Die Konjugationsklassenanzahlen der endlichen Untergruppen in der Norm-Eins-Gruppe von Maximalordnungen in Quaternionenalgebren

Norbert Krämer

Die Konjugationsklassenanzahlen der endlichen Untergruppen in der Norm-Eins-Gruppe von Maximalordnungen in Quaternionenalgebren

Diplomarbeit

von

Norbert Krämer

Bonn 1980

Einleitung

Gegeben sei ein algebraischer Zahlkörper mit Hauptordnung (Ring der ganzen Zahlen) o und über diesem Körper eine Quaternionenalgebra Q. (Unter den Begriff Quaternionenalgebra fasse ich sowohl k-zentrale Divisionsalgebren der Dimension 4 als auch die Algebra $M_2(k)$ der 2×2 - Matrizen über k.)
Ich untersuche zunächst, welche endlichen Untergruppen es bis auf Isomorphie in der Gruppe $\Gamma(Q)$ der Quaternionen mit (reduzierter) Norm Eins gibt.
Die zentrale Problemstellung dieser Arbeit besteht darin, für die verschiedenen maximalen Ordnungen $\mathfrak{M}$ aus Q die Konjugationsklassenzahlen der endlichen Gruppen in der Norm-Eins-Gruppe $\Gamma(\mathfrak{M})$ zu berechnen.
Dabei schließe ich natürlich den Fall aus, daß $\Gamma(\mathfrak{M})$ selbst eine endliche Gruppe ist. Dieser Fall tritt auf, wenn k total reell und Q an allen unendlichen Primstellen verzweigt (total definit) ist.
Es gelingt mir, die gesuchten Konjugationsklassenzahlen zu berechnen; ich kann sie im wesentlichen durch Idealklassenzahlen und Einheitengruppenindizes von algebraischen Zahlkörpern ausdrücken.
Die Konjugationsklassenzahlen sind i.a. für verschiedene Maximalordnungen von Q unterschiedlich; für eine konkret vorgegebene Maximalordnung $\mathfrak{M}$ hängen sie noch von der Position von $\mathfrak{M}$ zu gewissen ausgezeichneten Maximalordnungen ab.

Im folgenden skizziere ich den Inhalt der Arbeit. Eine genauere Erläuterung des Vorgehens und Hinweise auf die wichtigsten Sätze findet man in den Einleitungen zu den vier Teilen der Arbeit und zum Anhang.

Ist G eine endliche Untergruppe von $\Gamma(Q)$, so gibt es eine Q-Maximalordnung $\mathfrak{M}$ mit $G \subset \Gamma(\mathfrak{M})$. Es ist daher natürlich, zunächst die endlichen Untergruppen von $\Gamma(Q)$ zu untersuchen.
Q kann als Unterring von $Q \otimes_k \mathbb{C} \cong M_2(\mathbb{C})$ und deshalb $\Gamma(Q)$ als Untergruppe von $SL(2,\mathbb{C})$ aufgefaßt werden. Die endlichen Untergruppen von $SL(2,\mathbb{C})$ sind bekannt. Außer den zyklischen Gruppen (beliebiger Ordnung) handelt es sich um die (binären) n-Diedergruppen ($n \geq 2$), (binären) Tetraeder-, (binären) Oktaeder- und (binären) Ikosaedergruppen.

Eine (binäre) n-Diedergruppe hat die Ordnung 4n; für $n > 2$ ist sie zentrale Erweiterung mit $\{\pm 1\}$ der Symmetriegruppe eines regulären n-Ecks. Eine (binäre) 2-Diedergruppe ist isomorph zur Quaternionengruppe. Die (binären) Tetraeder-, Oktaeder- und Ikosaedergruppen haben die Ordnungen 24, 48 und 120. Sie sind zentrale Erweiterungen mit $\{\pm 1\}$ der Drehgruppen der entsprechenden regulären Polyeder.
Ich weise in der Arbeit nach, daß isomorphe endliche Untergruppen von $\Gamma(Q)$ stets $Q^{\times}$-konjugiert sind.
Für jede Quaternionenalgebra Q bestimme ich genau, welche endlichen Untergruppen $\Gamma(Q)$ (bis auf Isomorphie) enthält.
Über jedem algebraischen Zahlkörper gibt es bis auf Isomorphie höchstens eine Quaternionenalgebra, für die $\Gamma(Q)$ eine vorgegebene nichtzyklische Gruppe enthält. Ich bestimme die Verzweigungsstellen dieser Quaternionenalgebren.
Um zu entscheiden, ob eine zyklische Gruppe der Ordnung n in $\Gamma(Q)$ enthalten ist, muß untersucht werden, ob eine gewisse halbeinfache quadratische Erweiterung $k[E]$ (mit einem Element E der Ordnung n) in Q eingebettet werden kann. Dies läßt sich leicht als Kriterium für die Verzweigungsstellen von Q über k formulieren.
Enthält k Einheitswurzeln $\neq \pm 1$, so ist $k[E]$ im allgemeinen kein Körper. Daher muß ich eine Reihe von Ergebnissen, die für quadratische Körpererweiterungen wohlbekannt sind, auf halbeinfache quadratische Erweiterungen verallgemeinern.

Falls alle endlichen Untergruppen von $\Gamma(Q)$ zyklisch sind, so sind ihre Konjugationsklassenzahlen in $\Gamma(\mathfrak{M})$ für alle Q-Maximalordnungen $\mathfrak{M}$ gleich. Enthält aber etwa $\Gamma(Q)$ auch n-Diedergruppen, so sind die Konjugationsklassenzahlen der n-Diedergruppen und die der zyklischen Gruppen der Ordnung 2n in $\Gamma(\mathfrak{M})$ i.a. nicht für alle Q-Maximalordnungen $\mathfrak{M}$ gleich. Zur Bestimmung der Konjugationsklassenzahlen muß man dann alle Q-Maximalordnungen gleichzeitig betrachten.
Dazu ist es wichtig, die Klassifikation der Maximalordnungen nach ihrem Typ (d.h. Isomorphie) genau zu kennen.

Die Konjugationsklassenzahlen von Oktaeder- und Ikosaedergruppen in $\Gamma(\mathfrak{M})$ lassen sich auf direktem Wege bestimmen (da diese Gruppen maximal-endlich in $SL(2,\mathbb{C})$ sind).

Die Konjugationsklassenzahlen der anderen endlichen Untergruppen in $\Gamma(\mathfrak{M})$ bestimme ich, indem ich sie auf Konjugationsklassenzahlen von Erzeugenden bzw. Erzeugendensystemen zurückführe.
Bei diesem Verfahren zeigt sich, daß die Konjugationsklassenzahlen der verschiedenen endlichen Gruppen nicht völlig unabhängig voneinander sind. So bilden für jedes $n > 2$ die n-Diedergruppen und die zyklischen Gruppen der Ordnung 2n einen Verband; ihre Konjugationsklassenzahlen in $\Gamma(\mathfrak{M})$ lassen sich (nur) gemeinsam berechnen. Einen ähnlichen Verband bilden die zyklischen Gruppen der Ordnung 4, die 2-Diedergruppen und die Tetraedergruppen.

Ist k ein total reeller Zahlkörper, so ist die Situation im Vergleich zum allgemeinen Fall besonders einfach:
Bei allen in Frage kommenden Quaternionenalgebren Q sind alle endlichen Untergruppen von $\Gamma(Q)$ zyklisch (da alle endlichen Untergruppen von $SL(2,\mathbb{R})$ zyklisch sind).
Die Konjugationsklassenzahlen der zyklischen Gruppen einer festen Ordnung 2n in $\Gamma(\mathfrak{M})$ sind für alle Q-Maximalordnungen $\mathfrak{M}$ gleich.
Für diese Situation (total reeller Zahlkörper) haben bereits Shimizu /19/, Prestel /16/ und Schneider /17/ die Konjugationsklassenzahlen der endlichen Gruppen in $\Gamma(\mathfrak{M})$ berechnet.

Ist $k = \mathbb{Q}(i\sqrt{d})$ imaginärquadratischer Zahlkörper, so sind als endliche Untergruppen von $\Gamma(Q)$, die das Zentrum $\{\pm 1\}$ echt enthalten, nur zyklische Gruppen der Ordnung 4 und 6, 2-Dieder-, 3-Dieder- und Tetraedergruppen möglich.
Ich forme die Konjugationsklassenzahlen dieser Gruppen in einem teilweise komplizierten Prozeß soweit um, daß sie mit Hilfe von zahlentheoretischen Tabellen relativ leicht konkret berechnet werden können. Die Konjugationsklassenzahl in $\Gamma(\mathfrak{M})$ der zyklischen Gruppen der Ordnung 4 bzw. 6 (soweit vorhanden) hängt im wesentlichen von der Klassenzahl des reellquadratischen Zahlkörpers $\mathbb{Q}(\sqrt{d})$ bzw. $\mathbb{Q}(\sqrt{3d})$ ab. Die Konjugationsklassenzahl der nichtzyklischen Gruppen (soweit vorhanden) in $\Gamma(\mathfrak{M})$ hängt im wesentlichen von der Zahl der Primteiler von d ab.

Im Anhang zur Arbeit untersuche ich genauer die Maximalordnung $M_2(\mathfrak{o})$ in der Quaternionenalgebra $M_2(k)$ für imaginärquadratische Zahlkörper $k = \mathbb{Q}(i\sqrt{d})$. Für $1 \leq d \leq 101$ habe ich die Ergebnisse tabelliert.

Für die interessante Themenstellung und die geduldige Betreuung möchte ich Herrn Prof. Dr. Jürgen Rohlfs herzlich danken.

Inhaltsverzeichnis

Teil I
Quaternionenalgebren und halbeinfache quadratische Erweiterungen

Teil I hat vorbereitenden Charakter. In ihm sammle bzw. entwickle ich ausführlich grundlegende Tatsachen für die ganze Arbeit, insbesondere für die Teile II und III.
Algebraische und $\mathfrak{p}$-adische Zahlentheorie setze ich als bekannt voraus.
Ich gebe im folgenden eine Übersicht über den Inhalt von Teil I und versuche jeweils zu erläutern, in welchem Zusammenhang die Ergebnisse gebraucht werden.

1. § 1 ist eine Übersicht über einige algebraische Eigenschaften von Quaternionenalgebren.

2. Ist Q eine Quaternionenalgebra über dem algebraischen Zahlkörper k und $E \neq \pm 1$ ein Element endlicher Ordnung in der Norm-Eins-Gruppe $\Gamma(Q)$, dann ist $K = k[E]$ eine halbeinfache quadratische Erweiterung von k.
In § 2 entwickle ich einige (vermutlich bekannte) algebraische Eigenschaften von halbeinfachen quadratischen Erweiterungen.

3. In /19/, /16/ und /17/ wird vorausgesetzt, daß k total reell ist. Dann ist $k[E]$ immer ein Körper, also auch eine einfache k-Algebra.
In dieser Arbeit untersuche ich aber auch den Fall, daß k Einheitswurzeln $\zeta_n \neq \pm 1$ enthält. Hat E die Ordnung n, dann ist $k[E]$ kein Körper und nicht einfache k-Algebra. Daher muß ich oft Ergebnisse, die für quadratische Erweiterungskörper K beziehungsweise einfache Unteralgebren K von Q bekannt sind, auf halbeinfache quadratische Erweiterungen verallgemeinern. Wichtige Beispiele dafür sind:
i) Quadratische Erweiterungen sind maximalkommutativ (Satz 3.2) und
ii) Ein Isomorphismus zwischen Unteralgebren von Q läßt sich zu einem Automorphismus von Q fortsetzen (Satz 3.3).
((3.2) und (3.3) gelten sogar für Unteralgebren von Q mit Radikal.)
Der Beweis von (3.2) und (3.3) ist der Inhalt von § 3.
Die beiden Sätze sind mir aus der Literatur nicht bekannt.

4. Ich berechne später die Konjugationsklassenzahlen der endlichen Untergruppen in der Norm-Eins-Gruppe $\Gamma(\mathfrak{M})$ einer Q-Maximalordnung $\mathfrak{M}$.
Dazu wird es notwendig, die Maximalordnungen und die Durchschnitte $\mathfrak{M} \cap k[E]$ zu untersuchen. Vorbereitend sammle ich in § 4 bekannte Eigenschaften von Ordnungen und ihren Idealen in halbeinfachen Algebren.
Wie bemerkt, sind dabei für diese Arbeit nur Maximalordnungen in Quaternionenalgebren und Ordnungen in halbeinfachen quadratischen Erweiterungen interessant.

5. $\Gamma(Q)$ enthält genau dann eine zyklische Untergruppe der Ordnung n, wenn die von einem E mit Norm 1 und Ordnung n über k erzeugte halbeinfache Algebra $k[E]$ in Q eingebettet werden kann. Satz (5.6) beschreibt, welche halbeinfachen quadratischen Erweiterungen K von k in eine vorgegebene k-Quaternionenalgebra eingebettet werden können. Das ist das Hauptergebnis von § 5. Satz (5.6) ist im wesentlichen bekannt. Um ihn exakt und allgemein formulieren zu können, habe ich zu Beginn von § 5 einige Eigenschaften der Hauptordnung von K aufgelistet für den Fall, daß K kein Körper ist.

6. Das wesentliche Resultat von § 6 ist folgendes:
Sei o die Hauptordnung von k und $\mathfrak{O}_0$ die Hauptordnung der halbeinfachen quadratischen Erweiterung K von k. Jede Ordnung $\mathfrak{O}$ in K, die o enthält, läßt sich schreiben als $\mathfrak{O} = o + \mathfrak{f}\mathfrak{O}_0$ mit einem eindeutig bestimmten, ganzen o-Ideal $\mathfrak{f}$ (Satz 6.8). $\mathfrak{f} =: f(\mathfrak{O})$ heißt der o-Führer von $\mathfrak{O}$ und ich schreibe $\mathfrak{O}^{\mathfrak{f}} := o + \mathfrak{f}\mathfrak{O}_0 = \mathfrak{O}$.

7. In § 7 definiere ich zunächst die Gruppe $I^{\mathfrak{f}}$ der $\mathfrak{O}^{\mathfrak{f}}$-Ideale als lokale Hauptideale. Im Rest von § 7 arbeite ich auf Satz (7.25) hin; das ist eine Formel für die Klassenzahl von $I^{\mathfrak{f}}$. Diese Formel ist für die Beispiele wichtig (§§ 20,21).

Zusatzbemerkungen zu 6. und 7.:

i) Viele Lemmata und Methoden in den Paragrafen 6 und 7 sind lokaler Natur. Auf einige von ihnen komme ich in späteren Paragrafen zurück.

ii) Für Körper K ist Satz (7.25) schon bewiesen (siehe /16/ S.188 (2.8)) und Satz (6.8) folgt relativ leicht aus /16/ § 4. Da ich aber auch den Fall untersuchen muß, daß K kein Körper ist, habe ich eigene Beweise entwickelt und die Gelegenheit genutzt, neue Bezeichnungen einzuführen, die meines Erachtens für diese Arbeit nützlicher sind.

8. Sei I^k die Gruppe der o-Ideale. Sei $\mathfrak{m}$ der Idealmodul, der aus den unendlichen (reellen) Verzweigungsstellen von Q über k zusammengesetzt ist, und sei $S_{\mathfrak{m}}$ der Strahl mod $\mathfrak{m}$. Bei der Konjugationsklassenzahlberechnung in den Paragrafen 16 und 17 spielt der Index $[I^k : N(I^K)S_{\mathfrak{m}}]$ eine wichtige Rolle. Er kann gleich 1 oder gleich 2 werden. Das läßt sich mit der Klassenkörpertheorie entscheiden (siehe 8.4). In Korollar (8.4), dem wichtigsten Satz in § 8, sind die Aussagen aus der Klassenkörpertheorie zusammengefaßt, die ich später benutzen werde.

Bemerkung:
Wenn Q an allen unendlichen Primstellen von k verzweigt ist, ist $\Gamma(\mathfrak{M})$ eine endliche Gruppe für alle Q-Maximalordnungen $\mathfrak{M}$ (siehe Satz 15.11).

Das muß ich bei der Berechnung der Konjugationsklassenzahlen immer ausschließen. Für total reelle Zahlkörper tritt daher nur der einfachere Fall $\left[I^k : N(I^K)S_{\mathfrak{M}}\right] = 1$ auf (denn $K = k[E]$ ist an allen reellen Primstellen von k verzweigt).

9. In § 9 sammle ich einige (bekannte) Eigenschaften von Maximalordnungen und ihren Idealen in Quaternionenalgebren.

10. Falls k total reell ist, sind alle endlichen Untergruppen von $\Gamma(Q)$ zyklisch. In diesem Fall hat die Konjugationsklassenzahl der endlichen Gruppen in $\Gamma(\mathfrak{M})$ für alle Q-Maximalordnungen $\mathfrak{M}$ den gleichen Wert (sie hängt nur von der Gruppenordnung n ab).

Falls $\Gamma(Q)$ auch Diedergruppen enthält, können die Konjugationsklassenzahlen für Q-Maximalordnungen, die nicht vom gleichen Typ sind (d.h. nicht o-algebrenisomorph sind), verschiedene Werte annehmen. Daher wird es sehr wichtig, die Klassifikation der Q-Maximalordnungen nach ihrem Typ zu untersuchen. Die Resultate, die ich bei dieser Untersuchung gefunden habe, sind die Sätze (10.9) und (10.10):

Ist $\mathfrak{M}$ eine feste Maximalordnung, so wird durch die Vorschrift $\mathfrak{M}' \to N(\mathfrak{M}\,\mathfrak{M}')$, ($\mathfrak{M}'$ Maximalordnung) , eine Bijektion von der Menge $\tilde{Q}$ der Q-Maximalordnungstypen auf die Quotientengruppe $I^k/RI^{k(2)}S_{\mathfrak{M}}$ induziert. Dabei wird $R \subset I^k$ von den in Q verzweigten Primidealen erzeugt. (10.10). $I^k/RI^{k(2)}S_{\mathfrak{M}}$ operiert in natürlicher Weise auf $\tilde{Q}$ (10.9).

Der Beweis stützt sich im wesentlichen auf den Satz von Eichler über Hauptideale (10.4).

Die von mir entdeckte Klassifikation der Maximalordnungstypen ist meines Wissens in der Literatur nicht zu finden.

11. Wie in Punkt 4 bemerkt, muß ich Durchschnitte von halbeinfachen quadratischen Erweiterungen K mit Q-Maximalordnungen $\mathfrak{M}$ untersuchen. Dies geschieht hauptsächlich in den Paragrafen 16, 18 und 23. Um § 16 kürzer zu halten, habe ich einen Teil, der sich leicht allgemein für halbeinfache quadratische Erweiterungen formulieren läßt, abgetrennt und § 11 genannt. Das Hauptergebnis von § 11 ist Satz (11.9). Auch auf die Lemmata (11.1), (11.4) und (11.6) komme ich später zurück.

Der Großteil der Ergebnisse aus § 11 ist (für Körper K) bekannt und geht auf eine Arbeit von Eichler zurück /7/. Duch eine Verfeinerung der Eichlerschen Methoden erhalte ich darüberhinaus ein entscheidend neues Ergebnis (siehe 11.9.i), das es ermöglichen wird, die gegenseitige Abhängigkeit des o-Führers $f(\mathfrak{M} \cap K)$ und des Maximalordnungstypen $\tilde{\mathfrak{M}}$ zu untersuchen (für festes K). (In den §§ 18, 23 beweise ich vergleichbare Ergebnisse.)

§ 1 . Quaternionenalgebren

In § 1 werden bekannte Definitionen und Sätze aus der Theorie der Quaternionenalgebren zusammengestellt.

Unter einem algebraischen Zahlkörper wollen wir einen Körper k mit $\mathbb{Q} \subset k \subset \mathbb{C}$ und $[k : \mathbb{Q}] < \infty$ verstehen. Daß k in $\mathbb{C}$ fest eingebettet ist, werden wir in Teil I nicht wirklich benutzen. Diese Voraussetzung wird erst später wichtig.

Ist k ein algebraischer Zahlkörper und $\mathfrak{p}$ eine (endliche oder unendliche) Primstelle von k, so bezeichne $k_\mathfrak{p}$ die Vervollständigung von k bezüglich einer $\mathfrak{p}$-adischen Bewertung von k. Ist $\mathfrak{p}$ eine endliche Primstelle von k, so heißt $k_\mathfrak{p}$ ein $\mathfrak{p}$-adischer Zahlkörper. Ist k algebraischer Zahlkörper, so identifizieren wir die endlichen Primstellen von k mit den dazugehörenden Primidealen.

Soweit nicht ausdrücklich anders gesagt, sollen in dieser Arbeit alle Körper algebraische oder $\mathfrak{p}$-adische Zahlkörper oder $\mathbb{R}$ oder $\mathbb{C}$ sein.

Ist k ein Körper, so wollen wir k-Algebren immer als endlichdimensional voraussetzen.

Ist k Körper und A eine k-Algebra mit Eins, dann heißt A einfach, wenn sie außer {0} und A kein zweiseitiges Ideal enthält.

Ist R ein Ring mit Eins, dann bezeichne $R^\times$ die (multiplikative) Gruppe der invertierbaren Elemente von R.

Eine Algebra A mit Eins heißt Divisionsalgebra, wenn $A^\times = A - \{0\}$, also wenn A ein Schiefkörper ist

Ist k ein Körper, A eine k-Algebra, $n \in \mathbb{N}$, so bezeichne $M_n(A) = M_n(k) \otimes_k A$ den Ring der n×n-Matrizen mit Koeffizienten aus A. Auf natürliche Weise ist $M_n(A)$ eine k-Algebra und es gilt:

$$[M_n(A) : k] = n^2 [A : k] \qquad (1.1)$$

Wir fassen A (auf natürliche Weise) als Unterring von $M_n(A)$ auf.

(1.2) Definition: Sei R ein Ring und seien A und B zwei R-Algebren. Sind A und B R-algebrenisomorph, so sagen wir kurz: A und B sind R-isomorph und schreiben: $A \cong_R B$.

(1.3) Satz: Sei k ein Körper, A eine k-Algebra.
A ist genau dann einfach, wenn es eine k-Divisionsalgebra D und ein $n \in \mathbb{N}$ gibt mit $A \cong_k M_n(D)$.

Bew.: siehe /3/ S. 18 Satz 3 und S. 21 Satz 5

Ist k ein Körper, K ein Erweiterungskörper von k und A eine k-Algebra, dann ist $K \otimes_k A$ eine K-Algebra und es gilt: $[K \otimes_k A : K] = [A : k]$. Wir fassen A (auf natürliche Weise) als Unterring von $K \otimes_k A$ auf. Falls $k \subset A$, fassen wir auch K (auf natürliche Weise) als Unterring von $K \otimes_k A$ auf.
(Vergleiche dazu /14/ S.418/419,§3 und /3/ S.7,§2.4)

(1.4) Definition: Ist k ein algebraischer Zahlkörper, $\mathfrak{p}$ eine Primstelle von k und A eine k-Algebra, dann sei $A_\mathfrak{p} := k_\mathfrak{p} \otimes_k A$.

Ist k ein Körper und A eine k-Algebra mit $k \subset A$, dann heißt A zentral, wenn das Zentrum des Ringes A gleich k ist.

(1.5) Lemma: Ist k ein Körper, K ein Erweiterungskörper von k und A eine einfache zentrale k-Algebra, dann ist $K \otimes_k A$ eine einfache, zentrale K-Algebra.

Bew.: siehe /3/ S.46 Satz 12

(1.6) Definition: Sei k Körper, K Erweiterungskörper von k und A einfache zentrale k-Algebra.
i) Wir sagen, daß A zerfällt, wenn es $n \in \mathbb{N}$ gibt mit $A \underset{k}{\sim} M_n(k)$.
ii) K heißt Zerfällungskörper von A, wenn $K \otimes_k A$ zerfällt.
iii) Ist k algebraischer Zahlkörper, $\mathfrak{p}$ eine Primstelle von k, dann sagen wir, daß A an der Stelle $\mathfrak{p}$ zerfällt, wenn $k_\mathfrak{p}$ Zerfällungskörper von A ist (d.h. wenn $A_\mathfrak{p}$ zerfällt).
iv) Ist k algebraischer Zahlkörper und $\mathfrak{p}$ eine Primstelle von k, an der A nicht zerfällt, dann heißt $\mathfrak{p}$ Verzweigungsstelle von A. Wir sagen auch: A ist an der Stelle $\mathfrak{p}$ verzweigt (über k).

(1.7) Definition: Sei Q eine einfache, zentrale Algebra über dem Körper k und sei $[Q : k] = 4$. Dann heißt Q eine k-Quaternionenalgebra. Die Elemente von Q heißen Quaternionen.

(1.8) Lemma: Sei k ein Körper. Ist Q eine k-Quaternionenalgebra, dann gilt entweder i) Q ist k-Divisionsalgebra
oder ii) $Q \underset{k}{\sim} M_2(k)$
Ist umgekehrt Q eine zentrale k-Algebra mit $[Q : k] = 4$ und gilt i) oder ii), dann ist Q eine k-Quaternionenalgebra.

Bew.: Sei Q eine k-Quaternionenalgebra. Nach Satz (1.3) gibt es eine k-Divisionsalgebra D und $n \in \mathbb{N}$ mit $Q \underset{k}{\sim} M_n(D)$.
Wegen (1.1) sind nur die beiden folgenden Fälle möglich:

i) $n = 1$, $[D : k] = 4$, also $Q \underset{k}{\cong} M_1(D) \underset{k}{\cong} D$

ii) $n = 2$, $[D : k] = 1$, also $Q \underset{k}{\cong} M_2(D) \underset{k}{\cong} M_2(k)$

(i) und (ii) schließen sich aus, da $M_2(k)$ keine Divisionsalgebra ist. Die Umkehrung folgt sofort aus Satz (1.3).

(1.9) Korollar: Sei k algebraischer Zahlkörper, $\mathfrak{p}$ eine Primstelle von k und Q eine k-Quaternionenalgebra. Dann gilt:

i) Q zerfällt an der Stelle $\mathfrak{p}$ genau dann, wenn $Q_{\mathfrak{p}} \underset{k_{\mathfrak{p}}}{\cong} M_2(k_{\mathfrak{p}})$.

ii) Q ist an der Stelle $\mathfrak{p}$ genau dann verzweigt, wenn $Q_{\mathfrak{p}}$ Divisionsalgebra ist.

Bew.: klar

Für eine Menge M bezeichne $\#M$ die Kardinalzahl von M.

(1.10) Satz: Sei k algebraischer Zahlkörper

i) Sei Q eine k-Quaternionenalgebra. Dann ist die Zahl der Verzweigungsstellen von Q (endlich und) gerade.

ii) Sei M eine endliche Menge von Primstellen von k und sei $\#M$ gerade. Dann gibt es eine k-Quaternionenalgebra Q, deren Verzweigungsstellen genau die Elemente aus M sind.

iii) Seien Q und Q' zwei k-Quaternionenalgebren. Es gilt $Q \underset{k}{\cong} Q'$ genau dann, wenn Q und Q' die gleichen Verzweigungsstellen haben.

Bew.: folgt aus /3/ S.119 Sätze 8 und 9

Aus dem Satz folgt unmittelbar, daß eine Quaternionenalgebra über einem algebraischen Zahlkörper k genau dann zerfällt, wenn sie an allen Primstellen von k zerfällt.

(1.11) Definition: Sei k Körper. Seien X und Y Unbestimmte, sei $F = F(X,Y)$ die durch X und Y erzeugte freie Gruppe, sei $k[F]$ die Gruppenalgebra. Für $a,b \in k^{\times}$ sei $I(a,b)$ das von X^2-a und Y^2-b und $XY + YX$ erzeugte zweiseitige Ideal in $k[F]$. Wir definieren $(a,b)_k := k[F]/I(a,b)$ und fassen k auf natürliche Weise als Unterring von $(a,b)_k$ auf.

Sind $U,V,W \in (a,b)_k$ die Bilder von X,Y,XY unter der Quotientenabbildung, dann sieht man leicht, daß $(a,b)_k$ eine k-Algebra mit Basis $\{1,U,V,W\}$ ist und daß folgende Multiplikationstabelle gilt:

	1	U	V	W
1	1	U	V	W
U	U	a	W	aV
V	V	-W	b	-bU
W	W	-aV	bU	-ab

(1.12)

Diese Multiplikationstabelle ist äquivalent zu den Regeln:

$U^2 = a$, $V^2 = b$, $UV = -VU = W$ (1.13)

(1.14) Lemma: Sei k ein Körper, seien $a,b \in k^\times$, sei Q eine k-Algebra mit $k \subset Q$. Es gilt $Q \tilde{\underset{k}{}} (a,b)_k$ genau dann, wenn es eine Basis $\{1,U,V,W\}$ von Q über k gibt mit der Multiplikationstabelle (1.12).

Bew.: klar

(1.15) Lemma: Sei k Körper und seien $a,b \in k^\times$

i) Seien $c,d \in k^\times$. Dann gilt: $(a,b)_k \tilde{\underset{k}{}} (ac^2,bd^2)_k$

ii) Sei K Erweiterungskörper von k. Dann gilt: $K \otimes_k (a,b)_k \tilde{\underset{K}{}} (a,b)_K$.

Bew.: i) klar (oder siehe /13/ S. 52 Prop. 1.1.1)

ii) klar

(1.16) Lemma: i) Sei k Körper. Dann ist $M_2(k) \tilde{\underset{k}{}} (-1,+1)_k$

ii) Sei $D \supset \mathbb{C}$ Divisionsalgebra über $\mathbb{C}$. Dann ist $D = \mathbb{C}$

iii) Sei $D \neq \mathbb{R}$ eine zentrale Divisionsalgebra über $\mathbb{R}$. Dann ist $D \tilde{\underset{\mathbb{R}}{}} (-1,-1)_{\mathbb{R}}$

Bew.: i) Wir setzen $U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $V = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Die Behauptung kann jetzt leicht nachgerechnet werden. (Der Beweis stammt aus /13/ S.52 Prop. 1.1.4)

ii) Wäre $D \neq \mathbb{C}$, so gäbe es $A \in D - \mathbb{C}$. Dann wäre $\mathbb{C}[A]$ eine (echte) endliche Körpererweiterung von $\mathbb{C}$. ↯

iii) siehe /3/ S.50 Satz 2

(1.17) Satz: Sei k Körper und sei Q eine k-Algebra mit $k \subset Q$. Dann gilt: Q ist genau dann k-Quaternionenalgebra, wenn es $a,b \in k^\times$ gibt mit $Q \tilde{\underset{k}{}} (a,b)_k$.

Bew.: "→": Für $k = \mathbb{R},\mathbb{C}$ folgt die Behauptung leicht aus (1.16), sonst siehe /3/ S. 135 §9.1 (sowie S.112 Satz 2 und S.118 Satz 5)

"←": siehe /13/ S. 52, Prop. 1.1.2 und 1.1.3

(1.18) Definition: Sei k Körper und Q eine k-Quaternionenalgebra. Seien $a,b \in k^\times$ mit $Q \tilde{\underset{k}{}} (a,b)_k$. Sei $\{1,U,V,W\}$ eine Basis von Q über k mit Multiplikationstabelle (1.12). Ist $A = t+uU+vV+wW$ mit $t,u,v,w \in k$, dann heißt $A^* := t-uU-vV-wW$ das zu A konjugierte Quaternion.

$S(A) := A+A^* = 2t$ heißt Spur von A.

$N(A) := AA^* = A^*A = t^2-u^2a-v^2b+w^2ab$ heißt Norm von A.

(1.19) Lemma: Sei k Körper und Q eine k-Quaternionenalgebra. Sei $A \in Q$. Dann ist A Nullstelle des Polynoms $X^2-S(A)X+N(A)$. Falls $A \in Q-k$, ist dieses Polynom das Minimalpolynom von A in $k[X]$. (Für $A \in k$ ist $S(A) = 2A$, $N(A) = A^2$).

Bew.: Es ist $0 = (A - A)(A - A^*) = A^2 - S(A)A + N(A)$.
Für $A \notin k$ muß das Minimalpolynom mindestens den Grad 2 haben, also ist $X^2 - S(A)X + N(A)$ schon Minimalpolynom.

Aus dem Lemma folgt unmittelbar, daß S und N nicht von der speziellen Wahl für a,b,U,V abhängen, sondern nur von k und Q. Wegen $A^* = S(A) - A$ für $A \in Q$ hängt auch die Abbildung * nur von Q und k ab.

(1.20) Lemma: Sei k Körper und Q eine k-Quaternionenalgebra.
i) * und S sind k-Vektorraumhomomorphismen.
ii) Die Fixpunktmenge von $^*: Q \to Q$ ist genau k. Für $A,B \in Q$ gilt:
$(AB)^* = B^*A^*$ und $A^{**} = A$, $S(A^*) = S(A)$, $N(A^*) = N(A)$.
iii) Für $A,B \in Q$ gilt: $N(AB) = N(A)N(B)$. Es ist $A \in Q^\times$ genau dann, wenn $N(A) \in k^\times$; dann ist $A^{-1} = A^* N(A)^{-1}$. Die durch N induzierte Abbildung $N: Q^\times \to k^\times$ ist ein Homomorphismus der multiplikativen Gruppen.

Bew.: direkte Berechnung

(1.21) Bemerkung: Spur und Norm für eine Quaternionenalgebra stimmen mit den für beliebige Algebren definierten Abbildungen Hauptspur und Hauptnorm überein (vgl. /3/ S. 50 - 52, §7). Ferner stimmen sie mit den für halbeinfache Algebren definierten Abbildungen reduzierte Spur und reduzierte Norm überein (vgl. /3/ S. 32/33 §4).

§ 2 . Halbeinfache quadratische Erweiterungen

In §2 werden einfache Sätze über halbeinfache quadratische Erweiterungen zusammengestellt.
Ist k ein Körper und A eine k-Algebra mit $k \subset A$ und $[A : k] = 2$, dann heißt A quadratische Erweiterung von k.

(2.1) Lemma: Sei k ein Körper und A eine quadratische Erweiterung von k. Dann ist A kommutativ. Sei $a \in A-k$. Dann ist $A = k+ka = k[a]$.

Bew.: Sei $a \in A-k$. Sei X Unbestimmte und $P \in k[X]$ Minimalpolynom von a. Wegen $a \notin k$ ist grad $P > 2$, wegen $[A : k] = 2$ ist grad $P < 2$. Also ist $k[X]/Pk[X]$ eine quadratische Erweiterung von k und man prüft leicht nach, daß durch die Vorschrift $X \mapsto a$ ein k-Algebrenisomorphismus $k[X]/Pk[X] \to A$ induziert wird. Jetzt folgen leicht alle Behauptungen.

Ein Element a eines Ringes heißt nilpotent, wenn $a^n = 0$ für ein $n \in \mathbb{N}$.
Ein (Links-, Rechts-, zweiseitiges) Ideal eines Ringes oder einer Algebra heißt Nilideal, wenn es nur nilpotente Elemente enthält. Eine Algebra

heißt halbeinfach, wenn sie außer {0} kein Nilideal enthält.

(2.2) Satz: Sei k Körper und A eine halbeinfache k-Algebra. Dann ist A direkte Summe von eindeutig bestimmten einfachen k-Algebren.

Bew.: siehe / 3/ S. 17 §7 Satz 1

(2.3) Definition: Sei R ein Ring. Ein $e \in R$ mit $e \neq 0$ und $e^2 = e$ heißt R-Idempotent.

(2.4) Lemma: Sei k Körper. Dann ist jede einfache, kommutative k-Algebra ein Körper.

Bew.: siehe /3/ S. 23 Satz 4

(2.5) Korollar: Sei k Körper und K halbeinfache, quadratische Erweiterung von k. Dann ist entweder K quadratischer Erweiterungskörper von k oder es gibt (bis auf die Reihenfolge) eindeutig bestimmte K-Idempotente e_1, e_2 mit $K = ke_1 \oplus ke_2$ (direkte Summe von k-Algebren). Im zweiten Fall ist $e_1 + e_2 = 1$ und $e_1 e_2 = 0$.

Bew.: Wegen $[K : k] = 2$ ist nach (2.2) entweder K einfach oder $K = K_1 \oplus K_2$ mit einfachen k-Algebren K_1, K_2. Da K kommutativ ist, ist nach (2.4) entweder K ein Körper oder $K = K_1 \oplus K_2$ mit Körpern K_1, K_2. Im zweiten Fall enthalten K_1, K_2 (eindeutig bestimmte) Einsen e_1, e_2 und es gilt $e_1 e_2 = 0$. Wegen $[K_1 : k] = [K_2 : k] = 1$ ist $K_1 = ke_1$, $K_2 = ke_2$. Die Behauptung $e_1 + e_2 = 1$ kann man direkt nachrechnen.

(2.6) Satz: Sei k Körper und K halbeinfache, quadratische Erweiterung von k. Dann gibt es genau einen nichttrivialen k-Algebrenautomorphismus * von K. Falls $K = ke_1 \oplus ke_2$ mit K-Idempotenten e_1, e_2 und $A = ae_1 + be_2$ mit $a, b \in k$, dann ist $A^* = be_1 + ae_2$.

Bew.: Falls K Körper ist, ist der Beweis bekannt. Sei also $K = ke_1 \oplus ke_2$ mit K-Idempotenten e_1, e_2. Man kann leicht direkt nachrechnen, daß die angegebene Abbildung * ein k-Algebrenautomorphismus von K ist. Sei umgekehrt σ ein k-Algebrenautomorphismus von K. Dann sind $\sigma(e_1)$ und $\sigma(e_2)$ K-Idempotente und es ist $K = k\sigma(e_1) \oplus k\sigma(e_2)$. Da die K-Idempotente e_1, e_2 eindeutig bestimmt sind, ist entweder $\sigma(e_1) = e_1$, $\sigma(e_2) = e_2$ oder $\sigma(e_1) = e_2$, $\sigma(e_2) = e_1$; also entweder $\sigma = id$ oder $\sigma = {}^*$.

(2.7) Definition: Sei k Körper und K halbeinfache quadratische Erweiterung von k. Sei $A \in K$. Dann heißt $S(A) := A + A^*$ die Spur von A und $N(A) := AA^*$ die Norm von A.

(2.8) Bemerkung: Bemerkung (1.21) überträgt sich auf halbeinfache quadratische Erweiterungen.

(2.9) Lemma: Sei k Körper und K halbeinfache quadratische Erweiterung von k. Sei $A \in K$. Dann ist A Nullstelle des Polynoms $X^2 - S(A)X + N(A)$. Falls $A \in K-k$, ist dieses Polynom das Minimalpolynom von A in $k[X]$. (Für $A \in k$ ist $S(A) = 2A$ und $N(A) = A^2$).

Bew.: wie Lemma (1.19)

(2.10) Korollar: Sei k Körper, Q eine k-Quaternionenalgebra, K eine halbeinfache quadratische Erweiterung von k mit $K \subset Q$.
Dann stimmen die auf K definierten Abbildungen $^*, S, N$ mit den Einschränkungen der auf Q definierten Abbildungen $^*, S, N$ überein.

Bew.: Vergleiche (1.19) mit (2.9)

(2.11) Lemma: Sei k Körper und K halbeinfache quadratische Erweiterung von k. Dann gilt:
i) S ist k-Vektorraumhomomorphismus
ii) Die Fixpunktmenge von $^*: K \to K$ ist genau k. Für $A \in K$ gilt:
$A^{**} = A$, $S(A^*) = S(A)$ und $N(A^*) = N(A)$.
iii) Für $A, B \in K$ gilt: $N(AB) = N(A)N(B)$. Es ist $A \in K^\times$ genau dann, wenn $N(A) \in k^\times$; dann ist $A^{-1} = A^* N(A)^{-1}$. Die durch N induzierte Abbildung $N: K^\times \to k^\times$ ist ein Homomorphismus der multiplikativen Gruppen.

Bew.: Falls K Körper ist, ist der Beweis bekannt. Sonst können die Behauptungen leicht direkt nachgerechnet werden.

(2.12) Korollar: Sei k Körper und K halbeinfache quadratische Erweiterung von k. Sei $A \in K-k$. Die Nullstellen von $X^2 - S(A)X + N(A)$ in K-k sind dann genau A und A^*.

Bew.: A und A^* sind Nullstellen von $X^2 - S(A)X + N(A)$ nach (2.9).
Sei $B \in K-k$ Nullstelle von $X^2 - S(A)X + N(A)$. Dann ist $X^2 - S(A)X + N(A)$ Minimalpolynom von B in $k[X]$. Daher wird durch die Vorschrift $A \mapsto B$ ein k-Algebrenautomorphismus $K = k[A] \to k[B] = K$ induziert.
Nach (2.6) ist $B = A$ oder $B = A^*$.

§ 3 , Vertauschungssatz und Isomorphismensatz

In §3 beweisen wir die Sätze (3.2) und (3.3). Es handelt sich um Verallgemeinerungen bekannter Sätze über einfache, zentrale Algebren.

(3.1) Lemma: Sei k Körper, Q eine k-Quaternionenalgebra. Sei $A \in Q-k$. Dann ist $k[A]$ quadratische Erweiterung von k.

Bew.: siehe Lemma (1.19)

(3.2) Vertauschungssatz: Sei k Körper, Q eine k-Quaternionenalgebra. Seien $A,B \in Q-k$. Dann gilt: $AB = BA$ genau dann, wenn $k[A] = k[B]$.

Bew.: "→": Quadratische Erweiterungen sind kommutativ (2.1)

"←": (direkte Berechnung) Seien $a,b \in k^\times$ mit $Q \cong_k (a,b)_k$.

Sei $\{1,U,V,W\}$ eine Basis von Q über k mit Multiplikationstabelle (1.12).

Sei $A = c + dU + eV + fW$ und $B = C + DU + EV + FW$ mit $c,d,e,f,C,D,E,F \in k$.

c und C liegen im Zentrum von Q; wegen $AB = BA$ ist daher auch

$(A - c)(B - C) = (B - C)(A - c)$. Mit (1.12) erhält man:

$$(A - c)(B - C) = (dU + eV + fW)(DU + EV + FW)$$
$$= dDa + eEb - fFab + (-eF+fE)bU + (dF-fD)aV + (dE-eD)W$$
$$(B - C)(A - c) = (DU + EV + FW)(dU + eV + fW)$$
$$= Dda + Eeb - Ffab + (-Ef+Fe)bU + (Df-Fd)aV + (De - Ed)W$$

Ein Vergleich zeigt: $-eF + fE = dF - fD = dE - eD = 0$

Da $A \notin k$, sind d,e,f nicht alle 0. Sei o.B.d.A. $d \neq 0$ und $\lambda := Dd^{-1}$.

Dann ist $D = \lambda d$, $E = \lambda e$ und $F = \lambda f$.

Wegen $C = (C - \lambda c) + \lambda c$ ist $B = (C - \lambda c) + \lambda A \in k + kA = k[A]$,

also $k[B] \subset k[A]$. Genauso folgt $k[A] \subset k[B]$.

Der Vertauschungssatz ist eine Verallgemeinerung des Satzes, daß quadratische Erweiterungskörper in Quaternionenalgebren maximalkommutativ sind.

(3.3) Isomorphismensatz: Sei k Körper, Q eine k-Quaternionenalgebra. Seien R und R' zwei k-Algebren mit $k \subset R \subset Q$ und $k \subset R' \subset Q$.

Ist $\sigma: R \to R'$ ein k-Algebrenisomorphismus, dann läßt sich σ zu einem k-Algebrenautomorphismus $\sigma: Q \to Q$ fortsetzen.

Es gibt ein $W \in Q^\times$ mit $\sigma(A) = WAW^{-1}$ für $A \in Q$.

(3.4) Korollar: Sei k Körper, Q eine k-Quaternionenalgebra.

Seien $A,A' \in Q-k$ und sei $S(A) = S(A')$ und $N(A) = N(A')$.

Dann gibt es $W \in Q^\times$ mit $A' = WAW^{-1}$.

Der Isomorphismensatz ist (für Quaternionenalgebren) eine Verallgemeinerung des folgenden Satzes:

(3.5) Satz: Sei k Körper, Q eine einfache, zentrale k-Algebra.
Seien R,R' einfache k-Algebren mit $k \subset R \subset Q$ und $k \subset R' \subset Q$.
Ist $\sigma: R \to R'$ ein k-Algebrenisomorphismus, dann läßt sich σ zu einem k-Algebrenautomorphismus $\sigma: Q \to Q$ fortsetzen.
Es gibt $M \in Q^{\times}$ mit $\sigma(A) = MAM^{-1}$ für alle $A \in Q$.
Insbesondere ist jeder k-Algebrenautomorphismus von Q ein innerer Automorphismus.

Bew.: siehe /3/ S. 42 Satz 3

Zur Vorbereitung des Beweises von (3.3) brauchen wir zwei Definitionen und einen Satz.

(3.6) Definition: Sei k Körper, E ein k-Vektorraum und $g: E \times E \to k$ eine Abbildung. g heißt symmetrische Form auf E, wenn g bilinear und symmetrisch ist. g heißt nicht degeneriert, wenn für alle $A \in E$ gilt:
Wenn $g(A,E) = \{0\}$, dann ist $A = 0$.

(3.7) Definition: Sei k Körper. Seien E,E' zwei k-Vektorräume mit symmetrischen Formen g,g'. Ist $\sigma: E \to E'$ ein k-Vektorraumisomorphismus mit $g'(\sigma(A),\sigma(B)) = g(A,B)$ für alle $A,B \in E$, dann heißt σ Isometrie (bezüglich g,g').

(3.8) Satz (Wittsches Theorem): Sei k Körper, E ein k-Vektorraum und g eine nicht degenerierte symmetrische Form auf E.
Seien F,F' zwei k-Untervektorräume von E und sei $\sigma: F \to F'$ eine Isometrie (bezüglich der durch g induzierten symmetrischen Formen auf F,F').
Dann kann σ zu einer Isometrie $\sigma: E \to E$ fortgesetzt werden

Bew.: siehe /14/ S. 360 Theorem 2

Beweis von (3.3): Wir definieren $g(A,B) := S(AB^*) = AB^* + BA^*$ für $A,B \in Q$.
Dann ist g eine symmetrische Form auf Q (siehe 1.20.i).
Seien $a,b \in k^{\times}$ mit $Q \underset{k}{\cong} (a,b)_k$. Sei $\{1,U,V,W\}$ eine Basis von Q über k. mit Multiplikationstabelle (1.12).
Sei $A \in Q$ und $A = c + dU + eV + fW$ mit $c,d,e,f \in k$.
Dann ist $g(A,1) = S(A) = 2c$, $g(A,U) = S(AU^*) = -2da$, $g(A,V) = S(AV^*) = -2eb$ und $g(A,W) = S(AW^*) = 2fab$.
Wenn $g(A,E) = \{0\}$, dann ist $2c = -2da = -2eb = 2fab = 0$, also $A = 0$.
g ist also nicht degeneriert.

Da σ ein k-Algebrenisomorphismus ist, gilt für $A \in R$:
$S(\sigma(A)) = S(A) = \sigma(S(A))$. Daraus folgt:
$\sigma(A)^* = S(\sigma(A)) - \sigma(A) = \sigma(S(A)) - \sigma(A) = \sigma(S(A) - A) = \sigma(A^*)$.
Für $A,B \in R$ gilt daher: $g(\sigma(A),\sigma(B)) = S(\sigma(A)\sigma(B)^*)$

$= S(\sigma(A)\sigma(B^*))$

$= S(\sigma(AB^*))$

$= S(AB^*)$

$= g(A,B)$

σ ist also eine Isometrie (bezüglich der durch g induzierten Formen).
Wegen Satz (3.8) läßt sich σ zu einer Isometrie $\sigma: Q \to Q$ fortsetzen.
Man beachte, daß $\sigma(1) = 1$.
Wir wollen zeigen, daß σ ein k-Algebrenautomorphismus von Q ist.
Daß σ ein innerer Automorphismus ist, folgt dann mit (3.5).
Wegen $\sigma(1) = 1$ müssen wir nur noch zeigen, daß i) $\sigma(U)^2 = a$,
ii) $\sigma(V)^2 = b$ und iii) $\sigma(U)\sigma(V) + \sigma(V)\sigma(U) = 0$ ist.
Für $A \in Q$ gilt: $S(\sigma(A)) = S(\sigma(A)\sigma(1)^*) = g(\sigma(A),\sigma(1)) = g(A,1) = S(A)$
und: $N(\sigma(A)) = \sigma(A)\sigma(A)^* = 1/2 \cdot g(\sigma(A),\sigma(A)) = 1/2 \cdot g(A,A) = N(A)$.
Damit folgen i) und ii).
Wegen $S(U) = S(V) = 0$ folgt außerdem: $\sigma(U)^* = -\sigma(U)$ und $\sigma(V)^* = -\sigma(V)$.
Also gilt: $\sigma(U)\sigma(V) + \sigma(V)\sigma(U) = -(\sigma(U)\sigma(V)^* + \sigma(V)\sigma(U)^*)$

$= -g(\sigma(U),\sigma(V))$

$= -g(U,V)$

$= UV + VU$

$= 0.$

§ 4 . Ordnungen und Ideale in halbeinfachen Algebren

Bei §4 handelt es sich um eine Zusammenstellung bekannter Definitionen und Sätze über Ideale und Ordnungen in halbeinfachen Algebren.
Die Definitionen und Sätze dieses Paragraphen sind allgemein gehalten.
Wir werden sie aber nur für halbeinfache quadratische Erweiterungen und insbesondere für Quaternionenalgebren gebrauchen.
Ist A eine halbeinfache Algebra über dem Körper k, so identifizieren wir die Eins von A mit der Eins von k, d.h. wir fassen k als Unterring von A auf.

(4.1) Definition: Sei k algebraischer Zahlkörper.
i) Den ganzen Abschluß von $\mathbb{Z}$ in k nennen wir die Hauptordnung von k.
ii) Ist $\mathfrak{o}$ die Hauptordnung von k und $\mathfrak{p}$ eine endliche Primstelle von k, dann bezeichne $\mathfrak{o}_\mathfrak{p}$ den Abschluß von $\mathfrak{o}$ in $k_\mathfrak{p}$ bezüglich der $\mathfrak{p}$-adischen Topologie.
Wir nennen $\mathfrak{o}_\mathfrak{p}$ die Hauptordnung von $k_\mathfrak{p}$.

Bekanntlich ist $\mathfrak{o}_\mathfrak{p}$ ganz abgeschlossen in $k_\mathfrak{p}$.

(4.2) Definition: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei A eine halbeinfache k-Algebra. $\mathfrak{O} \subset A$ heißt A-Ordnung, wenn gilt: i) $\mathfrak{O}$ ist Ring

ii) $\mathfrak{o} \subset \mathfrak{O}$

iii) jedes $a \in \mathfrak{O}$ ist ganz über $\mathfrak{o}$

iv) $k\mathfrak{O} = A$, d.h. $\mathfrak{O}$ enthält eine Basis von A über k.

Eine A-Ordnung, die in keiner echt größeren A-Ordnung enthalten ist, heißt A-Maximalordnung.

(4.3) Lemma: Man erhält eine mit (4.2) gleichwertige Definition, wenn man iii) durch folgende Bedingung ersetzt: $\mathfrak{O}$ ist endlich erzeugter $\mathfrak{o}$-Modul.

Bew.: siehe /3/ S. 70/71 Sätze 5 und 9

(4.4) Lemma: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper und A eine halbeinfache k-Algebra. Dann gilt: Es gibt A-Ordnungen und jede A-Ordnung ist in einer A-Maximalordnung enthalten.

Bew.: siehe /3/ S69 und S. 70 Satz 6

(4.5) Satz: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei A halbeinfache kommutative k-Algebra. Dann gibt es genau eine A-Maximalordnung. Sie enthält alle über $\mathfrak{o}$ ganzen Zahlen aus A.

Bew.: siehe /3/ S. 68 Satz 2

(4.6) Definition: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei A halbeinfache k-Algebra und sei $[A : k] = n \in \mathbb{N}$.
i) Seien $u_1, \ldots, u_n \in A$. Dann heißt $D_k(u_1, \ldots, u_n) := \det (S(u_i u_j)_{i,j=1,\ldots,n})$ die Diskriminante von $\{u_1, \ldots, u_n\}$.
ii) Sei $\mathfrak{O}$ eine A-Ordnung. Dann heißt das von allen $D_k(u_1, \ldots, u_n)$ mit $u_1, \ldots, u_n \in \mathfrak{O}$ erzeugte $\mathfrak{o}$-Ideal die Diskriminante von $\mathfrak{O}$ über k.
Sie wird mit $D_k(\mathfrak{O})$ bezeichnet.

(4.7) Lemma : Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper, A eine halbeinfache k-Algebra.
i) Sind $\mathfrak{O}, \mathfrak{O}'$ zwei A-Ordnungen und ist $\mathfrak{O} \subset \mathfrak{O}'$, so ist $D_k(\mathfrak{O}) \subset D_k(\mathfrak{O}')$, also $D_k(\mathfrak{O}') \mid D_k(\mathfrak{O})$.
ii) Sind $\mathfrak{M}, \mathfrak{M}'$ zwei A-Maximalordnungen, so ist $D_k(\mathfrak{M}) = D_k(\mathfrak{M}')$

Bew.: i) klar

ii) siehe /3/ S. 88

(4.8) Definition: Unter den gleichen Voraussetzungen wie in (4.7) sei $\mathfrak{M}$ eine A-Maximalordnung. Dann heißt $D_k(A) := D_k(\mathfrak{M})$ die Diskriminante von A über k.

(4.9) Definition: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper, A eine halbeinfache k-Algebra, $\mathfrak{O}$ eine A-Ordnung. $\mathfrak{A} \subset A$ heißt Rechts- (Links-, zweiseitiges) Ideal von $\mathfrak{O}$, wenn gilt:
i) $\mathfrak{A}$ ist rechts- (links-, zwei-) seitiger $\mathfrak{O}$-Modul
ii) $\mathfrak{A} \cap k \neq \{0\}$
iii) Es gibt $a \in k^\times$ mit $a\mathfrak{A} \subset \mathfrak{O}$

Achtung: Für Ideale von Ordnungen in halbeinfachen quadratischen Erweiterungen werden wir eine andre Definition verwenden (7.2).

Ist $\mathfrak{o}$ die Hauptordnung des Körpers k, dann ist jedes Ideal ein endlich erzeugter $\mathfrak{o}$-Modul. Ist $\mathfrak{A}$ ein Ideal, dann sind $\mathfrak{L} := \{a \in A \mid a\mathfrak{A} \subset \mathfrak{A}\}$ und $\mathfrak{R} := \{a \in A \mid \mathfrak{A}a \subset \mathfrak{A}\}$ A-Ordnungen. $\mathfrak{L}$ heißt Linksordnung, $\mathfrak{R}$ Rechtsordnung von $\mathfrak{A}$. $\mathfrak{A}$ ist dann Linksideal von $\mathfrak{L}$ und Rechtsideal von $\mathfrak{R}$.
Ist $\mathfrak{A} \subset \mathfrak{L}$, dann ist auch $\mathfrak{A} \subset \mathfrak{R}$ (und umgekehrt). In diesem Fall heißt $\mathfrak{A}$ ganz. Ein ganzes gleichseitiges Ideal $\mathfrak{P}$ einer Ordnung $\mathfrak{O}$ heißt Primideal, wenn für alle ganzen gleichseitigen Ideale $\mathfrak{A}, \mathfrak{B}$ von $\mathfrak{O}$ gilt:
$\mathfrak{AB} \subset \mathfrak{P} \Rightarrow (\mathfrak{A} \subset \mathfrak{P}$ oder $\mathfrak{B} \subset \mathfrak{P})$. (siehe hierzu /3/ S. 71)

(4.10) Satz: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper, A eine halbeinfache k-Algebra, $\mathfrak{M}$ eine A-Maximalordnung. Dann gilt:
Die gleichseitigen Ideale von $\mathfrak{M}$ bilden eine freie abelsche (multiplikative) Gruppe mit den Primidealen von $\mathfrak{M}$ als freien Erzeugenden.

Bew.: siehe /3/ S.74 Satz 9

(4.11) Lemma: Sei k algebraischer Zahlkörper, A eine halbeinfache k-Algebra, $\mathfrak{p}$ eine Primstelle von k. Dann ist $A_\mathfrak{p}$ eine halbeinfache $k_\mathfrak{p}$-Algebra.

Bew.: siehe /3/ S.37 §2.3

(4.12) Definition: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$, A eine halbeinfache k-Algebra und $\mathfrak{A} \subset A$ ein $\mathfrak{o}$-Modul. Ist $\mathfrak{p}$ eine endliche Primstelle von k, dann heißt $\mathfrak{A}_\mathfrak{p} := \mathfrak{o}_\mathfrak{p}\mathfrak{A}$ die $\mathfrak{p}$-Komponente von $\mathfrak{A}$.

(4.13) Satz: Unter den gleichen Voraussetzungen wie in (4.12) ist $\mathfrak{A} = A \cap (\bigcap_\mathfrak{p} \mathfrak{A}_\mathfrak{p})$, wobei $\mathfrak{p}$ alle endlichen Primstellen von k durchläuft.

Bew.: siehe /15/ S. 11 Hilfssatz und Fußnote (8)

(4.14) Korollar: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und sei A eine halbeinfache k-Algebra. Dann gilt:
i) Sind $\mathfrak{A},\mathfrak{B} \subset A$ zwei $\mathfrak{o}$-Moduln, dann ist $\mathfrak{A} \subset \mathfrak{B}$ genau dann, wenn $\mathfrak{A}_\mathfrak{p} \subset \mathfrak{B}_\mathfrak{p}$ für alle endlichen Primstellen $\mathfrak{p}$ von k.
ii) Ist $\mathfrak{O}$ eine A-Ordnung, dann ist $\mathfrak{O}_\mathfrak{p}$ eine $A_\mathfrak{p}$-Ordnung für alle endlichen Primstellen $\mathfrak{p}$ von k.
iii) Sind $\mathfrak{A},\mathfrak{B} \subset A$ zwei $\mathfrak{o}$-Moduln, dann gilt für alle endlichen Primstellen $\mathfrak{p}$ von k: $\mathfrak{A}_\mathfrak{p}\,\mathfrak{B}_\mathfrak{p} = (\mathfrak{A}\mathfrak{B})_\mathfrak{p}$
iv) Ist $\mathfrak{A}$ ein Rechts- (Links-, zweiseitiges) Ideal der A-Ordnung $\mathfrak{O}$, dann ist $\mathfrak{A}_\mathfrak{p}$ ein Rechts- (Links- , zweiseitiges) Ideal von $\mathfrak{O}_\mathfrak{p}$ für alle endlichen Primstellen $\mathfrak{p}$ von k.

Bew.: i) folgt sofort aus (Def. 4.12 und) Satz (4.13)
ii),iii),iv) folgen leicht aus den Definitionen (man beachte Lemma 4.3).

(4.15) Lemma: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei A halbeinfache k-Algebra und seien $\mathfrak{A},\mathfrak{B}$ Ideale in A. Dann gilt:
i) Für jedes $E \in A$ gibt es $a \in k^\times$ mit $aE \in \mathfrak{A}$.
ii) Es gibt $a \in k^\times$ mit $a\mathfrak{B} \subset \mathfrak{A}$
iii) Ist k algebraischer Zahlkörper, so ist $\mathfrak{A}_\mathfrak{p} = \mathfrak{B}_\mathfrak{p}$ für fast alle endlichen Primstellen $\mathfrak{p}$ von k.

Bew.: i) $\mathfrak{A}$ enthält eine Basis $\{A_1,\ldots,A_n\}$ von A über k (4.9.i,ii). Sei $E = a_1A_1 + \ldots + a_nA_n$ mit $a_i \in k$ für $i = 1,\ldots,n$. Es gibt $a \in k^\times$ mit $aa_i \in \mathfrak{o}$ für $i = 1,\ldots,n$. Dann ist $aE \in \mathfrak{A}$.
ii) Sei $\{B_1,\ldots,B_n\}$ ein Erzeugendensystem von $\mathfrak{B}$ als $\mathfrak{o}$-Modul. Es gibt $a_1,\ldots,a_n \in k^\times$ mit $a_iB_i \in \mathfrak{A}$ für $i = 1,\ldots,n$. Sei a gemeinsames Vielfaches aller a_i. Dann ist $a\mathfrak{B} \subset \mathfrak{A}$.
iii) Es gibt $a,b \in k^\times$ mit $a\mathfrak{B} \subset \mathfrak{A}, b\mathfrak{A} \subset \mathfrak{B}$. Für fast alle endlichen Primstellen von k sind $a,b \in \mathfrak{o}_\mathfrak{p}^\times$, also $\mathfrak{A}_\mathfrak{p} \subset \mathfrak{B}_\mathfrak{p}$ und $\mathfrak{B}_\mathfrak{p} \subset \mathfrak{A}_\mathfrak{p}$

(4.16) Korollar: Sei k algebraischer Zahlkörper, A eine halbeinfache k-Algebra und $\mathfrak{M}$ eine A-Ordnung. Dann gilt: $\mathfrak{M}$ ist A-Maximalordnung genau dann, wenn $\mathfrak{M}_\mathfrak{p}$ eine A -Maximalordnung ist für alle endlichen Primstellen $\mathfrak{p}$ von k.

Bew.: Sei $\mathfrak{o}$ die Hauptordnung von k.
i) Sei $\mathfrak{M}$ eine A-Maximalordnung und $\mathfrak{p}$ eine endliche Primstelle von k. Sei $\mathfrak{M}'$ eine A -Ordnung mit $\mathfrak{M}' \supset \mathfrak{M}_\mathfrak{p}$. Nach (4.15.ii) gibt es $a \in k^\times$ mit $a\mathfrak{M}' \subset \mathfrak{M}_\mathfrak{p}$. Wir können annehmen, daß $a \in \mathfrak{o}$.

Sei $\mathfrak{M}' := \Lambda \cap \mathfrak{M}'_{\mathfrak{p}} \cap (\bigcap_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{M}_{\mathfrak{q}})$, wobei $\mathfrak{q}$ alle endlichen Primstellen $\neq \mathfrak{p}$ von k durchläuft. Dann ist $a\mathfrak{M}' \subset \mathfrak{M}$. Daher ist $\mathfrak{M}'$ ein zweiseitiges Ideal von $\mathfrak{M}$ und insbesondere ein endlich erzeugter $\mathfrak{o}$-Modul. Jetzt folgt sofort, daß $\mathfrak{M}'$ eine A-Ordnung ist. Da $\mathfrak{M}' \supset \mathfrak{M}$, ist nach Voraussetzung $\mathfrak{M}' = \mathfrak{M}$ und insbesondere $\mathfrak{M}'_{\mathfrak{p}} = \mathfrak{M}_{\mathfrak{p}}$. Wir müssen noch zeigen: $\mathfrak{M}'^{\mathfrak{p}} \subset \mathfrak{M}'_{\mathfrak{p}}$.
Da $\mathfrak{M}'$ eine Basis von A über k enthält, ist $A_{\mathfrak{p}} = \mathfrak{M}'_{\mathfrak{p}} + A$.
Sei $E \in \mathfrak{M}'^{\mathfrak{p}}$. Wegen $\mathfrak{M}'_{\mathfrak{p}} \subset \mathfrak{M}'^{\mathfrak{p}}$ gibt es also $E' \in \mathfrak{M}'_{\mathfrak{p}}$, $E'' \in \mathfrak{M}'^{\mathfrak{p}} \cap A$, so daß $E = E' + E''$. Es gibt ein $a \in \mathfrak{o} - \{0\}$, so daß $aE'' \in \mathfrak{M}'$, also ein $a' \in \mathfrak{o} \cap \mathfrak{o}_{\mathfrak{p}}^{\times}$, so daß $a'E'' \in A \cap \bigcap_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{M}'_{\mathfrak{q}}$. Dann ist $a'E'' \in A \cap \mathfrak{M}'^{\mathfrak{p}} \cap (\bigcap_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{M}'_{\mathfrak{q}}) = \mathfrak{M}' \subset \mathfrak{M}'_{\mathfrak{p}}$ und wegen $a' \in \mathfrak{o}_{\mathfrak{p}}^{\times}$ auch $E'' \in \mathfrak{M}'_{\mathfrak{p}}$ und $E = E' + E'' \in \mathfrak{M}'_{\mathfrak{p}}$.
ii) Sei $\mathfrak{M}_{\mathfrak{p}}$ Maximalordnung für alle endlichen Primstellen $\mathfrak{p}$ von k. Sei $\mathfrak{M}'$ eine A-Ordnung mit $\mathfrak{M} \subset \mathfrak{M}'$. Nach (4.14.i) ist $\mathfrak{M}_{\mathfrak{p}} \subset \mathfrak{M}'_{\mathfrak{p}}$ für alle $\mathfrak{p}$. Nach Vorraussetzung ist also $\mathfrak{M}_{\mathfrak{p}} = \mathfrak{M}'_{\mathfrak{p}}$ für alle $\mathfrak{p}$; mit (4.13) folgt $\mathfrak{M} = \mathfrak{M}'$.

(4.17) Lemma: Sei k algebraischer Zahlkörper, A eine halbeinfache k-Algebra und $\mathfrak{p}$ eine endliche Primstelle von k. Dann gilt:
i) Ist $\mathfrak{O}$ eine Λ-Ordnung, dann ist $D_k(\mathfrak{O})_{\mathfrak{p}} = D_{k_{\mathfrak{p}}}(\mathfrak{O}_{\mathfrak{p}})$.
ii) $D_k(A)_{\mathfrak{p}} = D_{k_{\mathfrak{p}}}(A_{\mathfrak{p}})$.

Bew.: i) folgt leicht aus den Definitionen
ii) folgt wegen (4.16) sofort aus i)

Bemerkung: (4.16) ist wohlbekannt. Ich habe nur deshalb einen Beweis angegeben, weil er in der mir bekannten Literatur (etwa /3/) nicht explizit formuliert und bewiesen ist.

§ 5. Einbettung von halbeinfachen quadratischen Erweiterungen in Quaternionenalgebren

Wesentliches Ergebnis von §5 ist Satz (5.6), der beschreibt, welche halbeinfachen quadratischen Erweiterungen K eines algebraischen Zahlkörpers k in eine vorgegebene k-Quaternionenalgebra eingebettet werden können. Der Satz ist im wesentlichen bekannt.
Um ihn exakt formulieren zu können, untersuchen wir zu Beginn die Hauptordnung einer halbeinfachen quadratischen Erweiterung $K = ke_1 \oplus ke_2$.

(5.1) Definition: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper und sei K eine halbeinfache quadratische Erweiterung von k. Dann nennen wir die Maximalordnung in K Hauptordnung von K.

Die Hauptordnung von K ist wohldefiniert wegen Satz (4.5).
Falls K Körper ist, stimmt (5.1) mit Definition (4.1) überein.

Ist k algebraischer Zahlkörper und $\mathcal{O}$ die Hauptordnung von K, dann ist $\mathcal{O}_\mathfrak{p}$ die Hauptordnung von $K_\mathfrak{p}$ für alle endlichen Primstellen $\mathfrak{p}$ von k (4.16).

(5.2) Satz: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei K halbeinfache quadratische Erweiterung von k, $K = ke_1 \oplus ke_2$ mit K-Idempotenten e_1, e_2. Sei $\mathcal{O}$ die Hauptordnung von K. Dann gilt:

i) $\mathcal{O} = \mathfrak{o}e_1 + \mathfrak{o}e_2$

ii) $D_k(K) = D_k(\mathcal{O}) = \mathfrak{o}$

iii) Ist $\mathfrak{p}$ ein Primideal von $\mathfrak{o}$, dann ist $\mathfrak{p}\mathcal{O} = \mathfrak{q}_1\mathfrak{q}_2$, wobei $\mathfrak{q}_1 = \mathfrak{p}e_1 + \mathfrak{o}e_2$ und $\mathfrak{q}_2 = \mathfrak{o}e_1 + \mathfrak{p}e_2$ Primideale von $\mathcal{O}$ sind. Alle Primideale von $\mathcal{O}$ sind von der Gestalt $\mathfrak{q}_1$ oder $\mathfrak{q}_2$; sie sind freie Erzeugende der freien abelschen Gruppe der Ideale von $\mathcal{O}$.

iv) Falls k $\mathfrak{p}$-adischer Zahlkörper ist, sind alle Ideale von $\mathcal{O}$ Hauptideale.

Bew.: i) Sei $A = ae_1 + be_2$ mit $a,b \in \mathfrak{o}$. Dann ist $S(A) = a + b \in \mathfrak{o}$ und $N(A) = ab \in \mathfrak{o}$, also $A \in \mathcal{O}$. Sei umgekehrt $A \in \mathcal{O}$, $A = ae_1 + be_2$ mit $a,b \in k$. Wegen $e_1, e_2 \in \mathcal{O}$ ist dann $a = S(ae_1) = S(Ae_1) \in \mathfrak{o}$ und $b = S(Ae_2) \in \mathfrak{o}$.

ii) Da $\{e_1, e_2\}$ eine $\mathfrak{o}$-Basis von $\mathcal{O}$ ist, ist $D_k(K) = D_k(\mathcal{O}) = D_k(e_1, e_2)\,\mathfrak{o}$

$$D_k(e_1, e_2) = \det \begin{pmatrix} S(e_1e_1) & S(e_1e_2) \\ S(e_2e_1) & S(e_2e_2) \end{pmatrix} = \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$$

iii) Direkte Rechnung zeigt: $\mathfrak{p}\mathcal{O} = \mathfrak{q}_1\mathfrak{q}_2$

Da $\mathcal{O}/\mathfrak{q}_1 = (\mathfrak{o}e_1 + \mathfrak{o}e_2)/(\mathfrak{p}e_1 + \mathfrak{o}e_2) \cong \mathfrak{o}/\mathfrak{p}$ Integritätsbereich ist, folgt leicht, daß $\mathfrak{q}_1$ Primideal ist. Genauso ist $\mathfrak{q}_2$ Primideal.

