HAL
open science

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-00720823v7

HAL Id: hal-00720823

https://hal.science/hal-00720823v7

Preprint submitted on 20 Feb 2017

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

20. Februar 2017

Zusammenfassung

Seien k ein imaginärquadratischer Zahlkörper mit Hauptordnung $\mathfrak{o}$, F eine $\mathbb{Q}$-Quaternionenalgebra und M eine Erweiterung von F zur k-Algebra. Wir klassifizieren die F-Ordnungen $\mathfrak{G}$, die sich optimal in eine M-Maximalordnung $\mathfrak{N}$ einbetten lassen, d. h. für die $\mathfrak{G} = F \cap \mathfrak{N}$ gilt (Definition 5.3, Satz 5.6). Der Isomorphietyp von $\mathfrak{N}$ hängt nur von der Diskriminante von $\mathfrak{G}$ ab. Ist $F' \subset M$ eine zweite $\mathbb{Q}$-Quaternionenalgebra und $\mathfrak{N}'$ eine zweite M-Maximalordnung, so ist unser Hauptergebnis der Nachweis einer Beziehung zwischen den Einbettungen $\mathfrak{G} = F \cap \mathfrak{N}$ und $\mathfrak{G}' = F' \cap \mathfrak{N}'$ (Satz 5.9).

Auf dieser Grundlage können wir speziell ermitteln, ob die Bianchi-Gruppe $PSL_2(\mathfrak{o})$ 3-Dieder-, Tetraeder- oder maximalendliche 2-Diedergruppen enthält (Satz 6.8)

Wir ermitteln die Anzahl optimaler Einbettungen $\mathfrak{G} \hookrightarrow \mathfrak{N}$ bis auf Konjugation mit Elementen aus $\mathfrak{N}^\times$ (Satz 7.3). Damit berechnen wir speziell die Konjugationsklassenzahlen nichtzyklischer endlicher Untergruppen der Bianchi-Gruppe neu (Satz 7.5).

Weiter zeigen wir für $m = 2, 3$, wie sich m-Diederuntergruppen in Gruppen der Ordnung m schneiden (Sätze 8.3 - 8.5). Schließlich dehnen wir unsere Ergebnisse auf Eichler-Ordnungen und speziell Kongruenzuntergruppen aus (Sätze 9.3 - 9.9).

Inhaltsverzeichnis

1 Einleitung **2**

2 Bezeichnungen und Grundlagen **4**

3 Einbettung rationaler Quaternionenalgebren **6**

4 Einbettung p-adischer Quaternionenordnungen **9**

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 **18**

6 Die nichtzyklischen endlichen Untergruppen **23**

7 Konjugationsklassenanzahlen **27**

8 Einige Durchschnitte nichtzyklischer endlicher Gruppen **31**

9 Eichler-Ordnungen und Kongruenz-Untergruppen **36**

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 mit Diskriminante $n^2\mathbb{Z}$ und $n \in \mathbb{N}$, 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 $\mathfrak{G} \subset \mathfrak{F}$, dann sei $\Lambda(\mathfrak{G}) := [\mathfrak{F} : \mathfrak{G}]$. Wir bezeichnen $\mathfrak{G}$ als $\mathfrak{o}$-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 5.4 mit den Sätzen 4.2, 4.3 und 4.5), 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, und dass der Isomorphietyp von $\mathfrak{M}$ dann nur von $\Delta(\mathfrak{G})$ abhängt (Satz 5.6).

Unser Hauptergebnis ist der nachstehende Satz 5.9, 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 5.5).

Satz 5.9. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Seien F, F' zwei $\mathbb{Q}$-Quaternionenalgebren, sei M eine gemeinsame Erweiterung von F und F' zur k-Quaternionenalgebra, und seien $\mathfrak{M}, \mathfrak{M}'$ zwei M-Maximalordnungen.
Dann gibt es ein $f \in \mathbb{N}$ mit $f \mid \Sigma_k(F)$, so dass für alle Stellen p von $\mathbb{Q}$ gilt:
$$\left(\frac{\Delta(F \cap \mathfrak{M}) f \Lambda(\mathfrak{M} \cap \mathfrak{M}') \Delta(F' \cap \mathfrak{M}'), -d}{p}\right) = \left(\frac{F}{p}\right)\left(\frac{F'}{p}\right).$$

Wir zeigen die oben genannten Aussagen über die Einbettungen $\mathfrak{G} = F \cap \mathfrak{N}$ einschließlich Satz 5.9, indem wir erstens je zwei $\mathbb{Q}$-Quaternionenalgebren $F, F' \subset M$ zueinander in

Beziehung setzen (Satz 3.3), zweitens in Kapitel 4 die 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 in Kapitel 5 diese lokalen Ergebnisse zusammenfügen und mit Satz 3.3 kombinieren. Falls k Zerfällungskörper von F ist, folgen aus den Sätzen 3.3 und 5.9 die Korollare 3.4 und 5.10.

Als Anwendung von Korollar 5.10 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.

Wir führen Satz 6.8 wie folgt auf Satz 5.9 zurück: Enthält $PSL_2(k)$ eine Untergruppe vom Isomorphietyp $\mathcal{D}_3$, $\mathcal{T}$ oder $\mathcal{D}_2$, dann erzeugt deren Urbild in $SL_2(k)$ eine $\mathbb{Q}$-Quaternionenalgebra $F \subset M_2(k)$ und über $\mathbb{Z}$ eine F-Ordnung $\mathfrak{F}$. Wir wenden Satz 5.9 auf die Einbettungen $M_2(\mathbb{Z}) = M_2(\mathbb{Q}) \cap M_2(\mathfrak{o})$ und $\mathfrak{F} = F \cap \mathfrak{N}$ mit einer $M_2(k)$-Maximalordnung $\mathfrak{N}$ an. Wir erhalten die Sätze 6.4 und 6.6, sowie Satz 6.7 mit dem Spezialfall Satz 6.8.

Für eine $\mathfrak{o}$-kompatible F-Ordnung $\mathfrak{G}$ ermitteln wir zusätzlich die Anzahl der M-Maximalordnungen $\mathfrak{N}$ mit $\mathfrak{G} = F \cap \mathfrak{N}$ und 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, auf Basis des lokalen Satzes 4.9).

Als Anwendung von Satz 7.3 berechnen wir dann unter anderem die Konjugationsklassenanzahlen der nichtzyklischen maximalendlichen Untergruppen von $PSL_2(\mathfrak{o})$ (Satz 7.5).

Unter Verwendung der Ergebnisse von [5] lassen sich dann auch unter anderem die Konjugationsklassenanzahlen der zyklischen Untergruppen einer Bianchi-Gruppe angeben. Rahm hat in [7] die homologische Torsion und die Farrell-Tate-Kohomologie der Bianchi-Gruppen ermittelt und als Funktion dieser Konjugationsklassenanzahlen ausgedrückt.

In Kapitel 8 untersuchen wir die Durchschnitte nichtzyklischer endlicher Untergruppen (wird fortgesetzt). Fürs Erste zeigen wir für $m = 2, 3$, ob und wie sich m-Diedergruppen in Gruppen der Ordnung m schneiden (Sätze 8.3 - 8.5 und Korollar 8.6).
Berkove und Rahm haben gezeigt, dass daraus eine Klassifikation der Zusammenhangskomponenten reduzierter 2-Torsionsunterkomplexe folgt, was es erlaubt, Formeln für die 2-Torsionskohomologie aufzustellen, siehe [1, Corollary 7].

Im Schlusskapitel 9 dehnen wir die Ergebnisse der Kapitel 6 bis 8 auf Eichler-Ordnungen und speziell auf die Bianchi-Kongruenzuntergruppen aus (Sätze 9.3 - 9.9). Nur relativ wenige Kongruenzuntergruppen enthalten maximalendliche nichtzyklische Untergruppen, und wenn, dann jeweils nur Untergruppen eines einzigen Isomorphietyps.

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 [2] für imaginärquadratische Zahlkörper und [6] 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 [2, 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 $M_2(\mathbb{C})$.

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 $\overline{\mathfrak{p}}$, so 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, so 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 ab Kapitel 4.

Eine F-Ordnung $\mathfrak{G}$ heißt optimal eingebettet in eine M-Ordnung $\mathfrak{M}$, wenn $\mathfrak{G} = F \cap \mathfrak{M}$ 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, $U_{11}, U_{12}, U_{21}, U_{22} \in Q$ Matrixeinheiten 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 Matrixeinheiten die Gleichung (oder Darstellung) $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Für eine Darstellung bezüglich Matrixeinheiten gelten die bekannten Matrix-Rechenregeln.

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 2.1. *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 [6, Theorem 2.9.8]. Sonst können wir $Q = M_2(K)$ annehmen. Das charakteristische Polynom von A hat in K zwei Nullstellen $a \neq b$. Nun folgt, dass es $X, Y \in GL_2(K)$ gibt mit $XAX^{-1} = YBY^{-1} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Sei $J := Y^{-1}X$. □

Lemma 2.2. *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 Matrixeinheiten in Q, bezüglich derer gilt:
$\mathfrak{M} = \begin{pmatrix} \mathfrak{O} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{O} \end{pmatrix}$ *und* $\mathfrak{M}' = \begin{pmatrix} \mathfrak{O} & \Pi^{-r}\mathfrak{O} \\ \Pi^r\mathfrak{O} & \mathfrak{O} \end{pmatrix} = J\mathfrak{M}J^{-1}$ *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 [3, 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 [6, 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 2.3. *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 [3, Satz 7], Beweis siehe dort, Fall b).

□

Lemma 2.4. *Sei K ein $\mathfrak{p}$-adischer Zahlkörper, und sei $Q \cong M_2(K)$ eine K-Quaternionenalgebra. Seien $\mathfrak{M} \neq \mathfrak{M}'$ sowie $\mathfrak{N} \neq \mathfrak{N}'$ jeweils Q-Maximalordnungen mit $\mathfrak{M} \cap \mathfrak{M}' = \mathfrak{N} \cap \mathfrak{N}'$. Dann gilt entweder $\mathfrak{M} = \mathfrak{N}$ und $\mathfrak{M}' = \mathfrak{N}'$ oder $\mathfrak{M} = \mathfrak{N}'$ und $\mathfrak{M}' = \mathfrak{N}$.*

Beweis. Sei $\mathfrak{O}$ die Hauptordnung von K, und sei $\Pi \in \mathfrak{O}$ ein Primelement. Nach Lemma 2.2.(i) gibt es ein $r \in \mathbb{N}$ und Matrixeinheiten in Q, bezüglich derer gilt: $\mathfrak{M} = \begin{pmatrix} \mathfrak{O} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{O} \end{pmatrix}$, $\mathfrak{M}' = \begin{pmatrix} \mathfrak{O} & \Pi^{-r}\mathfrak{O} \\ \Pi^r\mathfrak{O} & \mathfrak{O} \end{pmatrix}$ und $\mathfrak{M} \cap \mathfrak{M}' = \begin{pmatrix} \mathfrak{O} & \mathfrak{O} \\ \Pi^r\mathfrak{O} & \mathfrak{O} \end{pmatrix}$. Dann ist $L := \begin{pmatrix} K & 0 \\ 0 & K \end{pmatrix}$ halbeinfache quadratische Erweiterung von K mit Hauptordnung $\mathfrak{L} := \begin{pmatrix} \mathfrak{O} & 0 \\ 0 & \mathfrak{O} \end{pmatrix} \subset \mathfrak{M} \cap \mathfrak{M}' = \mathfrak{N} \cap \mathfrak{N}'$. Speziell gilt $\mathfrak{L} \subset L \cap \mathfrak{N}$. Da $\mathfrak{L}$ die Hauptordnung von L ist, folgt $L \cap \mathfrak{N} = \mathfrak{L} = L \cap \mathfrak{M}$. Nach Lemma 2.3 gibt es ein $J \in L^\times$ mit $\mathfrak{N} = J\mathfrak{M}J^{-1}$. Wir können o.B.d.A. annehmen, dass $J = \begin{pmatrix} 1 & 0 \\ 0 & \Pi^s \end{pmatrix}$ mit $s \in \mathbb{Z}$, also dass $\mathfrak{N} = \begin{pmatrix} \mathfrak{O} & \Pi^{-s}\mathfrak{O} \\ \Pi^s\mathfrak{O} & \mathfrak{O} \end{pmatrix}$ gilt. Aus $\mathfrak{M} \cap \mathfrak{M}' \subset \mathfrak{N}$ folgt $0 \leq s \leq r$. Genauso gibt es ein $s' \in \mathbb{Z}$ mit $0 \leq s' \leq r$ und $\mathfrak{N}' = \begin{pmatrix} \mathfrak{O} & \Pi^{-s'}\mathfrak{O} \\ \Pi^{s'}\mathfrak{O} & \mathfrak{O} \end{pmatrix}$. Dann ist $\mathfrak{N} \cap \mathfrak{N}' = \begin{pmatrix} \mathfrak{O} & \Pi^{-t'}\mathfrak{O} \\ \Pi^t\mathfrak{O} & \mathfrak{O} \end{pmatrix}$ mit $t = \max(s, s') = r$ und $t' = \min(s, s') = 0$, also entweder $s = r$ und $s' = 0$ oder $s = 0$ und $s' = r$, was zu beweisen war.

□

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 $F(F,T) := \{A \in M \mid T\Phi_F(A)T^{-1} = A\}$.

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 [6, 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 [6, 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 [6, Theorem 7.3.6].

□

Satz 3.3. *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 gibt es ein, bis auf einen Faktor aus $\mathbb{Q}^\times$ eindeutiges, $T \in M^\times$ mit $\Phi_E(T) = T^*$ und $F = F(E,T)$. 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-Algebrenautomorphismus von M_p fortsetzen. Daher gibt es ein $J \in M_p^\times$ mit $F(T)_p = JE_pJ^{-1}$. Dann gilt $JAJ^{-1} = \Phi_{F(T)}(JAJ^{-1}) = T\Phi(JAJ^{-1})T^{-1} = T\Phi(J)A\Phi(J)^{-1}T^{-1}$ für $A \in E_p$ Also gibt es $\lambda \in k_p^\times$ mit $T = \lambda J\Phi(J)^{-1}$ und $N(T) = T\Phi(T) = \lambda\overline{\lambda}$.

Sei $\epsilon \in \mathbb{Z}$ teilerfremd zu $D\Sigma(E)$ mit $\tau := \epsilon\Sigma(E) < 0$ und $\left(\frac{\tau,-d}{p}\right) = -1$.
An allen Verzweigungsstellen q von E ist $\mathbb{Q}(\sqrt{\tau})_q$ quadratischer Erweiterungskörper von $\mathbb{Q}_q$, also ist $\mathbb{Q}(\sqrt{\tau})$ Zerfällungskörper von E, siehe [6, Theorems 2.6.5 and 2.7.3]. Es gibt ein $U \in E^\times$ mit $U^2 = \tau$. Sei $T' := i\sqrt{d}U$. Dann gilt $\Phi(T') = -T' = T'^*$. Aus $N(T') = d\tau$ folgt $\left(\frac{N(T'),-d}{p}\right) = -1$ und notwendig $\left(\frac{E}{p}\right)\left(\frac{F(T')}{p}\right) = -1$.

- Im Fall $\left(\frac{E}{p}\right)\left(\frac{F(T)}{p}\right) = -1$ ist $F(T')_p$ isomorph zu $F(T)_p$.
  Daher gibt es ein $J \in M_p^\times$ mit $JAJ^{-1} = \Phi_{F(T)}(JAJ^{-1})$ für $A \in F(T')_p$, also $JAJ^{-1} = T\Phi(J)\Phi(A)\Phi(J)^{-1}T^{-1} = T\Phi(J)T'^{-1}\Phi_{F(T')}(A)T'\Phi(J)^{-1}T^{-1}$. Also gibt es $\lambda \in k_p^\times$ 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 [6, 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 $X \in \mathbb{Q}[i\sqrt{d}(T - T^*)]$.

□

Korollar 3.4. *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 ist $\mathfrak{F}(\tau) := F(\tau) \cap M_2(\mathfrak{o})$ eine $F(\tau)$-Ordnung mit Diskriminante $\tau^2 D^2 \mathbb{Z}$.
Falls $\tau \neq 1$, gilt $F(\tau) \cap M_2(\mathbb{Q}) \cong \mathbb{Q}(\sqrt{\tau})$ 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 3.3.(iii) gibt es ein $T \in M^\times$ mit $\Phi_E(T) = T^*$, so dass F isomorph ist zu $F(E, T)$. Nach Satz 3.3.(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

Definition 4.1. *Seien F eine $\mathbb{Q}$-Quaternionenalgebra und p eine endliche Stelle von $\mathbb{Q}$. Sei $r \in \mathbb{N}_0$, und sei $\mathfrak{G}_p$ eine F_p-Ordnung mit Diskriminante $p^{2r}\mathbb{Z}_p$.*
Dann sei $\Delta_p(\mathfrak{G}_p) := \pm p^r$, je nachdem ob F an der Stelle p zerfällt oder verzweigt ist.

