 2$ mit $a' \in 3\mathfrak{o}$ und $(a' - b') \in 2\mathfrak{o}$. Wegen $(V_t' - V_t)V^{-1} \in \mathfrak{o}[U]$ gilt $(b' - b) \in 3\mathfrak{o}$, und man sieht leicht ein, dass $a' + b'Y = (6V_t' + 2Y)V$ durch $\mathcal{T}'$ bis auf einen Faktor $U^{\pm 2}$ eindeutig bestimmt ist. (Man kann V_t' durch U_t' oder $U_t'V_t'$ ersetzen.)
Sind umgekehrt $a', b' \in \mathfrak{o}$ mit $a'^2 + 3b'^2 = 24$ sowie $(b' - b) \in 3\mathfrak{o}$, so sind $U_t' := (-2Y + (a' + 3b')V/2 - (a' - b')YV/2)/6$, $V_t' := (-2Y - a'V - b'YV)/6$, U Erzeugende von $P^{-1}(\mathcal{T}')$ für eine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_3 \subset \mathcal{T}'$.
Sind $\mathcal{T}$ und $\mathcal{T}'$ zueinander $P\Gamma(\mathfrak{M})$-kongugiert, so gibt es ein $J' \in \Gamma(\mathfrak{M})$ mit $J'U_tJ'^{-1} = U_t'$, $J'V_tJ'^{-1} = V_t'$ (und $J'UJ'^{-1} = U$) oder mit $J'U_tJ'^{-1} = -V_t'$, $J'V_tJ'^{-1} = -U_t'$ (und $J'UJ'^{-1} = U^{-1}$). Also (ersetze ggf. J' durch $J'V$) gibt es ein $J' \in \Gamma(\mathfrak{M})$ mit $J'U_tJ'^{-1} = U_t'$, $J'V_tJ'^{-1} = V_t'$ (und $J'UJ'^{-1} = U$) oder mit $J'U_{-t}J'^{-1} = U_t'$, $J'V_{-t}J'^{-1} = V_t'$ (und $J'UJ'^{-1} = U$). Dann ist $J' \in \Gamma(\mathfrak{o}[U])$. Mit $J'V = VJ'^*$ und $J'^* = J'^{-1}$ sowie $a' + b'Y = (6V_t' + 2Y)V$ folgt $a' + b'Y = J'(6V_t + 2Y)J'^{-1}V = (a + bY)J'^2$ oder $a' + b'Y = (x + yi\sqrt{d}Y)J'^2$. Also gilt $J'^2 = (a + bY)^{-1}(a' + b'Y)$ oder $J'^2 = (x + yi\sqrt{d}Y)^{-1}(a' + b'Y)$.
Gibt es umgekehrt ein $J' \in \Gamma(\mathfrak{o}[U])$ mit $J'^2 = (a + bY)^{-1}(a' + b'Y)$ oder mit $J'^2 = (x + yi\sqrt{d}Y)^{-1}(a' + b'Y)$, so prüft man ebenso leicht, dass $J'V_tJ'^{-1} = V_t'$ bzw. $J'V_{-t}J'^{-1} = V_t'$ gilt. Mit $UV_t'U^{-1} = U_t'$ folgt dann auch $J'U_tJ'^{-1} = U_t'$ bzw. $J'U_{-t}J'^{-1} = U_t'$. Also sind $\mathcal{T}$ und $\mathcal{T}'$ zueinander $P\Gamma(\mathfrak{M})$-kongugiert.
Seien $X_+' := (a + bY)^{-1}(a' + b'Y)$ und $X_-' := (x + yi\sqrt{d}Y)^{-1}(a' + b'Y)$.
Falls $X_\pm' \in \mathfrak{o}[U]$, gilt dann $X_\pm' \in \Gamma_3(\mathfrak{o}[U]) := \{X \in \Gamma(\mathfrak{o}[U]) \mid (X - 1) \in Y\mathfrak{o}[U]\}$. (Die Behauptung folgt für $X_+ = ((aa' + 3bb') + (a'b - ab')Y)/24$ mit $\mathfrak{R} = Y\mathfrak{o}[U]$ aus $(aa' + 3bb' - 24) = (a(a' - a) + 3b(b' - b)) \in 9\mathfrak{o}$, und ähnlich für X_-'.)
Ist umgekehrt ein $X' \in \Gamma_3(\mathfrak{o}[U])$ gegeben, so gilt $(a + bY)X' = a' + b'Y$ bzw. $(x + yi\sqrt{d}Y)X' = a' + b'Y$ mit $a', b' \in \mathfrak{o}$ und $a'^2 + 3b'^2 = 24$ sowie $(b' - b) \in 3\mathfrak{o}$.