Ist $\mathfrak{q}$ ein Primideal von $\mathcal{O}$, so ist $\mathcal{O}/\mathfrak{q}$ Integritätsbereich. Wegen $\mathfrak{o} \subset \mathcal{O}$ muß auch $\mathfrak{o}/\mathfrak{o}\cap\mathfrak{q}$ Integritätsbereich sein, d.h. $\mathfrak{p} := \mathfrak{o}\cap\mathfrak{q}$ ist Primideal von $\mathfrak{o}$. Es ist $\mathfrak{q} \supset \mathfrak{p}\mathcal{O}$ und $\mathfrak{p}\mathcal{O}$ faktorisiert nach Satz (4.10) eindeutig in $\mathfrak{q}_1\mathfrak{q}_2$. Also ist $\mathfrak{q}_1 = \mathfrak{q}$ oder $\mathfrak{q}_2 = \mathfrak{q}$. Die letzte Behauptung ist Satz (4.10).

iv) Aus iii) folgt, daß jedes Ideal $\mathcal{A}$ von $\mathcal{O}$ von der Gestalt $\mathcal{A} = \mathfrak{a}e_1 + \mathfrak{b}e_2$ ist, wo $\mathfrak{a}, \mathfrak{b}$ Ideale von $\mathfrak{o}$ sind. Da $\mathfrak{o}$ Hauptidealring ist, gibt es $a,b \in \mathfrak{o}$ mit $\mathfrak{a} = a\mathfrak{o}$, $\mathfrak{b} = b\mathfrak{o}$, also $\mathcal{A} = (ae_1 + be_2)\mathcal{O}$.

Wegen iii) sagen wir in Anlehnung an die entsprechenden Begriffe bei quadratischen Körpererweiterungen, daß die Primideale (endliche Primstellen) von k in $K = ke_1 \oplus ke_2$ zerlegt, nicht verzweigt und nicht träge sind. Ist $\mathfrak{p}$ eine unendliche Primstelle des algebraischen Zahlkörpers k und $K = ke_1 \oplus ke_2$, so ist $K_\mathfrak{p} = k_\mathfrak{p}e_1 + k_\mathfrak{p}e_2$ kein Körper. Deshalb sagen wir wie bei quadratischen Körpererweiterungen: $\mathfrak{p}$ ist zerlegt und nicht verzweigt.

(5.3) Definition: Sind $k \subset K$ algebraische Zahlkörper und ist $\mathfrak{q}$ eine Primstelle von K, dann bezeichnen wir den Trägheits- bzw. Verzweigungsgrad von $\mathfrak{q}$ über k mit $t_k(\mathfrak{q})$ bzw. $v_k(\mathfrak{q})$. Wir kürzen außerdem $t(\mathfrak{q}) := t_\mathbb{Q}(\mathfrak{q})$, $v(\mathfrak{q}) := v_\mathbb{Q}(\mathfrak{q})$ ab.

Ist $\mathfrak{q}$ die Fortsetzung der Primstelle $\mathfrak{p}$ von k, dann ist bekanntlich $[K_{\mathfrak{q}} : k_{\mathfrak{p}}] = t_k(\mathfrak{q}) v_k(\mathfrak{q})$.

(5.4) Lemma: Seien $k \subset K$ algebraische Zahlkörper und sei Q eine k-Quaternionenalgebra

i) Seien $\mathfrak{p}, \mathfrak{q}$ Primstellen von k,K. Sei $\mathfrak{q}$ Fortsetzung von $\mathfrak{p}$.
$\mathfrak{q}$ ist genau dann Verzweigungsstelle von $Q \otimes_k K$, wenn $\mathfrak{p}$ Verzweigungsstelle von Q über k ist und $[K_{\mathfrak{q}} : k_{\mathfrak{p}}]$ ungerade ist.

ii) K ist genau dann Zerfällungskörper von Q, wenn für alle Verzweigungsstellen $\mathfrak{p}$ von Q über k gilt: Ist $\mathfrak{q}$ eine Fortsetzung von $\mathfrak{p}$ auf K, dann ist $[K_{\mathfrak{q}} : k_{\mathfrak{p}}]$ gerade.

Bew.: i) siehe /3/ S. 113 Satz 4

ii) Nach (1.10.iii) zerfällt $Q \otimes_k K$ genau dann, wenn $Q \otimes_k K$ an allen Primstellen $\mathfrak{q}$ von K zerfällt. Jetzt folgt die Beh. sofort aus i).

(5.5) Lemma: Sei k Körper, K quadratischer Erweiterungskörper von k und Q eine k-Quaternionenalgebra. Dann gilt:

i) Wenn $k \subset K \subset Q$, dann ist K Zerfällungskörper von Q.

ii) Wenn K Zerfällungskörper von Q ist, gibt es $K' \tilde{}_k K$ mit $k \subset K' \subset Q$.

Anders ausgedrückt: Die über k quadratischen Zerfällungskörper von Q stimmen bis auf Isomorphie mit den maximalen Erweiterungskörpern von k in Q überein (3.2).

Bew.: siehe /3/ S. 46/47 Sätze 13 und 17

(5.6) Satz: Sei k algebraischer Zahlkörper, K halbeinfache quadratische Erweiterung von k und Q eine k-Quaternionenalgebra. Genau dann gibt es $K' \tilde{}_k K$ mit $k \subset K' \subset Q$, wenn alle Verzweigungsstellen von Q über k in K träge oder verzweigt sind.

Bew.: Falls K Körper ist, folgt die Behauptung sofort aus den Lemmata (5.4.ii), (5.5).
Sei also $K = ke_1 \oplus ke_2$ mit K-Idempotenten e_1, e_2.
Ist $K' \tilde{}_k K$ mit $k \subset K' \subset Q$, dann enthält K' Nullteiler; Q ist also keine Divisionsalgebra, d.h. $Q \tilde{}_k M_2(k)$ (1.8). Q hat dann keine Verzweigungsstellen.
Sind umgekehrt alle Verzweigungsstellen von Q über k in K träge oder verzweigt, so kann Q keine Verzweigungsstellen haben, da alle Primstellen von k in K zerlegt sind. Also ist o.B.d.A. $Q = M_2(k)$.
Eine Einbettung von K in Q erhält man dann durch die Vorschrift:
$e_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ und $e_2 \mapsto \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

§ 6 . Ordnungen in halbeinfachen, quadratischen Erweiterungen

Das Hauptergebnis von §6 ist Satz (6.8), der die Ordnungen einer halbeinfachen, quadratischen Erweiterung K nach ihren $\mathfrak{o}$-Führern klassifiziert (Def. 6.1). Falls man sich auf Körper K beschränkt, folgen die Sätze dieses Paragrafen relativ leicht aus /16/ §4. Da wir aber auch den Fall betrachten müssen, daß K kein Körper ist, habe ich die Gelegenheit benutzt, um die Ergebnisse in eine Form zu bringen, die mir für diese Arbeit insgesamt geeigneter erschien.

(6.1) Definition: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und sei K eine halbeinfache quadratische Erweiterung von k mit Hauptordnung $\mathfrak{O}_0$ Sei $\mathfrak{O}$ eine K-Ordnung.
Dann heißt $f(\mathfrak{O}) := \{a \in \mathfrak{o} \mid a\mathfrak{O}_0 \subset \mathfrak{O}\}$ der $\mathfrak{o}$-Führer von $\mathfrak{O}$.

Man beachte, daß wir entsprechend Definition (4.2) stets $\mathfrak{o} \subset \mathfrak{O}$ voraussetzen. $f(\mathfrak{O})$ ist der Durchschnitt von $\mathfrak{o}$ mit dem Führer von $\mathfrak{O}$ in $\mathfrak{O}_0$.

(6.2) Lemma: Unter den Voraussetzungen von (6.1) ist $f(\mathfrak{O}) \neq \{0\}$.
$f(\mathfrak{O})$ ist ein ganzes $\mathfrak{o}$-Ideal. $f(\mathfrak{O})\mathfrak{O}_0 \subset \mathfrak{O}$.
$f(\mathfrak{O})$ ist das größte unter den $\mathfrak{o}$-Idealen $\mathfrak{a}$, für die $\mathfrak{a}\mathfrak{O}_0 \subset \mathfrak{O}$.

Bew.: $f(\mathfrak{O}) \neq \{0\}$ folgt aus Lemma (4.15.ii). Die übrigen Behauptungen sind unmittelbar klar.

(6.3) Lemma: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei K halbeinfache quadratische Erweiterung von k. Sei $\mathfrak{O}$ eine K-Ordnung. Sei $\mathfrak{p}$ eine endliche Primstelle von k. Dann gilt: $f(\mathfrak{O})_\mathfrak{p} = f(\mathfrak{O}_\mathfrak{p})$.
(Dabei bezeichne f jeweils den $\mathfrak{o}$-Führer bzw. den $\mathfrak{o}_\mathfrak{p}$-Führer.)

Bew.: Sei $\mathfrak{O}_0$ die Hauptordnung von K. Dann ist $\mathfrak{o}_\mathfrak{p}$ die Hauptordnung von k und $\mathfrak{O}_{0\mathfrak{p}}$ die Hauptordnung von $K_\mathfrak{p}$ (4.16). Wegen $f(\mathfrak{O})\mathfrak{O}_0 \subset \mathfrak{O}$ ist $f(\mathfrak{O})_\mathfrak{p}\mathfrak{O}_{0\mathfrak{p}} \subset \mathfrak{O}_\mathfrak{p}$ (4.14). Sei $\mathfrak{a}^\mathfrak{p}$ ein $\mathfrak{o}_\mathfrak{p}$-Ideal mit $f(\mathfrak{O})_\mathfrak{p} \subset \mathfrak{a}^\mathfrak{p}$ und $\mathfrak{a}^\mathfrak{p}\mathfrak{O}_{0\mathfrak{p}} \subset \mathfrak{O}_\mathfrak{p}$. Durch die Vorschriften $\mathfrak{a}_\mathfrak{p} := \mathfrak{a}^\mathfrak{p}$ und $\mathfrak{a}_\mathfrak{q} := f(\mathfrak{O})_\mathfrak{q}$ für alle endlichen Primstellen $\mathfrak{q} \neq \mathfrak{p}$ von k wird ein $\mathfrak{o}$-Ideal $\mathfrak{a}$ definiert mit $f(\mathfrak{O}) \subset \mathfrak{a}$ und $\mathfrak{a}\mathfrak{O}_0 \subset \mathfrak{O}$ (4.14). Wegen der Maximalitätseigenschaft (6.2) von $f(\mathfrak{O})$ ist $\mathfrak{a} = f(\mathfrak{O})$ und insbesondere $\mathfrak{a}^\mathfrak{p} = \mathfrak{a}_\mathfrak{p} = f(\mathfrak{O})_\mathfrak{p}$. Daraus folgt, daß $f(\mathfrak{O})_\mathfrak{p}$ die Maximalitätseigenschaft (6.2) hat, also $f(\mathfrak{O})_\mathfrak{p} = f(\mathfrak{O}_\mathfrak{p})$.

(6.4) Lemma: Sei R Integritätsbereich und Hauptidealring. Sei F endlich erzeugter, torsionsfreier R-Modul. Dann ist F freier R-Modul

Bew.: folgt aus /14/ S. 388 Theorem 2

(6.5) Lemma: Sei R Integritätsbereich und Hauptidealring. Sei F ein freier R-Modul und $G \neq \{0\}$ ein endlich erzeugter Untermodul. Dann gibt es eine Basis B von F, eine endliche Teilmenge $\{b_1,\ldots,b_r\} \subset B$, sowie $a_1,\ldots,a_r \in R-\{0\}$, so daß $\{a_1b_1,\ldots,a_rb_r\}$ eine Basis von G über R ist.
Bew.: siehe /14/ S.393 Theorem 5.i

(6.6) Lemma: Sei k ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und sei K eine halbeinfache quadratische Erweiterung von k mit Hauptordnung $\mathfrak{O}$. Dann gibt es $\omega \in \mathfrak{O}$, so daß $\{1,\omega\}$ eine Basis von $\mathfrak{O}$ über $\mathfrak{o}$ ist.

Bew.: $\mathfrak{o}$ ist Integritätsbereich und Hauptidealring. $\mathfrak{O}$ ist torsionsfreier $\mathfrak{o}$-Modul und endlich erzeugt (4.3), also freier $\mathfrak{o}$-Modul (6.4). $\mathfrak{o}$ ist endlich erzeugter $\mathfrak{o}$-Untermodul von $\mathfrak{O}$. Jede Basis von $\mathfrak{o}$ über $\mathfrak{o}$ hat genau ein Element. Nach Lemma (6.5) gibt es eine Basis B von $\mathfrak{O}$ über $\mathfrak{o}$, $b \in B$ und $a \in \mathfrak{o}-\{0\}$, so daß $\{ab\}$ eine Basis von $\mathfrak{o}$ über $\mathfrak{o}$ ist. Wegen $1 \in \mathfrak{o}$ gibt es $c \in \mathfrak{o}$ mit $1 = cab$. Wegen $ca \in k$ folgt $b \in k$. Wegen $b \in \mathfrak{O}$ ist also $b \in \mathfrak{O} \cap k = \mathfrak{o}$. Wegen $ca \in \mathfrak{o}$ ist sogar $b \in \mathfrak{o}^\times$. B bleibt daher Basis von $\mathfrak{O}$ über $\mathfrak{o}$, wenn wir b durch 1 ersetzen. Aus $[K : k] = 2$ folgt leicht, daß B genau 2 Elemente enthalten muß. Es gibt also $\omega \in \mathfrak{O}$ mit $B = \{1,\omega\}$.

(6.7) Satz: Sei k ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei π ein Primelement von $\mathfrak{o}$. Sei K eine halbeinfache quadratische Erweiterung von k mit Hauptordnung $\mathfrak{O}_0$ und sei $\{1,\omega\}$ eine Basis von $\mathfrak{O}_0$ über $\mathfrak{o}$. Dann gilt:
i) Für jedes $r \in \mathbb{N}_0$ ist der $\mathfrak{o}$-Modul $\mathfrak{O}$ mit Basis $\{1,\pi^r\omega\}$ eine K-Ordnung.
ii) Ist umgekehrt $\mathfrak{O}$ eine k-Ordnung, dann gibt es ein eindeutig bestimmtes $r \in \mathbb{N}_0$, so daß $\{1,\pi^r\omega\}$ eine Basis von $\mathfrak{O}$ über $\mathfrak{o}$ ist. Darüberhinaus gilt:
   a) $r = \min\{s \in \mathbb{N}_0 \mid \pi^s\omega \in \mathfrak{O}\}$
   b) $\mathfrak{O} = \mathfrak{o} + \pi^r\mathfrak{O}_0$
   c) $f(\mathfrak{O}) = \pi^r\mathfrak{o}$
   d) $D_k(\mathfrak{O}) = \pi^{2r}D_k(K)$

Bew.: i) Wegen $1 \in \mathfrak{O}$ ist $\mathfrak{o} \subset \mathfrak{O}$. Daß $\mathfrak{O}$ multiplikativ abgeschlossen ist, läßt sich leicht direkt nachrechnen. Die anderen Behauptungen (4.2) sind offensichtlich.
ii) Für $r \in \mathbb{N}_0$ ist $\pi^{r-1}\omega$ nicht in dem $\mathfrak{o}$-Modul mit Basis $\{1,\pi^r\omega\}$ enthalten; denn da $\{1,\pi^r\omega\}$ auch eine Basis von K über k ist, ist $\pi^{r-1}\omega = 0\cdot 1 + \pi^{-1}\cdot\pi^r\omega$ die einzige Darstellung von $\pi^{r-1}\omega$ als Linearkombination von 1 und $\pi^r\omega$ mit Koeffizienten aus k; und es ist $\pi^{-1} \notin \mathfrak{o}$. Daher ist r, falls es existiert, eindeutig.

Nach Lemma (4.15) gibt es $a \in k^*$ mit $a\mathcal{O}_0 \subset \mathcal{O}$. Es ist sicher $a \in \mathcal{O}$, also gibt es $b \in \mathcal{O}^\times$ und $s \in \mathbb{N}_0$ mit $a = b\pi^s$. Wegen $\mathcal{O}^\times \subset \mathcal{O}$ ist auch $\pi^s\mathcal{O}_0 \subset \mathcal{O}$.
Sei $r := \min \{s \in \mathbb{N}_0 \mid \pi^s\mathcal{O}_0 \subset \mathcal{O}\}$.
Jedes ganze $\mathcal{O}$-Ideal ist von der Form $\pi^s\mathcal{O}$. Wegen der Maximalitätseigenschaft (6.2) des $\mathcal{O}$-Führers ist $f(\mathcal{O}) = \pi^r\mathcal{O}$.
Für $s \in \mathbb{N}_0$ ist $\pi^s\mathcal{O}_0 \subset \mathcal{O}$ gleichwertig mit: $\pi^s \cdot 1 \in \mathcal{O}$ und $\pi^s\omega \in \mathcal{O}$;
wegen $\pi^s \in \mathcal{O} \subset \mathcal{O}$ also gleichwertig mit $\pi^s\omega \in \mathcal{O}$.
Es gilt $\mathcal{O} + \mathcal{O}\pi^r\omega \subset \mathcal{O}$. Sei umgekehrt $A \in \mathcal{O}$. Wegen $\mathcal{O} \subset \mathcal{O}_0$ gibt es $a,b \in \mathcal{O}$ mit $A = a + b\omega$. Wegen $a \in \mathcal{O} \subset \mathcal{O}$ ist dann $b\omega \in \mathcal{O}$. Sei o.B.d.A. $b \neq 0$ und sei $b = c\pi^s$ mit $c \in \mathcal{O}^\times$ und $s \in \mathbb{N}_0$. Dann ist auch $\pi^s\omega = c^{-1}b\omega \in \mathcal{O}$, nach Definition also $s \geq r$ und $A = a + c\pi^s\omega \in \mathcal{O} + \mathcal{O}\pi^r\omega$.
Damit ist die Existenz von r sowie a),c) gezeigt.
zu b): $\mathcal{O} + \pi^r\mathcal{O}_0 = \mathcal{O} + \pi^r\mathcal{O} + \pi^r\mathcal{O}\omega = \mathcal{O} + \mathcal{O}\pi^r\omega = \mathcal{O}$
zu d): $\{1,\omega\}$ bzw. $\{1,\pi^r\omega\}$ sind Basen von $\mathcal{O}_0$ bzw. $\mathcal{O}$ über $\mathcal{O}$. Daher:
$D_k(\mathcal{O}) = D_k(1,\pi^r\omega)\mathcal{O} = \pi^{2r}D_k(1,\omega)\mathcal{O} = \pi^{2r}D_k(\mathcal{O}_0) = \pi^{2r}D_k(K)$

(6.8) Satz: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathcal{O}$.
Sei K halbeinfache quadratische Erweiterung von k mit Hauptordnung $\mathcal{O}_0$.
Dann ist die Abbildung

$$f : \{\mathcal{O} \mid \mathcal{O} \text{ ist K-Ordnung}\} \to \{\mathfrak{f} \mid \mathfrak{f} \text{ ist ganzes } \mathcal{O}\text{-Ideal}\}$$
$$\mathcal{O} \to f(\mathcal{O}) \qquad \text{bijektiv.}$$

Die Umkehrabbildung wird gegeben durch: $\mathfrak{f} \to \mathcal{O} + \mathfrak{f}\mathcal{O}_0$.

Bew.: Für $\mathfrak{p}$-adische Zahlkörper ist die Behauptung in (6.7) enthalten.
Für algebraische Zahlkörper folgt sie jetzt leicht mit (6.3).

(6.9) Korollar: Die Voraussetzungen seien die gleichen wie in (6.8).
i) Sei $\mathcal{O}$ eine K-Ordnung. Dann ist $D_k(\mathcal{O}) = f(\mathcal{O})^2D_k(K)$
ii) Seien $\mathcal{O},\mathcal{O}'$ zwei K-Ordnungen. Dann gilt: $\mathcal{O} \subset \mathcal{O}' \Leftrightarrow f(\mathcal{O}') \mid f(\mathcal{O}) \Leftrightarrow D_k(\mathcal{O}') \mid D_k(\mathcal{O})$
iii) Sei $E \in \mathcal{O}_0 - \mathcal{O}$. Dann ist $\mathcal{O}[E] = \mathcal{O} + \mathcal{O}E$ die kleinste K-Ordnung, die E enthält. Es ist $D_k(\mathcal{O}[E]) = D_k(1,E)\mathcal{O}$. Sei $\mathcal{O}$ eine K-Ordnung. Es ist $E \in \mathcal{O}$ genau dann, wenn $D_k(\mathcal{O}) \mid D_k(1,E)\mathcal{O}$ und genau dann, wenn $f(\mathcal{O}) \mid f(\mathcal{O}[E])$.
iv) Sei $E \in \mathcal{O}_0$. Dann ist $D_k(1,E) = (E - E^*)^2 = S(E)^2 - 4N(E)$.

Bew.: i) Für $\mathfrak{p}$-adische Zahlkörper ist das (6.7d). Für algebraische Zahlkörper folgt die Behauptung jetzt mit (4.17).
ii) klar
iii) klar
iv) $D_k(1,E) = \det \begin{pmatrix} S(1) & S(E) \\ S(E) & S(E^2) \end{pmatrix} = 2S(E^2) - S(E)^2$.
Es ist $S(E^2) = E^2 + E^{*2} = (E + E^*)^2 - 2EE^* = S(E)^2 - 2N(E)$,
also $D_k(1,E) = S(E)^2 - 4N(E) = E^2 + 2EE^* + E^{*2} - 4EE^* = (E - E^*)^2$.

(6.10) Definition: Die Voraussetzungen seien die gleichen wie in (6.8). Dann setzen wir $\mathcal{O}^{\mathfrak{f}}(K) := \mathfrak{o} + \mathfrak{f}\mathcal{O}_0$ für ganze $\mathfrak{o}$-Ideale $\mathfrak{f}$.

Wir werden oft $\mathcal{O}^{\mathfrak{f}} := \mathcal{O}^{\mathfrak{f}}(K)$ abkürzen. $\mathcal{O}^{\mathfrak{o}}$ ist dann die Hauptordnung von K und allgemein ist $f(\mathcal{O}^{\mathfrak{f}}) = \mathfrak{f}$ für ganze $\mathfrak{o}$-Ideale $\mathfrak{f}$.
Ist k algebraischer Zahlkörper und $\mathfrak{p}$ eine endliche Primstelle von k, dann ergibt sich wegen (6.3) für alle ganzen $\mathfrak{o}$-Ideale $\mathfrak{f}$:
$\mathcal{O}^{\mathfrak{f}\mathfrak{p}} = \mathcal{O}^{\mathfrak{f}}_{\mathfrak{p}}$, wobei $\mathcal{O}^{\mathfrak{f}\mathfrak{p}} = \mathcal{O}^{\mathfrak{f}\mathfrak{p}}(K)$ und $\mathcal{O}^{\mathfrak{f}} = \mathcal{O}^{\mathfrak{f}}(K)$ abgekürzt wurde.
Es ist $\mathcal{O}^{\mathfrak{f}} = \mathfrak{o} + \mathfrak{f}\mathcal{O}^{\mathfrak{o}}$ und für $\mathfrak{p} \nmid \mathfrak{f}$ daher: $\mathcal{O}^{\mathfrak{f}}_{\mathfrak{p}} = \mathcal{O}^{\mathfrak{o}}_{\mathfrak{p}}$.

(6.11) Lemma: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper. Seien K,K' halbeinfache quadratische Erweiterungen von k, sei $\sigma: K \to K'$ ein k-Algebrenisomorphismus und sei $\mathcal{O}$ eine K-Ordnung.
Dann ist $\sigma\mathcal{O}$ eine K'-Ordnung und $f(\sigma\mathcal{O}) = f(\mathcal{O})$.

Bew.: σ läßt k und insbesondere $\mathfrak{o}$, die Hauptordnung von k, elementweise fest. Daher überführt σ ganze Zahlen in ganze Zahlen: $\sigma(\mathcal{O}^{\mathfrak{o}}(K)) = \mathcal{O}^{\mathfrak{o}}(K')$, also $\sigma(\mathcal{O}) = \sigma(\mathfrak{o} + f(\mathcal{O})\mathcal{O}^{\mathfrak{o}}(K)) = \mathfrak{o} + f(\mathcal{O})\mathcal{O}^{\mathfrak{o}}(K')$, also $f(\sigma\mathcal{O}) = f(\mathcal{O})$.

(6.12) Korollar: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper, K halbeinfache quadratische Erweiterung von k und $\mathcal{O}$ eine K-Ordnung. Dann ist $\mathcal{O}^* = \mathcal{O}$.

Bew.: Nach (6.11) ist $f(\mathcal{O}^*) = f(\mathcal{O})$, nach (6.8) also $\mathcal{O}^* = \mathcal{O}$. Wir geben noch einen direkten Beweis: Sei $\mathfrak{o}$ die Hauptordnung von k. Sei $A \in \mathcal{O}$. Dann ist $S(A) \in \mathfrak{o} \subset \mathcal{O}$, also $A^* = S(A) - A \in \mathcal{O}$ und $A = A^{**} \in \mathcal{O}^*$.
Daher $\mathcal{O} \subset \mathcal{O}^* \subset \mathcal{O}^{**} = \mathcal{O}$.

(6.13) Lemma: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$, sei K halbeinfache, quadratische Erweiterung von k und sei $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal. Dann gilt:
i) Sei $E \in \mathcal{O}^{\mathfrak{f}}$. Dann ist $E \in \mathcal{O}^{\mathfrak{f}\times}$ genau dann, wenn $N(E) \in \mathfrak{o}^\times$.
ii) $\mathcal{O}^{\mathfrak{o}\times} \cap \mathcal{O}^{\mathfrak{f}} = \mathcal{O}^{\mathfrak{f}\times}$.

Bew.: i) Wenn $E \in \mathcal{O}^{\mathfrak{f}\times}$, so $N(E) \in \mathfrak{o}^\times$. Sei umgekehrt $N(E) \in \mathfrak{o}^\times \subset \mathcal{O}^{\mathfrak{f}\times}$. Dann ist $E^{-1} = N(E)^{-1}E^* \in \mathcal{O}^{\mathfrak{f}\times}$.
ii) folgt sofort aus i)

§ 7 . Ideale von Ordnungen halbeinfacher quadratischer Erweiterungen; ihre Klassenzahl.

Bis einschließlich (7.5) definieren wir die Ideale von Ordnungen halbeinfacher quadratischer Erweiterungen K und leiten ihre einfachsten Eigenschaften ab. Der Rest des Paragrafen dient dem Beweis von Satz (7.25), der für die Anwendungen der Ergebnisse aus Teil III (§§ 16,17) wichtig ist. Die Methoden von §7 tauchen später (bei Anwendungen und Beispielen) mehrfach wieder auf.
Für Körper K ist Satz (7.25) schon bewiesen (/16/ S. 188 (2.8)). Siehe dazu /2/ und /16/ §2. Mein Beweis von (7.25) lebt stark von den Ideen Dedekinds, hat aber eine völlig neue Form erhalten.

Für diesen Paragrafen machen wir folgende Generalvoraussetzung.
(7.1): Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei K halbeinfache quadratische Erweiterung von k. Sei $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal.
Wir kürzen $\mathcal{O}^{\mathfrak{f}} = \mathcal{O}^{\mathfrak{f}}(K)$, $\mathcal{O}^{\mathfrak{o}} = \mathcal{O}^{\mathfrak{o}}(K)$ ab.

(7.2) Definition: (Voraussetzung 7.1)
i) Wir bezeichnen die Gruppe der $\mathfrak{o}$-Ideale mit I^k. Ist $\mathfrak{p}$ endliche Primstelle von k, so bezeichnen wir die Gruppe der $\mathfrak{o}_{\mathfrak{p}}$-Ideale mit $I_{\mathfrak{p}}^k = I^{k_{\mathfrak{p}}}$.
Die Gruppe der Hauptideale aus I^k bezeichnen wir mit H^k. (Alle Ideale aus $I_{\mathfrak{p}}^k$ sind Hauptideale)
ii) Ist $\mathfrak{p}$ eine endliche Primstelle von k, dann heißt $\alpha \subset K_{\mathfrak{p}}$ ein $\mathcal{O}_{\mathfrak{p}}^{\mathfrak{f}}$-Ideal, wenn es $a \in K_{\mathfrak{p}}^{\times}$ gibt mit $\alpha = a\mathcal{O}_{\mathfrak{p}}^{\mathfrak{f}}$. Die Gruppe der $\mathcal{O}_{\mathfrak{p}}^{\mathfrak{f}}$-Ideale bezeichnen wir mit $I_{\mathfrak{p}}^{\mathfrak{f}}$.
iii) $\alpha \subset K$ heißt $\mathcal{O}^{\mathfrak{f}}$-Ideal, wenn α nach Definition (4.9) ein Ideal von $\mathcal{O}^{\mathfrak{f}}$ ist und $\alpha_{\mathfrak{p}} \in I_{\mathfrak{p}}^{\mathfrak{f}}$ für alle endlichen Primstellen $\mathfrak{p}$ von k. Die Gruppe der $\mathcal{O}^{\mathfrak{f}}$-Ideale bezeichnen wir mit $I^{\mathfrak{f}}$, die Untergruppe der $\mathcal{O}^{\mathfrak{f}}$-Hauptideale (d.h. der $a\mathcal{O}^{\mathfrak{f}}$ mit $a \in K^{\times}$) mit $H^{\mathfrak{f}}$.

Das neutrale Element in $I^{\mathfrak{f}}$ ist $\mathcal{O}^{\mathfrak{f}}$. Daß $I^{\mathfrak{f}}$ tatsächlich eine Gruppe ist, d.h. daß jedes $\mathcal{O}^{\mathfrak{f}}$-Ideal ein Inverses hat, folgt leicht aus dem folgenden Satz.

(7.3) Satz: (Voraussetzung 7.1)
i) Ist α ein $\mathcal{O}^{\mathfrak{f}}$-Ideal, so ist $\alpha_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}^{\mathfrak{f}}$ für fast alle endlichen Primstellen $\mathfrak{p}$ von k.
ii) Sei $n \in \mathbb{N}$ und $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ eine Menge von endlichen Primstellen von k. Seien $a_i \in K_{\mathfrak{p}_i}^{\times}$ für $i = 1,\ldots n$. Dann wird durch $\alpha_{\mathfrak{p}_i} := a_i \mathcal{O}_{\mathfrak{p}_i}^{\mathfrak{f}}$ für $i = 1,\ldots,n$ und $\alpha_{\mathfrak{p}} := \mathcal{O}_{\mathfrak{p}}^{\mathfrak{f}}$ für alle endlichen Primstellen $\mathfrak{p}$ von k mit $\mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ ein $\mathcal{O}^{\mathfrak{f}}$-Ideal α definiert.

Bew.: i) folgt aus Lemma (4.15.iii)
ii) Sei $\mathfrak{a}' := K \cap (\bigcap_{\mathfrak{p}} \mathfrak{a}_{\mathfrak{p}})$. K und alle $\mathfrak{a}_{\mathfrak{p}}$ sind $\mathcal{O}'$-Moduln, daher ist auch $\mathfrak{a}'$ ein $\mathcal{O}'$-Modul. Es gibt $a \in \mathcal{O}-\{0\}$, so daß aa_i^{-1} ganz ist über $\mathcal{O}_{\mathfrak{p}_i}$ für alle $i = 1,\ldots,n$. Ist $b \in f(\mathcal{O})-\{0\}$, so ist also $ba \in \mathfrak{a}_{\mathfrak{p}_i}$ für alle $i = 1,\ldots,n$ und natürlich $ba \in \mathfrak{a}_{\mathfrak{p}}$ für $\mathfrak{p} \neq \{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\}$. Daher $ba \in \mathfrak{a}' \cap k^{\times}$. Genauso zeigt man, daß es $c \in k^{\times}$ gibt mit $c\mathfrak{a}' \subset \mathcal{O}'$. Daher ist $\mathfrak{a}'$ ein Ideal von $\mathcal{O}'$ im Sinne von Definition (4.9). Wir müssen noch zeigen, daß $\mathfrak{a}'_{\mathfrak{p}} = \mathfrak{a}_{\mathfrak{p}}$ für alle endlichen Primstellen $\mathfrak{p}$ von k. Wegen $\mathfrak{a}' \subset \mathfrak{a}_{\mathfrak{p}}$ folgt jedenfalls $\mathfrak{a}'_{\mathfrak{p}} \subset \mathfrak{a}_{\mathfrak{p}}$. $\mathfrak{a}_{\mathfrak{p}} \subset \mathfrak{a}'_{\mathfrak{p}}$ zeigt man genauso wie $\mathfrak{M}'' \subset \mathfrak{M}'_{\mathfrak{p}}$ im Beweis von (4.16). (Man muß nur A durch K, $\mathfrak{M}'$ durch $\mathfrak{a}'$ und $\mathfrak{M}''$ durch $\mathfrak{a}_{\mathfrak{p}}$ ersetzen)

(7.4) Bemerkung: Wegen Satz (5.2.iv) und dem entsprechenden Satz für Körper K ist Definition (7.2) für die Hauptordnung $\mathcal{O}^{\sigma}$ identisch mit Definition (4.9).

(7.5) Definition: (Voraussetzung 7.1)
i) Sei $\mathfrak{p}$ eine endliche Primstelle von k. Wir definieren einen Homomorphismus $N: I_{\mathfrak{p}}^{f} \to I_{\mathfrak{p}}^{k}$ durch $N(a\mathcal{O}_{\mathfrak{p}}^{f}) := N(a)\mathfrak{o}_{\mathfrak{p}}$ für $a \in K_{\mathfrak{p}}^{\times}$.
Für $\mathfrak{a} \in I_{\mathfrak{p}}^{f}$ heißt $N(\mathfrak{a})$ die Norm von $\mathfrak{a}$.
ii) Wir definieren einen Homomorphismus $N: I^{f} \to I^{k}$ durch:
$N(\mathfrak{a})_{\mathfrak{p}} := N(\mathfrak{a}_{\mathfrak{p}})$ für alle endlichen Primstellen $\mathfrak{p}$ von k. Ist $\mathfrak{a} \in I^{f}$, so heißt $N(\mathfrak{a})$ Norm von $\mathfrak{a}$.

Man sieht leicht, daß die Norm wohldefiniert ist. Definition (7.5) stimmt mit der allgemeinen Definition der Norm eines Ideals in halbeinfachen Algebren überein (vergleiche /3/ S. 79 - 83 §4 und S. 106 Satz 24)
Wir wollen in diesem Paragrafen den Quotienten $\frac{[I^{f} : H^{f}]}{[I^{\sigma} : H^{\sigma}]}$ berechnen.
Dabei brauchen wir mehrfach das folgende Lemma, das auch in späteren Paragrafen Verwendung findet.

(7.6) Lemma (Homomorphiesatz): Seien G,G' Gruppen und $\phi: G \to G'$ ein Homomorphismus. Ist H Untergruppe von G, so gilt:
$[G : H] = [\text{Kern } \phi : H \cap \text{Kern } \phi] \cdot [\phi(G) : \phi(H)]$

Bew.: siehe etwa /11/ S. 149 Satz 110

(7.7) Definition: (Voraussetzung 7.1). Wir definieren einen Homomorphismus $(\mathfrak{f} \to \mathfrak{f}): I^{f} \to I^{\mathfrak{f}}$ durch $(\mathfrak{f} \to \mathfrak{f})(\mathfrak{a}) := \mathfrak{a}\mathcal{O}^{\mathfrak{f}}$ für $\mathfrak{a} \in I^{f}$.

Wegen $\mathcal{O}^{f} \subset \mathcal{O}^{\mathfrak{f}}$ ist $(\mathfrak{f} \to \mathfrak{f})$ wohldefiniert.

(7.8) Lemma: (Voraussetzung 7.1). $(\mathfrak{f} \to \mathfrak{f})$ ist surjektiv.

Bew.: Sei $\mathfrak{A} \subset I^{\mathfrak{o}}$. Wir konstruieren ein $\alpha \in (\varphi\to\mathfrak{o})^{-1}(\mathfrak{A})$ folgendermaßen: Für fast alle endlichen Primstellen $\mathfrak{p}$ von k ist $\mathfrak{A}_{\mathfrak{p}} = U_{\mathfrak{p}}^{\mathfrak{o}}$, hier setzen wir $\alpha_{\mathfrak{p}} := U_{\mathfrak{p}}^{\mathfrak{p}}$. Ist $\mathfrak{p}$ eine der übrigen (endlich vielen) endlichen Primstellen von k, so gibt es $A \in K_{\mathfrak{p}}^{\times}$ mit $\mathfrak{A}_{\mathfrak{p}} = AU_{\mathfrak{p}}^{\mathfrak{o}}$, hier setzen wir $\alpha_{\mathfrak{p}} := AU_{\mathfrak{p}}^{\mathfrak{p}}$.

(7.9) Korollar: (Voraussetzung 7.1)

i) Für $\alpha \in I^{\mathfrak{p}}$ ist $N(\alpha) = N(\alpha U^{\mathfrak{o}}) = N((\varphi\to\mathfrak{o})(\alpha))$.

ii) $N(I^{\mathfrak{p}}) = N(I^{\mathfrak{o}})$

Bew.: klar

(7.10) Lemma: Voraussetzung (7.1). $(\varphi\to\mathfrak{o})(H^{\mathfrak{p}}) = H^{\mathfrak{o}}$.

Bew.: klar

Mit (7.8), (7.10) und dem Homomorphiesatz (7.6) folgt:
$[I^{\mathfrak{p}} : H^{\mathfrak{p}}] = [(\varphi\to\mathfrak{o})^{-1}(U^{\mathfrak{o}}) : H^{\mathfrak{p}} \cap (\varphi\to\mathfrak{o})^{-1}(U^{\mathfrak{o}})] \cdot [I^{\mathfrak{o}} : H^{\mathfrak{o}}]$, also:

$$\frac{[I^{\mathfrak{p}} : H^{\mathfrak{p}}]}{[I^{\mathfrak{o}} : H^{\mathfrak{o}}]} = \frac{[(\varphi\to\mathfrak{o})^{-1}(U^{\mathfrak{o}}) : U^{\mathfrak{p}}]}{[H^{\mathfrak{p}} \cap (\varphi\to\mathfrak{o})^{-1}(U^{\mathfrak{o}}) : U^{\mathfrak{p}}]} \qquad (7.11)$$

(7.12) Definition: (Voraussetzung 7.1). Wir definieren einen Homomorphismus $\eta^{\mathfrak{p}} : K^{\times} \to H^{\mathfrak{p}}$ durch $\eta^{\mathfrak{p}}(A) := AU^{\mathfrak{p}}$ für $A \in K^{\times}$.

(7.13) Lemma: (Voraussetzung 7.1)

i) $\eta^{\mathfrak{p}}$ ist surjektiv

ii) Kern $\eta^{\mathfrak{p}} = (\eta^{\mathfrak{p}})^{-1}(U^{\mathfrak{p}}) = U^{\mathfrak{p}\times}$

iii) $(\eta^{\mathfrak{p}})^{-1}(H^{\mathfrak{p}} \cap (\varphi\to\mathfrak{o})^{-1}(U^{\mathfrak{o}})) = U^{\mathfrak{o}\times}$

Bew.: i) klar

ii) $A \in \text{Kern } \eta^{\mathfrak{p}} \Leftrightarrow AU^{\mathfrak{p}} = U^{\mathfrak{p}} \Leftrightarrow A \in U^{\mathfrak{p}\times}$

iii) $\eta^{\mathfrak{p}}(A) \in (\varphi\to\mathfrak{o})^{-1}(U^{\mathfrak{o}}) \Leftrightarrow AU^{\mathfrak{p}}U^{\mathfrak{o}} = U^{\mathfrak{o}} \Leftrightarrow A \in U^{\mathfrak{o}\times}$

Aus (7.13) folgt mit dem Homomorphiesatz, angewandt auf $\eta^{\mathfrak{p}}$:

$$[U^{\mathfrak{o}\times} : U^{\mathfrak{p}\times}] = [H^{\mathfrak{p}} \cap (\varphi\to\mathfrak{o})^{-1}(U^{\mathfrak{o}}) : U^{\mathfrak{p}}] \qquad (7.14)$$

Für das direkte Produkt von abelschen Gruppen verwenden wir das Zeichen Π.

(7.15) Definition: (Voraussetzung 7.1). Wir definieren Homomorphismen:

i) $(\varphi\to\mathfrak{o})_{\mathfrak{p}} : I_{\mathfrak{p}}^{\mathfrak{p}} \to I_{\mathfrak{p}}^{\mathfrak{o}}$ für endliche Primstellen $\mathfrak{p}$ von k.

Es sei $(\varphi\to\mathfrak{o})_{\mathfrak{p}}(\alpha) = \alpha(\mathfrak{p})$ für $\alpha \in I_{\mathfrak{p}}^{\mathfrak{p}}$

ii) $\Pi^{\mathfrak{p}} : I^{\mathfrak{p}} \to \prod_{\mathfrak{p}_1} I_{\mathfrak{p}_1}^{\mathfrak{p}}$.

$\Pi^{\mathfrak{p}}$ ordne jedem $\alpha \in I^{\mathfrak{p}}$ das Tupel seiner Komponenten $\alpha_{\mathfrak{p}_1}$ mit $\mathfrak{p}_1 \mid \mathfrak{p}$ zu.

(7.16) Lemma: (Voraussetzung 7.1). $\Pi^{\mathfrak{p}}$ induziert einen Isomorphismus $\Pi^{\mathfrak{p}} : (\varphi\to\mathfrak{o})^{-1}(U^{\mathfrak{o}}) \to \prod_{\mathfrak{p}_1} (\varphi\to\mathfrak{o})_{\mathfrak{p}_1}^{-1}(U_{\mathfrak{p}_1}^{\mathfrak{o}})$. Insbesondere gilt also:

$$[(\varphi\to\mathfrak{o})^{-1}(U^{\mathfrak{o}}) : \{\alpha^{\mathfrak{p}}\}^{\mathfrak{p}}] = \prod_{\mathfrak{p}_1} [(\varphi\to\mathfrak{o})_{\mathfrak{p}_1}^{-1}(U_{\mathfrak{p}_1}^{\mathfrak{o}}) : \{\alpha_{\mathfrak{p}_1}^{\mathfrak{p}}\}].$$

Bew.: Sei $\alpha \in (\mathfrak{f}\to\mathfrak{o})^{-1}(\mathcal{O}^\circ)$, also $\alpha\mathcal{O}^\circ = \mathcal{O}^\circ$. Dann ist $\alpha_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\circ = \mathcal{O}_\mathfrak{p}^\circ$ für alle $\mathfrak{p}|\mathfrak{f}$, also $\alpha_\mathfrak{p} \in (\mathfrak{f}\to\mathfrak{o})_\mathfrak{p}^{-1}(\mathcal{O}_\mathfrak{p}^\circ)$. $\Pi^\mathfrak{f}$ ist also richtig definiert.
Injektivität: Sei $\alpha \in (\mathfrak{f}\to\mathfrak{o})^{-1}(\mathcal{O}^\circ)$ und $\alpha_\mathfrak{p} = \mathcal{O}_\mathfrak{p}^\mathfrak{f}$ für alle $\mathfrak{p}|\mathfrak{f}$.
Es ist $\alpha\,\mathcal{O}^\circ = \mathcal{O}^\circ$. Für alle endlichen Primstellen $\mathfrak{p}$ von k mit $\mathfrak{p}\nmid\mathfrak{f}$ ist $\mathcal{O}_\mathfrak{p}^\mathfrak{f} = \mathcal{O}_\mathfrak{p}^\circ$, also $\alpha_\mathfrak{p} = \alpha_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{f} = \alpha_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\circ = \mathcal{O}_\mathfrak{p}^\circ = \mathcal{O}_\mathfrak{p}^\mathfrak{f}$. Insgesamt ergibt sich also: $\mathcal{A} = \mathcal{O}^\mathfrak{f}$.
Surjektivität: Für alle $\mathfrak{p}|\mathfrak{f}$ seien $\alpha_\mathfrak{p} \in (\mathfrak{f}\to\mathfrak{o})_\mathfrak{p}^{-1}(\mathcal{O}_\mathfrak{p}^\circ)$ gegeben.
Wir definieren (7.3) ein $\alpha \in (\mathfrak{f}\to\mathfrak{o})^{-1}(\mathcal{O}^\circ)$ durch folgende Vorschriften:
Für $\mathfrak{p}|\mathfrak{f}$ sei $\alpha_\mathfrak{p} := \alpha^\mathfrak{p}$. Für $\mathfrak{p}\nmid\mathfrak{f}$ sei $\alpha_\mathfrak{p} = \mathcal{O}_\mathfrak{p}^\mathfrak{f}$. Dann folgt die Beh.

Da $I_\mathfrak{p}^\mathfrak{f}$ nur Hauptideale enthält, läßt sich genau wie (7.14) beweisen:

Für $\mathfrak{p}|\mathfrak{f}$ ist $\left[\mathcal{O}_\mathfrak{p}^{\mathfrak{o}\times} : \mathcal{O}_\mathfrak{p}^{\mathfrak{f}\times}\right] = \left[(\mathfrak{f}\to\mathfrak{o})_\mathfrak{p}^{-1}(\mathcal{O}_\mathfrak{p}^\circ) : \{\mathcal{O}_\mathfrak{p}^\mathfrak{f}\}\right]$ (7.17)

(7.18) Definition: (Voraussetzung 7.1). Für $\mathfrak{p}|\mathfrak{f}$ sei $P_\mathfrak{p}: \mathcal{O}_\mathfrak{p}^{\mathfrak{o}\times} \to (\mathcal{O}_\mathfrak{p}^\mathfrak{o}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o})^\times$ die durch die natürliche Projektion induzierte Abbildung.
Für $A \in \mathcal{O}_\mathfrak{p}^\mathfrak{o}$ bezeichnen wir die Restklasse in $\mathcal{O}_\mathfrak{p}^\mathfrak{o}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o}$ auch mit $\overline{A}$.

(7.19) Lemma: (Voraussetzung 7.1). Sei $\mathfrak{p}|\mathfrak{f}$. Dann gilt:
i) Kern $P_\mathfrak{p} = 1 + \mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o}$ und $1 + \mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o} \subset \mathcal{O}_\mathfrak{p}^{\mathfrak{f}\times}$
ii) $P_\mathfrak{p}$ ist surjektiv
iii) $P_\mathfrak{p}(\mathcal{O}_\mathfrak{p}^{\mathfrak{f}\times}) = (\alpha_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times$
iv) $\left[\mathcal{O}_\mathfrak{p}^{\mathfrak{o}\times} : \mathcal{O}_\mathfrak{p}^{\mathfrak{f}\times}\right] = \dfrac{\#\,(\mathcal{O}_\mathfrak{p}^\mathfrak{o}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o})^\times}{\#\,(\alpha_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times}$

Bew.: i) Die erste Behauptung ist klar. Es ist $1 + \mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o} \subset \alpha_\mathfrak{p} + \mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o} = \mathcal{O}_\mathfrak{p}^\mathfrak{f}$.
Wegen Lemma (6.13.ii) brauchen wir nur noch zu zeigen: $1 + \mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o} \subset \mathcal{O}_\mathfrak{p}^{\alpha\times}$.
Sei π Primelement von $\alpha_\mathfrak{p}$. Wenn $A \in 1 + \mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o}$, gibt es wegen $\mathfrak{p}|\mathfrak{f}$ ein $B \in \mathcal{O}_\mathfrak{p}^\mathfrak{o}$ mit $A = 1 + \pi B$. Also ist $A^{-1} = (1 + \pi B)^{-1} = \sum_{i=0}^{\infty}(-\pi B)^i \in \mathcal{O}_\mathfrak{p}^\mathfrak{o}$.
ii) Sei $A \in \mathcal{O}_\mathfrak{p}^\mathfrak{o}$ mit $\overline{A} \in (\mathcal{O}_\mathfrak{p}^\mathfrak{o}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o})^\times$. Dann gibt es $B \in \mathcal{O}_\mathfrak{p}^\mathfrak{o}$ mit $\overline{AB} = \overline{1}$,
also $AB \in 1 + \mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o} \subset \mathcal{O}_\mathfrak{p}^{\alpha\times}$. Deshalb ist $A \in \mathcal{O}_\mathfrak{p}^{\mathfrak{o}\times}$.
iii) Wegen $\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o} \subset \mathcal{O}_\mathfrak{p}^\mathfrak{f}$ erhält man $P_\mathfrak{p}(\mathcal{O}_\mathfrak{p}^{\mathfrak{f}\times}) \subset (\mathcal{O}_\mathfrak{p}^\mathfrak{f}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o})^\times$.
Wie in ii) kann man dann zeigen, daß $P_\mathfrak{p}(\mathcal{O}_\mathfrak{p}^{\mathfrak{f}\times}) = (\mathcal{O}_\mathfrak{p}^\mathfrak{f}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o})^\times$.
Es ist $(\mathcal{O}_\mathfrak{p}^\mathfrak{f}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o})^\times = ((\alpha_\mathfrak{p} + \mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o})/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o})^\times \cong (\alpha_\mathfrak{p}/(\alpha_\mathfrak{p} \cap \mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o}))^\times = (\alpha_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times$.
Die letzte Gleichung folgt leicht, da $\mathfrak{f}_\mathfrak{p}$ Hauptideal ist.
iv) Nach dem Homomorphiesatz (7.6) ergibt sich:

$$\left[\mathcal{O}_\mathfrak{p}^{\mathfrak{o}\times} : \mathcal{O}_\mathfrak{p}^{\mathfrak{f}\times}\right] = \left[P_\mathfrak{p}(\mathcal{O}_\mathfrak{p}^{\mathfrak{o}\times}) : P_\mathfrak{p}(\mathcal{O}_\mathfrak{p}^{\mathfrak{f}\times})\right]$$
$$= \frac{\#\,P_\mathfrak{p}(\mathcal{O}_\mathfrak{p}^{\mathfrak{o}\times})}{\#\,P_\mathfrak{p}(\mathcal{O}_\mathfrak{p}^{\mathfrak{f}\times})}$$
$$= \frac{\#\,(\mathcal{O}_\mathfrak{p}^\mathfrak{o}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathfrak{o})^\times}{\#\,(\alpha_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times}$$

(7.20) Definition: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathcal{O}$. Ist $\mathfrak{f}$ ein ganzes $\mathcal{O}$-Ideal, so heißt $\mathcal{N}(\mathfrak{f}) := \#\, \mathcal{O}/\mathfrak{f}$ die Absolutnorm von $\mathfrak{f}$.

(7.21) Lemma: (Voraussetzung 7.1). Sei $\mathfrak{p}$ endliche Primstelle von k mit $\mathfrak{p} \mid \mathfrak{f}$. Sei $\mathfrak{f}_\mathfrak{p} = \mathfrak{p}^r \mathcal{O}_\mathfrak{p}$ (also $r \geq 1$). Dann ist $\#\, (\mathcal{O}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times = \mathcal{N}(\mathfrak{p}^r)(1 - \mathcal{N}(\mathfrak{p})^{-1})$.

Bew.: $(\mathcal{O}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times = (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^r\mathcal{O}_\mathfrak{p})^\times = (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^r\mathcal{O}_\mathfrak{p}) - (\mathfrak{p}\mathcal{O}_\mathfrak{p}/\mathfrak{p}^r\mathcal{O}_\mathfrak{p})$
Ist π ein Primelement von $\mathcal{O}_\mathfrak{p}$, dann induziert Multiplikation mit π eine Bijektion: $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^{r-1}\mathcal{O}_\mathfrak{p} \to \mathfrak{p}\mathcal{O}_\mathfrak{p}/\mathfrak{p}^r\mathcal{O}_\mathfrak{p}$. Daher ist

$$\begin{aligned}\#\, (\mathcal{O}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times &= \#\, (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^r\mathcal{O}_\mathfrak{p}) - \#\, (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^{r-1}\mathcal{O}_\mathfrak{p}) \\ &= \#\, (\mathcal{O}/\mathfrak{p}^r) - \#\, (\mathcal{O}/\mathfrak{p}^{r-1}) \\ &= \mathcal{N}(\mathfrak{p}^r) - \mathcal{N}(\mathfrak{p}^{r-1})\end{aligned}$$

(7.22) Definition: Sei k algebraischer Zahlkörper und $\mathfrak{p}$ eine Primstelle von k. Sei K halbeinfache quadratische Erweiterung von k. Wir definieren:

$$\left(\frac{K}{\mathfrak{p}}\right) := \begin{cases} -1, & \text{wenn } \mathfrak{p} \text{ träge in K ist} \\ 0, & \text{wenn } \mathfrak{p} \text{ verzweigt in K ist} \\ 1, & \text{wenn } \mathfrak{p} \text{ zerlegt in K ist} \end{cases}$$

(7.23) Lemma: Unter den gleichen Voraussetzungen wie in (7.21) ist

$$\frac{\#\, (\mathcal{O}_\mathfrak{p}^\mathcal{O}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathcal{O})^\times}{\#\, (\mathcal{O}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times} = \mathcal{N}(\mathfrak{p}^r)\left(1 - \left(\frac{K}{\mathfrak{p}}\right)\mathcal{N}(\mathfrak{p})^{-1}\right)$$

Bew.: i) Sei $\mathfrak{p}$ träge in K. Dann ist K Körper und $\mathfrak{q} = \mathfrak{p}\mathcal{O}^\mathcal{O}$ ist Primideal mit $\mathcal{N}(\mathfrak{q}) = \mathcal{N}(\mathfrak{p})^2$. Wie in (7.21) ergibt sich:
$\#\, (\mathcal{O}_\mathfrak{p}^\mathcal{O}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathcal{O})^\times = \#\, (\mathcal{O}_\mathfrak{q}^\mathcal{O}/(\mathfrak{f}\mathcal{O}^\mathcal{O})_\mathfrak{q})^\times = \mathcal{N}(\mathfrak{q}^r)(1 - \mathcal{N}(\mathfrak{q})^{-1})$, also

$$\frac{\#\, (\mathcal{O}_\mathfrak{p}^\mathcal{O}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathcal{O})^\times}{\#\, (\mathcal{O}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times} = \frac{\mathcal{N}(\mathfrak{p}^{2r})(1 - \mathcal{N}(\mathfrak{p})^{-2})}{\mathcal{N}(\mathfrak{p}^r)(1 - \mathcal{N}(\mathfrak{p})^{-1})} = \mathcal{N}(\mathfrak{p}^r)(1 + \mathcal{N}(\mathfrak{p})^{-1})$$

ii) Sei $\mathfrak{p}$ verzweigt in K. Dann ist K Körper, $\mathfrak{q}^2 = \mathfrak{p}\mathcal{O}^\mathcal{O}$ und $\mathfrak{q}$ Primideal mit $\mathcal{N}(\mathfrak{q}) = \mathcal{N}(\mathfrak{p})$. Wie in (7.21) ergibt sich:
$\#\, (\mathcal{O}_\mathfrak{p}^\mathcal{O}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathcal{O})^\times = \#\, (\mathcal{O}_\mathfrak{q}^\mathcal{O}/(\mathfrak{f}\mathcal{O}^\mathcal{O})_\mathfrak{q})^\times = \mathcal{N}(\mathfrak{q}^{2r})(1 - \mathcal{N}(\mathfrak{q})^{-1})$, also

$$\frac{\#\, (\mathcal{O}_\mathfrak{p}^\mathcal{O}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathcal{O})^\times}{\#\, (\mathcal{O}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times} = \frac{\mathcal{N}(\mathfrak{p}^{2r})(1 - \mathcal{N}(\mathfrak{p})^{-1})}{\mathcal{N}(\mathfrak{p}^r)(1 - \mathcal{N}(\mathfrak{p})^{-1})} = \mathcal{N}(\mathfrak{p}^r)$$

iii) Sei $\mathfrak{p}$ zerlegt in K. Dann ist $K_\mathfrak{p}$ kein Körper. Es gibt $K_\mathfrak{p}$-Idempotente e_1, e_2 mit $K_\mathfrak{p} = k_\mathfrak{p}e_1 \oplus k_\mathfrak{p}e_2$ und $\mathcal{O}_\mathfrak{p}^\mathcal{O} = \mathcal{O}_\mathfrak{p}e_1 \oplus \mathcal{O}_\mathfrak{p}e_2$. Dann ist nach dem chinesischen Restsatz:

$$\begin{aligned}\mathcal{O}_\mathfrak{p}^\mathcal{O}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathcal{O} &\simeq ((\mathcal{O}_\mathfrak{p}e_1 \oplus \mathcal{O}_\mathfrak{p}e_2)/(\mathfrak{f}_\mathfrak{p}e_1 \oplus \mathcal{O}_\mathfrak{p}e_2)) \oplus ((\mathcal{O}_\mathfrak{p}e_1 \oplus \mathcal{O}_\mathfrak{p}e_2)/(\mathcal{O}_\mathfrak{p}e_1 \oplus \mathfrak{f}_\mathfrak{p}e_2)) \\ &\simeq (\mathcal{O}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p}) \oplus (\mathcal{O}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})\end{aligned}$$

Hieraus folgt leicht $\#\, (\mathcal{O}_\mathfrak{p}^\mathcal{O}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathcal{O})^\times = (\#\, (\mathcal{O}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times)^2$, also

$$\frac{\#\, (\mathcal{O}_\mathfrak{p}^\mathcal{O}/\mathfrak{f}_\mathfrak{p}\mathcal{O}_\mathfrak{p}^\mathcal{O})^\times}{\#\, (\mathcal{O}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times} = \#\, (\mathcal{O}_\mathfrak{p}/\mathfrak{f}_\mathfrak{p})^\times = \mathcal{N}(\mathfrak{p}^r)(1 - \mathcal{N}(\mathfrak{p})^{-1})$$

(7.16), (7.17), (7.19.iv) und (7.23) ergeben:

$$\left[(\mathfrak{f}\to\mathfrak{o})^{-1}(\mathcal{O}^{\mathfrak{o}}) : (\mathcal{O}^{\mathfrak{f}})\right] = \prod_{\mathfrak{p}\mid\mathfrak{f}} \mathcal{N}(\mathfrak{p}^{r})\left(1-\left(\frac{K}{\mathfrak{p}}\right)\mathcal{N}(\mathfrak{p})^{-1}\right)$$

Dabei soll für $\mathfrak{p}\mid\mathfrak{f}$ gelten: $\mathfrak{f}_{\mathfrak{p}} = \mathfrak{p}^{r}\mathfrak{o}_{\mathfrak{p}}$. Ausmultiplizieren ergibt:

$$\left[(\mathfrak{f}\to\mathfrak{o})^{-1}(\mathcal{O}^{\mathfrak{o}}) : (\mathcal{O}^{\mathfrak{f}})\right] = \mathcal{N}(\mathfrak{f}) \prod_{\mathfrak{p}\mid\mathfrak{f}}\left(1-\left(\frac{K}{\mathfrak{p}}\right)\mathcal{N}(\mathfrak{p})^{-1}\right) \qquad (7.24)$$

Aus (7.11), (7.14) und (7.24) folgt jetzt der Satz:

(7.25) Satz: (Voraussetzung 7.1). Dann gilt:

$$\frac{\left[I^{\mathfrak{f}} : H^{\mathfrak{f}}\right]}{\left[I^{\mathfrak{o}} : H^{\mathfrak{o}}\right]} = \frac{\mathcal{N}(\mathfrak{f})}{\left[\mathcal{O}^{\mathfrak{o}\times} : \mathcal{O}^{\mathfrak{f}\times}\right]} \prod_{\mathfrak{p}\mid\mathfrak{f}}\left(1-\left(\frac{K}{\mathfrak{p}}\right)\mathcal{N}(\mathfrak{p})^{-1}\right)$$

(7.26) Lemma: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei K halbeinfache quadratische Erweiterung von k, sei $K = ke_1 \oplus ke_2$ mit K-Idempotenten e_1, e_2. Dann ist:

i) $\left[I^{\mathfrak{o}} : H^{\mathfrak{o}}\right] = \left[I^{k} : H^{k}\right]^{2}$

ii) $N(I^{\mathfrak{o}}) = I^{k}$

Bew.: i) $\phi : I^{\mathfrak{o}} \to I^{k} \times I^{k}$

$\mathfrak{a}e_1 + \mathfrak{b}e_2 \mapsto (\mathfrak{a},\mathfrak{b})$ ist ein Isomorphismus.

$\mathcal{A} = \mathfrak{a}e_1 + \mathfrak{b}e_2$ ist genau dann Hauptideal, wenn $\mathfrak{a}$ und $\mathfrak{b}$ Hauptideale sind. (Wenn $\mathcal{A} = (ae_1 + be_2)\mathcal{O}^{\mathfrak{o}}$, ist $\mathfrak{a} = a\mathfrak{o}$ und $\mathfrak{b} = b\mathfrak{o}$; und umgekehrt)

Daher induziert ϕ einen Isomorphismus $\overline{\phi} : I^{\mathfrak{o}}/H^{\mathfrak{o}} \to (I^{k}/H^{k}) \times (I^{k}/H^{k})$

ii) $N(\mathfrak{a}e_1 + \mathfrak{o}e_2) = \mathfrak{a}$.

§ 8. Hilfsmittel aus der Klassenkörpertheorie

In §8 sind die Definitionen und Sätze der Klassenkörpertheorie (aus /11/) zusammengestellt, die wir in dieser Arbeit brauchen. Am wichtigsten ist das Korollar (8.4), mit dessen Hilfe wir in §16 ein durchsichtiges Ergebnis erhalten.

(8.1) Definition: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$.

i) Ist $\mathfrak{p}$ reelle Primstelle von k, $n\in\mathbb{N}$, $a\in k$, so sagen wir $a \equiv 1 \bmod \mathfrak{p}^{n}$, wenn a in der $\mathfrak{p}$-adischen Bewertung von k positiv ist.

ii) Ist $\mathfrak{p}$ komplexe Primstelle von k, $n\in\mathbb{N}$, $a\in k$, so sagen wir $a \equiv 1 \bmod \mathfrak{p}^{n}$, wenn $a \neq 0$.

iii) Ist $\mathfrak{p}$ unendliche Primstelle von k, $n\in\mathbb{N}$, so heißen alle $\mathfrak{o}$-Ideale prim zu $\mathfrak{p}^{n}$.

iv) Ein Idealmodul $\mathfrak{m}$ ist ein formales direktes Produkt von endlich vielen positiven positiven Primstellenpotenzen: $\mathfrak{m} = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}$ $(r\in\mathbb{N}_0, n_i\in\mathbb{N})$

v) Ist $\mathfrak{m} = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}$ ein Idealmodul, $a \in k$, so sagen wir $a \equiv 1 \bmod \mathfrak{m}$, wenn $a \equiv 1 \bmod \mathfrak{p}_i^{n_i}$ für alle $i = 1,\ldots,r$.

vi) Sei $\mathfrak{m} = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}$ ein Idealmodul. Ein $\mathcal{O}$-Ideal $\mathfrak{a}$ heißt <u>prim zu</u> $\mathfrak{m}$, wenn $\mathfrak{a}$ prim zu allen $\mathfrak{p}_i^{n_i}$ $(i = 1,\ldots,r)$ ist. Die Gruppe der zu $\mathfrak{m}$ primen Ideale bezeichnen wir mit $J_{\mathfrak{m}}$.

vii) Sei $\mathfrak{m} = \prod_{i=1}^{r} \mathfrak{p}_i^{n_i}$ ein Idealmodul und sei $K \supset k$ algebraischer Zahlkörper mit Hauptordnung $\mathcal{O}$. Dann bezeichne $J_{\mathfrak{m}}^{K}$ die Gruppe der $\mathcal{O}$-Ideale, die zu allen Fortsetzungen der $\mathfrak{p}_i$ in K prim sind.

viii) Ist $\mathfrak{m}$ ein Idealmodul, dann heißt $S_{\mathfrak{m}} := \{a\mathcal{O} \mid a \equiv 1 \bmod \mathfrak{m}\} \subset H^k$ der <u>Strahl mod</u> $\mathfrak{m}$.

<u>(8.2) Satz:</u> Seien $k \subset K$ algebraische Zahlkörper und $\mathfrak{m}$ ein Idealmodul in k. Dann gilt: (N bezeichne die Norm N: $I^K \to I^k$):

i) $\left[J_{\mathfrak{m}} : N(J_{\mathfrak{m}}^{K}) S_{\mathfrak{m}}\right] \leq \left[K : k\right]$

ii) Ist K galoissch über k mit abelscher Galoisgruppe, dann gilt: $\left[J_{\mathfrak{m}} : N(J_{\mathfrak{m}}^{K}) S_{\mathfrak{m}}\right] = \left[K : k\right]$ genau dann, wenn $\mathfrak{m}$ die Verzweigungsstellen von K über k in genügend hoher Potenz ≥ 1 enthält.

<u>Bemerkung:</u> ii) läßt sich genauer fassen: $\left[J_{\mathfrak{m}} : N(J_{\mathfrak{m}}^{K}) S_{\mathfrak{m}}\right] = \left[K : k\right]$ genau dann, wenn $\mathfrak{m}$ Vielfaches des Führers von K in k ist.
Der Führer von K in k ist ein Idealmodul in k, der Potenzen von genau den Primstellen enthält, die in K verzweigt sind.

<u>Bew.:</u> siehe /11/ §§ 5,9 und 10; insbesondere zu i) S. 130 Satz 91, zu ii) S. 132 Satz 92 und S. 139 Satz IX

<u>(8.3) Satz:</u> Seien $k \subset K$ algebraische Zahlkörper. K sei galoissch über k mit abelscher Galoisgruppe, $\mathfrak{m}$ sei ein Idealmodul in k mit $\left[J_{\mathfrak{m}} : N(J_{\mathfrak{m}}^{K}) S_{\mathfrak{m}}\right] = \left[K : k\right]$. Dann gilt:
Ist $\mathfrak{p}$ ein Primideal in k mit $\mathfrak{p} \nmid \mathfrak{m}$ und $\mathfrak{P}$ ein Primteiler von $\mathfrak{p}$ in K, so ist $t_k(\mathfrak{P}) = \min\{r \in \mathbb{N} \mid \mathfrak{p}^r \in N(J_{\mathfrak{m}}^{K})\ S_{\mathfrak{m}}\}$.
<u>Bew.:</u> siehe /11/ S. 136 Satz IV

In dieser Arbeit werden wir es nur mit dem Fall zu tun haben, daß K quadratische Erweiterung von k ist und $\mathfrak{m}$ nur reelle Primstellen enthält. In diesem Fall ist $J_{\mathfrak{m}} = I^k$ und $J_{\mathfrak{m}}^{K} = I^{\mathcal{O}} = I^K$.
Jede quadratische Körpererweiterung ist galoissch mit abelscher Galoisgruppe. Daher haben wir:

<u>(8.4) Korollar:</u> Sei k algebraischer Zahlkörper, K eine quadratische Körpererweiterung von k und $\mathfrak{a}$ ein Idealmodul in k, der nur reelle Primstellen enthält. Dann gilt:

i) $\left[I^k : N(I^K) S_{\mathfrak{a}}\right] \leq 2$

ii) $\left[I^k : N(I^K)S_{\mathfrak{u}} \right] = 2$ genau dann, wenn $\mathfrak{u}$ alle Verzweigungsstellen von K über k enthält, d.h. genau dann, wenn K über k höchstens an den Primstellen $\mathfrak{p}$ verzweigt ist, für die $\mathfrak{p} | \mathfrak{u}$.
iii) Sind die Bedingungen in ii) erfüllt, dann sind alle Primideale $\mathfrak{p}$ aus k in K unverzweigt und es gilt:
$\mathfrak{p}$ ist zerlegt in K genau dann, wenn $\mathfrak{p} \in N(I^K)S_{\mathfrak{u}}$.
$\mathfrak{p}$ ist träge in K genau dann, wenn $\mathfrak{p} \notin N(I^K)S_{\mathfrak{u}}$.

(8.5) Lemma: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$; sei $\mathfrak{u}$ ein Idealmodul, der nur reelle Primstellen enthält, sei u die Zahl der verschiedenen reellen Primstellen $\mathfrak{p}$ mit $\mathfrak{p} | \mathfrak{u}$ und sei $\mathfrak{u}^\times := \{ a \in \mathfrak{o}^\times \mid a \equiv 1 \bmod \mathfrak{u} \}$. Dann ist $\mathfrak{u}^\times$ Untergruppe von $\mathfrak{o}^\times$ und: $\dfrac{\left[I^k : S_{\mathfrak{u}} \right]}{\left[I^k : H^k \right]} = \dfrac{2^u}{\left[\mathfrak{o}^\times : \mathfrak{u}^\times \right]}$.

Bew.: siehe /11/ S. 68 Satz 48 und S. 72 Satz 52

§ 9 . Idealtheorie in Quaternionenalgebren

In §9 leiten wir aus der Idealtheorie einfacher Algebren spezielle Aussagen über die Idealtheorie in Quaternionenalgebren her.
Im wesentlichen ist dies eine Zusammenstellung bekannter Tatsachen.

Wir machen folgende Generalvoraussetzung:
(9.1) Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$.
Sei Q eine k-Quaternionenalgebra.

(9.2) Lemma: Die Rechtsordnung eines Ideals $\mathfrak{A}$ in Q ist genau dann maximal, wenn die Linksordnung von $\mathfrak{A}$ maximal ist.

Bew.: siehe /3/ S. 75 Satz 12

(9.3) Definition: (Voraussetzung 9.1). Ein Ideal in Q heißt normal, wenn seine Links- und Rechtsordnung Maximalordnungen sind.

(9.4) Satz: (Voraussetzung 9.1). Sei $\mathfrak{A}$ ein normales Ideal mit Linksordnung $\mathfrak{M}$ und Rechtsordnung $\mathfrak{M}'$. Dann gibt es genau ein Ideal $\mathfrak{A}^{-1}$ mit Linksordnung $\mathfrak{M}'$ und Rechtsordnung $\mathfrak{M}$, so daß $\mathfrak{A}\mathfrak{A}^{-1} = \mathfrak{M}$ und $\mathfrak{A}^{-1}\mathfrak{A} = \mathfrak{M}'$.

Bew.: siehe /3/ S. 74 Satz 7

(9.5) Korollar: (Voraussetzung 9.1). Seien $\mathfrak{M}$ und $\mathfrak{M}'$ zwei Q-Maximalordnungen und sei $\mathfrak{A}$ ein Ideal mit Linksordnung $\mathfrak{M}$ und Rechtsordnung $\mathfrak{M}'$. Dann gilt:
i) $\mathfrak{M}\mathfrak{M}'$ ist ein Ideal mit Linksordnung $\mathfrak{M}$, Rechtsordnung $\mathfrak{M}'$.
ii) Es gibt ein zweiseitiges $\mathfrak{M}$-Ideal $\mathfrak{B}$ und ein zweiseitiges $\mathfrak{M}'$-Ideal $\mathfrak{B}'$, so daß $\mathfrak{A} = \mathfrak{B}\mathfrak{M}\mathfrak{M}' = \mathfrak{M}\mathfrak{M}'\mathfrak{B}'$.