Satz 4.2. *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 $F_p \cong M_2(\mathbb{Q}_p)$. Dann gilt:
$\Pi\mathfrak{F}_p\Pi^{-1}$ ist eine F_p-Maximalordnung mit $\mathfrak{O}_p \subset \Pi\mathfrak{F}_p\Pi^{-1} \neq \mathfrak{F}_p$.
Ist $\mathfrak{G}_p$ eine F_p-Ordnung mit $\mathfrak{O}_p \subset \mathfrak{G}_p \not\subset \mathfrak{F}_p$, so ist $\mathfrak{G}_p = \Pi\mathfrak{F}_p\Pi^{-1}$.
Ist $\mathfrak{F}'_p$ eine F_p-Maximalordnung mit $\mathfrak{O}'_p \subset \mathfrak{F}'_p$, so ist $\mathfrak{F}'_p = \mathfrak{F}_p$.

Bemerkung: Man kann jede quadratische Körpererweiterung von $\mathbb{Q}_p$ in F_p und ihre Hauptordnung in eine F_p-Maximalordnung einbetten. Alle F_p-Maximalordnungen sind isomorph. Daher gibt es stets die im Satz genannten $K_p, K'_p \subset F_p$ und $\mathfrak{O}_p, \mathfrak{O}'_p \subset \mathfrak{F}_p$.

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 $\mathfrak{O}_p \subset \mathfrak{F}'_p$. Aus $\mathfrak{O}_p = K_p \cap \mathfrak{F}_p = K_p \cap \mathfrak{F}'_p$ folgt mit Lemma 2.3, dass $\mathfrak{F}'_p = X\mathfrak{F}_pX^{-1}$ für ein $X \in K_p^\times$. Wegen $\Pi^2p^{-1} \in \mathfrak{O}_p^\times$ gibt es $r \in \mathbb{Z}$

und $Y \in \mathfrak{O}_p^\times$ mit $X = p^r Y$ oder $X = \Pi p^r Y$. 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 [6, Theorem 6.5.3.2]. Weiter folgt $\mathfrak{G}_p \subset \mathfrak{F}_p$ oder $\mathfrak{G}_p \subset \Pi\mathfrak{F}_p\Pi^{-1}$. Falls $\mathfrak{G}_p \subsetneqq \Pi\mathfrak{F}_p\Pi^{-1}$, gibt es nach (i) ein $r \in \mathbb{N}$ mit $\mathfrak{G}_p = \mathfrak{O}_p + \mathfrak{O}_p\Pi^r\Pi\Omega\Pi^{-1} = \mathfrak{O}_p + \mathfrak{O}_p N(\Pi)^{-1}\Pi^{r+1}\Omega\Pi^* = \mathfrak{O}_p + \mathfrak{O}_p\Pi^{r-1}\Omega\Pi^* \subset \mathfrak{F}_p$.

Die Behauptung $\mathfrak{F}_p' = \mathfrak{F}_p$ für $\mathfrak{O}_p' \subset \mathfrak{F}_p'$ folgt analog, da $p \in \mathfrak{O}_p'$ ein Primelement ist.

□

Satz 4.3. *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 Matrixeinheiten in F_p, bezüglich derer $\mathfrak{O}_p = \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$. Weiter gibt es dann $r, s \in \mathbb{Z}$ mit $\mathfrak{G}_p = \begin{pmatrix} \mathbb{Z}_p & p^s\mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$. Damit ist $[\mathfrak{F}_p : \mathfrak{G}_p] = \Delta_p(\mathfrak{G}_p) = p^{r+s}$.

(ii) Seien $r, s \in \mathbb{Z}$ mit $r + s \geq 0$, und seien (beliebige) Matrixeinheiten in F_p gegeben. Bezüglich dieser Matrixeinheiten 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 2.1 gibt es also Matrixeinheiten $U_{11}, U_{12}, U_{21}, U_{22} \in F_p$, 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 $\mathfrak{G}_p$.

(ii) leicht nachzurechnen

□

Lemma 4.4. *Sei p eine endliche Stelle von $\mathbb{Q}$, und sei F_p eine $\mathbb{Q}_p$-Quaternionenalgebra. Seien $\mathfrak{G}_p, \mathfrak{G}_p'$ zwei F_p-Ordnungen mit $\Delta_p(\mathfrak{G}_p) = \Delta_p(\mathfrak{G}_p')$, und seien $K_p, K_p' \subset F_p$ halbeinfache quadratische Erweiterungen von $\mathbb{Q}_p$ mit den Hauptordnungen $\mathfrak{O}_p \subset \mathfrak{G}_p$, $\mathfrak{O}_p' \subset \mathfrak{G}_p'$. Ein Isomorphismus $\mathfrak{O}_p \to \mathfrak{O}_p'$ ist dann zu einem Isomorphismus $\mathfrak{G}_p \to \mathfrak{G}_p'$ fortsetzbar.*

Beweis. $\mathfrak{F}_p, \mathfrak{F}_p'$ seien F_p-Maximalordnungen mit $\mathfrak{G}_p \subset \mathfrak{F}_p$, $\mathfrak{G}_p' \subset \mathfrak{F}_p'$. Nach Lemma 2.1 ist ein Isomorphismus $\mathfrak{O}_p \to \mathfrak{O}_p'$ zu einem Automorphismus $j : F_p \to F_p$ fortsetzbar. Nach Lemma 2.3 gibt es wegen $K_p' \cap j(\mathfrak{F}_p) = \mathfrak{O}_p' = K_p' \cap \mathfrak{F}_p'$. ein $X \in K_p'^\times$ mit $\mathfrak{F}_p' = Xj(\mathfrak{F}_p)X^{-1}$ und $\mathfrak{O}_p' \subset Xj(\mathfrak{G}_p)X^{-1} \subset \mathfrak{F}_p'$. Mit Satz 4.2 folgt $Xj(\mathfrak{G}_p)X^{-1} = \mathfrak{G}_p'$, falls K_p Körper ist. Falls K_p zerfällt, gibt es nach Satz 4.3.(i) Matrixeinheiten 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 $Y := \begin{pmatrix} p^r & 0 \\ 0 & p^{r'} \end{pmatrix} \in K_p'^{\times}$ folgt $YXj(\mathfrak{G}_p)X^{-1}Y^{-1} = \mathfrak{G}'_p$.

□

Satz 4.5. *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 Matrixeinheiten 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 4.2.(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 [3, Satz 3]

□

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 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 $\mathfrak{F}_p \subset \mathfrak{M}_p$. Es gilt $[\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{M}'_p)] = p^2$.

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 2.3 ein $X \in L_p^\times$ mit $\mathfrak{M}'_p = X \mathfrak{M}_p X^{-1}$.

(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 $\mathfrak{M}'_p = \pi^r Y \mathfrak{M}_p Y^{-1} \pi^{-r} = \mathfrak{M}_p$.

(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 $X = p^r Y$ oder $X = \Pi p^r Y$. 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 [6, Theorem 6.5.3.2]. Aus $N(\Pi) \in p\mathfrak{O}_p^\times$ folgt mit Lemma 2.2, dass $[\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{M}'_p)] = N_{abs}(p\mathfrak{O}_p) = p^2$.

□

Lemma 4.7. *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. Falls F_p zerfällt, hat $\mathfrak{F}_p$ die Diskriminante $\mathbb{Z}_p$. Dann hat $\mathfrak{M}_p := \mathfrak{o}_p \mathfrak{F}_p$ die Diskriminante $\mathfrak{o}_p$, ist also die einzige M_p-Maximalordnung mit $\mathfrak{F}_p \subset \mathfrak{M}_p$.
Falls F_p Divisionsalgebra ist und p in k zerlegt ist, gilt $M_p \cong F_p \times F_p$, 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 4.8. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung $\mathfrak{o}$.*
Seien F eine $\mathbb{Q}$-Quaternionenalgebra, 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.
F_p ist diagonal in $M_p \cong F_p \times F_p$ eingebettet, und wegen $p \nmid \Sigma_k(F)$ gilt $F_p \cong M_2(\mathbb{Q}_p)$. Daher gilt $\mathfrak{N}_p \cong \mathfrak{F}_p \times \mathfrak{F}'_p$ mit zwei F_p-Maximalordnungen $\mathfrak{F}'_p$, $\mathfrak{F}''_p$. Es gibt ein $r \in \mathbb{N}_0$ und Matrixeinheiten 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. Damit gilt $\mathfrak{G}_p = F_p \cap \mathfrak{N}_p = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ und $\mathfrak{o}_p \cong \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix} \subset \mathfrak{G}_p$. Nach Satz 4.3.(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 $0 \leq s \leq r$ und $[\mathfrak{F}_p : \mathfrak{G}_p)] = p^r$. Nach Lemma 4.7 ist $\mathfrak{M}_p \cong \mathfrak{F}_p \times \mathfrak{F}_p$ die einzige M_p-Maximalordnung mit $\mathfrak{F}_p \subset \mathfrak{M}_p$, und aus $\mathfrak{M}_p \cap \mathfrak{N}_p \cong \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^s\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix} \times \begin{pmatrix} \mathbb{Z}_p & p^{-s}\mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ folgt $[\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)] = p^s p^{r-s} = p^r$. Damit induziert die Einbettung $\mathfrak{F}_p \hookrightarrow \mathfrak{M}_p$ einen Isomorphismus $\mathfrak{F}_p/\mathfrak{G}_p \to \mathfrak{M}_p/(\mathfrak{M}_p \cap \mathfrak{N}_p)$.

• Sei nun p verzweigt oder träge in k.

k_p ist quadratische Körpererweiterung von $\mathbb{Q}_p$, und nach Lemma 3.2.(i) gilt $M_p \cong M_2(k_p)$. Sei $\mathfrak{o}_p = \mathbb{Z}_p[\omega]$, und sei $\pi \in \mathfrak{o}_p$ ein Primelement. Falls p in k verzweigt ist, sei $\omega = \pi$. Falls p in k träge ist, sei $\pi = p$. Sei $\mathfrak{M}_p$ eine M_p-Maximalordnung mit $\mathfrak{F}_p \subset \mathfrak{M}_p$. Falls p in k träge ist, müssen wir $\mathfrak{M}_p$ im Beweisverlauf eventuell ersetzen, siehe Lemma 4.6. 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 Matrixeinheiten $U_{11}, U_{12}, U_{21}, U_{22} \in M_p$, 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), (ii) zuerst im Fall $\pi^r \notin p\mathfrak{o}_p$: 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 $[\mathfrak{F}_p : \mathfrak{G}_p] \leq [\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)] = p$. 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 4.5 ist $\mathfrak{G}_p$ bis auf Isomorphie eindeutig, enthält nach Satz 4.2 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 $[\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)] \geq p^2$.

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

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. Damit folgt leicht $UM_pU^* \subset k_pU_{12}$ und $UU_{12}U^* = a^2U_{12}$. 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 $UXU^* \neq 0$. Dann gilt $X \notin \mathbb{Q}_p$. Wir ersetzen U durch $UXU^* \in F_p \smallsetminus \mathbb{Q}_p$ 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. 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 $\pi^r \in p\mathfrak{o}_p$ 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 zeigen die Surjektivität von $\mathfrak{F}_p/\mathfrak{G}_p \to \mathfrak{M}_p/(\mathfrak{M}_p \cap \mathfrak{N}_p)$. 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 $K_p \subset F_p$ 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 4.6.(i) und 4.7 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 $\gamma \in \mathfrak{o}_p^\times$, $\{\gamma, \gamma\omega\}$ ist $\mathbb{Z}_p$-Basis von $\mathfrak{o}_p$, f_{21} 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 $\Pi \in \mathfrak{O}_p$ 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 eben, dass f_{21} surjektiv ist. Wir dürfen also $\gamma = p^s\gamma'$ mit $\gamma' \in \mathfrak{o}_p^\times$, $s \in \mathbb{N}$ annehmen. Mit $\Pi U = \begin{pmatrix} \alpha\omega & \alpha b + \beta\overline{\omega} \\ \gamma\omega & \gamma b + \delta\overline{\omega} \end{pmatrix}$ folgt $\mathfrak{F}_p \subset \begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ p^s\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$. Also ist F_p Divisionsalgebra, mit $\Delta_p(\mathfrak{F}_p) = -p$ folgt $s = 1$.

Bezüglich der Matrixeinheiten $U_{11}, p^{-1}U_{12}, pU_{21}, U_{22}$ gilt $\mathfrak{N}_p = \begin{pmatrix} \mathfrak{o}_p & p^{1-r}\mathfrak{o}_p \\ p^{r-1}\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ mit $r \in \mathbb{N}$, $\mathfrak{M}_p = \begin{pmatrix} \mathfrak{o}_p & p\mathfrak{o}_p \\ p^{-1}\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ und $\Pi = \begin{pmatrix} \alpha & p\beta \\ \gamma' & \delta \end{pmatrix}$, $\Pi U = \begin{pmatrix} \alpha\omega & p(\alpha b + \beta\overline{\omega}) \\ \gamma'\omega & p\gamma' b + \delta\overline{\omega} \end{pmatrix}$
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.

(iii) Wir zeigen die Eindeutigkeit von $\mathfrak{M}_p$. Sei $\mathfrak{M}'_p \neq \mathfrak{M}_p$ eine M_p-Maximalordnung mit $\mathfrak{F}_p \subset \mathfrak{M}'_p$, also p träge in k und F_p Divisionsalgebra. Seien $X, Y \in \mathfrak{M}_p \setminus p\mathfrak{M}_p$ mit $N(X) = p, N(Y) = p^r$, sowie $\mathfrak{M}'_p = X\mathfrak{M}_pX^{-1}$ und $\mathfrak{N}_p = Y\mathfrak{M}_pY^{-1}$. Sei $t \in \mathbb{Z}$ mit $Z := p^tX^{-1}Y \in \mathfrak{M}'_p \setminus p\mathfrak{M}'_p$. Aus $Z\mathfrak{M}'_pZ^{-1} = \mathfrak{N}_p$ und $N(Z) = p^{2t-1+r} \neq p^r = N(Y)$ folgt nach Lemma 2.2.(iv) also $[\mathfrak{M}'_p : (\mathfrak{M}'_p \cap \mathfrak{N}_p)] \neq [\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)] = [\mathfrak{F}_p : \mathfrak{G}_p]$.

□

Satz 4.9. *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 $\mathfrak{O}_p \subset F_p$ eine zu $\mathfrak{o}_p$ isomorphe Ordnung und $\mathfrak{G}_p$ eine F_p-Ordnung mit $\mathfrak{O}_p \subset \mathfrak{G}_p$. Bezeichne $C_p(\mathfrak{G}_p)$ die Anzahl der M_p-Maximalordnungen $\mathfrak{N}_p$ mit $\mathfrak{G}_p = F_p \cap \mathfrak{N}_p$. Dann gilt:

- *Falls $\Delta_p(\mathfrak{G}_p) = 1$ ist, so ist $C_p(\mathfrak{G}_p) = 1$.*
- *Falls p zerlegt oder träge in k ist und $\Delta_p(\mathfrak{G}_p) \neq 1$ ist, so ist $C_p(\mathfrak{G}_p) = 2$.*
- *Falls p verzweigt in k ist, so gilt:*
  Falls $\Delta_p(\mathfrak{G}_p) = \pm p$ ist, so ist $C_p(\mathfrak{G}_p) = 1$.
  Falls $\Delta_p(\mathfrak{G}_p) = +p^2$ ist, so ist $C_p(\mathfrak{G}_p) = p - 1$.
  Falls $\Delta_p(\mathfrak{G}_p) = -p^2$ ist, so ist $C_p(\mathfrak{G}_p) = p + 1$.
  Falls $p \neq 2$ und $|\Delta_p(\mathfrak{G}_p)| \geq p^3$ ist, so ist $C_p(\mathfrak{G}_p) = 2p$.
  Falls $p = 2$ und $|\Delta_p(\mathfrak{G}_p)| \geq p^3$ ist, so wird $C_p(\mathfrak{G}_p)$ durch folgende Tabelle dargestellt:

$\lvert\Delta_2(\mathfrak{G}_2)\rvert$	$C_2(\mathfrak{G}_2)$	
	$d \equiv 1 \pmod 4$	$d \equiv 2 \pmod 4$
8	2	2
16	4	4
32	8	4
64	8	8
≥ 128	8	16