- Falls $d \not\equiv 3 \pmod 4$, ist 2 in k verzweigt. Sei $2\mathfrak{o} = \mathfrak{p}^2$. Da 2 in $\mathbb{Q}(U)$ träge

ist, ist $\mathfrak{p}$ in $k(U)$ träge. Sei $\mathfrak{p}\mathfrak{o}[U] = \mathfrak{P}$. Wegen $N(a+bY) = 24$ ist notwendig $(a+bY)\mathfrak{O} = (x+yi\sqrt{d}Y)\mathfrak{O} = (a'+b'Y)\mathfrak{O} = 2\mathfrak{P}\mathfrak{R}$, also $X'_{\pm} \in \Gamma_3(\mathfrak{o}[V])$. Wären $\mathcal{T}$ und $\mathcal{T}'$ nicht $P\Gamma(\mathfrak{M})$-kongugiert, so wäre weder $X'_+ \in \Gamma(\mathfrak{o}[U])^{(2)}$ noch $X'_- \in \Gamma(\mathfrak{o}[U])^{(2)}$. Nach Lemma 8.10.(ii) ist $[\Gamma_3(\mathfrak{o}[U]) : \Gamma(\mathfrak{o}[U])^{(2)}] = 2$. Also wäre ${X'_+}^{-1}X'_- \in \Gamma(\mathfrak{o}[U])^{(2)}$, das heißt es gäbe ein $J \in \Gamma(\mathfrak{o}[U])$ mit $(a+bY)(x+yi\sqrt{d}Y)^{-1} = J^2$. Sei $J = \alpha + \beta Y$ mit $\alpha, \beta \in k$. Damit folgt $(\alpha-\beta Y)(a+bY) = (\alpha+\beta Y)(x+yi\sqrt{d}Y)$, und daraus folgt $\alpha\overline{a} = 3\beta\overline{b}$. Mit $1 = N(J) = \alpha^2 + 3\beta^2$ und $a^2 + 3b^2 = 24$ folgt $(12\beta/\overline{a})^2 = 2$, Widerspruch.