Bew.: i) leicht zu sehen

ii) $\mathfrak{A}(\mathfrak{M}\mathfrak{M}')^{-1} = :\mathfrak{B}$ ist ein zweiseitiges $\mathfrak{M}$-Ideal und es gilt:
$\mathfrak{A} = \mathfrak{A}\mathfrak{M}' = \mathfrak{A}(\mathfrak{M}\mathfrak{M}')^{-1}\mathfrak{M}\mathfrak{M}' = \mathfrak{B}\mathfrak{M}\mathfrak{M}'$. Genauso folgt die zweite Beh.

(9.6) Satz: Sei k algebraischer Zahlkörper, Q eine k-Quaternionenalgebra, $\mathfrak{M}$ eine Q-Maximalordnung. Dann gilt:

i) Ist $\mathfrak{A}$ ein Links- (Rechts-, zweiseitiges) Ideal von $\mathfrak{M}$, so ist $\mathfrak{M}_\mathfrak{p} = \mathfrak{A}_\mathfrak{p}$ für fast alle endlichen Primstellen $\mathfrak{p}$ von k.

ii) Sei $n \in \mathbb{N}$, sei $\{\mathfrak{p}_1,\dots,\mathfrak{p}_n\}$ eine Menge von endlichen Primstellen von k und seien $\mathfrak{A}_i$ Links- (Rechts-, zweiseitige) Ideale von $\mathfrak{M}_{\mathfrak{p}_i}$ für $i = 1,\dots,n$. Dann gibt es ein Links- (Rechts-, zweiseitiges) Ideal $\mathfrak{A}$ von $\mathfrak{M}$ mit $\mathfrak{A}_{\mathfrak{p}_i} = \mathfrak{A}_i$ für $i = 1,\dots,n$ und $\mathfrak{A}_\mathfrak{p} = \mathfrak{M}_\mathfrak{p}$ für alle endlichen Primstellen $\mathfrak{p}$ von k mit $\mathfrak{p} \notin \{\mathfrak{p}_1,\dots,\mathfrak{p}_n\}$.

iii) Sei $n \in \mathbb{N}$, sei $\{\mathfrak{p}_1,\dots,\mathfrak{p}_n\}$ eine Menge von endlichen Primstellen von k und seien $\mathfrak{M}_i$ $Q_{\mathfrak{p}_i}$-Maximalordnungen für $i = 1,\dots,n$. Dann gibt es eine Q-Maximalordnung $\mathfrak{M}'$ mit $\mathfrak{M}'_{\mathfrak{p}_i} = \mathfrak{M}_i$ für $i = 1,\dots,n$ und $\mathfrak{M}'_\mathfrak{p} = \mathfrak{M}_\mathfrak{p}$ für alle endlichen Primstellen $\mathfrak{p}$ von k mit $\mathfrak{p} \notin \{\mathfrak{p}_1,\dots,\mathfrak{p}_n\}$.

Bew.: i) folgt aus Lemma (4.15.iii)

ii) siehe /3/ S. 105 Satz 23

iii) Wir setzen $\mathfrak{A}_i := \mathfrak{M}_{\mathfrak{p}_i}\mathfrak{M}_i$ für $i = 1,\dots,n$ und bestimmen nach ii) ein $\mathfrak{M}$-Linksideal $\mathfrak{A}$. Dann ist die Rechtsordnung $\mathfrak{M}'$ von $\mathfrak{A}$ die gesuchte Maximalordnung.

(9.7) Definition: (Voraussetzung 9.1). Sei $Q \underset{k}{\cong} M_2(k)$. Dann heißen $M_{11}, M_{12}, M_{21}, M_{22} \in Q - \{0\}$ (in dieser Reihenfolge) Matrizeseinheiten, wenn für alle $r,s,t,u \in \{1,2\}$ gilt: $M_{rs}M_{tu} = \begin{cases} M_{ru}, & \text{wenn } s = t \\ 0, & \text{wenn } s \neq t \end{cases}$

Wir werden Matrizeseinheiten oft mit $\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix}$ bezeichnen und brauchen dann folgende Definition:

(9.8) Definition: (Voraussetzung 9.1) Sei $Q \underset{k}{\cong} M_2(k)$ und seien $M_{11} = \begin{pmatrix}1&0\\0&0\end{pmatrix}$, $M_{12} = \begin{pmatrix}0&1\\0&0\end{pmatrix}$, $M_{21} = \begin{pmatrix}0&0\\1&0\end{pmatrix}$, $M_{22} = \begin{pmatrix}0&0\\0&1\end{pmatrix} \in Q$ Matrizeseinheiten. Dann definieren wir:

i) Für $a,b,c,d \in k$: $\begin{pmatrix}a&b\\c&d\end{pmatrix} := aM_{11} + bM_{12} + cM_{21} + dM_{22}$

ii) Für $A,B,C,D \subset k$: $\begin{pmatrix}A&B\\C&D\end{pmatrix} := \left\{ \begin{pmatrix}a&b\\c&d\end{pmatrix} \mid a \in A, b \in B, c \in C, d \in D \right\}$

(9.9) Lemma: (Voraussetzung 9.1) Sei $Q \underset{K}{\cong} M_2(k)$ und seien $M_{11},M_{12},M_{21},M_{22} \in Q$ Matrizeseinheiten. Dann gilt:

i) $D_k(M_{11},M_{12},M_{21},M_{22}) = -1$. Insbesondere ist $\{M_{11},M_{12},M_{21},M_{22}\}$ Basis von Q über k.

ii) Sind $M'_{11},M'_{12},M'_{21},M'_{22} \in Q$ Matrizeseinheiten, so gibt es $M \in Q^\times$ mit $M'_{rs} = MM_{rs}M^{-1}$ für $r,s \in \{1,2\}$.

Bew.: i) Es ist $M_{rr}^2 = M_{rr}$ und $M_{rs}^2 = 0$ für $r \neq s$; außerdem ist $M_{rs} \notin k$ (für $r,s \in \{1,2\}$). Daher rechnet man leicht nach:

$$D_k(M_{11},M_{12},M_{21},M_{22}) = \det \begin{pmatrix} 1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1 \end{pmatrix} = -1$$

Die M_{rs}, $r,s \in \{1,2\}$ sind also linear unabhängig. Wegen $[Q : k] = 4$ folgt die Behauptung.

ii) Wegen $M_{11} + M_{22} = 1 = M'_{11} + M'_{22}$ wird durch die Vorschriften $M_{rs} \mapsto M'_{rs}$ für $r,s \in \{1,2\}$ ein k-Algebrenautomorphismus von Q definiert. Nach (3.5) ist dies ein innerer Automorphismus.

(9.10) Lemma: (Voraussetzung 9.1). Sei $Q \underset{K}{\cong} M_2(k)$. Seien $\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix} \in Q$ Matrizeseinheiten. Dann ist $\begin{pmatrix}\mathfrak{o}&\mathfrak{o}\\\mathfrak{o}&\mathfrak{o}\end{pmatrix}$ eine Q-Maximalordnung.

Bew.: siehe /3/ S. 72 Satz 11

(9.11) Satz: Sei k ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und Primideal $\mathfrak{p}$. Sei Q eine k-Quaternionenalgebra. Dann gilt:

i) Wenn Q Divisionsalgebra ist, ist die Menge $\mathfrak{M}$ der über $\mathfrak{o}$ ganzen Größen ein Ring. $\mathfrak{M}$ ist also die einzige Q-Maximalordnung. Alle Ideale von $\mathfrak{M}$ sind zweiseitig und Hauptideale, d.h. zu jedem $\mathfrak{M}$-Ideal $\mathfrak{A}$ gibt es $A \in Q^\times$ mit $\mathfrak{A} = A\mathfrak{M} = \mathfrak{M}A$. $\mathfrak{M}$ hat ein einziges Primideal $\mathfrak{P}$. Alle $\mathfrak{M}$-Ideale sind also Potenzen von $\mathfrak{P}$; die Gruppe der $\mathfrak{M}$-Ideale ist unendlich zyklisch. Es ist $\mathfrak{M}\mathfrak{p} = \mathfrak{P}^2$.

ii) Sei $Q \underset{K}{\cong} M_2(k)$ und $\mathfrak{M}$ eine Q-Maximalordnung. Dann gibt es Matrizeseinheiten $\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix} \in Q$, so daß $\mathfrak{M} = \begin{pmatrix}\mathfrak{o}&\mathfrak{o}\\\mathfrak{o}&\mathfrak{o}\end{pmatrix}$. $\mathfrak{M}$ hat ein einziges Primideal $\mathfrak{P}$. Es ist $\mathfrak{P} = \mathfrak{M}\mathfrak{p}$. Alle Ideale von $\mathfrak{M}$ sind Hauptideale.

Bew.: i) siehe /3/ S. 100 Satz 12 und S. 112 Satz 1

ii) siehe /3/ S. 100 Satz 13.

(9.12) Lemma: Unter den gleichen Voraussetzungen wie in (9.11) ist Q genau dann Divisionsalgebra, wenn $\mathfrak{p} | D_k(Q)$.

Bew.: siehe /3/ S. 114 Satz 5

(9.13) Satz : Sei k algebraischer Zahlkörper, Q eine k-Quaternionenalgebra und $\mathfrak{p}$ eine endliche Primstelle von k. Dann gilt:
i) Wenn $\mathfrak{p} | D_k(Q)$, ist $\mathfrak{p}$ Verzweigungsstelle von Q. Ist $\mathfrak{M}$ eine Q-Maximalordnung, so ist $\mathfrak{M}\mathfrak{p} = \mathfrak{P}^2$ mit einem Primideal $\mathfrak{P}$ von $\mathfrak{M}$.
ii) Wenn $\mathfrak{p} \nmid D_k(Q)$, dann zerfällt Q an der Stelle $\mathfrak{p}$. Ist $\mathfrak{M}$ eine Q-Maximalordnung, so ist $\mathfrak{M}_{\mathfrak{P}}$ Primideal von $\mathfrak{M}$.
iii) Ist $\mathfrak{M}$ eine Q-Maximalordnung, so ist jedes Primideal von $\mathfrak{M}$ von der in i) oder ii) angegebenen Form.

Bew.: i) und ii) folgen ganz kanonisch aus (9.11) und (9.12).
iii) Ist $\mathfrak{P}$ ein $\mathfrak{M}$-Primideal, so ist $\mathfrak{P} \cap \mathfrak{O} = : \mathfrak{a}$ ein ganzes $\mathfrak{o}$-Ideal ($\mathfrak{o}$ = Hauptordnung von k). $\mathfrak{P}$ ist Teiler von $\mathfrak{M}\mathfrak{a}$. Aber $\mathfrak{M}\mathfrak{a}$ hat nur Primteiler von der Form i) oder ii).

(9.14) Definition: (Voraussetzung 9.1). Sei $\mathfrak{M}$ eine Q-Maximalordnung.
i) Sei k ein $\mathfrak{p}$-adischer Zahlkörper. Sei $\mathfrak{A}$ ein $\mathfrak{M}$-Linksideal, d.h. sei $\mathfrak{A} = \mathfrak{M}A$ mit $A \in Q^\times$ (9.11). Dann setzen wir $N(\mathfrak{A}) := N(A)\mathfrak{o}$. $N(\mathfrak{A})$ heißt Norm von $\mathfrak{A}$.
ii) Sei k algebraischer Zahlkörper. Sei $\mathfrak{A}$ ein $\mathfrak{M}$-Linksideal. Dann definieren wir $N(\mathfrak{A})$ durch die Vorschrift: $N(\mathfrak{A})_{\mathfrak{p}} := N(\mathfrak{A}_{\mathfrak{p}})$ für alle endlichen Primstellen $\mathfrak{p}$ von k. $N(\mathfrak{A})$ heißt Norm von $\mathfrak{A}$.

Bemerkung: Wenn wir auf die gleiche Weise Normen von Rechtsidealen definieren, gelangen wir zum selben Ergebnis. Ist etwa k ein $\mathfrak{p}$-adischer Zahlkörper, $\mathfrak{A} = \mathfrak{M}A$, so ist $\mathfrak{A} = A(A^{-1}\mathfrak{M}A)$ und $A^{-1}\mathfrak{M}A$ ist Maximalordnung, die Rechtsordnung von $\mathfrak{A}$.
Die Norm ist wohldefiniert und stimmt mit der allgemeinen Definition der Norm eines Ideals in halbeinfachen Algebren überein.
(Vergleiche dazu /3/ S. 79 -83 §4 und S. 106 Satz 24)

(9.15) Lemma: (Voraussetzung 9.1). Sei $\mathfrak{M}$ eine Q-Maximalordnung, sei $\mathfrak{A}$ ein Ideal mit Linksordnung $\mathfrak{M}$, sei $\mathfrak{B}$ ein Ideal mit Rechtsordnung $\mathfrak{M}$. Dann ist $N(\mathfrak{B}\mathfrak{A}) = N(\mathfrak{B})N(\mathfrak{A})$.

Bew.: siehe /3/ S. 80 Satz 3

(9.16) Definition: (Voraussetzung 9.1)
i) Sei $\mathfrak{M}$ eine Q-Maximalordnung. Dann bezeichne ${}^{\mathfrak{M}}I$ (bzw. $I^{\mathfrak{M}}$) die Menge der Links- (bzw. Rechts-) Ideale von $\mathfrak{M}$ und ${}^{\mathfrak{M}}I^{\mathfrak{M}}$ die Gruppe der zweiseitigen Ideale von $\mathfrak{M}$.
ii) Sei k algebraischer Zahlkörper. Dann bezeichne $R = R(Q) \subset I^k$ die Gruppe, die von den Primidealen (endlichen Primstellen) erzeugt wird, an denen Q verzweigt ist.

(9.17) Definition: Ist G eine abelsche Gruppe, dann bezeichne $G^{(2)}$ die Untergruppe der Quadrate.

(9.18) Korollar: Sei k algebraischer Zahlkörper, Q eine k-Quaternionenalgebra, $\mathfrak{M}$ eine Q-Maximalordnung. Dann gilt für die durch Normbildung induzierten Abbildungen:
i) $N : {}^{\mathfrak{M}}I \to I^k$ ist surjektiv.
ii) $N : {}^{\mathfrak{M}}I^{\mathfrak{M}} \to RI^{k(2)}$ ist ein Isomorphismus.

Bew.: i) Es genügt zu zeigen, daß für jedes Primideal $\mathfrak{p} \in I^k$ gilt: $\mathfrak{p} \in N({}^{\mathfrak{M}}I)$. Wenn $\mathfrak{p} \in R$, also wenn $\mathfrak{p}$ Verzweigungsstelle von Q ist, ist $\mathfrak{M}\mathfrak{p} = \mathfrak{q}^2$ mit einem Primideal $\mathfrak{q}$ und es ist $N(\mathfrak{q})^2 = N(\mathfrak{q}^2) = N(\mathfrak{M}\mathfrak{p}) = \mathfrak{p}^2$, also $N(\mathfrak{q}) = \mathfrak{p}$.
(Da $N(\mathfrak{M}\mathfrak{a}) = \mathfrak{a}^2$ für $\mathfrak{a} \in I^k$, folgt $N({}^{\mathfrak{M}}I^{\mathfrak{M}}) = RI^{k(2)}$.)
Sei jetzt $\mathfrak{p}$ keine Verzweigungsstelle von Q. Wir konstruieren $\mathfrak{A} \in {}^{\mathfrak{M}}I$ mit $N(\mathfrak{A}) = \mathfrak{p}$ folgendermaßen: Für alle endlichen Primstellen $\mathfrak{q}$ von k mit $\mathfrak{q} \neq \mathfrak{p}$ sei $\mathfrak{A}_{\mathfrak{q}} := \mathfrak{M}_{\mathfrak{q}}$. Nach (9.11.ii) gibt es Matrizeseinheiten $\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix} \in Q_{\mathfrak{p}}$, so daß $\mathfrak{M}_{\mathfrak{p}} = \begin{pmatrix}\mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}}\\ \mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}}\end{pmatrix}$.
Sei π ein Primelement von $\mathfrak{o}_{\mathfrak{p}}$, d.h. $\pi\,\mathfrak{o}_{\mathfrak{p}} = \mathfrak{p}\,\mathfrak{o}_{\mathfrak{p}}$. Dann setzen wir $\mathfrak{A}_{\mathfrak{p}} := \mathfrak{M}_{\mathfrak{p}} \cdot \begin{pmatrix}\pi&0\\0&1\end{pmatrix}$. Es wird $N(\mathfrak{A}_{\mathfrak{p}}) = \pi\,\mathfrak{o}_{\mathfrak{p}} = \mathfrak{p}\,\mathfrak{o}_{\mathfrak{p}}$, also $N(\mathfrak{A}) = \mathfrak{p}$.
ii) Daß N Homomorphismus ist, folgt aus (9.15). Surjektivität ist schon gezeigt. Sei jetzt $\mathfrak{A} \in {}^{\mathfrak{M}}I^{\mathfrak{M}}$ mit $N(\mathfrak{A}) = \mathfrak{o}$. Dann ist für alle endlichen Primstellen $\mathfrak{p}$ von k: $\mathfrak{A}_{\mathfrak{p}} \in {}^{\mathfrak{M}_{\mathfrak{p}}}I^{\mathfrak{M}_{\mathfrak{p}}}$ und $N(\mathfrak{A}_{\mathfrak{p}}) = \mathfrak{o}_{\mathfrak{p}}$. ${}^{\mathfrak{M}_{\mathfrak{p}}}I^{\mathfrak{M}_{\mathfrak{p}}}$ ist unendlich zyklisch und wird von einem Primideal $\mathfrak{q}_{\mathfrak{p}}$ erzeugt (4.10 und 9.11) mit $N(\mathfrak{q}_{\mathfrak{p}}) = \mathfrak{p}_{\mathfrak{p}}$ oder $N(\mathfrak{q}_{\mathfrak{p}}) = \mathfrak{p}_{\mathfrak{p}}^2$. Also ist (da N Homomorphismus ist und $I_{\mathfrak{p}}^k$ ebenfalls unendlich zyklisch ist) notwendig $\mathfrak{A}_{\mathfrak{p}} = \mathfrak{M}_{\mathfrak{p}}$.

(9.19) Definition: (Voraussetzung 9.1). Sei $\mathfrak{M}$ eine Q-Maximalordnung. Dann sei $\Gamma(\mathfrak{M}) = \{A \in \mathfrak{M} \mid N(A) = 1\}$.

(9.20) Lemma: (Voraussetzung 9.1). Sei $\mathfrak{M}$ eine Q-Maximalordnung. Dann gilt:

i) $\mathfrak{M}^* = \mathfrak{M}$

ii) Sei $E \in \mathfrak{M}$. Dann ist $E \in \mathfrak{M}^\times$ genau dann, wenn $N(E) \in \mathfrak{o}^\times$.

iii) Sei $E \in \Gamma(\mathfrak{M})$. Dann ist $E^{-1} = E^*$

iv) $\Gamma(\mathfrak{M})$ ist Untergruppe von $\mathfrak{M}^\times$

Bew.: i) wie der direkte Beweis von Korollar (6.12)

ii) wie der Beweis von Lemma (6.13.i)

iii) und iv) sind jetzt klar

Bemerkung: ii) und iv) gelten auch für einfache zentrale Algebren höherer Dimension (siehe /3/ S. 88 §7).

§ 10 . Maximalordnungstypen in Quaternionenalgebren

Ausgehend vom wichtigen "Satz von Eichler" über Hauptideale (10.4) untersuchen wir die Einteilung der Maximalordnungen nach ihrem Typ (Def. 10.6). Hauptergebnis sind die Sätze (10.9) und (10.10). Sie finden Anwendung in den Paragrafen 16,18 und 23.

(10.1) Lemma: Für jedes Element $A \neq 0$ der Divisionsalgebra $(-1,-1)_{\mathbb{R}}$ ist $N(A) > 0$.

Bew.: leichte Rechnung (vgl. 1.18)

(10.2) Definition: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei Q eine k-Quaternionenalgebra. Dann definieren wir:

i) Sei $\mu = \mu(Q)$ der Idealmodul in k, der aus den unendlichen Verzweigungsstellen von Q über k zusammengesetzt ist.

ii) Sei u die Zahl der unendlichen Verzweigungsstellen von Q, d.h. die Zahl der Primstellen $\mathfrak{p}$ mit $\mathfrak{p} | \mu$.

iii) Sei $\mu^\times = \{a \in \mathfrak{o}^\times | a \equiv 1 \bmod \mu\}$.

Da es über $\mathbb{C}$ keine Divisionsalgebra $\neq \mathbb{C}$ gibt, ist μ nur aus reellen Primstellen von k zusammengesetzt. Wenn μ alle unendlichen Primstellen von k enthält, so heißt das also: k ist total reell und Q ist an allen unendlichen (reellen) Primstellen von k verzweigt.

Für die wichtigsten Sätze dieses Paragrafen machen wir die

Voraussetzung (10.3): Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$, sei Q eine k-Quaternionenalgebra, μ enthalte nicht alle unendlichen Primstellen von k.

Wenn ein normales Ideal $\mathcal{A} \subset Q$ Linkshauptideal ist, d.h. $\mathcal{A} = \mathfrak{M}A$ mit einer Q-Maximalordnung $\mathfrak{M}$ und $A \in Q^\times$, so ist es wegen $\mathcal{A} = A(A^{-1}\mathfrak{M}A)$ auch Rechtshauptideal und umgekehrt. Wir können also von normalen Hauptidealen schlechthin sprechen.

(10.4) Satz: (Eichler) (Voraussetzung 10.3). Dann gilt:
Ein normales Ideal $\mathcal{A}$ ist genau dann Hauptideal, wenn $N(\mathcal{A}) \in S_\infty$.

Bew.: siehe /4/,/5/ Satz 1

(10.5) Satz: (Voraussetzung 10.3). Sei $\mathfrak{M}$ eine Q-Maximalordnung.
Dann ist $N(\mathfrak{M}^\times) = u^\times$.

Bew.: "$\subset$": Sei $A \in \mathfrak{M}^\times$ und $\mathfrak{p}$ eine unendliche (reelle) Verzweigungsstelle von Q über k. Dann gilt wegen (1.16.iii) und (10.1): $Q_\mathfrak{p} \cong_{K_\mathfrak{p}} (-1,-1)_{K_\mathfrak{p}}$ und N(A) ist positiv bezüglich der $\mathfrak{p}$-adischen Bewertung.
"$\supset$": siehe /6/ S. 239 Satz 5

(10.6) Definition: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei Q eine k-Quaternionenalgebra.
i) Seien $\mathfrak{M}, \mathfrak{M}'$ zwei Q-Maximalordnungen. Wir sagen, daß $\mathfrak{M}$ und $\mathfrak{M}'$ vom gleichen Typ sind, wenn $\mathfrak{M} \cong_\mathfrak{o} \mathfrak{M}'$.
ii) Sei $\mathfrak{M}$ eine Q-Maximalordnung. Dann definieren wir:
$\widetilde{\mathfrak{M}} := \{\mathfrak{M}' \mid \mathfrak{M}'$ ist Q-Maximalordnung und $\mathfrak{M} \cong_\mathfrak{o} \mathfrak{M}'\}$ und nennen $\widetilde{\mathfrak{M}}$ den Typ von $\mathfrak{M}$.
iii) $\widetilde{Q} := \{\widetilde{\mathfrak{M}} \mid \mathfrak{M}$ ist Q-Maximalordnung$\}$

$\cong_\mathfrak{o}$ ist offensichtlich eine Äquivalenzrelation auf der Menge der Maximalordnungen von Q.

(10.7) Lemma: Unter den Voraussetzungen von (10.6) seien $\mathfrak{M}, \mathfrak{M}'$ zwei Q-Maximalordnungen. Dann gilt $\mathfrak{M} \cong_\mathfrak{o} \mathfrak{M}$ genau dann, wenn es $M \in Q^\times$ gibt mit $\mathfrak{M}' = M\mathfrak{M}M^{-1}$.

Bew.: Ein $\mathfrak{o}$-Algebrenisomorphismus $\sigma: \mathfrak{M} \to \mathfrak{M}'$ läßt sich auf natürliche und eindeutige Weise zu einem k-Algebrenautomorphismus $\sigma: Q \to Q$ fortsetzen. Nach (3.5) ist dies ein innerer Automorphismus. Die Umkehrung ist trivial.

Ist k ein $\mathfrak{p}$-adischer Zahlkörper, so sind nach (9.11) und (9.9.ii) alle Q-Maximalordnungen vom gleichen Typ.

(10.8) Lemma: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper. Sei Q eine k-Quaternionenalgebra und seien $\mathfrak{M}, \mathfrak{M}'$ zwei Q-Maximalordnungen.
Dann ist $N(\mathfrak{M}\mathfrak{M}') = N(\mathfrak{M}'\mathfrak{M})$.

Bew.: Sei $A \in Q^\times$. Dann ist $N((\mathfrak{M}A)^*) = N(A^*\mathfrak{M}^*) = N(A^*\mathfrak{M}) = N(A^*)\omega = N(A)\omega =$ $= N(\mathfrak{M}A)$. Nach Definition der Norm folgt für alle normalen Ideale $\mathcal{A}$: $N(\mathcal{A}^*) = N(\mathcal{A})$. Jetzt folgt die Behauptung wegen $(\mathfrak{M}\mathfrak{N})^* = \mathfrak{N}^*\mathfrak{M}^* = \mathfrak{N}'\mathfrak{M}$.

(10.9) Satz: (Voraussetzung 10.3). Dann gilt für alle Q-Maximalordnungen $\mathfrak{M}$, $\mathfrak{M}'$, $\mathfrak{M}''$:

i) $\widetilde{\mathfrak{M}} = \widetilde{\mathfrak{M}'}$ genau dann, wenn $N(\mathfrak{M}\mathfrak{M}') \in RI^{k(2)}S_\mu$.

ii) $N(\mathfrak{M}\mathfrak{M}')N(\mathfrak{M}'\mathfrak{M}'')N(\mathfrak{M}''\mathfrak{M}) \in RI^{k(2)}S_\mu$.

Bew.: i) Sei $\widetilde{\mathfrak{M}} = \widetilde{\mathfrak{M}'}$. Dann gibt es $M \in Q^\times$ mit $\mathfrak{M}' = M\mathfrak{M}M^{-1}$.
$\mathfrak{M}'M = M\mathfrak{M}$ ist ein Ideal mit Linksordnung $\mathfrak{M}'$, Rechtsordnung $\mathfrak{M}$.
Nach (9.5) gibt es ein zweiseitiges $\mathfrak{M}$-Ideal $\mathcal{A}$ mit $M\mathfrak{M} = (\mathfrak{M}'\mathfrak{M})\mathcal{A}$,
also $\mathfrak{M}'\mathfrak{M} = M\mathfrak{M}\mathcal{A}^{-1}$. Nach dem Normenmultiplikationssatz (9.15) ist
$N(\mathfrak{M}'\mathfrak{M}) = N(M\mathfrak{M})N(\mathcal{A}^{-1})$. Nach (9.18.ii) und (10.4) ist $N(\mathfrak{M}'\mathfrak{M}) \in RI^{k(2)}S_\mu$.
Mit Lemma (10.8) folgt jetzt die Beh.
Sei umgekehrt $N(\mathfrak{M}\mathfrak{M}') \in RI^{k(2)}S_\mu$. Nach (9.18.ii) gibt es ein zweiseitiges $\mathfrak{M}$-Ideal $\mathcal{A}$, so daß $N(\mathcal{A}\mathfrak{M}\mathfrak{M}') \notin S_\mu$. Nach (10.4) gibt es $M \in Q^\times$ mit $\mathcal{A}\mathfrak{M}\mathfrak{M}' = \mathfrak{M}M$. Die Rechtsordnung dieses Ideals ist $\mathfrak{M}' = M^{-1}\mathfrak{M}M$,
also ist $\widetilde{\mathfrak{M}'} = \widetilde{\mathfrak{M}}$.
ii) Nach dem Normenmultiplikationssatz (9.15) ist
$N(\mathfrak{M}\mathfrak{M}')N(\mathfrak{M}'\mathfrak{M}'') = N(\mathfrak{M}\mathfrak{M}'\mathfrak{M}'')$. Da $\mathfrak{M}\mathfrak{M}'\mathfrak{M}''$ ein Ideal mit Linksordnung $\mathfrak{M}$ und Rechtsordnung $\mathfrak{M}''$ ist, gibt es nach (9.5) ein zweiseitiges $\mathfrak{M}$-Ideal $\mathcal{A}$ mit $\mathfrak{M}\mathfrak{M}'\mathfrak{M}'' = \mathcal{A}\mathfrak{M}\mathfrak{M}''$. Daher wird:

$$\begin{aligned} N(\mathfrak{M}\mathfrak{M}')N(\mathfrak{M}'\mathfrak{M}'')N(\mathfrak{M}''\mathfrak{M}) &= N(\mathfrak{M}\mathfrak{M}'\mathfrak{M}'')N(\mathfrak{M}\mathfrak{M}'') \\ &= N(\mathcal{A})N(\mathfrak{M}\mathfrak{M}'')N(\mathfrak{M}\mathfrak{M}'') \\ &\in RI^{k(2)}S_\mu \end{aligned}$$

(10.10) Satz: (Voraussetzung 10.3). Sei $\mathfrak{M}$ eine Q-Maximalordnung.
Dann wird durch die Vorschrift $\mathfrak{M}' \mapsto N(\mathfrak{M}\mathfrak{M}')$ für jede Q-Maximalordnung $\mathfrak{M}'$ eine Bijektion $\widetilde{Q} \to I^k/RI^{k(2)}S_\mu$ induziert. Insbesondere gilt:
$\# \widetilde{Q} = \left[I^k : RI^{k(2)}S_\mu\right]$.

Bew.: i) Wohldefiniertheit: Seien $\mathfrak{M}'$ und $\mathfrak{M}''$ zwei Q-Maximalordnungen mit $\widetilde{\mathfrak{M}'} = \widetilde{\mathfrak{M}''}$. Nach (10.9.i) ist $N(\mathfrak{M}'\mathfrak{M}'') \in RI^{k(2)}S_\mu$. Nach (10.9.ii) ist

$$\begin{aligned} N(\mathfrak{M}\mathfrak{M}')N(\mathfrak{M}\mathfrak{M}'')^{-1} &= N(\mathfrak{M}\mathfrak{M}')N(\mathfrak{M}''\mathfrak{M})N(\mathfrak{M}''\mathfrak{M})^{-2} \\ &\in RI^{k(2)}S_\mu \end{aligned}$$

ii) Injektivität: Seien $\mathfrak{M}'$, $\mathfrak{M}''$ zwei Q-Maximalordnungen mit
$N(\mathfrak{M}\mathfrak{M}')N(\mathfrak{M}\mathfrak{M}'')^{-1} \in RI^{k(2)}S_\mu$. Dann folgt mit (10.8):
$N(\mathfrak{M}\mathfrak{M}')N(\mathfrak{M}''\mathfrak{M}) = N(\mathfrak{M}\mathfrak{M}')N(\mathfrak{M}\mathfrak{M}'')^{-1}N(\mathfrak{M}\mathfrak{M}'')^2 \in RI^{k(2)}S_\mu$.
Nach (10.9.ii) folgt $N(\mathfrak{M}'\mathfrak{M}'') \in RI^{k(2)}S_\mu$. Nach (10.9.i) ist $\widetilde{\mathfrak{M}'} = \widetilde{\mathfrak{M}''}$.

iii) Surjektivität: Sei $\mathfrak{a} \in I^k$. Nach (9.18.i) gibt es ein Ideal $\mathcal{A}$ mit Linksordnung $\mathcal{M}$ und $N(\mathcal{A}) = \mathfrak{a}$. Sei $\mathcal{M}'$ die Rechtsordnung von $\mathcal{A}$. Nach(9.5) gibt es ein zweiseitiges $\mathcal{M}$-Ideal $\mathcal{B}$ mit $\mathcal{A} = \mathcal{B}\mathcal{M}\mathcal{M}'$. Dann ist $N(\mathcal{M}\mathcal{M}')\mathfrak{a}^{-1} = N(\mathcal{B}^{-1}\mathcal{A})\mathfrak{a}^{-1} = N(\mathcal{B}^{-1}) \in RI^{k(2)}S_u$.

(10.11) Bemerkung: Wie in (10.9) und (10.10) beschrieben und gezeigt, operiert $I^k/RI^{k(2)}S_u$ fixpunktfrei und transitiv auf $\widetilde{Q}$. Da $I^k/RI^{k(2)}S_u$ ein Vektorraum über $\mathbb{Z}/2\mathbb{Z}$ ist, können wir $\widetilde{Q}$ als affinen Raum über $\mathbb{Z}/2\mathbb{Z}$ auffassen.

(10.12) Lemma: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei Q eine k-Quaternionenalgebra, sei $Q \underset{k}{\cong} M_2(k)$ und seien $\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix} \in Q$ Matrizeseinheiten. Dann gilt:

i) Ist $\mathfrak{a} \in I^k$, so ist $\begin{pmatrix}\mathfrak{o}&\mathfrak{a}^{-1}\\ \mathfrak{a}&\mathfrak{o}\end{pmatrix}$ eine Q-Maximalordnung.

ii) Sind $\mathfrak{a}, \mathfrak{b} \in I^k$, so ist $N\left(\begin{pmatrix}\mathfrak{o}&\mathfrak{a}^{-1}\\ \mathfrak{a}&\mathfrak{o}\end{pmatrix}\begin{pmatrix}\mathfrak{o}&\mathfrak{b}^{-1}\\ \mathfrak{b}&\mathfrak{o}\end{pmatrix}\right) = \mathfrak{a}^{-1}\mathfrak{b} + \mathfrak{a}\mathfrak{b}^{-1}$.

Bew.: i) Ist k algebraischer Zahlkörper, $\mathfrak{p}$ endliche Primstelle von k, so ist $\begin{pmatrix}\mathfrak{o}&\mathfrak{a}^{-1}\\ \mathfrak{a}&\mathfrak{o}\end{pmatrix}_{\mathfrak{p}} = \begin{pmatrix}\mathfrak{o}_{\mathfrak{p}}&\mathfrak{a}_{\mathfrak{p}}^{-1}\\ \mathfrak{a}_{\mathfrak{p}}&\mathfrak{o}_{\mathfrak{p}}\end{pmatrix}$. Wegen (4.16) brauchen wir die Beh. nur für $\mathfrak{p}$-adische Zahlkörper k zu zeigen. Sei $\mathfrak{a} = a\mathfrak{o}$ mit $a \in k^\times$. Dann ist $\begin{pmatrix}\mathfrak{o}&\mathfrak{a}^{-1}\\ \mathfrak{a}&\mathfrak{o}\end{pmatrix} = \begin{pmatrix}1&0\\0&a\end{pmatrix}\begin{pmatrix}\mathfrak{o}&\mathfrak{o}\\ \mathfrak{o}&\mathfrak{o}\end{pmatrix}\begin{pmatrix}1&0\\0&a\end{pmatrix}^{-1}$ eine Q-Maximalordnung (9.10).

ii) Wir brauchen die Beh. nur für $\mathfrak{p}$-adische Zahlkörper k zu zeigen. Sei π Primelement von $\mathfrak{o}$, $\mathfrak{a} = \pi^a\mathfrak{o}$, $\mathfrak{b} = \pi^b\mathfrak{o}$ und o.B.d.A. $a \geq b$. Dann ist

$$\begin{pmatrix}\mathfrak{o}&\mathfrak{a}^{-1}\\ \mathfrak{a}&\mathfrak{o}\end{pmatrix}\begin{pmatrix}\mathfrak{o}&\mathfrak{b}^{-1}\\ \mathfrak{b}&\mathfrak{o}\end{pmatrix} = \begin{pmatrix}\mathfrak{o}&\pi^{-a}\mathfrak{o}\\ \pi^a&\mathfrak{o}\end{pmatrix}\begin{pmatrix}\mathfrak{o}&\pi^{-b}\mathfrak{o}\\ \pi^b\mathfrak{o}&\mathfrak{o}\end{pmatrix}$$
$$= \begin{pmatrix}\pi^{-a+b}\mathfrak{o}&\pi^{-a}\mathfrak{o}\\ \pi^b\mathfrak{o}&\mathfrak{o}\end{pmatrix} = \begin{pmatrix}\mathfrak{o}&\pi^{-a}\mathfrak{o}\\ \pi^a\mathfrak{o}&\mathfrak{o}\end{pmatrix}\begin{pmatrix}\pi^{-a+b}&0\\0&1\end{pmatrix},$$

also
$$N\left(\begin{pmatrix}\mathfrak{o}&\mathfrak{a}^{-1}\\ \mathfrak{a}&\mathfrak{o}\end{pmatrix}\begin{pmatrix}\mathfrak{o}&\mathfrak{b}^{-1}\\ \mathfrak{b}&\mathfrak{o}\end{pmatrix}\right) = N\left(\begin{pmatrix}\pi^{-a+b}&0\\0&1\end{pmatrix}\right)\mathfrak{o}$$
$$= \pi^{-a+b}\mathfrak{o}$$
$$= \mathfrak{a}^{-1}\mathfrak{b}$$
$$= \mathfrak{a}^{-1}\mathfrak{b} + \mathfrak{a}\mathfrak{b}^{-1}$$

(10.13) Korollar: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und sei $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_n\} \subset I^k$ ein Repräsentantensystem von $I^k/I^{k(2)}H^k$. Dann ist $\left\{\begin{pmatrix}\mathfrak{o}&\mathfrak{a}_i^{-1}\\ \mathfrak{a}_i&\mathfrak{o}\end{pmatrix} \;\middle|\; i = 1, \ldots, n\right\}$ ein Repräsentantensystem von $\widetilde{M_2(k)}$.

Bew.: $M_2(k)$ ist unverzweigt über k, also $R = \{\mathfrak{o}\}$ und $S_u = H^k$; daher $RI^{k(2)}S_u = I^{k(2)}H^k$.

Sei $\mathfrak{M}_i := \begin{pmatrix} \mathfrak{o} & \mathfrak{a}_i^{-1} \\ \mathfrak{a}_i & \mathfrak{o} \end{pmatrix}$ für $i = 1,\dots,n$.

Wie man aus (10.12.ii) direkt oder dem Beweis von (10.12.ii) sieht, ist $N(\mathfrak{M}_i\mathfrak{M}_j)\,\mathfrak{a}_i\,\mathfrak{a}_j \in I^{k(2)} \subset I^{k(2)}H^k$ für $i,j \in \{1,\dots,n\}$.
Wenn j von 1 bis n läuft, durchläuft also $N(\mathfrak{M}_1\mathfrak{M}_j)$ ein Repräsentantensystem von $I^k/I^{k(2)}H^k$. Nach Satz (10.10) durchläuft dann $\mathfrak{M}_j$ ein Repräsentantensystem von $\widetilde{M_2(k)}$.

§ 11 . Optimale Einbettung

Das wichtigste Ergebnis von §11 ist Satz (11.9). Er macht Aussagen über den Durchschnitt $\mathfrak{M} \cap K$ einer Q-Maximalordnung $\mathfrak{M}$ mit einer halbeinfachen quadratischen Erweiterung $K \subset Q$.
Satz (11.9) spielt eine wichtige Rolle vor allem in §16.
Auch die vorbereitenden Lemmata (11.1), (11.4) und (11.6) werden noch gebraucht
Durch eine Verfeinerung der Methoden von Eichler in /7/ erhalten wir in §11 ein Ergebnis, das es uns möglich machen wird, die oben genannten Durchschnitte $\mathfrak{M} \cap K$ im Zusammenhang mit Maximalordnungstypen zu untersuchen. Diese Möglichkeit ist entscheidend dafür, daß wir die Ergebnisse von Shimizu, Prestel und Schneider (für den total reellen Fall) verallgemeinern können.
Ähnliche Methoden wie in §11 entwickeln wir auch in §18 und §23.

(11.1) Lemma: Sei k ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und Primelement π. Sei Q eine k-Quaternionenalgebra, sei $Q \underset{k}{\simeq} M_2(k)$.
Seien $\mathfrak{M}$ und $\mathfrak{M}'$ zwei Q-Maximalordnungen. Dann gibt es Matrizeseinheiten $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in Q$, so daß $\mathfrak{M} = \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{o} \end{pmatrix}$ und $\mathfrak{M}' = \begin{pmatrix} \mathfrak{o} & \pi^{-r}\mathfrak{o} \\ \pi^{r}\mathfrak{o} & \mathfrak{o} \end{pmatrix}$
mit $r \in \mathbb{N}_0$. Durch $\mathfrak{M}$ und $\mathfrak{M}'$ ist r eindeutig bestimmt, und zwar gilt: $N(\mathfrak{M}\mathfrak{M}') = \pi^{-r}\mathfrak{o}$.

Bew.: Nach Lemma (9.10) gibt es Matrizeseinheiten
$M_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $M_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $M_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $M_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in Q$, so daß
$\mathfrak{M} = \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{o} \end{pmatrix}$. Es gibt $M \in Q^\times$ mit $\mathfrak{M}' = M\mathfrak{M}M^{-1}$. O.B.d.A. können wir annehmen, daß $M \in \mathfrak{M}$ und $\pi^{-1}M \notin \mathfrak{M}$.

Durch eventuelles Vertauschen von Zeilen (d.h. Linksmultiplikation mit $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathfrak{M}^\times$) und Spalten (d.h. Rechtsmultiplikation mit $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathfrak{M}^\times$) verwandeln wir M in $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mit $a \in \mathfrak{o}^\times$ und $b,c,d \in \mathfrak{o}$. Durch Addition eines geeigneten Vielfachen der ersten Zeile zur zweiten (Multiplikation von links mit $\begin{pmatrix} 1 & 0 \\ e & 1 \end{pmatrix} \in \mathfrak{M}^\times$) und Addition eines geeigneten Vielfachen der ersten Spalte zur zweiten (Multiplikation von rechts mit $\begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} \in \mathfrak{M}^\times$) erhalten wir dann $\begin{pmatrix} a & 0 \\ 0 & g \end{pmatrix}$ mit $g \in \mathfrak{o}$. Wenn wir schließlich erste und zweite Zeile mit geeigneten Einheiten aus $\mathfrak{o}$ multiplizieren (Multiplikation mit $\begin{pmatrix} a^{-1} & 0 \\ 0 & h \end{pmatrix} \in \mathfrak{M}^\times$), erhalten wir $\begin{pmatrix} 1 & 0 \\ 0 & \pi^r \end{pmatrix}$ mit $r \in \mathbb{N}_0$. Zusammengefaßt:

Es gibt $E,F \in \mathfrak{M}^\times$ und $r \in \mathbb{N}_0$ mit $EMF = \begin{pmatrix} 1 & 0 \\ 0 & \pi^r \end{pmatrix}$.

Dann ist $E\mathfrak{M}E^{-1} = \mathfrak{M} = \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{o} \end{pmatrix}$.

und
$$\begin{aligned} E\mathfrak{M}'E^{-1} &= EM\mathfrak{M}M^{-1}E^{-1} \\ &= EMF\mathfrak{M}F^{-1}M^{-1}E^{-1} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & \pi^r \end{pmatrix}\begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{o} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \pi^{-r} \end{pmatrix} \\ &= \begin{pmatrix} \mathfrak{o} & \pi^{-r}\mathfrak{o} \\ \pi^r\mathfrak{o} & \mathfrak{o} \end{pmatrix} \end{aligned}$$

Die erste Behauptung wird dann durch die Matrizeseinheiten $E^{-1}M_{ij}E$ $(i,j \in \{1,2\})$ erfüllt.

$N(\mathfrak{M}\mathfrak{M}') = \pi^{-r}\mathfrak{o}$ folgt durch direkte Rechnung (siehe 10.12.ii).

Der Beweis stammt aus /7/ S. 135 (Bew. von Satz 7).

(11.2) Definition: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper, Q eine k-Quaternionenalgebra, K halbeinfache, quadratische Erweiterung von k mit $k \subset K \subset Q$. Sei $\mathcal{O}$ eine K-Ordnung, $\mathfrak{M}$ eine Q-Maximalordnung. Dann heißt $\mathcal{O}$ optimal eingebettet in $\mathfrak{M}$, wenn $\mathfrak{M} \cap K = \mathcal{O}$. Wir sagen dann auch: $\mathcal{O}$ liegt optimal in $\mathfrak{M}$; oder: $\mathfrak{M}$ enthält $\mathcal{O}$ optimal.

(11.3) Lemma: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper, Q eine k-Quaternionenalgebra, K halbeinfache quadratische Erweiterung von k mit Hauptordnung $\mathcal{O}$. Sei $k \subset K \subset Q$.
Dann gibt es eine Q-Maximalordnung $\mathfrak{M}$, die $\mathcal{O}$ optimal enthält.

Bew.: Sei $\mathfrak{M}'$ eine beliebige Q-Maximalordnung. Dann ist $\mathfrak{M}'\mathfrak{O}$ ein $\mathfrak{M}'$-Linksideal. Die Rechtsordnung $\mathfrak{M}$ von $\mathfrak{M}'\mathfrak{O}$ ist Q-Maximalordnung (9.2) und offensichtlich ist $\mathfrak{O} \subset \mathfrak{M} \cap K$. Außerdem ist $\mathfrak{M} \cap K$ eine K-Ordnung, also $\mathfrak{M} \cap K \in \mathfrak{O}$. (Jede Maximalordnung, die die Hauptordnung $\mathfrak{O}$ enthält, enthält $\mathfrak{O}$ optimal.)
Der Beweis stammt von E. Artin, siehe /9/ S. 12 Satz 1.

(11.4) Lemma: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$, sei Q eine k-Quaternionenalgebra und sei K halbeinfache quadratische Erweiterung von k mit $k \subset K \subset Q$. Sei $\mathfrak{M}$ eine Q-Maximalordnung und $\mathfrak{O}$ eine K-Ordnung. Wenn $\mathfrak{M} \cap K = \mathfrak{O}$, dann ist notwendig $f(\mathfrak{O}) + D_k(Q) = \mathfrak{o}$. (d.h. $f(\mathfrak{O})$ ist prim zu $D_k(Q)$)

Bew.: Wegen Satz (6.3) und Satz (4.17) brauchen wir nur den Fall zu untersuchen, daß k ein $\mathfrak{p}$-adischer Zahlkörper ist. Sei $\mathfrak{p}$ das Primideal von k. Wenn $\mathfrak{p} | D_k(Q)$, ist Q Divisionsalgebra (9.12). Dann ist $\mathfrak{M}$, die Menge der über $\mathfrak{o}$ ganzen Größen aus Q, die einzige Q-Maximalordnung (9.11.i). Sie enthält die Hauptordnung von K, also ist $\mathfrak{O}$ die Hauptordnung von K, d.h. $f(\mathfrak{O}) = \mathfrak{o}$.
Der Beweis stammt aus /7/ S. 134 (Bew. von Satz 6)

(11.5) Lemma: Sei k ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und Primelement π. Sei Q eine k-Quaternionenalgebra, sei $Q \underset{k}{\cong} M_2(k)$.
Sei K halbeinfache quadratische Erweiterung von k mit $k \subset K \subset Q$.
Dann gebt es ein System $\{\mathfrak{M}_i \mid i \in \mathbb{N}_0\}$ von Q-Maximalordnungen mit
$f(\mathfrak{M}_i \cap K) = \pi^i \mathfrak{o}$ und $N(\mathfrak{M}_i \mathfrak{M}_j) = \pi^{-|i-j|} \mathfrak{o}$ für $i,j \in \mathbb{N}_0$.

Bew.: Nach (11.3) gibt es eine Q-Maximalordnung $\mathfrak{M}$ mit $\mathfrak{M} \cap K = \mathfrak{O}^{\mathfrak{o}}(K)$.
Nach (9.10) gibt es Matrizeseinheiten $\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix} \in Q$
mit $\mathfrak{M} = \begin{pmatrix}\mathfrak{o}&\mathfrak{o}\\\mathfrak{o}&\mathfrak{o}\end{pmatrix}$. Sei $\{1,\omega\}$ eine Basis von $\mathfrak{O}^{\mathfrak{o}}(K)$ über $\mathfrak{o}$;
sei $\omega = \begin{pmatrix}a&b\\\pi^r c&d\end{pmatrix}$ mit $a,b,c,d \in \mathfrak{o}$ und $r \in \mathbb{N}_0$.
Wir können o.B.d.A. annehmen, daß $c \in \mathfrak{o}^\times$. (Falls $c = 0$, konjugieren wir die Matrizeseinheiten mit einem geeigneten $E \in \mathfrak{M}^\times$.)

Wir setzen $\mathfrak{M}_i := \begin{pmatrix}\mathfrak{o}&\pi^{-r-i}\mathfrak{o}\\\pi^{r+i}\mathfrak{o}&\mathfrak{o}\end{pmatrix}$ für $i \in \mathbb{N}_0$.

Für $i \in \mathbb{N}_0$ gilt dann offensichtlich: $\pi^i \omega \in \mathfrak{M}_i$, aber $\pi^{i-1}\omega \notin \mathfrak{M}_i$.

Also ist $f(\mathfrak{M}_i \cap K) = \pi^i \mathfrak{o}$ (siehe 6.7.a und c)

Direkte Rechnung zeigt: $N(\mathfrak{M}_i \mathfrak{M}_j) = \pi^{-|i-j|}\mathfrak{o}$ für $i,j \in \mathbb{N}_0$ (siehe 10.12.ii).

(11.6) Lemma: Sei k ein $\mathfrak{p}$-adischer Zahlkörper, Q eine k-Quaternionenalgebra, sei $Q \underset{K}{\cong} M_2(k)$ und sei K halbeinfache quadratische Erweiterung von k mit $k \subset K \subset Q$. Seien $\mathfrak{M}$ und $\mathfrak{M}'$ zwei Q-Maximalordnungen.
Genau dann ist $\mathfrak{M} \cap K = \mathfrak{M}' \cap K$, wenn es $M \in K^\times$ gibt mit $\mathfrak{M}' = M \mathfrak{M} M^{-1}$.

Bew.: i) Sei $\mathfrak{M}' = M \mathfrak{M} M^{-1}$ mit $M \in K^\times$. Dann ist
$\mathfrak{M}' \cap K = M \mathfrak{M} M^{-1} \cap K = M \mathfrak{M} M^{-1} \cap MKM^{-1} = M(\mathfrak{M} \cap K) M^{-1} = \mathfrak{M} \cap K$.
ii) Sei $\mathfrak{O} := \mathfrak{M} \cap K = \mathfrak{M}' \cap K$. Sei $\mathfrak{o}$ die Hauptordnung von k und π ein Primelement von $\mathfrak{o}$. Nach (11.1) gibt es Matrizeseinheiten
$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in Q$ und $r \in \mathbb{N}_0$, so daß $\mathfrak{M} = \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{o} \end{pmatrix}$
und $\mathfrak{M}' = \begin{pmatrix} \mathfrak{o} & \pi^{-r}\mathfrak{o} \\ \pi^r\mathfrak{o} & \mathfrak{o} \end{pmatrix}$. Es ist $\mathfrak{M}' = A \mathfrak{M} A^{-1}$ mit $A = \begin{pmatrix} 1 & 0 \\ 0 & \pi^r \end{pmatrix}$.
Sei o.B.d.A. $\mathfrak{M} \neq \mathfrak{M}'$, d.h. $r > 0$.
Sei $\{1, \omega\}$ Basis von $\mathfrak{O}$ über $\mathfrak{o}$ (6.7.ii) mit $\omega = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Wir können o.B.d.A. annehmen, daß $d = 0$ (wir ersetzen ω durch $\omega - d$).
Wegen $\omega \in \mathfrak{M} \cap \mathfrak{M}'$ sind $a, b, \pi^{-r}c \in \mathfrak{o}$.
Es ist $\pi^{-1}\omega \notin \mathfrak{O}$, nach Voraussetzung also $\pi^{-1}\omega \notin \mathfrak{M}$ und $\pi^{-1}\omega \notin \mathfrak{M}'$.
Damit haben wir: $a\mathfrak{o} + b\mathfrak{o} + c\mathfrak{o} = a\mathfrak{o} + \pi^r b\mathfrak{o} + \pi^{-r}c\mathfrak{o} = \mathfrak{o}$.

Daraus folgt: $a\mathfrak{o} + b\mathfrak{o} = a\mathfrak{o} + \pi^{-r}c\mathfrak{o} = \mathfrak{o}$ (11.7)

Wenn es $M \in K^\times$ gibt mit $M\mathfrak{M} = A\mathfrak{M}$, folgt die Behauptung.
Denn für die Linksordnung dieses Ideals gilt dann: $M\mathfrak{M}M^{-1} = A\mathfrak{M}A^{-1} = \mathfrak{M}'$.
Wir wollen also $M \in K^\times$ finden mit $A^{-1}M \in \mathfrak{M}^\times$.
Dazu machen wir den Ansatz $M = \pi^r e + \omega$ mit $e \in \mathfrak{o}$. Dann ergibt sich:

$$A^{-1}M = \begin{pmatrix} 1 & 0 \\ 0 & \pi^{-r} \end{pmatrix} \begin{pmatrix} a + \pi^r e & b \\ c & \pi^r e \end{pmatrix} = \begin{pmatrix} a + \pi^r e & b \\ \pi^{-r}c & e \end{pmatrix} \in \mathfrak{M}.$$

Wir müssen also nur noch erreichen, daß die Determinante
$ae + \pi^r e^2 - b\pi^{-r}c$ in $\mathfrak{o}^\times$ liegt.
Falls $b\pi^{-r}c \in \mathfrak{o}^\times$, können wir $e = 0$ setzen.
Falls $b\pi^{-r}c \notin \mathfrak{o}^\times$, ist $b \notin \mathfrak{o}^\times$ oder $\pi^{-r}c \notin \mathfrak{o}^\times$; nach (11.7) also $a \in \mathfrak{o}^\times$ und wir können $e = 1$ setzen.
Der Beweis stammt (mit einer kleinen Änderung) aus /7/ S.135 (Bew. von Satz 7).

(11.8) Lemma: Sei k ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und Primelement π. Sei Q eine k-Quaternionenalgebra mit $Q \underset{k}{\cong} M_2(k)$.
Sei K eine halbeinfache quadratische Erweiterung von k mit $k \subset K \subset Q$.
Seien $i, j \in \mathbb{N}_0$ und sei $\mathfrak{M}$ eine Q-Maximalordnung mit $f(\mathfrak{M} \cap K) = \pi^i\mathfrak{o}$.
Dann gibt es eine Q-Maximalordnung $\mathfrak{M}'$ mit $f(\mathfrak{M}' \cap K) = \pi^j\mathfrak{o}$, so daß außerdem gilt: $N(\mathfrak{M}\mathfrak{M}') = \pi^{-|i-j|}\mathfrak{o}$.

Bew.: Nach (11.5) gibt es Q-Maximalordnungen $\mathfrak{M}_i$ und $\mathfrak{M}_j$ mit $N(\mathfrak{M}_i\mathfrak{M}_j) = \pi^{-|i-j|}\mathfrak{o}$, so daß $f(\mathfrak{M}_i \cap K) = \pi^i\mathfrak{o}$ und $f(\mathfrak{M}_j \cap K) = \pi^j\mathfrak{o}$. Nach (11.6) gibt es $M \in K^\times$ mit $\mathfrak{M} = M\mathfrak{M}_iM^{-1}$. Wir setzen $\mathfrak{M}' = M\mathfrak{M}_jM^{-1}$. Nach (11.6) gilt dann $f(\mathfrak{M}' \cap K) = \pi^j\mathfrak{o}$. Außerdem gilt: $N(\mathfrak{M}\mathfrak{M}') = N(M\mathfrak{M}_iM^{-1}M\mathfrak{M}_jM^{-1}) = N(M)N(\mathfrak{M}_i\mathfrak{M}_j)N(M)^{-1} = \pi^{-|i-j|}\mathfrak{o}$.

(11.9) Satz: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei Q eine k-Quaternionenalgebra. Sei K halbeinfache quadratische Erweiterung von k mit $k \subset K \subset Q$. Sei $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal mit $\mathfrak{f} + D_k(Q) = \mathfrak{o}$. Dann gilt:

i) Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{M} \cap K = \mathcal{O}^{\mathfrak{f}}(K) = \mathcal{O}^{\mathfrak{f}}$ und sei $\mathfrak{f}'$ ein ganzes $\mathfrak{o}$-Ideal mit $\mathfrak{f}' + D_k(Q) = \mathfrak{o}$. Dann gibt es eine Q-Maximalordnung $\mathfrak{M}'$ mit $\mathfrak{M}' \cap K = \mathcal{O}^{\mathfrak{f}'}$ und $N(\mathfrak{M}\mathfrak{M}') = \mathfrak{f}^{-1}\mathfrak{f}' + \mathfrak{f}\mathfrak{f}'^{-1}$, also insbesondere $N(\mathfrak{M}\mathfrak{M}')\mathfrak{f}\mathfrak{f}'^{-1} \in I^{k(2)}$.

ii) Es gibt eine Q-Maximalordnung $\mathfrak{M}$ mit $\mathfrak{M} \cap K = \mathcal{O}^{\mathfrak{f}}$.

iii) Seien $\mathfrak{M}$ und $\mathfrak{M}'$ zwei Q-Maximalordnungen mit $\mathfrak{M} \cap K = \mathfrak{M}' \cap K = \mathcal{O}^{\mathfrak{f}}$. Dann gibt es $\alpha \in I^{\mathfrak{f}}$ mit $\mathfrak{M}' = \alpha\mathfrak{M}\alpha^{-1}$.

iv) Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{M} \cap K = \mathcal{O}^{\mathfrak{f}}$ und sei $\alpha \in I^{\mathfrak{f}}$. Dann ist $\alpha\mathfrak{M}\alpha^{-1} \cap K = \mathcal{O}^{\mathfrak{f}}$.

Bew.: i) Sei $\mathfrak{p}$ ein Primteiler von $\mathfrak{f}\mathfrak{f}'$ mit $\mathfrak{f}_\mathfrak{p} = \mathfrak{p}^i\mathfrak{o}_\mathfrak{p}$ und $\mathfrak{f}'_\mathfrak{p} = \mathfrak{p}^j\mathfrak{o}_\mathfrak{p}$. Wegen $\mathfrak{p} \nmid D_k(Q)$ ist $Q_\mathfrak{p} \cong_{k_\mathfrak{p}} M_2(k_\mathfrak{p})$. $\mathfrak{M}_\mathfrak{p}$ ist $Q_\mathfrak{p}$-Maximalordnung, die $\mathcal{O}^{\mathfrak{f}}_\mathfrak{p}$ optimal enthält. Nach (11.8) gibt es eine $Q_\mathfrak{p}$-Maximalordnung $\mathfrak{M}^\mathfrak{p}$, die $\mathcal{O}^{\mathfrak{f}'}_\mathfrak{p}$ optimal enthält und daß gilt $N(\mathfrak{M}_\mathfrak{p}\mathfrak{M}^\mathfrak{p}) = \mathfrak{p}^{-|i-j|}\mathfrak{o}_\mathfrak{p}$. Wir definieren nun die Q-Maximalordnung $\mathfrak{M}'$ durch die Vorschriften (siehe 9.6.ii): $\mathfrak{M}'_\mathfrak{p} := \mathfrak{M}^\mathfrak{p}$ für $\mathfrak{p} \mid \mathfrak{f}\mathfrak{f}'$ und $\mathfrak{M}'_\mathfrak{p} = \mathfrak{M}_\mathfrak{p}$ für alle endlichen Primstellen $\mathfrak{p}$ von k mit $\mathfrak{p} \nmid \mathfrak{f}\mathfrak{f}'$. Die Beh. folgt sofort.

ii) Nach (11.3) gibt es eine Q-Maximalordnung $\mathfrak{M}$ mit $\mathfrak{M} \cap K = \mathcal{O}^{\mathfrak{o}}$. Nach i) gibt es eine Q-Maximalordnung $\mathfrak{M}'$ mit $\mathfrak{M}' \cap K = \mathcal{O}^{\mathfrak{f}}$. (Ersetze in i) $\mathfrak{f}$ durch $\mathfrak{o}$ und $\mathfrak{f}'$ durch $\mathfrak{f}$)

iii) Für fast alle endlichen Primstellen $\mathfrak{p}$ von k ist $\mathfrak{M}_\mathfrak{p} = \mathfrak{M}'_\mathfrak{p}$ nach (4.15.iii). Für $\mathfrak{p} \mid D_K(Q)$ ist $Q_\mathfrak{p}$ Divisionsalgebra, also $\mathfrak{M}_\mathfrak{p} = \mathfrak{M}'_\mathfrak{p}$ nach Satz (9.11.i)

Sei $\mathfrak{p}$ eine endliche Primstelle von k mit $\mathfrak{M}_\mathfrak{p} \neq \mathfrak{M}'_\mathfrak{p}$. Dann ist $Q_\mathfrak{p} \cong_{k_\mathfrak{p}} M_2(k_\mathfrak{p})$ und $\mathfrak{M}_\mathfrak{p} \cap K_\mathfrak{p} = \mathfrak{M}'_\mathfrak{p} \cap K_\mathfrak{p}$. Nach Satz (11.6) gibt es $M_\mathfrak{p} \in K_\mathfrak{p}^\times$ mit $\mathfrak{M}'_\mathfrak{p} = M_\mathfrak{p}\mathfrak{M}_\mathfrak{p}M_\mathfrak{p}^{-1}$. Wir definieren nun $\alpha \in I^{\mathfrak{f}}$ durch folgende Vorschriften (siehe 7.3.ii): Ist $\mathfrak{p}$ eine endliche Primstelle von k mit $\mathfrak{M}_\mathfrak{p} \neq \mathfrak{M}'_\mathfrak{p}$, so sei $\alpha_\mathfrak{p} := M_\mathfrak{p}\mathcal{O}^{\mathfrak{f}}_\mathfrak{p}$.

Ist $\mathfrak{p}$ eine endliche Primstelle von k mit $\mathfrak{M}_\mathfrak{p} = \mathfrak{M}'_\mathfrak{p}$, so sei $\mathfrak{a}_\mathfrak{p} := \mathfrak{O}_\mathfrak{p}^\times$.
Dann ergibt sich:
für $\mathfrak{M}_\mathfrak{p} \neq \mathfrak{M}'_\mathfrak{p}$: $(\mathfrak{a}\,\mathfrak{M}\,\mathfrak{a}^{-1})_\mathfrak{p} = M_\mathfrak{p}\mathfrak{O}_\mathfrak{p}^\times\mathfrak{M}_\mathfrak{p}(M_\mathfrak{p}\mathfrak{O}_\mathfrak{p}^\times)^{-1} = M_\mathfrak{p}\mathfrak{M}_\mathfrak{p}M_\mathfrak{p}^{-1} = \mathfrak{M}'_\mathfrak{p}$;
für $\mathfrak{M}_\mathfrak{p} = \mathfrak{M}'_\mathfrak{p}$: $(\mathfrak{a}\,\mathfrak{M}\,\mathfrak{a}^{-1})_\mathfrak{p} = \mathfrak{O}_\mathfrak{p}^\times\mathfrak{M}_\mathfrak{p}\mathfrak{O}_\mathfrak{p}^\times = \mathfrak{M}_\mathfrak{p} = \mathfrak{M}'_\mathfrak{p}$.
Insgesamt gilt also $\mathfrak{a}\,\mathfrak{M}\mathfrak{a}^{-1} = \mathfrak{M}'$.
iv) Sei $\mathfrak{p}$ eine endliche Primstelle von k und $\mathfrak{a}_\mathfrak{p} = a\,\mathfrak{O}_\mathfrak{p}^\times$ mit $a \in K_\mathfrak{p}^\times$.
Dann ist $(\mathfrak{a}\,\mathfrak{M}\mathfrak{a}^{-1} \cap K)_\mathfrak{p} = (\mathfrak{a}\,\mathfrak{M}\,\mathfrak{a}^{-1})_\mathfrak{p} \cap K_\mathfrak{p}$
$= a\mathfrak{M}_\mathfrak{p}a^{-1} \cap K_\mathfrak{p}$
$= (\mathfrak{a}(\mathfrak{M} \cap K)\mathfrak{a}^{-1})_\mathfrak{p}$
Insgesamt ergibt sich also:
$\mathfrak{a}\,\mathfrak{M}\mathfrak{a}^{-1} \cap K = \mathfrak{a}(\mathfrak{M} \cap K)\mathfrak{a}^{-1} = \mathfrak{a}\mathfrak{O}^\times\mathfrak{a}^{-1} = \mathfrak{O}^\times$.

(11.10) Lemma: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper. Sei Q eine k-Quaternionenalgebra. Sei K halbeinfache quadratische Erweiterung von k mit $k \subset K \subset Q$. Sei $\mathfrak{M}$ eine Q-Maximalordnung und $\mathfrak{O} := \mathfrak{M} \cap K$. Sei $\mathfrak{a}$ ein $\mathfrak{O}$-Ideal. Dann ist $N(\mathfrak{M}\mathfrak{a}) = N(\mathfrak{a}\,\mathfrak{M}) = N(\mathfrak{a})$

Bew.: Nach Definition der Norm können wir uns darauf beschränken, den Fall zu untersuchen, daß k ein $\mathfrak{p}$-adischer Zahlkörper ist.
Sei $\mathfrak{a} = a\mathfrak{O}$ mit $a \in K^\times$. Dann ist $N(\mathfrak{M}\,\mathfrak{a}) = N(\mathfrak{M}\,a\,\mathfrak{O}) = N(\mathfrak{M}a) =$
$= N(a)\mathfrak{o} = N(a\mathfrak{O}) = N(\mathfrak{a})$.

Teil II

Die binären Polyedergruppen in Quaternionenalgebren

Ist $\mathfrak{M}$ eine Maximalordnung der Quaternionenalgebra Q und G eine endliche Untergruppe von $\Gamma(\mathfrak{M})$, dann ist natürlich G in der Norm-Eins-Gruppe $\Gamma(Q)$ enthalten.
Ist umgekehrt G eine endliche Untergruppe von $\Gamma(Q)$, so läßt sich leicht zeigen, daß es eine Q-Maximalordnung $\mathfrak{M}$ mit $G \subset \Gamma(\mathfrak{M})$ gibt.
Es ist daher sinnvoll (bis zu einem gewissen Grad), die endlichen Untergruppen von $\Gamma(Q)$ zu untersuchen, ohne auf die speziellen Maximalordnungen Rücksicht zu nehmen.
Diese Untersuchung führe ich in Teil II.
Ich gebe nun eine Inhaltsübersicht von Teil II:
1. Ich betrachte nur solche Gruppen G, die das Zentrum $\{\pm 1\}$ von $\Gamma(Q)$ als echte Untergruppe enthalten.
Ist k algebraischer Zahlkörper, so kann man wegen $Q \otimes_k \mathbb{C} \cong M_2(\mathbb{C})$ jede endliche Untergruppe von $\Gamma(Q)$ als endliche Untergruppe von $SL(2,\mathbb{C})$ auffassen; sie ist also, wie bekannt (12.4), eine binäre Polyedergruppe (Def. 12.3). Das Beiwort "binär" bei den Polyedergruppen lasse ich i.a. weg.
Ich definiere Polyedergruppen als Untergruppen von $\Gamma(Q)$, die von Elementen mit bestimmten Relationen erzeugt werden. (Dabei ist Q eine Quaternionenalgebra über einem beliebigen Körper, d.h. über $\mathbb{R}$, $\mathbb{C}$, über einem algebraischen oder $\mathfrak{p}$-adischen Zahlkörper.)
Dann leite ich Satz (12.6) (und weiter Satz (12.8)) her, in dem ich die Existenz von speziellen Erzeugenden (mit vorgegebener Spur usw.) für Polyedergruppen nachweise. In Zukunft dient meistens Satz (12.6) (bzw. (12.8)) praktisch als Definition für binäre Polyedergruppen.
Aus diesem Satz geht dann mit Hilfe von (3.3) sofort hervor, daß isomorphe Polyedergruppen $Q^\times$-konjugiert sind (12.9).
Bemerkung: Daß eine binäre Polyedergruppe spezielle Erzeugende besitzt, wie sie in (12.6) bzw. (12.8) angegeben werden, ist für Unterkörper von $\mathbb{C}$ wohlbekannt (siehe /20/). Die aufwendige Rechnung bei der Herleitung von (12.6) bzw. (12.8) schien mir der einzige Weg zu sein, den Satz auch für $\mathfrak{p}$-adische Zahlkörper zu zeigen.
Für $n \in \mathbb{N}$ bezeichne ich mit ζ_n die normierte n-te Einheitswurzel $e^{2\pi i/n} \in \mathbb{C}$.
Ist Q eine Quaternionenalgebra über einem algebraischen Zahlkörper k und enthält $\Gamma(Q)$ eine zyklische Gruppe der Ordnung n, so muß notwendig $\zeta_n + \zeta_n^{-1} \in k$ sein (12.7). Für die anderen Polyedergruppen gilt eine entsprechende notwendige Bedingung an k. (12.7) folgt leicht aus (12.6).

2. In § 13 untersuche ich zuerst genau, welche endlichen Untergruppen $\Gamma(Q)$ enthält, wenn Q eine Quaternionenalgebra über einem algebraischen Zahlkörper ist. $\Gamma(Q)$ enthält genau dann eine zyklische Gruppe der Ordnung 2n, wenn sich $K := k[X]/(X^2 - (\zeta_{2n} + \zeta_{2n}^{-1})X + 1)k[X]$ in Q einbetten läßt, also (5.6) genau dann, wenn alle Primteiler von $D_k(Q)$ in K träge oder verzweigt sind. (13.2)
Ist $G \subset \Gamma(Q)$ endlich und nicht zyklisch, so enthält G eine Basis von Q über k. Es folgt nun leicht, daß es bis auf Isomorphie nur eine Quaternionenalgebra Q über k geben kann, für die $\Gamma(Q)$ eine bestimmte nichtzyklische Polyedergruppe enthält (13.3).
Im Rest von § 13 bestimme ich die Verzweigungsstellen der Quaternionenalgebren Q, für die $\Gamma(Q)$ nichtzyklische Polyedergruppen G enthält (Sätze 13.4 und 13.8). Beim Beweis nutze ich aus, daß die Diskriminante $D_k(Q)$ Teiler von $D_k(1,E,B,EB)$ ist (dabei sind E, B Erzeuger einer in G gelegenen Diedergruppe). Ich brauche daher nur das Verzweigungsverhalten von Q an endlich vielen Stellen zu untersuchen.
Satz 13.4 und die anderen Ergebnisse des § 13 sind mir aus der Literatur nicht bekannt.
3. In der ganzen Arbeit benutze ich imaginärquadratische Zahlkörper als Beispiele für die allgemeinen Sätze. In § 14 konkretisiere ich die Ergebnisse der Paragrafen 12 und 13 für imaginärquadratische Zahlkörper.
Ist Q Quaternionenalgebra über einem imaginärquadratischen Zahlkörper k, so muß jede endliche Untergruppe $G \supsetneq \{\pm 1\}$ von $\Gamma(Q)$ entweder zyklisch von der Ordnung 4 oder 6, eine 2-Dieder-, 3-Dieder- oder Tetraedergruppe sein (14.1).
Die Sätze (14.5) und (14.6) beschreiben, welche Bedingungen Q erfüllen muß, damit $\Gamma(Q)$ eine 4-zyklische bzw. 6-zyklische Untergruppe enthält. Über jedem imaginärquadratischen Zahlkörper gibt es bis auf Isomorphie genau eine Quaternionenalgebra Q, so daß $\Gamma(Q)$ 2-Dieder- und Tetraedergruppen enthält, und genau eine Quaternionenalgebra Q, so daß $\Gamma(Q)$ 3-Diedergruppen enthält. Diese Algebren werden in (14.7) und (14.8) beschrieben.