Beweis. Sei $\mathfrak{F}_p$ eine F_p-Maximalordnung mit $\mathfrak{G}_p \subset \mathfrak{F}_p$.
• Sei $\Delta_p(\mathfrak{G}_p) = 1$. Dann zerfällt F_p, es gilt $\mathfrak{G}_p = \mathfrak{F}_p$, und mit Lemma 4.7 folgt $C_p(\mathfrak{G}_p) = 1$.
• Sei p zerlegt in k, und sei $\Delta_p(\mathfrak{G}_p) \neq 1$.
Nach Satz 4.3.(i) gibt es $r, s \in \mathbb{Z}$ und Matrixeinheiten in F_p, bezüglich derer gilt:
$\mathfrak{O}_p = \begin{pmatrix} \mathbb{Z}_p & 0 \\ 0 & \mathbb{Z}_p \end{pmatrix}$ und $\mathfrak{G}_p = \begin{pmatrix} \mathbb{Z}_p & p^s\mathbb{Z}_p \\ p^r\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$. Da $\mathfrak{O}_p$ diagonal in $\mathfrak{N}_p$ enthalten ist, gilt $\mathfrak{N}_p \cong \begin{pmatrix} \mathbb{Z}_p & p^{-x}\mathbb{Z}_p \\ p^x\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix} \times \begin{pmatrix} \mathbb{Z}_p & p^{-y}\mathbb{Z}_p \\ p^y\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ mit $x, y \in \mathbb{Z}$. Man rechnet nun leicht nach, dass $\mathfrak{G}_p = F_p \cap \mathfrak{N}_p$ genau dann gilt, wenn entweder $x = r$, $y = -s$ oder $x = -s$, $y = r$.
• Sei p träge in k, und sei $\Delta_p(\mathfrak{G}_p) \neq 1$.
F_p ist isomorph zur p-Komponente einer $\mathbb{Q}$-Algebra mit Zerfällungskörper k. Es gibt also $\tau \in \mathbb{Z}$ mit den Eigenschaften laut Korollar 3.4 sowie Matrixeinheiten in M_p, bezüglich derer $F_p = \left\{ \begin{pmatrix} a & b \\ \tau\overline{b} & \overline{a} \end{pmatrix} \middle| a, b \in k_p \right\}$. Für $r \in \mathbb{N}_0$ ist $\mathfrak{G}(r)_p := \left\{ \begin{pmatrix} a & p^r b \\ p^r\tau\overline{b} & \overline{a} \end{pmatrix} \middle| a, b \in \mathfrak{o}_p \right\}$ eine F_p-Ordnung und enthält die zu $\mathfrak{o}_p$ isomorphe Ordnung $\mathfrak{O}_p := \left\{ \begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix} \middle| a \in \mathfrak{o}_p \right\}$. Sei $L_p := \begin{pmatrix} k_p & 0 \\ 0 & k_p \end{pmatrix}$ mit Hauptordnung $\mathfrak{L}_p = \begin{pmatrix} \mathfrak{o}_p & 0 \\ 0 & \mathfrak{o}_p \end{pmatrix}$. Mit $\mathfrak{N}(r)_p := \begin{pmatrix} \mathfrak{o}_p & p^r\mathfrak{o}_p \\ p^{-r}\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ und $\mathfrak{N}(-r)_p := \begin{pmatrix} \mathfrak{o}_p & (p^r\tau)^{-1}\mathfrak{o}_p \\ p^r\tau\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ 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 $F_p \cap \mathfrak{N}_p = \mathfrak{G}(r)_p$. Da p in k träge ist, gilt $\mathfrak{L}_p = \mathfrak{o}_p\mathfrak{O}_p \subset \mathfrak{N}_p$. Nach Lemma 2.3 gibt es ein $J \in L_p^\times$ mit $\mathfrak{N}_p = JM_2(\mathfrak{o}_p)J^{-1}$. Dann ist $\mathfrak{N}_p = \begin{pmatrix} \mathfrak{o}_p & p^{-s}\mathfrak{o}_p \\ p^s\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ mit $s \in \mathbb{Z}$, also $\mathfrak{N}_p = \mathfrak{N}(r)_p$ oder $\mathfrak{N}_p = \mathfrak{N}(-r)_p$. Nach Lemma 4.4 ist $\mathfrak{G}_p$ isomorph zu $\mathfrak{G}(r)_p$ mit $r \in \mathbb{N}_0$, und $\mathfrak{N}(r)_p = \mathfrak{N}(-r)_p$ gilt nur dann, wenn $r = 0$ und F_p zerlegt ist.
• Sei p verzweigt in k, sei $\pi \in \mathfrak{o}_p$ ein Primelement, und sei $\Delta_p(\mathfrak{G}_p) \neq 1$.
Sei $\mathfrak{F}_p$ eine F_p-Maximalordnung und $\mathfrak{M}_p$ die M_p-Maximalordnung mit $\mathfrak{F}_p \subset \mathfrak{M}_p$. Wie im Beweis von Lemma 4.8 folgt, dass es $b, \alpha, \beta, \delta \in \mathfrak{o}_p$, $\gamma \in \mathfrak{o}_p^\times$ und Matrixeinheiten in M_p gibt, bezüglich derer $\left\{ 1, \Pi := \begin{pmatrix} \pi & b \\ 0 & \overline{\pi} \end{pmatrix}, \Omega := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \Pi\Omega \right\}$ eine $\mathbb{Z}_p$-Basis von $\mathfrak{F}_p$ ist, p träge in $K_p' = \mathbb{Q}_p(\Omega)$ mit Hauptordnung $\mathfrak{O}_p' = \mathbb{Z}_p[\Omega]$ ist, und $\mathfrak{M}_p = \begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ gilt. 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 Lemma 4.2.(i) und 4.4. Sei zunächst $\mathfrak{N}_p$ eine M_p-Maximalordnung mit $\mathfrak{G}(r)_p = F_p \cap \mathfrak{N}_p$. Nach Lemma 4.8.(ii)

und den Lemmata 4.6.(i), 4.7 ist dann $[\mathfrak{F}_p : \mathfrak{G}(r)_p] = [\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)] = p^r$. Nach Lemma 2.2.(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 [6, 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 gleichwertig $J^{-1}\Pi J \in \mathfrak{M}_p$ 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 drei Vorbemerkungen:

(P1) 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.

(P2) Genau dann gilt $b \in \mathfrak{o}_p^\times$, wenn F_p zerfällt.
Zum Beweis sei $b \in \pi\mathfrak{o}_p$. Dann ist $\Pi/\pi \in \mathfrak{M}_p$, also $\mathfrak{o}_p\mathfrak{F}_p \subsetneqq \mathfrak{M}_p$, also $\Delta_p(\mathfrak{F}_p) = -p$.
Sei umgekehrt $\Delta_p(\mathfrak{F}_p) = -p$, und sei $\mathfrak{M}'_p$ der $\mathfrak{o}_p$-Modul mit Basis $\{1, \Pi/\pi, \Omega, \Pi\Omega/\pi\}$.
Multiplikation von links mit (Π/π) oder von rechts mit Ω überführt $\mathfrak{M}'_p$ in sich. Mit $\Omega\Pi/\pi = (\Pi/\pi)(\Pi^{-1}\Omega\Pi) \in (\Pi/\pi)\mathfrak{F}_p \subset \mathfrak{M}'_p$ folgt, dass $\mathfrak{M}'_p$ multiplikativ abgeschlossen, also M_p-Maximalordnung ist. Dann ist notwendig $\mathfrak{M}'_p = \mathfrak{M}_p$, also $b \in \pi\mathfrak{o}_p$.

(P3) Falls $p = 2$, gilt $b \notin \pi^2\mathfrak{o}_p$.
Zum Beweis 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 $1 = (u + w\delta)\pi b' + (v + w)\beta \in \pi\mathfrak{o}_p$, 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 $p \neq 2$	
	$\Delta_p(\mathfrak{F}_p) = 1$	$\Delta_p(\mathfrak{F}_p) = -p$
$m = 0, n \geq 0$	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 $p=2$			
	$d \equiv 1 \pmod 4$		$d \equiv 2 \pmod 4$	
	$\Delta_p(\mathfrak{F}_p)=1$	$\Delta_p(\mathfrak{F}_p)=-p$	$\Delta_p(\mathfrak{F}_p)=1$	$\Delta_p(\mathfrak{F}_p)=-p$
$m=0, n\geq 0$	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 $m,n\in\mathbb{N}_0$ mit $m+n=r$ und $c\in\mathfrak{o}_p$, 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 Lemma 4.8.(ii) und 2.2, dass $[\mathfrak{F}_p:\mathfrak{H}_p]=[\mathfrak{M}_p:(\mathfrak{M}_p\cap\mathfrak{N}_p)]=p^r$, mit Lemma 4.2.(i) also $\mathfrak{H}_p=\mathfrak{G}(r)_p$. Falls $\mathfrak{H}_p\not\subset\mathfrak{F}_p$, folgt mit Lemma 4.2.(iv) und 4.6.(i), dass $\mathfrak{H}_p=\Pi\mathfrak{F}_p\Pi^{-1}$ 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 $C_p(\mathfrak{G}_p)$ 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. Zum Schluss addieren wir die passenden Tabelleneinträge unter $\Delta_p(\mathfrak{G}_p)=\Delta_p(\mathfrak{F}_p)p^r$.

□

5 Einbettung rationaler Quaternionenordnungen

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

Definition 5.2. *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.*

Wir bezeichnen $\Delta(\mathfrak{G})$ auch als reduzierte Diskriminante von $\mathfrak{G}$, siehe [6, Definition 2.7.4]. Es gilt $\Delta(\mathfrak{G})=\Sigma(F)\Lambda(\mathfrak{G})$. Für eine F-Maximalordnung $\mathfrak{F}$ gilt speziell $\Delta(\mathfrak{F})=\Sigma(F)$. $\Delta(\mathfrak{G})$ ist das Produkt der $\Delta_p(\mathfrak{G}_p)$ über alle Primzahlen $p\in\mathbb{N}$, siehe [6, Theorem 2.7.3].

Definition 5.3. *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 5.4. *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 4.2, 4.3 und 4.5 dargelegt.

Beweis. jeweils durch Zusammenfügen der Ergebnisse für alle endlichen Stellen p von $\mathbb{Q}$.

(i) Falls $p \mid \Lambda(\mathfrak{G})$, lässt sich $\mathfrak{o}_p$ in $\mathfrak{G}_p$, also k_p in F_p einbetten. Wenn dann auch $p \mid \Sigma_k(F)$ gelten würde, so wäre F_p eine Divisionsalgebra, aber k_p kein Körper, Widerspruch. Falls $p \nmid \Sigma_k(F)$, gibt es nach den Sätzen 4.2 und 4.3 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) Falls $p \nmid \lambda$, sei $\mathfrak{G}_p = \mathfrak{F}_p$.
Falls $p \mid \lambda$, sei λ_p der p-Anteil von λ. Dann gibt es ein $r \in \mathbb{N}$ 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. Wegen $p \nmid \Sigma_k(F)$ enthält $\mathfrak{F}_p$ eine zu $\mathfrak{o}_p$ isomorphe Ordnung $\mathfrak{O}_p$. Nach den Sätzen 4.2 und 4.3 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 einzige F_p-Maximalordnung.
Falls $p \nmid \Sigma_k(F)$, gibt es nach Lemma 4.4 einen Isomorphismus $\mathfrak{G}_p \to \mathfrak{G}'_p$.

□

Lemma 5.5. *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) Beweis durch Zusammenfügen des folgenden Ergebnisses für alle endlichen Stellen p von $\mathbb{Q}$. Seien dazu $\mathfrak{p} \mid p$ eine Stelle von k und $\pi \in \mathfrak{o}_\mathfrak{p}$ ein Primelement. Falls $\mathfrak{p} \mid \Sigma_k(F)$, gilt $\mathfrak{N}_\mathfrak{p} = \mathfrak{N}'_\mathfrak{p}$, also $\Lambda(\mathfrak{N} \cap \mathfrak{N}')_\mathfrak{p} = 1$ und $N(\mathfrak{N}\mathfrak{N}')_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}$. Falls $\mathfrak{p} \nmid \Sigma_k(F)$, gibt es nach Lemma 2.2 ein $r \in \mathbb{N}_0$ mit $[\mathfrak{N}_\mathfrak{p} : (\mathfrak{N} \cap \mathfrak{N}')_\mathfrak{p}] = N_{abs}(\pi\mathfrak{o}_\mathfrak{p})^r = N_{abs}(N(\mathfrak{N}\mathfrak{N}')_\mathfrak{p})^{-1}$.

(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 [6, 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) 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 [6, 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 [2, 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 [2, Kapitel I, § 7, Satz 1] (Minkowski-Hasse) also genau dann, wenn $\left(\frac{N_{abs}(\mathfrak{f})\Lambda(\mathfrak{N} \cap \mathfrak{N}'), -d}{p}\right) = 1$ für alle p.
Sei f der quadratfreie Anteil von $N_{abs}(\mathfrak{f})$. Nach Lemma 3.2.(i) gilt dann $f \mid \Sigma_k(F)$.
Ist umgekehrt $f \in \mathbb{N}$ mit $f \mid \Sigma_k(F)$, so gibt es ein $\mathfrak{f} \in R$ mit $f = N_{abs}(\mathfrak{f})$.

□

Satz 5.6. *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: $\Delta(F \cap \mathfrak{N})\Lambda(\mathfrak{N} \cap \mathfrak{N}')\Delta(F \cap \mathfrak{N}') \in \mathbb{Q}^{\times(2)}$.
Speziell ist $\mathfrak{N}$ isomorph zu $\mathfrak{N}'$, falls $\Delta(F \cap \mathfrak{N}) = \Delta(F \cap \mathfrak{N}')$ gilt.

Beweis. jeweils durch Zusammenfügen der Ergebnisse für alle endlichen Stellen p von $\mathbb{Q}$.

(i) Falls $p \mid \Lambda(F \cap \mathfrak{N})$, enthält $F_p \cap \mathfrak{N}_p$ nach 4.8.(i) eine zu $\mathfrak{o}_p$ isomorphe Ordnung.

(ii) Falls $p \mid \Sigma_k(F)$, ist $\mathfrak{G}_p$ die F_p-Maximalordnung. Sei $\mathfrak{N}_p$ die M_p-Maximalordnung. Falls $p \nmid \Sigma_k(F)$, gibt es nach 4.9 eine M_p-Maximalordnung $\mathfrak{N}_p$ mit $\mathfrak{G}_p = F_p \cap \mathfrak{N}_p$.

(iii) Falls $p \mid \Sigma_k(F)$, ist $F_p \cap \mathfrak{N}_p = \mathfrak{F}_p$ die F_p-Maximalordnung, und mit $\mathfrak{M}_p = \mathfrak{N}_p$ gilt $[\mathfrak{F}_p : (F \cap \mathfrak{N})_p] = [\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)] = 1$. Falls $p \nmid \Sigma_k(F)$, gibt es nach 4.8.(ii) genau eine M_p-Maximalordnung $\mathfrak{M}_p$ mit $\mathfrak{F}_p \subset \mathfrak{M}_p$ und $[\mathfrak{F}_p : (F_p \cap \mathfrak{N}_p)] = [\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{N}_p)]$.
$\mathfrak{F}/(F \cap \mathfrak{N}) \to \mathfrak{M}/(\mathfrak{M} \cap \mathfrak{N})$ 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 5.5.(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 $\Lambda(\mathfrak{M} \cap \mathfrak{N}')\Lambda(\mathfrak{M} \cap \mathfrak{M}')\Lambda(F \cap \mathfrak{N}') \in \mathbb{Q}^{\times(2)}$, also $\Delta(F \cap \mathfrak{N})\Lambda(\mathfrak{N} \cap \mathfrak{N}')\Delta(F \cap \mathfrak{N}')\Lambda(\mathfrak{M} \cap \mathfrak{M}') \in \mathbb{Q}^{\times(2)}$. Wir zeigen $\Lambda(\mathfrak{M} \cap \mathfrak{M}') \in \mathbb{Q}^{\times(2)}$:
Falls F an der Stelle p verzweigt ist, gilt $\mathfrak{F}_p = \mathfrak{F}'_p$, und nach Lemma 4.6 bzw. 4.7 gilt $\mathfrak{M}_p = \mathfrak{M}'_p$ oder $[\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{M}'_p)] = p^2$.
Falls F an der Stelle p zerfällt, gibt es nach Lemma 2.2.(i) ein $r \in \mathbb{N}_0$ und Matrixeinheiten 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. Damit ist $\mathfrak{M}_p = \begin{pmatrix} \mathfrak{o}_p & \mathfrak{o}_p \\ \mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$ und $\mathfrak{M}'_p = \begin{pmatrix} \mathfrak{o}_p & p^{-r}\mathfrak{o}_p \\ p^r\mathfrak{o}_p & \mathfrak{o}_p \end{pmatrix}$, also $[\mathfrak{M}_p : (\mathfrak{M}_p \cap \mathfrak{M}'_p)] = p^{2r}$.