- Falls $d \equiv 3 \pmod 8$, ist 2 in k träge und in $\mathbb{Q}(i\sqrt{d}Y)$ zerlegt. Also ist $2\mathfrak{o}$ in $k(U)$ zerlegt. Sei $2\mathfrak{o}[U] = \mathfrak{P}\mathfrak{P}^*$ und $(a+bY)\mathfrak{o}[U] = 2\mathfrak{P}\mathfrak{R}$. Mit $(a+bY)(x+yi\sqrt{d}Y) = 24U$ folgt $(x+yi\sqrt{d}Y)\mathfrak{o}[U] = 2\mathfrak{P}^*\mathfrak{R}$. Wegen $(a'+b'Y) \in 2\mathfrak{o}[U]$ gilt dann entweder $X'_+ \in \Gamma_3(\mathfrak{o}[U])$ oder $X'_- \in \Gamma_3(\mathfrak{o}[U])$. Wir wählen $\mathcal{T}'$ so, dass $X'_+ \in \Gamma_3(\mathfrak{o}[U]) \setminus \Gamma(\mathfrak{o}[U])^{(2)}$. Dann sind $\mathcal{T}, \mathcal{T}'$ nicht $P\Gamma(\mathfrak{M})$-kongugiert, weil weder $X'_+ \in \Gamma(\mathfrak{o}[U])^{(2)}$ noch $X'_- \in \Gamma(\mathfrak{o}[U])^{(2)}$ gilt. Wir prüfen nun die $P\Gamma(\mathfrak{M})$-Konjugationsklasse einer (beliebigen) Tetraedergruppe $\mathcal{T}'' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_3 \subset \mathcal{T}''$. Es gibt $a'', b'' \in \mathfrak{o}$ mit $a''^2 + 3b''^2 = 24$ und $(b''-b) \in 3\mathfrak{o}$, so dass $U''_t := (-2Y + (a''+3b'')V/2 - (a''-b'')YV/2)/6$, $V''_t := (-2Y - a''V - b''YV)/6$ und U Erzeugende von $P^{-1}(\mathcal{T}'')$ sind. Wegen $VV''_tV^{-1} = (1 + a''V - b''YV)/2$ und $(-a'' + b''Y) = -(a'' + b''Y)^*$ können wir o.B.d.A. annehmen, dass $X''_+ := (a+bY)^{-1}(a''+b''V) \in \Gamma_3(\mathfrak{o}[U])$ gilt. Ist $\mathcal{T}''$ nicht $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{T}$, so ist $X''_+ \notin \Gamma(\mathfrak{o}[U])^{(2)}$. Also gibt es ein $J \in \Gamma(\mathfrak{o}[U])$ mit $(a'+b'Y)^{-1}(a''+b''Y) = {X'_+}^{-1}X''_+ = J^2$. Damit folgt elementar $JV'_tJ^{-1} = V''_t$. Mit $UV''_tU^{-1} = U''_t$ folgt auch $JU'_tJ^{-1} = U''_t$. Also ist $\mathcal{T}''$ dann $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{T}'$.

(b) Sei t die Anzahl der verschiedenen Primteiler von D. Nach Satz 7.5.(i) gibt es bis auf $P\Gamma(\mathfrak{M})$-Konjugation genau 2^t 3-Diedergruppen $\mathcal{D}_3$ in $P\Gamma(\mathfrak{M})$. Nach Satz 8.5 gibt es daher bis auf $P\Gamma(\mathfrak{M})$-Konjugation genau 2^{t-1} Gruppen $\mathcal{C}'_3 \subset P\Gamma(\mathfrak{M})$ der Ordnung 3, die in einer 3-Diedergruppe $\mathcal{D}_3$ in $P\Gamma(\mathfrak{M})$ enthalten sind.
Nach (a) ist die Anzahl der Tetraedergruppen $\mathcal{T}$ in $P\Gamma(\mathfrak{M})$, die eine solche Gruppe $\mathcal{C}'_3$ enthalten, bis auf $P\Gamma(\mathfrak{M})$-Konjugation gleich

- 2^{t-1}, falls $d \not\equiv 3 \pmod 4$
- 2^t, falls $d \equiv 3 \pmod 8$

Nach Satz 7.5.(ii) ist diese Anzahl gleich der Anzahl aller $P\Gamma(\mathfrak{M})$-Konjugationsklassen von Tetraedergruppen $\mathcal{T}$ in $P\Gamma(\mathfrak{M})$. Also enthält jede Tetraedergruppe $\mathcal{T}$ in $P\Gamma(\mathfrak{M})$ eine solche Gruppe $\mathcal{C}'_3$. Die Behauptung folgt nun mit Satz 8.5.

□

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] Martin Eichler, *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. **195** (1955), 127–151. MR0080767 (18,297c)

[3] Helmut Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952, Reprint 1985.

[4] Norbert Krämer, *Die Konjugationsklassenanzahlen 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 cohomology of discrete groups above their virtual cohomological dimension*, Journal of Algebra **404** (2014), no. C, 152–175. DOI: 10.1016/j.jalgebra.2014.01.025, `http://hal.archives-ouvertes.fr/hal-00618167`

[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