§ 12 . Die (binären) Polyedergruppen

Zwei (binäre) Polyedergruppen in der Norm-Eins-Gruppe $\Gamma(Q)$ sind $Q^\times$-konjugiert, wenn sie isomorph sind (12.9). Dies gilt für Quaternionenalgebren über $\mathbb{R}$, $\mathbb{C}$, über algebraischen und p-adischen Zahlkörpern.
Zur Vorbereitung dieses Satzes dient Satz (12.6) (bzw. (12.8)), in dem wir die Existenz von speziellen Erzeugenden für (binäre) Polyedergruppen nachweisen. Satz (12.6) (bzw.(12.8)) wird später immer wieder gebraucht (er ersetzt praktisch die Definition der Polyedergruppen (12.3)).
Ein weiteres wichtiges Ergebnis ist Satz (12.7): Ein algebraischer Zahlkörper k muß eine notwendige Bedingung erfüllen, damit $\Gamma(Q)$ eine bestimmte Polyedergruppe enthalten kann.

(12.1) Definition: Sei k Körper, Q eine k-Quaternionenalgebra. Dann definieren wir: $\Gamma(Q) := \{M \in Q \mid N(M) = 1\}$.

(12.2) Lemma: Unter den Voraussetzungen von (12.1) ist $\Gamma(Q)$ eine Untergruppe von $Q^\times$. Für $M \in \Gamma(Q)$ ist $M^{-1} = \overline{M}$. Es ist $\Gamma(Q) \cap k = \{\pm 1\}$.

Beweis: Die ersten beiden Behauptungen sind klar.
Sei $M \in k$. Dann ist $M \in \Gamma(Q)$ äquivalent zu $M^2 = N(M) = 1$, d.h. $M = \pm 1$.

Wir wollen die endlichen Untergruppen G von $\Gamma(Q)$ mit $\{\pm 1\} \subsetneq G$ bestimmen für den Fall, daß k algebraischer Zahlkörper ist.

(12.3) Definition: Sei k Körper, Q eine k-Quaternionenalgebra.
i) Sei $n \in \mathbb{N}$, $n \geq 2$. Ist G eine zyklische Untergruppe der Ordnung 2n von $\Gamma(Q)$, so nennen wir G eine (binäre) 2n-zyklische Gruppe.
ii) Sei $n \in \mathbb{N}$, $n \geq 2$. Eine (endliche) Untergruppe $G \subset \Gamma(Q)$ heißt (binäre) n-Diedergruppe, wenn sie von zwei Elementen E,B erzeugt wird, für die gilt: E hat Ordnung 2n, B hat Ordnung 4, $BEB^{-1} = E^{-1}$.
iii) Eine Untergruppe $G \subset \Gamma(Q)$ heißt (binäre) Tetraedergruppe, wenn sie von drei Elementen U,V,T erzeugt wird, für die gilt: U und V haben Ordnung 4, T hat Ordnung 6, $VUV^{-1} = U^{-1}$, $UT^{-1}U^{-1} = VT^{-1}$, $T^{-1}V = UT^{-1}$.
iv) Eine Untergruppe $G \subset \Gamma(Q)$ heißt (binäre) Oktaedergruppe, wenn sie von drei Elementen U',V,T erzeugt wird, so daß $U := U'^2$,V,T die gleichen Relationen wie in iii) angegeben erfüllen.
v) Eine Untergruppe $G \subset \Gamma(Q)$ heißt (binäre) Ikosaedergruppe, wenn sie von drei Elementen A,B,C erzeugt wird, für die gilt: A hat Ordnung 10, B und C haben Ordnung 4, $BAB^{-1} = A^{-1}$, $BCB^{-1} = C^{-1}$, $CAC = ACBA$, $CA^2C = A^{-2}CA^{-2}$.
vi) Ist $G \subset \Gamma(Q)$ eine der in i) - v) definierten Gruppen, dann heißt G (binäre) Polyedergruppe.

Bemerkung: Sei $n \in \mathbb{N}$, $n \geq 3$. Ist G eine 2n-zyklische Gruppe, so ist $G/\{\pm 1\}$ zyklisch der Ordnung n und daher isomorph zu der Gruppe der Drehungen der Ebene, die ein reguläres n-Eck in sich überführen. Ist G eine (binäre) n-Diedergruppe, so ist $G/\{\pm 1\}$ isomorph zur Gruppe der Drehungen und Spiegelungen der Ebene, die ein reguläres n-Eck in sich überführen. Ist G eine (binäre) Tetraedergruppe, so ist $G/\{\pm 1\}$ isomorph zur Gruppe der Drehungen des Raumes, die ein (reguläres) Tetraeder in sich überführen. Ist G eine binäre Oktaedergruppe (Ikosaedergruppe), so ist $G/\{\pm 1\}$ isomorph zur Gruppe der Drehungen des Raumes, die ein Oktaeder oder einen Würfel (Ikosaeder oder Dodekaeder) in sich überführen.

Achtung! Wir werden in Zukunft das Beiwort "binär" bei den binären Polyedergruppen fortlassen.

(12.4) Lemma:
i) Die verschiedenen in (12.3) definierten Polyedergruppen sind paarweise nicht isomorph.
ii) $SL(2,\mathbb{C}) = \Gamma(M_2(\mathbb{C}))$ enthält Tetraeder-, Oktaeder- und Ikosaedergruppen sowie für alle $n \in \mathbb{N}$, $n \geq 2$ auch 2n-zyklische Gruppen und n-Diedergruppen.
iii) Ist G eine endliche Untergruppe von $SL(2,\mathbb{C})$, $\{\pm 1\} \subsetneq G$, so ist G eine Polyedergruppe.
iv) Ist k algebraischer Zahlkörper, Q eine k-Quaternionenalgebra und G eine endliche Untergruppe von $\Gamma(Q)$ mit $\{\pm 1\} \subsetneq G$, dann ist G eine Polyedergruppe.

Bew.: i), ii), iii) siehe /20/ S. 86 -94. Man vergleiche dazu auch den nachfolgenden Satz (12.6).
iv) Bis auf Isomorphie ist $M_2(\mathbb{C})$ die einzige Quaternionenalgebra über $\mathbb{C}$ (siehe 1.16.ii). Daher ist $\mathbb{C} \otimes_k Q \cong_{\mathbb{C}} M_2(\mathbb{C})$ und wir können diese beiden Algebren miteinander identifizieren. Dann ist $Q \subset M_2(\mathbb{C})$ und die Norm auf $M_2(\mathbb{C})$ ist Fortsetzung der Norm auf Q. Also ist $\Gamma(Q) \subset SL(2,\mathbb{C})$ und die Behauptung folgt aus iii).

(12.5) Definition: Für $n \in \mathbb{N}$ sei $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$.

(12.6) Satz: Sei k algebraischer Zahlkörper, Q eine k-Quaternionenalgebra.
i) Sei $n \in \mathbb{N}$, $n \geq 2$. Genau dann ist $G \subset \Gamma(Q)$ eine 2n-zyklische Gruppe, wenn G von einem $E \in \Gamma(Q)$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$ erzeugt wird. G hat dann die Ordnung 2n und besteht genau aus den Elementen E^j mit $0 \leq j < 2n$.
Jedes dieser Elemente läßt sich auf eindeutige, von G unabhängige (nur von n und j abhängige) Weise als Linearkombination von 1 und E über k darstellen.

ii) Sei $n \in \mathbb{N}$, $n \geq 2$. Genau dann ist $G \subset \Gamma(Q)$ eine n-Diedergruppe, wenn G von zwei Elementen $E,B \in \Gamma(Q)$ erzeugt wird mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$, $S(B) = 0$, $BEB^{-1} = E^{-1}$. Dann ist $D_k(1,E,B,EB) = -(\zeta_{2n} - \zeta_{2n}^{-1})^4$, also ist $\{1,E,B,EB\}$ Basis von Q über k. G hat die Ordnung 4n und besteht genau aus den Elementen E^j, E^jB $(0 \leq j < 2n)$. Jedes dieser Elemente läßt sich auf eindeutige, von G unabhängige Weise als Linearkombination von 1,E,B und EB über k darstellen.

iii) Insbesondere wird eine 2-Diedergruppe $G \subset \Gamma(Q)$ erzeugt von zwei Elementen $U,V \in \Gamma(Q)$ mit $S(U) = S(V) = 0$ und $UV = -VU$. Es ist $D_k(1,U,V,UV) = -16$ und $G = \{\pm 1, \pm U, \pm V, \pm UV\}$.

iv) $G \subset \Gamma(Q)$ ist genau dann Tetraedergruppe, wenn G von drei Elementen $U,V,T \in \Gamma(Q)$ erzeugt wird mit $S(U) = S(V) = 0$, $UV = -VU$, $T = 1/2 \cdot (1 + U + V + UV)$.
Weitere Relationen sind dann: $TUT^{-1} = V$, $TVT^{-1} = UV$, $TUVT^{-1} = U$.
G hat die Ordnung 24 und zwar ist $G = \{\pm 1, \pm U, \pm V, \pm UV, 1/2 \cdot (\pm 1 \pm U \pm V \pm UV)\}$.
Es ist $D_k(1,U,V,T) = -4$.
(Wegen $TUT^{-1} = V$ wird G schon von den zwei Elementen U und T erzeugt.)

v) $G \subset \Gamma(Q)$ ist genau dann Oktaedergruppe, wenn G von zwei Elementen $U', V' \in \Gamma(Q)$ erzeugt wird mit $S(U') = S(V') = \sqrt{2}$ und $U'^2V'^2 = -V'^2U'^2$.
Dann ist $D_k(1,U',V',U'V') = -1$.
$U := U'^2$, $V := V'^2$ und $T := U'V'$ erzeugen eine Tetraedergruppe $G' \subset G$.
G hat die Ordnung 48 und zwar ist $G = G' \cup U'G'$.
Jedes Element aus G läßt sich auf eindeutige, von G unabhängige, Weise als Linearkombination von 1,U,V und UV über k darstellen.

vi) $G \subset \Gamma(Q)$ ist genau dann Ikosaedergruppe, wenn G von drei Elementen $A,B,C \in \Gamma(Q)$ erzeugt wird mit $S(B) = S(C) = 0$, $BC = -CB$ und $A = 1/4 \cdot (1 + \sqrt{5} + (1 - \sqrt{5})C - 2BC)$.
G hat dann die Ordnung 120 und besteht genau aus den Elementen A^h, BA^h, A^hCA^j, A^hCBA^j mit $0 \leq h < 10$, $0 \leq j < 5$. Jedes dieser Elemente läßt sich auf eindeutige, von G unabhängige Weise als Linearkombination von 1,B,C und BC über k darstellen.

Bew.: i) Sei $G \subset \Gamma(Q)$ eine 2n-zyklische Gruppe und E ein Erzeuger von G. Dann ist $E^{2n} - 1 = 0$. Da $E \in \Gamma(Q) - k$, ist das Minimalpolynom von E über k ein Polynom zweiten Grades mit dem letzten Koeffizienten 1. Also ist $E^2 - (\zeta + \zeta^{-1})E + 1 = 0$, wo ζ eine 2n-te Einheitswurzel in C ist. Da $2n = \min\{m \in \mathbb{N} \mid E^m = 1\}$, muß ζ eine primitive 2n-te Einheitswurzel sein. Wählt man unter den verschiedenen Erzeugern von G einen geeigneten aus, so erhält man: $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$.

Sei umgekehrt $E \in \Gamma(Q)$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$, also $E^2 - (\zeta_{2n} + \zeta_{2n}^{-1})E + 1 = 0$. Dann ist $E^{2n} - 1 = 0$ und $2n = \min\{m \in \mathbb{N} \mid E^m = 1\}$, also erzeugt E eine 2n-zyklische Gruppe $G = \{E^j \mid 0 \leq j < 2n\}$. Daß jedes E^j sich auf eindeutige, von G unabhängige Weise als Linearkombination von 1 und E über k darstellen läßt, folgt leicht durch Induktion aus: $E^2 = (\zeta_{2n} + \zeta_{2n}^{-1})E - 1$.

ii) Sei $G \subset \Gamma(Q)$ eine n-Diedergruppe. Seien E', B Erzeuger von G; E' habe Ordnung 2n, B habe Ordnung 4 und sei $BE'B^{-1} = E'^{-1}$.
E' erzeugt eine 2n-zyklische Gruppe G'. Für alle $E \in G'$ gilt: $BEB^{-1} = E^{-1}$.
Nach i) gibt es einen Erzeuger E von G' mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$.
Dann sind E und B Erzeuger von G. Da B die Ordnung 4 hat, folgt wie in i): $B^2 - (\zeta + \zeta^{-1})B + 1 = 0$, wo ζ primitive 4-te Einheitswurzel in $\mathbb{C}$ ist, also $\zeta = \pm i$. Daher $B^2 + 1 = 0$, also $S(B) = 0$.
Sind umgekehrt $E, B \in \Gamma(Q)$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$ und $S(B) = 0$, so erzeugen E,B eine n-Diedergruppe G (Beweis wie in i)). Weiter ist:

$1 \cdot 1 = 1$, $1 \cdot E = E$, $1 \cdot B = B$, $1 \cdot EB = EB$
$E \cdot 1 = E$, $E \cdot E = (\zeta_{2n} + \zeta_{2n}^{-1})E - 1$, $E \cdot B = EB$, $E \cdot EB = (\zeta_{2n} + \zeta_{2n}^{-1})EB - B$
$B \cdot 1 = B$, $B \cdot E = E^{-1}B$, $B \cdot B = -1$, $B \cdot EB = -E^{-1} = E - (\zeta_{2n} + \zeta_{2n}^{-1})$
$EB \cdot 1 = EB$, $EB \cdot E = B$, $EB \cdot B = -E$, $EB \cdot EB = -1$

Wegen $(EB)^2 = -1$ wird $S(EB) = 0$, genauso $S(E^{-1}B) = 0$. Also

$$D_k(1,E,B,EB) = \det \begin{pmatrix} 2 & \zeta_{2n} + \zeta_{2n}^{-1} & 0 & 0 \\ \zeta_{2n} + \zeta_{2n}^{-1} & (\zeta_{2n} + \zeta_{2n}^{-1})^2 - 2 & 0 & 0 \\ 0 & 0 & -2 & -(\zeta_{2n} + \zeta_{2n}^{-1}) \\ 0 & 0 & -(\zeta_{2n} + \zeta_{2n}^{-1}) & -2 \end{pmatrix}$$

$$= ((\zeta_{2n} + \zeta_{2n}^{-1})^2 - 4)(4 - (\zeta_{2n} + \zeta_{2n}^{-1})^2)$$
$$= -(\zeta_{2n} - \zeta_{2n}^{-1})^4$$

1, E, B, EB sind also linear unabhängig über k und wegen $[Q : k] = 4$ bilden sie eine Basis von Q über k. Daß die Darstellung der Elemente von $G = \{E^j, E^jB \mid 0 \leq j < 2n\}$ als Linearkombination von 1, E, B, EB über k unabhängig von der speziellen Gruppe G ist, folgt wieder leicht durch Induktion aus $E^2 = (\zeta_{2n} + \zeta_{2n}^{-1})E - 1$.

iii) Es ist $\zeta_4 = i$. Ist $U \in \Gamma(Q)$ von der Ordnung 4, so ist $S(U) = 0$, $U^2 = -1$ und $U^{-1} = -U$. Jetzt folgen die Behauptungen leicht aus ii).

iv) Sei $G \subset \Gamma(Q)$ Tetraedergruppe. Seien U,V,T Erzeugende von G; U und V haben Ordnung 4; T habe Ordnung 6; $VUV^{-1} = U^{-1}$; $UT^{-1}U^{-1} = VT^{-1}$; $T^{-1}V = UT^{-1}$.
Wie in iii) bemerkt, ist dann $S(U) = S(V) = 0$, $U^{-1} = -U$, $V^{-1} = -V$.
$VUV^{-1} = U^{-1}$ ist also äquivalent mit $UV = -VU$. U und V erzeugen eine 2-Diedergruppe, $\{1,U,V,UV\}$ ist eine Basis von Q über k.
Sei $T =: a + bU + cV + dUV$ mit $a,b,c,d \in k$, also $T^{-1} = T^{*} = a - bU - cV - dUV$.
Aus den beiden Relationen für T folgt dann:
$a - bU + cV + dUV = aV + bUV + c - dU$ und
$aV - bUV + c + dU = aU + b - cUV + dV$, also $a = b = c = d$.
Wegen $T \in \Gamma(Q)$ wird $a^2 + b^2 + c^2 + d^2 = N(T) = 1$ (vgl. (1.14), (1.18)),
also $a = \pm 1/2$; $S(T) = 2a = \pm 1$; $T^2 \mp T + 1 = 0$. Da T Ordnung 6 und nicht Ordnung 3 hat, wird $T^2 - T + 1 = 0$, also $T = 1/2 \cdot (1 + U + V + UV)$.
Umgekehrt erzeugen natürlich U,V,T mit den in (12.6.iv) genannten Eigenschaften eine Tetraedergruppe. Die weiteren Relationen und die Tatsache, daß $G = \{\pm 1, \pm U, \pm V, \pm UV, 1/2 \cdot (\pm 1 \pm U \pm V \pm UV)\}$, lassen sich leicht direkt nachrechnen.
Es ist $D_k(1,U,V,T) = 1/4 \cdot D_k(1,U,V,1+U+V+UV) = 1/4 \cdot D_k(1,U,V,UV) = -4$.
v) Sei $G \subset \Gamma(Q)$ Oktaedergruppe. Seien U',V,T Erzeuger von G, so daß mit $U =: U'^2$ gilt: $S(U) = S(V) = 0$, $UV = -VU$, $T = 1/2 \cdot (1 + U + V + UV)$.
(Ein solches Erzeugendensystem gibt es nach (iv))
Wegen $U \in k[U'] = k$ ist $k[U] = k[U']$ (vgl. (2.1) und (3.1)).
Seien $a, b \in k$ mit $U' = a + bU$. Dann ist $a^2 - b^2 + 2abU = U'^2 = U$,
also $a^2 = b^2$ und $2ab = 1$, also $4a^4 = 1$, d.h. $a = \pm 1/2 \cdot \sqrt{2}$ oder $a = \pm i/2 \cdot \sqrt{2}$.
Wäre $a = \pm i/2\sqrt{2}$, so wäre $a^2 + b^2 = N(U') = -1$. Es muß daher $a = \pm 1/2 \cdot \sqrt{2}$, $b = \pm 1/2\sqrt{2}$, $U' = \pm 1/2 \cdot \sqrt{2}(1 + U)$ sein. Wir können o.B.d.A. $U' = 1/2 \cdot \sqrt{2}(1 + U)$ annehmen (sonst ersetzen wir U' durch -U').
Wir erhalten $S(U') = \sqrt{2}$ und setzen $V' := TU'T^{-1} = 1/2 \cdot \sqrt{2}(1 + V)$.
Dann ist $S(V') = \sqrt{2}$; $V'^2 = V$; $U'V' = 1/2 \cdot (1 + U)(1 + V) = T$.
U' und V' erzeugen also G.
Es ist $D_k(1,U',V',U'V') = 1/2 \cdot 1/2 \cdot D_k(1,1+U,1+V,T) = 1/4 \cdot D_k(1,U,V,T) = -1$.
Die anderen Behauptungen sind jetzt leicht einzusehen.
vi) Sei $G \subset \Gamma(Q)$ Ikosaedergruppe. Seien A,B,C Erzeugende von G;
A habe Ordnung 10, B und C haben Ordnung 4; sei $BAB^{-1} = A^{-1}$, $BCB^{-1} = C^{-1}$, $CAC = ACBA$ und $CA^2C = A^{-2}CA^{-2}$.
Dann erzeugen B und C eine 2-Diedergruppe, also ist $S(B) = S(C) = 0$ und die Relation $CA^2C = A^{-2}CA^{-2}$ rechnet man leicht um in $(A^2C)^3 = -1$.
$\{1,B,C,BC\}$ ist eine Basis von Q über k. Seien $a,b,c,d \in k$ mit $A = a + bB + cC + dBC$. Dann ist $A^{-1} = a - bB - cC - dBC$.
Aus $BAB^{-1} = A^{-1}$ folgt: $a + bB - cC - dBC = a - bB - cC - dBC$, also $b = 0$.
Die nächste Relation ergibt:

$-a - cC + dBC = CAC = ACBA = (aC - c - dB)(aB + cBC - dC)$

$= -a^2BC + acB + ad - acB - c^2BC + cdC + ad + cdC + d^2BC$

$= 2ad + (-a^2 - c^2 + d^2)BC + 2cdC$

Daraus folgt $\underline{d = -1/2}$. Es ist $0 = A^2 - S(A)A + 1 = A^2 - 2aA + 1$

A^2C hat die Ordnung 6, ist also notwendig Nullstelle des Polynoms $X^2 - X + 1$, d.h. es ist $S(A^2C) = 1$. Nun ist

$A^2C = (2aA - 1)C = (2a^2 - 1)C - 2ac - 2adB$, also $-4ac = 1$.

Außerdem ist $a^2 + b^2 + c^2 + d^2 = N(A) = 1$, also $a^2 + c^2 = 3/4$,

daher $16a^4 + 16\,a^2c^2 = 12a^2$, also $(2a)^4 - 3\cdot(2a)^2 + 1 = 0$.

Daraus folgt: $(2a)^2 = 3/2 \pm \sqrt{9/4 - 1} = (3 \pm \sqrt{5})/2 = 1/4\cdot(1 \pm \sqrt{5})^2$,

d.h. $a = \pm\, 1/4\cdot(1 \pm \sqrt{5})$. Wäre $a = -1/4\cdot(1 \pm \sqrt{5})$, also

$S(A) = -1/2(1 \pm \sqrt{5})$, so hätte A die Ordnung 5. Daher muß

$a = 1/4\cdot(1 \pm \sqrt{5})$ sein.

Wir können o.B.d.A. $a = 1/4\cdot(1 + \sqrt{5})$ annehmen (sonst ersetzen wir A und C durch A^3 und CB, das erhält die Relationen).

Jetzt wird $c^2 = 3/4 - a^2 = (3 - \sqrt{5})/8 = 1/16\cdot(1 - \sqrt{5})^2$, also

$c = \pm\, 1/4\cdot(1 - \sqrt{5})$. Wir können o.B.d.A. $c = +1/4\cdot(1 - \sqrt{5})$ annehmen (sonst ersetzen wir A und C durch A^{-1} und C^{-1}).

Es ist umgekehrt klar, daß A,B,C mit den in (12.6.vi) genannten Eigenschaften eine Ikosaedergruppe G erzeugen. Es läßt sich direkt nachrechnen, daß $G = \{A^h,\ BA^h,\ A^hCA^j,\ A^hCBA^j \mid 0 \leq h < 10,\ 0 \leq j < 5\}$.

Daß sich alle Elemente auf eindeutige, von G unabhängige, Weise als Linearkombination von 1,B,C und BC über k darstellen lassen, folgt aus:

$A = 1/4\cdot(1 + \sqrt{5} + (1 - \sqrt{5})C - 2BC)$

$\underline{(12.7)\ \text{Satz:}}$ Sei k algebraischer Zahlkörper, Q eine k-Quaternionenalgebra.

i) Sei $n \in \mathbb{N}$, $n \geq 2$. Wenn $\Gamma(Q)$ eine 2n-zyklische oder n-Diedergruppe enthält, ist notwendig $\zeta_{2n} + \zeta_{2n}^{-1} \in k$.

ii) Wenn $\Gamma(Q)$ eine Oktaedergruppe (bzw. Ikosaedergruppe) enthält, ist notwendig $\sqrt{2} \in k$ (bzw. $\sqrt{5} \in k$).

$\underline{\text{Bew.:}}$ $\underline{\text{i)}}$ Sei $G \subset \Gamma(Q)$ eine 2n-zyklische oder n-Diedergruppe. Dann enthält G ein Element E mit $\zeta_{2n} + \zeta_{2n}^{-1} = S(E) \in k$ (12.6.i,ii).

ii) Sei $G \subset \Gamma(Q)$ eine Oktaedergruppe (bzw. Ikosaedergruppe). Mit den Bezeichnungen von 12.6 ist $1/2\cdot\sqrt{2}\cdot(1 + U) = U' \in k[U]$ (bzw. $1/4\cdot(1 + \sqrt{5} + (1 - \sqrt{5})C - 2BC) \in k[B,C]$), also $\sqrt{2} \in k$ (bzw. $\sqrt{5} \in k$).

$\underline{(12.8)\ \text{Satz:}}$ Sei k Körper, Q eine k-Quaternionenalgebra

i) Sei $n \in \mathbb{N}$, $n \geq 2$. Wenn $\zeta_{2n} + \zeta_{2n}^{-1} \in k$, gilt (12.6.i) und (12.6.ii).

ii) Es gelten (12.6.iii) und (12.6.iv).

iii) Wenn $\sqrt{2} \in k$ (bzw. $\sqrt{5} \in k$), gilt (12.6.v) (bzw. (12.6.vi)).

$\underline{\text{Bew.:}}$ wie Bew. von (12.6).

(12.9) Korollar: Sei k Körper, Q eine k-Quaternionenalgebra.
i) Sei $n \in \mathbb{N}$, $n \geq 2$, $\zeta_{2n} + \zeta_{2n}^{-1} \in k$. Seien $G,G' \subset \Gamma(Q)$ zwei 2n-zyklische Gruppen (n-Diedergruppen). Dann gibt es $M \in Q^\times$ mit $G' = MGM^{-1}$.
ii) Seien $G,G' \subset \Gamma(Q)$ Tetraedergruppen. Dann gibt es $M \in Q^\times$ mit $G' = MGM^{-1}$.
iii) Sei $\sqrt{2} \in k$ (bzw. $\sqrt{5} \in k$). Seien $G,G' \subset \Gamma(Q)$ Oktaedergruppen (bzw. Ikosaedergruppen). Dann gibt es $M \in Q^\times$ mit $MGM^{-1} = G'$.

Bew.: Sei $n \in \mathbb{N}$ mit $n \geq 2$ und sei $\zeta_{2n} + \zeta_{2n}^{-1} \in k$. Seien G,G' zwei 2n-zyklische Gruppen. Nach (12.8.i) gibt es Erzeuger $E,E' \in \Gamma(Q)$ von G,G' mit $S(E) = S(E') = \zeta_{2n} + \zeta_{2n}^{-1}$. Durch die Vorschriften $1 \mapsto 1$ und $E \mapsto E'$ wird ein k-Vektorraumisomorphismus $\sigma: k[E] \to k[E']$ definiert.
Da E,E' das gleiche Minimalpolynom über k haben und sich die Elemente E^j bzw. E'^j aus G bzw. G' jeweils auf die gleiche Weise als Linearkombination von E und 1 bzw. E' und 1 darstellen lassen, ist dies sogar ein k-Algebrenisomorphismus $\sigma: k[E] \to k[E']$.
Nach Satz (3.3) läßt sich σ zu einem k-Algebrenautomorphismus $\sigma: Q \to Q$ fortsetzen und es gibt $M \in Q^\times$ mit $MAM^{-1} = \sigma A$ für alle $A \in Q$. Insbesondere ist $MEM^{-1} = E'$ und $MGM^{-1} = G'$.
Die anderen Bahauptungen zeigt man genauso.

Bemerkung: Man überlegt sich leicht, daß die Voraussetzungen $\zeta_{2n} + \zeta_{2n}^{-1} \in k$ usw. in (12.9) überflüssig sind und daß allgemein gilt:
Isomorphe Polyedergruppen sind $Q^\times$-konjugiert.
Beim Beweis geht man so vor wie in (12.6), (12.9): Zu einem festen Teiler $X^2 - sX + 1$ von $X^{2n} - 1$ sucht man in allen 2n-zyklischen Gruppen $G \subset \Gamma(Q)$ Erzeuger E, die Nullstellen dieses Polynoms sind usw.

§ 13 . Das Verzweigungsverhalten der Quaternionenalgebren, die Polyedergruppen enthalten.

Sei k algebraischer Zahlkörper, Q eine k-Quaternionenalgebra.
In (12.7) haben wir notwendige Bedingungen an k dafür gefunden, daß $\Gamma(Q)$ eine bestimmte Polyedergruppe enthält. In diesem Paragrafen ermitteln wir (unter diesen Bedingungen) genau, welche endlichen Untergruppen $\Gamma(Q)$ bis auf Isomorphie enthält (Sätze 13.2 und 13.3).
Außerdem berechnen wir das genaue Verzweigungsverhalten von Q für den Fall, daß $\Gamma(Q)$ Dieder- bzw. Oktaeder- oder Ikosaedergruppen enthält (Sätze 13.4 und 13.8).

(13.1) Lemma: Sei k algebraischer Zahlkörper und Q eine k-Quaternionenalgebra. Sei $n \in \mathbb{N}$, $n \geq 2$ und $\zeta_{2n} + \zeta_{2n}^{-1} \in k$. Sei $E \in \Gamma(Q)$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$.
Dann ist $k[E]$ halbeinfache quadratische Erweiterung von k und
$D_k(1,E) = (\zeta_{2n} - \zeta_{2n}^{-1})^2$.

Bew.: Sei X Unbestimmte. Dann ist $k[E] \underset{k}{\cong} k[X]/(X^2 - (\zeta_{2n} + \zeta_{2n}^{-1})X + 1)k[X]$.
Wenn $\zeta_{2n} \notin k$, ist $k[E]$ Körper. Wenn $\zeta_{2n} \in k$, ist

$$k[E] \underset{k}{\cong} k[X]/(X - \zeta_{2n})(X - \zeta_{2n}^{-1})k[X]$$
$$\underset{k}{\cong} k[X]/(X - \zeta_{2n})k[X] \oplus k[X]/(X - \zeta_{2n}^{-1})k[X]$$
$$\underset{k}{\cong} k \oplus k$$

$D_k(1,E) = (\zeta_{2n} - \zeta_{2n}^{-1})^2$ folgt leicht (vergleiche die Berechnung von $D_k(1,E,B,EB)$ in (12.6.ii)).

(13.2) Satz: Sei $n \in \mathbb{N}$, $n \geq 2$. Sei k algebraischer Zahlkörper mit $\zeta_{2n} + \zeta_{2n}^{-1} \in k$ und sei Q eine k-Quaternionenalgebra.
Genau dann enthält $\Gamma(Q)$ eine 2n-zyklische Gruppe, wenn alle Primteiler von $D_k(Q)$ in $k[X]/(X^2 - (\zeta_{2n} + \zeta_{2n}^{-1})X + 1)k[X]$ verzweigt oder träge sind.

Bew.: Sei $K := k[X]/(X^2 - (\zeta_{2n} + \zeta_{2n}^{-1})X + 1)k[X]$.
$\Gamma(Q)$ enthält genau dann eine 2n-zyklische Gruppe, wenn es $E \in Q$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$ und $N(E) = 1$ gibt, d.h. genau dann, wenn es K' gibt mit $k \subset K' \subset Q$ und $K' \underset{k}{\cong} K$. Dies gilt nach Satz (5.6) genau dann, wenn alle Verzweigungsstellen von Q über k in K träge oder verzweigt sind.
Sei $\mathfrak{p}$ eine unendliche Verzweigungsstelle von Q. Dann ist $\mathfrak{p}$ reell. $\mathbb{Q}(\zeta_{2n})$ hat keine reellen Primstellen, also hat erst recht K keine reellen Primstellen. Daher ist $\mathfrak{p}$ in K verzweigt.
$\Gamma(Q)$ enthält also genau dann 2n-zyklische Gruppen, wenn alle endlichen Verzweigungsstellen von Q über k (d.h. die Primteiler von $D_k(Q)$) in K verzweigt oder träge sind.

(13.3) Satz: Sei k algebraischer Zahlkörper und Q eine k-Quaternionenalgebra.

i) Sei $n \in \mathbb{N}$, $n \geq 2$ und $\zeta_{2n} + \zeta_{2n}^{-1} \in k$. Genau dann enthält $\Gamma(Q)$ eine n-Diedergruppe, wenn $Q \tilde{k} ((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_k$.

ii) Genau dann enthält $\Gamma(Q)$ eine Tetraedergruppe, wenn $Q \tilde{k} (-1,-1)_k$.

iii) Sei $\sqrt{2} \in k$ (bzw. $\sqrt{5} \in k$). Genau dann enthält $\Gamma(Q)$ eine Oktaedergruppe (bzw. Ikosaedergruppe), wenn $Q \tilde{k} (-1,-1)_k$.

Bew.: i) Sei $G \subset \Gamma(Q)$ eine n-Diedergruppe. Seien E, B Erzeuger von G mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$, $S(B) = 0$ und $BEB^{-1} = E^{-1}$.

Wir definieren $U := 2E - (\zeta_{2n} + \zeta_{2n}^{-1})$ und $V := B$.

Dann ist $\{1,U,V,UV\}$ eine Basis von Q über k und es ist $U^2 = (\zeta_{2n} - \zeta_{2n}^{-1})^2 \in k^\times$, $V^2 = -1 \in k^\times$ und $UV = -VU$, wie man leicht nachrechnet. Also ist $Q \tilde{k} ((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_k$.

Diese Beweisschritte lassen sich umkehren.

ii), iii). $\Gamma(Q)$ enthalte eine Tetraeder-, Oktaeder- oder Ikosaedergruppe. Dann enthält $\Gamma(Q)$ eine 2-Diedergruppe (Wenn wir die Bezeichnungen von (12.6.iv,v,vi) verwenden, erzeugen U und V bzw. B und C eine 2-Diedergruppe). Nach i) ist dann also $Q \tilde{k} ((\zeta_4 - \zeta_4^{-1})^2, -1)_k = (-4,-1)_k \tilde{k} (-1,-1)_k$ (1.15.i). (Die Beh. folgt auch direkt aus 12.6.iii)

Sei umgekehrt $Q \tilde{k} (-1,-1)_k$ und sei $\{1,U,V,UV\}$ eine Basis von Q über k mit $U^2 = V^2 = -1$ und $UV = -VU$.

Dann erzeugen U und V eine 2-Diedergruppe in $\Gamma(Q)$.

U, V und $T := 1/2 \cdot (1 + U + V + UV) \in k[U,V] = Q$ erzeugen eine Tetraedergruppe in $\Gamma(Q)$.

Wenn $\sqrt{2} \in k$ (bzw. $\sqrt{5} \in k$), erzeugen $1/2 \cdot \sqrt{2} \cdot (1 + U) \in k[U,V] = Q$ und $1/2 \cdot \sqrt{2} \cdot (1 + V) \in Q$ (bzw. U, V und $A := 1/4 \cdot (1 + \sqrt{5} + (1 - \sqrt{5})U - 2UV) \in Q$) eine Oktaedergruppe (bzw. Ikosaedergruppe) in $\Gamma(Q)$.

(13.4) Satz: Sei $n \in \mathbb{N}$, $n \geq 2$. Sei k algebraischer Zahlkörper mit Hauptordnung $\mathcal{O}$ und mit $\zeta_{2n} + \zeta_{2n}^{-1} \in k$ und sei Q eine k-Quaternionenalgebra.

Sei $Q \tilde{k} ((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_k$, d.h. $\Gamma(Q)$ enthalte eine n-Diedergruppe.

Dann gilt:

i) Q ist an allen reellen Primstellen von k verzweigt.

ii) Sei $n = p^r$ mit: p ist Primzahl; $p \equiv 1 \bmod 4$; $r \in \mathbb{N}$.

Oder sei $n = 2^r$ mit: $r \in \mathbb{N}$; $r \geq 2$.

Oder sei n durch zwei verschiedene Primzahlen teilbar.

Dann hat Q keine endlichen Verzweigungsstellen, d.h. $D_k(Q) = \mathcal{O}$.

iii) Sei $n = p^r$ mit: p ist Primzahl; $p \equiv 3 \bmod 4$; $r \in \mathbb{N}$.

Oder sei $n = p = 2$ (also insbesondere $Q \tilde{\in} (-1,-1)_k$).

Eine endliche Primstelle $\mathfrak{p}$ von k ist Verzweigungsstelle von Q über k genau dann, wenn $\mathfrak{p} \mid p$ und $[k_\mathfrak{p} : \mathbb{Q}_p]$ ungerade ist.

iv) Jede Verzweigungsstelle $\mathfrak{p}$ von Q über k ist auch Verzweigungsstelle von $k[X]/(X^2 - (\zeta_{2n} + \zeta_{2n}^{-1})X + 1)k[X]$ über k.

Bew.: i) $\zeta_{2n} - \zeta_{2n}^{-1}$ ist total rein imaginär, $(\zeta_{2n} - \zeta_{2n}^{-1})^2$ ist daher total reell und total negativ. Sei $\mathfrak{p}$ eine reelle Primstelle von k.

Jede positive reelle Zahl ist Quadrat einer reellen Zahl. Daher folgt aus (1.15.i): $Q_\mathfrak{p} \tilde{\in} ((\zeta_{2n} - \zeta_{2n}^{-1})^2,-1)_{k_\mathfrak{p}} \tilde{\in} (-1,-1)_{k_\mathfrak{p}}$.

Also ist $Q_\mathfrak{p}$ Divisionsalgebra, d.h. $\mathfrak{p}$ ist Verzweigungsstelle von Q über k.

ii),iii) a) Wir beweisen die Behauptung zunächst für den Körper $k := \mathbb{Q}[\zeta_{2n} + \zeta_{2n}^{-1}]$. k ist total reell, $k = \mathbb{Q}(\zeta_{2n}) \cap \mathbb{R}$.

Ebenfalls bekannt und leicht einzusehen ist: $[\mathbb{Q}(\zeta_{2n}) : k] = 2$.

Sei ϕ die Eulerfunktion, d.h. $\phi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times$ für $m \in \mathbb{N} - \{1\}$.

Dann ist bekanntlich $[\mathbb{Q}(\zeta_{2n}) : \mathbb{Q}] = \phi(2n)$, also $[k : \mathbb{Q}] = 1/2 \cdot \phi(2n)$.

Mit i) folgt: Q ist an allen $1/2 \cdot \phi(2n)$ unendlichen (reellen) Primstellen von k verzweigt.

Sei $G \subset \Gamma(Q)$ eine n-Diedergruppe. Seien E, B Erzeuger von G mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$, $S(B) = 0$ und $BEB^{-1} = E^{-1}$. Dann ist $\mathcal{O} := \mathfrak{o}[E,B]$ eine Q-Ordnung mit Basis $\{1,E,B,EB\}$ über $\mathfrak{o}$. Daher gilt $D_k(\mathcal{O}) = D_k(1,E,B,EB)\mathfrak{o} = (\zeta_{2n} - \zeta_{2n}^{-1})^4 \mathfrak{o}$ (12.6.ii). Wegen Satz (4.7) folgt daraus: $D_k(Q) \mid (\zeta_{2n} - \zeta_{2n}^{-1})^4 \mathfrak{o}$, d.h.:

Ist $\mathfrak{p}$ eine endliche Verzweigungsstelle von Q über k, dann ist notwendig $\mathfrak{p} \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}$.

Sei $n = p^r$ mit: p ist Primzahl; $p \neq 2$; $r \in \mathbb{N}$.

Dann ist bekanntlich $\phi(2n) = \phi(n) = (p-1) \cdot p^{r-1}$ und p ist in $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$ höchstverzweigt. Genauer: Ist $\mathfrak{o}'$ die Hauptordnung von $\mathbb{Q}(\zeta_n)$, so ist $(1 - \zeta_n)\mathfrak{o}'$ Primideal und $p\mathfrak{o}' = (1 - \zeta_n)^{\phi(n)}\mathfrak{o}'$ (siehe /12/ S. 199/200 §95).

Es ist $(1 - \zeta_n)\mathfrak{o}' = (1 - \zeta_{2n}^2)\mathfrak{o}' = \zeta_{2n}(\zeta_{2n}^{-1} - \zeta_{2n})\mathfrak{o}' = (\zeta_{2n} - \zeta_{2n}^{-1})\mathfrak{o}'$.

Da p in $\mathbb{Q}(\zeta_n)$ höchstverzweigt ist, ist p auch in k höchstverzweigt und der Primteiler $\mathfrak{p}$ von $p\mathbb{Z}$ in k ist in $\mathbb{Q}(\zeta_n)$ verzweigt. Es ist also $\mathfrak{p}\mathfrak{o}' = (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}'$, d.h. $\mathfrak{p} = (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}$. Wir haben damit:

Q ist an den $1/2\cdot(p-1)\cdot p^{r-1}$ unendlichen Primstellen von k sowie höchstens noch an der endlichen Primstelle $\mathfrak{p}$ verzweigt. Da die Anzahl der Verzweigungsstellen von Q über k gerade ist (1.10.i), ist Q genau dann an der Stelle $\mathfrak{p}$ verzweigt, wenn $1/2\cdot(p-1)\cdot p^{r-1}$ ungerade ist, also wenn $p \equiv 3 \bmod 4$.
In diesem Fall ist $[k_{\mathfrak{p}} : \mathbb{Q}_p] = v(\mathfrak{p}) = 1/2\cdot(p-1)\cdot p^{r-1}$ ungerade.
Für Potenzen von Primzahlen $p \neq 2$ ist die Beh. also gezeigt.
Für später halten wir außerdem fest:

(13.5) Korollar: Sei $n = p^r$; p ungerade Primzahl; $r \in \mathbb{N}$.
Dann gilt: $(\zeta_{2n} - \zeta_{2n}^{-1})^2 \mid p$.

Sei jetzt $n = 2^r$; $r \in \mathbb{N}$. Dann ist $\phi(2n) = 2\phi(n) = n$.
2 ist in $\mathbb{Q}(\zeta_{2n})$ und $\mathbb{Q}(\zeta_n)$ höchstverzweigt.
Seien σ', σ'' die Hauptordnungen von $\mathbb{Q}(\zeta_{2n})$, $\mathbb{Q}(\zeta_n)$. Der Primteiler von $2\mathbb{Z}$ in $\mathbb{Q}(\zeta_{2n})$ bzw. $\mathbb{Q}(\zeta_n)$ ist dann $(1-\zeta_{2n})\sigma'$ bzw $(1-\zeta_n)\sigma''$.
$(1-\zeta_n)\sigma''$ ist in $\mathbb{Q}(\zeta_{2n})$ (höchst)verzweigt, also $(1-\zeta_n)\sigma' = (1-\zeta_{2n})^2\sigma'$.
Dieselbe Rechnung wie eben zeigt: $(1-\zeta_n)\sigma' = (\zeta_{2n} - \zeta_{2n}^{-1})\sigma'$.
Sei $\mathfrak{p}$ der Primteiler von $2\mathbb{Z}$ in k. Dann ist $\mathfrak{p}$ verzweigt in $\mathbb{Q}(\zeta_{2n})$, also $\mathfrak{p}\sigma' = (1-\zeta_{2n})^2\sigma' = (\zeta_{2n} - \zeta_{2n}^{-1})\sigma'$; daher: $\mathfrak{p}^2 = (\zeta_{2n} - \zeta_{2n}^{-1})^2\sigma$.
Wir haben damit: Q ist an den $1/2\cdot\phi(2n) = 2^{r-1}$ unendlichen Primstellen von k sowie höchstens noch an der endlichen Primstelle $\mathfrak{p}$ verzweigt.
Da die Anzahl der Verzweigungsstellen von Q herade ist, ist Q genau dann an der Stelle $\mathfrak{p}$ verzweigt, wenn 2^{r-1} ungerade ist, also wenn $r = 1$, d.h. $n = 2$. In diesem Fall ist $k = \mathbb{Q}$, also $[k_{\mathfrak{p}} : \mathbb{Q}_2] = 1$ ungerade.
Damit folgt die Beh. für Potenzen von 2.
Falls $r \geq 2$, ist $v(\mathfrak{p}) = 2^{r-1}$ gerade. also $\mathfrak{p}^2 \mid 2\sigma$.

(13.6) Korollar: i) $(\zeta_4 - \zeta_4^{-1})^2 = -4$.

ii) Ist $n = 2^r$ mit $r \in \mathbb{N}$, $r \geq 2$, dann gilt: $(\zeta_{2n} - \zeta_{2n}^{-1})^2 \mid 2$.

Sei jetzt n durch zwei verschiedene Primzahlen teilbar, sei $n = pqr$ mit Primzahlen $p \neq q$.

Dann ist $(\zeta_{2n} - \zeta_{2n}^{-1})\left(\sum_{j=0}^{qr-1} \zeta_{2n}^{j}\zeta_{2n}^{-(qr-1-j)}\right) = \zeta_{2n}^{qr} - \zeta_{2n}^{-qr} = \zeta_{2p} - \zeta_{2p}^{-1}$.

Da $(\zeta_{2p} - \zeta_{2p}^{-1})^2 \mid p^2$, ist $(\zeta_{2n} - \zeta_{2n}^{-1})^2 \mid p^2$. Genauso: $(\zeta_{2n} - \zeta_{2n}^{-1})^2 \mid q^2$.

(13.7) Korollar: Sei $n \in \mathbb{N}$ durch zwei verschiedenen Primzahlen teilbar. Sei k algebraischer Zahlkörper mit Hauptordnung $\mathcal{O}$. Sei $(\zeta_{2n} + \zeta_{2n}^{-1}) \in k$. Dann ist $(\zeta_{2n} - \zeta_{2n}^{-1})^2 \in \mathcal{O}^\times$.

Wir haben damit: Q ist genau an den $1/2 \cdot \phi(n)$ unendlichen Primstellen von k verzweigt.

ii),iii) b) Sei jetzt $k^n := \mathbb{Q}[\zeta_{2n} + \zeta_{2n}^{-1}]$ und k beliebiger algebraischer Zahlkörper mit $\zeta_{2n} + \zeta_{2n}^{-1} \in k$, d.h. mit $k^n \subset k$.

Es ist $Q \tilde{k} ((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_k \tilde{k} ((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_{k^n} \otimes_{k^n} k$.

Sei $n = p^r$ mit: p ist Primzahl; $p \equiv 1 \bmod 4$; $r \in \mathbb{N}$.

Oder sei $n = 2^r$ mit: $r \in \mathbb{N}$; $r \geq 2$.

Oder sei n durch zwei verschiedene Primzahlen teilbar.

Dann hat nach a) $((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_{k^n}$ keine endlichen Verzweigungsstellen.

Also hat auch Q keine endlichen Verzweigungsstellen. (5.4.i)

Sei $n = p^r$ mit: p ist Primzahl; $p \equiv 3 \bmod 4$; $r \in \mathbb{N}$. Oder sei $n = p = 2$.

Sei $\mathfrak{q}$ eine endliche Verzweigungsstelle von Q über k. Nach (5.4.i) ist $\mathfrak{q}$ Fortsetzung einer endlichen Verzweigungsstelle $\mathfrak{p}$ von $((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_k$ über k^n und $[k_{\mathfrak{q}} : k^n_{\mathfrak{p}}]$ ist ungerade.

Nach a) ist dann $\mathfrak{p}$ der Primteiler von $p\mathbb{Z}$ in k^n und $[k^n_{\mathfrak{p}} : \mathbb{Q}_p]$ ist ungerade.

Also gilt $\mathfrak{q} \mid p$ und $[k_{\mathfrak{q}} : \mathbb{Q}_p]$ ist ungerade.

Ist umgekehrt $\mathfrak{q}$ endliche Primstelle von k mit $\mathfrak{q} \mid p$ und $[k_{\mathfrak{q}} : \mathbb{Q}_p]$ ungerade, so gilt $\mathfrak{q} \mid \mathfrak{p}$ und $[k_{\mathfrak{q}} : k^n_{\mathfrak{p}}]$ ist ungerade (wobei $\mathfrak{p}$ der Primteiler von $p\mathbb{Z}$ in k^n ist). Nach a) ist $\mathfrak{p}$ Verzweigungsstelle von $((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_{k^n}$ über k^n. Nach (5.4.i) ist also $\mathfrak{q}$ Verzweigungsstelle von Q über k.

iv) Sei $K := k[X]/(X^2 - (\zeta_{2n} + \zeta_{2n}^{-1})X + 1)k[X]$.

Sei $\mathfrak{p}$ Verzweigungsstelle von Q über k. Ist $\mathfrak{p}$ eine unendliche, also reelle Primstelle, dann ist $\mathfrak{p}$ in K verzweigt. wie wir schon im Bew. von (13.2) gesehen haben. Sei also $\mathfrak{p}$ eine endliche Primstelle.

Nach ii) und iii) ist notwendig $n = p^r$ mit p Primzahl, $p \equiv 3 \bmod 4$, $r \in \mathbb{N}$ oder $n = p = 2$ und es ist notwendig $\mathfrak{p} \mid p$ und $[k_{\mathfrak{p}} : \mathbb{Q}_p]$ ungerade.

$\Gamma(Q)$ enthält eine n-Diedergruppe, also auch eine 2n-zyklische Gruppe.

Nach Satz (13.2) ist also $\mathfrak{p}$ verzweigt oder träge in K, insbesondere ist K Körper, $\zeta_{2n} \notin k$ und wir können $K = k(\zeta_{2n})$ identifizieren.

Sei $\mathfrak{q}$ eine Fortsetzung von $\mathfrak{p}$ auf K. Dann ist $v(\mathfrak{q}) = v_k(\mathfrak{q}) \cdot v(\mathfrak{p})$.

Sei $\mathfrak{q}'$ Primstelle von $\mathbb{Q}(\zeta_{2n})$ mit $\mathfrak{q} \mid \mathfrak{q}'$. Dann ist $v(\mathfrak{q}')$ Teiler von $v(\mathfrak{q})$.

Es ist $\mathfrak{q}' \mid p$ und daher ist $v(\mathfrak{q}') = [\mathbb{Q}(\zeta_{2n}) : \mathbb{Q}] = \phi(2n)$ gerade.

Also ist auch $v(\mathfrak{q})$ gerade. $v(\mathfrak{p})$ ist Teiler von $[k_{\mathfrak{p}} : \mathbb{Q}_p]$, also ungerade. Daher ist notwendig $v_k(\mathfrak{q})$ gerade, d.h. $v_k(\mathfrak{q}) = 2$.

(13.8) Satz: Sei k algebraischer Zahlkörper mit $\sqrt{2} \in k$ (bzw. $\sqrt{5} \in k$). Sei Q eine k-Quaternionenalgebra. Sei $Q \tilde{\in}_k (-1,-1)_k$, d.h. $\Gamma(Q)$ enthalte eine Oktaedergruppe (bzw. Ikosaedergruppe).
Dann ist Q genau an den reellen Primstellen von k verzweigt.

Bew.: Q ist an den reellen Primstellen von k verzweigt (13.4.i).
2 ist verzweigt in $\mathbb{Q}(\sqrt{2})$, träge in $\mathbb{Q}(\sqrt{5})$.
Da $\mathbb{Q}(\sqrt{2}) \subset k$ (bzw. $\mathbb{Q}(\sqrt{5}) \subset k$), gilt für jede Primstelle $\mathfrak{p}$ von k mit $\mathfrak{p}|2$: $[k_{\mathfrak{p}} : \mathbb{Q}_2]$ ist gerade. Nach (13.4.iii) hat Q keine endlichen Verzweigungsstellen.

§ 14 . Beispiel: Quaternionenalgebren über imaginärquadratischen Zahlkörpern.

In § 14 konkretisieren wir die Ergebnisse der Paragrafen 12 und 13 für imaginärquadratische Zahlkörper (Sätze 14.1, 14.5, 14.6, 14.7 und 14.8).

(14.1) Satz: Sei $d \in \mathbb{N}$ quadratfrei, sei $k = \mathbb{Q}(i\sqrt{d})$, sei Q eine k-Quaternionenalgebra und sei $G \subset \Gamma(Q)$ eine endliche Gruppe mit $\{\pm 1\} \subsetneq G$.
Dann ist G entweder 4-zyklische Gruppe, 6-zyklische Gruppe, 2-Diedergruppe, 3-Diedergruppe oder Tetraedergruppe.

Bew.: k ist algebraischer Zahlkörper, also ist G Polyedergruppe (12.4.iv).
Da $\sqrt{2} \notin k$, $\sqrt{5} \notin k$, ist G keine Oktaeder- oder Ikosaedergruppe (12.7.ii).
Sei $n \in \mathbb{N}$, $n \geq 2$ und G eine 2n-zyklische Gruppe oder n-Diedergruppe.
Nach (12.7.i) ist notwendig $\zeta_{2n} + \zeta_{2n}^{-1} \in k$; wegen $\zeta_{2n} + \zeta_{2n}^{-1} \in \mathbb{R}$ also $\zeta_{2n} + \zeta_{2n}^{-1} \in k \cap \mathbb{R} = \mathbb{Q}$. Daher ist $\mathbb{Q}[\zeta_{2n} + \zeta_{2n}^{-1}] = \mathbb{Q}$ und
$1/2 \cdot \phi(2n) = [\mathbb{Q}[\zeta_{2n} + \zeta_{2n}^{-1}] : \mathbb{Q}] = 1$, d.h. $\phi(2n) = 2$.
Man sieht leicht, daß daraus $n = 2$ oder $n = 3$ folgt.

(4.2) Bemerkung: Da $\zeta_4 = i$, $\zeta_6 = 1/2 \cdot (1 + i\sqrt{3})$, ist $\zeta_4 + \zeta_4^{-1} = 0$, $\zeta_6 + \zeta_6^{-1} = 1$ und $(\zeta_4 - \zeta_4^{-1})^2 = -4$, $(\zeta_6 - \zeta_6^{-1})^2 = -3$.

Wir wollen jetzt Satz (13.2) auf imaginärquadratische Zahlkörper anwenden. Dazu benötigen wir vorweg zwei Lemmata:

(14.3) Lemma: Seien k, K_1, K_2 algebraische Zahlkörper; $k \subset K_1$, $k \subset K_2$.
Sei $K = K_1K_2$ das Kompositum von K_1 und K_2 (in $\mathbb{C}$).
Ist $\mathfrak{P}$ ein über k voll zerlegtes (unverzweigtes) Primideal von K_1, so ist auch jeder Primteiler $\mathfrak{q}$ von $\mathfrak{P}$ in K über K_2 voll zerlegt (unverzweigt).

Bew.: siehe /11/ S. 61 Satz 44

(14.4) Lemma: Seien $D, D' \in \mathbb{Z}$; $D,D' \neq 1$; $D \neq D'$; D,D' quadratfrei.
Sei $k = \mathbb{Q}(\sqrt{D})$. Sei $\mathfrak{p}$ ein Primideal von k und $p \in \mathbb{N}$ die Primzahl mit $\mathfrak{p}|p$.
Dann gilt: $\mathfrak{p}$ ist genau dann zerlegt (unverzweigt) in $K := k(\sqrt{D'}) = k(\sqrt{DD'})$, wenn p in $\mathbb{Q}(\sqrt{D'})$ oder $\mathbb{Q}(\sqrt{DD'})$ zerlegt (unverzweigt) ist.

Bew.: K ist galoissche Körpererweiterung von $\mathbb{Q}$ mit der Kleinschen Vierergruppe als Galoisgruppe. Seine Unterkörper sind außer $\mathbb{Q}$ und K selbst noch: $k = \mathbb{Q}(\sqrt{D})$, $\mathbb{Q}(\sqrt{D'})$ und $\mathbb{Q}(\sqrt{DD'})$.
Sei p zerlegt (unverzweigt) in $\mathbb{Q}(\sqrt{D'})$ oder $\mathbb{Q}(\sqrt{DD'})$. Nach Lemma (14.3) ist dann $\mathfrak{p}$ zerlegt (unverzweigt) in $K = k(\sqrt{D'}) = k(\sqrt{DD'})$.
Sei umgekehrt $\mathfrak{p}$ zerlegt (unverzweigt) in K. Sei $\mathfrak{q}$ Primteiler von $\mathfrak{p}$ in K. Der Zerlegungskörper (Trägheitskörper) von $\mathfrak{q}$ über $\mathbb{Q}$ ist dann $\neq \mathbb{Q}$ und $\neq k$. Er muß also einen der beiden Körper $\mathbb{Q}(\sqrt{D})$ oder $\mathbb{Q}(\sqrt{DD'})$ enthalten, d.h. p muß in mindestens einem der beiden Körper zerlegt (unverzweigt) sein.

(14.5) Satz: Sei $d \in \mathbb{N}$ quadratfrei, sei $k = \mathbb{Q}(i\sqrt{d})$ und sei Q eine k-Quaternionenalgebra. Genau dann enthält $\Gamma(Q)$ eine 4-zyklische Untergruppe, wenn für alle Primteiler $\mathfrak{p}$ von $D_k(Q)$ gilt:
Ist $p \in \mathbb{N}$ die Primzahl mit $\mathfrak{p}|p$, dann ist

i) $p = 2$ und $d \not\equiv 1 \bmod 8$

oder ii) $p \equiv 3 \bmod 4$ und $\left(\frac{d}{p}\right) \neq 1$

Bew.: Wir müssen Satz (13.2) anwenden. Sei $K := k[X]/(X^2 + 1)k[X]$.
Falls $d = 1$, ist K kein Körper. Alle Primideale von k sind in K zerlegt. $\Gamma(Q)$ enthält also genau dann eine 4-zyklische Untergruppe, wenn Q nur reelle Verzweigungsstellen über k hat. Da k keine reellen Primstellen hat, ist dies genau dann der Fall, wenn Q keine Verzweigungsstellen über k hat, also wenn $Q \tilde{}_k M_2(k)$. Da keine Primzahl $p \in \mathbb{N}$ die Bedingungen i), ii) erfüllt, ist die Beh. für $d = 1$ bewiesen.
Sei jetzt $d \neq 1$. Dann ist K Körper und wir identifizieren $K = k(i)$.
Ist $\mathfrak{p}$ ein Primideal von k und $p \in \mathbb{N}$ die Primzahl mit $\mathfrak{p}|p$, so ist $\mathfrak{p}$ genau dann zerlegt in K, wenn p in $\mathbb{Q}(i)$ oder $\mathbb{Q}(\sqrt{d})$ zerlegt ist.
Nun gilt: 2 ist in $\mathbb{Q}(i)$ verzweigt.
2 ist in $\mathbb{Q}(\sqrt{d})$ genau dann zerlegt, wenn $d \equiv 1 \bmod 8$.

Ist $p \in \mathbb{N}$ Primzahl und $p \neq 2$, dann gilt:

p ist in $\mathbb{Q}(i)$ genau dann zerlegt, wenn $\left(\frac{-1}{p}\right) = 1$, d.h. wenn $p \equiv 1 \bmod 4$.

p ist in $\mathbb{Q}(\sqrt{d})$ genau dann zerlegt, wenn $\left(\frac{d}{p}\right) = 1$.

Jetzt folgt die Beh. sofort aus Satz (13.2).

(14.6) Satz: Sei $d \in \mathbb{N}$ quadratfrei, $k = \mathbb{Q}(i\sqrt{d})$, Q eine k-Quaternionenalgebra. Genau dann enthält $\Gamma(Q)$ eine 6-zyklische Untergruppe, wenn für alle Primteiler $\mathfrak{p} \mid D_k(Q)$ gilt:

Ist $p \in \mathbb{N}$ die Primzahl mit $\mathfrak{p} \mid p$, so ist

i) $p = 2$ und $d \not\equiv 3 \bmod 8$

oder ii) $p = 3$ und $d \not\equiv 3 \bmod 9$

oder iii) $p \neq 2$; $p \equiv 2 \bmod 3$ und $\left(\frac{3d}{p}\right) \neq 1$.

Bew.: Sei $d = 3$. Dann ist $K := k[X]/(X^2 - X + 1)k[X]$ kein Körper.
Wie im Beweis von (14.5) für $d = 1$ zeigt man, daß $\Gamma(Q)$ genau dann eine 6-zyklische Gruppe enthält, wenn $Q \underset{k}{\simeq} M_2(k)$.
Da keine Primzahl $p \in \mathbb{N}$ die Bedingungen i), ii), iii) erfüllt, ist die Beh. für $d = 3$ bewiesen.
Sei jetzt $d \neq 3$. Dann ist K Körper und wir können identifizieren: $K = k(i\sqrt{3})$.
Ist $\mathfrak{p}$ ein Primideal von k und $p \in \mathbb{N}$ die Primzahl mit $\mathfrak{p} \mid p$, so ist $\mathfrak{p}$ genau dann zerlegt in K, wenn p in $\mathbb{Q}(i\sqrt{3})$ oder $\mathbb{Q}(\sqrt{3d})$ zerlegt ist.
Nun gilt: 2 ist in $\mathbb{Q}(i\sqrt{3})$ träge.

2 ist in $\mathbb{Q}(\sqrt{3d})$ genau dann zerlegt, wenn $3d \equiv 1 \bmod 8$, d.h. wenn $d \equiv 3 \bmod 8$.

3 ist in $\mathbb{Q}(i\sqrt{3})$ verzweigt.

Wenn $3 \nmid d$, so ist 3 auch in $\mathbb{Q}(\sqrt{3d})$ verzweigt.

Wenn $3 \mid d$, so ist $\mathbb{Q}(\sqrt{3d}) = \mathbb{Q}(\sqrt{d/3})$ und 3 ist genau dann in $\mathbb{Q}(\sqrt{d/3})$ zerlegt, wenn $\left(\frac{d/3}{3}\right) = 1$, d.h. wenn $d/3 \equiv 1 \bmod 3$, d.h. wenn $d \equiv 3 \bmod 9$.

Ist $p \in \mathbb{N}$ Primzahl, $p \neq 2, 3$, dann gilt:
p ist in $\mathbb{Q}(i\sqrt{3})$ genau dann zerlegt, wenn

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)(-1)^{(3-1)/2\cdot(p-1)/2} = \left(\frac{p}{3}\right),$$

d.h. wenn $p \equiv 1 \bmod 3$.

p ist in $\mathbb{Q}(\sqrt{3d})$ genau dann zerlegt, wenn $\left(\frac{3d}{p}\right) = 1$.

Jetzt folgt die Beh. aus Satz (13.2).

(14.7) Satz: Sei $d \in \mathbb{N}$ quadratfrei, sei $k = \mathbb{Q}(i\sqrt{d})$ und sei Q eine k-Quaternionenalgebra.

i) $\Gamma(Q)$ enthält genau dann 2-Diedergruppen und Tetraedergruppen, wenn $Q \tilde{\in}_k (-1,-1)_k$.

ii) Genau dann enthält $\Gamma(Q)$ 3-Diedergruppen, wenn $Q \tilde{\in}_k (-3,-1)_k$.

Bew.: folgt sofort aus (13.3.i, ii).

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

i) Wenn $d \not\equiv 7 \bmod 8$, ist $(-1,-1)_k \tilde{\in}_k M_2(k)$.

ii) Wenn $d \equiv 7 \bmod 8$, ist 2 in k zerlegt und $(-1,-1)_k$ ist über k genau an den beiden Primteilern von 2 in k verzweigt.

iii) Wenn $d \not\equiv 2 \cdot \bmod 3$, ist $(-3,-1)_k \tilde{\in}_k M_2(k)$.

iv) Wenn $d \equiv 2 \bmod 3$, ist 3 in k zerlegt und $(-3,-1)_k$ ist über k genau an den beiden Primteilern von 3 in k verzweigt.

Bew.: Da k keine reellen Primstellen hat, hat jede k-Quaternionenalgebra nur endliche Verzweigungsstellen über k.

Wir wenden Satz (13.4.iii) an mit $n = p \notin \{2,3\}$.

Ist $\mathfrak{p}$ ein Primteiler von p in k, so ist $[k_{\mathfrak{p}} : \mathbb{Q}_p] \leq [k : \mathbb{Q}] = 2$.

$\mathfrak{p}$ ist also genau dann Verzweigungsstelle von $Q \notin \{(-1,-1)_k, (-3,-1)_k\}$, wenn $[k_{\mathfrak{p}} : \mathbb{Q}_p] = 1$, d.h. wenn p in k zerlegt ist.

Nun ist 2 bzw. 3 genau dann zerlegt in $k = \mathbb{Q}(i\sqrt{d})$, wenn $d \equiv 7 \bmod 8$ bzw. $d \equiv 2 \bmod 3$.

Teil III

Die Konjugationsklassenzahlen der zyklischen Gruppen

Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und sei Q eine k-Quaternionenalgebra. Sei $n \in \mathbb{N}$, $n > 2$.
In Teil III will ich folgendes Problem lösen:
Sei $\mathfrak{M}$ eine Q-Maximalordnung. Wie groß ist dann die $\Gamma(\mathfrak{M})$-Konjugationsklassenzahl $\lambda_{2n}(\mathfrak{M})$ von zyklischen Gruppen der Ordnung 2n in der Norm-Eins-Gruppe $\Gamma(\mathfrak{M})$?
Zur Lösung des Problems einige Vorbemerkungen:

i) Der Fall, daß $\Gamma(\mathfrak{M})$ eine endliche Gruppe ist, ist hier uninteressant. Ich kann also (siehe 15.11) voraussetzen, daß der Idealmodul $\mathfrak{m} = \mathfrak{m}(Q)$, der aus den unendlichen Verzweigungsstellen von Q über k zusammengesetzt ist, nicht alle unendlichen Primstellen von k enthält. Dadurch wird es möglich, den Satz von Eichler über Hauptideale (10.4) und seine Korollare zu benutzen.

ii) Natürlich setze ich voraus, daß $\zeta_{2n} + \zeta_{2n}^{-1} \in k$ ist und daß alle endlichen Verzweigungsstellen von Q in $K := k[X]/\left(X^2 - (\zeta_{2n}+\zeta_{2n}^{-1})X + 1\right)k[X]$ verzweigt oder träge sind. Genau dann nämlich sind 2n-zyklische Gruppen in $\Gamma(Q)$ enthalten (12.7.i und 13.2) und dies ist natürlich eine notwendige Bedingung dafür, daß $\lambda_{2n}(\mathfrak{M}) > 0$ werden kann.

iii) Ich bestimme die Klassenzahl $\lambda_{2n}(\mathfrak{M})$ indirekt, indem ich sie auf die Konjugationsklassenzahlen von speziellen Erzeugenden 2n-zyklischer Gruppen zurückführe (§15). Auf diese Weise erhalte ich zusätzlich die Konjugationsklassenzahlen $\lambda_{2n}^{*}(\mathfrak{M})$ derjenigen 2n-zyklischen Gruppen in $\Gamma(\mathfrak{M})$, die in einer n-Diedergruppe in $\Gamma(\mathfrak{M})$ enthalten sind.
($\lambda_{2n}^{*}(\mathfrak{M})$ wird wieder in Teil IV bei der Bestimmung der Konjugationsklassenzahlen nichtzyklischer Gruppen wichtig.)

iv) $\lambda_{2n}(\mathfrak{M})$ und $\lambda_{2n}^{*}(\mathfrak{M})$ hängen offensichtlich nur vom Typ $\tilde{\mathfrak{M}}$ der Maximalordnung ab. Man kann λ_{2n} und λ_{2n}^{*} also als Abbildungen von $\tilde{Q}$ nach $\mathbb{N}_0$ verstehen. Ich kann diese Funktionen genau angeben.
Ist $\mathfrak{M}$ eine Q-Maximalordnung, so hängt $\lambda_{2n}(\mathfrak{M})$ i.a. außer von k, Q und n noch von der Position von $\mathfrak{M}$ zu gewissen ausgezeichneten Maximalordnungen ab (siehe 2. und 4. in dieser Einleitung).
In Spezialfällen kann man $\lambda_{2n}(\mathfrak{M})$ bestimmen, wenn man weiß, welche endlichen Untergruppen (bis auf Isomorphie) in $\Gamma(\mathfrak{M})$ enthalten sind.

Ich gebe nun eine Inhaltsübersicht über Teil III:

1. Jede 2n-zyklische Untergruppe G von $\Gamma(\mathfrak{M})$ hat genau 2 Erzeuger mit Spur $\zeta_{2n}+\zeta_{2n}^{-1}$. Ist E der eine, so ist $E^{-1} = E^*$ der andere.
E und E^{-1} sind genau dann $\Gamma(\mathfrak{M})$-konjugiert, wenn G in einer n-Diedergruppe in $\Gamma(\mathfrak{M})$ enthalten ist (Lemma 15.9).
$l_{2n}(\mathfrak{M})$ (bzw. $l_{2n}^*(\mathfrak{M})$) bezeichnet die $\Gamma(\mathfrak{M})$-Konjugationsklassenzahl von Elementen $E \in \Gamma(\mathfrak{M})$ mit $S(E) = \zeta_{2n}+\zeta_{2n}^{-1}$ (bzw. für die außerdem E in einer n-Diedergruppe in $\Gamma(\mathfrak{M})$ enthalten ist).
Aus Lemma (15.9) folgen jetzt leicht die wichtigen neuen Formeln:
$\lambda_{2n}^*(\mathfrak{M}) = l_{2n}^*(\mathfrak{M})$ und $\lambda_{2n}(\mathfrak{M}) = 1/2\cdot(l_{2n}(\mathfrak{M}) + l_{2n}^*(\mathfrak{M}))$ (siehe 15.10.iii).
Ich habe damit in § 15 das Problem der Bestimmung von λ_{2n} (und λ_{2n}^*) auf das Problem der Bestimmung von l_{2n} und l_{2n}^* zurückgeführt.
Diese Größen berechne ich in den Paragrafen 16 bis 18.
Bemerkung: In /19/, /16/ und /17/ werden nur total reelle Zahlkörper betrachtet. Da Q nicht an allen unendlichen Primstellen von k verzweigt ist, enthält dann $\Gamma(0)$ keine Diedergruppen (vgl. 13.4.i).
Dadurch vereinfachen sich die o.a. Formeln zu $\lambda_{2n}(\mathfrak{M}) = 1/2\cdot l_{2n}(\mathfrak{M})$.
Der in der Literatur angegebenen Berechnung von $\lambda_{2n}(\mathfrak{M})$ (dort l(s,n) genannt) liegt diese Zurückführung auf $l_{2n}(\mathfrak{M})$ zugrunde. Das wird in diesem Beweis, der mit Fallunterscheidung operiert, allerdings nicht deutlich, vgl. /16/ S. 192, Bew. von Satz 3.