□

Lemma 5.7. *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 $T \in M^\times$ mit $\Phi_E(T) = T^*$, $N(T) \in \mathbb{Z}$, $S(T) \in 4\mathbb{Z}$ 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. Es gibt Matrixeinheiten in E_p, bezüglich derer $T = \begin{pmatrix} \sigma + \alpha i\sqrt{d} & \beta i\sqrt{d} \\ \gamma i\sqrt{d} & \sigma - \alpha i\sqrt{d} \end{pmatrix}$ mit $\sigma, \alpha, \beta, \gamma \in \mathbb{Q}_p$. Sei $\tau := N(T) - S(T)^2/4 \in \mathbb{Z}$. 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 Matrixeinheiten 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 $\mathfrak{N}_p = M_2(\mathfrak{o}_p)$. Dann ist $\left\{1, U := \begin{pmatrix} 0 & 1 \\ \tau d & 0 \end{pmatrix}, V := \begin{pmatrix} \sigma d & -i\sqrt{d} \\ \tau d i\sqrt{d} & -\sigma d \end{pmatrix}, W := \begin{pmatrix} i\sqrt{d} & 0 \\ 2\sigma d & -i\sqrt{d} \end{pmatrix} = (\sigma U + UV/d)/\tau\right\}$ $\mathbb{Z}_p$-Basis einer $F(E,T)_p$-Ordnung $\mathfrak{G}_p \subset \mathfrak{N}_p$ mit Diskriminante $16d^4N(T)^2\mathbb{Z}_p$. Ist $p = 2$ in k verzweigt oder $p \neq 2$, so gilt $\mathfrak{G}_p = F(E,T)_p \cap \mathfrak{N}_p$. Ist $p = 2$ in k träge oder zerlegt, so ist $\{1, (U+V)/2, V, (1+W)/2\}$ $\mathbb{Z}_p$-Basis von $F(E,T)_p \cap \mathfrak{N}_p$ mit Diskriminante $d^4N(T)^2\mathbb{Z}_p$.
□

Lemma 5.8. *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 3.3.(iii) gibt es ein $T \in M^\times$ mit $\Phi_E(T) = T^*$ und $F = F(E,T)$. Falls $S(T)^2 = 4N(T)$, gilt $N(T) \in \mathbb{Q}^{\times(2)}$. Nach Satz 3.3.(ii) ist F isomorph zu E, also $\Sigma(F) = \Sigma(E)$. Seien $\mathfrak{E}, \mathfrak{F}$ Maximalordnungen in E, F, und seien $\mathfrak{N}, \mathfrak{L}$ zwei M-Maximalordnungen mit $\mathfrak{E} \subset \mathfrak{N}$ und $\mathfrak{F} \subset \mathfrak{N}$, so dass $\mathfrak{E}$ zu $\mathfrak{F}$ und $\mathfrak{N}$ zu $\mathfrak{L}$ isomorph ist. Nach Lemma 5.5.(iii) gibt es $e \in \mathbb{N}$ mit $e \mid \Sigma_k(E)$ und $\left(\frac{e\Lambda(\mathfrak{L} \cap \mathfrak{N}), -d}{p}\right) = 1 = \left(\frac{E}{p}\right)\left(\frac{F}{p}\right)$ für alle p. Wir können nun also $S(T)^2 \neq 4N(T)$ und o.B.d.A. $N(T) \in \mathbb{Z}$, $S(T) \in 4\mathbb{Z}$ annehmen. Falls $p \mid \Sigma_k(E)$, ist $F_p \cap \mathfrak{N}_p$ die F_p-Maximalordnung, hat also die Diskriminante $p^2\mathbb{Z}_p$. Nach Lemma 5.7 gibt es eine E-Maximalordnung $\mathfrak{E}$ und eine M-Maximalordnung $\mathfrak{N}$ mit $\mathfrak{E} \subset \mathfrak{N}$, so dass die F_p-Ordnung $F_p \cap \mathfrak{N}_p$ an allen endlichen Stellen p mit $p \nmid \Sigma_k(E)$ die Diskriminante $D^2d^2N(T)^2\mathbb{Z}_p$ hat. 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. Dann hat $F \cap \mathfrak{N}$ 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 3.3.(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 5.6.(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 jetzt mit Satz 3.3.(ii). □

Satz 5.9. *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 5.6.(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 5.8. Mit Lemma 5.5.(ii) folgt $\Lambda(\mathfrak{L} \cap \mathfrak{N})\Lambda(\mathfrak{L} \cap \mathfrak{L}')\Lambda(\mathfrak{L}' \cap \mathfrak{M})\Lambda(\mathfrak{M} \cap \mathfrak{N}) \in \mathbb{Q}^{\times(2)}$, und nach Satz 5.6.(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 5.8 und $\Sigma(F)\Lambda(F \cap \mathfrak{M}) = \Delta(F \cap \mathfrak{M})$ folgt $\left(\frac{\Delta(F \cap \mathfrak{M}) e \Lambda(\mathfrak{M} \cap \mathfrak{N})\Sigma(E), -d}{p}\right) = \left(\frac{E}{p}\right)\left(\frac{F}{p}\right)$ für alle Stellen p von $\mathbb{Q}$. Entsprechend gibt es ein $e' \in \mathbb{N}$ mit $e' \mid \Sigma_k(E)$, eine E-Maximalordnung $\mathfrak{E}'$ und 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 durch Multiplikation der beiden Gleichungen, denn nach Satz 5.6.(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 5.5.(ii) folgt $\Lambda(\mathfrak{M} \cap \mathfrak{M}')\Lambda(\mathfrak{M} \cap \mathfrak{N})\Lambda(\mathfrak{N} \cap \mathfrak{N}')\Lambda(\mathfrak{N}' \cap \mathfrak{M}') \in \mathbb{Q}^{\times(2)}$. □

Korollar 5.10. *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 5.9.

□

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 $\Gamma \subset SL_2(\mathbb{C})$ kürzen wir $P\Gamma := P(\Gamma) \cong \Gamma/(\Gamma \cap \{\pm 1\})$ 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.

(iv) Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung $\mathfrak{o}$.
Seien M eine k-Quaternionenalgebra und $\mathfrak{M}$ eine M-Maximalordnung.
Dann bezeichnen wir $P\Gamma(\mathfrak{M})$ als verallgemeinerte Bianchi-Gruppe,
und speziell bezeichnen wir $P\Gamma(M_2(\mathfrak{o})) = PSL_2(\mathfrak{o})$ als 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 [8, 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 [8, 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 [8, 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 [8, 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 $P\Gamma(\mathfrak{F}(\mathcal{D}_2)) \subsetneqq P\Gamma(\mathfrak{F}(\mathcal{T})) = \mathcal{T}$ 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 $d \not\equiv 7 \pmod 8$.

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, also 3 bzw. 2 in k nicht zerlegt ist, also wenn $-d \not\equiv 1 \pmod 3$ bzw. $-d \not\equiv 1 \pmod 8$ ist.

□

$\mathcal{D}_3 \subset P\Gamma(\mathfrak{M})$ 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 $\mathfrak{F}(\mathcal{D}_2) \subsetneqq F \cap \mathfrak{M}$ 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 4.5.(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 5.4 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 und Satz 5.6.(i)(ii).
Die zweite Behauptung folgt wegen $d \not\equiv 7 \pmod 8$ mit Satz 6.4.(ii) und Satz 5.6.(iv). $\square$

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 Korollar 5.10 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 $\mathcal{D}_3' \subset P\Gamma(\mathfrak{M}')$. Dann ist $\left(\dfrac{-3\Lambda(\mathfrak{M}' \cap M_2(\mathfrak{o})), -d}{p}\right) = \left(\dfrac{-3\lambda, -d}{p}\right)$ für alle Stellen p. Nach Lemma 5.5.(ii) ist $\Lambda(\mathfrak{M} \cap \mathfrak{M}')\lambda\Lambda(M_2(\mathfrak{o}) \cap \mathfrak{M}') \in \mathbb{Q}^{\times(2)}$. Nach Lemma 5.5.(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), Korollar 5.10 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 Satz 5.6.(i) und 5.4.(i) gilt $\lambda \in N_{abs}(I)$, der quadratfreie Anteil von λ wäre 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 5.5.(ii), 5.5.(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-Ordnung.*

(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 [5, § 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, sei $k = \mathbb{Q}(i\sqrt{d})$ mit Diskriminante D, und bezeichne t die Anzahl der verschiedenen Primteiler von D. Sei F eine $\mathbb{Q}$-Quaternionenalgebra, und bezeichne r die Anzahl der Primteiler von $\Sigma_k(F)$. Sei s der Rang der $t \times r$-Matrix (h_{pq}) mit Koeffizienten in $\mathbb{Z}/2\mathbb{Z}$ und $h_{pq} := 0$ oder 1, je nachdem, ob $\left(\frac{q, -d}{p}\right) = 1$ oder -1 gilt, wo p die verschiedenen Primteiler von D und q die Primteiler von $\Sigma_k(F)$ durchläuft. Seien M eine Erweiterung von F zur k-Quaternionenalgebra und $\mathfrak{M}$ eine M-Maximalordnung. Dann gilt $[\mathcal{A}(\mathfrak{M}) : \mathcal{I}(\mathfrak{M})] = 2^{t+2r-s-1}$.*

Beweis. Sei R sei die von den Verzweigungsstellen von M erzeugte $\mathfrak{o}$-Idealgruppe. Ist $j \in \mathcal{A}(\mathfrak{M})$, so gibt es ein $J \in M^\times$ mit $j(A) = JAJ^{-1}$ für alle $A \in \mathfrak{M}$, und $\mathfrak{J} := \mathfrak{M}J$ ist ein zweiseitiges $\mathfrak{M}$-Ideal mit $\mathfrak{j} := N(\mathfrak{J}) \in RI^{(2)} \cap H$. Da J bis auf einen Faktor $a \in k^\times$ eindeutig ist, induziert die Zuordnung $j \mapsto \mathfrak{j}$ wegen $N(a) = a^2$ einen surjektiven Homomorphismus $\mathcal{A}(\mathfrak{M}) \to (RI^{(2)} \cap H)/H^{(2)}$ mit Kern $\mathcal{I}(\mathfrak{M})$, siehe [6, Lemma 6.7.5, Theorem 7.7.7]. Also gilt $[\mathcal{A}(\mathfrak{M}) : \mathcal{I}(\mathfrak{M})] = [(RI^{(2)} \cap H) : (I^{(2)} \cap H)][(I^{(2)} \cap H) : H^{(2)}]$.

Die Zuordnungsvorschrift $\mathfrak{a} \mapsto \mathfrak{a}^2$ induziert einen Isomorphismus $I/H \to I^{(2)}/H^{(2)}$. 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 $[(I^{(2)} \cap H) : H^{(2)}] = [I : I^{(2)}H] = 2^{t-1}$. Weiter gilt $[RI^{(2)} : (RI^{(2)} \cap H)] = [RI^{(2)}H : H] = [RI^{(2)}H : I^{(2)}H][(I^{(2)} : (I^{(2)} \cap H)]$ und $[RI^{(2)} : I^{(2)}][(I^{(2)} : (I^{(2)} \cap H)] = [RI^{(2)} : (RI^{(2)} \cap H)][(RI^{(2)} \cap H) : (I^{(2)} \cap H)]$, also $[(RI^{(2)} \cap H) : (I^{(2)} \cap H)] = [RI^{(2)} : I^{(2)}][RI^{(2)}H : I^{(2)}H]^{-1} = 2^{2r}[R : (R \cap I^{(2)}H)]^{-1}$.

Wir zeigen noch $[R : (R \cap I^{(2)}H)] = 2^s$: Mit der Multiplikation als Verknüpfung ist $R/(R \cap I^{(2)}H)$ ein $\mathbb{Z}/2\mathbb{Z}$-Modul. Für $f \in \mathbb{N}$ sei (f_p) das t-Tupel mit Koeffizienten aus $\mathbb{Z}/2\mathbb{Z}$ und $f_p := 0$ oder 1, je nachdem, ob $\left(\frac{f, -d}{p}\right) = 1$ oder -1 gilt, wo p die verschiedenen Primteiler von D durchläuft. Die Zuordnungsvorschrift $\mathfrak{f} \mapsto (N_{abs}(\mathfrak{f})_p)$ induziert einen $\mathbb{Z}/2\mathbb{Z}$-Modulhomomphismus $\Psi : R/(R \cap I^{(2)}H) \to (\mathbb{Z}/2\mathbb{Z})^t$. Das Bild von Ψ wird von den Tupeln (q_p) erzeugt, wo q die Primteiler von $\Sigma_k(F)$ durchläuft, hat also die Dimension s. Nach [2, 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 $\mathbb{Q}$ (mit $p \mid D$). Also ist Ψ Isomorphismus.

□

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 $\mathfrak{G} = F \cap \mathfrak{N}$. Sei $C(\mathfrak{G})$ gleich dem Produkt der in Satz 4.9 angegebenen $C_p(\mathfrak{G}_p)$ über alle endlichen Stellen p von $\mathbb{Q}$. Dann ist $B(\mathfrak{G}, \mathfrak{N}) = C(\mathfrak{G})[\mathcal{A}(\mathfrak{N}) : \mathcal{I}(\mathfrak{N})]$ und $B_1(\mathfrak{G}, \mathfrak{N}) = 2B(\mathfrak{G}, \mathfrak{N})$.

Beweis. $C(\mathfrak{G})$ ist gleich der Anzahl der M-Maximalordnungen $\mathfrak{L}$ mit $\mathfrak{G} = F \cap \mathfrak{L}$. Ist $\mathfrak{L}$ eine M-Maximalordnung mit $\mathfrak{G} = F \cap \mathfrak{L}$, so gibt es nach Satz 5.6.(iv) einen Automorphismus j von M mit $j(\mathfrak{L}) = \mathfrak{N}$ und $j(\mathfrak{G}) = j(F) \cap \mathfrak{N}$. Für jedes $\mathfrak{L}$ 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 erste Behauptung.
Sei $\mathcal{I}_1(\mathfrak{N})$ die Gruppe der Konjugationen von $\mathfrak{N}$ mit Elementen aus $\Gamma(\mathfrak{N})$. Offenbar gilt $B(\mathfrak{G}, \mathfrak{N}) = C(\mathfrak{G})[\mathcal{A}(\mathfrak{N}) : \mathcal{I}_1(\mathfrak{N})] = B(\mathfrak{G}, \mathfrak{N})[\mathcal{I}(\mathfrak{N}) : \mathcal{I}_1(\mathfrak{N})]$ und $\mathcal{I}(\mathfrak{N}) \cong \mathfrak{N}^\times/\mathfrak{o}^\times$ sowie $\mathcal{I}_1(\mathfrak{N}) \cong \Gamma(\mathfrak{N})/\{\pm 1\}$. Nach [6, 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-Ordnung.
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 $\mu(\mathcal{G}, \mathfrak{N}) = B_1(\mathfrak{F}(\mathcal{G}), \mathfrak{N})[\mathcal{A}'(\mathcal{G}) : \mathcal{I}'(\mathcal{G})]^{-1}$, 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 $W = (1-U-V-UV)/2$.
$j \in \mathcal{A}(\mathfrak{F}(\mathcal{T}))$ 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 hat $\mu(\mathcal{D}_3, \mathfrak{N})$ den Wert
2^{t-1}, *falls* $d \equiv 0 \pmod 3$
2^t, *falls* $d \equiv 1 \pmod 3$
2^t, *falls* $d \equiv 2 \pmod 3$, *und d einen Primteiler* $p \equiv \pm 5 \pmod{12}$ *hat*
2^{t+1}, *falls* $d \equiv 2 \pmod 3$, *und* $p \equiv \pm 1 \pmod{12}$ *für alle Primteiler* $p \neq 2$ *von* d

(ii) Sei $\mathcal{T} \subset P\Gamma(\mathfrak{N})$ eine Tetraedergruppe. Dann hat $\mu(\mathcal{T}, \mathfrak{N})$ den Wert
2^{t-1}, *falls* $d \not\equiv 3 \pmod 4$
2^t, *falls* $d \equiv 3 \pmod 8$
2^t, *falls* $d \equiv 7 \pmod 8$, *und d einen Primteiler* $p \equiv \pm 3 \pmod 8$ *hat*
2^{t+1}, *falls* $d \equiv 7 \pmod 8$, *und* $p \equiv \pm 1 \pmod 8$ *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 $\mu(\mathcal{D}_2, \mathfrak{N})$ hat den Wert* 2^{t-1}.

Bemerkung: Satz 7.5 geht schon aus [5, 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 4.9 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 $\Sigma_k(F(\mathcal{D}_3)) = 3$. Wenn in diesem Fall $\left(\frac{3,-d}{p}\right) = 1$ an allen Stellen p von $\mathbb{Q}$ gilt, 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 Behauptungen folgen jetzt durch Auswertung der Hilbertsymbole.

(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 $\Sigma_k(F(\mathcal{T})) = 2$. Wenn in diesem Fall $\left(\frac{2,-d}{p}\right) = 1$ an allen Stellen p von $\mathbb{Q}$ gilt, 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 Behauptungen folgen jetzt durch Auswertung der Hilbertsymbole.

(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 $F(\mathcal{D}_2)_2 \not\cong M_2(\mathbb{Q}_2)$. 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 Einige Durchschnitte nichtzyklischer endlicher Gruppen

Lemma 8.1. *Sei $d \in \mathbb{N}$ quadratfrei, $d \not\equiv 3 \pmod 4$. Sei $k = \mathbb{Q}(i\sqrt{d})$ mit der Hauptordnung $\mathfrak{o}$, und sei $\pi \in \mathfrak{o}_2$ ein Primelement. Sei M eine k-Quaternionenalgebra. Sei $\mathcal{D}_2 \subset P\Gamma(M)$ eine 2-Diedergruppe, und sei $\mathcal{T}$ die Tetraedergruppe mit $\mathcal{D}_2 \subset \mathcal{T} \subset P\Gamma(M)$. Seien U, V Erzeugende von $P^{-1}(\mathcal{D}_2)$ mit $U^2 = -1$ und $VUV^{-1} = U^{-1}$, und seien U, V und $W := (1 - U - V - UV)$ Erzeugende von $P^{-1}(\mathcal{T})$. Dann gilt $M \cong M_2(k)$, sowie:*

(i) Sei $\mathfrak{N}$ die M-Maximalordnung mit $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{N}$. Dann ist $\{1, (1+U)/\pi, (1+V)/\pi, W\}$ eine $\mathfrak{o}_2$-Basis von $\mathfrak{N}_2$. Für alle $X \in \{U, V, UV\}$ gilt $k[X]_2 \cap \mathfrak{N}_2 = \mathfrak{o}_2[(1 + X)/\pi]$.

(ii) Sei $\mathfrak{N}(U)$ der $\mathfrak{o}$-Modul mit $\mathfrak{o}$-Basis
$\{1, (i\sqrt{d} + U)/2, V, (i\sqrt{d}V + UV)/2\}$, falls $d \equiv 1 \pmod 4$,
$\{1, (1 + i\sqrt{d}V + U)/2, V, (i\sqrt{d} + V + UV)/2\}$, falls $d \equiv 2 \pmod 4$.
Dann sind $\mathfrak{N}(U)$, $\mathfrak{N}(V) := W^{-1}\mathfrak{N}(U)W$ und $\mathfrak{N}(UV) := W^{-1}\mathfrak{N}(V)W$ paarweise verschiedene M-Maximalordnungen. Ist $\mathfrak{N}'$ eine M-Maximalordnung, dann gilt $\mathfrak{F}(\mathcal{D}_2) = F(\mathcal{D}_2) \cap \mathfrak{N}'$ genau dann, wenn $\mathfrak{N}' = \mathfrak{N}(U)$, $\mathfrak{N}' = \mathfrak{N}(V)$ oder $\mathfrak{N}' = \mathfrak{N}(UV)$.

(iii) Sei $X \in \{U, V, UV\}$. Dann ist $k[X] \cap \mathfrak{N}(X)$ die Hauptordnung von $k[X]$:
$k[X] \cap \mathfrak{N}(X) = \mathfrak{o}[(i\sqrt{d} + X)/2]$, falls $d \equiv 1 \pmod 4$.
$k[X]_2 \cap \mathfrak{N}(X)_2 = \mathfrak{o}_2[(1 + X)/\pi]$, falls $d \equiv 2 \pmod 4$.
Für $Y \in \{U, V, UV\}$ mit $Y \neq X$ gilt dann $k[Y] \cap \mathfrak{N}(X) = \mathfrak{o}[Y]$.

(iv) $\Lambda(\mathfrak{N} \cap \mathfrak{N}(U)) = \Lambda(\mathfrak{N} \cap \mathfrak{N}(V)) = \Lambda(\mathfrak{N} \cap \mathfrak{N}(UV)) = 2$. Ist $\mathfrak{N}'$ eine M-Maximalordnung mit $\Lambda(\mathfrak{N} \cap \mathfrak{N}') = 2$, so gilt umgekehrt $\mathfrak{N}' = \mathfrak{N}(U)$, $\mathfrak{N}' = \mathfrak{N}(V)$ oder $\mathfrak{N}' = \mathfrak{N}(UV)$. Weiter gilt $\Lambda(\mathfrak{N}(U) \cap \mathfrak{N}(V)) = \Lambda(\mathfrak{N}(V) \cap \mathfrak{N}(UV)) = \Lambda(\mathfrak{N}(UV) \cap \mathfrak{N}(U)) = 4$.

Beweis. Nach 6.4.(ii) gilt $M \cong M_2(k)$. Nach Satz 4.9 gibt es genau eine M-Maximalordnung $\mathfrak{N}$ mit $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{N}$ und genau drei M-Maxmalordnungen $\mathfrak{N}'$ mit $\mathfrak{F}(\mathcal{D}_2) = F(\mathcal{D}_2) \cap \mathfrak{N}'$. Die Aussagen in (i)-(iii) lassen sich elementar nachprüfen. Die erste Aussage in (iv) folgt mit Lemma 4.8.(ii), die zweite Aussage lässt sich leicht mit [6, Theorem 6.5.3.3] zeigen, und die dritte Aussage folgt mit $\pi W \in \mathfrak{N}_2' \smallsetminus \pi\mathfrak{N}_2'$ aus Lemma 2.2.(iii)-(iv).

□

Lemma 8.2. *Sei $d \in \mathbb{N}$ quadratfrei, $d \equiv 2 \pmod 4$. Sei $k = \mathbb{Q}(i\sqrt{d})$ mit der Hauptordnung $\mathfrak{o}$. Sei $U \in SL_2(\mathbb{C})$ mit $U^2 = -1$, und sei $K := k(U)$ mit der Hauptordnung $\mathfrak{O}$. Dann gilt $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] \leq 2$, und insbesondere gilt $\Gamma(\mathfrak{O})^{(2)} \subset \Gamma(\mathfrak{o}[U])$.*
Weiter gilt $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] = 2$ genau dann, wenn es $x, y \in \mathbb{Z}$ gibt mit $x^2 - dy^2 = 2$.

Beweis. Man sieht leicht ein (siehe Lemma 6.2), dass U die Gruppe $\mathcal{U}$ der Einheitswurzeln von K mit Norm 1 erzeugt. Sei $k_+ := \mathbb{Q}(i\sqrt{d}U)$ mit Hauptordnung $\mathfrak{o}_+ = \mathbb{Z}[i\sqrt{d}U] \subset \mathfrak{o}[U]$. Seien ϵ eine Grundeinheit von K und ϵ_+ eine Grundeinheit von k_+.

Falls $d = 2$, wird $\mathfrak{O}^\times$ von $U' := i\sqrt{2}(1-U)/2$ und $\epsilon_+ = 1 + i\sqrt{2}U$ erzeugt, siehe [4, § 26 (9)]. Daher wird $\Gamma(\mathfrak{O})$ von $U = U'^2$ und $U'\epsilon_+$ erzeugt. Wegen $U'\epsilon_+ \notin \Gamma(\mathfrak{o}[U])$, aber $(U'\epsilon_+)^2 \in \Gamma(\mathfrak{o}[U])$ gilt also $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] = 2$, und mit $x = 2$, $y = 1$ ist $x^2 - dy^2 = 2$.

Falls $d \neq 2$, ist $\mathcal{U}$ die Gruppe aller Einheitswurzeln von K. Nach [4, § 20, Satz 14] gilt $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] \leq [\Gamma(\mathfrak{O}) : \mathcal{U}\Gamma(\mathfrak{o}_+)] \leq [\mathfrak{O}^\times : \mathcal{U}\mathfrak{o}_+^\times] \leq 2$. Es ist $\epsilon = (a + bU)/2$ mit $a, b \in \mathfrak{o}$ und $a = \alpha + \alpha' i\sqrt{d}$, $\epsilon_+ = \gamma + \gamma' i\sqrt{d}U$ mit $\alpha, \alpha', \gamma, \gamma' \in \mathbb{Z}$. Falls $[\mathfrak{O}^\times : \mathcal{U}\mathfrak{o}_+^\times] = 2$, nehmen wir $\epsilon_+ = \epsilon^2 U \in \Gamma(\mathfrak{o}_+)$ an, siehe [4, § 26 (8)]. Es folgt $\gamma' i\sqrt{d} - \gamma U = \epsilon^2 = (a^2 - b^2 + abU)/4$, also $2N(\epsilon) + 2\gamma' i\sqrt{d} = a^2 = (\alpha^2 - d\alpha'^2) + 2\alpha\alpha' i\sqrt{d}$, und speziell $\alpha^2 - d\alpha'^2 = 2N(\epsilon)$.

- Sei $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] = 2$. 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 [4, § 26 (12_{II})] gilt dann $[\mathfrak{O}^\times : \mathcal{U}\mathfrak{o}_+^\times] = 2$. Wäre $N(\epsilon) = -1$, so wäre $N(\alpha + \alpha' i\sqrt{d}U)) = -2$, also $N(e_+) = -1$, Widerspruch zu [4, § 26 (9)]. Also ist $N(\epsilon) = 1$, und offenbar ist α' ungerade. Damit erkennt man leicht, dass $\epsilon \notin \Gamma(\mathfrak{o}[U])$. Also ist $[\Gamma(\mathfrak{O}) : \Gamma(\mathfrak{o}[U])] = 2$.

□

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, und 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 $\mathcal{C}_2 \subset \mathcal{D}_2'$.

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 $d \not\equiv 3 \pmod 4$, folgt mit Lemma 8.1.(i), dass $(k(U) \cap \mathfrak{M})_2 = \mathfrak{o}_2[(1+U)/\pi]$ gilt. 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.(iii) 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 $X' \in \Gamma(\mathfrak{o}[U])$, also $X' = a + bU$ mit $a, b \in \mathfrak{o}$ und $a^2 + b^2 = 1$. Wegen $[\mathfrak{o}_2 : \pi\mathfrak{o}_2] = 2$ ist $(1-a+b) \in \pi\mathfrak{o}_2$ und $(1-X')/\pi = (1-a+b)/\pi - b(1+U)/\pi \in \mathfrak{M}_2$, also $W' := (1-U-V'-UV')/2 = W + (1+U)V(1-X')/2 \in \mathfrak{M}_2$. Dann sind U, V' und W' Erzeugende von $P^{-1}(\mathcal{T}')$ für eine Tetraedergruppe $\mathcal{T}'$ mit $\mathcal{C}_2 \subset \mathcal{T}' \subset P\Gamma(\mathfrak{M})$.

Genau dann ist $\mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$ maximalendliche 2-Diedergruppe, wenn $X' \notin \Gamma(\mathfrak{o}[U])$, wegen $(k(U) \cap \Gamma(\mathfrak{M}))^{(2)} P^{-1}(\mathcal{C}_2) \subset \Gamma(\mathfrak{o}[U])$ also wenn $[(k(U) \cap \Gamma(\mathfrak{M})) : \Gamma(\mathfrak{o}[U])] = 2$, nach Lemma 8.2 also 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 $\mathfrak{M}$ eine M-Maximalordnung.
Sei $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$ 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 $\mathcal{T}' \subset P\Gamma(\mathfrak{M})$ 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 $\mathcal{C}_2''$ nicht zu $\mathcal{C}_2$, aber zueinander $P\Gamma(\mathfrak{M})$-konjugiert.

(c) *Jede maximalendliche 2-Diedergruppe $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2''$, $\mathcal{C}_2' \subset \mathcal{D}_2''$ oder $\mathcal{C}_2'' \subset \mathcal{D}_2''$ 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 $x^2 - dy^2 \neq 2$.*

(a) *Sei $\mathcal{C}_2 \subset \mathcal{D}_2$ eine Untergruppe der Ordnung 2.*
Dann gibt es keine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{M})$ 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 $P\Gamma(\mathfrak{M})$-konjugiert.

(c) *Es gibt eine maximalendliche 2-Diedergruppe $\mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2'$, die nicht $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{D}_2$ ist.*
Jede maximalendliche 2-Diedergruppe $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{M})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2''$, $\mathcal{C}_2' \subset \mathcal{D}_2''$ oder $\mathcal{C}_2'' \subset \mathcal{D}_2''$ ist $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{D}_2$ oder $\mathcal{D}_2'$.

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) - (c) 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 $\mathcal{T} \subset P\Gamma(\mathfrak{M})$. Nach Satz 8.3(i) 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 $P\Gamma(\mathfrak{M})$-Konjugationsklasse von $\mathcal{D}_2'$ ist durch die $P\Gamma(\mathfrak{M})$-Konjugationsklasse von $\mathcal{T}$ eineindeutig bestimmt. Nach Satz 7.5 gilt $\mu(\mathcal{D}_2, \mathfrak{M}) = \mu(\mathcal{T}, \mathfrak{M})$. Also gibt es auch eine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{M})$, 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 $(k(X) \cap \mathfrak{M})_2 = \mathfrak{o}_2[(1+X)/\pi]$, Nach Lemma 8.1.(iii) ist dadurch X bis aufs Vorzeichen, also $\mathcal{C}_2$ eindeutig bestimmt.

Sei umgekehrt $\mathcal{T}' \subset P\Gamma(\mathfrak{M})$ 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 $(k(UV) \cap \mathfrak{M})_2 = \mathfrak{o}_2[(1+UV)/\pi]$.
Sei $\epsilon := (x + yi\sqrt{d}U + yi\sqrt{d}V - xUV)/2 = (1 - UV)x/2 + yU(1 - UV)i\sqrt{d}/2 \in \mathfrak{M}$
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 $P\Gamma(\mathfrak{M})$-konjugiert. Wir können o.B.d.A. $\epsilon V \epsilon^{-1} = U$ mit $\epsilon \in \Gamma(\mathfrak{M})$ annehmen. Dann gilt

$k(V) \cap \mathfrak{M} \cong k(U) \cap \mathfrak{M}$ und mit Lemma 8.1 folgt $(1+UV)/\pi \in \mathfrak{M}_2$. Sei $V' = \epsilon U \epsilon^{-1}$, und sei $\mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$ 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. Sei $T := \epsilon \Phi_F(\epsilon)^*$. Dann gilt $\Phi_F(T) = T^*$, und für $A \in F$ gilt $T\Phi_F(\epsilon A \epsilon^{-1})T^{-1} = \epsilon \Phi_F(\epsilon)^{-1}\Phi_F(\epsilon)A\epsilon^{-1} = \epsilon A \epsilon^{-1}$. Daher gilt $F' = F(F,T)$ und $\Phi_{F'}(A) = T\Phi_F(A)T^{-1}$ für $A \in M$. Mit Lemma 8.1 folgt aus $k(V) \cap \Phi_F(\mathfrak{M}) \cong k(U) \cap \Phi_F(\mathfrak{M})$, dass $\Phi_F(\mathfrak{M}) = \mathfrak{M}$, und analog $\Phi_{F'}(\mathfrak{M}) = \mathfrak{M}$. Wegen $U \in F \cap F'$ gilt $TUT^{-1} = U$, also $T \in k(U) \cap \mathfrak{M} = \mathfrak{o}[U]$. Mit $\Phi_F(T) = T^*$ folgt $T = \gamma + \gamma' i\sqrt{d}U$ mit $\gamma, \gamma' \in \mathbb{Z}$ und $\gamma^2 - d\gamma'^2 = N(T) = 1$, γ ungerade, γ' gerade. Mit $T \in k(U)$ folgt weiter $\Phi_{F'}(TV) = TT^*VT^{-1} = TV$ und $(TV)U(TV)^{-1} = U^{-1}$. Also erzeugen $P(U)$ und $P(TV)$ eine 2-Diedergruppe $\mathcal{D}_2''$ mit $P^{-1}(\mathcal{D}_2'') \subset F' \cap \mathfrak{M}$. Mit Lemma 6.3 folgt $P^{-1}(\mathcal{D}_2'') \subset \Gamma(F' \cap \mathfrak{M}) = \Gamma(\mathfrak{F}(\mathcal{D}_2')) = P^{-1}(\mathcal{D}_2')$, also $\mathcal{D}_2'' = \mathcal{D}_2'$. Wegen $(1+UTV)/\pi = (1+\gamma UV)/\pi - \gamma' i\sqrt{d}V/\pi \in \mathfrak{M}_2$ ist notwendig $TV = \pm V'$. Aus $\epsilon V \epsilon^{-1} = U$ folgt $\epsilon = (a + bU + bV - aUV)/2$ mit $a, b \in \mathfrak{o}$ und $a^2 + b^2 = 2$, und $V' = \epsilon U \epsilon^{-1} = ((-a^2+b^2)/2 - abU)V$, also $\gamma + \gamma' i\sqrt{d}U = \pm(-a^2+b^2)/2 - abU)$. Seien $a = \alpha + \alpha' i\sqrt{d}$ 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 weiter folgt $d \not\equiv 1 \pmod 4$, also $d \equiv 2 \pmod 4$.

(c) Zunächst zeigen wir die Behauptung unter der Voraussetzung $\mathcal{C}_2 \subset \mathcal{D}_2''$.
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 im Beweisabschnitt (a) zu 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 $\Gamma(\mathfrak{M})$ zu U^{-1}, nach Satz 8.4.(ii)(b) aber nicht zu $V^{\pm 1}$ und $(UV)^{\pm 1}$ konjugiert ist.