2. Sind E, E' $\in \Gamma(\mathfrak{M})$ mit $S(E) = S(E') = \zeta_{2n} + \zeta_{2n}^{-1}$ zwei $\Gamma(\mathfrak{M})$-konjugierte Elemente, so ist offenbar $f(\mathfrak{M} \wedge k[E]) = f(\mathfrak{M} \wedge k[E'])$.
Daher zerfällt $l_{2n}(\mathfrak{M})$ kanonisch in eine Summe von $l_{2n}(\mathfrak{M}, \mathfrak{f})$, wo $\mathfrak{f}$ die ganzen σ-Ideale durchläuft.
In § 16 bestimme ich $F_{2n}(\mathfrak{M}) = \{\mathfrak{f} \in \Gamma^k \mid l_{2n}(\mathfrak{M}, \mathfrak{f}) > 0\}$ für die verschiedenen Maximalordnungen $\mathfrak{M}$ im wesentlichen mit Hilfe von Satz (11.9).
Zuerst kläre ich, welche $\mathfrak{f}$ überhaupt in irgendeinem $F_{2n}(\mathfrak{M})$ liegen (Lemma 16.5). Als zweites vergleiche ich die $F_{2n}(\mathfrak{M})$ für verschiedene Maximalordnungen $\mathfrak{M}$ miteinander (Lemma 16.7).
Unter Benutzung von (11.9.i) läßt sich dann aus einem bekannten $\mathfrak{f} \in F_{2n}(\mathfrak{M})$ die ganze Menge $F_{2n}(\mathfrak{M})$ berechnen (Lemma 16.8).
Das wichtige Gesamtergebnis ist Satz (16.10). Diesen Satz habe ich durch Lemma (16.9) außerdem in eine für spätere Anwendungen geeignetere Form gebracht.

Falls $[I^k : RN(I^K)S_\infty] = 1$ (d.h. wenn 16.11 nicht erfüllt ist), ist F_{2n} konstant auf der Menge aller Q-Maximalordnungen. Dies stimmt mit den Ergebnissen in /19/, /16/ und /17/ für total reelle Zahlkörper k überein.
Falls aber $[I^k : RN(I^K)S_\infty] = 2$, zerfällt die Menge der Q-Maximalordnungen in zwei Klassen. F_{2n} ist auf jeder dieser Klassen konstant; gehören aber zwei Maximalordnungen $\mathfrak{M}$, $\mathfrak{M}'$ zu verschiedenen Klassen, so ist $F_{2n}(\mathfrak{M}) \cap F_{2n}(\mathfrak{M}') = \emptyset$. Bei konkret vorgegebener Maximalordnung $\mathfrak{M}$ muß man dann zur Berechnung von $l_{2n}(\mathfrak{M})$ noch bestimmen, zu welcher der beiden Klassen $\mathfrak{M}$ gehört. Falls k imaginärquadratischer Zahlkörper ist, ist das Problem bei einem geeigneten Repräsentantensystem von $\tilde{Q}$ immer (leicht) lösbar; siehe Lemma (27.4).

3. In § 17 berechne ich schließlich für gegebenes $\mathfrak{M}$ und $f \in F_{2n}(\mathfrak{M})$ die Konjugationsklassenzahl $l_{2n}(\mathfrak{M}, f)$, d.h. ich führe sie zurück auf Größen, die aus der algebraischen Zahlentheorie bekannt sind. Die Lemmata (17.2) und (17.4) ergeben, daß $l_{2n}(\mathfrak{M}, f)$ gleich einer anderen, leichter zugänglichen Klassenzahl ist (Korollar 17.6). Die Berechnung von $l_{2n}(\mathfrak{M}, f)$ geschieht jetzt in 3 Schritten (Lemmata 17.7, 17.11 und 17.13). In jedem Schritt wird eine Menge (von Klassen) vermittels der kanonischen Äquivalenzrelation, die von einer Abbildung induziert wird, in Teilmengen aufgeteilt. Jedesmal ist die Anzahl der Teilmengen und beim letzten Schritt auch ihre Mächtigkeit bekannt. Da die genannten Abbildungen "fast" Homomorphismen sind, ergibt sich $l_{2n}(\mathfrak{M}, f)$ als Produkt und Quotient von Klassenzahlen; siehe Satz (17.4).
Falls $\Gamma(Q)$ keine n-Diedergruppen enthält, ist jetzt das Problem der Bestimmung von $\lambda_{2n}(\mathfrak{M})$ schon vollständig gelöst (Korollar 17.15).
Die Berechnung von $l_{2n}(\mathfrak{M}, f)$ in § 17 enthält inhaltlich gegenüber /19/, /16/ und /17/ keine wesentlich neuen Ideen. Der Paragraf unterscheidet sich fast nur formal von den entsprechenden Beweisen in der angegebenen Literatur.

4. Analog zur Berechnung von $l_{2n}(\mathfrak{M})$ in den Paragrafen 16 und 17 rechne ich in § 18 $l^*_{2n}(\mathfrak{M})$ aus. Ich setze dabei natürlich voraus, daß $\Gamma(Q)$ n-Diedergruppen enthält, d.h. daß $Q \tilde{\in}_k ((\zeta_{2n}-\zeta_{2n}^{-1})^2, -1)_k$.
Da einerseits Q an allen reellen Primstellen von k verzweigt ist (13.4.i), andererseits Q nicht an allen unendlichen Primstellen von k verzweigt sein darf (Vorbemerkung i), muß ich voraussetzen: k ist nicht total reell.

Genauso wie $l_{2n}(\mathfrak{M})$ in eine Summe von $l_{2n}(\mathfrak{M},\mathfrak{f})$ aufgespalten wird, wird $l^*_{2n}(\mathfrak{M})$ in eine Summe von $l^*_{2n}(\mathfrak{M},\mathfrak{f})$ aufgespalten. Sei entsprechend $F^*_{2n}(\mathfrak{M})$ die Menge der $\mathfrak{f} \in I^k$ mit $l^*_{2n}(\mathfrak{M},\mathfrak{f}) > 0$.

Als erstes untersuche ich $F^*_{2n}(\mathfrak{M})$ für die verschiedenen Maximalordnungen $\mathfrak{M}$. Die Methoden sind analog zu denen in § 11 und § 16: Ich bestimme die $\mathfrak{f} \in I^k$, für die es überhaupt eine Maximalordnung $\mathfrak{M}$ mit $\mathfrak{f} \in F^*_{2n}(\mathfrak{M})$ gibt. Dies ist im wesentlichen ein lokales Problem. Den größten Anteil bei der Lösung leistet Lemma (18.5). Es sichert, daß $\mathfrak{f}$ genügend "klein" werden kann. Eine Sonderrolle spielt dabei n = 2.

Jetzt ist es möglich (und wegen der Kompliziertheit des Problems unumgänglich), zu dem System der in Frage kommenden $\mathfrak{f}$ die Existenz eines Systems von Maximalordnungen $\mathfrak{M}^{\mathfrak{f}}$ mit $\mathfrak{f} \in F^*_{2n}(\mathfrak{M}^{\mathfrak{f}})$ nachzuweisen, so daß die $\mathfrak{M}^{\mathfrak{f}}$ bestimmte Beziehungen untereinander haben (Satz 18.9).

Als Analogon zu Satz (11.9.iii,iv) beweise ich Satz (18.16) (Hier spielt die Gruppe der ambigen $\mathfrak{U}^{\mathfrak{f}}$-Ideale die gleiche Rolle, wie in 11.9 die Gruppe aller $\mathfrak{U}^{\mathfrak{f}}$-Ideale): Ist $\mathfrak{f} \in F^*_{2n}(\mathfrak{M})$ für eine bestimmte Maximalordnung $\mathfrak{M}$, so kann ich mit seiner Hilfe alle anderen Maximalordnungen $\mathfrak{M}'$ mit $\mathfrak{f} \in F^*_{2n}(\mathfrak{M}')$ feststellen.

Eine Zusammenfassung der Sätze (18.9) und (18.16) ist Satz (18.18), der als Abschlußergebnis des bisherigen Teils von § 18 aufgefaßt werden kann. In Satz (18.18) wird $F^*_{2n}(\mathfrak{M})$ für alle Q-Maximalordnungen $\mathfrak{M}$ bestimmt. (Für konkrete Rechnungen muß man außerdem i.a. eine Q-Maximalordnung $\mathfrak{M}_0$ mit $\mathfrak{f}_0 \in F^*_{2n}(\mathfrak{M}_0)$ finden, siehe Vorbemerkung iv)

Jetzt bleibt noch $l^*_{2n}(\mathfrak{M},\mathfrak{f})$ für eine feste Q-Maximalordnung mit $\mathfrak{f} \in F^*_{2n}(\mathfrak{M})$ zu berechnen. Dies geschieht problemlos ganz analog zu der Bestimmung von $l_{2n}(\mathfrak{M},\mathfrak{f})$ in § 17 (Lemmata 18.23 und 18.24), nur daß jetzt sogar der erste der dort notwendigen 3 Schritte eingespart werden kann, weil die zweiseitigen $\mathfrak{M}$-Ideale immer einfache Struktur haben (Lemma 18.15).
Ergebnis der Rechnung ist Satz (18.25).

5. In § 19 beschäftige ich mich nur mit algebraischer Zahlentheorie (für Zahlkörper und halbeinfache quadratische Erweiterungen). Es handelt sich zum größten Teil um Folgerungen aus Ergebnissen in /8/. Ich brauche die Formeln des § 19, vom allem Satz (19.10), für die Beispielrechnung in den Paragrafen 20, 21 und 26.

6. $\lambda_{2n}(\mathfrak{M})$ und $\lambda^*_{2n}(\mathfrak{M})$ sind jetzt auf Größen des algebraischen Zahlkörpers k zurückgeführt. Für explizit vorgegebenen Körper k und Quaternionenalgebra Q lassen sich diese Größen im Prinzip berechnen, wenn auch evtl. mit erheblichem Aufwand.
In den Paragrafen 20 (für n = 3) und 21 (für n = 2) löse ich diese Aufgabe für imaginärquadratische Zahlkörper:
Ist $d \in \mathbb{N}$ quadratfrei und $k = \mathbb{Q}(i\sqrt{d})$, so lassen sich $\lambda_6(\mathfrak{M})$ und $\lambda^*_6(\mathfrak{M})$ (bzw. $\lambda_4(\mathfrak{M})$ und $\lambda^*_4(\mathfrak{M})$) im wesentlichen durch die Klassenzahl des (für $d \neq 3$ bzw. $d \neq 1$) reellquadratischen Zahlkörpers $k_+ = \mathbb{Q}(\sqrt{3d})$ (bzw. $k_+ = \mathbb{Q}(\sqrt{d})$) und Größen, die von seiner Grundeinheit abgeleitet sind, ausdrücken. Außerdem benötigt man die Zahl der Primteiler von d und in Einzelfällen müssen quadratische Formen untersucht werden.

Für die 6-zyklischen Gruppen sind die Ergebnisse in (20.39) - (20.41) zusammengefaßt. (Statt λ_6 habe ich jeweils $\lambda'_6 = \lambda_6 - \lambda^*_6$ berechnet.)
Für $1 \leq d \leq 101$ und die Quaternionenalgebra $Q = M_2(k)$ habe ich die Werte mit Hilfe der Tabellen in /1/ explizit berechnet und tabelliert (20.42).
Für die 4-zyklischen Gruppen habe ich die Zusammenfassung der Ergebnisse auf § 26 verschoben (siehe 26.12 - 26.15) und dort auch die Ergebnisse für 2-Dieder- und Tetraedergruppen eingebaut.
Die Methoden bei der Berechnung von $\lambda_6(\mathfrak{M})$, $\lambda^*_6(\mathfrak{M})$, $\lambda_4(\mathfrak{M})$, $\lambda^*_4(\mathfrak{M})$ sind vielfältig. Manche Rechnungen sind wohlbekannt (etwa 20.13) oder folgen fast kanonisch aus bekannten Ergebnissen der Zahlentheorie, andere sind etwas tieferliegend.
Ein neues Ergebnis ist (soviel ich weiß), daß ich für alle imaginärquadratischen Zahlkörper k den Index $[\mathfrak{o}^\times : N(\mathfrak{O}^{\nu\times})]$ berechnen kann. Dabei ist $\mathfrak{O}^\nu$ die Hauptordnung in $K := k(i\sqrt{3})$.
Für $d \not\equiv 1 \bmod 3$ ist die Berechnung mit Hilfe bekannter Ergebnisse leicht. Für $d \equiv 1 \bmod 3$ allerdings ist ein aufwendiger Beweis nötig (Lemma 20.18).
Für K = k(i) läßt sich der gesuchte Index mit Hilfe eines Tricks leichter berechnen; siehe 21.13.
In /16/ und /18/ sind $\lambda_6(\mathfrak{M})$ und $\lambda_4(\mathfrak{M})$ für den Fall reellquadratischer Zahlkörper berechnet worden.
Ein großer Teil der Rechnung verläuft für reell- und imaginärquadratische gleich. Ich konnte daher von den Rechnungen in /16/ profitieren.
Der reellquadratische Fall ist allerdings im Vergleich zum imaginärquadratischen einfacher, da sich schwer zu berechnende Indizes glücklich wegkürzen lassen.

§ 15 . Zurückführung auf Konjugationsklassenzahlen l_{2n} (l^*_{2n}) für Erzeugende von 2n-zyklischen Gruppen (die in n-Diedergruppen enthalten sind).

Für diesen Paragrafen machen wir folgende Generalvoraussetzung:
(15.1): Sei $n \in \mathbb{N}$, $n \geq 2$. Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei $\zeta_{2n} + \zeta_{2n}^{-1} \in k$. Sei Q eine k-Quaternionenalgebra und sei $\mathfrak{M}$ eine Q-Maximalordnung.

Die Konjugationsklassenzahlen λ_{2n} (λ^*_{2n}) der 2n-zyklischen Untergruppen in $\Gamma(\mathfrak{M})$ (die in n-Diedergruppen enthalten sind), lassen sich nicht direkt berechnen.
Das wesentliche Ergebnis von § 15 ist Satz 15.10.iii, der λ_{2n} und λ^*_{2n} durch die entsprechenden Konjugationsklassenzahlen l_{2n} und l^*_{2n} für spezielle Erzeugende der 2n-zyklischen Untergruppen von $\Gamma(\mathfrak{M})$ ausdrückt.
(Die Schlüsselrolle beim Beweis spielt Lemma (15.9).)
Methoden für die Berechnung von l_{2n} und l^*_{2n} entwickeln wir in den folgenden Paragrafen.

(15.2) Definition:
i) $\Lambda_{2n}(\mathfrak{M}) := \{G \subset \Gamma(\mathfrak{M}) \mid G \text{ ist 2n-zyklische Gruppe}\}$
ii) $\Lambda^*_{2n}(\mathfrak{M}) := \{G \in \Lambda_{2n}(\mathfrak{M}) \mid \text{Es gibt eine n-Diedergruppe } G' \text{ mit } G \subset G' \subset \Gamma(\mathfrak{M})\}$
iii) $\Lambda'_{2n}(\mathfrak{M}) := \Lambda_{2n}(\mathfrak{M}) - \Lambda^*_{2n}(\mathfrak{M})$
iv) $L_{2n}(\mathfrak{M}) := \{E \in \Gamma(\mathfrak{M}) \mid S(E) = \zeta_{2n} + \zeta_{2n}^{-1}\}$
v) Sei c die (natürliche) Abbildung $c: L_{2n}(\mathfrak{M}) \to \Lambda_{2n}(\mathfrak{M})$
$E \mapsto \{E^j \mid 0 \leq j < 2n\}$.
vi) $L^*_{2n}(\mathfrak{M}) := c^{-1}(\Lambda^*_{2n}(\mathfrak{M}))$ und $L'_{2n}(\mathfrak{M}) := c^{-1}(\Lambda'_{2n}(\mathfrak{M}))$.

(15.3) Lemma: Sei $n \in \mathbb{N}$, $n > 2$ und sei D eine n-Diedergruppe.
Dann enthält D genau eine 2n-zyklische Gruppe.

Bew.: Seien E, B Erzeuger von D mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$, $S(B) = 0$ und $BEB^{-1} = E^{-1}$. E erzeugt eine 2n-zyklische Gruppe in D.
Es ist $D = \{E^j, E^jB \mid 0 \leq j < 2n\}$. Enthielte D eine weitere 2n-zyklische Gruppe, so würde sie von einem E^jB erzeugt. Aber $(E^jB)^2 = E^jE^{-j}B^2 = -1$.
E^jB hat also die Ordnung $4 < 2n$.

(15.4) Lemma: i) c ist surjektiv.
ii) Für $E \in L_{2n}(\mathfrak{M})$ ist $c^{-1}(c(E)) = \{E, E^{-1}\}$.
iii) $L^*_{2n}(\mathfrak{M}) = \left\{E \in \Gamma(\mathfrak{M}) \;\middle|\; S(E) = \zeta_{2n} + \zeta_{2n}^{-1} \text{ und es gibt } B \in \Gamma(\mathfrak{M}) \text{ mit } S(B) = 0 \text{ und } BEB^{-1} = E^{-1}\right\}$

Bew.: i) klar

ii) "$\supset$" klar

"$\subset$": Sei $E' \in L_{2n}(\mathfrak{M})$ mit $c(E') = c(E)$. Dann ist $E' \in k[E]$ und $S(E') = S(E)$, $N(E') = N(E)$. Nach (2.12) ist $E' = E$ oder $E' = E^*$.

iii) "$\subset$": Sei $E \in L^*_{2n}(\mathfrak{M})$. Falls $n > 2$, erzeugt E die einzige $2n$-zyklische Untergruppe einer n-Diedergruppe $D \subset \Gamma(\mathfrak{M})$. Aus (12.6.ii) folgt jetzt leicht die Existenz des gesuchten B. Für $n = 2$ folgt die Beh. auch leicht aus (12.6.iii).

"$\supset$": klar

(15.5) Definition: i) Zwei Untergruppen $G, G' \subset \Gamma(\mathfrak{M})$ heißen $\Gamma(\mathfrak{M})$-konjugiert, wenn es $M \in \Gamma(\mathfrak{M})$ gibt mit $G' = MGM^{-1}$. Wir schreiben $G \sim G'$.

ii) Zwei Elemente $E, E' \in \Gamma(\mathfrak{M})$ heißen $\Gamma(\mathfrak{M})$-konjugiert, wenn es $M \in \Gamma(\mathfrak{M})$ gibt mit $E' = MEM^{-1}$. Wir schreiben $E \sim E'$.

$\Gamma(\mathfrak{M})$-Konjugation ist in beiden Fällen Äquivalenzrelation.

(15.6) Lemma: i) Seien $E, E' \in L_{2n}(\mathfrak{M})$. Wenn $E \sim E'$, dann $c(E) \sim c(E')$.

ii) Sei $E \in L^*_{2n}(\mathfrak{M})$, $E' \in L'_{2n}(\mathfrak{M})$ (bzw. $G \in \Lambda^*_{2n}(\mathfrak{M})$, $G' \in \Lambda'_{2n}(\mathfrak{M})$). Dann ist $E \not\sim E'$ (bzw. $G \not\sim G'$).

Bew.: i) klar

ii) Es gibt $B \in \Gamma(\mathfrak{M})$ mit $S(B) = 0$, $BEB^{-1} = E^{-1}$. Wäre $E' \sim E$, d.h. $E' = MEM^{-1}$ mit $M \in \Gamma(\mathfrak{M})$, so wäre $B' := MBM^{-1} \in \Gamma(\mathfrak{M})$ und $S(B') = 0$, $B'E'B'^{-1} = E'^{-1}$, also $E' \in L^*_{2n}(\mathfrak{M})$ $\lightning$. Genauso folgt die Beh. für G, G'.

(15.7) Definition:

i) Für $E \in L_{2n}(\mathfrak{M})$ bzw. $G \in \Lambda_{2n}(\mathfrak{M})$ bezeichne $\overline{E}$ bzw. $\overline{G}$ die Restklasse in $L_{2n}(\mathfrak{M})/\sim$ bzw. $\Lambda_{2n}(\mathfrak{M})/\sim$.

ii) $\overline{c}$ bezeichne die durch c induzierte Quotientenabbildung

$$\overline{c}: L_{2n}(\mathfrak{M})/\sim \to \Lambda_{2n}(\mathfrak{M})/\sim .$$

iii) $\lambda_{2n}(\mathfrak{M}) := \not\equiv \Lambda_{2n}(\mathfrak{M})/\sim$; $l_{2n}(\mathfrak{M}) := \not\equiv L_{2n}(\mathfrak{M})/\sim$;

$\lambda^*_{2n}(\mathfrak{M}) := \not\equiv \Lambda^*_{2n}(\mathfrak{M})/\sim$; $l^*_{2n}(\mathfrak{M}) := \not\equiv L^*_{2n}(\mathfrak{M})/\sim$;

$\lambda'_{2n}(\mathfrak{M}) := \not\equiv \Lambda'_{2n}(\mathfrak{M})/\sim$; $l'_{2n}(\mathfrak{M}) := \not\equiv L'_{2n}(\mathfrak{M})/\sim$.

Dies ist alles wohldefiniert wegen Lemma (15.6) und es gilt:

(15.8) Lemma: i) $\overline{c}$ ist surjektiv.

ii) $\lambda_{2n}(\mathfrak{M}) = \lambda^*_{2n}(\mathfrak{M}) + \lambda'_{2n}(\mathfrak{M})$

iii) $l_{2n}(\mathfrak{M}) = l^*_{2n}(\mathfrak{M}) + l'_{2n}(\mathfrak{M})$

iv) Für $E \in L_{2n}(\mathfrak{M})$ gilt: $\overline{c}^{-1}(\overline{c}(\overline{E})) = \overline{c}^{-1}\overline{c(E)} = \{\overline{E}, \overline{E^{-1}}\}$.

Bew.: i), ii), iii) klar

iv) Die linke Gleichung ist klar nach Def. von $\overline{c}$. Zur rechten Gleichung:
"$\subset$": Sei $\overline{E'} \in \overline{c}^{-1}\overline{c(E)}$, d.h. $\overline{c(E')} = \overline{c(E)}$. Dann gibt es $M \in \Gamma(\mathfrak{M})$ mit $c(E') = Mc(E)M^{-1} = c(MEM^{-1})$. Nach (15.4.ii) ist $E' = MEM^{-1}$ oder $E' = (MEM^{-1})^{-1} = ME^{-1}M^{-1}$, also $\overline{E'} \in \{\overline{E}, \overline{E^{-1}}\}$.
"$\supset$" folgt sofort aus (15.4.ii).

(15.9) Lemma: Sei $E \in L_{2n}(\mathfrak{M})$. Genau dann ist $E \sim E^{-1}$, wenn $E \in L^{*}_{2n}(\mathfrak{M})$.

Bew.: Sei $E \in L^{*}_{2n}(\mathfrak{M})$. Dann gibt es $B \in \Gamma(\mathfrak{M})$ mit $BEB^{-1} = E^{-1}$, also ist $E \sim E^{-1}$.
Sei umgekehrt $E \sim E^{-1}$, also $BEB^{-1} = E^{-1}$ mit $B \in \Gamma(\mathfrak{M})$. Wir müssen zeigen, daß $S(B) = 0$. Jedenfalls ist $BE^{-1}B^{-1} = (BEB^{-1})^{-1} = E$.
Damit folgt: $B^2EB^{-2} = E$. B ist nicht mit E vertauschbar, also $B \notin k[E]$.
B^2 ist mit E vertauschbar. Aus (3.2) folgt daher: $B^2 \in k[B] \cap k[E] = k$.
Wegen $B^2 \in \Gamma(\mathfrak{M})$ ist also $B^2 = \pm 1$. Da $B \notin k$ und $N(B) = 1$, ist $B^2 + 1 = 0$ und $S(B) = 0$.

(15.10) Satz: i) Die durch $\overline{c}$ induzierte Abb. $\overline{c}: L^{*}_{2n}(\mathfrak{M})/\sim \to \lambda^{*}_{2n}(\mathfrak{M})/\sim$ ist bijektiv, insbesondere gilt also $\lambda^{*}_{2n}(\mathfrak{M}) = l^{*}_{2n}(\mathfrak{M})$.
ii) Für $G \in \lambda'_{2n}(\mathfrak{M})$ ist $\neq \overline{c}^{-1}(\overline{G}) = 2$, also $\lambda'_{2n}(\mathfrak{M}) = 1/2 \cdot l'_{2n}(\mathfrak{M})$.
iii) $\lambda^{*}_{2n}(\mathfrak{M}) = l^{*}_{2n}(\mathfrak{M})$; $\lambda'_{2n}(\mathfrak{M}) = 1/2 \cdot (l_{2n}(\mathfrak{M}) - l^{*}_{2n}(\mathfrak{M}))$;
$\lambda_{2n}(\mathfrak{M}) = 1/2 \cdot (l_{2n}(\mathfrak{M}) + l^{*}_{2n}(\mathfrak{M}))$.

Bew.: klar

Ein Ziel dieser Arbeit ist es, $\lambda_{2n}(\mathfrak{M})$ für die verschiedenen Maximalordnungen $\mathfrak{M}$ von Q zu berechnen. Dieses Ziel werden wir im wesentlichen erreichen. In den nächsten Paragraphen werden wir l_{2n} und l^{*}_{2n} berechnen. Wegen (15.10) kennen wir dann sogar λ^{*}_{2n} und λ'_{2n}. Wir müssen allerdings eine Einschränkung machen.

(15.11) Satz: Sei k total reeller algebraischer Zahlkörper. Sei Q eine k-Quaternionenalgebra, die an allen unendlichen Primstellen von k verzweigt ist (d.h. $\mu = \mu(Q)$ enthalte alle unendlichen Primstellen von k). Sei $\mathfrak{M}$ eine Q-Maximalordnung. Dann ist $\Gamma(\mathfrak{M})$ eine endliche Gruppe.

Bew.: siehe /7/ S. 129/130 Satz 2

Diesen Fall können wir mit den Mitteln dieser Arbeit nicht behandeln. Wir werden immer vorraussetzen müssen, daß μ nicht alle unendlichen Primstellen von k enthält.

§ 16 . Aufspaltung von l_{2n} in eine Summe $\sum l_{2n}(\mathfrak{f})$. Berechnung der $\mathfrak{f}$, über die summiert werden muß.

Für diesen Paragrafen machen wir folgende Generalvoraussetzung:

(16.1): Sei $n \in \mathbb{N}$, $n \geq 2$. Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei $\zeta_{2n} + \zeta_{2n}^{-1} \in k$. Sei Q eine k-Quaternionenalgebra. $\mathfrak{u} = \mathfrak{u}(Q)$ enthalte nicht alle unendlichen Primstellen von k. Alle Primteiler von $D_k(Q)$ seien verzweigt oder träge in $K := k[X]/\left(X^2-(\zeta_{2n}+\zeta_{2n}^{-1})X+1\right)k[X]$.

In § 16 untersuchen wir (für alle Q-Maximalordnungen $\mathfrak{M}$), welchen Wert $f(\mathfrak{M} \cap k[E])$ für die verschiedenen Erzeugenden E von 2n-zyklischen Gruppen in $\Gamma(\mathfrak{M})$ annimmt (d.h. wir berechnen $F_{2n}(\mathfrak{M})$).
Das wesentliche Ergebnis ist Satz (16.10). Durch ihn sind wir dann Lage, $l_{2n}(\mathfrak{M})$ in eine Summe aufzuspalten (16.4.i), deren Summanden wir im nächsten Paragrafen berechnen werden.
Der Beweis von Satz (16.10) beruht im wesentlichen (wie dort schon angekündigt) auf einer Kombination der Methoden aus § 10 und § 11 (Lemmata 16.7 und 16.8). Um (16.10.i) für die folgenden Paragrafen nützlich formulieren zu können, ziehen wir ein Ergebnis aus der Klassenkörpertheorie (§8) heran (Lemma 16.9).

(16.2) Lemma: Sei $\mathfrak{M}$ eine Q-Maximalordnung und seien $E, E' \in L_{2n}(\mathfrak{M})$. Wenn $E \sim E'$, dann ist $f(\mathfrak{M} \cap k[E]) = f(\mathfrak{M} \cap k[E'])$.

Bew.: Es gibt $M \in \Gamma(\mathfrak{M})$ mit $E' = MEM^{-1}$. Konjugation mit M bewirkt einen k-Algebrenisororphismus $k[E] \to k[E']$. Es ist $M(\mathfrak{M} \cap k[E])M^{-1} = M\mathfrak{M}M^{-1} \cap Mk[E]M^{-1} = \mathfrak{M} \cap k[E']$. Die Beh. folgt aus (6.11).

(16.3) Definition: Sei $\mathfrak{M}$ eine Q-Maximalordnung.

i) Sei $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal. Dann definieren wir

$L_{2n}(\mathfrak{M}, \mathfrak{f}) := \{E \in L_{2n}(\mathfrak{M}) \mid f(\mathfrak{M} \cap k[E]) = \mathfrak{f}\}$ und

$l_{2n}(\mathfrak{M}, \mathfrak{f}) := \#\, L_{2n}(\mathfrak{M}, \mathfrak{f})/\sim$

ii) $$F_{2n}(\mathfrak{M}) := \left\{ \mathfrak{f} \in I^k \;\middle|\; \text{Es gibt } E \in \Gamma(\mathfrak{M}) \text{ mit } S(E) = \zeta_{2n} + \zeta_{2n}^{-1} \text{ und } f(\mathfrak{M} \cap k[E]) = \mathfrak{f} \right\}$$
$$= \{\mathfrak{f} \in I^k \mid L_{2n}(\mathfrak{M}, \mathfrak{f}) \neq \emptyset\}$$

(16.4) Lemma: Sei $\mathfrak{M}$ eine Q-Maximalordnung. Dann gilt:

i) $$l_{2n}(\mathfrak{M}) = \sum_{\mathfrak{f} \in F_{2n}(\mathfrak{M})} l_{2n}(\mathfrak{M}, \mathfrak{f})$$

ii) Ist $\mathfrak{M}'$ eine Q-Maximalordnung vom gleichen Typ wie $\mathfrak{M}$, dann ist $F_{2n}(\mathfrak{M}') = F_{2n}(\mathfrak{M})$. Ist $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal, so ist $l_{2n}(\mathfrak{M}', \mathfrak{f}) = l_{2n}(\mathfrak{M}, \mathfrak{f})$.

Bew.: klar

Wir werden im nächsten Paragrafen sehen, daß für alle Maximalordnungen $\mathfrak{M}$ mit $\mathfrak{f} \in F_{2n}(\mathfrak{M})$ die Werte $l_{2n}(\mathfrak{M}, \mathfrak{f})$ gleich sind (aber abhängig von $\mathfrak{f}$). In diesem Paragrafen wollen wir eine Übersicht über die $F_{2n}(\mathfrak{M})$ gewinnen.

(16.5) Lemma: i) Sei $\mathfrak{M}$ eine Q-Maximalordnung und $\mathfrak{f} \in F_{2n}(\mathfrak{M})$. Dann gilt:

$$\left.\begin{aligned} &\mathfrak{f} + D_k(Q) = \mathfrak{o} \\ \text{und}\quad &\mathfrak{f}^2 D_k(K) \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o} \end{aligned}\right\} \quad (16.6)$$

ii) Sei umgekehrt $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal, das der Bedingung (16.6) genügt. Dann gibt es eine Q-Maximalordnung $\mathfrak{M}$ mit $\mathfrak{f} \in F_{2n}(\mathfrak{M})$.

Bew.: i) Es gibt $E \in \Gamma(\mathfrak{M})$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$ und $f(\mathfrak{M} \cap k[E]) = \mathfrak{f}$. $k[E]$ ist halbeinfache quadratische Erweiterung von k. Nach (11.4) ist $\mathfrak{f} + D_k(Q) = \mathfrak{o}$. Da $E \in \mathfrak{M} \cap k[E]$, gilt $\mathfrak{f}^2 D_k(K) \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}$ nach (6.9.iii), denn $D_k(\mathfrak{M} \cap k[E]) = \mathfrak{f}^2 D_k(K)$ und $D_k(1,E) = (\zeta_{2n} - \zeta_{2n}^{-1})^2$.

ii) Nach Vor. (16.1) und Satz (13.2) gibt es $E \in \Gamma(Q)$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$. $k[E]$ ist halbeinfache quadratische Erweiterung von k. Nach Satz (11.9.ii) gibt es eine Q-Maximalordnung $\mathfrak{M}$ mit $\mathfrak{M} \cap k[E] = \mathfrak{O}^3(k[E])$, d.h. $f(\mathfrak{M} \cap k[E]) = \mathfrak{f}$. Da $\mathfrak{f}^2 D_k(K) \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}$, gilt $E \in \mathfrak{M} \cap k[E]$ nach (6.9.iii). Also ist $E \in \mathfrak{M} \cap \Gamma(Q) = \Gamma(\mathfrak{M})$ und damit $E \in L_{2n}(\mathfrak{M}, \mathfrak{f})$.

(16.7) Lemma: $\mathfrak{M}$, $\mathfrak{M}'$ seien Q-Maximalordnungen. Dann gilt:

i) $F_{2n}(\mathfrak{M}) \cap F_{2n}(\mathfrak{M}') \neq \emptyset \Longrightarrow N(\mathfrak{M}\mathfrak{M}') \in RN(I^K)S_\infty$

ii) $N(\mathfrak{M}\mathfrak{M}') \in RN(I^K)S_\infty \Longrightarrow F_{2n}(\mathfrak{M}) = F_{2n}(\mathfrak{M}')$

(Dabei ist I^K die Gruppe der Ideale (der Hauptordnung) von K; R wie in 9.16.ii)

Bew.: i) Sei $\mathfrak{f} \in F_{2n}(\mathfrak{M}) \cap F_{2n}(\mathfrak{M}')$. Sei $E \in \Gamma(\mathfrak{M})$, $E' \in \Gamma(\mathfrak{M}')$ und $S(E) = S(E') = \zeta_{2n} + \zeta_{2n}^{-1}$ und $f(\mathfrak{M} \cap k[E]) = f(\mathfrak{M}' \cap k[E']) = \mathfrak{f}$. Durch die Vorschrift $E' \mapsto E$ wird ein k-Algebrenisomorphismus $\sigma: k[E'] \to k[E]$ definiert, der sich nach Satz (3.3) zu einem k-Algebrenautomorphismus $\sigma: Q \to Q$ fortsetzen läßt. Es gibt $M \in Q^\times$ mit $MxM^{-1} = \sigma x$ für alle $x \in Q$. Nach Lemma (6.11) ist $\sigma(\mathfrak{M}' \cap k[E']) = \mathfrak{M} \cap k[E]$, also $M\mathfrak{M}'M^{-1} \cap k[E] = \mathfrak{M} \cap k[E]$.
Nach Satz (11.9.iii) gibt es ein $(\mathfrak{M} \cap k[E])$-Ideal $\mathfrak{a}$ mit $\mathfrak{M} = \mathfrak{a}M\mathfrak{M}'M^{-1}\mathfrak{a}^{-1}$. Dann ist $\mathfrak{M}\mathfrak{a}M = \mathfrak{a}M\mathfrak{M}'$ ein Ideal mit Linksordnung $\mathfrak{M}$ und Rechtsordnung $\mathfrak{M}'$. Es gibt also ein zweiseitiges $\mathfrak{M}$-Ideal $\mathfrak{A}$ mit $\mathfrak{A}\mathfrak{M}\mathfrak{M}' = \mathfrak{M}\mathfrak{a}M$. Wegen $I^{k(2)} \subset N(I^K)$ folgt mit (7.9.ii): $N(\mathfrak{M}\mathfrak{M}') = N(\mathfrak{A})^{-1}N(\mathfrak{a})N(M) \in RN(I^K)S_\infty$.

ii) Wir zeigen: $F_{2n}(\mathfrak{M}) \subset F_{2n}(\mathfrak{M}')$. Wenn $F_{2n}(\mathfrak{M}) = \emptyset$, ist nichts zu zeigen. Sei also $\mathfrak{f} \in F_{2n}(\mathfrak{M})$, sei $E \in \Gamma(\mathfrak{M})$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$ und $f(\mathfrak{M} \cap k[E]) = \mathfrak{f}$. Sei $\mathcal{O} := \mathfrak{M} \cap k[E]$.
Nach Vor. gibt es ein zweiseitiges $\mathfrak{M}'$-Ideal $\mathfrak{A}$, ein $\mathcal{O}$-Ideal $\mathfrak{a}$ und $M \in Q^\times$ mit $\mathfrak{a}\mathfrak{M}\mathfrak{M}'\mathfrak{A} = M\mathfrak{M}'$. Die Linksordnung dieses Ideals ist $\mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1} = M\mathfrak{M}'M^{-1}$. Nach Satz (11.9.iv) ist $M\mathfrak{M}'M^{-1} \cap k[E] = \mathcal{O}$, also $f(M\mathfrak{M}'M \cap k[E]) = \mathfrak{f}$ und $E \in M\mathfrak{M}'M^{-1}$.
Das heißt: $\mathfrak{f} \in F_{2n}(M\mathfrak{M}'M^{-1}) = F_{2n}(\mathfrak{M}')$.

(16.8) Lemma: Seien $\mathfrak{f}$ und $\mathfrak{f}'$ ganze $\mathfrak{o}$-Ideale, die der Bedingung (16.6) genügen. Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{f} \in F_{2n}(\mathfrak{M})$.
Genau dann ist $\mathfrak{f}' \in F_{2n}(\mathfrak{M})$, wenn $\mathfrak{f}\mathfrak{f}'^{-1} \in RN(I^K)S_{\mathfrak{m}}$.

Bew.: Sei $E \in \Gamma(\mathfrak{M})$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$ und $f(\mathfrak{M} \cap k[E]) = \mathfrak{f}$.
Nach Satz (11.9.i) gibt es eine Q-Maximalordnung $\mathfrak{M}'$ mit $f(\mathfrak{M}' \cap k[E]) = \mathfrak{f}'$ und $N(\mathfrak{M}\mathfrak{M}')\mathfrak{f}\mathfrak{f}'^{-1} \in I^{k(2)} \subset RN(I^K)S_{\mathfrak{m}}$.
Da $\mathfrak{f}'^2 D_k(K) \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}$, ist $E \in \mathfrak{M}' \cap k[E]$, also $\mathfrak{f}' \in F_{2n}(\mathfrak{M}')$.
i) Sei $\mathfrak{f}' \in F_{2n}(\mathfrak{M})$. Nach (16.7.i) ist dann $N(\mathfrak{M}\mathfrak{M}') \in RN(I^K)S_{\mathfrak{m}}$, also $\mathfrak{f}\mathfrak{f}'^{-1} \in RN(I^K)S_{\mathfrak{m}}$.
ii) Sei umgekehrt $\mathfrak{f}\mathfrak{f}' \in RN(I^K)S_{\mathfrak{m}}$. Dann ist $N(\mathfrak{M}\mathfrak{M}') \in RN(I^K)S_{\mathfrak{m}}$, nach (16.7.ii) also $\mathfrak{f}' \in F_{2n}(\mathfrak{M})$.

(16.9) Lemma: Es ist $[I^k : RN(I^K)S_{\mathfrak{m}}] = 2$ genau dann, wenn $\zeta_{2n} \notin k$, $D_k(K) = \mathfrak{o}$ und $Q \tilde{k} ((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_k$.
Sonst ist $[I^k : RN(I^K)S_{\mathfrak{m}}] = 1$.

Bew.: Es ist $[I^k : RN(I^K)S_{\mathfrak{m}}] \leq [I^k : N(I^K)S_{\mathfrak{m}}] \leq 2$ nach (7.26.ii) und (8.4.i).
i) Sei $[I^k : RN(I^K)S_{\mathfrak{m}}] = 2$. Wegen (7.26.ii) muß K Körper sein, d.h. $\zeta_{2n} \notin k$. Es ist $[I^k : N(I^K)S_{\mathfrak{m}}] = 2$. Nach (8.4.ii) ist $D_K(K) = \mathfrak{o}$ und K ist höchstens an den reellen Primstellen $\mathfrak{p}$ verzweigt, für die gilt: $\mathfrak{p} \mid \mathfrak{m}$. Da aber K an allen reellen Primstellen von k verzweigt ist, enthält $\mathfrak{m}$ alle reellen Primstellen von k, d.h. Q ist an allen reellen Primstellen von k verzweigt.
Sei jetzt $\mathfrak{p}$ eine endliche Verzweigungsstelle von Q über k (Widerspruchsannahme). Nach Vor (16.1) ist $\mathfrak{p}$ verzweigt oder träge in K.
Wegen $D_k(K) = \mathfrak{o}$ ist $\mathfrak{p}$ träge in K. Nach (8.4.iii) ist $\mathfrak{p} \notin N(I^K)S_{\mathfrak{m}}$.
Da $\mathfrak{p} \in R$, ist $[I^k : RN(I^K)S_{\mathfrak{m}}] < [I^k : N(I^K)S_{\mathfrak{m}}]$, also $[I^k : RN(I^K)S_{\mathfrak{m}}] = 1$ ↯.

Q ist also genau an den reellen Primstellen von k verzweigt.
Wir müssen noch $Q \tilde{k} ((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_k$ zeigen. Wegen Satz (1.10.iii) müssen wir also zeigen, daß auch $Q' := ((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_k$ genau an den reellen Primstellen von k verzweigt ist. Nach (13.4.i) ist Q' an allen reellen Primstellen von k verzweigt. Da K keine endlichen Verzweigungsstellen über k hat, hat nach (13.4.iv) auch Q' keine endlichen Verzweigungsstellen über k.

ii) Sei $\zeta_{2n} \notin k$, $D_k(K) = \mathfrak{o}$ und $Q \tilde{k} ((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_k$.
Wie in i) zeigt man, daß Q und K genau an den reellen Primstellen von k verzweigt sind. K ist Körper und $R = \{\mathfrak{o}\}$. Wegen (8.4.ii) ist also $[I^k : RN(I^K)S_\mathfrak{u}] = [I^k : N(I^K)S_\mathfrak{u}] = 2$.

(16.10) Satz: Voraussetzung (16.1).

i) Sei $\zeta_{2n} \notin k$
und $D_k(K) = \mathfrak{o}$
und $Q \tilde{k} ((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_k$ } (16.11)

Sei $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal mit $\mathfrak{f}^2 \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}$ und sei $\mathfrak{M}$ eine (wegen 16.5.ii existierende) Q-Maximalordnung mit $\mathfrak{f} \in F_{2n}(\mathfrak{M})$.
Dann gilt für alle Q-Maximalordnungen $\mathfrak{M}'$:

$$F_{2n}(\mathfrak{M}') = \begin{cases} \{\mathfrak{f}' \in I^k \mid \mathfrak{f}'^2 \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o} \text{ und } \mathfrak{f}\mathfrak{f}'^{-1} \in N(I^K)S_\mathfrak{u}\}, \\ \text{falls } N(\mathfrak{M}\mathfrak{M}') \in N(I^K)S_\mathfrak{u} \\ \{\mathfrak{f}' \in I^k \mid \mathfrak{f}'^2 \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o} \text{ und } \mathfrak{f}\mathfrak{f}'^{-1} \notin N(I^K)S_\mathfrak{u}\}, \\ \text{falls } N(\mathfrak{M}\mathfrak{M}') \notin N(I^K)S_\mathfrak{u} \end{cases}$$

ii) Sei (16.11) nicht erfüllt. Dann gilt für alle Q-Maximalordnungen $\mathfrak{M}$:

$$F_{2n}(\mathfrak{M}) = \{\mathfrak{f} \in I^k \mid \mathfrak{f} + D_k(Q) = \mathfrak{o} \text{ und } \mathfrak{f}^2 D_k(K) \mid (\zeta_{2n} - \zeta_{2n}^{-1})\mathfrak{o}\}.$$

Bew.: i) Sei $\mathfrak{f}' \in I^k$ mit $\mathfrak{f}'^2 \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}$ und sei $\mathfrak{M}'$ eine Q-Maximalordnung.
Falls $N(\mathfrak{M}\mathfrak{M}') \in RN(I^K)S_\mathfrak{u} = N(I^K)S_\mathfrak{u}$, ist $\mathfrak{f} \in F_{2n}(\mathfrak{M}')$ wegen (16.7.ii).
Also ist $\mathfrak{f}' \in F_{2n}(\mathfrak{M}')$ genau dann, wenn $\mathfrak{f}\mathfrak{f}'^{-1} \in N(I^K)S_\mathfrak{u}$ wegen (16.8).
Sei jetzt $N(\mathfrak{M}\mathfrak{M}') \notin N(I^K)S_\mathfrak{u}$. Wegen (16.7.i) ist $\mathfrak{f} \notin F_{2n}(\mathfrak{M}')$.
Falls $\mathfrak{f}\mathfrak{f}'^{-1} \in N(I^K)S_\mathfrak{u}$, ist $\mathfrak{f}' \notin F_{2n}(\mathfrak{M}')$ wegen (16.8). Sei $\mathfrak{f}\mathfrak{f}'^{-1} \notin N(I^K)S_\mathfrak{u}$.
Wegen (16.8) ist $\mathfrak{f}' \notin F_{2n}(\mathfrak{M})$.

Wegen (16.5.ii) gibt es eine Q-Maximalordnung $\mathfrak{M}''$ mit $f' \in F_{2n}(\mathfrak{M}'')$.

Wegen (16.7.ii) ist $N(\mathfrak{M}''\mathfrak{M}) \notin N(I^K)S_{\mathfrak{M}}$.
Da $[I^k : N(I^K)S_{\mathfrak{M}}] = 2$, ist $N(\mathfrak{M}''\mathfrak{M})N(\mathfrak{M}\mathfrak{M}') \in N(I^K)S_{\mathfrak{M}}$. Wegen (10.9.ii) ist $N(\mathfrak{M}'\mathfrak{M}'')N(\mathfrak{M}''\mathfrak{M})N(\mathfrak{M}\mathfrak{M}') \in RI^{k(2)}S_{\mathfrak{M}} \subset N(I^K)S_{\mathfrak{M}}$, also $N(\mathfrak{M}'\mathfrak{M}'') \in N(I^K)S_{\mathfrak{M}}$. Nach (16.7.ii) ist $f' \in F_{2n}(\mathfrak{M}')$.
Die Beh. folgt mit (16.5.i).

ii) Wegen $I^k = RN(I^K)S_{\mathfrak{M}}$ folgt die Beh. leicht aus den Lemmata 16.5, 16.7, 16.8.

(16.12) Lemma: Voraussetzung (16.1). Sei (16.11) erfüllt. Sei $\mathfrak{g} \in I^k$.
Dann gilt: $\mathfrak{g} \in N(I^K)S_{\mathfrak{M}}$ genau dann, wenn $\prod_{\mathfrak{p}} \left(\frac{K}{\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{g})} = 1$.

Dabei ist das Produkt über alle endlichen Primstellen $\mathfrak{p}$ von k (mit $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{g}) \neq 0$) zu nehmen.

Bew.: Sei $\mathfrak{p}$ ein Primideal aus k. Nach (8.4.iii) ist
$\mathfrak{p} \in N(I^K)S_{\mathfrak{M}}$ genau dann, wenn $\left(\frac{K}{\mathfrak{p}}\right) = 1$ und
$\mathfrak{p} \notin N(I^K)S_{\mathfrak{M}}$ genau dann, wenn $\left(\frac{K}{\mathfrak{p}}\right) = -1$.
Wegen $[I^k : N(I^K)S_{\mathfrak{M}}] = 2$ folgt die Beh. jetzt leicht durch Zusammensetzen.

(16.13) Bemerkung:
i) Falls (16.11) nicht erfüllt ist, ist das Problem der Berechnung von $F_{2n}(\mathfrak{M})$ vollständig gelöst (16.10.ii).
Falls (16.11) erfüllt ist, bleibt noch folgendes Problem offen:
Wie findet man für vorgegebenes $f \in I^k$ mit $f^2 \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}$ aus einem gegebenen Repräsentantensystem von $\tilde{Q}$ eine "Anfangsmaximalordnung" $\mathfrak{M}$ mit $f \in F_{2n}(\mathfrak{M})$?
ii) Falls (16.11) erfüllt ist und alle Primteiler von $(\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}$ in K zerlegt sind (und nur dann), ist für die Hälfte aller Maximalordnungstypen $\tilde{\mathfrak{M}} \in \tilde{Q}$: $F_{2n}(\mathfrak{M}) = \emptyset$, also $l_{2n}(\mathfrak{M}) = 0$.

§ 17 . Berechnung von $l_{2n}(\mathfrak{f})$

Für diesen Paragrafen machen wir folgende Generalvoraussetzung:

(17.1) Sei $n \in \mathbb{N}$, $n \geq 2$. Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei $\zeta_{2n} + \zeta_{2n}^{-1} \in k$. Sei Q eine k-Quaternionenalgebra. $\mathcal{M} = \mathcal{M}(Q)$ enthalte nicht alle unendlichen Primstellen von k. Alle Primteiler von $D_k(Q)$ seien verzweigt oder träge in $K := k[X]/(X^2 - (\zeta_{2n} + \zeta_{2n}^{-1})X + 1)k[X]$. Sei $t = t(Q,n)$ die Zahl der Primteiler von $D_k(Q)$, die in K träge sind. Sei $\mathfrak{f} \in I^k$ mit $\mathfrak{f} + D_k(Q) = \mathfrak{o}$ und $\mathfrak{f}^2 D_k(K) \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}$. Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{f} \in F_{2n}(\mathfrak{M})$. Wir kürzen $\Gamma := \Gamma(\mathfrak{M})$ ab.

Wir wollen $l_{2n}(\mathfrak{M}, \mathfrak{f})$ berechnen. Nach Vor. ist $L_{2n}(\mathfrak{M}, \mathfrak{f}) \neq \emptyset$. Wir wählen (für diesen Paragrafen) ein festes $E \in \Gamma(\mathfrak{M})$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$ und $\mathfrak{o}^{\mathfrak{f}} := \mathfrak{o}^{\mathfrak{f}}(k[E]) = \mathfrak{M} \cap k[E]$. $I^{\mathfrak{f}}$ sei die Gruppe der $\mathfrak{o}^{\mathfrak{f}}$-Ideale usw.

(17.2) Lemma: i) Zu jedem $E' \in L_{2n}(\mathfrak{M}, \mathfrak{f})$ gibt es $M \in Q^\times$ mit $E' = MEM^{-1}$.

ii) Sei $M \in Q^\times$. Genau dann ist $MEM^{-1} \in L_{2n}(\mathfrak{M}, \mathfrak{f})$, wenn es $\mathcal{A} \in \mathfrak{M}_I\mathfrak{M}$ und $\mathfrak{a} \in I^{\mathfrak{f}}$ gibt mit $\mathfrak{M}M = \mathcal{A}\mathfrak{a}$.

Bew.: i) klar wegen (3.4)

ii) Sei $MEM^{-1} \in L_{2n}(\mathfrak{M}, \mathfrak{f})$. Dann ist $f(M^{-1}\mathfrak{M}M \cap k[E]) = f(M^{-1}(\mathfrak{M} \cap k[MEM^{-1}])M) = f(\mathfrak{M} \cap k[MEM^{-1}]) = \mathfrak{f}$. Nach Satz (11.9.iii) gibt es $\mathfrak{a} \in I^{\mathfrak{f}}$ mit $\mathfrak{M} = \mathfrak{a}M^{-1}\mathfrak{M}M\mathfrak{a}^{-1}$. Dann ist $\mathcal{A} := M\mathfrak{a}^{-1}\mathfrak{M} = \mathfrak{M}M\mathfrak{a}^{-1} \in \mathfrak{M}_I\mathfrak{M}$ und $\mathfrak{M}M = \mathcal{A}\mathfrak{a}$.
Seien umgekehrt $\mathcal{A} \in \mathfrak{M}_I\mathfrak{M}$ und $\mathfrak{a} \in I^{\mathfrak{f}}$ mit $\mathfrak{M}M = \mathcal{A}\mathfrak{a}$ gegeben. Die Rechtsordnung dieses Ideals ist $M^{-1}\mathfrak{M}M = \mathfrak{a}^{-1}\mathfrak{M}\mathfrak{a}$. Nach Satz (11.9.iv) ist $f(M^{-1}\mathfrak{M}M \cap k[E]) = \mathfrak{f}$, also $f(\mathfrak{M} \cap k[MEM^{-1}]) = \mathfrak{f}$.
Aus $\mathfrak{f}^2 D_k(K) \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}$ folgt $MEM^{-1} \in \mathfrak{M} \cap k[MEM^{-1}]$, also $MEM^{-1} \in L_{2n}(\mathfrak{M}, \mathfrak{f})$.

(17.3) Definition: i) Sei $\eta: Q^\times \to \mathfrak{M}_I$ die Abbildung mit $\eta(M) = \mathfrak{M}M$ für $M \in Q^\times$.

ii) Sei $e: Q^\times \to \Gamma(Q)$ die Abbildung mit $e(M) = MEM^{-1}$ für $M \in Q^\times$.

iii) Sei $\mathfrak{M}_I\mathfrak{M}_I^{\mathfrak{f}}$ die Menge der Produkte $\mathcal{A}\mathfrak{a}$ mit $\mathcal{A} \in \mathfrak{M}_I\mathfrak{M}$, $\mathfrak{a} \in I^{\mathfrak{f}}$.

iv) Sei $\mathfrak{M}_I^{\mathfrak{f}}$ die Menge der Ideale $\mathfrak{M}\mathfrak{a}$ mit $\mathfrak{a} \in I^{\mathfrak{f}}$.

Lemma (17.2) besagt dann: $e^{-1}(L_{2n}(\mathfrak{M}, \mathfrak{f})) = \eta^{-1}(\mathfrak{M}_I\mathfrak{M}_I^{\mathfrak{f}})$ und e induziert eine surjektive Abb. $e: \eta^{-1}(\mathfrak{M}_I\mathfrak{M}_I^{\mathfrak{f}}) \to L_{2n}(\mathfrak{M}, \mathfrak{f})$.

(17.4) Lemma: Sei $M \in \eta^{-1}(\mathfrak{M}_I \mathfrak{M}_I \mathfrak{f})$

i) Sei $\gamma \in \Gamma$ und $a \in k[E]^\times$. Dann ist $\gamma Ma \in \eta^{-1}(\mathfrak{M}_I \mathfrak{M}_I \mathfrak{f})$.

ii) Sei $M' \in \eta^{-1}(\mathfrak{M}_I \mathfrak{M}_I \mathfrak{f})$. Genau dann ist $M'EM'^{-1} \sim MEM^{-1}$, wenn es $\gamma \in \Gamma$ und $a \in k[E]^\times$ gibt mit $M' = \gamma MA$.

Bew.: i) Sei $\mathfrak{M} M = \mathcal{A}\mathfrak{a}$ mit $\mathcal{A} \in \mathfrak{M}_I\mathfrak{M}$ und $\mathfrak{a} \in I^\mathfrak{f}$.
Dann ist $\mathfrak{M}\gamma Ma = \mathfrak{M} Ma = \mathcal{A}\mathfrak{a}a$ und $\mathfrak{a}a \in I^\mathfrak{f}$.

ii) Sei $M'EM'^{-1} \sim MEM^{-1}$. Dann gibt es $\gamma \in \Gamma$ mit $M'EM'^{-1} = \gamma MEM^{-1}\gamma^{-1}$
d.h. $M^{-1}\gamma^{-1}M'E = EM^{-1}\gamma^{-1}M'$. Aus (3.2) folgt: $a := M^{-1}\gamma^{-1}M' \in k[E] \cap Q^\times = k[E]^\times$.
Sei umgekehrt $M' = \gamma Ma$ mit $\gamma \in \Gamma$ und $a \in k[E]^\times$. Dann ist
$M'EM'^{-1} = \gamma MaEa^{-1}M^{-1}\gamma^{-1} = \gamma MEM^{-1}\gamma^{-1}$, also $M'EM'^{-1} \sim MEM^{-1}$.

(17.5) Definition: Sei $p: \eta^{-1}(\mathfrak{M}_I \mathfrak{M}_I \mathfrak{f}) \to \Gamma\backslash\eta^{-1}(\mathfrak{M}_I \mathfrak{M}_I \mathfrak{f})/k[E]^\times$
die natürliche Projektion.

Nach Lemma (17.4) induziert e eine Abbildung $\bar{e}$:

$$\bar{e}: \Gamma\backslash\eta^{-1}(\mathfrak{M}_I \mathfrak{M}_I \mathfrak{f})/k[E]^\times \to L_{2n}(\mathfrak{M}, \mathfrak{f})/\sim$$
$$p(M) \qquad\qquad \mapsto \overline{MEM^{-1}}$$

Da e surjektiv ist, ist auch $\bar{e}$ surjektiv. Nach (17.4.ii) ist $\bar{e}$ injektiv.

(17.6) Korollar: $l_{2n}(\mathfrak{M}, \mathfrak{f}) = \#\,(\Gamma\backslash\eta^{-1}(\mathfrak{M}_I \mathfrak{M}_I \mathfrak{f})/k[E]^\times)$

Wie man leicht sieht, ist $\mathfrak{M}_I\mathfrak{M} \cap \mathfrak{M}_I\mathfrak{f}$ eine Untergruppe von $\mathfrak{M}_I\mathfrak{M}$.
Für $\mathcal{A} \in \mathfrak{M}_I\mathfrak{M}$ bezeichnen wir mit $\bar{\mathcal{A}}$ die Restklasse im Quotienten
$\mathfrak{M}_I\mathfrak{M}/(\mathfrak{M}_I\mathfrak{M} \cap \mathfrak{M}_I\mathfrak{f})$.

(17.7) Lemma: Wir können eine Abbildung
$\phi: \Gamma\backslash\eta^{-1}(\mathfrak{M}_I \mathfrak{M}_I \mathfrak{f})/k[E]^\times \to \mathfrak{M}_I\mathfrak{M}/(\mathfrak{M}_I\mathfrak{M} \cap \mathfrak{M}_I\mathfrak{f})$
folgendermaßen definieren: Ist $M \in \eta^{-1}(\mathfrak{M}_I \mathfrak{M}_I \mathfrak{f})$, also $\mathfrak{M} M = \mathcal{A}\mathfrak{a}$
mit $\mathcal{A} \in \mathfrak{M}_I\mathfrak{M}$ und $\mathfrak{a} \in I^\mathfrak{f}$, so setzen wir $\phi(p(M)) := \bar{\mathcal{A}}$.
ϕ hat folgende Eigenschaften:

i) $$l_{2n}(\mathfrak{M}, \mathfrak{f}) = \sum_{\bar{\mathcal{A}} \in \mathrm{Bild}\ \phi} \#\,\phi^{-1}(\bar{\mathcal{A}})$$

ii) $$\#\,\mathrm{Bild}\ \phi = 2^t \cdot \frac{[I^k : RN(I^K)S_n]}{[I^k : N(I^K)S_n]}$$

Bew.: Wohldefiniertheit: Seien $M, M' \in \eta^{-1}(\mathfrak{M}_I \mathfrak{M}_I \mathfrak{f})$, sei $\mathfrak{M} M = \mathcal{A}\mathfrak{a}$
und $\mathfrak{M} M' = \mathcal{A}'\mathfrak{a}'$ mit $\mathcal{A}, \mathcal{A}' \in \mathfrak{M}_I\mathfrak{M}$ und $\mathfrak{a}, \mathfrak{a}' \in I^\mathfrak{f}$.
Sei $M' = \gamma Ma$ mit $\gamma \in \Gamma$ und $a \in k[E]^\times$. Dann ist
$\mathcal{A}^{-1}\mathcal{A}' = \mathcal{A}^{-1}M'\mathfrak{a}'^{-1} = \mathcal{A}^{-1}\gamma Ma\mathfrak{a}'^{-1} = \mathcal{A}^{-1}Ma\mathfrak{a}'^{-1} = \mathcal{A}^{-1}\mathcal{A}\mathfrak{a}a\mathfrak{a}'^{-1} = \mathfrak{M}\mathfrak{a}a\mathfrak{a}'^{-1}$.

i) folgt sofort mit (17.6)

ii) Sei $\mathcal{A} \in {}^{\mathfrak{M}}I^{\mathfrak{M}}$. Man sieht leicht ein, daß $\overline{\mathcal{A}} \in$ Bild ϕ genau dann, wenn es $M \in Q^{\times}$ und $\alpha \in I^{\mathfrak{f}}$ gibt mit $\mathfrak{M} M = \mathcal{A} \alpha$. Dies ist genau dann der Fall, wenn $N(\mathcal{A}) \in N(I^{\mathfrak{f}})S_{\mathfrak{m}}$. Bild ϕ ist also Untergruppe von ${}^{\mathfrak{M}}I^{\mathfrak{M}} / ({}^{\mathfrak{M}}I^{\mathfrak{M}} \cap {}^{\mathfrak{M}}I^{\mathfrak{f}})$ und zwar ist Bild ϕ gleich dem Kern des durch Normbildung induzierten Homomorphismus:

$\overline{N}$: ${}^{\mathfrak{M}}I^{\mathfrak{M}} / ({}^{\mathfrak{M}}I^{\mathfrak{M}} \cap {}^{\mathfrak{M}}I^{\mathfrak{f}}) \to N({}^{\mathfrak{M}}I^{\mathfrak{M}}) / \left(N({}^{\mathfrak{M}}I^{\mathfrak{M}}) \cap N(I^{\mathfrak{f}})S_{\mathfrak{m}}\right)$.

Wegen $N(I^{\mathfrak{f}}) = N(I^K)$ also: $\#$ Bild $\phi = \dfrac{\left[{}^{\mathfrak{M}}I^{\mathfrak{M}} : {}^{\mathfrak{M}}I^{\mathfrak{M}} \cap {}^{\mathfrak{M}}I^{\mathfrak{f}}\right]}{\left[N({}^{\mathfrak{M}}I^{\mathfrak{M}}) : N({}^{\mathfrak{M}}I^{\mathfrak{M}}) \cap N(I^K)S_{\mathfrak{m}}\right]}$

Wegen (9.18.ii) ist $\left[N({}^{\mathfrak{M}}I^{\mathfrak{M}}) : N({}^{\mathfrak{M}}I^{\mathfrak{M}}) \cap N(I^K)S_{\mathfrak{m}}\right] =$

$= \left[RI^{k(2)} : RI^{k(2)} \cap N(I^K)S_{\mathfrak{m}}\right] = \left[RN(I^K)S_{\mathfrak{m}} : N(I^K)S_{\mathfrak{m}}\right] = \dfrac{\left[I^k : N(I^K)S_{\mathfrak{m}}\right]}{\left[I^k : RN(I^K)S_{\mathfrak{m}}\right]}$

Wir müssen also noch zeigen:

(17.8) Lemma: $\left[{}^{\mathfrak{M}}I^{\mathfrak{M}} : {}^{\mathfrak{M}}I^{\mathfrak{M}} \cap {}^{\mathfrak{M}}I^{\mathfrak{f}}\right] = 2^t$

Bew.: Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ die endlichen Verzweigungsstellen von Q über k, die in K träge sind. Die anderen endlichen Primstellen von k seien auch mit Nummern, von t+1 an, versehen. Für $i \in \mathbb{N}$ sei $\mathfrak{q}_i$ das Primideal von $\mathfrak{M}$ mit $\mathfrak{q}_i = \mathfrak{M}\,\mathfrak{p}_i$ bzw. $\mathfrak{q}_i^2 = \mathfrak{M}\,\mathfrak{p}_i$. Einem Ideal $\mathcal{A} \in {}^{\mathfrak{M}}I^{\mathfrak{M}}$, $\mathcal{A} = \prod_i \mathfrak{q}_i^{r_i}$ ordnen wir das Tupel $T(\mathcal{A}) := (\bar{r}_1, \ldots, \bar{r}_t)$ zu, wobei $\bar{r}_i$ die Restklasse von r_i in $\mathbb{Z}/2\mathbb{Z}$ ist. Wir haben so einen surjektiven Homomorphismus T: ${}^{\mathfrak{M}}I^{\mathfrak{M}} \to (\mathbb{Z}/2\mathbb{Z})^t$ definiert.

Wir müssen noch zeigen, daß Kern $T = {}^{\mathfrak{M}}I^{\mathfrak{M}} \cap {}^{\mathfrak{M}}I^{\mathfrak{f}}$.

zu "$\supset$": Sei $\mathcal{A} = \prod_i \mathfrak{q}_i^{r_i} \in {}^{\mathfrak{M}}I^{\mathfrak{M}} \cap {}^{\mathfrak{M}}I^{\mathfrak{f}}$. Es ist $N(\mathcal{A}) = \left(\prod_{i \le t} \mathfrak{p}_i^{r_i}\right) N\left(\prod_{i>t} \mathfrak{q}_i^{r_i}\right)$

Es ist $N(\mathcal{A}) \in N(I^{\mathfrak{f}}) = N(I^K)$. Da $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ träge in K sind, müssen die $r_1, \ldots, r_t$ gerade sein.

zu "$\subset$": Sei $\mathcal{A} = \prod_i \mathfrak{q}_i^{r_i} \in$ Kern T. Wir zeigen, daß für alle $i \in \mathbb{N}$ gilt:

$$\mathfrak{q}_i^{r_i} \in {}^{\mathfrak{M}}I^{\mathfrak{M}} \cap {}^{\mathfrak{M}}I^{\mathfrak{f}}.$$

a) Sei $\mathfrak{q}_i = \mathfrak{M}\,\mathfrak{p}_i$ mit einem Primideal $\mathfrak{p}_i$ aus k. Dann ist

$\mathfrak{q}_i^{r_i} = \mathfrak{M}(\mathfrak{p}_i \mathfrak{U}^{\mathfrak{f}})^{r_i}$.

b) Sei $\mathfrak{q}_i^2 = \mathfrak{M}\,\mathfrak{p}_i$ und $1 < i < t$. Dann ist nach Voraussetzung r_i gerade und $\mathfrak{q}_i^{r_i} = \mathfrak{M}(\mathfrak{p}_i \mathfrak{U}^{\mathfrak{f}})^{r_i/2}$.

c) Sei $\mathfrak{p}_i^2 = \mathfrak{M}\mathfrak{p}_i$ und $\mathfrak{p}_i$ verzweigt in K. Wir lassen den Index i weg. Da $\mathfrak{p} \mid D_k(Q)$, ist $\mathfrak{p} + \mathfrak{f} = \mathfrak{o}$. Es gibt also ein $\mathfrak{O}_\mathfrak{p}^\mathfrak{f}$-Ideal $\mathfrak{a}^\mathfrak{p}$ mit $\mathfrak{p}\,\mathfrak{O}_\mathfrak{p}^\mathfrak{f} = (\mathfrak{a}^\mathfrak{p})^2$, $\mathfrak{a}^{\mathfrak{p}*} = \mathfrak{a}^\mathfrak{p}$. Nach Satz (9.11.i) ist $\mathfrak{M}_\mathfrak{p}\,\mathfrak{a}^\mathfrak{p}$ ein zweiseitiges $\mathfrak{M}_\mathfrak{p}$-Ideal. Da $N(\mathfrak{M}_\mathfrak{p}\,\mathfrak{a}^\mathfrak{p}) = \mathfrak{p}_\mathfrak{p}$, ist $\mathfrak{p}_\mathfrak{p} = \mathfrak{M}_\mathfrak{p}\,\mathfrak{a}^\mathfrak{p}$. Wir definieren ein $\mathfrak{O}^\mathfrak{f}$-Ideal $\mathfrak{a}$ durch die Vorschrift $\mathfrak{a}_\mathfrak{p} := \mathfrak{a}^\mathfrak{p}$ und $\mathfrak{a}_{\mathfrak{p}'} = \mathfrak{O}_{\mathfrak{p}'}^\mathfrak{f}$ für $\mathfrak{p}' \neq \mathfrak{p}$. Dann ist $\mathfrak{p} = \mathfrak{M}\mathfrak{a}$, $\mathfrak{p}^r = \mathfrak{M}\mathfrak{a}^r$. q.e.d.
Wir haben außerdem folgendes Korollar bewiesen, das wir später brauchen:

(17.9) Korollar: Falls $\mathcal{A} \in {}^{\mathfrak{M}_I}\mathfrak{M} \cap \mathfrak{M}_{I^\mathfrak{f}}$, dann gibt es $\mathfrak{a} \in I^\mathfrak{f}$ mit $\mathcal{A} = \mathfrak{M}\mathfrak{a}$ und $\mathfrak{a}^* = \mathfrak{a}$.

Zur weiteren Berechnung von $l_{2n}(\mathfrak{M}, \mathfrak{f})$ brauchen wir:

(17.10) Lemma: Seien $\mathfrak{a}, \mathfrak{a}' \in I^\mathfrak{f}$ mit $\mathfrak{M}\mathfrak{a} = \mathfrak{M}\mathfrak{a}'$. Dann ist $\mathfrak{a} = \mathfrak{a}'$.

Bew.: Wir zeigen $\mathfrak{a}_\mathfrak{p} = \mathfrak{a}'_\mathfrak{p}$ für alle endlichen Primstellen $\mathfrak{p}$ von k. Sei $\mathfrak{a}_\mathfrak{p} = a\,\mathfrak{O}_\mathfrak{p}^\mathfrak{f}$, $\mathfrak{a}'_\mathfrak{p} = a'\mathfrak{O}_\mathfrak{p}^\mathfrak{f}$ mit $a, a' \in k[E]_\mathfrak{p}^\times$. Dann ist $\mathfrak{M}_\mathfrak{p} a = \mathfrak{M}_\mathfrak{p} a'$, also $\mathfrak{M}_\mathfrak{p} a a'^{-1} = \mathfrak{M}_\mathfrak{p}$, also $aa'^{-1} \in \mathfrak{M}_\mathfrak{p}^\times \cap k[E]_\mathfrak{p} = \mathfrak{O}_\mathfrak{p}^{\mathfrak{f}\times}$ (6.13.i, 9.20.ii).