Nun zeigen wir die Behauptung unter der Voraussetzung $\mathcal{C}_2' \subset \mathcal{D}_2''$ aus. Es genügt zu zeigen, dass es eine 2-Diedergruppe $\mathcal{D}_2'$ mit $\mathcal{C}_2 \subset \mathcal{D}_2' \subset P\Gamma(\mathfrak{M})$ gibt, die $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{D}_2''$ ist. (Unter der Voraussetzung $\mathcal{C}_2'' \subset \mathcal{D}_2''$ erfolgt der Beweis analog.) $P^{-1}(\mathcal{D}_2)$ wird von U, V mit $U^2 = -1$ und $VUV^{-1} = U^{-1}$ erzeugt. O.B.d.A. nehmen wir $U \in P^{-1}(\mathcal{C}_2')$ mit $k(U) \cap \mathfrak{M} = \mathfrak{o}[U]$ und $V \in P^{-1}(\mathcal{C}_2'')$ mit $k(V) \cap \mathfrak{M} = \mathfrak{o}[V]$ an. $P^{-1}(\mathcal{D}_2'')$ wird von U, V' mit $V'UV'^{-1} = U^{-1}$ erzeugt. Dann gilt $V^{-1}V' \in \mathfrak{o}[U]$.
Sei $V' = V(a+bU)$ mit $a, b \in \mathfrak{o}$, $a^2 + b^2 = 1$. Wir können V' durch $UV' = V(b - aU)$ ersetzen, o.B.d.A. also $(a-1), b \in \pi\mathfrak{o}_2$ annehmen. Wäre $(a-1) \notin 2\mathfrak{o}_2$, so wäre $a^2 = 1 + \pi^2 + 2\pi + 4a'$ mit $a' \in \mathfrak{o}_2$ und $b^2 = \pi^2 + 4b'$ mit $b' \in \mathfrak{o}_2$, Widerspruch. Jetzt folgt $(a-1), b \in 2\mathfrak{o}$. und $\epsilon := ((a+1) + bU + (a-1)V - bUV)/2 \in \Gamma(\mathfrak{M})$ sowie $\epsilon UV'\epsilon^{-1} = UV$. Sei $\mathcal{D}_2'$ die von $P(\epsilon U \epsilon^{-1})$ und $P(\epsilon V' \epsilon^{-1})$ erzeugte 2-Diedergruppe.

□

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 $\mathcal{D}_3'$.

Beweis. wie im Beweisabschnitt (a) zu 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. □

Korollar 8.6. *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.
Für $m = 3$ oder $m = 2$ bezeichne $\lambda_m^*(\mathfrak{M})$ die Anzahl der $P\Gamma(\mathfrak{M})$-Konjugationsklassen von Gruppen der Ordnung m, die in einer m-Diedergruppe $\mathcal{D}_m \subset P\Gamma(\mathfrak{M})$ enthalten sind.
Dann ist $2\lambda_3^*(\mathfrak{M}) = \mu(\mathcal{D}_3, \mathfrak{M})$ für $d \neq 3$, und $2\lambda_2^*(\mathfrak{M}) = \mu(\mathcal{T}, \mathfrak{M}) + 3\mu(\mathcal{D}_2, \mathfrak{M})$ für $d \neq 1$.

Bemerkung: $\lambda_m^*(\mathfrak{M})$ entspricht der in [5, § 15] definierten Bezeichnung $\lambda_{2m}^*(\mathfrak{M})$.
Korollar 8.6 geht schon aus [5, Sätze 20.39 und 26.12, Tabellen 20.40 und 26.13] hervor. Erstmals explizit formuliert und auf andere Art bewiesen wurde er in [7, Corollary 23].

Beweis. Für $d \neq 3$ geht die Behauptung $2\lambda_3^*(\mathfrak{M}) = \mu(\mathcal{D}_3, \mathfrak{M})$ direkt aus Satz 8.5 hervor.
Sei nun zunächst $d \equiv 2 \pmod 4$, und es gebe $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 2$.
Nach Satz 8.3.(i) und 8.4.(i) schneiden sich dann je eine Tetraedergruppe $\mathcal{T} \subset P\Gamma(\mathfrak{M})$ und eine 2-Diedergruppe $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$ in einer Gruppe $\mathcal{C}_2$ der Ordnung 2. Bis auf $P\Gamma(\mathfrak{M})$-Konjugation sind $\mathcal{T}$ und $\mathcal{D}_2$ durch $\mathcal{C}_2$ eindeutig bestimmt, und bis auf $P\Gamma(\mathfrak{M})$-Konjugation enthalten sie außer $\mathcal{C}_2$ keine bzw. genau eine Gruppe der Ordnung 2.
Sei schließlich $d \not\equiv 2 \pmod 4$ oder $x^2 - dy^2 \neq 2$ für alle $x, y \in \mathbb{Z}$, und sei $d \neq 1$.
Dann ist der Durchschnitt einer Tetraedergruppe $\mathcal{T} \subset P\Gamma(\mathfrak{M})$ und einer 2-Diedergruppe $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$ trivial, siehe Satz 8.3.(ii). Die Behauptung folgt mit 8.3.(ii) und 8.4.(ii). □

9 Eichler-Ordnungen und Kongruenz-Untergruppen

Definition 9.1. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung $\mathfrak{o}$.*
Seien M eine k-Quaternionenalgebra, $\mathfrak{E}$ eine M-Ordnung, und $\mathfrak{c} \neq \mathfrak{o}$ ein ganzes $\mathfrak{o}$-Ideal.

(i) Wir nennen $\mathfrak{E}$ eine M-Eichler-Ordnung, wenn es M-Maximalordnungen $\mathfrak{M} \neq \mathfrak{M}'$ gibt mit $\mathfrak{E} = \mathfrak{M} \cap \mathfrak{M}'$. Dann sei $\mathfrak{n}(\mathfrak{E}) := N(\mathfrak{M}\mathfrak{M}')^{-1}$.

(ii) Sei $\Gamma_0(\mathfrak{c}) := \left\{ \begin{pmatrix} a & b \\ c & d' \end{pmatrix} \in SL_2(\mathfrak{o}) \middle| c \in \mathfrak{c} \right\}$.
Sei $\Gamma_1(\mathfrak{c}) := \left\{ \begin{pmatrix} a & b \\ c & d' \end{pmatrix} \in \Gamma_0(\mathfrak{c}) \middle| (a-1) \in \mathfrak{c} \right\}$.
Sei $\Gamma(\mathfrak{c}) := \left\{ \begin{pmatrix} a & b \\ c & d' \end{pmatrix} \in \Gamma_1(\mathfrak{c}) \middle| b \in \mathfrak{c} \right\}$.
Wir bezeichnen $P\Gamma_0(\mathfrak{c})$, $P\Gamma_1(\mathfrak{c})$ und $P\Gamma(\mathfrak{c})$ als Bianchi-Kongruenzuntergruppen.

Bemerkung: $\mathfrak{n}(\mathfrak{E})$ ist wohldefiniert, mit $N_{abs}(\mathfrak{n}(\mathfrak{E})) = \Lambda(\mathfrak{E})$, siehe Lemma 2.4 und 5.5.(i).

Lemma 9.2. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Sei M eine k-Quaternionenalgebra, und seien $\mathfrak{M} \neq \mathfrak{M}'$ zwei M-Maximalordnungen.

(i) Sei $\mathfrak{M}''$ eine M-Maximalordnung mit $N(\mathfrak{M}\mathfrak{M}')^{-1} = N(\mathfrak{M}\mathfrak{M}'')^{-1}$.
Dann gibt es ein $A \in \Gamma(\mathfrak{M})$ mit $A\mathfrak{M}'A^{-1} = \mathfrak{M}''$.

(ii) Seien $\mathfrak{M}$ und $\mathfrak{M}'$ isomorph zueinander.
Dann gibt es ein $A \in M^\times$ mit $A\mathfrak{M}A^{-1} = \mathfrak{M}'$ und $A\mathfrak{M}'A^{-1} = \mathfrak{M}$.

Beweis. jeweils mit [6, Theorem 7.7.5 (Strong Approximation)] und $S = \{\infty\}$ auf Basis der folgenden Aussagen. Sei $\mathfrak{p}$ eine endliche Stelle von k, und sei $\pi \in \mathfrak{o}_\mathfrak{p}$ ein Primelement.

(i) Wir zeigen, dass es ein $A \in \Gamma(\mathfrak{M}_\mathfrak{p})$ gibt mit $A\mathfrak{M}'_\mathfrak{p}A^{-1} = \mathfrak{M}''_\mathfrak{p}$. Sei o.B.d.A. $\mathfrak{M}_\mathfrak{p} \neq \mathfrak{M}''_\mathfrak{p}$. Dann zerfällt M_p und es gibt ein $r \in \mathbb{N}$ mit $N(\mathfrak{M}_\mathfrak{p}\mathfrak{M}''_\mathfrak{p})^{-1} = \pi^r\mathfrak{o}_\mathfrak{p}$ und Matrixeinheiten in $M_\mathfrak{p}$, bezüglich derer $\mathfrak{M}_\mathfrak{p} = M_2(\mathfrak{o}_\mathfrak{p})$ gilt. Für $m, n \in \mathbb{N}_0$ und $c \in \mathfrak{o}_\mathfrak{p}$ definieren wir $J(m,n,c) := \begin{pmatrix} \pi^m & c \\ 0 & \pi^n \end{pmatrix}$. Nach [6, Theorem 6.5.3.3] gibt es $m, n \in \mathbb{N}_0$ und $c \in \mathfrak{o}_\mathfrak{p}$ mit $\mathfrak{M}'_\mathfrak{p} = J(m,n,c)\mathfrak{M}_\mathfrak{p}J(m,n,c)^{-1}$ und $m + n = r$, sowie $c \in \mathfrak{o}_\mathfrak{p}^\times$, falls $mn > 0$. Für $mn > 0$ sei $A(m,n,c) := \begin{pmatrix} c^{-1}(1-\pi^n) & 1 \\ -\pi^n & c \end{pmatrix}$. Seien $A(r,0,c) := \begin{pmatrix} 0 & -1 \\ 1 & -c \end{pmatrix}$ und $A(0,r,0) := 1$. Mit $A' := A(m,n,c)$ gilt dann $A'\mathfrak{M}'_\mathfrak{p}A'^{-1} = \begin{pmatrix} \mathfrak{o}_\mathfrak{p} & \pi^{-r}\mathfrak{o}_\mathfrak{p} \\ \pi^r\mathfrak{o}_\mathfrak{p} & \mathfrak{o}_\mathfrak{p} \end{pmatrix}$. Ebenso gibt es $A'' \in \Gamma(\mathfrak{M}_\mathfrak{p})$ mit $A''\mathfrak{M}''_\mathfrak{p}A''^{-1} = \begin{pmatrix} \mathfrak{o}_\mathfrak{p} & \pi^{-r}\mathfrak{o}_\mathfrak{p} \\ \pi^{-r}\mathfrak{o}_\mathfrak{p} & \mathfrak{o}_\mathfrak{p} \end{pmatrix}$. Wir setzen $A := A''^{-1}A'$.

(ii) Sei $A \in M^\times$ mit $A\mathfrak{M}A^{-1} = \mathfrak{M}'$. Wir zeigen, dass es ein $E \in \Gamma(\mathfrak{M}_\mathfrak{p})$ gibt mit $(AE)\mathfrak{M}_\mathfrak{p}(AE)^{-1} = \mathfrak{M}'_\mathfrak{p}$ und $(AE)\mathfrak{M}'_\mathfrak{p}(AE)^{-1} = \mathfrak{M}_\mathfrak{p}$. Sei o.B.d.A. $\mathfrak{M}_\mathfrak{p} \neq \mathfrak{M}'_\mathfrak{p}$. Dann gibt es ein $r \in \mathbb{N}$ und Matrixeinheiten in $M_2(k_\mathfrak{p})$, bezüglich derer $\mathfrak{M}_\mathfrak{p} = \begin{pmatrix} \mathfrak{o}_\mathfrak{p} & \mathfrak{o}_\mathfrak{p} \\ \mathfrak{o}_\mathfrak{p} & \mathfrak{o}_\mathfrak{p} \end{pmatrix}$, $\mathfrak{M}'_\mathfrak{p} = \begin{pmatrix} \mathfrak{o}_\mathfrak{p} & \pi^r\mathfrak{o}_\mathfrak{p} \\ \pi^{-r}\mathfrak{o}_\mathfrak{p} & \mathfrak{o}_\mathfrak{p} \end{pmatrix}$ gilt. Mit $A' = \begin{pmatrix} \pi^r & 0 \\ 0 & 1 \end{pmatrix}$ ist $\mathfrak{M}'_\mathfrak{p} = A'\mathfrak{M}_\mathfrak{p}A'^{-1}$ und $A = \pi^s A'B$ mit $s \in \mathbb{Z}$, $B \in \mathfrak{M}_\mathfrak{p}^\times$. Mit $E := B^{-1}\begin{pmatrix} 0 & N(B) \\ -1 & 0 \end{pmatrix}$ gilt $AE = \begin{pmatrix} 0 & \pi^{-s}N(A) \\ -\pi^s & 0 \end{pmatrix}$, $E \in \Gamma(\mathfrak{M}_\mathfrak{p})$ und $S(AE) = 0$, also $(AE)\mathfrak{M}'_\mathfrak{p}(AE)^{-1} = (AE)^2\mathfrak{M}_\mathfrak{p}(AE)^{-2} = \mathfrak{M}_\mathfrak{p}$.

□

Satz 9.3. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung $\mathfrak{o}$.*
Sei M eine k-Quaternionenalgebra, und seien $\mathfrak{M} \neq \mathfrak{M}'$ zwei M-Maximalordnungen.
Dann gilt für die M-Eichler-Ordnung $\mathfrak{E} = \mathfrak{M} \cap \mathfrak{M}'$:

(i) $P\Gamma(\mathfrak{E})$ enthält genau dann eine Tetraedergruppe, wenn
$d \equiv 3 \pmod 8$ ist, $\mathfrak{n}(\mathfrak{E}) = 2\mathfrak{o}$ ist, und $P\Gamma(\mathfrak{M})$ eine Tetraedergruppe enthält.

(ii) $P\Gamma(\mathfrak{E})$ *enthält genau dann eine* 3*-Diedergruppe, wenn* $d \equiv 1 \pmod 3$ *ist,* $\mathfrak{n}(\mathfrak{E}) = 3\mathfrak{o}$ *ist, und* $P\Gamma(\mathfrak{M})$ *eine* 3*-Diedergruppe enthält.*

(iii) $P\Gamma(\mathfrak{E})$ *enthält genau dann eine maximalendliche* 2*-Diedergruppe, wenn* $d \not\equiv 3 \pmod 4$ *ist,* $\mathfrak{n}(\mathfrak{E}) = 2\mathfrak{o}$ *oder* $\mathfrak{n}(\mathfrak{E})^2 = 2\mathfrak{o}$ *ist, und* $P\Gamma(\mathfrak{M})$ *oder* $P\Gamma(\mathfrak{M}')$ *eine maximalendliche* 2*-Diedergruppe enthält.*

Hier gilt $M \cong M_2(k)$*, und* $\mathfrak{M}, \mathfrak{M}'$ *sind bis auf die Reihenfolge eindeutig durch* $\mathfrak{E}$ *bestimmt.*

Beweis.

(i) Sei $\mathcal{T} \subset P\Gamma(\mathfrak{E})$ Tetraedergruppe. Dann gilt $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{M}$ mit $\Delta(\mathfrak{F}(\mathcal{T})) = 2$. Nach Satz 4.9 gibt es genau dann eine M-Maximalordnung $\mathfrak{M}'' \neq \mathfrak{M}$ mit $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{M}''$, wenn 2 in k träge, also $d \equiv 3 \pmod 8$ ist. Dann ist $\mathfrak{E}' := \mathfrak{M} \cap \mathfrak{M}''$ eine M-Eichler-Ordnung mit $\mathcal{T} \subset P\Gamma(\mathfrak{E}')$ und $\mathfrak{n}(\mathfrak{E}') = 2\mathfrak{o}$. Mit Lemma 4.6.(ii) folgt $\mathfrak{M}'' = \mathfrak{M}'$ und $\mathfrak{E}' = \mathfrak{E}$.

Seien umgekehrt $\mathcal{T} \subset P\Gamma(\mathfrak{M})$ eine Tetraedergruppe, $d \equiv 3 \pmod 8$ und $\mathfrak{n}(\mathfrak{E}) = 2\mathfrak{o}$. Wie eben gezeigt, gibt es eine M-Maximalordnung $\mathfrak{M}'' \neq \mathfrak{M}$ und eine M-Eichler-Ordnung $\mathfrak{E}' := \mathfrak{M} \cap \mathfrak{M}''$ mit $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{E}'$ und $\mathfrak{n}(\mathfrak{E}') = N(\mathfrak{M}\mathfrak{M}'')^{-1} = 2\mathfrak{o}$.
Aus $N(\mathfrak{M}\mathfrak{M}')^{-1} = 2\mathfrak{o}$ folgt mit Lemma 9.2.(i), dass es ein $A \in \Gamma(\mathfrak{M})$ gibt mit $A\mathfrak{M}''A^{-1} = \mathfrak{M}'$. Dann ist $\mathcal{T}' = P(AP^{-1}(\mathcal{T})A^{-1})$ Tetraedergruppe mit $\mathcal{T}' \subset P\Gamma(\mathfrak{E})$.

(ii) analog zum Beweis von (i), mit $p = 3$ anstelle von $p = 2$.