Wir wählen jetzt ein festes $\mathcal{A} \in {}^{\mathfrak{M}_I}\mathfrak{M}$ mit $\overline{\mathcal{A}} \in \text{Bild } \phi$.
Zu jedem $M \in p^{-1}(\phi^{-1}(\overline{\mathcal{A}}))$ gibt es ein eindeutig bestimmtes $\mathfrak{a} \in I^\mathfrak{f}$ mit $\mathfrak{M}M = \mathcal{A}\mathfrak{a}$. Wir wählen ein festes $M_0 \in p^{-1}(\phi^{-1}(\overline{\mathcal{A}}))$.
Zu jedem $M \in p^{-1}(\phi^{-1}(\overline{\mathcal{A}}))$ gibt es dann ein eindeutig bestimmtes $\mathfrak{a} \in I^\mathfrak{f}$ mit $\mathfrak{M}M = \mathfrak{M}M_0\,\mathfrak{a}$.

Für $\mathfrak{a} \in I^\mathfrak{f}$ bezeichnen wir die Restklasse in $I^\mathfrak{f}/H^\mathfrak{f}$ mit $\overline{\mathfrak{a}}$.

(17.11) Lemma: Wir können eine Abbildung $\psi: \phi^{-1}(\overline{\mathcal{A}}) \to I^\mathfrak{f}/H^\mathfrak{f}$ folgendermaßen definieren: Ist $M \in p^{-1}(\phi^{-1}(\overline{\mathcal{A}}))$, also $\mathfrak{M}M = \mathfrak{M}M_0\,\mathfrak{a}$ mit $\mathfrak{a} \in I^\mathfrak{f}$, so setzen wir $\psi(p(M)) := \overline{\mathfrak{a}}$.
ψ hat folgende Eigenschaften:

i) $\#\,\phi^{-1}(\overline{\mathcal{A}}) = \sum_{\overline{\mathfrak{a}} \in \text{Bild } \psi} \#\,\psi^{-1}(\overline{\mathfrak{a}})$

ii) $\#\,\text{Bild } \psi = \dfrac{[I^\mathfrak{f} : H^\mathfrak{f}]}{[I^k : S_\mathcal{A}]} \cdot [I^k : N(I^K)S_\mathcal{A}]$

Bew.: Wohldefiniertheit: Seien $M, M' \in p^{-1}(\phi^{-1}(\overline{\mathcal{A}}))$, sei $\mathfrak{M}M = \mathfrak{M}M_0\,\mathfrak{a}$ und $\mathfrak{M}M' = \mathfrak{M}M_0\,\mathfrak{a}'$ mit $\mathfrak{a}, \mathfrak{a}' \in I^\mathfrak{f}$ und sei $M' = \gamma M a$ mit $\gamma \in \Gamma$ und $a \in k[E]^\times$. Dann ist $\mathfrak{M}M_0\,\mathfrak{a}' = \mathfrak{M}M' = \mathfrak{M}\gamma M a = \mathfrak{M}Ma = \mathfrak{M}M_0\,\mathfrak{a}a$, also $\mathfrak{a}' = \mathfrak{a}a$.

i) klar

ii) Sei $\alpha \in I^{\mathfrak{p}}$. Man sieht leicht ein, daß $\bar{\alpha} \in$ Bild ψ genau dann, wenn es $M \in Q^{\times}$ gibt mit $\mathfrak{M} M = \mathfrak{M} M_0 \alpha$. Dies ist genau dann der Fall, wenn $N(\alpha) \in S_{\mathfrak{u}}$. Falls $\alpha \in H^{\mathfrak{p}}$, ist selbstverständlich $N(\alpha) \in S_{\mathfrak{u}}$.
Bild ψ ist also Untergruppe von $I^{\mathfrak{p}}/H^{\mathfrak{p}}$ und zwar ist Bild ψ genau der Kern der durch Normbildung induzierten Abb. $\overline{N}: I^{\mathfrak{p}}/H^{\mathfrak{p}} \to N(I^{\mathfrak{p}})/S_{\mathfrak{u}} \cap N(I^{\mathfrak{p}})$
Also ist $\#$ Bild $\psi = [I^{\mathfrak{p}} : H^{\mathfrak{p}}]/[N(I^{\mathfrak{p}}) : S_{\mathfrak{u}} \cap N(I^{\mathfrak{p}})]$ und es ist

$$[N(I^{\mathfrak{p}}) : S_{\mathfrak{u}} \cap N(I^{\mathfrak{p}})] = [N(I^K)S_{\mathfrak{u}} : S_{\mathfrak{u}}] = \frac{[I^K : S_{\mathfrak{u}}]}{[I^K : N(I^K)S_{\mathfrak{u}}]} .$$

Wir wählen jetzt ein <u>festes</u> $\alpha \in I^{\mathfrak{p}}$ mit $\bar{\alpha} \in$ Bild ψ und ein <u>festes</u> $M \in p^{-1}(\psi^{-1}(\bar{\alpha}))$. Es gibt dann zu jedem $M' \in p^{-1}(\psi^{-1}(\bar{\alpha}))$ ein $a \in k[E]^{\times}$ mit $\mathfrak{M} M' = \mathfrak{M} Ma$.

<u>(17.12) Lemma:</u> $\Gamma(M\mathcal{O}^{\mathfrak{p}}M^{-1})^{\times} = \Gamma\mathcal{O}^{\mathfrak{p}\times}$ ist Normalteiler von $\mathfrak{M}^{\times}$.

<u>Bew.:</u> Wir betrachten die Normabbildung $N: \mathfrak{M}^{\times} \to \mathfrak{u}^{\times}$.
Es sind $\mathcal{O}^{\mathfrak{p}} \subset \mathfrak{M}$ und $M\mathcal{O}^{\mathfrak{p}}M^{-1} \subset \mathfrak{M}$ und offensichtlich gilt $N(\mathcal{O}^{\mathfrak{p}\times}) = N((M\mathcal{O}^{\mathfrak{p}}M^{-1})^{\times})$. Also ist $\Gamma\mathcal{O}^{\mathfrak{p}\times} = N^{-1}(N(\mathcal{O}^{\mathfrak{p}\times})) = \Gamma(M\mathcal{O}^{\mathfrak{p}}M^{-1})^{\times}$ Normalteiler.

Für die Restklasse von $\varepsilon \in \mathfrak{M}^{\times}$ in $\mathfrak{M}^{\times}/\Gamma(M\mathcal{O}^{\mathfrak{p}}M^{-1})^{\times}$ schreiben wir $\bar{\varepsilon}$.

<u>(17.13) Lemma:</u> Wir können eine Abbildung $\chi: \psi^{-1}(\bar{\alpha}) \to \mathfrak{M}^{\times}/\Gamma(M\mathcal{O}^{\mathfrak{p}}M^{-1})^{\times}$ folgendermaßen definieren: Ist $M' \in p^{-1}(\psi^{-1}(\bar{\alpha}))$, also $\mathfrak{M} M' = \mathfrak{M} Ma$ mit $a \in k[E]^{\times}$, so setzen wir $\chi(p(M')) := \overline{M'a^{-1}M^{-1}}$.
χ ist bijektiv. Insbesondere gilt: $\# \psi^{-1}(\bar{\alpha}) = [\mathfrak{u}^{\times} : N(\mathcal{O}^{\mathfrak{p}\times})]$.

<u>Bew.:</u> <u>Wohldefiniertheit:</u> Seien M', $M'' \in p^{-1}(\psi^{-1}(\bar{\alpha}))$, sei $\mathfrak{M} M' = \mathfrak{M} Ma'$ und $\mathfrak{M} M'' = \mathfrak{M} Ma''$ mit $a', a'' \in k[E]^{\times}$ und sei $M'' = \gamma M'a$ mit $\gamma \in \Gamma$ und $a \in k[E]^{\times}$. Dann ist
$\mathfrak{M} M'a'^{-1}M^{-1} = \mathfrak{M} M''a''^{-1}M^{-1} = \mathfrak{M}$, also sind $M'a'^{-1}M^{-1}$, $M''a''^{-1}M^{-1} \in \mathfrak{M}^{\times}$.
Daher gibt es $\gamma' \in \Gamma$ mit $(M'a'^{-1}M^{-1})^{-1}\gamma = \gamma'(M'a'^{-1}M^{-1})^{-1} = \gamma' Ma'M'^{-1}$.
Also: $(M'a'^{-1}M^{-1})^{-1}(M''a''^{-1}M^{-1}) = \gamma' Ma'M'^{-1}\gamma^{-1}\gamma M'aa''^{-1}M^{-1}$
$= \gamma' Ma'aa''^{-1}M^{-1}$
Die Beh. folgt wegen $Ma'aa''^{-1}M^{-1} \in \mathfrak{M}^{\times} \cap Mk[E]^{\times}M^{-1} = M\mathcal{O}^{\mathfrak{p}\times}M^{-1}$.
<u>Injektivität:</u> Seien M', $M'' \in p^{-1}(\psi^{-1}(\bar{\alpha}))$, sei $\mathfrak{M} M' = \mathfrak{M} Ma'$ und $\mathfrak{M} M'' = \mathfrak{M} Ma''$ mit $a', a'' \in k[E]^{\times}$. Sei $\overline{M'a'^{-1}M^{-1}} = \overline{M''a''^{-1}M^{-1}}$.
Dann gibt es $\gamma \in \Gamma$ und $a \in \mathcal{O}^{\mathfrak{p}\times}$ mit $M''a''^{-1}M^{-1} = (M'a'^{-1}M^{-1})\gamma(MaM^{-1})$.
Es gibt $\gamma' \in \Gamma$ mit $M'a'^{-1}M^{-1}\gamma = \gamma' M'a'^{-1}M^{-1}$, also
$M'' = \gamma'(M'a'^{-1}M^{-1})(MaM^{-1})Ma'' = \gamma' M'a'^{-1}aa''$, d.h. $p(M'') = p(M')$.

Surjektivität: Sei $\varepsilon \in \mathfrak{M}^\times$. Wir setzen $M' := \varepsilon M$. Dann ist $\mathfrak{M} M' = \mathfrak{M} \varepsilon M = \mathfrak{M} M$, also $M' \in p^{-1}(\psi^{-1}(\bar{\alpha}))$. Es ist $\chi(p(M')) = \overline{M'M^{-1}} = \bar{\varepsilon}$.
Wir haben damit: $\# \psi^{-1}(\bar{\alpha}) = [\mathfrak{M}^\times : \Gamma(M\mathcal{O}^\beta M^{-1})^\times]$.
Nach dem Homomorphiesatz (7.6), angewandt auf N, gilt:
$\# \psi^{-1}(\bar{\alpha}) = [N(\mathfrak{M}^\times) : N(\Gamma(M\mathcal{O}^\beta M^{-1})^\times)] \cdot [\Gamma : \Gamma \cap \Gamma(M\mathcal{O}^\beta M^{-1})^\times]$.
Nach Satz (10.5) ist also $\# \psi^{-1}(\alpha) = [\mathfrak{U}^\times : N(\mathcal{O}^{\beta\times})]$.

Aus den Lemmata (17.7), (17.11) und (17.13) folgt jetzt:

(17.14) Satz: Voraussetzung (17.1). Dann ist

$$l_{2n}(\mathfrak{M}, \beta) = 2^t \cdot [I^k : RN(I^K)S_\mathfrak{u}] \frac{[I^\beta : H^\beta]}{[I^k : S_\mathfrak{u}]} \cdot [\mathfrak{U}^\times : N(\mathcal{O}^{\beta\times})].$$

Ist u die Zahl der unendlichen (d.h. reellen) Verzweigungsstellen von Q über k, so ist:

$$l_{2n}(\mathfrak{M}, \beta) =$$

$$2^{t-u} \cdot [I^k : RN(I^K)S_\mathfrak{u}] \frac{[I^K : H^K]}{[I^k : H^k]} \cdot \frac{[\mathfrak{o}^\times : N(\mathcal{O}^{\beta\times})]}{[\mathcal{O}^\times : \mathcal{O}^{\beta\times}]} \cdot \mathfrak{N}(\beta) \cdot \prod_{\mathfrak{p} \mid \beta} \left(1 - \left(\frac{K}{\mathfrak{p}}\right) \mathfrak{N}(\mathfrak{p})^{-1}\right)$$

Die zweite Formel folgt mit (7.25) und (8.5)

(17.15) Korollar: Sei $n \in \mathbb{N}$, $n \geq 2$. Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei $\zeta_{2n} + \zeta_{2n}^{-1} \in k$. Sei Q eine k-Quaternionenalgebra. $\mathfrak{u}$ enthalte nicht alle unendlichen Primstellen von k. Alle Primteiler von $D_k(Q)$ seien verzweigt oder träge in $K := k[X]/(X^2 - (\zeta_{2n}+\zeta_{2n}^{-1})X + 1)k[X]$.
Sei $Q \not\cong_k ((\zeta_{2n} - \zeta_{2n}^{-1})^2, -1)_k$.
Dann ist für alle Q-Maximalordnungen $\mathfrak{M}$: $\lambda_{2n}^*(\mathfrak{M}) = 0$,

$$F_{2n}(\mathfrak{M}) = \{ \beta \in I^k \mid \beta + D_k(Q) = \mathfrak{o} \text{ und } \beta^2 D_k(K) \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o} \} \text{ und}$$

$$\lambda_{2n}(\mathfrak{M}) = 2^{t-u-1} \frac{[I^K : H^K]}{[I^k : H^k]} \sum_{\beta \in F_{2n}(\mathfrak{M})} \left(\frac{[\mathfrak{o}^\times : N(\mathcal{O}^{\beta\times})]}{[\mathcal{O}^\times : \mathcal{O}^{\beta\times}]} \cdot \mathfrak{N}(\beta) \cdot \prod_{\mathfrak{p} \mid \beta} \left(1 - \left(\frac{K}{\mathfrak{p}}\right) \mathfrak{N}(\mathfrak{p})^{-1}\right) \right)$$

Hierin sind die Ergebnisse für die (engeren) Modulgruppen aus /16/ und /17/ enthalten.

§ 18 . Berechnung der $l_{2n}^* = \sum l_{2n}^*(\mathfrak{f})$

Ähnlich, wie wir in den Paragrafen 16 und 17 die Klassenzahlen l_{2n} berechnet haben, wollen wir jetzt l_{2n}^* berechnen. (Hauptergebnisse sind 18.18 und 18.25) Dazu müssen wir in diesem Paragrafen noch einige Lemmata über optimale Einbettung erarbeiten, da die allgemeinen Ergebnisse aus § 11 nicht ausreichen. Außer für diese Lemmata machen wir für den ganzen Paragrafen folgende

Generalvoraussetzung (18.1): Sei $n \in \mathbb{N}$, $n \geq 2$. Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei $\zeta_{2n} + \zeta_{2n}^{-1} \in k$. k sei nicht total reell. Sei Q eine k-Quaternionenalgebra, sei
$Q \cong_k ((\zeta_{2n}-\zeta_{2n}^{-1})^2, -1)_k$ und sei $K := k[X]/(X^2 - (\zeta_{2n}+\zeta_{2n}^{-1})X + 1)k[X]$.

Da Q an allen reellen Primstellen von k verzweigt ist, ist die Bedingung, daß k nicht total reell ist, äquivalent zu der Bedingung, daß $\mathfrak{m}$ nicht alle unendlichen Primstellen von k enthält.

Ist $\mathfrak{M}$ eine Q-Maximalordnung, so gilt Lemma (16.2) für $L_{2n}^*(\mathfrak{M})$ entsprechend. Wir können also definieren:

(18.2) Definition: Sei $\mathfrak{M}$ eine Q-Maximalordnung.
i) Sei $\mathfrak{f} \in I^k$. Dann definieren wir:

$$L_{2n}^*(\mathfrak{M},\mathfrak{f}) := \{E \in L_{2n}^*(\mathfrak{M}) \mid f(\mathfrak{M} \cap k[E]) = \mathfrak{f}\}$$

$$= \left\{ E \in \Gamma(\mathfrak{M}) \;\middle|\; \begin{array}{l} S(E) = \zeta_{2n}+\zeta_{2n}^{-1},\ f(\mathfrak{M} \cap k[E]) = \mathfrak{f} \\ \text{und es gibt } B \in \Gamma(\mathfrak{M}) \text{ mit } BEB^{-1} = E^{-1} \end{array} \right\}$$

$$l_{2n}^*(\mathfrak{M},\mathfrak{f}) := \#\, L_{2n}^*(\mathfrak{M},\mathfrak{f})/\sim$$

ii) $$F_{2n}^*(\mathfrak{M}) := \left\{ \mathfrak{f} \in I^k \;\middle|\; \begin{array}{l} \text{Es gibt } E, B \in \Gamma(\mathfrak{M}) \text{ mit } S(E) = \zeta_{2n}+\zeta_{2n}^{-1}, \\ BEB^{-1} = E^{-1} \text{ und } f(\mathfrak{M} \cap k[E]) = \mathfrak{f} \end{array} \right\}$$

$$= \{\mathfrak{f} \in I^k \mid L_{2n}^*(\mathfrak{M},\mathfrak{f}) \neq \emptyset\}$$

(18.3) Lemma: Sei $\mathfrak{M}$ eine Q-Maximalordnung. Dann gilt:
i) $l_{2n}^*(\mathfrak{M}) = \sum_{\mathfrak{f} \in F_{2n}^*(\mathfrak{M})} l_{2n}^*(\mathfrak{M},\mathfrak{f})$
ii) Ist $\mathfrak{M}'$ eine Q-Maximalordnung vom gleichen Typ wie $\mathfrak{M}$, dann ist $F_{2n}^*(\mathfrak{M}') = F_{2n}^*(\mathfrak{M})$. Ist $\mathfrak{f} \in I^k$, so ist $l_{2n}^*(\mathfrak{M}',\mathfrak{f}) = l_{2n}^*(\mathfrak{M},\mathfrak{f})$.
iii) $F_{2n}^*(\mathfrak{M}) \subset F_{2n}(\mathfrak{M})$.

Bew.: klar

(18.4) Lemma: Sei $n \in \mathbb{N}$, $n \geq 2$. Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathcal{O}$. Sei $\zeta_{2n}+\zeta_{2n}^{-1} \in k$ und $Q = ((\zeta_{2n}-\zeta_{2n}^{-1})^2, -1)_k$. Seien $E, B \in \Gamma(Q)$ mit $S(E) = \zeta_{2n}+\zeta_{2n}^{-1}$ und $BEB^{-1} = E^{-1}$ und sei $\mathcal{U}$ die Hauptordnung in $k[E]$. Dann gibt es eine Q-Maximalordnung $\mathfrak{M}$ mit $B \in \mathfrak{M}$ und $\mathfrak{M} \cap k[E] = \mathcal{U}$.

Bew.: Wegen $BEB^{-1} = E^*$ ist $BAB^{-1} = A^*$ für alle $A \in k[E]$. Jetzt rechnet man leicht nach, daß $(\mathcal{U} + \mathcal{U}B)\cdot(\mathcal{U} + \mathcal{U}B) = \mathcal{U} + \mathcal{U}B$. Also ist $\mathcal{U} + \mathcal{U}B$ eine Q-Ordnung. Sie ist in einer Q-Maximalordnung $\mathfrak{M}$ enthalten.
Es gilt $B \in \mathfrak{M}$ und $\mathcal{U} \subset \mathfrak{M}$, also $\mathfrak{M} \cap k[E] = \mathcal{U}$.

(18.5) Lemma: Sei $n \in \mathbb{N}$, $n \geq 2$. Sei k ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathcal{O}$. Sei $\zeta_{2n}+\zeta_{2n}^{-1} \in k$. Sei Q eine k-Quaternionenalgebra, $Q \tilde{k} ((\zeta_{2n}-\zeta_{2n}^{-1})^2, -1)_k \tilde{k} M_2(k)$. Seien $E, B \in \Gamma(Q)$ mit $S(E) = \zeta_{2n}+\zeta_{2n}^{-1}$ und $BEB^{-1} = E^{-1}$.
Sei -1 Quadratrest mod $(\zeta_{2n}-\zeta_{2n}^{-1})^2$ in $\mathcal{O}$ oder sei $n = 2$.
Dann gibt es eine Q-Maximalordnung $\mathfrak{M}$ mit $\mathfrak{M} \cap k[E] \subset \mathcal{O}[E]$ und $B \in \mathfrak{M}$.

Bew.: Sei $\mathcal{U}$ die Hauptordnung von $k[E]$, sei $\{1,\omega\}$ eine Basis von $\mathcal{U}$ über $\mathcal{O}$.
Sei π ein Primelement von $\mathcal{O}$ und $D_k(\mathcal{U}) = D_k(1,\omega)\mathcal{O} =: \pi^r\mathcal{O}$.
Sei $f(\mathcal{O}[E]) =: \pi^s\mathcal{O}$. Dann ist $\{1,\pi^s\omega\}$ eine Basis von $\mathcal{O}[E]$ über $\mathcal{O}$
und $(\zeta_{2n}-\zeta_{2n}^{-1})^2\mathcal{O} = D_k(1,E)\mathcal{O} = D_k(\mathcal{O}[E]) = \pi^{r+2s}\mathcal{O}$.
i) Sei -1 Quadratrest mod $(\zeta_{2n}-\zeta_{2n}^{-1})^2$ in $\mathcal{O}$.
Seien $a, b \in \mathcal{O}$ mit $-1 = a^2 + b(\zeta_{2n}-\zeta_{2n}^{-1})^2$. Seien $M_{11}, M_{12}, M_{21}, M_{22} \in Q$
Matrizeseinheiten und sei $B' := aM_{11} + bM_{12} + (\zeta_{2n}-\zeta_{2n}^{-1})^2M_{21} - aM_{22}$.
Dann ist $S(B') = 0 = S(B)$ und $N(B') = -a^2 - b(\zeta_{2n}-\zeta_{2n}^{-1})^2 = 1 = N(B)$.
Nach Satz (3.3) gibt es einen k-Algebrenautomorphismus $\sigma: Q \to Q$ mit $\sigma B' = B$.
Dann sind $\begin{pmatrix}1&0\\0&0\end{pmatrix} := \sigma M_{11}$, $\begin{pmatrix}0&1\\0&0\end{pmatrix} := \sigma M_{12}$, $\begin{pmatrix}0&0\\1&0\end{pmatrix} := \sigma M_{21}$, $\begin{pmatrix}0&0\\0&1\end{pmatrix} := \sigma M_{22}$
Matrizeseinheiten und es ist $B = \begin{pmatrix}a & b\\ (\zeta_{2n}-\zeta_{2n}^{-1})^2 & -a\end{pmatrix} \in \begin{pmatrix}\mathcal{O} & \mathcal{O}\\ \pi^{r+2s}\mathcal{O} & \mathcal{O}\end{pmatrix} =: \mathfrak{M}'$.
Sei $f(\mathfrak{M}' \cap k[E]) =: \pi^t\mathcal{O}$, dann ist $t = \min\{t' \mid \pi^{t'}\omega \in \mathfrak{M}'\}$.
$\mathfrak{M}'' := \mathcal{O} + \mathcal{O}\pi^t\omega + \mathcal{O}B + \mathcal{O}\pi^t\omega B$ ist offenbar eine Q-Ordnung und es ist $\mathfrak{M}'' \subset \mathfrak{M}'$, also $D_k(\mathfrak{M}') \mid D_k(\mathfrak{M}'')$. Offenbar ist $D_k(\mathfrak{M}') = \pi^{2r+4s}\mathcal{O}$ und

$$
\begin{aligned}
D_k(\mathfrak{M}'') &= D_k(1,\pi^t\omega,B,\pi^t\omega B)\,\mathfrak{o} \\
&= \pi^{4(t-s)} D_k(1,\pi^s\omega,B,\pi^s\omega B)\,\mathfrak{o} \\
&= \pi^{4t-4s} D_k(\mathfrak{o} + \pi^s\omega\,\mathfrak{o} + B\,\mathfrak{o} + \pi^s\omega B\,\mathfrak{o}) \\
&= \pi^{4t-4s} D_k(\mathfrak{o} + \mathfrak{o}E + \mathfrak{o}B + \mathfrak{o}EB) \\
&= \pi^{4t-4s} D_k(1,E,B,EB)\,\mathfrak{o} \\
&= \pi^{4t-4s} (\zeta_{2n}-\zeta_{2n}^{-1})^4\,\mathfrak{o} \\
&= \pi^{4t-4s}\,\pi^{2r+4s}\,\mathfrak{o}
\end{aligned}
$$

Es ist also $t \geq s$.

Sei $\mathfrak{M}_0 := \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{o} \end{pmatrix}$, $\mathfrak{M}_1 := \begin{pmatrix} \mathfrak{o} & \pi^{-r-2s}\mathfrak{o} \\ \pi^{r+2s}\mathfrak{o} & \mathfrak{o} \end{pmatrix}$.

$\mathfrak{M}_0$ und $\mathfrak{M}_1$ sind Q-Maximalordnungen mit $\mathfrak{M}' \subset \mathfrak{M}_0$, $\mathfrak{M}' \subset \mathfrak{M}_1$.

Insbesondere ist $B \in \mathfrak{M}_i$ und $\pi^t\omega \in \mathfrak{M}_i$ für $i = 0, 1$.

Es ist $\mathfrak{M}' = \mathfrak{M}_0 \cap \mathfrak{M}_1$. Wegen $\pi^{t-1}\omega \notin \mathfrak{M}'$ gibt es also $\mathfrak{M} \in \{\mathfrak{M}_0, \mathfrak{M}_1\}$ mit $\pi^{t-1}\omega \notin \mathfrak{M}$. Dann ist also $f(\mathfrak{M} \cap k[E]) = \pi^t\mathfrak{o}$.

Wegen $t \geq s$ und $f(\mathfrak{o}[E]) = \pi^s\mathfrak{o}$ ist also $\mathfrak{M} \cap k[E] \subset \mathfrak{o}[E]$.

<u>ii)</u> Sei $n = 2$, d.h. $\zeta_{2n} + \zeta_{2n}^{-1} = 0$ und $(\zeta_{2n} - \zeta_{2n}^{-1})^2 = -4$.

Es sind $E,B \in \Gamma(Q)$ und $S(E) = S(B) = 0$ und $EB = -BE$.

Nach (18.4) gibt es eine Q-Maximalordnung $\mathfrak{M}'$ mit $E, B \in \mathfrak{M}'$.

Es gibt Matrizeseinheiten $\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix} \in Q$ mit $\mathfrak{M}' = \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{o} \end{pmatrix}$.

Es gibt also $a,b,c,d \in \mathfrak{o}$ und $i \in \mathbb{N}_0$ mit $E = \begin{pmatrix} a & b \\ \pi^i c & d \end{pmatrix}$.

Wenn $c = 0$ ist, ist $0 = S(E) = a+d$ und $1 = N(E) = -a^2$.

Insbesondere ist dann -1 Quadratrest mod $(\zeta_{2n}-\zeta_{2n}^{-1})^2$ in $\mathfrak{o}$ und die Behauptung folgt wie in i).

Sei also $c \neq 0$ und i sei o.B.d.A. so gewählt, daß $c \in \mathfrak{o}^\times$.

Genauso können wir annehmen, daß es $a',b',d' \in \mathfrak{o}$, $c' \in \mathfrak{o}^\times$ und $j \in \mathbb{N}_0$ gibt mit $B = \begin{pmatrix} a' & b' \\ \pi^j c' & d' \end{pmatrix}$. Wir machen eine Fallunterscheidung.

<u>a) Sei $i \leq j$.</u> Wir definieren $\mathfrak{M} := \begin{pmatrix} \mathfrak{o} & \pi^{-i}\mathfrak{o} \\ \pi^i\mathfrak{o} & \mathfrak{o} \end{pmatrix}$. Es sind $E, B \in \mathfrak{M}$.

$\{1,E\}$ und $\{1,\pi^s\omega\}$ sind Basen von $\mathfrak{o}[E]$ über $\mathfrak{o}$. Daher gibt es

$\alpha,\beta,\gamma,\delta \in \mathfrak{o}$ mit: $\pi^s\omega = \alpha E + \beta\cdot 1$

$1 = \gamma E + \delta\cdot 1$

und $\alpha\delta - \beta\gamma \in \mathfrak{o}^\times$.

Wegen der zweiten Gleichung muß $\gamma = 0$ sein, wegen der dritten also $\alpha \in \mathfrak{o}^\times$.

Natürlich ist $\pi^s\omega = \alpha E + \beta \in \mathfrak{M}$.

Aber $\pi^{s-1}\omega = \begin{pmatrix} \pi^{-1}\alpha a + \pi^{-1}\beta & \pi^{-1}\alpha b \\ \pi^{i-1}\alpha c & \pi^{-1}\alpha d + \pi^{-1}\beta \end{pmatrix} \notin \mathfrak{M}$ wegen $\alpha c \in \mathfrak{o}^\times$.

Also ist $f(\mathfrak{M} \cap k[E]) = \pi^s\mathfrak{o} = f(\mathfrak{o}[E])$, d.h. $\mathfrak{M} \cap k[E] = \mathfrak{o}[E]$.

b) Sei $i > j$. Wie in a) kann man zeigen, daß es eine Maximalordnung $\mathfrak{M}'$ gibt mit $E, B \in \mathfrak{M}'$ und $\mathfrak{M}' \cap k[B] = \mathfrak{o}[B]$. (Man vertausche E und B)

Durch die Vorschriften $E \mapsto B$ und $B \mapsto E$ wird ein k-Algebrenautomorphismus $\sigma: Q \to Q$ definiert. Wir setzen $\mathfrak{M} = \sigma\mathfrak{M}'$.

Dann sind $E, B \in \mathfrak{M}$ und $\mathfrak{M} \cap k[E] = \sigma(\mathfrak{M}' \cap k[B]) = \sigma(\mathfrak{o}[B]) = \mathfrak{o}[E]$.

(18.6) Lemma: Gleiche Voraussetzung wie in (18.5). Dann gibt es ein System $\{\mathfrak{M}^{\mathfrak{f}} \mid \mathfrak{f}$ ist ganzes $\mathfrak{o}$-Ideal und $\mathfrak{f} \mid f(\mathfrak{o}[E])\}$ von Q-Maximalordnungen, so daß für alle ganzen $\mathfrak{o}$-Ideale $\mathfrak{f}, \mathfrak{f}'$ mit $\mathfrak{f} \mid f(\mathfrak{o}[E])$ und $\mathfrak{f}' \mid f(\mathfrak{o}[E])$ gilt: $B \in \mathfrak{M}^{\mathfrak{f}}$, $f(\mathfrak{M}^{\mathfrak{f}} \cap k[E]) = \mathfrak{f}$ und $N(\mathfrak{M}^{\mathfrak{f}}\mathfrak{M}^{\mathfrak{f}'}) = \mathfrak{f}^{-1}\mathfrak{f}' + \mathfrak{f}\mathfrak{f}'^{-1}$, also insbesondere $N(\mathfrak{M}^{\mathfrak{f}}\mathfrak{M}^{\mathfrak{f}'})\mathfrak{f}\mathfrak{f}'^{-1} \in I^{k(2)}$.

Bew.: Wir kürzen $\mathfrak{O}^{\mathfrak{f}} = \mathfrak{O}^{\mathfrak{f}}(k[E])$ ab. Sei π ein Primelement in $\mathfrak{o}$.

Nach (18.4) und (18.5) gibt es Q-Maximalordnungen $\mathfrak{M}, \mathfrak{M}'$ mit $B \in \mathfrak{M} \cap \mathfrak{M}'$, $\mathfrak{M} \cap k[E] = \mathfrak{O}^{\mathfrak{o}}$ und $\mathfrak{M}' \cap k[E] \subset \mathfrak{o}[E]$. Nach (11.1) gibt es Matrizeseinheiten $\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix} \in Q$ und $t \in \mathbb{N}_0$ mit $\mathfrak{M} = \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{o} \end{pmatrix}$ und $\mathfrak{M}' = \begin{pmatrix} \mathfrak{o} & \pi^{-t}\mathfrak{o} \\ \pi^t\mathfrak{o} & \mathfrak{o} \end{pmatrix}$.

Falls $f(\mathfrak{o}[E]) = \mathfrak{o}$, ist nichts zu zeigen.

Sei also $f(\mathfrak{o}[E]) \neq \mathfrak{o}$, insbesondere also $t > 0$.

Sei $\{1, \omega\}$ Basis von $\mathfrak{O}^{\mathfrak{o}}$ über $\mathfrak{o}$. Wegen $\mathfrak{O}^{\mathfrak{o}} \subset \mathfrak{M}$ gibt es $a,b,c,d \in \mathfrak{o}$ und $u \in \mathbb{N}_0$ mit $\omega = \begin{pmatrix} a & b \\ \pi^u c & d \end{pmatrix}$. Wäre $c = 0$, so wäre $\omega \in \mathfrak{M}'$, also auch $\omega \in \mathfrak{o}[E]$ entgegen unserer Annahme. Es ist also $c \neq 0$. Sei u so gewählt, daß $c \in \mathfrak{o}^\times$. Wegen $\omega \notin \mathfrak{M}'$ ist $t > u$.

Es ist $\pi^{t-u}\omega = \begin{pmatrix} \pi^{t-u}a & \pi^{t-u}b \\ \pi^t c & \pi^{t-u}d \end{pmatrix} \in \mathfrak{M}'$, aberwegen $c \in \mathfrak{o}^\times$ ist $\pi^{t-u-1}\omega \notin \mathfrak{M}'$, also $f(\mathfrak{M}' \cap k[E]) = \pi^{t-u}\mathfrak{o}$.

Ist nun $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal mit $\mathfrak{f} \mid f(\mathfrak{o}[E])$, dann ist $\mathfrak{f} = \pi^v\mathfrak{o}$ mit $v \leq t - u$. Wir setzen $\mathfrak{M}^{\mathfrak{f}} := \begin{pmatrix} \mathfrak{o} & \pi^{-u-v}\mathfrak{o} \\ \pi^{u+v}\mathfrak{o} & \mathfrak{o} \end{pmatrix}$.

Wegen $u + v < t$ ist $B \in \mathfrak{M} \cap \mathfrak{M}' = \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \pi^t\mathfrak{o} & \mathfrak{o} \end{pmatrix} \subset \mathfrak{M}^{\mathfrak{f}}$.

$f(\mathfrak{M}^{\mathfrak{f}} \cap k[E]) = \mathfrak{f}$ berechnet man genauso wie oben $f(\mathfrak{M}' \cap k[E])$.

$N(\mathfrak{M}^{\mathfrak{f}}\mathfrak{M}^{\mathfrak{f}'}) = \mathfrak{f}^{-1}\mathfrak{f}' + \mathfrak{f}\mathfrak{f}'^{-1}$ läßt sich direkt nachrechnen (vgl. 10.12.ii).

(18.7) Lemma: Sei k ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und Primelement π. Sei $p \in \mathbb{N}$ Primzahl mit $\pi | p$ (in $\mathfrak{o}$). Dann gilt:
i) Wenn $p \equiv 1 \bmod 4$ oder $p = 2$, dann ist -1 Quadratrest mod π in $\mathfrak{o}$.
ii) Wenn p ungerade ist, gilt:
Falls -1 Quadratrest mod π in $\mathfrak{o}$ ist, ist -1 Quadratrest mod π^s in $\mathfrak{o}$ für alle $s \in \mathbb{N}$.
iii) Sei $n = p^r$ mit $r \in \mathbb{N}$, sei $n \neq 2$. Sei $\zeta_{2n} + \zeta_{2n}^{-1} \in k$.
Falls -1 Quadratrest mod π in $\mathfrak{o}$ ist, ist -1 Quadratrest mod $(\zeta_{2n} - \zeta_{2n}^{-1})^2$ in $\mathfrak{o}$.

Bew.: i) -1 ist Quadratrest mod p, also erst recht mod π.
ii) mit vollständiger Induktion.
Sei $s > 1$ und $-1 = x^2 + \pi^{s-1} y$ mit $x, y \in \mathfrak{o}$.
Offensichtlich ist notwendig $x \in \mathfrak{o}^\times$, also gilt:

$$-1 = (x + 1/2 \cdot x^{-1} \pi^{s-1} y)^2 - 1/4 \cdot x^{-2} \pi^{s+(s-2)} y^2$$
$$\equiv (x + 1/2 \cdot x^{-1} \pi^{s-1} y)^2 \bmod \pi^s$$

Hier ist $2 \in \mathfrak{o}^\times$, da $\pi \nmid 2$.
iii) Für ungerades p folgt die Beh. aus ii).
Sei $p = 2$. Wegen unserer Forderung $n \neq 2$ wird $r > 1$.
Die Beh. folgt wegen $(\zeta_{2n} - \zeta_{2n}^{-1})^2 \mid 2$ (siehe 13.6).

(18.8) Lemma: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$.
Sei $p \in \mathbb{N}$ Primzahl und $p \equiv 3 \bmod 4$. Sei $\mathfrak{P}$ ein Primideal von $\mathfrak{o}$ mit $\mathfrak{P} | p$.
-1 ist genau dann Quadratrest mod $\mathfrak{P}$ in $\mathfrak{o}$, wenn $t(\mathfrak{P})$ gerade ist.

Bew.: Sei $t := t(\mathfrak{P}) = [\mathfrak{o}/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}]$ gerade. Wegen $p \equiv 3 \bmod 4$ ist dies gleichbedeutend mit $p^t \equiv 1 \bmod 4$, d.h.

$$\#(\mathfrak{o}/\mathfrak{P})^\times = \#(\mathfrak{o}/\mathfrak{P}) - 1 = (\#(\mathbb{Z}/p\mathbb{Z}))^{[\mathfrak{o}/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}]} - 1 = p^t - 1 \equiv 0 \bmod 4.$$

$(\mathfrak{o}/\mathfrak{P})^\times$ ist als endliche multiplikative Gruppe eines Körpers zyklisch.
$\#(\mathfrak{o}/\mathfrak{P})^\times \equiv 0 \bmod 4$ ist also äquivalent dazu, daß $(\mathfrak{o}/\mathfrak{P})^\times$ ein Element der Ordnung 4 enthält, d.h. daß es $x \in \mathfrak{o}$ gibt mit $x^4 \equiv 1 \bmod \mathfrak{P}$ und $x^2 \not\equiv 1 \bmod \mathfrak{P}$, also $x^2 \equiv -1 \bmod \mathfrak{P}$.

(18.9) Satz: Voraussetzung (18.1)
i) Sei $\mathfrak{M}$ eine Q-Maximalordnung und $\mathfrak{f} \in F_{2n}^*(\mathfrak{M})$. Dann gilt:

a) $\mathfrak{f}^{2 D_K(K)} \mid (\zeta_{2n} - \zeta_{2n}^{-1})^2 \mathfrak{o}$

b) Falls $n = p^r$ mit einer Primzahl $p \equiv 3 \bmod 4$ und $r \in \mathbb{N}$, dann ist für alle Primteiler $\mathfrak{P}$ von $\mathfrak{f}$ der Trägheitsgrad $t(\mathfrak{P})$ gerade.

c) Falls $n = 2$, dann ist für alle Primteiler $\mathfrak{P}$ von $\mathfrak{f}$ der Trägheitsgrad $t(\mathfrak{P})$ oder der Verzweigungsgrad $v(\mathfrak{P})$ gerade.

} (18.10)

ii) Es gibt ein System $\{ \mathfrak{M}^{\mathfrak{f}} \mid \mathfrak{f}$ ist ganzes $\mathfrak{o}$-Ideal und erfüllt (18.10)$\}$ von Q-Maximalordnungen, so daß für alle ganzen $\mathfrak{o}$-Ideale $\mathfrak{f}, \mathfrak{f}'$, die der Bedingung (18.10) genügen, gilt: $\mathfrak{f} \in F_{2n}^{*}(\mathfrak{M}^{\mathfrak{f}})$ und $N(\mathfrak{M}^{\mathfrak{f}} \mathfrak{M}^{\mathfrak{f}'}) = \mathfrak{f}^{-1}\mathfrak{f}' + \mathfrak{f}\mathfrak{f}'^{-1}$, insbesondere also $N(\mathfrak{M}^{\mathfrak{f}} \mathfrak{M}^{\mathfrak{f}'}) \mathfrak{f}\mathfrak{f}'^{-1} \in I^{k(2)}$.

Bew.: i) Es ist $F_{2n}^{*}(\mathfrak{M}) \subset F_{2n}(\mathfrak{M})$. Mit (16.5.i) folgt a)
Sei $n = 2$. Wegen a) gilt: $\mathfrak{f} \mid 2\mathfrak{o}$. Wegen (16.5.i) dürfen die Primteiler $\mathfrak{p}$ von $\mathfrak{f}$ in Q nicht verzweigt sein Wegen (13.4.iii) ist dann $t(\mathfrak{p}) \cdot v(\mathfrak{p}) = [k_{\mathfrak{p}} : \mathbb{Q}_2]$ gerade.

Sei $n = p^r$ mit einer Primzahl $p \equiv 3 \bmod 4$ und $r \in \mathbb{N}$. Sei $\mathfrak{p}$ ein Primteiler von $\mathfrak{f}$. Wegen a) gilt $\mathfrak{p} \mid p$ (siehe 13.5).
Wegen (16.5.i) ist $\mathfrak{p}$ in Q nicht verzweigt.
Wegen Lemma (18.8) müssen wir zeigen, daß -1 Quadratrest mod $\mathfrak{p}$ in $\mathfrak{o}$ ist.
Dies ist äquivalent dazu, daß -1 Quadratrest mod $\mathfrak{p}_{\mathfrak{p}}$ in $\mathfrak{o}_{\mathfrak{p}}$ ist.
Seien $E, B \in \Gamma(\mathfrak{M})$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$, $BEB^{-1} = E^{-1}$ und $f(\mathfrak{M} \cap k[E]) = \mathfrak{f}$.
Nach Lemma (18.4) gibt es eine Q-Maximalordnung $\mathfrak{M}'$ mit $E, B \in \mathfrak{M}'$ und $f(\mathfrak{M}' \cap k[E]) = \mathfrak{o}$. Wegen $\mathfrak{p} \mid \mathfrak{f}$ ist dann $\mathfrak{M}_{\mathfrak{p}} \neq \mathfrak{M}'_{\mathfrak{p}}$.
Sei π ein Primelement von $\mathfrak{o}_{\mathfrak{p}}$. Wegen $\mathfrak{p} \nmid D_k(Q)$ ist $Q_{\mathfrak{p}} \cong_{k_{\mathfrak{p}}} M_2(k_{\mathfrak{p}})$.
Nach (11.1) gibt es Matrizeseinheiten $\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix} \in Q_{\mathfrak{p}}$
und $s \in \mathbb{N}_0$ mit $\mathfrak{M}_{\mathfrak{p}} = \begin{pmatrix}\mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}}\\ \mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}}\end{pmatrix}$ und $\mathfrak{M}'_{\mathfrak{p}} = \begin{pmatrix}\mathfrak{o}_{\mathfrak{p}} & \pi^{-s}\mathfrak{o}_{\mathfrak{p}}\\ \pi^{s}\mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}}\end{pmatrix}$.
Wegen $\mathfrak{M}_{\mathfrak{p}} \neq \mathfrak{M}'_{\mathfrak{p}}$ ist $s > 0$. Da $B \in \mathfrak{M} \cap \mathfrak{M}' \subset \mathfrak{M}_{\mathfrak{p}} \cap \mathfrak{M}'_{\mathfrak{p}} = \begin{pmatrix}\mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}}\\ \pi^{s}\mathfrak{o}_{\mathfrak{p}} & \mathfrak{o}_{\mathfrak{p}}\end{pmatrix}$,
gibt es $a,b,c,d \in \mathfrak{o}_{\mathfrak{p}}$ mit $B = \begin{pmatrix}a & b\\ \pi c & d\end{pmatrix}$. Wegen $S(B) = 0$ und $N(B) = 1$ ist $d = -a$ und $-a^2 - \pi bc = 1$, also -1 Quadrest mod $\pi\mathfrak{o}_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}$ in $\mathfrak{o}_{\mathfrak{p}}$.

ii) Es gibt (nach 13.3.i) $E, B \in \Gamma(Q)$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$ und $BEB^{-1} = E^{-1}$.
Nach Lemma (18.4) gibt es eine Q-Maximalordnung $\mathfrak{M}$ mit $E, B \in \Gamma(\mathfrak{M})$ und $f(\mathfrak{M} \cap k[E]) = \mathfrak{o}$.
Ist n durch zwei verschiedene Primzahlen teilbar, so ist $(\zeta_{2n} - \zeta_{2n}^{-1})^2 \in \mathfrak{o}^{\times}$ (siehe 13.7). Wegen Bedingung (18.10.a) ist nichts mehr zu zeigen.
Sei also $n = p^r$ mit einer Primzahl $p \in \mathbb{N}$ und $r \in \mathbb{N}$. Wegen (18.10.a) gilt $\mathfrak{f} \mid p$ für alle ganzen $\mathfrak{o}$-Ideale $\mathfrak{f}$, die (18.10) erfüllen.
Sei $\mathfrak{f}_0$ das kleinste gemeinsame Vielfache aller $\mathfrak{f}$, die (18.10) erfüllen.
Dann erfüllt auch $\mathfrak{f}_0$ Bedingung (18.10). Wir definieren nun das System der $\mathfrak{M}^{\mathfrak{f}}$ folgendermaßen:

Für alle endlichen Primstellen $\mathfrak{p}$ von k mit $\mathfrak{p} \nmid \mathfrak{f}_0$ sei $\mathfrak{M}_{\mathfrak{p}}^{\mathfrak{f}} := \mathfrak{M}_{\mathfrak{p}}$.
Falls $\mathfrak{p} \mid \mathfrak{f}_0$, ist $Q_{\mathfrak{p}} \tilde{=} M_2(k_{\mathfrak{p}})$, was man mit (13.4) leicht sieht.
Ist $p \equiv 3 \bmod 4$, folgt mit Lemma (18.8), daß -1 Quadratrest mod $\mathfrak{p}$ in $\mathfrak{o}$ ist.
Jetzt folgt leicht (für beliebiges p) mit Lemma (18.7.i) und (18.7.iii), daß für alle $n \neq 2$ die Zahl -1 Quadratrest mod $(\zeta_{2n} - \zeta_{2n}^{-1})^2$ in $\mathfrak{o}_{\mathfrak{p}}$ ist.
Für $k_{\mathfrak{p}}$ und $Q_{\mathfrak{p}}$ sind also die Voraussetzungen von Lemma (18.6) erfüllt und wir können definieren: $\mathfrak{M}_{\mathfrak{p}}^{\mathfrak{f}} := \mathfrak{M}^{\mathfrak{f}_{\mathfrak{p}}}$.
Die verlangten Eigenschaften des so definierten Systems folgen aus den Eigenschaften der Komponenten (siehe 18.6).

(18.11) Definition: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei K eine halbeinfache quadratische Erweiterung von k. Sei $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal. Sei $\mathfrak{O}^{\mathfrak{f}} = \mathfrak{O}^{\mathfrak{f}}(K)$ abgekürzt.
i) Ein $\mathfrak{O}^{\mathfrak{f}}$-Ideal $\mathfrak{a}$ heißt ambig, wenn $\mathfrak{a} = \mathfrak{a}^*$.
ii) Die Gruppe der ambigen $\mathfrak{O}^{\mathfrak{f}}$-Ideale bezeichnen wir mit $A^{\mathfrak{f}}$.
Ist k algebraischer Zahlkörper und $\mathfrak{p}$ eine endliche Primstelle von k, so sei $A_{\mathfrak{p}}^{\mathfrak{f}} := A^{\mathfrak{f}_{\mathfrak{p}}}$.
iii) Wir definieren einen Homomorphismus $(k \to \mathfrak{f}): I^k \to I^{\mathfrak{f}}$ durch $(k \to \mathfrak{f})(\mathfrak{a}) := \mathfrak{a}\mathfrak{O}^{\mathfrak{f}}$ für $\mathfrak{a} \in I^k$. Ist k algebraischer Zahlkörper und $\mathfrak{p}$ eine endliche Primstelle von k, so sei $(k \to \mathfrak{f})_{\mathfrak{p}} := (k_{\mathfrak{p}} \to \mathfrak{f}_{\mathfrak{p}})$.
iv) Wir definieren einen Homomorphismus $\Delta: K^\times \to K^\times$ durch $\Delta(a) = aa^{*-1}$ für $a \in K^\times$.

Man erinnere sich auch an die Definition von $n^{\mathfrak{f}}$ (siehe 7.12).
$n^{\mathfrak{f}}$ sei entsprechend auch für $\mathfrak{p}$-adische Zahlkörper definiert.

(18.12) Lemma: Gleiche Voraussetzung wie in (18.11). Dann gilt:
i) Sei k algebraischer Zahlkörper und sei $\mathfrak{a} \in I^{\mathfrak{f}}$.
Dann ist $\mathfrak{a} \in A^{\mathfrak{f}}$ genau dann, wenn $\mathfrak{a}_{\mathfrak{p}} \in A_{\mathfrak{p}}^{\mathfrak{f}}$ für alle endlichen Primstellen $\mathfrak{p}$ von k.
ii) $(k \to \mathfrak{f})(I^k) \subset A^{\mathfrak{f}}$ und $I^{k(2)} \subset N(A^{\mathfrak{f}})$
iii) $A^{\mathfrak{f}} \cap H^{\mathfrak{f}} = n^{\mathfrak{f}}(\Delta^{-1}(\mathfrak{O}^{\mathfrak{f}\times}))$ und $(n^{\mathfrak{f}})^{-1}(A^{\mathfrak{f}}) = (n^{\mathfrak{f}})^{-1}(A^{\mathfrak{f}} \cap H^{\mathfrak{f}}) = \Delta^{-1}(\mathfrak{O}^{\mathfrak{f}\times})$.

Bew.: i), ii) klar
iii) Da Bild $n^{\mathfrak{f}} = H^{\mathfrak{f}}$, folgt die erste Beh. aus der zweiten.
Sei $a \in (n^{\mathfrak{f}})^{-1}(A^{\mathfrak{f}})$, d.h. $(a\mathfrak{O}^{\mathfrak{f}})^* = a\mathfrak{O}^{\mathfrak{f}}$, d.h. $a^*\mathfrak{O}^{\mathfrak{f}} = a\mathfrak{O}^{\mathfrak{f}}$.
Dies ist äquivalent zu $aa^{*-1}\mathfrak{O}^{\mathfrak{f}} = \mathfrak{O}^{\mathfrak{f}}$, d.h. $aa^{*-1} = \Delta(a) \in \mathfrak{O}^{\mathfrak{f}\times}$.

(18.13) Lemma: Voraussetzung (18.1).
Seien $E, B \in \Gamma(Q)$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$ und $BEB^{-1} = E^{-1}$. Sei $\mathfrak{f}$ ein ganzes $\mathcal{O}$-Ideal, das der Bedingung (18.10) genügt. Sei $\mathcal{O}^{\mathfrak{f}} := \mathcal{O}^{\mathfrak{f}}(k[E])$ abgekürzt usw.
$\mathfrak{M}$ sei eine Q-Maximalordnung mit $B \in \mathfrak{M}$ und $\mathfrak{M} \cap k[E] = \mathcal{O}^{\mathfrak{f}}$.
i) Sei $\mathfrak{M}'$ eine Q-Maximalordnung mit $B \in \mathfrak{M}'$ und $\mathfrak{M}' \cap k[E] = \mathcal{O}^{\mathfrak{f}}$.
Dann gibt es $\mathfrak{a} \in A^{\mathfrak{f}}$ mit $\mathfrak{M}' = \mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1}$.
ii) Sei $\mathfrak{a} \in A^{\mathfrak{f}}$. Dann ist $B \in \mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1}$ und $\mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1} \cap k[E] = \mathcal{O}^{\mathfrak{f}}$.

Bew.: i) Nach (11.9.iii) gibt es $\mathfrak{a} \in I^{\mathfrak{f}}$ mit $\mathfrak{M}' = \mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1}$.
Die Rechtsordnung des Ideals $\mathfrak{M}'\mathfrak{a}$ ist $\mathfrak{M}$. Wegen $B \in \mathfrak{M}^{\times} \cap \mathfrak{M}'^{\times}$ ist $\mathfrak{M}'\mathfrak{a} = \mathfrak{M}'\mathfrak{a}B = \mathfrak{M}'B\mathfrak{a}^{*} = \mathfrak{M}'\mathfrak{a}^{*}$. Nach Lemma (17.10) also $\mathfrak{a} = \mathfrak{a}^{*}$.
ii) Nach (11.9.iv) ist $\mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1} \cap k[E] = \mathcal{O}^{\mathfrak{f}}$. Da $\mathfrak{a}\mathfrak{a}^{*-1} = \mathcal{O}^{\mathfrak{f}}$, gibt es $m \in \mathbb{N}$ und $a_1, \ldots, a_m \in \mathfrak{a}$ sowie $b_1, \ldots, b_m \in \mathfrak{a}^{-1}$ mit $\sum_{i=1}^{m} a_i b_i^{*} = 1$. Da $B \in \mathfrak{M}$, ist $B = 1 \cdot B = \sum_{i=1}^{m} a_i b_i^{*} B = \sum_{i=1}^{m} a_i B b_i \in \mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1}$.

(18.14) Definition: Gleiche Voraussetzung wie in (18.13).
Dann sei ${}^{\mathfrak{M}}A^{\mathfrak{f}}$ die Menge der Ideale $\mathfrak{M}\mathfrak{a}$ mit $\mathfrak{a} \in A^{\mathfrak{f}}$.

(18.15) Lemma: Gleiche Voraussetzung wie in (18.13).
Dann ist ${}^{\mathfrak{M}}I^{\mathfrak{M}} \subset {}^{\mathfrak{M}}A^{\mathfrak{f}}$, insbesondere also $RI^{k(2)} \subset N(A^{\mathfrak{f}})$.

Bew.: Nach (13.4.iv) sind alle Verzweigungsstellen von Q über k in K verzweigt (und nicht träge). Nach Lemma (17.8) ist also ${}^{\mathfrak{M}}I^{\mathfrak{M}} \subset {}^{\mathfrak{M}}I^{\mathfrak{f}}$ und nach (17.9) sogar ${}^{\mathfrak{M}}I^{\mathfrak{M}} \subset {}^{\mathfrak{M}}A^{\mathfrak{f}}$.

(18.16) Satz: Voraussetzung (18.1).
Sei $\mathfrak{f}$ ein ganzes $\mathcal{O}$-Ideal, das der Bedingung (18.10) genügt.
Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{f} \in F_{2n}^{*}(\mathfrak{M})$.
Sei $\mathfrak{M}'$ eine weitere Q-Maximalordnung.
Genau dann ist $\mathfrak{f} \in F_{2n}^{*}(\mathfrak{M}')$, wenn $N(\mathfrak{M}\mathfrak{M}') \in N(A^{\mathfrak{f}})S_{\mathcal{M}}$.

Bew.: Seien $E, B \in \Gamma(\mathfrak{M})$ mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$ und $BEB^{-1} = E^{-1}$ und sei $f(\mathfrak{M} \cap k[E]) = \mathfrak{f}$.
i) Sei $\mathfrak{f} \in F_{2n}^{*}(\mathfrak{M}')$. Seien $E', B' \in \Gamma(\mathfrak{M}')$ mit $S(E') = \zeta_{2n} + \zeta_{2n}^{-1}$ und $B'E'B'^{-1} = E'^{-1}$ und sei $f(\mathfrak{M}' \cap k[E']) = \mathfrak{f}$.
Durch die Vorschriften $E' \mapsto E$, $B' \mapsto B$ wird ein k-Algebrenautomorphismus $\sigma: Q \to Q$ definiert. Es gibt $M \in Q^{\times}$ mit $x = MxM^{-1}$ für alle $x \in Q$.
Wegen $f(\mathfrak{M} \cap k[E]) = f(\mathfrak{M}' \cap k[E'])$ ist $\sigma(\mathfrak{M}' \cap k[E']) = \mathfrak{M} \cap k[E]$ (siehe 6.11). Also gilt $M\mathfrak{M}'M^{-1} \cap k[E] = \mathfrak{M} \cap k[E]$.

Wegen $\sigma B' = B$ ist $B \in M\mathfrak{M}'M^{-1}$.
Nach (18.13.i) gibt es ein ambiges $(\mathfrak{M} \cap k[E])$-Ideal $\mathfrak{a}$ mit $\mathfrak{M} = \mathfrak{a}M\mathfrak{M}'M^{-1}\mathfrak{a}^{-1}$. Dann ist $\mathfrak{M}\mathfrak{a}M = \mathfrak{a}M\mathfrak{M}'$ ein Ideal mit Linksordnung $\mathfrak{M}$ und Rechtsordnung $\mathfrak{M}'$. Es gibt also ein $\mathfrak{A} \in \mathfrak{m}_I\mathfrak{M}$ mit $\mathfrak{A}\mathfrak{M}\mathfrak{M}' = \mathfrak{M}\mathfrak{a}M$. Daher ist $N(\mathfrak{M}\mathfrak{M}') = N(\mathfrak{A})^{-1}N(\mathfrak{a})N(M) \in N(A^{\mathfrak{f}})S_u$

ii) Sei $N(\mathfrak{M}\mathfrak{M}') \in N(A^{\mathfrak{f}})S_u$.
Dann gibt es ein ambiges $(\mathfrak{M} \cap k[E])$-Ideal $\mathfrak{a}$ und $M \in Q^\times$ mit $\mathfrak{a}\mathfrak{M}\mathfrak{M}' = M\mathfrak{M}'$ (siehe 10.4). Die Linksordnung dieses Ideals ist $\mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1} = M\mathfrak{M}'M^{-1}$. Nach (18.13.ii) ist $B \in M\mathfrak{M}'M^{-1}$ und $M\mathfrak{M}'M^{-1} \cap k[E] = \mathfrak{M} \cap k[E]$. Also ist $\mathfrak{f} \in F^*_{2n}(M\mathfrak{M}'M^{-1}) = F^*_{2n}(\mathfrak{M}')$.

Bemerkung: Die Sätze (18.9) und (18.16) gestatten es, eine Übersicht über $F^*_{2n}(\mathfrak{M})$ für alle Maximalordnungstypen $\tilde{\mathfrak{M}}$ zu bekommen.
Wir wollen noch Satz (18.18) beweisen, der eine etwas einfachere Übersicht ermöglicht. Wir brauchen folgendes (leichte) Lemma.

(18.17) Lemma: Sei k algebraischer oder $\mathfrak{p}$-adischer Zahlkörper. Sei K halbeinfache quadratische Erweiterung von k. Seien $\mathfrak{f}, \mathfrak{f}'$ ganze Ideale aus k. Wenn $\mathfrak{f} \mid \mathfrak{f}'$, dann ist $N(A^{\mathfrak{f}'}) \subset N(A^{\mathfrak{f}})$.

Bew.: Sei $\mathfrak{a} \in A^{\mathfrak{f}'}$. Wegen $\mathcal{O}^{\mathfrak{f}'} \subset \mathcal{O}^{\mathfrak{f}}$ ist $\mathfrak{a}\mathcal{O}^{\mathfrak{f}} \in I^{\mathfrak{f}}$. Offensichtlich gilt sogar $\mathfrak{a}\mathcal{O}^{\mathfrak{f}} \in A^{\mathfrak{f}}$. Es ist $N(\mathfrak{a}) = N(\mathfrak{a}\mathcal{O}^{\mathfrak{f}}) \in N(A^{\mathfrak{f}})$.

(18.18) Satz: Voraussetzung (18.1).
Sei $\mathfrak{f}_0$ das kleinste gemeinsame Vielfache aller ganzen $\mathcal{O}$-Ideale, die Bedingung (18.10) erfüllen und sei $\mathfrak{M}_0$ eine Q-Maximalordnung mit $\mathfrak{f}_0 \in F^*_{2n}(\mathfrak{M}_0)$. ($\mathfrak{M}_0$ existiert nach 18.9.ii)
Sei $\mathfrak{M}$ eine Q-Maximalordnung und $\mathfrak{f}$ ein ganzes $\mathcal{O}$-Ideal.
Genau dann ist $\mathfrak{f} \in F^*_{2n}(\mathfrak{M})$, wenn $\mathfrak{f}$ die Bedingung (18.10) erfüllt und $N(\mathfrak{M}_0\mathfrak{M})\mathfrak{f}_0\mathfrak{f}^{-1} \in N(A^{\mathfrak{f}})S_u$.

Bew.: Wir setzen voraus, daß $\mathfrak{f}$ die Bedingung (18.10) erfüllt (siehe 18.9.i). Nach (18.9.ii) gibt es Q-Maximalordnungen $\mathfrak{M}^{\mathfrak{f}_0}$ und $\mathfrak{M}^{\mathfrak{f}}$ mit $\mathfrak{f}_0 \in F^*_{2n}(\mathfrak{M}^{\mathfrak{f}_0})$, $\mathfrak{f} \in F^*_{2n}(\mathfrak{M}^{\mathfrak{f}})$ und $N(\mathfrak{M}^{\mathfrak{f}_0}\mathfrak{M}^{\mathfrak{f}})\mathfrak{f}_0\mathfrak{f}^{-1} \in I^{k(2)} \subset N(A^{\mathfrak{f}})S_u$.
Aus (10,9.ii) folgt leicht (durch Induktion), daß
$N(\mathfrak{M}_0\mathfrak{M})N(\mathfrak{M}\mathfrak{M}^{\mathfrak{f}})N(\mathfrak{M}^{\mathfrak{f}}\mathfrak{M}^{\mathfrak{f}_0})N(\mathfrak{M}^{\mathfrak{f}_0}\mathfrak{M}_0) \in RI^{k(2)}S_u \subset N(A^{\mathfrak{f}})S_u$.
Nach Satz (18.16) ist $N(\mathfrak{M}^{\mathfrak{f}_0}\mathfrak{M}_0) \in N(A^{\mathfrak{f}_0})S_u \subset N(A^{\mathfrak{f}})S_u$. Also ist $N(\mathfrak{M}_0\mathfrak{M})N(\mathfrak{M}\mathfrak{M}^{\mathfrak{f}})\mathfrak{f}_0\mathfrak{f}^{-1} \in N(A^{\mathfrak{f}})S_u$. Nach Satz (18.16) ist $\mathfrak{f} \in F^*_{2n}(\mathfrak{M})$ genau dann, wenn $N(\mathfrak{M}\mathfrak{M}^{\mathfrak{f}}) \in N(A^{\mathfrak{f}})S_u$, d.h. wenn $N(\mathfrak{M}_0\mathfrak{M})\mathfrak{f}_0\mathfrak{f}^{-1} \in N(A^{\mathfrak{f}})S_u$.

(18.19) Bemerkung:

i) Das in (16.13.i) genannte Problem stellt sich hier noch schärfer: Wie findet man aus einem Repräsentantensystem von $\tilde{Q}$ eine Q-Maximalordnung $\mathfrak{M}_0$ mit $\mathfrak{f}_0 \in F_{2n}^*(\mathfrak{M}_0)$?

ii) Falls alle Primteiler von $\mathfrak{f}_0$ in K unverzweigt sind oder n keine Potenz von 2 ist (also $\mathfrak{f}_0 + 2\mathfrak{o} = \mathfrak{o}$), dann sind alle Primteiler von $\mathfrak{f}_0$ in K unverzweigt oder zahm verzweigt. In diesem Fall ist $N(A^{\mathfrak{f}_0}) = N(A^{\mathfrak{o}})$. In Satz (18.18) können wir dann $\mathfrak{f}_0$ durch irgendein ganzes $\mathfrak{o}$-Ideal ersetzen, das Bedingung (18.10) erfüllt.
Für je zwei Q-Maximalordnungen $\mathfrak{M}$ und $\mathfrak{M}'$ gilt dann:
$F_{2n}^*(\mathfrak{M}) \cap F_{2n}^*(\mathfrak{M}') \neq \emptyset \Longrightarrow F_{2n}^*(\mathfrak{M}) = F_{2n}^*(\mathfrak{M}')$.

iii) Wegen der Kompliziertheit der Bedingung $N(\mathfrak{M}_0\mathfrak{M})\,\mathfrak{f}_0\mathfrak{f}^{-1} \in N(A^{\mathfrak{f}})S_m$ läßt sich (meines Wissens) i.a. kein einfacher Ausdruck für die Anzahl der verschiedenen Maximalordnungstypen $\tilde{\mathfrak{M}}$ mit $l_{2n}^*(\mathfrak{M}) \neq 0$ angeben. Sind die Bedingungen aus ii) erfüllt und ist R' die Untergruppe von I^k, die von den Primteilern von $\mathfrak{f}_0$ erzeugt wird, dann gibt es offenbar $[R'N(A^{\mathfrak{o}})S_m : N(A^{\mathfrak{o}})S_m]$ Teilmengen mit jeweils $[N(A^{\mathfrak{o}})S_m : RI^{k(2)}S_m]$ Elementen, so daß gilt: Für alle $\tilde{\mathfrak{M}}$ aus einer solchen Teilmenge hat $F_{2n}^*(\mathfrak{M})$ den gleichen Wert $\neq 0$.
Im Sinne von (10.11) sind die genannten Mengen affine Unterräume von $\tilde{Q}$.

Für den Rest dieses Paragrafen sei $\mathfrak{f}$ ein (festes) ganzes $\mathfrak{o}$-Ideal, das Bedingung (18.10) erfüllt und $\mathfrak{M}$ eine (feste) Q-Maximalordnung mit $\mathfrak{f} \in F_{2n}^*(\mathfrak{M})$. Wir wollen $l_{2n}^*(\mathfrak{M}, \mathfrak{f})$ berechnen.
Seien dazu E, $B \in \Gamma(\mathfrak{M})$ fest gewählt mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$, $BEB^{-1} = E^{-1}$ und $f(\mathfrak{M} \cap k[E]) = \mathfrak{f}$.
Wir kürzen $\Gamma := \Gamma(\mathfrak{M})$ und $\mathfrak{o}^{\mathfrak{f}} := \mathfrak{o}^{\mathfrak{f}}(k[E]) = \mathfrak{M} \cap k[E]$ ab.

(18.20) Lemma: i) Zu jedem $E' \in L_{2n}^*(\mathfrak{M}, \mathfrak{f})$ gibt es $M \in Q^\times$, so daß

$$MEM^{-1} = E' \text{ und } MBM^{-1} \in \mathfrak{M}.$$

ii) Sei $M \in Q^\times$. Genau dann ist $MEM^{-1} \in L_{2n}^*(\mathfrak{M}, \mathfrak{f})$ und $MBM^{-1} \in \mathfrak{M}$, wenn es $\mathfrak{a} \in A^{\mathfrak{f}}$ gibt mit $\mathfrak{M}M = \mathfrak{M}\mathfrak{a}$.

Bew.: i) Da $E' \in L_{2n}^*(\mathfrak{M}, \mathfrak{f})$, ist $E' \in \Gamma(\mathfrak{M})$, $S(E') = \zeta_{2n} + \zeta_{2n}^{-1}$ und es gibt $B' \in \Gamma(\mathfrak{M})$ mit $B'E'B'^{-1} = E'^{-1}$. Mit Satz (3.3) folgt, daß es $M \in Q^\times$ gibt mit $MEM^{-1} = E'$ und $MBM^{-1} = B' \in \mathfrak{M}$.

ii) Sei $MEM^{-1} \in L_{2n}^{*}(\mathfrak{M}, \mathfrak{f})$ und $MBM^{-1} \in \mathfrak{M}$, d.h. $B \in M^{-1}\mathfrak{M}M$.
Dann ist $f(M^{-1}\mathfrak{M}M \cap k[E]) = f(\mathfrak{M} \cap k[MEM^{-1}]) = \mathfrak{f}$.
Nach Lemma (18.13.i) gibt es $\alpha \in A^{\mathfrak{f}}$ mit $\mathfrak{M} = \alpha M^{-1}\mathfrak{M}M\alpha^{-1}$.
Das Ideal $\mathfrak{A} := M\alpha^{-1}\mathfrak{M} = \mathfrak{M}M\alpha^{-1}$ ist dann ein zweiseitiges $\mathfrak{M}$-Ideal.
Nach Lemma (18.15) gibt es $\alpha' \in A^{\mathfrak{f}}$ mit $\mathfrak{A} = \mathfrak{M}\alpha'$;
also $\mathfrak{M}M = \mathfrak{M}\alpha'\alpha$ und $\alpha'\alpha \in A^{\mathfrak{f}}$.
Sei umgekehrt $\alpha \in A^{\mathfrak{f}}$ mit $\mathfrak{M}M = \mathfrak{M}\alpha$. Die Rechtsordnung dieses Ideals ist $M^{-1}\mathfrak{M}M = \alpha^{-1}\mathfrak{M}\alpha$. Nach Lemma (18.13.ii) ist $f(\mathfrak{M} \cap k[MEM^{-1}]) = f(M^{-1}\mathfrak{M}M \cap k[E]) = \mathfrak{f}$ und $B \in M^{-1}\mathfrak{M}M$, also $MBM^{-1} \in \mathfrak{M}$. Wegen $(MEM^{-1})(MEM^{-1})(MBM^{-1})^{-1} = (MEM^{-1})^{-1}$ folgt: $MEM^{-1} \in L_{2n}^{*}(\mathfrak{M}, \mathfrak{f})$.

Seien η und e wie in (17.3) definiert. Lemma (18.20) besagt dann:
e induziert eine surjektive Abb. $e: \eta^{-1}(\mathfrak{M}A^{\mathfrak{f}}) \to L_{2n}^{*}(\mathfrak{M}, \mathfrak{f})$.
Sei $\eta^{\mathfrak{f}}$ die in (7.12) definierte natürliche Abbildung: $\eta^{\mathfrak{f}}: k[E]^{\times} \to H^{\mathfrak{f}}$.

(18.21) Lemma: Sei $M \in \eta^{-1}(\mathfrak{M}A^{\mathfrak{f}})$.
i) Sei $\gamma \in \Gamma$ und $a \in (\eta^{\mathfrak{f}})^{-1}(A^{\mathfrak{f}})$. Dann ist $\gamma Ma \in \eta^{-1}(\mathfrak{M}A^{\mathfrak{f}})$.
ii) Sei $M' \in \eta^{-1}(\mathfrak{M}A^{\mathfrak{f}})$. Genau dann ist $M'EM'^{-1} \sim MEM^{-1}$, wenn es $\gamma \in \Gamma$ und $a \in (\eta^{\mathfrak{f}})^{-1}(A^{\mathfrak{f}})$ gibt mit $M' = \gamma Ma$.

Bew.: Sei $\mathfrak{M}M = \mathfrak{M}\alpha$ mit $\alpha \in A^{\mathfrak{f}}$.
i) $\mathfrak{M}\gamma Ma = \mathfrak{M}Ma = \mathfrak{M}\alpha a$ und $\alpha a \in A^{\mathfrak{f}}$.
ii) Sei $M'EM'^{-1} \sim MEM^{-1}$. Dann gibt es $\gamma \in \Gamma$ mit $M'EM'^{-1} = \gamma MEM^{-1}\gamma^{-1}$, d.h. $M^{-1}\gamma^{-1}M'E = EM^{-1}\gamma^{-1}M'$. Nach (3.2) ist $a := M^{-1}\gamma^{-1}M' \in k[E]^{\times}$.
Sei $\mathfrak{M}M' = \mathfrak{M}\alpha'$ mit $\alpha' \in A^{\mathfrak{f}}$. Dann ist $\mathfrak{M}\alpha a = \mathfrak{M}Ma = \mathfrak{M}\gamma^{-1}M' = \mathfrak{M}M' = \mathfrak{M}\alpha'$, nach (17.10) also $\alpha a = \alpha'$, d.h. $a\mathcal{O}^{\mathfrak{f}} = \alpha'\alpha^{-1} \in A^{\mathfrak{f}}$.
Sei umgekehrt $M' = \gamma Ma$ mit $\gamma \in \Gamma$ und $a \in (\eta^{\mathfrak{f}})^{-1}(A^{\mathfrak{f}})$. Dann ist $M'EM'^{-1} = \gamma MaEa^{-1}M^{-1}\gamma^{-1} = \gamma MEM^{-1}\gamma^{-1}$, also $M'EM'^{-1} \sim MEM^{-1}$.

Sei $p: \eta^{-1}(\mathfrak{M}A^{\mathfrak{f}}) \to \Gamma\backslash\eta^{-1}(\mathfrak{M}A^{\mathfrak{f}})/(\eta^{\mathfrak{f}})^{-1}(A^{\mathfrak{f}})$ die natürliche Projektion.
Nach Lemma (18.21) induziert e eine Abb. $\overline{e}$
$\overline{e}: \Gamma\backslash\eta^{-1}(\mathfrak{M}A^{\mathfrak{f}})/(\eta^{\mathfrak{f}})^{-1}(A^{\mathfrak{f}}) \to L_{2n}^{*}(\mathfrak{M}, \mathfrak{f})/\sim$
$p(M) \mapsto \overline{MEM^{-1}}$
Da e surjektiv ist, ist auch $\overline{e}$ surjektiv. Nach (18.21.ii) ist $\overline{e}$ injektiv.

(18.22) Korollar: $1_{2n}^{*}(\mathfrak{M}, \mathfrak{f}) = \#\left(\Gamma\backslash\eta^{-1}(\mathfrak{M}A^{\mathfrak{f}})/(\eta^{\mathfrak{f}})^{-1}(A^{\mathfrak{f}})\right)$

Für $\alpha \in A^\flat$ bezeichnen wir die Restklasse in $A^\flat/A^\flat \cap H^\flat$ mit $\overline{\alpha}$.

(18.23) Lemma: Wir können eine Abbildung
$\psi\colon \Gamma\backslash n^{-1}(\mathfrak{M}A^\flat)/(n^\flat)^{-1}(A^\flat) \to A^\flat/A^\flat \cap H^\flat$ folgendermaßen definieren:
Ist $M \in n^{-1}(\mathfrak{M}A^\flat)$, also $\mathfrak{M}M = \mathfrak{M}\alpha$ mit $\alpha \in A^\flat$, so setzen wir $\psi(p(M)) := \overline{\alpha}$.
ψ hat folgende Eigenschaften:
i) $l^*_{2n}(\mathfrak{M},\mathfrak{f}) = \sum_{\overline{\alpha} \in \mathrm{Bild}\,\psi} \# \psi^{-1}(\overline{\alpha})$
ii) $\# \mathrm{Bild}\,\psi = [A^\flat : A^\flat \cap H^\flat]/[N(A^\flat) : N(A^\flat) \cap S_u]$

Bew.: Wohldefiniertheit: Seien $M,M' \in n^{-1}(\mathfrak{M}A^\flat)$, sei $\mathfrak{M}M = \mathfrak{M}\alpha$ und $\mathfrak{M}M' = \mathfrak{M}\alpha'$ mit $\alpha, \alpha' \in A^\flat$ und sei $M' = \gamma M a$ mit $\gamma \in \Gamma$ und $a \in (n^\flat)^{-1}(A^\flat)$. Dann ist $\mathfrak{M}\alpha' = \mathfrak{M}M' = \mathfrak{M}\gamma M a = \mathfrak{M}Ma = \mathfrak{M}\alpha a$. Nach (17.10) ist $\alpha' = \alpha a$.
i) folgt sofort mit (18.22)
ii) Sei $\alpha \in A^\flat$. Man sieht leicht ein, daß $\overline{\alpha} \in \mathrm{Bild}\,\psi$ genau dann, wenn es $M \in Q^\times$ gibt mit $\mathfrak{M}M = \mathfrak{M}\alpha$. Dies ist genau dann der Fall, wenn $N(\alpha) \in S_u$. Falls $\alpha \in H^\flat \cap A^\flat$, ist selbstverständlich $N(\alpha) \in S_u$.
Bild ψ ist also Untergruppe von $A^\flat/A^\flat \cap H^\flat$ und zwar ist es genau der Kern der durch Normbildung induzierten Abbildung $\overline{N}$:
$\overline{N}\colon A^\flat/A^\flat \cap H^\flat \to N(A^\flat)/N(A^\flat) \cap S_u$, also folgt die Beh.

Wir wählen jetzt ein festes $\alpha \in A^\flat$ mit $\overline{\alpha} \in \mathrm{Bild}\,\psi$ und ein festes $M \in p^{-1}(\psi^{-1}(\overline{\alpha}))$. Es gibt dann zu jedem $M' \in p^{-1}(\psi^{-1}(\overline{\alpha}))$ ein $a \in (n^\flat)^{-1}(A^\flat)$ mit $\mathfrak{M}M' = \mathfrak{M}Ma$.
Die Restklasse von $\varepsilon \in \mathfrak{M}^\times$ in $\mathfrak{M}^\times/\Gamma(M\mathfrak{O}^\flat M^{-1})^\times$ bezeichnen wir mit $\overline{\varepsilon}$.

(18.24) Lemma: Wir können eine Abb. $\chi\colon \psi^{-1}(\overline{\alpha}) \to \mathfrak{M}^\times/\Gamma(M\mathfrak{O}^\flat M^{-1})^\times$ folgendermaßen definieren. Ist $M' \in p^{-1}(\psi^{-1}(\overline{\alpha}))$, also $\mathfrak{M}M' = \mathfrak{M}Ma$ mit $a \in (n^\flat)^{-1}(A^\flat)$, dann setzen wir $\chi(p(M')) = \overline{M'a^{-1}M^{-1}}$.
χ ist bijektiv. Insbesondere gilt: $\# \psi^{-1}(\overline{\alpha}) = [u^\times : N(\mathfrak{O}^{\flat\times})]$.

Bew.: wie Bew. von (17.13). (Man ersetze dort $k[E]^\times$ durch $(n^\flat)^{-1}(A^\flat)$ und beachte, daß $\mathfrak{O}^{\flat\times} \subset (n^\flat)^{-1}(A^\flat)$.)

Aus den Lemmata (18.23) und (18.24) folgt jetzt:

(18.25) Satz: Voraussetzung (18.1).
Sei $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal, das Bedingung (18.10) erfüllt und sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{f} \in F^*_{2n}(\mathfrak{M})$. Dann ist
$l^*_{2n}(\mathfrak{M},\mathfrak{f}) = [u^\times : N(\mathfrak{O}^{\flat\times})] \cdot [A^\flat : A^\flat \cap H^\flat]/[N(A^\flat) : N(A^\flat) \cap S_u]$.

(18.26) Bemerkung: Für $Q = ((\zeta_{2n}-\zeta_{2n}^{-1})^2, -1)_k$ gibt es keinen so einfachen Satz, wie es (17.15) ist. Um $\lambda^*_{2n}(\mathfrak{M})$ und $\lambda'_{2n}(\mathfrak{M})$ für alle Q-Maximalordnungen $\mathfrak{M}$ zu berechnen, muß man (wie schon bewiesen) so vorgehen:

i) Man bestimmt mit den Sätzen (16.10) und (18.18) die Mengen $F_{2n}(\mathfrak{M})$ und $F^*_{2n}(\mathfrak{M})$.

ii) Man bestimmt mit den Sätzen (17.14) und (18.25) für alle $\mathfrak{f} \in F_{2n}(\mathfrak{M})$ bzw. $\mathfrak{f} \in F^*_{2n}(\mathfrak{M})$ die Größen $l_{2n}(\mathfrak{M},\mathfrak{f})$ und $l^*_{2n}(\mathfrak{M},\mathfrak{f})$.

iii) Man berechnet $l_{2n}(\mathfrak{M}) = \overline{\prod_{\mathfrak{f} \in F_{2n}(\mathfrak{M})}} l_{2n}(\mathfrak{M},\mathfrak{f})$ und

$l^*_{2n}(\mathfrak{M}) = \overline{\prod_{\mathfrak{f} \in F^*_{2n}(\mathfrak{M})}} l^*_{2n}(\mathfrak{M},\mathfrak{f})$; und schließlich

$\lambda^*_{2n}(\mathfrak{M})$ und $\lambda'_{2n}(\mathfrak{M})$ mit (15.10.iii).

§ 19 . Umrechnung der Ergebnisse aus § 18 (Vorbereitung für Beispiele).

In § 7 haben wir $[I^{\mathfrak{f}} : H^{\mathfrak{f}}]$ auf andere Größen zurückgeführt. Ähnlich wollen wir in diesem Paragrafen das Ergebnis für $l^*_{2n}(\mathfrak{M},\mathfrak{f})$ umrechnen. Diese Umrechnung und die vorbereitenden Lemmata brauchen wir, um unsere Ergebnisse aus den Paragrafen 17 und 18 für imaginärquadratische Zahlkörper realisieren zu können.

Wir machen folgende Generalvoraussetzung:

(19.1) Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$.
Sei K halbeinfache quadratische Erweiterung von k. Sei $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal. Wir kürzen $\mathcal{O}^{\mathfrak{f}} := \mathcal{O}^{\mathfrak{f}}(K)$ ab usw.

(19.2) Definition:

Sei $\kappa := \begin{cases} 2, & K \text{ ist Körper} \\ 1, & K = ke_1 \oplus ke_2 \text{ mit K-Idempotenten } e_1, e_2. \end{cases}$

(19.3) Lemma: Sei r die Zahl der unendlichen Verzweigungsstellen von K über k. Dann ist $[\mathcal{O}^{\mathfrak{o}\times} \cap N^{-1}(1) : \Delta(\mathcal{O}^{\mathfrak{o}\times})] = 2^{-r}\kappa[\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{o}\times})]$.

Bew.: Falls K Körper ist, siehe /8/ S. 268 Satz 12 (1),(2),(3).
Sei $K = ke_1 \oplus ke_2$ mit K-Idempotenten e_1, e_2. Dann ist $r = 0$, $\kappa = 1$ und $[\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{o}\times})] = 1$. Denn für $\varepsilon \in \mathfrak{o}^\times$ ist $\varepsilon e_1 + e_2 \in \mathcal{O}^{\mathfrak{o}\times}$ und $\varepsilon = N(\varepsilon e_1 + e_2)$.
Also ist zu zeigen: $\mathcal{O}^{\mathfrak{o}\times} \cap N^{-1}(1) = \Delta(\mathcal{O}^{\mathfrak{o}\times})$. Sei $E = ae_1 + be_2 \in \mathcal{O}^{\mathfrak{o}\times} \cap N^{-1}(1)$.
Dann ist $ab = N(E) = 1$, d.h. $b = a^{-1}$ und $E = \Delta(ae_1 + e_2)$.

(19.4) Lemma: $\dfrac{[\mathfrak{o}^{\mathfrak{p}\times} \cap N^{-1}(1) : \Delta(\mathfrak{o}^{\mathfrak{p}\times})]}{[\mathfrak{o}^{\sigma\times} \cap N^{-1}(1) : \Delta(\mathfrak{o}^{\sigma\times})]} = [N(\mathfrak{o}^{\sigma\times}) : N(\mathfrak{o}^{\mathfrak{p}\times})]$

Bew.: es ist
$$\frac{[\mathfrak{o}^{\mathfrak{p}\times} \cap N^{-1}(1) : \Delta(\mathfrak{o}^{\mathfrak{p}\times})]}{[\mathfrak{o}^{\sigma\times} \cap N^{-1}(1) : \Delta(\mathfrak{o}^{\sigma\times})]} = \frac{[\Delta(\mathfrak{o}^{\sigma\times}) : \Delta(\mathfrak{o}^{\mathfrak{p}\times})]}{[\mathfrak{o}^{\sigma\times} \cap N^{-1}(1) : \mathfrak{o}^{\mathfrak{p}\times} \cap N^{-1}(1)]}$$
Anwendung des Homomorphiesatzes (7.6) auf Δ ergibt:
$$[\mathfrak{o}^{\sigma\times} : \mathfrak{o}^{\mathfrak{p}\times}] = [\Delta(\mathfrak{o}^{\sigma\times}) : \Delta(\mathfrak{o}^{\mathfrak{p}\times})] \cdot [\mathfrak{o}^{\sigma\times} \cap \Delta^{-1}(1) : \mathfrak{o}^{\mathfrak{p}\times} \cap \Delta^{-1}(1)]$$
Wegen (2.11.ii) ist $\Delta^{-1}(1) = k^{\times}$. Also ist
$\mathfrak{o}^{\sigma\times} \cap \Delta^{-1}(1) = \mathfrak{o}^{\mathfrak{p}\times} \cap \Delta^{-1}(1) = \mathfrak{o}^{\times}$ und $[\mathfrak{o}^{\sigma\times} : \mathfrak{o}^{\mathfrak{p}\times}] = [\Delta(\mathfrak{o}^{\sigma\times}) : \Delta(\mathfrak{o}^{\mathfrak{p}\times})]$.
Anwendung des Homomorphiesatzes (7.6) auf N ergibt:
$$[\mathfrak{o}^{\sigma\times} : \mathfrak{o}^{\mathfrak{p}\times}] = [N(\mathfrak{o}^{\sigma\times}) : N(\mathfrak{o}^{\mathfrak{p}\times})][\mathfrak{o}^{\sigma\times} \cap N^{-1}(1) : \mathfrak{o}^{\mathfrak{p}\times} \cap N^{-1}(1)]$$
Damit folgt die Beh.

Aus (19.3) und (19.4) folgt sofort (als Verallgemeinerung von 19.3):

(19.5) Satz: Sei r die Zahl der unendlichen Verzweigungsstellen von K über k. Dann ist $[\mathfrak{o}^{\mathfrak{p}\times} \cap N^{-1}(1) : \Delta(\mathfrak{o}^{\mathfrak{p}\times})] = 2^{-r} \cdot \kappa \cdot [\mathfrak{o}^{\times} : N(\mathfrak{o}^{\mathfrak{p}\times})]$.

(19.6) Lemma: $\Delta(K^{\times}) = N^{-1}(1)$

Bew.: Falls K Körper ist, ist das /12/ S. 149 Satz 90.
Falls $K = ke_1 \oplus ke_2$ mit K-Idempotenten e_1, e_2, läßt sich die Beh. leicht direkt nachrechnen (siehe Bew. 19.3).

(19.7) Lemma: Sei r die Zahl der unendlichen Verzweigungsstellen von K über k. Dann ist $[A^{\mathfrak{p}} : A^{\mathfrak{p}} \cap H^{\mathfrak{P}}] = 2^{r} \dfrac{[A^{\mathfrak{p}} : (k\to\mathfrak{p})(I^k)][I^k : H^k]}{\kappa\,[\mathfrak{o}^{\times} : N(\mathfrak{o}^{\mathfrak{p}\times})]}$

Bew.: Es ist $[A^{\mathfrak{P}} : A^{\mathfrak{p}} \cap H^{\mathfrak{P}}] = \dfrac{[A^{\mathfrak{p}} : (k\to\mathfrak{p})(H^k)]}{[A^{\mathfrak{p}} \cap H^{\mathfrak{P}} : (k\to\mathfrak{p})(H^k)]}$
$$= \frac{[A^{\mathfrak{p}} : (k\to\mathfrak{p})(I^k)] \cdot [(k\to\mathfrak{p})(I^k) : (k\to\mathfrak{p})(H^k)]}{[A^{\mathfrak{p}} \cap H^{\mathfrak{P}} : (k\to\mathfrak{p})(H^k)]}$$
$(k\to\mathfrak{p})$ ist injektiv. Denn sei $\alpha \in I^k$ mit $\alpha\,\mathfrak{o}^{\mathfrak{p}} = \mathfrak{o}^{\mathfrak{p}}$. Dann ist auch $\alpha^{-1}\mathfrak{o}^{\mathfrak{p}} = \mathfrak{o}^{\mathfrak{p}}$ und wir erhalten $\alpha \in \mathfrak{o}^{\mathfrak{p}} \cap k = \mathfrak{o}$ und $\alpha^{-1} \in \mathfrak{o}^{\mathfrak{p}} \cap k = \mathfrak{o}$, also $\alpha = \mathfrak{o}$. Daher ist $[(k\to\mathfrak{p})(I^k) : (k\to\mathfrak{p})(H^k)] = [I^k : H^k]$.
Wir müssen noch den Nenner des Bruches umformen. Da $\eta^{\mathfrak{p}}: K^{\times} \to H^{\mathfrak{p}}$ surjektiv ist, ist $[A^{\mathfrak{p}} \cap H^{\mathfrak{p}} : (k\to\mathfrak{p})(H^k)] = [(\eta^{\mathfrak{p}})^{-1}(A^{\mathfrak{p}} \cap H^{\mathfrak{P}}) : (\eta^{\mathfrak{p}})^{-1}((k\to\mathfrak{p})(H^k))]$.
Man rechnet leicht nach, daß $(\eta^{\mathfrak{p}})^{-1}((k\to\mathfrak{p})(H^k)) = k^{\times}\mathfrak{o}^{\mathfrak{p}\times}$. Mit (18.12.iii) folgt: $[A^{\mathfrak{p}} \cap H^{\mathfrak{p}} : (k\to\mathfrak{p})(H^k)] = [\Delta^{-1}(\mathfrak{o}^{\mathfrak{p}\times}) : k^{\times}\mathfrak{o}^{\mathfrak{p}\times}]$.
Anwendung des Homomorphiesatzes (7.6) auf Δ und Lemma (19.6) ergeben:
$$[A^{\mathfrak{p}} \cap H^{\mathfrak{p}} : (k\to\mathfrak{p})(H^k)] = [\Delta(\Delta^{-1}(\mathfrak{o}^{\mathfrak{p}\times})) : \Delta(k^{\times}\mathfrak{o}^{\mathfrak{p}\times})]$$
$$= [\mathfrak{o}^{\mathfrak{p}\times} \cap N^{-1}(1) : \Delta(\mathfrak{o}^{\mathfrak{p}\times})]$$
Jetzt folgt die Beh. mit (19.5)

(19.8) Lemma: Sei e die Zahl der endlichen Verzweigungsstellen von K über k. Dann ist $[A^\sigma : (k\to\sigma)(I^k)] = 2^e$.

Bew.: klar (oder siehe /8/ S. 275)

(19.9) Satz: Sei d die Zahl der Verzweigungsstellen von K über k. Dann ist

$$[A^\mathfrak{k} : A^\mathfrak{k} \cap H^\mathfrak{k}] = \frac{2^d\,[I^k : H^k]}{\kappa\cdot[\sigma^\times : N(\mathcal{O}^{\mathfrak{k}\times})]} \cdot \frac{[A^\mathfrak{k} \cap (\mathfrak{k}\to\sigma)^{-1}(\mathcal{O}^\sigma) : \{\mathcal{O}^\mathfrak{k}\}]}{[A^\sigma : (\mathfrak{k}\to\sigma)(A^\mathfrak{k})]}$$

Insbesondere ist also $[A^\sigma : A^\sigma \cap H^\sigma] = \dfrac{2^d\cdot[I^k : H^k]}{\kappa\cdot[\sigma^\times : N(\mathcal{O}^{\sigma\times})]}$

Bew.: Wegen (19.7) ist noch zu zeigen:

$$[A^\mathfrak{k} : (k\to\mathfrak{k})(I^k)] = 2^e\,\frac{[A^\mathfrak{k} \cap (\mathfrak{k}\to\sigma)^{-1}(\mathcal{O}^\sigma) : \{\mathcal{O}^\mathfrak{k}\}]}{[A^\sigma : (\mathfrak{k}\to\sigma)(A^\mathfrak{k})]}$$

Wie wir im Beweis von (18.17) gesehen haben, ist $(\mathfrak{k}\to\sigma)(A^\mathfrak{k}) \subset A^\sigma$,
Wegen Lemma (19.8) ergibt sich dann mit dem Homororphiesatz (7.6),
angewandt auf $(\mathfrak{k}\to\sigma)$:

$$[A^\mathfrak{k} : (k\to\mathfrak{k})(I^k)] = [(\mathfrak{k}\to\sigma)(A^\mathfrak{k}) : (k\to\sigma)(I^k)]\cdot[A^\mathfrak{k} \cap (\mathfrak{k}\to\sigma)^{-1}(\mathcal{O}^\sigma) : (k\to\mathfrak{k})(I^k) \cap (\mathfrak{k}\to\sigma)^{-1}(\mathcal{O}^\sigma)]$$

$$= \frac{2^e}{[A^\sigma : (\mathfrak{k}\to\sigma)(A^\mathfrak{k})]} \cdot [A^\mathfrak{k} \cap (\mathfrak{k}\to\sigma)^{-1}(\mathcal{O}^\sigma) : \{\mathcal{O}^\mathfrak{k}\}]$$

Dabei ergibt sich $(k\to\mathfrak{k})(I^k) \cap (\mathfrak{k}\to\sigma)^{-1}(\mathcal{O}^\sigma) = \{\mathcal{O}^\mathfrak{k}\}$ folgendermaßen:
Sei $\alpha \in I^k$ und $\alpha\,\mathcal{O}^\mathfrak{k}\mathcal{O}^\sigma = \mathcal{O}^\sigma$, also $\alpha\,\mathcal{O}^\sigma = \mathcal{O}^\sigma$.
Da $(k\to\sigma)$ injektiv ist, ist $\alpha = \sigma$ und $\alpha\,\mathcal{O}^\mathfrak{k} = \mathcal{O}^\mathfrak{k}$.

(19.10) Satz: Gleiche Voraussetzung wie in (18.25).
Sei e die Zahl der endlichen Verzweigungsstellen von K über k. Dann ist:

i) $$l^*_{2n}(\mathfrak{M},\mathfrak{k}) = \frac{2^e[I^k : I^{k(2)}S_\mathfrak{M}]}{\kappa[N(A^\mathfrak{k})S_\mathfrak{M} : I^{k(2)}S_\mathfrak{M}]} \cdot \frac{[A^\mathfrak{k} \cap (\mathfrak{k}\to\sigma)^{-1}(\mathcal{O}^\sigma) : \{\mathcal{O}^\mathfrak{k}\}]}{[A^\sigma : (\mathfrak{k}\to\sigma)(A^\mathfrak{k})]}$$

ii) $$[A^\mathfrak{k} \cap (\mathfrak{k}\to\sigma)^{-1}(\mathcal{O}^\sigma) : \{\mathcal{O}^\mathfrak{k}\}] = \prod_{\mathfrak{p}\mid\mathfrak{k}} [\mathcal{O}_\mathfrak{p}^{\sigma\times} \cap \Delta^{-1}(\mathcal{O}_\mathfrak{p}^{\mathfrak{k}\times}) : \mathcal{O}_\mathfrak{p}^{\mathfrak{k}\times}]$$

iii) $$[A^\sigma : (\mathfrak{k}\to\sigma)(A^\mathfrak{k})] = \prod_{\mathfrak{p}\mid\mathfrak{k}} [\Delta^{-1}(\mathcal{O}_\mathfrak{p}^{\sigma\times}) : \Delta^{-1}(\mathcal{O}_\mathfrak{p}^{\mathfrak{k}\times})\mathcal{O}_\mathfrak{p}^{\sigma\times}]$$

Bew.: i) Vergleich von (18.25) und (19.9) mit unserer Beh. lehrt, daß wir zeigen müssen:

$$\frac{[\mu^\times : N(\mathcal{O}^{\mathfrak{f}\times})]}{[N(A^{\mathfrak{f}}) : N(A^{\mathfrak{f}}) \cap S_\mu]} \cdot \frac{2^d[I^k : H^k]}{[\sigma^\times : N(\mathcal{O}^{\mathfrak{f}\times})]} = \frac{2^e[I^k : I^{k(2)}S_\mu]}{[N(A^{\mathfrak{f}})S_\mu : I^{k(2)}S_\mu]}$$

d.h. $$\frac{2^{d-e}[I^k : H^k]}{[N(A^{\mathfrak{f}})S_\mu : S_\mu]\cdot[\sigma^\times : \mu^\times]} = [I^k : N(A^{\mathfrak{f}})S_\mu]$$

d.h. $$\frac{2^{d-e}[I^k : H^k]}{[I^k : S_\mu]\cdot[\sigma^\times : \mu^\times]} = 1$$

d-e ist die Zahl der unendlichen (reellen) Verzweigungsstellen von K über k. Da K und Q an allen reellen Primstellen von k verzweigt sind (siehe 13.4.i und iv), ist d-e die Zahl der verschiedenen Primstellen, die μ teilen. Die Beh. folgt jetzt mit Lemma (8.5).

ii) Wegen (18.12.i) folgt genauso wie Lemma (7.16), daß wir einen natürlichen Isomorphismus $\Pi^{\mathfrak{f}}$ haben:

$$\Pi^{\mathfrak{f}}: A^{\mathfrak{f}} \cap (\mathfrak{f}\to\sigma)^{-1}(\mathcal{O}^\sigma) \to \prod_{\mathfrak{P}\mid\mathfrak{f}} \left(A_{\mathfrak{P}}^{\mathfrak{f}} \cap (\mathfrak{f}\to\sigma)_{\mathfrak{P}}^{-1}(\mathcal{O}_{\mathfrak{P}}^\sigma)\right)$$

Insbesondere ist $[A^{\mathfrak{f}} \cap (\mathfrak{f}\to\sigma)^{-1}(\mathcal{O}^\sigma) : \{\mathcal{O}^{\mathfrak{f}}\}] = \prod_{\mathfrak{P}\mid\mathfrak{f}} [A_{\mathfrak{P}}^{\mathfrak{f}} \cap (\mathfrak{f}\to\sigma)_{\mathfrak{P}}^{-1}(\mathcal{O}_{\mathfrak{P}}^\sigma) : \{\mathcal{O}_{\mathfrak{P}}^{\mathfrak{f}}\}]$.

Sei jetzt $\mathfrak{P}$ ein Primteiler von $\mathfrak{f}$.

Sei $\eta_{\mathfrak{P}}^{\mathfrak{f}}: K_{\mathfrak{P}}^\times \to I_{\mathfrak{P}}^{\mathfrak{f}}$ die Abb. mit $\eta_{\mathfrak{P}}^{\mathfrak{f}}(a) = a\mathcal{O}_{\mathfrak{P}}^{\mathfrak{f}}$ für $a \in K_{\mathfrak{P}}^\times$.

Da $I_{\mathfrak{P}}^{\mathfrak{f}}$ nur Hauptideale enthält, folgt wie Lemma (18.12.iii), daß $(\eta_{\mathfrak{P}}^{\mathfrak{f}})^{-1}(A_{\mathfrak{P}}^{\mathfrak{f}}) = \Delta^{-1}(\mathcal{O}_{\mathfrak{P}}^{\mathfrak{f}\times})$. Man sieht leicht, daß $\eta_{\mathfrak{P}}^{\mathfrak{f}}$ surjektiv ist und daß $(\eta_{\mathfrak{P}}^{\mathfrak{f}})^{-1}((\mathfrak{f}\to\sigma)_{\mathfrak{P}}^{-1}(\mathcal{O}_{\mathfrak{P}}^\sigma)) = \mathcal{O}_{\mathfrak{P}}^{\sigma\times}$ und $(\eta_{\mathfrak{P}}^{\mathfrak{f}})^{-1}(\mathcal{O}_{\mathfrak{P}}^{\mathfrak{f}}) = \mathcal{O}_{\mathfrak{P}}^{\mathfrak{f}\times}$.

Nach dem Homomorphiesatz (7.6), angewandt auf $\eta_{\mathfrak{P}}^{\mathfrak{f}}$, ist also:

$$[A_{\mathfrak{P}}^{\mathfrak{f}} \cap (\mathfrak{f}\to\sigma)_{\mathfrak{P}}^{-1}(\mathcal{O}_{\mathfrak{P}}^\sigma) : \{\mathcal{O}_{\mathfrak{P}}^{\mathfrak{f}}\}] = [\Delta^{-1}(\mathcal{O}_{\mathfrak{P}}^{\mathfrak{f}\times}) \cap \mathcal{O}_{\mathfrak{P}}^{\sigma\times} : \mathcal{O}_{\mathfrak{P}}^{\mathfrak{f}\times}]$$

iii) Mit einer ähnlichen Argumentation wie im Beweis von Lemma (7.16) zeigt man, daß $[A^\sigma : (\mathfrak{f}\to\sigma)(A^{\mathfrak{f}})] = \prod_{\mathfrak{P}\mid\mathfrak{f}} [A_{\mathfrak{P}}^\sigma : (\mathfrak{f}\to\sigma)_{\mathfrak{P}}(A_{\mathfrak{P}}^{\mathfrak{f}})]$.

Mansieht leicht ein, daß für alle Primteiler $\mathfrak{P}$ von $\mathfrak{f}$ gilt:

$$(\eta_{\mathfrak{P}}^\sigma)^{-1}\left((\mathfrak{f}\to\sigma)_{\mathfrak{P}}(A_{\mathfrak{P}}^{\mathfrak{f}})\right) = \Delta^{-1}(\mathcal{O}_{\mathfrak{P}}^{\mathfrak{f}\times})\mathcal{O}_{\mathfrak{P}}^{\sigma\times}.$$

Wegen $(\eta_{\mathfrak{P}}^\sigma)^{-1}(A_{\mathfrak{P}}^\sigma) = \Delta^{-1}(\mathcal{O}_{\mathfrak{P}}^{\sigma\times})$ folgt die Beh. (aus dem Homomorphiesatz).

§ 20 . Beispiel: Zyklische Gruppen der Ordnung 6 in Quaternionenalgebren über imaginärquadratischen Zahlkörpern.

In diesem und im nächsten Paragrafen wollen wir die Ergebnisse der Paragrafen 16, 17 und 18 für imaginärquadratische Körper so weit konkretisieren, daß man die gesuchten Konjugationsklassenzahlen relativ leicht mit Hilfe von zahlentheoretischen Tabellen berechnen kann.

In diesem Paragrafen untersuchen wir die 6-zyklischen Gruppen. Hauptergebnisse sind die Sätze (20.39) (mit Tabelle 20.40) und (20.41). Für die Körper $k = \mathbb{Q}(i\sqrt{d})$ mit $1 \leq d \leq 101$ und die Quaternionenalgebra $M_2(k)$ tabellieren wir das Ergebnis am Ende des Paragrafen (20.42).

Wir machen folgende Generalvoraussetzung:

(20.1) Sei $d \in \mathbb{N}$ quadratfrei, sei $k = \mathbb{Q}(i\sqrt{d})$, sei $\mathfrak{o}$ die Hauptordnung von k. Sei Q eine k-Quaternionenalgebra. Alle Primteiler von $D_k(Q)$ seien verzweigt oder träge in $K := k[X]/(X^2-X+1)k[X]$, d.h. die Bedingungen von Satz (14.6) seien erfüllt, $\Gamma(Q)$ enthalte 6-zyklische Untergruppen.

Da k keine reellen Primstellen hat, enthält $\mathfrak{u} = \mathfrak{u}(Q)$ keine Primstellen. Die Voraussetzungen der Paragrafen 16 und 17 (und 18) sind also erfüllt und es ist $\mathfrak{u}^\times = \mathfrak{o}^\times$ und $S_\mathfrak{u} = H^k$.

Wir müssen $F_6(\mathfrak{M})$ und $F_6^*(\mathfrak{M})$ für die verschiedenen Maximalordnungen berechnen sowie die Größen (für $\mathfrak{f} \in F_6(\mathfrak{M})$ bzw. $\mathfrak{f} \in F_6^*(\mathfrak{M})$):

$$\left.\begin{aligned} &l_6(\mathfrak{M},\mathfrak{f}) = \\ &2^t \cdot \left[I^k : \mathrm{RN}(I^K)H^k\right] \cdot \frac{\left[I^K : H^K\right]}{\left[I^k : H^k\right]} \cdot \frac{\left[\mathfrak{o}^\times : N(\mathfrak{O}^{\mathfrak{f}\times})\right]}{\left[\mathfrak{O}^{\mathfrak{o}\times} : \mathfrak{O}^{\mathfrak{f}\times}\right]} \cdot \varkappa(\mathfrak{f}) \prod_{\mathfrak{P}\mid\mathfrak{f}} \left(1-\left(\frac{K}{\mathfrak{P}}\right)\mathfrak{N}(\mathfrak{P})^{-1}\right) \\ &l_6^*(\mathfrak{M},\mathfrak{f}) = \\ &\frac{2^e \cdot \left[I^k : I^{k(2)}H^k\right]}{\kappa \cdot \left[N(A^\mathfrak{f})H^k : I^{k(2)}H^k\right]} \cdot \frac{\left[A^\mathfrak{f} \cap (\mathfrak{f}\to\mathfrak{o})^{-1}(\mathfrak{O}^\mathfrak{o}) : (\mathfrak{O}^\mathfrak{f})\right]}{\left[A^\mathfrak{o} : (\mathfrak{f}\to\mathfrak{o})A^\mathfrak{f}\right]} \end{aligned}\right\} \quad (20.2)$$

siehe (17.14 und 19.10). Wir berechnen zuerst $F_6(\mathfrak{M})$ und $l_6(\mathfrak{M},\mathfrak{f})$.

Sei zuerst $d = 3$. Dann ist notwendig $Q \underset{k}{\simeq} M_2(k)$ (siehe 14.6). Bekanntlich ist hier $\left[I^k : H^k\right] = 1$, also auch $\left[I^k : I^{k(2)}H^k\right] = 1$. Es gibt also nur einen einzigen Maximalordnungstyp in Q (siehe 10.13). Q hat keine Verzweigungsstellen über k, insbesondere $D_k(Q) = \mathfrak{o}$ und $t = 0$.

K ist kein Körper, da $\zeta_6 \in k$. Insbesondere ist $D_k(K) = \mathfrak{o}$ und $[I^k : RN(I^K)H^k] = 1$.
Es ist $(\zeta_6 - \zeta_6^{-1})^2 = -3$. Ist $\mathfrak{M}$ eine Q-Maximalordnung, so folgt mit (16.5):

$F_6(\mathfrak{M}) = \{ \mathfrak{f} \mid \mathfrak{f}$ ist ganzes $\mathfrak{o}$-Ideal und $\mathfrak{f}^2 | 3\mathfrak{o} \}$.

3 ist verzweigt in k. Sei $3\mathfrak{o} = \mathfrak{p}^2$ (also $\mathfrak{p} = i\sqrt{3}\,\mathfrak{o}$).
Dann ist also $\underline{F_6(\mathfrak{M}) = \{\mathfrak{o}, \mathfrak{p}\}}$.

Nach (7.26.i) ist $[I^K : H^K] = [I^k : H^k]^2 = 1$.
Wie im Bew. von (19.3) gesehen, ist $[\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{o}\times})] = 1$. Also $\underline{l_6(\mathfrak{M}, \mathfrak{o}) = 1}$
Es gibt K-Idempotente e_1, e_2, so daß $K = ke_1 \oplus ke_2$ und $\mathcal{O}^{\mathfrak{o}} = \mathfrak{o}e_1 + \mathfrak{o}e_2$.
Es ist $\mathcal{O}^{\mathfrak{p}} = \mathfrak{o} + \mathfrak{p}\mathcal{O}^{\mathfrak{o}}$. Daraus leitet man leicht her, daß
$\mathcal{O}^{\mathfrak{p}} = \{ae_1 + be_2 \mid a,b \in \mathfrak{o}$ und $a-b \in \mathfrak{p}\}$.
ζ_6 ist erzeugendes Element von $\mathfrak{o}^\times$ und man sieht leicht, daß
$\zeta_6 = \zeta_6 e_1 + \zeta_6 e_2$ und $E := e_1 + \zeta_6 e_2$ erzeugende Elemente von $\mathcal{O}^{\mathfrak{o}\times}$ sind.
Es ist $\zeta_6 \in \mathfrak{o}^\times \subset \mathcal{O}^{\mathfrak{p}\times}$, aber $E \notin \mathcal{O}^{\mathfrak{p}\times}$, da $1 - \zeta_6 = \zeta_6^{-1} \notin \mathfrak{p}$.
Da $1 - \zeta_6^2 = (1 - \zeta_6)(1 + \zeta_6) = \zeta_6^{-1}(3/2 + i/2\cdot\sqrt{3}) \in \mathfrak{p}$, ist
$E^2 = e_1 + \zeta_6^2 e_2 \in \mathcal{O}^{\mathfrak{p}\times}$ und wir erhalten $[\mathcal{O}^{\mathfrak{o}\times} : \mathcal{O}^{\mathfrak{p}\times}] = 2$.
Wegen $N(\zeta_6) = N(E^2) = \zeta_6^2$ wird $[\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{p}\times})] = [\mathfrak{o}^\times : \mathfrak{o}^{\times(2)}] = 2$.
Da $\mathfrak{p}$ über $\mathbb{Q}$ verzweigt ist, ist $\mathfrak{N}(\mathfrak{p}) = 3$. Außerdem ist $\left(\frac{K}{\mathfrak{p}}\right) = 1$.
(siehe 5.2.ii). Man erhält also $l_6(\mathfrak{M}, \mathfrak{p}) = 3(1 - 1/3) = 2$.

<u>(20.3) Lemma:</u> Voraussetzung (20.1). Wenn $d = 3$, ist notwendig $Q \underset{k}{\cong} M_2(k)$.
Alle Q-Maximalordnungen sind vom gleichen Typ. Ist $\mathfrak{M}$ eine Q-Maximalordnung, so ist $F_6(\mathfrak{M}) = \{\mathfrak{o}, \mathfrak{p}\}$ und $l_6(\mathfrak{M}, \mathfrak{o}) = 1$ sowie
$l_6(\mathfrak{M}, \mathfrak{p}) = 2$, also $l_6(\mathfrak{M}) = 3$.
(Dabei sei $\mathfrak{p} = i\sqrt{3}$ der Primteiler von $3\mathbb{Z}$ in $\mathfrak{o}$.)

Sei von jetzt an $\underline{d \neq 3}$. Dann ist K Körper und wir können identifizieren:
$K = k(\zeta_6) = k(i\sqrt{3})$.
Nach Lemma (14.4) sind in K über k höchstens die Primteiler von 3 verzweigt, da 3 die einzige endliche Verzweigungsstelle von $\mathbb{Q}(i\sqrt{3})$ über $\mathbb{Q}$ ist.

<u>(20.4) Lemma:</u> Sei $d \neq 3$. Dann ist $D_k(K) = \begin{cases} \mathfrak{o} & , \text{wenn } 3|d \\ 3\mathfrak{o} & , \text{wenn } 3\nmid d \end{cases}$

Bew.: Falls $3|d$, ist 3 in $\mathbb{Q}(\sqrt{3d}) = \mathbb{Q}(\sqrt{d/3})$ unverzweigt; nach Lemma (14.4) ist K über k unverzweigt.
Falls $3\nmid d$, ist entweder $3\mathfrak{o}$ Primideal oder $3\mathfrak{o} = \mathfrak{p}\mathfrak{q}$ mit Primidealen $\mathfrak{p} \neq \mathfrak{q}$. Da 3 in $\mathbb{Q}(\sqrt{3d})$ verzweigt ist, ist nach Lemma (14.4) auch $3\mathfrak{o}$ bzw. $\mathfrak{p}$ und $\mathfrak{q}$ in K verzweigt. In jedem Fall ist $D_k(K)$ Vielfaches von $3\mathfrak{o}$. Es ist aber $D_k(K)$ auch Teiler von $D_k(\mathfrak{o}[\zeta_6]) = 3\mathfrak{o}$ (siehe 6.9.iii).

(20.5) Lemma: Es ist $[I^k : RN(I^K)H^k] = 2$ genau dann, wenn $d \neq 3$, $d \equiv 0 \bmod 3$ und $Q \tilde{\tilde{k}} M_2(k)$.

Bew.: (siehe 16.9) Genau in diesem Fall ist $\zeta_6 \notin k$, $D_k(K) = \mathfrak{o}$ und $Q \tilde{\tilde{k}} (-3, -1)_k$ (vgl. 14.8.iii).

(20.6) Definition: Ist k algebraischer Zahlkörper, so sei $h(k) := [I^k : H^k]$.

(20.7) Definition: Sei $d \neq 3$.
i) Dann sei $k_+ := \mathbb{Q}(\sqrt{3d})$, sei $\mathfrak{o}_+$ die Hauptordnung von k_+.
ii) Sei Z die Gruppe der Einheitswurzeln aus $\mathfrak{o}^{\mathfrak{o}\times}$.
iii) Sei $q := [\mathfrak{o}^{\mathfrak{o}\times} : Z\,\mathfrak{o}_+^\times]$.

(20.8) Satz: ($d \neq 3$). Es ist $h(K) = q/2 \cdot h(k) \cdot h(k_+)$

Bew.: siehe /10/ S. 74 (6)

(20.9) Lemma: Es ist immer $q \leq 2$ und es gilt:
i) Wenn $d \equiv 0 \bmod 3$ ($d \neq 3$), dann ist $q = 1$.
ii) Wenn $d \not\equiv 0 \bmod 3$, dann ist $q = \begin{cases} 2, \text{ wenn } \pm 3 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+) \\ 1, \text{ sonst} \end{cases}$

Bew.: zu $q \leq 2$ siehe /10/ S. 54 Satz 14
i) siehe /10/ S. 75 (10_I)
ii) Falls $d = 1$, ist wegen (20.8) notwendig $q = 2$. Es ist $-3 = 0^2 - 3\cdot 1^2$.
Für $d \neq 1$ siehe /10/ S.75/76 (10_I), (11_I), (12_I).

Bemerkung: Falls $d \not\equiv 0 \bmod 3$, ist 3 in k_+ verzweigt.
$\pm 3 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+)$ ist also äquivalent dazu, daß der Primteiler von $3\mathbb{Z}$ in $\mathfrak{o}_+$ Hauptideal ist.

(20.10) Definition: i) Sei $\varepsilon > 1$ die Grundeinheit in $\mathfrak{o}_+^\times$.
ii) Sei $x := [\mathbb{Z}^\times : N_{k_+|\mathbb{Q}}(\mathfrak{o}_+^\times)] = \begin{cases} 2, \text{ wenn } N_{k_+|\mathbb{Q}}(\varepsilon) = 1 \\ 1, \text{ wenn } N_{k_+|\mathbb{Q}}(\varepsilon) = -1 \end{cases}$

(20.11) Lemma: $[\mathfrak{o}^\times : N(Z\,\mathfrak{o}_+^\times)] = x$.

Für $d \not\equiv 0 \bmod 3$ ist daher $[\mathfrak{o}^\times : N(Z\,\mathfrak{o}_+^\times)] = 2$.

Bew.: Falls $d \neq 1$, ist $\mathfrak{o}^\times = \{\pm 1\}$. Man sieht auch leicht, daß Z von ζ_6 erzeugt wird. Es ist $N(\zeta_6) = \zeta_6\zeta_6^{-1} = 1$. Also wird

$$[\mathfrak{o}^\times : N(Z\,\mathfrak{o}_+^\times)] = [\mathfrak{o}^\times : N(\mathfrak{o}_+^\times)] = [\{\pm 1\} : N_{k_+|\mathbb{Q}}(\mathfrak{o}_+^\times)] = x.$$

Bekanntlich ist $x = 1$ nur möglich, wenn für alle Primteiler p von $D_{\mathbb{Q}}(k_+)$ gilt: $p = 2$ oder $p \equiv 1 \bmod 4$. Wenn $d \not\equiv 0 \bmod 3$, ist aber 3 ein Teiler von $D_{\mathbb{Q}}(k_+) = D_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3d}))$.

Sei jetzt $d = 1$. Dann ist $x = 2$, d.h. $N(\varepsilon) = N_{k_+|\mathbb{Q}}(\varepsilon) = 1$.

Es ist $\mathfrak{o}^\times = \{\pm 1, \pm i\}$ und Z wird von $\zeta_{12} = \zeta_4\zeta_6^{-1} = i\zeta_6^{-1}$ erzeugt.

Es ist $N(\zeta_{12}) = i^2 N(\zeta_6)^{-1} = -1$, also $[\mathfrak{o}^\times : N(Z\,\mathfrak{o}_+^\times)] = [\mathfrak{o}^\times : N(Z)] = 2$.

Wir machen jetzt Fallunterscheidungen:

Wir untersuchen zuerst den Fall, daß $d \not\equiv 0 \bmod 3$.

Dann ist $D_K(K) = 3\mathfrak{o}$. Mit (16.10.ii) folgt:

(20.12) Lemma: Sei $d \not\equiv 0 \bmod 3$.

Für alle $\mathbb{Q}$-Maximalordnungen $\mathfrak{M}$ ist dann $F_6(\mathfrak{M}) = \{\mathfrak{o}\}$.

Wir müssen noch $l_6(\mathfrak{M}) = l_6(\mathfrak{M}, \mathfrak{o}) = 2^{t-1} qh(k_+)\,[\mathfrak{o}^\times : N(\mathfrak{O}^{\mathfrak{o}\times})]$ berechnen.

(20.13) Lemma: Sei $d \not\equiv 0 \bmod 3$.

i) Wenn $-3 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+)$, dann gilt für alle Primteiler $p \in \mathbb{N}$ von d die Kongruenz: $p \equiv 1 \bmod 3$. Insbesondere ist also $d \equiv 1 \bmod 3$.

ii) Wenn $+3 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+)$, dann gilt für alle Primteiler $p \in \mathbb{N}$ von d entweder $p = 2$ oder $p \equiv \pm 1 \bmod 12$. Außerdem ist dann $d \equiv 2 \bmod 3$.

Bew.: i) Sei $-3 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+)$ und sei $p \neq 2$ Primteiler von d.

Dann gibt es $a, b \in 1/2 \cdot \mathbb{Z}$ mit $-3 = a^2 - 3db^2$. Es muß also $\left(\frac{-3}{p}\right) = 1$ sein.

Es ist $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2} \cdot (-1)^{(p-1)/2 \cdot (3-1)/2} \cdot \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$.

Also ist notwendig $\left(\frac{p}{3}\right) = 1$, d.h. $p \equiv 1 \bmod 3$.

Wenn $2 \mid d$, muß es $a, b \in \mathbb{Z}$ geben mit $-3 = a^2 - 3db^2$.

Dann folgt $a^2 \equiv -3 \bmod 2$, also $a \equiv 1 \bmod 2$, also $a^2 \equiv 1 \bmod 8$.

Damit folgt $3db^2 \equiv 4 \bmod 8$, also $b^2 \equiv 2 \bmod 4$. ↯

ii) Sei $+3 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+)$ und sei $p \neq 2$ Primteiler von d.

Es gibt $a, b \in 1/2 \cdot \mathbb{Z}$ mit $3 = a^2 - 3db^2$. Also ist $\left(\frac{3}{p}\right) = 1$.

Wegen $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)$ gilt: $\left(\frac{3}{p}\right) = 1$ genau dann, wenn

($p \equiv 1 \bmod 4$ und $p \equiv 1 \bmod 3$) oder ($p \equiv -1 \bmod 4$ und $p \equiv -1 \bmod 3$).

Außerdem muß gelten: $a^2 \equiv 0 \bmod 3$, also $a^2 \equiv 0 \bmod 9$.

Damit folgt: $3 \equiv -3db^2 \bmod 9$, also $1 \equiv -db^2 \bmod 3$.

Daher ist $b \not\equiv 0 \bmod 3$, also $b^2 \equiv 1 \bmod 3$ und $1 \equiv -d \bmod 3$.

Wir haben außerdem gezeigt:

(20.14) Lemma: Sei $p \neq 2, 3$ eine Primzahl. Dann gilt:
$\left(\frac{3}{p}\right) = 1$ genau dann, wenn $p \equiv \pm 1 \bmod 12$.

(20.15) Definition: Sei $z := \begin{cases} 2, \text{ wenn } +3 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+) \\ 1, \text{ sonst} \end{cases}$

Wir betrachten jetzt speziell den Fall $d \equiv 2 \bmod 3$.

Wie aus Lemma (20.13) hervorgeht, ist dann $q = z$.

Da $(-3, -1)_k$ Divisionsalgebra ist (14.8.iv), gibt es keine $a, b \in k$

mit $1 + a^2 + 3b^2 = 0$ (siehe 1.20.iii und 1.18), d.h. $N(a + bi\sqrt{3}) = -1$.

Insbesondere ist $[\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{o}\times})] = [\{\pm 1\} : \{1\}] = 2$.

(20.16) Lemma: Sei $d \equiv 2 \bmod 3$. Dann gilt für alle Q-Maximalordnungen $\mathfrak{M}$ die Gleichung: $l_6(\mathfrak{M}) = l_6(\mathfrak{M}, \mathfrak{o}) = 2^t z h(k_+)$.

Bemerkung: Es ist $z = 2$ genau dann, wenn der Primteiler von $3\mathbb{Z}$ in $\mathfrak{o}_+$ Hauptideal wird. Eine notwendige Bedingung ist (20.13.ii).

(20.17) Lemma: Sei $d \equiv 1 \bmod 3$. Dann gilt für alle Q-Maximalordnungen $\mathfrak{M}$ die Gleichung: $l_6(\mathfrak{M}) = l_6(\mathfrak{M}, \mathfrak{o}) = 2^t h(k_+)$.

Bew.: Wir müssen offensichtlich zeigen: $q \cdot [\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{o}\times})] = 2$.

Wenn $q = 1$, ist nach Definition von q und Lemma (20.11):

$q \cdot [\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{o}\times})] = [\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{o}\times})] = [\mathfrak{o}^\times : N(\mathbb{Z}\,\mathfrak{o}_+^\times)] = 2$.

Wir müssen also noch zeigen:

(20.18) Lemma: Sei $d \equiv 1 \bmod 3$ und sei $q = [\mathcal{O}^{\mathfrak{o}\times} : \mathbb{Z}\,\mathfrak{o}_+^\times] = 2$.

Dann ist $[\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{o}\times})] = 1$.

Der Beweis ist sehr umfangreich. Er geht bis (20.24).

Bew.: $3\mathbb{Z}$ ist in k träge. $3\mathfrak{o}$ ist daher die einzige Primstelle von k, die in K verzweigt ist. Aus (19.9) folgt also:
$[A^{\mathfrak{o}} : A^{\mathfrak{o}} \cap H^{\mathfrak{o}}] = [I^k : H^k] / [\mathfrak{o}^\times : N(\mathfrak{O}^{\mathfrak{o}\times})]$.
Wir müssen zeigen: $[A^{\mathfrak{o}} : A^{\mathfrak{o}} \cap H^{\mathfrak{o}}] = [I^k : H^k]$.
A wird erzeugt von den $\mathfrak{o}$-Idealen und $i\sqrt{3}\,\mathfrak{O}^{\mathfrak{o}} \in H^{\mathfrak{o}}$, dem einzigen über k verzweigten $\mathfrak{O}^{\mathfrak{o}}$-Ideal. Daher ist:

$$[A^{\mathfrak{o}} : A^{\mathfrak{o}} \cap H^{\mathfrak{o}}] = [A^{\mathfrak{o}} H^{\mathfrak{o}} : H^{\mathfrak{o}}] = [(k \to \mathfrak{o})(I^k) H^{\mathfrak{o}} : H^{\mathfrak{o}}]$$
$$= [(k \to \mathfrak{o})(I^k) : (k \to \mathfrak{o})(I^k) \cap H^{\mathfrak{o}}]$$

Wir müssen also zeigen, daß der durch $(k \to \mathfrak{o})$ induzierte surjektive Homomorphismus : $I^k/H^k \to (k \to \mathfrak{o})(I^k) / (k \to \mathfrak{o})(I^k) \cap H^{\mathfrak{o}}$ auch injektiv ist.
Seien $\mathfrak{a} \in I^k$ und $a \in K^\times$ mit $\mathfrak{a}\,\mathfrak{O}^{\mathfrak{o}} = a\,\mathfrak{O}^{\mathfrak{o}}$. (es ist zu zeigen: $\mathfrak{a} \in H^k$).
Dann ist $\mathfrak{a}^2 = N(\mathfrak{a}\,\mathfrak{O}^{\mathfrak{o}}) = N(a)\mathfrak{o} \in H^k$.

(20.19) Definition: Wir bezeichnen den nichttrivialen Automorphismus von K über k_+ mit '. Die Einschränkung von ' auf k (d.h. den nichttrivialen Automorphismus von k über $\mathbb{Q}$) bezeichnen wir ebenfalls mit '.

Für unser $\mathfrak{a}$ gilt dann: $\mathfrak{a}\,\mathfrak{a}'^{-1} = \mathfrak{a}^2(\mathfrak{a}\mathfrak{a}')^{-1} = \mathfrak{a}^2 N_{k|\mathbb{Q}}(\mathfrak{a})^{-1} \in H^k$, da $\mathbb{Z}$ Hauptidealring ist.

(20.20) Definition: Ist k ein über $\mathbb{Q}$ quadratischer Zahlkörper, dann bezeichnen wir die Gruppe der über $\mathbb{Q}$ ambigen Ideale aus k mit A^k.

(20.21) Lemma: Ist k ein imaginärquadratischer Zahlkörper mit nichttrivialem Automorphismus ' und ist $\mathfrak{a} \in I^k$ mit $\mathfrak{a}\,\mathfrak{a}'^{-1} \in H^k$, dann ist $\mathfrak{a} \in A^k H^k$.

Bew.: siehe /12/ S. 178 Satz 107

Unser $\mathfrak{a}$ liegt also in $A^k H^k$.
Offensichtlich müssen wir nur zeigen, daß der durch $(k \to \mathfrak{o})$ induzierte Homomorphismus $\overline{(k \to \mathfrak{o})}$ injektiv ist.

$$A^k/A^k \cap H^k \xrightarrow{\overline{(k\to\mathfrak{o})}} A^k H^k/H^k \to (k\to\mathfrak{o})(A^k H^k)/(k\to\mathfrak{o})(A^k H^k) \cap H^{\mathfrak{o}}$$
$$\nearrow$$
$$(k\to\mathfrak{o})(A^k)/(k\to\mathfrak{o})(A^k) \cap H^{\mathfrak{o}}$$

Zum Beweis faktorisieren wir $(k \to \mathfrak{o}) : A^k \to (k \to \mathfrak{o})(A^k)$ folgendermaßen:

$$A^k \xrightarrow{(k\to\mathfrak{o})} (k\to\mathfrak{o})(A^k) \subseteq I^{\mathfrak{o}}$$
$$(k \to k_+) \searrow \qquad \nearrow (k_+ \to \mathfrak{o})$$
$$A^{k_+}$$

Man sieht leicht, daß die endlichen Verzweigungsstellen von $k = \mathbb{Q}(i\sqrt{d})$ über $\mathbb{Q}$ auch Verzweigungsstellen von $k_+ = \mathbb{Q}(\sqrt{3d})$ über $\mathbb{Q}$ sind.
Dann sieht man ebenfalls leicht, daß durch die Vorschrift $\mathfrak{a} \mapsto \mathfrak{a}\mathfrak{O}^\sigma \cap k_+$ eine Abbildung $(k \to k_+)\colon A^k \to A^{k_+}$ wohldefiniert wird, daß $(k \to k_+)$ ein Homomorphismus ist und daß $(k \to \sigma) = (k_+ \to \sigma) \circ (k \to k_+)$. Dabei sei $(k_+ \to \sigma)$ die Einschränkung der Abbildung $(k_+ \to \sigma)\colon I^{k_+} \to I^\sigma$ mit Vorschrift $\mathfrak{b} \mapsto \mathfrak{b}\mathfrak{O}^\sigma$.
Wir müssen zeigen, daß $(k \to k_+)$ und $(k_+ \to \sigma)$ jeweils injektive Abbildungen

$\overline{(k \to k_+)}\colon A^k/A^k \cap H^k \to A^{k_+}/A^{k_+} \cap H^{k_+}$

$\overline{(k_+ \to \sigma)}\colon I^{k_+}/H^{k_+} \to I^\sigma/H^\sigma$ induzieren.

i) Wir untersuchen $\overline{(k \to k_+)}$

(20.22) Definition: Sei δ die Zahl der endlichen Verzweigungsstellen von k über $\mathbb{Q}$ (d.h. die Zahl der verschiedenen Primteiler von $D_{\mathbb{Q}}(k)$).

Da $[I^{\mathbb{Q}} : H^{\mathbb{Q}}] = 1$ und $N_{k|\mathbb{Q}}(a) > 0$ für alle $a \in k$ und da k genau eine unendliche Verzweigungsstelle über $\mathbb{Q}$ hat, folgt mit (19.9):
$[A^k : A^k \cap H^k] = 2^{\delta-1}$.
k_+ hat keine unendliche Verzweigungsstelle über $\mathbb{Q}$. Außer den δ endlichen Verzweigungsstellen über $\mathbb{Q}$, die er mit k gemeinsam hat, hat k_+ noch die Verzweigungsstelle 3 über $\mathbb{Q}$. Es ist $N_{k_+|\mathbb{Q}}(\varepsilon) = 1$ (siehe 20.11). Daher folgt mit (19.9):

$$[A^{k_+} : A^{k_+} \cap H^{k_+}] = 2^{\delta-1} = [A^k : A^k \cap H^k] \qquad (20.23)$$

Wegen $[A^k : A^k \cap H^k] = 2^{\delta-1}$ erkennt man leicht, daß $A^k \cap H^k$ durch die Ideale aus $\mathbb{Q}$ und durch $i\sqrt{d}\,\sigma$ erzeugt wird.
Sei $\mathfrak{p}$ der Primteiler von 3 in σ_+. Da $q = 2$ nach Voraussetzung, ist $\mathfrak{p}$ ein Hauptideal (siehe 20.9.ii). Da außerdem $\sqrt{3d}\,\sigma_+$ ein Hauptideal ist, ist offensichtlich $(k \to k_+)(i\sqrt{d}\,\sigma) = \sqrt{3d}\,\mathfrak{p}^{-1} \in A^{k_+} \cap H^{k_+}$;
also ist $\overline{(k \to k_+)}$ wohldefiniert.

Wir können $\overline{(k \to k_+)}$ auf natürliche Weise faktorisieren:

$$A^k/A^k \cap H^k \to (k \to k_+)(A^k)/(k \to k_+)(A^k) \cap H^{k_+} \to A^{k_+}/A^{k_+} \cap H^{k_+}.$$

A^{k_+} wird von den Idealen aus $(k \to k_+)(A^k)$ und von $\mathfrak{p}$ erzeugt.
Da $\mathfrak{p}$ ein Hauptideal ist, ist der rechte Teil der Faktorisierung ein Isomorphismus. Der linke Teil ist surjektiv.
Also ist $\overline{(k \to k_+)}$ surjektiv und wegen (20.23) auch injektiv.

ii) Wir untersuchen $\overline{(k_+ \to \sigma)}$

Sei A' die Gruppe der über k_+ (bzgl. ') ambigen $\mathcal{O}^\sigma$-Ideale.
Da (wie man leicht sieht) K über k_+ keine endlichen, aber zwei unendliche Verzweigungsstellen hat, ist $A' = (k_+ \to \sigma)(I^{k_+})$ und mit (19.9) folgt: $\left[(k_+ \to \sigma)(I^{k_+}) : (k_+ \to \sigma)(I^{k_+}) \cap H^\sigma\right] = 2 \cdot \left[I^{k_+} : H^{k_+}\right] / \left[\sigma_+^\times : N_{K|k_+}(\mathcal{O}^{\sigma\times})\right]$.

Wir müssen noch zeigen: $\left[\sigma_+^\times : N_{K|k_+}(\mathcal{O}^{\sigma\times})\right] = 2$

K ist algebraischer Zahlkörper mit zwei komplexen und keiner reellen Primstelle. Nach dem Dirichletschen Einheitensatz ist $\mathcal{O}^{\sigma\times}$ direktes Produkt von Z mit einer unendlichen zyklischen Gruppe, die von einer "Grundeinheit" ε_0 erzeugt wird.

(20.24) Lemma: Wenn q = 2, läßt sich ε_0 folgendermaßen wählen:
Es gibt $\zeta \in Z$ mit $\varepsilon = \zeta\varepsilon_0^2$.

Bew.: siehe /10/ S. 75 (8)

Da $N_{K|k_+}(a) \geq 0$ für alle $a \in K$, folgt jetzt leicht: $N_{K|k_+}(\varepsilon_0) = \varepsilon$ und:

$\sigma_+^\times$ ist direktes Produkt der von -1 und ε erzeugten Gruppen;

$N_{K|k_+}(\mathcal{O}^{\sigma\times})$ ist die von ε erzeugte Gruppe.

Damit folgt die Behauptung und (20.18) ist bewiesen.

Wir betrachten jetzt den Fall $d \equiv 0 \bmod 3$.
Wegen $D_k(K) = \sigma$ ist $F_6(\mathfrak{M}) \subset \{ \mathfrak{f} \mid \mathfrak{f}$ ist ganzes σ-Ideal und $\mathfrak{f}^2 | 3\sigma \}$ für alle Q-Maximalordnungen $\mathfrak{M}$.
Es ist 3 verzweigt in k, sei $3\sigma =: \mathfrak{p}^2$.
Dann ist $F_6(\mathfrak{M}) \subset \{ \sigma, \mathfrak{p} \}$.
3 ist in $\mathbb{Q}(i\sqrt{3})$ verzweigt.
Wenn $d \equiv 3 \bmod 9$, also $d/3 \equiv 1 \bmod 3$, ist 3 in $k_+ = \mathbb{Q}(\sqrt{d/3})$ zerlegt.
Wenn $d \equiv 6 \bmod 9$, also $d/3 \equiv 2 \bmod 3$, ist 3 in k_+ träge.
Also folgt mit Lemma (14.4), Satz (16.10) und Lemma (16.12):

(20.25) Lemma: Sei $d \neq 3$.
i) Wenn $d \equiv 3 \bmod 9$, dann ist $\left(\frac{K}{\mathfrak{p}}\right) = 1$ und es gilt:
a) Wenn $Q \underset{k}{\simeq} M_2(k) \underset{k}{\simeq} (-3, -1)_k$, dann gibt es eine Q-Maximalordnung $\mathfrak{M}$ mit $F_6(\mathfrak{M}) = \{ \sigma, \mathfrak{p} \}$. Ist $\mathfrak{M}'$ eine weitere Q-Maximalordnung, so gilt:

$$F_6(\mathfrak{M}') = \begin{cases} \{ \sigma, \mathfrak{p} \}, & \text{wenn } N(\mathfrak{M}\mathfrak{M}') \in N(I^K)H^k \\ \emptyset, & \text{wenn } N(\mathfrak{M}\mathfrak{M}') \notin N(I^K)H^k \end{cases}$$

b) Wenn Q Divisionsalgebra ist, ist $F_6(\mathfrak{M}) = \{\mathfrak{o}, \mathfrak{p}\}$ für alle Q-Maximalordnungen $\mathfrak{M}$.

ii) Wenn $d \equiv 6 \bmod 9$, dann ist $\left(\frac{K}{\mathfrak{p}}\right) = -1$ und es gilt:

a) Wenn $Q \underset{k}{\cong} M_2(k) \underset{k}{\cong} (-3, -1)_k$, dann gibt es eine Q-Maximalordnung $\mathfrak{M}$ mit $F_6(\mathfrak{M}) = \{\mathfrak{p}\}$. Ist $\mathfrak{M}'$ eine weitere Q-Maximalordnung, so gilt:

$$F_6(\mathfrak{M}') = \begin{cases} \{\mathfrak{p}\}, \text{ wenn } N(\mathfrak{M}\mathfrak{M}') \in N(I^K)H^k \\ \{\mathfrak{o}\}, \text{ wenn } N(\mathfrak{M}\mathfrak{M}') \notin N(I^K)H^k \end{cases}$$

b) Wenn Q Divisionsalgebra ist, aber Q nicht an der Stelle $\mathfrak{p}$ verzweigt ist, dann ist $F_6(\mathfrak{M}) = \{\mathfrak{o}, \mathfrak{p}\}$ für alle Q-Maximalordnungen $\mathfrak{M}$.

c) Wenn Q an der Stelle $\mathfrak{p}$ verzweigt ist, ist $F_6(\mathfrak{M}) = \{\mathfrak{o}\}$ für alle Q-Maximalordnungen $\mathfrak{M}$.

Nach Lemma (20.9.i) ist $q = 1$. Für $\mathfrak{f} \in F_6(\mathfrak{M})$ wird also

$$l_6(\mathfrak{M}, \mathfrak{f}) = 2^{t-1}\left[I^k : RN(I^K)H^k\right] \cdot h(k_+) \cdot \frac{\left[\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{f}\times})\right]}{\left[\mathcal{O}^{\mathfrak{o}\times} : \mathcal{O}^{\mathfrak{f}\times}\right]} \cdot \mathfrak{N}(\mathfrak{f}) \cdot \prod_{\mathfrak{p}\mid\mathfrak{f}} \left(1 - \left(\frac{K}{\mathfrak{p}}\right)\mathfrak{N}(\mathfrak{p})^{-1}\right)$$

Wegen $q = 1$ ist $\mathcal{O}^{\mathfrak{o}\times} = Z\,\mathfrak{o}_+^\times$. Mit Lemma (20.11) folgt:

(20.26) Lemma: Sei $d \neq 3$ und $d \equiv 0 \bmod 3$. Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{o} \in F_6(\mathfrak{M})$. Dann gilt:

i) Wenn $Q \underset{k}{\cong} M_2(k)$, so ist $l_6(\mathfrak{M}, \mathfrak{o}) = x \cdot h(k_+)$.

ii) Wenn Q Divisionsalgebra ist, ist $l_6(\mathfrak{M}, \mathfrak{o}) = 2^{t-1} \cdot x \cdot h(k_+)$.

Wir müssen noch $l_6(\mathfrak{M}, \mathfrak{p})$ berechnen. Es ist $\mathfrak{N}(\mathfrak{p}) = 3$.

Wegen $\mathcal{O}^{\mathfrak{o}\times} = Z\,\mathfrak{o}_+^\times$ ist $\mathcal{O}^{\mathfrak{o}\times}$ das direkte Produkt der von ζ_6 und ε erzeugten Untergruppen. $\mathcal{O}^{\mathfrak{p}\times}$ enthält ζ_6.

Also wird $\left[\mathcal{O}^{\mathfrak{o}\times} : \mathcal{O}^{\mathfrak{p}\times}\right]$ der kleinste Exponent e, so daß $\varepsilon^e \in \mathcal{O}^{\mathfrak{p}\times}$.

Es ist $\varepsilon^e \in \mathcal{O}^{\mathfrak{p}\times}$ genau dann, wenn $D_k(1, \varepsilon^e)\mathfrak{o}$ Vielfaches von $D_k(\mathcal{O}^{\mathfrak{p}}) = 3\mathfrak{o}$ ist.

(20.27) Definition: i) Seien $a, b \in \mathbb{N}$ so, daß $\varepsilon = 1/2 \cdot (a + b \cdot \sqrt{d/3})$.

ii) Sei $y := \begin{cases} 2, \text{ wenn } b \equiv 0 \bmod 3 \\ 1, \text{ wenn } b \not\equiv 0 \bmod 3 \end{cases}$

Es ist $D_k(1,\varepsilon) = D_{\mathbb{Q}}(1,\varepsilon) = b^2 \cdot d/3$ (vgl. 6.9.iv).

Wegen $\varepsilon^2 = 1/4 \cdot (a^2 + b^2 \cdot d/3 + 2ab \cdot \sqrt{d/3})$

und $\varepsilon^4 = 1/16 \cdot (a^2 + b^2 \cdot d/3)^2 + 1/4 \cdot a^2 b^2 \cdot d/3 + 1/4 \cdot (a^2 + b^2 \cdot d/3) \cdot ab \cdot \sqrt{d/3}$

wird genauso: $D_k(1,\varepsilon^2) = a^2 b^2 \cdot d/3$ und $D_k(1,\varepsilon^4) = 1/4 \cdot (a^2 + b^2 d/3)^2 a^2 b^2 d/3$.

Wir betrachten zunächst den Fall $d \equiv 3 \bmod 9$ (also $d/3 \equiv 1 \bmod 3$):

Wegen $4N_{k_+|\mathbb{Q}}(\varepsilon) = a^2 - b^2 d/3 = \pm 4$ gilt:

Wenn $x = 1$, also $N(\varepsilon) = -1$, ist $a^2 - b^2 \equiv -1 \bmod 3$,
also notwendig $a \equiv 0 \bmod 3$ und $b \not\equiv 0 \bmod 3$.

Daher gilt: $D_k(1,\varepsilon^2)$ ist Vielfaches von 3, aber $D_k(1,\varepsilon)$ ist kein Vielfaches von 3 Also ist $[\mathcal{O}^{\mathcal{O}\times} : \mathcal{O}^{\mathfrak{P}\times}] = 2 = 2/x$.

Wegen $N(\varepsilon^2) = 1$ folgt: $[\sigma^{\times} : N(\mathcal{O}^{\mathfrak{P}\times})] = 2$.

Wenn $x = 2$, also $N(\varepsilon) = +1$, ist $a^2 - b^2 \equiv +1 \bmod 3$,
also notwendig $a \not\equiv 0 \bmod 3$ und $b \equiv 0 \bmod 3$.