(iii) Sei $\mathcal{D}_2 \subset P\Gamma(\mathfrak{E})$ maximalendliche 2-Dieder-Untergruppe. Dann ist $\mathcal{D}_2$ maximalendlich in $P\Gamma(\mathfrak{M})$ oder $P\Gamma(\mathfrak{M}')$. Nach Satz 6.6 gilt $d \not\equiv 3 \pmod 4$. Mit den Bezeichnungen von Lemma 8.1 ist o.B.d.A. entweder $\mathfrak{E} = \mathfrak{N}(U) \cap \mathfrak{N}(V)$ oder $\mathfrak{E} = \mathfrak{N} \cap \mathfrak{N}(U)$, wegen $\Lambda(\mathfrak{N}(U) \cap \mathfrak{N}(V)) = 4$ und $\Lambda(\mathfrak{N} \cap \mathfrak{N}(U)) = 2$ also $\mathfrak{n}(\mathfrak{E}) = 2\mathfrak{o}$ oder $\mathfrak{n}(\mathfrak{E})^2 = 2\mathfrak{o}$.

Sei umgekehrt o.B.d.A. $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$ eine maximalendliche 2-Dieder-Untergruppe, $d \not\equiv 3 \pmod 4$ und $\mathfrak{n}(\mathfrak{E}) = 2\mathfrak{o}$ oder $\mathfrak{n}(\mathfrak{E})^2 = 2\mathfrak{o}$. Mit den Bezeichnungen von Lemma 8.1 sei $\mathfrak{M} = \mathfrak{N}(U)$, also $N(\mathfrak{M}\mathfrak{N}(V)) = N(\mathfrak{M}\mathfrak{M}')$ oder $N(\mathfrak{M}\mathfrak{N}) = N(\mathfrak{M}\mathfrak{M}')$. Nach Lemma 9.2.(i) gibt es ein $A \in \Gamma(\mathfrak{M})$ mit $A\mathfrak{N}(V)A^{-1} = \mathfrak{M}'$ bzw. $A\mathfrak{N}A^{-1} = \mathfrak{M}'$. Dann ist $\mathcal{D}_2' = P(AP^{-1}(\mathcal{D}_2)A^{-1}) \subset P\Gamma(\mathfrak{E})$ eine maximalendliche 2-Diedergruppe.

Nach Satz 6.4 bzw. 6.6 gilt $M \cong M_2(k)$, und nach Lemma 2.4 sind $\mathfrak{M}$ und $\mathfrak{M}'$ bis auf die Reihenfolge eindeutig durch $\mathfrak{E}$ bestimmt, da sie nur an einer Stelle verschieden sind. □

Satz 9.4. *Sei* $d \in \mathbb{N}$ *quadratfrei, und sei* $k = \mathbb{Q}(i\sqrt{d})$ *mit Hauptordnung* $\mathfrak{o}$*. Sei* $\mathfrak{c} \neq \mathfrak{o}$ *ein ganzes* $\mathfrak{o}$*-Ideal. Dann ist* $\mathfrak{E}_0(\mathfrak{c}) := \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{c} & \mathfrak{o} \end{pmatrix}$ *eine* $M_2(k)$*-Eichler-Ordnung mit* $\mathfrak{n}(\mathfrak{E}_0(\mathfrak{c})) = \mathfrak{c}$*. Nach Definition ist* $\Gamma_0(\mathfrak{c}) = \Gamma(\mathfrak{E}_0(\mathfrak{c}))$*, und damit gilt:*

(i) $P\Gamma_0(\mathfrak{c})$ *enthält genau dann eine Tetraedergruppe, wenn* $d \equiv 3 \pmod 8$ *ist und* $\mathfrak{c} = 2\mathfrak{o}$ *ist und* $p \equiv 1$ *oder* $p \equiv 3 \pmod 8$ *für alle Primteiler* p *von* d *gilt.*

(ii) $P\Gamma_0(\mathfrak{c})$ *enthält genau dann eine* 3*-Diedergruppe, wenn* $\mathfrak{c} = 3\mathfrak{o}$ *ist und* $p \equiv 1 \pmod 3$ *für alle Primteiler* p *von* d *gilt.*

(iii) $P\Gamma_0(\mathfrak{c})$ *enthält genau dann eine maximalendliche* 2*-Diedergruppe, wenn* $d \not\equiv 3 \pmod 4$ *ist und eine der folgenden Bedingungen erfüllt ist:*

(a) $\mathfrak{c} = 2\mathfrak{o}$ *und* $p \equiv 1 \pmod 4$ *für alle Primteiler* $p \neq 2$ *von* d.

(b) $\mathfrak{c}^2 = 2\mathfrak{o}$ *und* $n \not\equiv 7 \pmod 8$ *für alle Teiler* $n \in \mathbb{N}$ *von* d.

Beweis. Seien $\mathfrak{M} := \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{o} \end{pmatrix}$, $\mathfrak{M}' := \begin{pmatrix} \mathfrak{o} & \mathfrak{c}^{-1} \\ \mathfrak{c} & \mathfrak{o} \end{pmatrix}$ und $\mathfrak{E} := \mathfrak{M} \cap \mathfrak{M}' = \mathfrak{E}_0(\mathfrak{c}) = \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{c} & \mathfrak{o} \end{pmatrix}$.
Es gilt $\mathfrak{n}(\mathfrak{E}) = N(\mathfrak{M}\mathfrak{M}')^{-1} = \mathfrak{c}$, siehe Lemma 2.2.(i) und (ii).

(i) folgt mit Satz 9.3.(i) und Satz 6.8.(ii).

(ii) folgt mit Satz 9.3.(ii) und Satz 6.8.(i).

(iii) folgt mit Satz 9.3.(iii) und Satz 6.8.(iii).

(a) $\mathfrak{M}$ und $\mathfrak{M}'$ sind isomorph zueinander.

(b) Nach Satz 6.7.(iii), (ii) mit Lemma 5.5.(i) und Satz 6.8.(ii) enthält $P\Gamma(\mathfrak{M}')$ maximalendliche 2-Diedergruppen genau dann, wenn $P\Gamma(\mathfrak{M})$ Tetraedergruppen enthält, also $p \equiv 1$ oder $p \equiv 3 \pmod 8$ für alle Primteiler $p \neq 2$ von d gilt. Die Oder-Verknüpfung der Bedingungen für $\mathfrak{M}$ und $\mathfrak{M}'$ liefert die Behauptung.

□

Satz 9.5. *Sei* $d \in \mathbb{N}$ *quadratfrei, und sei* $k = \mathbb{Q}(i\sqrt{d})$ *mit Hauptordnung* $\mathfrak{o}$. *Sei* $\mathfrak{c} \neq \mathfrak{o}$ *ein ganzes* $\mathfrak{o}$*-Ideal. Dann ist* $\mathfrak{E}(\mathfrak{c}) := \begin{pmatrix} \mathfrak{o} & \mathfrak{c} \\ \mathfrak{c} & \mathfrak{o} \end{pmatrix}$ *eine* $M_2(k)$*-Eichler-Ordnung mit* $\mathfrak{n}(\mathfrak{E}(\mathfrak{c})) = \mathfrak{c}^2$.
$P\Gamma(\mathfrak{E}(\mathfrak{c}))$, $P\Gamma_1(\mathfrak{c})$ *und* $P\Gamma(\mathfrak{c})$ *enthalten weder Tetraeder- noch* 3*-Diedergruppen.*
Wenn $P\Gamma(\mathfrak{E}(\mathfrak{c}))$ *oder* $P\Gamma_1(\mathfrak{c})$ *oder* $P\Gamma(\mathfrak{c})$ *eine* 2*-Diedergruppe enthält, dann ist* $d \not\equiv 3 \pmod 4$ *und* $\mathfrak{c}^2 = 2\mathfrak{o}$, *sowie* $\Gamma_1(\mathfrak{c}) = \Gamma_0(\mathfrak{c})$ *und* $\Gamma(\mathfrak{c}) = \Gamma(\mathfrak{E}(\mathfrak{c}))$.
Weiter gilt dann: $P\Gamma(\mathfrak{c})$ *enthält genau dann eine maximalendliche* 2*-Diedergruppe, wenn* $p \equiv 1$ *oder* $p \equiv 3 \pmod 8$ *für alle Primteiler* $p \neq 2$ *von* d *gilt.*

Beweis. Seien $\mathfrak{M} := \begin{pmatrix} \mathfrak{o} & \mathfrak{c} \\ \mathfrak{c}^{-1} & \mathfrak{o} \end{pmatrix}$ und $\mathfrak{M}' := \begin{pmatrix} \mathfrak{o} & \mathfrak{c}^{-1} \\ \mathfrak{c} & \mathfrak{o} \end{pmatrix}$. Dann gilt $\mathfrak{E}(\mathfrak{c}) = \mathfrak{M} \cap \mathfrak{M}'$ mit $\mathfrak{n}(\mathfrak{E}(\mathfrak{c})) = N(\mathfrak{M}\mathfrak{M}')^{-1} = \mathfrak{c}^2$, und $\Gamma(\mathfrak{c}) = \Gamma_1(\mathfrak{c}) \cap \Gamma(\mathfrak{E}(\mathfrak{c}))$. Weiter gilt $N(\mathfrak{M}M_2(\mathfrak{o}))^{-1} = \mathfrak{c}$.
Enthält $P\Gamma(\mathfrak{E}(\mathfrak{c}))$ eine Tetraeder- oder 3-Diedergruppe, dann ist 2 bzw. 3 nach Satz 9.3 träge in k, also ist $\mathfrak{n}(\mathfrak{E}(\mathfrak{c})) = 2\mathfrak{o}$ bzw. $\mathfrak{n}(\mathfrak{E}(\mathfrak{c})) = 3\mathfrak{o}$ kein Quadrat, Widerspruch.
Enthält $P\Gamma_1(\mathfrak{c})$ eine Tetraeder- oder 3-Diedergruppe, dann gibt es $A \in P^{-1}(P\Gamma_1(\mathfrak{c}))$ mit $S(A) = 0$ und $B \in P^{-1}(P\Gamma_1(\mathfrak{c}))$ mit $S(B) = 1$. Für $X \in P^{-1}(P\Gamma_1(\mathfrak{c}))$ gilt $\pm X \in \Gamma_1(\mathfrak{c})$, also $(S(X) \pm 2) \in \mathfrak{c}$. Daher gilt $(S(A) \pm 2) \in \mathfrak{c}$, also $2 \in \mathfrak{c}$, sowie $(S(B) + 2) = 3 \in \mathfrak{c}$ oder $(S(B) - 2) = 1 \in \mathfrak{c}$. Damit folgt $3 - 2 = 1 \in \mathfrak{c}$, also $\mathfrak{c} = \mathfrak{o}$, Widerspruch.

Enthält $P\Gamma(\mathfrak{E}(\mathfrak{c}))$ eine 2-Diedergruppe, dann folgt mit Satz 9.3.(iii), dass $d \not\equiv 3 \pmod 4$ und $\mathfrak{n}(\mathfrak{E}) = \mathfrak{c}^2 = 2\mathfrak{o}$ gilt. Enthält $P\Gamma_1(\mathfrak{c})$ eine 2-Diedergruppe, so folgt mit $\Gamma_1(\mathfrak{c}) \subset \Gamma_0(\mathfrak{c})$ und Satz 9.4.(iii), dass $d \not\equiv 3 \pmod 4$ und $\mathfrak{c} = 2\mathfrak{o}$ oder $\mathfrak{c}^2 = 2\mathfrak{o}$ gilt. Wir führen die Annahme $\mathfrak{c} = 2\mathfrak{o}$ zum Widerspruch. Sei also $\mathcal{D}_2 \subset P\Gamma_1(2\mathfrak{o})$ eine 2-Diedergruppe, und sei

$2\mathfrak{o} = \mathfrak{p}^2$. Wegen $-1 \in \Gamma_1(2\mathfrak{o})$ wird $P^{-1}(\mathcal{D}_2)$ erzeugt von $U = \begin{pmatrix} 1+2a & b \\ 2c & -1-2a \end{pmatrix}$ und $V = \begin{pmatrix} 1+2a' & b' \\ 2c' & -1-2a' \end{pmatrix}$ mit $UV = -VU$ und $a, b, c, a', b', c' \in \mathfrak{o}$. Mit $N(U) = 1$ folgt $2a + 2a^2 + bc + 1 = 0$. Daher gilt $b \notin \mathfrak{p}$ und $b' \notin \mathfrak{p}$, wegen $[\mathfrak{o} : \mathfrak{p}] = 2$ also $(b - b') \in \mathfrak{p}$. Weiter gilt $2 = N(U - V) = -4(a - a')^2 - 2(b - b')(c - c')$, also $(b - b') \notin \mathfrak{p}$, Widerspruch. Also gilt $\mathfrak{c} = \mathfrak{p}$. Für $X = \begin{pmatrix} a & b \\ c & d' \end{pmatrix} \in \Gamma_0(\mathfrak{c})$ gilt $c \in \mathfrak{c}$ und $ad' - bc = 1$, also $ad' \notin \mathfrak{c}$. Wegen $[\mathfrak{o} : \mathfrak{c}] = 2$ folgt daraus $(a - 1) \in \mathfrak{c}$. Also ist $\Gamma_0(\mathfrak{c}) = \Gamma_1(\mathfrak{c})$, und genauso $\Gamma(\mathfrak{E}(\mathfrak{c})) = \Gamma(\mathfrak{c})$.

Nach Satz 6.7 und 6.8.(ii) enthalten $P\Gamma(\mathfrak{M}), P\Gamma(\mathfrak{M}')$ maximalendliche 2-Diedergruppen genau dann, wenn $P\Gamma(M_2(\mathfrak{o}))$ Tetraedergruppen enthält, also $p \equiv 1$ oder $p \equiv 3 \pmod 8$ für alle Primteiler $p \neq 2$ von d gilt. Die letzte Aussage folgt nun mit Satz 9.3.(iii).

□

Satz 9.6. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung $\mathfrak{o}$. Seien D die Diskriminante von k und t die Anzahl der verschiedenen Primteiler von D. Sei M eine k-Quaternionenalgebra, und sei $\mathfrak{E}$ eine M-Eichler-Ordnung. Dann gilt:*

(i) Sei $\mathcal{T} \subset P\Gamma(\mathfrak{E})$ eine Tetraedergruppe. Dann ist $\mu(\mathcal{T}, \mathfrak{E}) = 2^t$.

(ii) Sei $\mathcal{D}_3 \subset P\Gamma(\mathfrak{E})$ eine 3-Diedergruppe. Dann ist $\mu(\mathcal{D}_3, \mathfrak{E}) = 2^t$.

(iii) Sei $\mathcal{D}_2 \subset P\Gamma(\mathfrak{E})$ maximalendliche 2-Diedergruppe. Dann hat $\mu(\mathcal{D}_2, \mathfrak{E})$ den Wert
2^t, falls $\mathfrak{n}(\mathfrak{E}) = 2\mathfrak{o}$ ist oder $p \equiv \pm 1 \pmod 8$ für alle Primteiler $p \neq 2$ von d gilt
2^{t-1}, falls $\mathfrak{n}(\mathfrak{E})^2 = 2\mathfrak{o}$ ist und $p \equiv \pm 3 \pmod 8$ für einen Primteiler p von d gilt

Beweis. Sei $\mathcal{G} \subset P\Gamma(\mathfrak{E})$ eine nichttzyklische maximalendliche Untergruppe. Nach Lemma 7.4.(i) ist $\mu(\mathcal{G}, \mathfrak{E}) = B_1(\mathfrak{F}(\mathcal{G}), \mathfrak{E})[\mathcal{A}(\mathfrak{F}(\mathcal{G})) : \mathcal{I}(\mathfrak{F}(\mathcal{G}))]^{-1}$. Da [6, Theorem 11.6.1] auch für Eichler-Ordnungen gilt, ist $N(\mathfrak{E}^\times) = \mathfrak{o}^\times$ und $B_1(\mathfrak{F}(\mathcal{G}), \mathfrak{E}) = 2B(\mathfrak{F}(\mathcal{G}), \mathfrak{E})$, siehe Satz 7.3.

Falls $\mathcal{G} = \mathcal{T}$ oder $\mathcal{G} = \mathcal{D}_3$, ist $\mathfrak{E}$ nach Lemma 4.6.(ii) die einzige M-Eichler-Ordnung mit $\mathfrak{F}(\mathcal{T}) \subset \mathfrak{E}$. Falls $\mathcal{G} = \mathcal{D}_2$, gibt es mit den Bezeichnungen von Lemma 8.1 genau drei M-Eichler-Ordnungen $\mathfrak{E}(X) := \mathfrak{N} \cap \mathfrak{N}(X)$ mit $\mathcal{D}_2 \subset P\Gamma(\mathfrak{E}(X))$ und $\Lambda(\mathfrak{E}(X)) = 2$, und genau drei M-Eichler-Ordnungen $\mathfrak{E}(X, Y) := \mathfrak{N}(X) \cap \mathfrak{N}(Y)$ mit $\mathcal{D}_2 \subset P\Gamma(\mathfrak{E}(X, Y))$ und $\Lambda(\mathfrak{E}(X, Y)) = 4$. Konjugation mit W vertauscht diese Ordnungen jeweils zyklisch. Analog zum Beweis von Satz 7.3 kann man jetzt zeigen, dass $B(\mathfrak{F}(\mathcal{T}), \mathfrak{E}) = [\mathcal{A}(\mathfrak{E}) : \mathcal{I}(\mathfrak{E})]$, $B(\mathfrak{F}(\mathcal{D}_3), \mathfrak{E}) = [\mathcal{A}(\mathfrak{E}) : \mathcal{I}(\mathfrak{E})]$ und $B(\mathfrak{F}(\mathcal{D}_2), \mathfrak{E}) = 3[\mathcal{A}(\mathfrak{E}) : \mathcal{I}(\mathfrak{E})]$ gilt.

Seien $\mathfrak{M} \neq \mathfrak{M}'$ die beiden M-Maximalordnungen mit $\mathfrak{E} = \mathfrak{M} \cap \mathfrak{M}'$. Dann induziert die Inklusion $\mathcal{A}(\mathfrak{M}) \cap \mathcal{A}(\mathfrak{M}') \hookrightarrow \mathcal{A}(\mathfrak{M})$ nach Lemma 9.2.(i) eine surjektive Abbildung $\mathcal{A}(\mathfrak{M}) \cap \mathcal{A}(\mathfrak{M}') \to \mathcal{A}(\mathfrak{M})/\mathcal{I}(\mathfrak{M})$ mit Kern $\mathcal{I}(\mathfrak{M}) \cap \mathcal{A}(\mathfrak{M}')$. Ist $j \in \mathcal{I}(\mathfrak{M}) \cap \mathcal{A}(\mathfrak{M}')$, dann gibt es ein $J \in \mathfrak{M}^\times$ mit $j(A) = JAJ^{-1}$ für $A \in M$ und $J\mathfrak{M}'J^{-1} = \mathfrak{M}'$. Aus $N(J) \in \mathfrak{o}^\times$ folgt mit [6, Lemma 6.7.5], dass $J\mathfrak{M}' = \mathfrak{M}'J = \mathfrak{M}'$, also dass $J \in \mathfrak{M}'^\times$ und $j \in \mathcal{I}(\mathfrak{M}')$. Mit Lemma 7.2 folgt $[(\mathcal{A}(\mathfrak{M}) \cap \mathcal{A}(\mathfrak{M}')) : (\mathcal{I}(\mathfrak{M}) \cap \mathcal{I}(\mathfrak{M}'))] = [\mathcal{A}(\mathfrak{M}) : \mathcal{I}(\mathfrak{M})] = 2^{t-1}$.

Für $j \in \mathcal{A}(\mathfrak{E})$ ist entweder $j(\mathfrak{M}) = \mathfrak{M}$ und $j(\mathfrak{M}') = \mathfrak{M}'$ oder $j(\mathfrak{M}) = \mathfrak{M}'$ und $j(\mathfrak{M}') = \mathfrak{M}$. Ist $\mathfrak{M}$ nicht isomorph zu $\mathfrak{M}'$, so gilt $j(\mathfrak{M}) = \mathfrak{M}$ und $j(\mathfrak{M}') = \mathfrak{M}'$ für alle $j \in \mathcal{A}(\mathfrak{E})$. Wegen

$\mathcal{I}(\mathfrak{M} \cap \mathfrak{M}') \cap \mathcal{A}(\mathfrak{M}) \cap \mathcal{A}(\mathfrak{M}') = \mathcal{I}(\mathfrak{M}) \cap \mathcal{I}(\mathfrak{M}')$ folgt daraus $[\mathcal{A}(\mathfrak{E}) : \mathcal{I}(\mathfrak{E})] = 2^{t-1}$.
Ist $\mathfrak{M}$ isomorph zu $\mathfrak{M}'$, so gibt es nach Lemma 9.2.(ii) ein $j \in \mathcal{A}(\mathfrak{E})$, das $\mathfrak{M}$ mit $\mathfrak{M}'$ vertauscht. Dann ist $[\mathcal{A}(\mathfrak{M} \cap \mathfrak{M}') : (\mathcal{A}(\mathfrak{M}) \cap \mathcal{A}(\mathfrak{M}'))] = 2$ und daher $[\mathcal{A}(\mathfrak{E}) : \mathcal{I}(\mathfrak{E})] = 2^t$.
Nach Satz 9.3 und Lemma 5.5.(iii) ist $\mathfrak{M}$ genau dann nicht isomorph zu $\mathfrak{M}'$, wenn $\Lambda(\mathfrak{M} \cap \mathfrak{M}') = N_{abs}(\mathfrak{n}(\mathfrak{E})) = 2$ ist und es eine Stelle p von $\mathbb{Q}$ gibt mit $\left(\frac{2, -d}{p}\right) = -1$.
Die Aussagen des Satzes folgen mit Lemma 7.4.(ii) und Auswertung der Hilbert-Symbole.

□

Satz 9.7. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Sei M eine k-Quaternionenalgebra, und sei $\mathfrak{E}$ eine M-Eichler-Ordnung.
Sei $\mathcal{T} \subset P\Gamma(\mathfrak{E})$ eine Tetraedergruppe. Sei $\mathcal{C}_2 \subset \mathcal{T}$ eine Untergruppe der Ordnung 2. Dann gibt es eine Tetraedergruppe $\mathcal{T}' \subset P\Gamma(\mathfrak{E})$ mit $\mathcal{C}_2 \subset \mathcal{T}'$, die nicht $P\Gamma(\mathfrak{E})$-konjugiert zu $\mathcal{T}$ ist. Jede Tetraedergruppe $\mathcal{T}'' \subset P\Gamma(\mathfrak{E})$ mit $\mathcal{C}_2 \subset \mathcal{T}''$ ist $P\Gamma(\mathfrak{E})$-konjugiert zu $\mathcal{T}$ oder $\mathcal{T}'$.

Beweis. Nach Satz 9.3 gibt es in $P\Gamma(\mathfrak{E})$ keine maximalendlichen 2-Diedergruppen.
Der Beweis erfolgt dann wie der Beweis von Satz 8.3, mit $\mathfrak{E}$ anstelle von $\mathfrak{M}$.

□

Satz 9.8. *Sei $d \in \mathbb{N}$ quadratfrei, und sei $k = \mathbb{Q}(i\sqrt{d})$.*
Sei M eine k-Quaternionenalgebra, und sei $\mathfrak{E}$ eine M-Eichler-Ordnung.
Sei $\mathcal{D}_3 \subset P\Gamma(\mathfrak{E})$ eine 3-Diedergruppe und $\mathcal{C}_3 \subset \mathcal{D}_3$ die Untergruppe der Ordnung 3. Dann gibt es eine 3-Diedergruppe $\mathcal{D}_3' \subset P\Gamma(\mathfrak{E})$ mit $\mathcal{C}_3 \subset \mathcal{D}_3'$, die nicht $P\Gamma(\mathfrak{E})$-konjugiert zu $\mathcal{D}_3$ ist. Jede 3-Diedergruppe $\mathcal{D}_3'' \subset P\Gamma(\mathfrak{E})$ mit $\mathcal{C}_3 \subset \mathcal{D}_3''$ ist $P\Gamma(\mathfrak{E})$-konjugiert zu $\mathcal{D}_3$ oder $\mathcal{D}_3'$.

Beweis. wie der Beweis von Satz 8.5, mit $\mathfrak{E}$ anstelle von $\mathfrak{M}$

□

Satz 9.9. *Sei $d \in \mathbb{N}$ quadratfrei, sei $d \neq 1$, und sei $k = \mathbb{Q}(i\sqrt{d})$ mit Hauptordnung $\mathfrak{o}$.*
Sei M eine k-Quaternionenalgebra, und sei $\mathfrak{E}$ eine M-Eichler-Ordnung.
Sei $\mathcal{D}_2 \subset P\Gamma(\mathfrak{E})$ eine maximalendliche 2-Diedergruppe.

(i) Sei $\mathfrak{n}(\mathfrak{E})^2 = 2\mathfrak{o}$, sei $d \equiv 2 \pmod 4$, und es gebe $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 2$.
Dann gilt $p \equiv \pm 1 \pmod 8$ für alle Primteiler $p \neq 2$ von d, und weiter gilt dann:

(a) Es gibt eine Untergruppe $\mathcal{C}_2 \subset \mathcal{D}_2$ der Ordnung 2 und eine 2-Diedergruppe $\mathcal{D}_2' \subset P\Gamma(\mathfrak{E})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2'$, die nicht $P\Gamma(\mathfrak{E})$-konjugiert zu $\mathcal{D}_2$ ist.
Jede 2-Diedergruppe $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{E})$ mit $\mathcal{C}_2 \subset \mathcal{D}_2$
ist $P\Gamma(\mathfrak{E})$-konjugiert zu $\mathcal{D}_2$ oder zu $\mathcal{D}_2'$.

(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 $\mathcal{C}_2''$ nicht zu $\mathcal{C}_2$, aber zueinander $P\Gamma(\mathfrak{E})$-konjugiert.
Jede 2-Diedergruppe $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{E})$ mit $\mathcal{C}_2' \subset \mathcal{D}_2''$ oder $\mathcal{C}_2'' \subset \mathcal{D}_2''$
ist $P\Gamma(\mathfrak{E})$-konjugiert zu $\mathcal{D}_2$.

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

(a) *Seien* $\mathcal{C}_2, \mathcal{C}_2', \mathcal{C}_2'' \subset \mathcal{D}_2$ *die drei Untergruppen der Ordnung* 2.
Dann sind $\mathcal{C}_2$, $\mathcal{C}_2'$ *und* $\mathcal{C}_2''$ *paarweise nicht zueinander* $P\Gamma(\mathfrak{E})$*-konjugiert.*

(b) *Es gibt eine* 2*-Diedergruppe* $\mathcal{D}_2' \subset P\Gamma(\mathfrak{E})$ *mit* $\mathcal{C}_2 \subset \mathcal{D}_2'$,
die nicht $P\Gamma(\mathfrak{E})$*-konjugiert zu* $\mathcal{D}_2$ *ist.*
Jede 2*-Diedergruppe* $\mathcal{D}_2'' \subset P\Gamma(\mathfrak{E})$ *mit* $\mathcal{C}_2 \subset \mathcal{D}_2''$, $\mathcal{C}_2' \subset \mathcal{D}_2''$ *oder* $\mathcal{C}_2'' \subset \mathcal{D}_2''$
ist $P\Gamma(\mathfrak{E})$*-konjugiert zu* $\mathcal{D}_2$ *oder zu* $\mathcal{D}_2'$.

Beweis. Seien $\mathfrak{M}, \mathfrak{M}'$ die M-Maximalordnungen mit $\mathfrak{E} = \mathfrak{M} \cap \mathfrak{M}'$, sei $\mathcal{D}_2 \subset P\Gamma(\mathfrak{M})$ maximalendliche Untergruppe, $\mathcal{T} \subset P\Gamma(M)$ Tetraedergruppe mit $\mathcal{D}_2 \subset \mathcal{T}$, und $2\mathfrak{o} = \mathfrak{p}^2$.

(i) Sei $p \neq 2$ ein Primteiler von d. Dann gilt $x^2 \equiv 2 \pmod{p}$, und mit dem zweiten Ergänzungssatz zum quadratischen Reziprozitätsgesetz folgt $p \equiv \pm 1 \pmod 8$.

(a) Nach Satz 8.4.(i)(a) gibt es eine Gruppe $\mathcal{C}_2$ der Ordnung 2, eine 2-Diedergruppe $\mathcal{D}_2'$ und eine Tetraedergruppe $\mathcal{T}'$ mit $\mathcal{C}_2 \subset \mathcal{D}_2' \subset \mathcal{T} \subset P\Gamma(\mathfrak{M})$. Die Zuordnung $\mathcal{D}_2 \mapsto \mathcal{C}_2$ ist eindeutig, $\mathcal{C}_2', \mathcal{C}_2''$ sind in $P\Gamma(\mathfrak{E}) \subset P\Gamma(\mathfrak{M})$ nicht konjugiert zu $\mathcal{C}_2$. Da $P\Gamma(\mathfrak{E})$ keine Tetraedergruppe enthält, erfolgt der Beweis wie der von Satz 8.3, mit $\mathfrak{E}$ anstelle von $\mathfrak{M}$, wenn wir die Zwischenbemerkung wie folgt ersetzen:
Zwischenbemerkung: Wir können $JUJ^{-1} = U$ annehmen, da U in $\Gamma(\mathfrak{E})$ zu U^{-1}, aber (wie eben nachgewiesen) nicht zu $V^{\pm 1}$ und $(UV)^{\pm 1}$ konjugiert ist.

(b) Nach Satz 8.4.(i)(b) ist $\mathcal{C}_2'$ in $P\Gamma(\mathfrak{M})$-konjugiert zu $\mathcal{C}_2''$.
Wegen $\mathcal{D}_2 \subset \mathfrak{M}'$ und $N(\mathfrak{M}\mathfrak{M}')^{-1} = \mathfrak{p}$ folgt mit Lemma 8.1, dass $\mathcal{T} \subset P\Gamma(\mathfrak{M}')$. Mit den Bezeichnungen des ersten Absatzes von Beweisabschnitt (b) zu Satz 8.4 gilt daher $(k(UV) \cap \mathfrak{M}')_2 = \mathfrak{o}_2[(1+UV)/\pi]$, und damit auch $\epsilon \in \mathfrak{M}' \cap \mathfrak{M} = \mathfrak{E}$. Wie im zweiten Absatz von Beweisabschnitt (c) zu Satz 8.4 folgt, dass $\mathcal{D}_2''$ in $P\Gamma(\mathfrak{M})$ zu $\mathcal{D}_2$ oder $\mathcal{D}_2'$ konjugiert ist. Da es nach (a) keine Tetraedergruppe $\mathcal{T}''$ mit $\mathcal{D}_2'' \subset \mathcal{T}'' \subset P\Gamma(\mathfrak{M})$ gibt, ist $\mathcal{D}_2''$ in $P\Gamma(\mathfrak{E}) \subset P\Gamma(\mathfrak{M})$ nicht zu $\mathcal{D}_2'$ konjugiert.

(ii) (a) Falls $d \not\equiv 2 \pmod 4$ oder $x^2 - dy^2 \neq 2$ für alle $x, y \in \mathbb{Z}$, sind $\mathcal{C}_2$, $\mathcal{C}_2'$ und $\mathcal{C}_2''$ nach Satz 8.4.(ii)(b) paarweise nicht in $P\Gamma(\mathfrak{M})$, also auch nicht in $P\Gamma(\mathfrak{E})$ konjugiert. Seien also $\mathfrak{n}(\mathfrak{E}) = 2\mathfrak{o}$, $d \equiv 2 \pmod 4$, $x, y \in \mathbb{Z}$ mit $x^2 - dy^2 = 2$. Seien U, V, ϵ wie im ersten Absatz des Beweisabschnitts (b) zu Satz 8.4. Es genügt, die Annahme zum Widerspruch zu führen, dass es ein $\epsilon' \in \Gamma(\mathfrak{E})$ gibt mit $\epsilon' V \epsilon'^{-1} = U$. Mit $\epsilon\epsilon'^{-1} U = U \epsilon\epsilon'^{-1}$ folgt $\epsilon\epsilon'^{-1} \in k(U) \cap \Gamma(\mathfrak{M}) = \Gamma(\mathfrak{o}[U]) \subset \Gamma(\mathfrak{E})$, also $\epsilon \in \Gamma(\mathfrak{E})$. Da x gerade ist, gilt $yi\sqrt{d}(U+V)/2 \in \mathfrak{E}$ und $(1+UV)/\pi \in \mathfrak{E}_2 \subset \mathfrak{M}_2'$, Widerspruch.

(b) Für $\mathcal{C}_2 \subset \mathcal{D}_2''$ erfolgt der Beweis wie im Beweisabschnitt (a) zu Satz 8.3 mit $\mathfrak{E}$ anstelle von $\mathfrak{M}$, wenn wir dort die Zwischenbemerkung wie folgt ersetzen:
Zwischenbemerkung: Wir können $JUJ^{-1} = U$ annehmen,, da U in $\Gamma(\mathfrak{E})$ zu U^{-1}, nach Satz 9.9.(ii)(a) aber nicht zu $V^{\pm 1}$ und $(UV)^{\pm 1}$ konjugiert ist.

Für $\mathcal{C}_2' \subset \mathcal{D}_2''$ oder $\mathcal{C}_2'' \subset \mathcal{D}_2''$ erfolgt der Beweis analog zum zweiten Absatz im Beweisabschnitt (c) des Beweises von Satz 8.4, mit $\mathfrak{E}$ anstelle von $\mathfrak{M}$.

□

Literatur

[1] Ethan Berkove and Alexander D. Rahm, *The mod 2 cohomology rings of* SL_2 *of the imaginary quadratic integers*, J. Pure Appl. Algebra **220** (2016), no. 3, 944–975, DOI 10.1016/j.jpaa.2015.08.002. With an appendix by Aurel Page. MR3414403

[2] 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)

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

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

[5] 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/`

[6] Colin Maclachlan and Alan W. Reid, *The arithmetic of hyperbolic 3-manifolds*, Graduate texts in mathematics. 219, Springer-Verlag, New York, 2003.

[7] 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`

[8] 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