Daher gilt: $D_k(1,\varepsilon)$ ist Vielfaches von 3, also ist $[\mathcal{O}^{\mathcal{O}\times} : \mathcal{O}^{\mathfrak{P}\times}] = 1 = 2/x$.

Wegen $N(\varepsilon) = 1$ ist $[\sigma^{\times} : N(\mathcal{O}^{\mathfrak{P}\times})] = 2$. Wir erhalten also:

(20.28) Lemma: Sei $d \neq 3$ und $d \equiv 3 \bmod 9$. Sei $3\sigma = \mathfrak{P}^2$ und sei $\mathfrak{M}$ eine $\mathbb{Q}$-Maximalordnung mit $\mathfrak{p} \in F_6(\mathfrak{M})$. Dann gilt:

i) Wenn $Q \underset{k}{\cong} M_2(k)$, so ist $l_6(\mathfrak{M},\mathfrak{p}) = 2x \cdot h(k_+)$.

ii) Wenn Q Divisionsalgebra ist, so ist $l_6(\mathfrak{M},\mathfrak{p}) = 2^t x \cdot h(k_+)$.

Wir betrachten jetzt den Fall $d \equiv 6 \bmod 9$, d.h. $d/3 \equiv 2 \bmod 3$.

Wieder ist $4N(\varepsilon) = a^2 - b^2 d/3 = \pm 4$.

Wenn $x = 1$, also $N(\varepsilon) = -1$, ist $a^2 + b^2 \equiv -1 \bmod 3$, also notwendig $a \not\equiv 0 \bmod 3$ und $b \not\equiv 0 \bmod 3$ und insbesondere $1 = y$ und $\varepsilon^2 \notin \mathcal{O}^{\mathfrak{P}\times}$.

Aber dann ist $D_k(1,\varepsilon^4) = 1/4 \cdot (a^2 + b^2 d/3)^2 a^2 b^2 \equiv 0 \bmod 3$,
also liegt ε^4 als früheste Potenz von ε in $\mathcal{O}^{\mathfrak{P}\times}$. Daher ist $[\mathcal{O}^{\mathcal{O}\times} : \mathcal{O}^{\mathfrak{P}\times}] = 4 = 4/xy$. Wegen $N(\varepsilon^4) = 1$ ist $[\sigma^{\times} : N(\mathcal{O}^{\mathfrak{P}\times})] = 2$.

Wenn $x = 2$, also $N(\varepsilon) = 1$, ist $a^2 + b^2 \equiv 1 \bmod 3$,
also notwendig entweder $a \equiv 0 \bmod 3$ und $b \not\equiv 0 \bmod 3$
oder $a \not\equiv 0 \bmod 3$ und $b \equiv 0 \bmod 3$.

Im ersten Fall ist $y = 1$ und ε^2 als früheste Potenz in $\mathcal{O}^{\mathfrak{P}\times}$,
also $[\mathcal{O}^{\mathcal{O}\times} : \mathcal{O}^{\mathfrak{P}\times}] = 2 = 4/xy$.

Im zweiten Fall ist $y = 2$ und $\varepsilon \in \mathcal{O}^{\mathfrak{P}\times}$, also $[\mathcal{O}^{\mathcal{O}\times} : \mathcal{O}^{\mathfrak{P}\times}] = 1 = 4/xy$.

Wegen $N(\varepsilon) = 1$ ist in beiden Fällen $[\sigma^{\times} : N(\mathcal{O}^{\mathfrak{P}\times})] = 2$.

(20.29) Lemma: Sei $d \equiv 6 \bmod 9$. Sei $3\mathfrak{o} = \mathfrak{p}^2$ und sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{p} \in F_6(\mathfrak{M})$. Dann gilt:

i) Wenn $Q \tilde{\underset{k}{}} M_2(k)$, so ist $l_6(\mathfrak{M}, \mathfrak{p}) = 2xy \cdot h(k_+)$.

ii) Wenn Q Divisionsalgebra ist, so ist $l_6(\mathfrak{M}, \mathfrak{p}) = 2^t xy \cdot h(k_+)$.

Wir wollen jetzt $F_6^*(\mathfrak{M})$ und $l_6^*(\mathfrak{M}, \mathfrak{f})$ berechnen.
Dazu machen wir die Zusatzvoraussetzung: $Q \tilde{\underset{k}{}} (-3, -1)_k$.

Ist $\mathfrak{M}$ eine Q-Maximalordnung und $\mathfrak{f} \in F_6^*(\mathfrak{M})$, so ist nach (18.9.i) notwendig $\mathfrak{f}^2 D_k(K) \mid 3\mathfrak{o}$ und $t(\mathfrak{p}) \equiv 0 \bmod 2$ für alle Primteiler $\mathfrak{p}$ von $\mathfrak{f}$. Ist $\mathfrak{p}$ Primteiler von $\mathfrak{f}$ (Widerspruchsannahme), so gilt $\mathfrak{p} \mid 3\mathfrak{o}$ und $\mathfrak{p}$ ist träge über $\mathbb{Q}$. Dann ist notwendig $d \equiv 1 \bmod 3$, also $D_k(K) = 3\mathfrak{o}$. ↯
Wir haben also in jedem Falle $F_6^*(\mathfrak{M}) \subset \{\mathfrak{o}\}$.

Ist $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{o} \in F_6^*(\mathfrak{M})$, so ist

$$l_6^*(\mathfrak{M}) = l_6^*(\mathfrak{M}, \mathfrak{o}) = 2^e \cdot \left[I^k : I^{k(2)} H^k\right] \Big/ \left(\kappa \cdot \left[N(A^{\mathfrak{o}}) H^k : I^{k(2)} H^k\right]\right),$$

wobei e die Zahl der (endlichen) Verzweigungsstellen von K über k ist.

(20.30) Lemma: $\left[I^k : I^{k(2)} H^k\right] = 2^{\delta - 1}$.

Bew.: siehe /1/ S. 267 Satz 8

Ist $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{o} \in F_6^*(\mathfrak{M})$ und ist $\mathfrak{M}'$ eine weitere Q-Maximalordnung, so ist nach Satz (18.16) $\mathfrak{o} \in F_6^*(\mathfrak{M}')$ genau dann, wenn $N(\mathfrak{M}\mathfrak{M}') \in N(A^{\mathfrak{o}}) H^k$.
Es gibt also (vgl. 10.10) $\left[N(A^{\mathfrak{o}}) H^k : RI^{k(2)} H^k\right]$ verschiedene Maximalordnungstypen $\tilde{\mathfrak{M}}$ mit $F_6^*(\mathfrak{M}) = \{\mathfrak{o}\}$. Für alle anderen Maximalordnungstypen $\tilde{\mathfrak{M}}'$ ist $F_6^*(\mathfrak{M}') = \emptyset$.

Wir machen jetzt wieder Fallunterscheidungen.

Sei zuerst $d = 3$. Dann ist K kein Körper, also $\kappa = 1$.
K ist unverzweigt über k, also $e = 0$. Wegen $\left[I^k : H^k\right] = 1$ sind alle vorkommenden Idealgruppenindizes gleich 1. Also gilt:

(20.31) Lemma: Wenn $d = 3$, ist $Q \tilde{\underset{k}{}} M_2(k)$. Ist $\mathfrak{M}$ eine Q-Maximalordnung, so gilt $F_6^*(\mathfrak{M}) = \{\mathfrak{o}\}$ und $l_6^*(\mathfrak{M}) = l_6^*(\mathfrak{M}, \mathfrak{o}) = 1$.

Sei jetzt $d \equiv 2 \bmod 3$. Nach Satz (14.8.iv) ist $3\mathfrak{o} = \mathfrak{p}\mathfrak{q}$ mit Primidealen $\mathfrak{p}$, $\mathfrak{q}$ und $(-3, -1)_k$ ist über k genau an den Stellen $\mathfrak{p}$ und $\mathfrak{q}$ verzweigt. Auch K ist über k genau an den Stellen $\mathfrak{p}$ und $\mathfrak{q}$ verzweigt. Also ist $e = 2$ und $N(A^{\mathfrak{o}}) = RI^{k(2)}$. Daher gilt:

(20.32) Lemma: Wenn $d \equiv 2 \bmod 3$, gibt es genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $F_6^*(\mathfrak{M}) = \{\sigma\}$. (Für alle anderen Maximalordnungstypen $\widetilde{\mathfrak{M}}$ ist $F_6^*(\mathfrak{M}) = \emptyset$.)

$N(A^\sigma)H^k$ wird von den Idealen aus $I^{k(2)}H^k$ und von $\mathfrak{p}$ erzeugt. ($\sigma\mathfrak{p} = 3\mathfrak{p}^{-1}$ liegt auch in dieser Gruppe) Da $\mathfrak{p}^2 \in I^{k(2)}H^k$, ist $[N(A^\sigma)H^k : I^{k(2)}H^k] = 1$ oder $= 2$ je nachdem ob $\mathfrak{p} \in I^{k(2)}H^k$ oder $\mathfrak{p} \notin I^{k(2)}H^k$.

(20.33) Lemma: Sei k imaginärquadratischer Zahlkörper und $\mathfrak{a} \in I^k$. Genau dann ist $\mathfrak{a} \in I^{k(2)}H^k$, wenn es $a \in k^\times$ gibt mit $N_{k|\mathbb{Q}}(\mathfrak{a}) = N_{k|\mathbb{Q}}(a)\mathbb{Z}$.

Bew.: siehe /1/ S. 266 Sätze 6 und 7

Es ist also $\mathfrak{p} \in I^{k(2)}H^k$ genau dann, wenn es $a \in k^\times$ gibt mit $3\mathbb{Z} = N_{k|\mathbb{Q}}(\mathfrak{p}) = N_{k|\mathbb{Q}}(a)\mathbb{Z}$. Da $N_{k|\mathbb{Q}}(a) \geq 0$ für alle $a \in k$, ist dies gleichbedeutend damit, daß es $a, b \in \mathbb{Q}$ gibt mit
$3 = N_{k|\mathbb{Q}}(a + bi\sqrt{d}) = a^2 + b^2 d$, also $3d = 9/b^2 - 3a^2/b^2$.
Dies ist äquivalent zu $3d \in N_{\mathbb{Q}(\sqrt{3})|\mathbb{Q}}(\mathbb{Q}(\sqrt{3}))$.

(20.34) Lemma: Sei $d \equiv 2 \bmod 3$. Genau dann ist $3d \in \text{Bild } N_{\mathbb{Q}(\sqrt{3})|\mathbb{Q}} =: M$, wenn $\left(\frac{3}{p}\right) = 1$ für alle Primteiler $p \neq 2$ von d.

Bew.: Wegen $-3 = 0^2 - 3\cdot 1^2 \in M$ ist $3d \in M$ genau dann, wenn $-d \in M$.
i) Sei $-d \in M$. Da $\mathbb{Q}(\sqrt{3})$ Klassenzahl 1 hat, ist dann $\pm p \in M$ für alle Primteiler $p \neq 2$ von d. Es folgt sofort $\left(\frac{3}{p}\right) = 1$.
ii) Sei umgekehrt $\left(\frac{3}{p}\right) = 1$ für alle Primteiler $p \neq 2$ von d. (Wegen 20.14 also $p \equiv \pm 1 \bmod 12$)
Sei p ein Primteiler von d. Dann gibt es also $a, b \in \mathbb{Z}$ mit
$\pm p = a^2 - 3b^2 \in M$. Wir untersuchen die Gleichung mod 4:
Wenn $p \equiv 1 \bmod 12$, ist $-p \notin M$, also $p \in M$.
Wenn $p \equiv -1 \bmod 12$, ist $p \notin M$, also $-p \in M$.
Wenn $p = 2$, ist $-p = -2 = 1^2 - 3\cdot 1^2 \in M$
Sei λ die Zahl der Primteiler p von d mit $p \equiv 2 \bmod 3$.
Dann folgt (mit Multiplikation) sofort: $(-1)^\lambda d \in M$.
Da $d \equiv 2 \bmod 3$, ist λ ungerade, also $-d \in M$.

(20.35) Definition: Für $d \equiv 2 \bmod 3$ sei

$$w := \begin{cases} 2, & \text{wenn für alle Primteiler } p \neq 2 \text{ von } d \text{ gilt: } p \equiv \pm 1 \bmod 12 \\ 1, & \text{wenn } d \text{ einen Primteiler } p \equiv \pm 5 \bmod 12 \text{ hat} \end{cases}$$

Bemerkung: Wegen (20.13.ii) ist w immer Vielfaches von z.

Nach unseren Überlegungen ist $\gamma \in I^{k(2)}H^k$ genau dann, wenn $w = 2$. Es ist also $\left[N(A^\sigma)H^k : I^{k(2)}H^k\right] = 2/w$. Daher gilt:

(20.36) Lemma: Sei $d \equiv 2 \bmod 3$. Dann ist $\# \widetilde{Q} = \left[I^k : RI^{k(2)}H^k\right] = 2^{\delta-2}w$. Ist $\mathfrak{M}$ eine Q-Maximalordnung mit $F_6^*(\mathfrak{M}) = \{\sigma\}$, so ist $1_6^*(\mathfrak{M}) = 1_6^*(\mathfrak{M}, \sigma) = 2^{\delta-1}w$.

Sei jetzt $d \equiv 1 \bmod 3$. Nach (14.8.iii) ist Q unverzweigt über k. Die einzige Verzweigungsstelle von K über k ist das Hauptideal 3σ. Daher ist $e = 1$ und $N(A^\sigma)H^k = RI^{k(2)}H^k = I^{k(2)}H^k$.

(20.37) Lemma: Sei $d \equiv 1 \bmod 3$. Es ist $\# \widetilde{Q} = 2^{\delta-1}$. Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$ mit $F_6^*(\mathfrak{M}) = \{\sigma\}$. Dann ist $1_6^*(\mathfrak{M}) = 1_6^*(\mathfrak{M}, \sigma) = 2^{\delta-1}$.

Sei jetzt $d \neq 3$ und $d \equiv 0 \bmod 3$. Dann sind Q und K unverzweigt über k, also $e = 0$ und $N(A^\sigma)H^k = RI^{k(2)}H^k = I^{k(2)}H^k$.

(20.38) Lemma: Sei $d \equiv 0 \bmod 3$ und $d \neq 3$. Es ist $\# \widetilde{Q} = 2^{\delta-1}$. Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$ mit $F_6^*(\mathfrak{M}) = \{\sigma\}$. Dann ist $1_6^*(\mathfrak{M}) = 1_6^*(\mathfrak{M}, \sigma) = 2^{\delta-2}$.

Wir haben jetzt das Material gesammelt, um λ_6 und λ_6^* zu berechnen (vgl. 18.26). Wir fassen zusammen:

(20.39) Satz: Sei $d \in \mathbb{N}$ quadratfrei, sei $k = \mathbb{Q}(i\sqrt{d})$ und sei $Q = (-3, -1)_k$.

i) Wenn $d \equiv 2 \bmod 3$, ist Q an den beiden Primteilern von 3 in k verzweigt. Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $\lambda_6^*(\mathfrak{M}) = 2^{\delta-1}w$ und $\lambda_6'(\mathfrak{M}) = 1/2 \cdot \left(z \cdot h(k_+) - 2^{\delta-1}w\right)$.
Ist $\widetilde{\mathfrak{M}}'$ einer der anderen $2^{\delta-1}w - 1$ Maximalordnungstypen, dann ist $\lambda_6^*(\mathfrak{M}') = 0$ und $\lambda_6'(\mathfrak{M}') = z/2 \cdot h(k_+)$.

ii) Wenn $d \equiv 1 \bmod 3$, ist $Q \underset{k}{\simeq} M_2(k)$. Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $\lambda_6^*(\mathfrak{M}) = 2^{\delta-1}$ und $\lambda_6'(\mathfrak{M}) = 1/2 \cdot \left(h(k_+) - 2^{\delta-1}\right)$.
Ist $\widetilde{\mathfrak{M}}'$ einer der anderen $2^{\delta-1}$ Maximalordnungstypen von Q, dann ist $\lambda_6^*(\mathfrak{M}') = 0$ und $\lambda_6'(\mathfrak{M}') = 1/2 \cdot h(k_+)$.

iii) Wenn $d \equiv 3 \bmod 9$, aber $d \neq 3$, ist $Q \underset{k}{\cong} M_2(k)$.
Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $\lambda_6^*(\mathfrak{M}) = 2^{\delta-2}$ und $\lambda_6'(\mathfrak{M}) = 1/2 \cdot \left(3x \cdot h(k_+) - 2^{\delta-2}\right)$.
Es gibt $2^{\delta-2} - 1$ Maximalordnungstypen $\widetilde{\mathfrak{M}'}$, so daß $\lambda_6^*(\mathfrak{M}') = 0$ und $\lambda_6'(\mathfrak{M}') = 3x/2 \cdot h(k_+)$; und zwar sind das die Maximalordnungstypen mit $N(\mathfrak{M}\ \mathfrak{M}') \in N(I^K)H^k$, aber $\widetilde{\mathfrak{M}'} \neq \widetilde{\mathfrak{M}}$.
Für die restlichen $2^{\delta-2}$ Maximalordnungstypen $\widetilde{\mathfrak{M}''}$ ist $\lambda_6^*(\mathfrak{M}'') = \lambda_6'(\mathfrak{M}'') = 0$.

iv) Wenn $d \equiv 6 \bmod 9$, ist $Q \underset{k}{\cong} M_2(k)$.
Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $\lambda_6^*(\mathfrak{M}) = 2^{\delta-2}$ und $\lambda_6'(\mathfrak{M}) = 1/2 \cdot \left(x \cdot h(k_+) - 2^{\delta-2}\right)$
Es gibt $2^{\delta-2} - 1$ Maximalordnungstpyen $\widetilde{\mathfrak{M}'}$, so daß $\lambda_6^*(\mathfrak{M}') = 0$ und $\lambda_6'(\mathfrak{M}') = x/2 \cdot h(k_+)$; und zwar sind das die Maximalordnungstypen mit $N(\mathfrak{M}\ \mathfrak{M}') \in N(I^K)H^k$, aber $\widetilde{\mathfrak{M}'} \neq \widetilde{\mathfrak{M}}$.
Für die restlichen $2^{\delta-2}$ Maximalordnungstypen $\widetilde{\mathfrak{M}''}$ ist $\lambda_6^*(\mathfrak{M}'') = 0$ und $\lambda_6'(\mathfrak{M}'') = xy \cdot h(k_+)$.

v) Wenn $d = 3$, ist $Q \underset{k}{\cong} M_2(k)$.
In Q gibt es genau einen Maximalordnungstyp.
Für jede Q-Maximalordnung $\mathfrak{M}$ ist $\lambda_6^*(\mathfrak{M}) = \lambda_6'(\mathfrak{M}) = 1$.

Zur besseren Übersicht tabellieren wir die Klassenzahlen sowie F_6 und F_6^*. In der Spalte $\neq$ steht die Zahl der Maximalordnungstypen, für die die nebenstehenden Werte zutreffen. Die Maximalordnungstypen sind in der gleichen Reihenfolge aufgeführt wie in (20.39).
μ_3 bezeichnet die Konjugationsklassenzahlen von 3-Diedergruppen.
Sie sind schon im Vorgriff auf (22.14) eingetragen.

(20.40) Tabellarische Übersicht zu (20.39)

d	##	F_6	F_6^*	μ_3	λ_6^*	λ_6'
$d \equiv 2 \bmod 3$	1	$\mathfrak{o}$	$\mathfrak{o}$	$2^{\delta}w$	$2^{\delta-1}w$	$1/2 \cdot (z \cdot h(k_+) - 2^{\delta-1}w)$
	$2^{\delta-1}w - 1$	$\mathfrak{o}$	$\emptyset$	0	0	$1/2 \cdot z \cdot h(k_+)$
$d \equiv 1 \bmod 3$	1	$\mathfrak{o}$	$\mathfrak{o}$	2^{δ}	$2^{\delta-1}$	$1/2 \cdot (h(k_+) - 2^{\delta-1})$
	$2^{\delta-1} - 1$	$\mathfrak{o}$	$\emptyset$	0	0	$1/2 \cdot h(k_+)$
$d \equiv 3 \bmod 9$ und $d \neq 3$	1	$\mathfrak{o}, \mathfrak{p}$	$\mathfrak{o}$	$2^{\delta-1}$	$2^{\delta-2}$	$1/2 \cdot (3x \cdot h(k_+) - 2^{\delta-2})$
	$2^{\delta-2} - 1$	$\mathfrak{o}, \mathfrak{p}$	$\emptyset$	0	0	$1/2 \cdot 3x \cdot h(k_+)$
	$2^{\delta-2}$	$\emptyset$	$\emptyset$	0	0	0
$d \equiv 6 \bmod 9$	1	$\mathfrak{o}$	$\mathfrak{o}$	$2^{\delta-1}$	$2^{\delta-2}$	$1/2 \cdot (x \cdot h(k_+) - 2^{\delta-2})$
	$2^{\delta-2} - 1$	$\mathfrak{o}$	$\emptyset$	0	0	$1/2 \cdot x \cdot h(k_+)$
	$2^{\delta-2}$	$\mathfrak{p}$	$\emptyset$	0	0	$xy \cdot h(k_+)$
$d = 3$	1	$\mathfrak{o}, \mathfrak{p}$	$\mathfrak{o}$	1	1	1

(20.41) Satz: Sei $d \in \mathbb{N}$ quadratfrei; sei $k = \mathbb{Q}(i\sqrt{d})$.
Sei Q eine k-Quaternionenalgebra. Sei $Q \not\cong_K (-3, -1)_k$, aber alle Verzweigungsstellen von Q über k seien in K verzweigt oder träge, d.h. die Bedingungen aus Satz (14.6) seien erfüllt.
Dann ist $\lambda_6 = \lambda_6'$ konstant auf der Menge aller Q-Maximalordnungen.
Sei $\mathfrak{M}$ eine Q-Maximalordnung, dann gilt:

i) Wenn $d \equiv 2 \bmod 3$, ist $\lambda_6'(\mathfrak{M}) = 2^{t-1}z \cdot h(k_+)$.

ii) Wenn $d \equiv 1 \bmod 3$, ist $\lambda_6'(\mathfrak{M}) = 2^{t-1} \cdot h(k_+)$.

iii) Wenn $d \equiv 3 \bmod 9$, aber $d \neq 3$, ist $\lambda_6'(\mathfrak{M}) = 2^{t-2} \cdot 3x \cdot h(k_+)$.

iv) Wenn $d \equiv 6 \bmod 9$ und Q am Primteiler von 3 in k verzweigt ist, ist $\lambda_6'(\mathfrak{M}) = 2^{t-2} \cdot x \cdot h(k_+)$.

v) Wenn $d \equiv 6 \bmod 9$ und Q nicht am Primteiler von 3 in k verzweigt ist, ist $\lambda_6'(\mathfrak{M}) = 2^{t-2} \cdot x(1+2y) \cdot h(k_+)$.

vi) Für $d = 3$ ist die Voraussetzung des Satzes nicht erfüllbar.

Zeichenerklärung zu 20.39 - 20.41

δ ist die Zahl der endlichen Verzweigungsstellen von k über $\mathbb{Q}$.

$K := k[X]/(X^2-X+1)k[X]$.

Für $d \neq 3$ ist $k_+ = \mathbb{Q}(\sqrt{3d})$.

$h(k_+)$ ist die Idealklassenzahl von k_+.

$\mathfrak{o}$ ist die Hauptordnung von k.

Falls $d \equiv 0 \bmod 3$, ist $\mathfrak{p}$ das Primideal mit $3\mathfrak{o} = \mathfrak{p}^2$.

Falls $d \equiv 2 \bmod 3$, ist

$$w = \begin{cases} 2, & \text{wenn für alle Primteiler } p \neq 2 \text{ von } d \text{ gilt: } p \equiv \pm 1 \bmod 12. \\ 1, & \text{wenn } d \text{ einen Primteiler } p \equiv \pm 5 \bmod 12 \text{ hat.} \end{cases}$$

und $$z = \begin{cases} 2, & \text{wenn } +3 \text{ Norm einer ganzen Zahl aus } k_+ \text{ ist.} \\ 1, & \text{sonst.} \end{cases}$$

Falls $d \equiv 0 \bmod 3$, aber $d \neq 3$, ist $\varepsilon = 1/2 \cdot (a + b\sqrt{d/3}) > 1$ die Grundeinheit von k_+ $(a, b \in \mathbb{N})$. Dann ist

$$x = \begin{cases} 2, & \text{wenn } N_{k_+|\mathbb{Q}}(\varepsilon) = +1 \\ 1, & \text{wenn } N_{k_+|\mathbb{Q}}(\varepsilon) = -1 \end{cases}$$

und $$y = \begin{cases} 2, & \text{wenn } b \equiv 0 \bmod 3 \\ 1, & \text{wenn } b \not\equiv 0 \bmod 3 \end{cases}$$

(N bezeichnet immer die Norm von Idealen oder Zahlen aus Q oder K bzgl. k)

t ist die Zahl der Verzweigungsstellen von Q über k, die in K träge sind.

Erläuterungen zur Tabelle 20.42:

Wir wollen die Ergebnisse für $1 < d < 101$ und die Quaternionenalgebra $Q = M_2(k)$ tabellieren.

Dabei sei ## jeweils die Anzahl der verschiedenen Maximalordnungstypen, für die die nebenstehenden Werte gelten. Für jedes d sind die Maximalordnungstypen (falls notwendig) in derselben Reihenfolge wie in Satz (20.39) aufgeführt. Für $d \equiv 6 \bmod 9$ ist der besseren Übersicht wegen noch vermerkt, ob $F_6(\mathfrak{M}) = \{\mathfrak{o}\}$ oder $F_6(\mathfrak{M}) = \{\mathfrak{p}\}$. Dabei bezeichnet $\mathfrak{p}$ den Primteiler von $3\mathbb{Z}$ in k.

Es sind keine Nullen eingetragen. Die entsprechenden Felder sind stattdessen freigelassen.

Bei der Erstellung der Tabelle habe ich mit den Tabellen in /1/ gearbeitet. Alle notwendigen Werte außer z (für $d \equiv 2 \bmod 3$) lassen sich so ohne große Mühe bestimmen. Da aber $z = 2$ nur für $w = 2$ in Frage kommt, brauchen wir zur Bestimmung von z nur die $d \equiv 2 \bmod 3$ mit $w = 2$ untersuchen. Es ist $w = 2$ genau für $d = 2,11,23,26,47,59,71,74,83$. Außer für $d = 26$ und 74 ist $h(k_+) = 1$ (siehe die Tabellen in /1/). Also ist dann notwendig $z = 2$ (siehe 20.13). Aber auch für $d = 26$ und $d = 74$ ist $z = 2$ wegen $3 = 9^2 - 3 \cdot 26 \cdot 1^2$ und $3 = 15^2 - 3 \cdot 74 \cdot 1^2$.

Das x in der letzten Spalte zeigt, welche Klassenzahlen $\lambda_6^*(\mathfrak{M})$ und $\lambda_6'(\mathfrak{M})$ die Maximalordnung $\mathfrak{M} = \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{o} \end{pmatrix}$ hat, wobei $\mathfrak{o}$ die Hauptordnung von K ist (siehe Anhang zu dieser Arbeit).

(20.42) Tabelle der Konjugationsklassenzahlen $\lambda_6^* = \lambda_6^*(\mathfrak{M})$ und $\lambda_6' = \lambda_6'(\mathfrak{M})$ für $Q = M_2(k)$, wo $k = \mathbb{Q}(i\sqrt{d})$ für $1 \le d \le 101$ quadratfrei.

d	##	F_6	λ_6^*	λ_6'	
1	1		1		x
2	1			1	x
3	1		1	1	x
5	2			1	x
6	1	$\mathfrak{o}$	1		
	1	$\mathfrak{p}$		1	x
7	1		1		x
10	1		2		
	1			1	x
11	1			1	x
13	1		2		x
	1			1	
14	2			1	x
15	1	$\mathfrak{o}$	1		
	1	$\mathfrak{p}$		1	x
17	2			1	x
19	1		1		x
21	1		2	2	x
	1			3	
	2				
22	1		2		
	1			1	x
23	1			1	x
26	2			2	x
29	2			1	x
30	1		2	2	
	1			3	x
	2				
31	1		1		x
33	1	$\mathfrak{o}$	2		
	1	$\mathfrak{o}$		1	
	2	$\mathfrak{p}$		4	x
34	1		2		
	1			1	x

d	##	F_6	λ_6^*	λ_6'	
35	2			1	x
37	1		2		x
	1			1	
38	2			1	x
39	1		1	1	x
	1				
41	2			1	x
42	1	$\mathfrak{o}$	2		
	1	$\mathfrak{o}$		1	
	2	$\mathfrak{p}$		2	x
43	1		1		x
46	1		2		
	1			1	x
47	1			1	x
51	1	$\mathfrak{o}$	1		
	1	$\mathfrak{p}$		1	x
53	2			1	x
55	1		2		
	1			1	x
57	1		2	2	x
	1			3	
	2				
58	1		2		
	1			1	x
59	1			1	x
61	1		2		x
	1			1	
62	2			1	x
65	4			2	x
66	1		2	2	
	1			3	x
	2				
67	1		1		x

d	##	F_6	λ_6^*	λ_6'	
69	1	$\mathfrak{o}$	2		
	1	$\mathfrak{o}$		1	
	2	$\mathfrak{p}$		2	x
70	1		4		
	3			2	x
71	1			1	x
73	1		2	1	x
	1			2	
74	2			2	x
77	4			2	x
78	1	$\mathfrak{o}$	2		
	1	$\mathfrak{o}$		1	
	2	$\mathfrak{p}$		2	x
79	1		1		x
82	1		2		
	1			1	x
83	1			1	x
85	1		4		
	3			2	x
86	2			1	x
87	1	$\mathfrak{o}$	1		
	1	$\mathfrak{p}$		1	x
89	2			1	x
91	1		2		x
	1			1	
93	1		2	2	x
	1			3	
	2				
94	1		2		
	1			1	x
95	2			1	x
97	1		2	1	x
	1			2	
101	2			1	x

§ 21 . Beispiel: Zyklische Gruppen der Ordnung 4 in Quaternionenalgebren über imaginärquadratischen Zahlkörpern

Wir haben in § 20 die 6-zyklischen Gruppen untersucht.
Entsprechend untersuchen wir in § 21 die 4-zyklischen Gruppen.
Eine Zusammenfassung der Ergebnisse und tabellarische Übersicht, die (20.39 - 20.42) entspricht, verschieben wir aber auf § 26 (siehe 26.12 - 26.17), da wir dann auch die Klassenzahlen für 2-Dieder- und Tetraedergruppen berechnen können.

Achtung: In § 21 definieren wir K, k_+, q, w, z, x, y, ε, a, b, t und $\mathfrak{p}$ neu, d.h. anders als in § 20! (Vgl. dazu die Zeichenerklärungen zu 20.39 - 20.41 bzw. zu 26.12 - 26.14)

Wir machen für diesen Paragrafen folgende Generalvoraussetzung:
(21.1) Sei $d \in \mathbb{N}$ quadratfrei, sei $k = \mathbb{Q}(i\sqrt{d})$, sei $\mathfrak{o}$ die Hauptordnung von k. Sei Q eine k-Quaternionenalgebra. Alle Primteiler von $D_k(Q)$ seien verzweigt oder träge in $K := k[X]/(X^2+1)k[X]$, d.h. die Bedingungen von Satz (14.5) seien erfüllt, $\Gamma(Q)$ enthalte 4-zyklische Untergruppen.

Wie in § 20 wird $\mathfrak{a}^\times = \mathfrak{o}^\times$ und $S_{\mathfrak{a}} = H^k$.
Wir müssen $F_4(\mathfrak{M})$ und $F_4^*(\mathfrak{M})$ für die verschiedenen Maximalordnungen berechnen. Für $\mathfrak{f} \in F_4(\mathfrak{M})$ bzw. $\mathfrak{f} \in F_4^*(\mathfrak{M})$ gilt (20.2) entsprechend.

Wir berechnen zuerst $F_4(\mathfrak{M})$ und $l_4(\mathfrak{M}, \mathfrak{f})$.

Sei zuerst $d = 1$. Dann ist notwendig $Q \underset{k}{\cong} M_2(k)$ (siehe 14.5).
Bekanntlich ist hier $[I^k : H^k] = 1$, also auch $[I^k : I^{k(2)}H^k] = 1$.
Es gibt also nur einen Maximalordnungstyp in Q (siehe 10.13).
Q hat keine Verzweigungsstellen über k, insbesondere ist $D_k(Q) = \mathfrak{o}$ und $t = 0$.
K ist kein Körper, da $\zeta_4 = i \in k$. Insbesondere ist $D_k(K) = \mathfrak{o}$ und $[I^k : RN(I^K)H^k] = 1$.
Ist $\mathfrak{M}$ eine Q-Maximalordnung, so folgt mit (16.5):
$F_4(\mathfrak{M}) = \{ \mathfrak{f} \mid \mathfrak{f}$ ist ganzes $\mathfrak{o}$-Ideal und $\mathfrak{f}^2 | 4\mathfrak{o} \}$.
2 ist verzweigt in k. Sei $2\mathfrak{o} = \mathfrak{p}^2$, also $\mathfrak{p} = (1+i)\mathfrak{o}$.
Dann ist also $F_4(\mathfrak{M}) = \{ \mathfrak{o}, \mathfrak{p}, 2\mathfrak{o} \}$.

Nach (7.26.i) ist $[I^K : H^K] = [I^k : H^k]^2 = 1$.
Wie im Bew. von (19.3) gesehen, ist $\sigma^\times = N(\mathcal{O}^{\sigma\times})$. Also ist $l_4(\mathfrak{M}, \sigma) = 1$.

Es gibt K-Idempotente e_1, e_2 mit $K = ke_1 \oplus ke_2$ und $\mathcal{O}^\sigma = \sigma e_1 + \sigma e_2$.
Aus $\mathcal{O}^\mathfrak{p} = \sigma + \mathfrak{p}\mathcal{O}^\sigma$ folgt leicht: $\mathcal{O}^\mathfrak{p} = \{ae_1+be_2 \mid a,b \in \sigma \text{ und } a-b \in \mathfrak{p}\}$.
i ist erzeugendes Element von $\sigma^\times$ und man sieht leicht, daß $i = ie_1+ie_2$ und $E := e_1+ie_2$ erzeugende Elemente von $\mathcal{O}^{\sigma\times}$ sind.

Da $1-i \in \mathfrak{p}$, ist $\mathcal{O}^{\sigma\times} = \mathcal{O}^{\mathfrak{p}\times}$ und $\sigma^\times = N(\mathcal{O}^{\mathfrak{p}\times})$.
Da $\mathfrak{p}$ über $\mathbb{Q}$ verzweigt ist, ist $\pi(\mathfrak{p}) = 2$.
Außerdem ist $\left(\frac{K}{\mathfrak{p}}\right) = 1$ (siehe 5.2.iii). Also ist $l_4(\mathfrak{M}, \mathfrak{p}) = 1$.
Es ist $\mathcal{O}^{2\sigma} = \{ae_1+be_2 \mid a,b \in \sigma \text{ und } a-b \in 2\sigma\}$. Es ist $i \notin \mathcal{O}^{2\sigma\times}$.
Aber wegen $1-i \notin 2\sigma$ ist $E \notin \mathcal{O}^{2\sigma\times}$. Da $E^2 = e_1-e_2 \in \mathcal{O}^{2\sigma\times}$,
ist $[\mathcal{O}^{\sigma\times} : \mathcal{O}^{2\sigma\times}] = 2$. Wegen $N(i) = N(E^2) = -1$ ist $[\sigma^\times : N(\mathcal{O}^{2\sigma\times})] = 2$.
Mit $\pi(2\sigma) = 4$ ergibt sich also: $l_4(\mathfrak{M}, 2\sigma) = 2$

(21.2) Lemma: (Voraussetzung 21.1). Wenn $d = 1$, ist notwendig $Q \underset{k}{\cong} M_2(k)$.
Alle Q-Maximalordnungen sind vom gleichen Typ.
Ist $\mathfrak{M}$ eine Q-Maximalordnung, so ist $F_4(\mathfrak{M}) = \{\sigma, \mathfrak{p}, 2\sigma\}$ und
$l_4(\mathfrak{M}, \sigma) = l_4(\mathfrak{M}, \mathfrak{p}) = 1$ sowie $l_4(\mathfrak{M}, 2\sigma) = 2$, also $l_4(\mathfrak{M}) = 4$.
(Dabei ist $\mathfrak{p} = (1+i)\sigma$ der Primteiler von $2\mathbb{Z}$ in σ)

Sei von jetzt an $d \neq 1$. Dann ist K Körper und wir können identifizieren: $K = k(i)$. Nach Lemma (14.4) sind in K über k höchstens die Primteiler von 2 verzweigt, da 2 die einzige endliche Verzweigungsstelle von $\mathbb{Q}(i)$ über $\mathbb{Q}$ ist.

(21.3) Lemma: Sei $d \neq 1$. Dann ist

$$D_K(K) = \begin{cases} \sigma, & \text{wenn } d \equiv 1 \bmod 4 \\ 2\sigma, & \text{wenn } d \equiv 2 \bmod 4 \\ 4\sigma, & \text{wenn } d \equiv 3 \bmod 4 \end{cases}$$

Bew.: Falls $d \equiv 1 \bmod 4$, ist 2 in $\mathbb{Q}(\sqrt{d})$ unverzweigt, nach Lemma (14.4) ist K über k unverzweigt.
Falls $d \equiv 3 \bmod 8$, ist 2 in k träge, also 2σ Primideal.
2σ ist verzweigt in K, also gilt: $2\sigma \mid D_k(K)$. Andererseits ist
$D_k(K) f(\sigma[i])^2 = D_k(\sigma[i]) = 4\sigma$. Also ist notwendig $f(\sigma[i]) = \sigma$ und $D_k(K) = 4\sigma$.

Falls $d \equiv 7 \bmod 8$, ist 2 zerlegt in k. Jetzt führt eine ähnliche Betrachtung für die beiden Primteiler von 2σ zum Erfolg.

Falls $d \equiv 2 \bmod 4$, ist 2 in k verzweigt, $2\mathfrak{o} = \mathfrak{p}^2$ mit einem Primideal $\mathfrak{p}$ aus k. $\mathfrak{p}$ ist verzweigt in K, also $\mathfrak{p} \mid D_k(K)$.

Wegen $D_k(K) \cdot f(\mathfrak{o}[i])^2 = 4\mathfrak{o}$ sind nur die beiden folgenden Fälle möglich:

i) $f(\mathfrak{o}[i]) = \mathfrak{p}$ und $D_k(K) = 2\mathfrak{o}$ oder

ii) $f(\mathfrak{o}[i]) = \mathfrak{o}$ und $D_k(K) = 4\mathfrak{o}$.

Wenn ii) gelten würde, wäre $\mathfrak{o}[i] = \mathfrak{O}^{\mathfrak{o}}$, also wäre $\{1,i\}$ eine Basis von $\mathfrak{O}^{\mathfrak{o}}$ über $\mathfrak{o}$ und eine Basis von $\mathfrak{O}_{\mathfrak{p}}^{\mathfrak{o}}$ über $\mathfrak{o}_{\mathfrak{p}}$.

Sei π ein Primelement von $\mathfrak{o}_{\mathfrak{p}}$. Dann ist $S(\pi^{-1}(1+i)) = \pi^{-1} \cdot 2 \in \mathfrak{o}_{\mathfrak{p}}$ und $N(\pi^{-1}(1+i)) = \pi^{-2} \cdot 2 \in \mathfrak{o}_{\mathfrak{p}}^{\times}$, also $\pi^{-1} + \pi^{-1} i \in \mathfrak{O}_{\mathfrak{p}}^{\mathfrak{o}\times}$. ↯

(21.4) Lemma: Es ist $[I^k : RN(I^K)I^k] = 2$ genau dann, wenn $d \neq 1$, $d \equiv 1 \bmod 4$ und $Q \underset{k}{\simeq} M_2(k)$.

Bew.: siehe (16.9). Genau in diesem Fall ist $i \notin k$, $D_k(K) = \mathfrak{o}$ und $Q \underset{k}{\simeq} (-1,-1)_k$.

(21.5) Definition: Sei $d \neq 1$.

i) Sei $k_+ := \mathbb{Q}(\sqrt{d})$ und $\mathfrak{o}_+$ die Hauptordnung von k_+.

ii) Sei $\varepsilon > 1$ die Grundeinheit von k_+.

iii) Sei Z die Gruppe der Einheitswurzeln aus $\mathfrak{O}^{\mathfrak{o}\times}$.

iv) Sei $q := [\mathfrak{O}^{\mathfrak{o}\times} : Z\,\mathfrak{o}_+^{\times}]$.

v) Sei $x := [\mathbb{Z}^{\times} : N_{k_+|\mathbb{Q}}(\mathfrak{o}_+^{\times})] = \begin{cases} 2, \text{ wenn } N_{k_+|\mathbb{Q}}(\varepsilon) = 1 \\ 1, \text{ wenn } N_{k_+|\mathbb{Q}}(\varepsilon) = -1 \end{cases}$

vi) Sei $z := \begin{cases} 2, \text{ wenn } +2 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+) \\ 1, \text{ sonst} \end{cases}$

(21.6) Lemma: Sei $d \neq 1$.

i) Falls $d = 2$, ist $q = 1$ und $h(K) = q \cdot h(k_+) \cdot h(k) = 1$.

ii) Falls $d \neq 2$, ist $h(K) = 1/2 \cdot q \cdot h(k) \cdot h(k_+)$.

Bew.: siehe /10/ S. 74 (6)

(21.7) Lemma: Sei $d \neq 1, 2$.

i) Falls $d \equiv 1 \bmod 4$, ist $q = 1$.

ii) Falls $d \not\equiv 1 \bmod 4$, ist $q = \begin{cases} 2, \text{ wenn } \pm 2 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+) \\ 1, \text{ sonst} \end{cases}$

Bew.: siehe /10/ S. 77 (10_{II}), (11_{II}), (12_{II})

Bemerkung: Wenn $d \not\equiv 1 \bmod 4$, ist 2 in k_+ verzweigt. $\pm 2 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+)$ ist also äquivalent dazu, daß der Primteiler von $2\mathbb{Z}$ in $\mathfrak{o}$ Hauptideal ist.

(21.8) Lemma: ($d \neq 1$). Es ist $[\mathfrak{o}^\times : N(\mathbb{Z}\,\mathfrak{o}_+^\times)] = x$.

Bew.: Falls $d = 2$, ist $x = 1$, d.h. $N(\varepsilon) = N_{k_+|\mathbb{Q}}(\varepsilon) = -1$.
Also ist $\mathfrak{o}^\times = \{\pm 1\} = N(\mathbb{Z}\,\mathfrak{o}_+^\times)$.
Falls $d = 3$, ist $x = 2$, d.h. $N(\varepsilon) = N_{k_+|\mathbb{Q}}(\varepsilon) = 1$. $\mathbb{Z}$ wird von $\zeta_{12} = i\zeta_6^{-1}$ erzeugt und es ist $N(\zeta_{12}) = N(i)\cdot\zeta_6^{-2} = \zeta_6^{-2}$.
Da $\mathfrak{o}^\times$ von ζ_6 erzeugt wird, ist $[\mathfrak{o}^\times : N(\mathbb{Z}\,\mathfrak{o}_+^\times)] = 2$.
Falls $d > 3$, ist $\mathfrak{o}^\times = \{\pm 1\}$ und $\mathbb{Z}$ wird von i erzeugt.
Da $N(i) = 1$, ist $[\mathfrak{o}^\times : N(\mathbb{Z}\,\mathfrak{o}_+^\times)] = [\mathfrak{o}^\times : N(\mathfrak{o}_+^\times)] = [\{\pm 1\} : N_{k_+|\mathbb{Q}}(\mathfrak{o}_+^\times)] = x$.

(21.9) Lemma: ($d \neq 1$). $\mathfrak{o}^\times$ ist direktes Produkt von $\mathbb{Z}$ mit einer unendlichen zyklischen Gruppe, die von einer "Grundeinheit" ε_0 erzeugt wird.
i) Wenn $q = 1$, kann man $\varepsilon_0 = \varepsilon$ wählen.
ii) Wenn $q = 2$, kann man ε_0 so wählen, daß $\varepsilon = i\varepsilon_0^2$.

Bew.: siehe /10/ S. 75 (8)

(21.10) Lemma: ($d \neq 1$). Wenn $N_{k_+|\mathbb{Q}}(\varepsilon) = -1$, d.h. wenn $x = 1$, ist $q = 1$.

Bew.: folgt aus (21.9.ii); oder siehe /10/ S. 68 Satz 25

Wir machen jetzt Fallunterscheidungen und betrachten zunächst $d \not\equiv 1 \bmod 4$.

(21.11) Lemma: Sei $p \neq 2$ Primzahl.
i) Es ist $\left(\frac{2}{p}\right) = 1$ genau dann, wenn $p \equiv \pm 1 \bmod 8$.
ii) Es ist $\left(\frac{-2}{p}\right) = 1$ genau dann, wenn $p \equiv 1 \bmod 8$ oder $p \equiv 3 \bmod 8$.

Bew.: klar

(21.12) Lemma: Sei $d \not\equiv 1 \bmod 4$.
i) Wenn $-2 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+)$, dann gilt für alle Primteiler $p \neq 2$ von d:
$p \equiv 1 \bmod 8$ oder $p \equiv 3 \bmod 8$.
Insbesondere ist dann $d \equiv 3 \bmod 8$ oder $d \equiv 2 \bmod 16$ oder $d \equiv 6 \bmod 16$.
ii) Wenn $+2 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+)$, dann gilt für alle Primteiler $p \neq 2$ von d:
$p \equiv \pm 1 \bmod 8$. Insbesondere ist $d \equiv 7 \bmod 8$ oder $d \equiv \pm 2 \bmod 16$.

Bew.: leichte Rechnung (vgl. Lemma 20.13)

(21.13) Lemma: Sei $d \not\equiv 1 \bmod 4$ und $d \neq 2$.

Dann ist $q \cdot [\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{o}\times})] = xz$.

Bew.: Wenn $q = 1$, ist nach (21.7.ii) auch $z = 1$. Die Beh. folgt mit (21.8).
Sei also $q = 2$. Nach (21.10) ist $x = 2$. Wir müssen also zeigen:
$[\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{o}\times})] = z$.
Sei ε_0 wie in (21.9.ii). Dann ist $1 = N(\varepsilon) = N(\varepsilon_0)^2$, also $N(\varepsilon_0) = \pm 1$.
Wegen $[\mathfrak{o}^\times : N(\mathbb{Z}\,\mathfrak{o}_+^\times)] = 2$, d.h. $-1 \in N(\mathbb{Z}\,\mathfrak{o}_+^\times)$, müssen wir zeigen:
$N(\varepsilon_0) = +1$ genau dann, wenn $z = 2$.
Nach (21.3) ist $f(\mathfrak{o}[i]) = \mathfrak{o}$ oder $f(\mathfrak{o}[i]) = \mathfrak{P}$, wo $\mathfrak{P}^2 = 2\mathfrak{o}$.
Es gibt also $A, B \in \mathfrak{o}$ mit $2\varepsilon_0 = A + Bi$.
Es gibt $a, b \in \mathbb{Z}$ mit $\varepsilon = a + b\sqrt{d} = a - (bi\sqrt{d})\cdot i$.
Dann ist $\pm 4 = 4N(\varepsilon_0) = A^2 + B^2$
und $A^2 - B^2 + 2ABi = 4\varepsilon_0^2 = -4i\varepsilon = -4ai - 4bi\sqrt{d}$. Addition ergibt:

$$2A^2 + 2ABi = \pm 4 - 4bi\sqrt{d} - 4ai \qquad (21.14)$$

Insbesondere $2A^2 = \pm 4 - 4bi\sqrt{d}$.
Sei $A = 1/2\cdot(x + yi\sqrt{d})$ mit $x, y \in \mathbb{Z}$.
Dann ist $x^2 - y^2 d + 2xyi\sqrt{d} = \pm 8 - 8bi\sqrt{d}$.
Insbesondere ist $x^2 - y^2 d = \pm 8$ und $xy = 4b$, also sind x, y gerade.
Wenn $N(\varepsilon_0) = +1$, ist also $+2 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+)$, d.h. $z = 2$.
Wenn $N(\varepsilon_0) = -1$, ist $-2 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+)$. Da $N_{k_+|\mathbb{Q}}(\varepsilon) = +1$, ist
$+2 \in N_{k_+|\mathbb{Q}}(\mathfrak{o}_+)$ unmöglich. Also ist $z = 1$.

Sei jetzt $d \equiv 3 \bmod 4$. Da $D_k(K) = 4\mathfrak{o}$, folgt mit (16.10.ii):

(21.15) Lemma: Sei $d \equiv 3 \bmod 4$. Für alle $\mathbb{Q}$-Maximalordnungen $\mathfrak{M}$ ist dann $F_4(\mathfrak{M}) = \{\mathfrak{o}\}$.

Mit den Lemmata (21.6.ii) und (21.13) erhalten wir:
$l_4(\mathfrak{M}, \mathfrak{o}) = 2^{t-1}\cdot h(k_+)\cdot xz$.
Da d einen Primteiler $p \equiv 3 \bmod 4$ hat, ist $x = 2$.
Falls $d \equiv 3 \bmod 8$, ist $z = 1$ nach Lemma (21.12.ii).

(21.16) Lemma: Sei $\mathfrak{M}$ eine $\mathbb{Q}$-Maximalordnung.

i) Falls $d \equiv 7 \bmod 8$, ist $l_4(\mathfrak{M}) = l_4(\mathfrak{M}, \mathfrak{o}) = 2^t z\cdot h(k_+)$.

ii) Falls $d \equiv 3 \bmod 8$, ist $l_4(\mathfrak{M}) = l_4(\mathfrak{M}, \mathfrak{o}) = 2^t\cdot h(k_+)$.

Sei jetzt $d \equiv 2 \bmod 4$. Da $D_k(K) = 2\mathfrak{o}$, folgt mit (16.10.ii):

(21.17) Lemma: Sei $d \equiv 2 \bmod 4$ und sei $2\mathfrak{o} = \mathfrak{p}^2$.
i) Sei Q verzweigt an der Stelle $\mathfrak{p}$. Dann ist $F_4(\mathfrak{M}) = \{\mathfrak{o}\}$ für alle Q-Maximalordnungen $\mathfrak{M}$.
ii) Sei Q nicht verzweigt an der Stelle $\mathfrak{p}$. Dann ist $F_4(\mathfrak{M}) = \{\mathfrak{o}, \mathfrak{p}\}$ für alle Q-Maximalordnungen $\mathfrak{M}$.

(21.18) Lemma: Sei $d \equiv 2 \bmod 4$. Sei $\mathfrak{M}$ eine Q-Maximalordnung.
Dann ist $l_4(\mathfrak{M}, \mathfrak{o}) = 2^{t-1} xz \cdot h(k_+)$.

Bew.: Falls $d \neq 2$, folgt die Beh. mit (21.6.ii) und (21.13).
Falls $d = 2$, ist $q = 1$, $x = 1$ und $z = 2$.
Da $\mathcal{O}^{\mathfrak{o}\times} = \mathbb{Z}\,\varepsilon_+^{\times}$, ist $q \cdot [\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{o}\times})] = 1 = xz/2$. Die Beh. folgt mit (21.6.i).

(21.19) Lemma: Sei $d \equiv 2 \bmod 4$.
i) Wenn $d \neq 2$, ist $[\mathcal{O}^{\mathfrak{o}\times} : \mathcal{O}^{\mathfrak{p}\times}] = q$ und $\mathcal{O}^{\mathfrak{p}\times} = \mathbb{Z}\,\varepsilon_+^{\times}$.
ii) Wenn $d = 2$, ist $[\mathcal{O}^{\mathfrak{o}\times} : \mathcal{O}^{\mathfrak{p}\times}] = 2 = 2q$.

Bew.: i) Sei $\varepsilon = a + b\sqrt{d}$ mit $a, b \in \mathbb{N}$ und $\varepsilon_0 = 1/2 \cdot (A + Bi)$ mit $A, B \in \mathfrak{o}$ (vgl. Bew. von 21.13).
Es ist $\varepsilon = a - (bi\sqrt{d}) \cdot i \in \mathfrak{o}[i] = \mathcal{O}^{\mathfrak{p}}$. Außerdem ist $Z = \{\pm 1, \pm i\} \subset \mathcal{O}^{\mathfrak{p}}$.
Also $\mathbb{Z}\,\varepsilon_+^{\times} \subset \mathcal{O}^{\mathfrak{p}\times} \subset \mathcal{O}^{\mathfrak{o}\times}$ und daher $[\mathcal{O}^{\mathfrak{o}\times} : \mathcal{O}^{\mathfrak{p}\times}] \leq q$.
Für $q = 1$ folgt damit die Behauptung.
Für $q = 2$ genügt es zu zeigen, daß $1/2 \cdot (A + Bi) = \varepsilon_0 \notin \mathcal{O}^{\mathfrak{p}\times}$.
Wegen $1 = N_{k_+|\mathbb{Q}}(\varepsilon) = a^2 - b^2 d$ (siehe 21.10) und $d \in 2\mathbb{Z}$ ist $a \notin 2\mathbb{Z}$, d.h. $a/2 \notin \mathbb{Z}$. Aus Formel (21.14) folgt $a/2 = -A/2 \cdot B/2$.
Daher ist $A/2 \notin \mathfrak{o}$ oder $B/2 \notin \mathfrak{o}$, also $\varepsilon_0 \notin \mathfrak{o}[i] = \mathcal{O}^{\mathfrak{p}}$.
ii) Auch hier ist $\varepsilon_+^{\times} \subset \mathcal{O}^{\mathfrak{p}\times}$. Da $\zeta_8 = 1/2 \cdot (i\sqrt{2} - (i\sqrt{2})i) \notin \mathcal{O}^{\mathfrak{p}}$, aber $\zeta_8^2 = i \in \mathcal{O}^{\mathfrak{p}\times}$, ist $Z^{(2)}\,\varepsilon_+^{\times} \subset \mathcal{O}^{\mathfrak{p}\times} \subsetneq \mathbb{Z}\,\varepsilon_+^{\times} = \mathcal{O}^{\mathfrak{o}\times}$.
Daraus folgt leicht: $[\mathcal{O}^{\mathfrak{o}\times} : \mathcal{O}^{\mathfrak{p}\times}] = [Z : Z^{(2)}] = 2$.

Für $d \neq 2$ ist $[\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{p}\times})] = x$ nach (21.8) und (21.19.i).
Für $d = 2$ ist $[\mathfrak{o}^\times : N(\mathcal{O}^{\mathfrak{p}\times})] = [\mathfrak{o}^\times : N(\varepsilon_+^{\times})] = 1 = x$.
Es ist klar, daß $\mathcal{N}(\mathfrak{p}) = 2$ und $\left(\frac{K}{\mathfrak{p}}\right) = 0$. Daher gilt:

(21.20) Lemma: Sei $d \equiv 2 \bmod 4$. Sei $2\mathfrak{o} = \mathfrak{p}^2$.
Sei Q nicht an der Stelle $\mathfrak{p}$ verzweigt und sei $\mathfrak{M}$ eine Q-Maximalordnung.
Dann ist $l_4(\mathfrak{M}, \mathfrak{p}) = 2^{t_x} \cdot h(k_+)$.

Sei jetzt $d \neq 1$, $d \equiv 1 \bmod 4$. An der Stelle $2\mathbb{Z}$ ist k verzweigt über $\mathbb{Q}$.
Sei $2\mathfrak{o} = \mathfrak{p}^2$. Da $D_k(K) = \mathfrak{o}$, folgt mit (16.5.i) für alle Q-Maximalordnungen $\mathfrak{M}$, daß $F_4(\mathfrak{M}) \subset \{\mathfrak{o}, \mathfrak{p}, 2\mathfrak{o}\}$.
Wenn $d \neq 1$, $d \equiv 1 \bmod 8$, ist 2 in k_+ zerlegt, also $\mathfrak{p}$ in K zerlegt nach (14.4). Wenn $d \equiv 5 \bmod 8$, ist 2 in k_+ träge (und in $\mathbb{Q}(i)$ verzweigt), also ist $\mathfrak{p}$ in K träge nach (14.4).
Jetzt folgt mit Satz (16.10) und Lemma (16.12):

(21.21) Lemma: Sei $d \neq 1$.
i) Wenn $d \equiv 1 \bmod 8$, dann ist $\left(\frac{K}{\mathfrak{p}}\right) = 1$ und es gilt:
a) Wenn $Q \underset{k}{\tilde{}} M_2(k) \underset{k}{\tilde{}} (-1, -1)_k$, dann gibt es eine Q-Maximalordnung $\mathfrak{M}$ mit $F_4(\mathfrak{M}) = \{\mathfrak{o}, \mathfrak{p}, 2\mathfrak{o}\}$. Ist $\mathfrak{M}'$ eine weitere Q-Maximalordnung, so gilt: $F_4(\mathfrak{M}') = \begin{cases} \{\mathfrak{o}, \mathfrak{p}, 2\mathfrak{o}\}, & \text{wenn } N(\mathfrak{M}\mathfrak{M}') \in N(I^K)H^k \\ \emptyset, & \text{wenn } N(\mathfrak{M}\mathfrak{M}') \notin N(I^K)H^k \end{cases}$
b) Wenn Q Divisionsalgebra ist, ist für alle Q-Maximalordnungen $\mathfrak{M}$: $F_4(\mathfrak{M}) = \{\mathfrak{o}, \mathfrak{p}, 2\mathfrak{o}\}$.

ii) Wenn $d \equiv 5 \bmod 8$, ist $\left(\frac{K}{\mathfrak{p}}\right) = -1$ und es gilt:
a) Wenn $Q \underset{k}{\tilde{}} M_2(k) \underset{k}{\tilde{}} (-1, -1)_k$, dann gibt es eine Q-Maximalordnung $\mathfrak{M}$ mit $F_4(\mathfrak{M}) = \{\mathfrak{p}\}$. Ist $\mathfrak{M}'$ eine weitere Q-Maximalordnung, so gilt: $F_4(\mathfrak{M}') = \begin{cases} \{\mathfrak{p}\}, & \text{wenn } N(\mathfrak{M}\mathfrak{M}') \in N(I^K)H^k \\ \{\mathfrak{o}, 2\mathfrak{o}\}, & \text{wenn } N(\mathfrak{M}\mathfrak{M}') \notin N(I^K)H^k \end{cases}$
b) Wenn Q Divisionsalgebra ist, aber $\mathfrak{p}$ keine Verzweigungsstelle von Q über k ist, dann ist $F_4(\mathfrak{M}) = \{\mathfrak{o}, \mathfrak{p}, 2\mathfrak{o}\}$ für alle Q-Maximalordnungen $\mathfrak{M}$.
c) Wenn Q an der Stelle $\mathfrak{p}$ verzweigt ist, ist $F_4(\mathfrak{M}) = \{\mathfrak{o}\}$ für alle Q-Maximalordnungen $\mathfrak{M}$.

Nach Lemma (21.7.i) ist $q = 1$. Für $\mathfrak{f} \in F_4(\mathfrak{M})$ wird also

$$l_4(\mathfrak{M}, \mathfrak{f}) = 2^{t-1}\left[I^k : RN(I^K)H^k\right] \cdot h(k_+) \cdot \frac{\left[\mathfrak{o}^\times : N(\mathfrak{O}^{\mathfrak{f}\times})\right]}{\left[\mathfrak{O}^{\mathfrak{o}\times} : \mathfrak{O}^{\mathfrak{f}\times}\right]} \cdot \mathfrak{M}(\mathfrak{f}) \cdot \prod_{\mathfrak{p} \mid \mathfrak{f}} \left(1 - \left(\frac{K}{\mathfrak{p}}\right) \mathfrak{N}(\mathfrak{p})^{-1}\right)$$

Wegen $q = 1$ ist $\mathfrak{O}^{\mathfrak{o}\times} = \mathbb{Z} \mathfrak{o}_+^\times$. Mit Lemma (21.8) folgt:

(21.22) Lemma: Sei $d \neq 1$ und $d \equiv 1 \bmod 4$.
Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\sigma \in F_4(\mathfrak{M})$. Dann gilt:
i) Wenn $Q \cong_k M_2(k)$, so ist $l_4(\mathfrak{M}, \sigma) = x \cdot h(k_+)$.
ii) Wenn Q Divisionsalgebra ist, so ist $l_4(\mathfrak{M}, \sigma) = 2^{t-1} x \cdot h(k_+)$.

Wir müssen noch $l_4(\mathfrak{M}, \mathfrak{p})$ und $l_4(\mathfrak{M}, 2\sigma)$ berechnen. Es ist $\mathfrak{N}(\mathfrak{p}) = 2$.
$\mathcal{O}^{\sigma\times} = Z \sigma_+^{\times}$ ist das direkte Produkt der von i und ε erzeugten Untergruppen. Da $i \in \mathcal{O}^{2\sigma\times} < \mathcal{O}^{\mathfrak{p}\times}$, ist $[\mathcal{O}^{\sigma\times} : \mathcal{O}^{2\sigma\times}]$ bzw. $[\mathcal{O}^{\sigma\times} : \mathcal{O}^{\mathfrak{p}\times}]$ der kleinste Exponent e, so daß $\varepsilon^e \in \mathcal{O}^{2\sigma\times}$ bzw. $\mathcal{O}^{\mathfrak{p}\times}$.
Es ist $\varepsilon^e \in \mathcal{O}^{2\sigma\times}$ bzw. $\mathcal{O}^{\mathfrak{p}\times}$ genau dann, wenn $D_k(1, \varepsilon^e)$ Vielfaches von 2 bzw. 4 ist.

(21.23) Definition: ($d \neq 1$)
i) Seien $a, b \in \mathbb{N}$ so, daß $\varepsilon = 1/2 \cdot (a + b\sqrt{d})$.
ii) Sei $y := \begin{cases} 3, \text{ wenn } b \equiv 0 \bmod 2 \\ 1, \text{ wenn } b \not\equiv 0 \bmod 2 \end{cases}$

Es ist $D_k(1,\varepsilon) = D_{\mathbb{Q}}(1,\varepsilon) = b^2 d$ (siehe 6.9.iv).
Also gilt: $\varepsilon \in \mathcal{O}^{2\sigma\times}$ genau dann, wenn $\varepsilon \in \mathcal{O}^{\mathfrak{p}\times}$
genau dann, wenn $b \equiv 0 \bmod 2$.
Wegen $\varepsilon^3 = 1/8 \cdot (a^3 + 3a^2 bd) + 1/8 \cdot (3a^2 b + b^3 d) \cdot \sqrt{d}$ wird
$D_k(1,\varepsilon^3) = \left(1/4 \cdot (3a^2 b + b^3 d)\right)^2 d$.
Wir betrachten zunächst den Fall $d \equiv 1 \bmod 8$:
Es ist $a^2 - b^2 d = 4N(\varepsilon) = \pm 4$. Wäre $b \not\equiv 0 \bmod 2$, also $b^2 \equiv 1 \bmod 8$, so wäre $a^2 - 1 \equiv 4 \bmod 8$, was nicht geht. Es ist also $b \equiv 0 \bmod 2$ und daher $\varepsilon \in \mathcal{O}^{2\sigma\times} \subset \mathcal{O}^{\mathfrak{p}\times}$, also $\mathcal{O}^{\sigma\times} = \mathcal{O}^{\mathfrak{p}\times} = \mathcal{O}^{2\sigma\times}$.

(21.24) Lemma: Sei $d \neq 1$ und $d \equiv 1 \bmod 8$. Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{p} \in F_4(\mathfrak{M})$ bzw. $2\sigma \in F_4(\mathfrak{M})$. Dann gilt:
i) Wenn $Q \cong_k M_2(k)$, so ist $l_4(\mathfrak{M}, \mathfrak{p}) = x \cdot h(k_+)$ bzw. $l_4(\mathfrak{M}, 2\sigma) = 2x \cdot h(k_+)$.
ii) Wenn Q Divisionsalgebra ist, so ist $l_4(\mathfrak{M}, \mathfrak{p}) = 2^{t-1} x \cdot h(k_+)$
bzw. $l_4(\mathfrak{M}, 2\sigma) = 2^t x \cdot h(k_+)$.

Wir betrachten jetzt den Fall $d \equiv 5 \bmod 8$.
Wenn $b \equiv 0 \bmod 2$, ist $[\mathcal{O}^{\sigma\times} : \mathcal{O}^{\mathfrak{p}\times}] = [\mathcal{O}^{\sigma\times} : \mathcal{O}^{2\sigma\times}] = 1 = 3/v$.
Wenn $b \not\equiv 0 \bmod 2$, ist wegen $a^2 - b^2 d = 4N(\varepsilon) = \pm 4$ auch $a \not\equiv 0 \bmod 2$.
Also ist $b^2 \equiv a^2 \equiv 1 \bmod 8$, also $3a^2 + b^2 d \equiv 0 \bmod 8$ und daher $D_k(1,\varepsilon^3) \equiv 0 \bmod 4$. Dann ist $\varepsilon^3 \in \mathcal{O}^{2\sigma\times} < \mathcal{O}^{\mathfrak{p}\times}$ und es folgt leicht
$[\mathcal{O}^{\sigma\times} : \mathcal{O}^{2\sigma\times}] = [\mathcal{O}^{\sigma\times} : \mathcal{O}^{\mathfrak{p}\times}] = 3 = 3/v$.

Wegen $N(\varepsilon^3) = N(\varepsilon)$ ist beidesmal

$$[\sigma^\times : N(\mathcal{O}^{2\sigma\times})] = [\sigma^\times : N(\mathcal{O}^{\mathfrak{p}\times})] = [\sigma^\times : N(\mathcal{O}^{\sigma\times})] = x.$$

(21.25) Lemma: Sei $d \equiv 5 \bmod 8$. Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{p} \in F_4(\mathfrak{M})$ bzw. $2\sigma \in F_4(\mathfrak{M})$. Dann gilt:

i) Wenn $Q \tilde{k} M_2(k)$, so ist $l_4(\mathfrak{M}, \mathfrak{p}) = xy \cdot h(k_+)$ bzw. $l_4(\mathfrak{M}, 2\sigma) = 2xy \cdot h(k_+)$.

ii) Wenn Q Divisionsalgebra ist, so ist $l_4(\mathfrak{M}, \mathfrak{p}) = 2^{t-1} xy \cdot h(k_+)$ bzw. $l_4(\mathfrak{M}, 2\sigma) = 2^t xy \cdot h(k_+)$.

Wir wollen jetzt $F_4^*(\mathfrak{M})$ und $l_4^*(\mathfrak{M}, \mathfrak{f})$ berechnen.

Dazu machen wir die Zusatzvoraussetzung: $Q \tilde{k} (-1, -1)_k$.

Es ist immer $F_4^*(\mathfrak{M}) \subset F_4(\mathfrak{M})$.

Bedingung (18.10) stellt keine zusätzlichen Forderungen an $F_4^*(\mathfrak{M})$.

Für $\mathfrak{f} \in F_4^*(\mathfrak{M})$ wird nach (19.10.i) und (20.30):

$$l_4^*(\mathfrak{M}, \mathfrak{f}) = \frac{2^{e+\delta-1}}{\kappa \left[N(A^{\mathfrak{f}}) H^k : I^{k(2)} H^k\right]} \cdot \frac{\left[A^{\mathfrak{f}} \cap (\mathfrak{f} \to \sigma)^{-1}(\mathcal{O}^\sigma) : \{\mathcal{O}^{\mathfrak{f}}\}\right]}{\left[A^\sigma : (\mathfrak{f} \to \sigma)(A^{\mathfrak{f}})\right]}$$

Wir untersuchen zuerst $d \equiv 3 \bmod 4$.

Für jede Q-Maximalordnung ist dann $F_4^*(\mathfrak{M}) \subset F_4(\mathfrak{M}) = \{\sigma\}$.

Ist $\mathfrak{M}$ eine Q-Maximalordnung mit $\sigma \in F_4^*(\mathfrak{M})$ und ist $\mathfrak{M}'$ eine weitere Q-Maximalordnung, so ist nach Satz (18.16) $\sigma \in F_4^*(\mathfrak{M}')$ genau dann, wenn $N(\mathfrak{M}\mathfrak{M}') \in N(A^\sigma) H^k$.

Es gibt also (vgl. 10.10) $\left[N(A^\sigma) H^k : RI^{k(2)} H^k\right]$ verschiedene Maximalordnungstypen $\tilde{\mathfrak{M}}$ mit $F_4^*(\mathfrak{M}) = \{\sigma\}$. Für alle anderen Maximalordnungstypen $\tilde{\mathfrak{M}}$ ist $F_4^*(\mathfrak{M}) = \emptyset$.

Sei zuerst $d \equiv 3 \bmod 8$. Nach (14.8.i) ist Q unverzweigt über k. Die einzige Verzweigungsstelle von K über k ist das Hauptideal 2σ. Daher ist $e = 1$ und $N(A^\sigma) H^k = I^{k(2)} H^k = RI^{k(2)} H^k$.

(21.26) Lemma: Sei $d \equiv 3 \bmod 8$. Es ist $\neq \tilde{Q} = 2^{\delta-1}$.

Es gibt genau einen Maximalordnungstyp $\tilde{\mathfrak{M}}$ mit $F_4^*(\mathfrak{M}) = \{\sigma\}$.

Dann ist $l_4^*(\mathfrak{M}) = l_4^*(\mathfrak{M}, \sigma) = 2^{\delta-1}$.

Sei jetzt $d \equiv 7 \bmod 8$. Nach Satz (14.8.ii) ist $2\sigma = \mathfrak{p}\mathfrak{q}$ mit Primidealen $\mathfrak{p} \neq \mathfrak{q}$ und $(-1, -1)_k$ ist über k genau an den Stellen $\mathfrak{p}$ und $\mathfrak{q}$ verzweigt. Auch K ist über k genau an den Stellen $\mathfrak{p}$ und $\mathfrak{q}$ verzweigt. Also ist $e = 2$ und $N(A^\sigma) = RI^{k(2)}$. Daher gilt:

(21.27) Lemma: Wenn $d \equiv 7 \bmod 8$, gibt es genau einen Maximalordnungstyp $\tilde{\mathfrak{M}}$ mit $F_4^*(\mathfrak{M}) = \{\sigma\}$.

$N(A^{\mathfrak{o}})H^k$ wird von den Idealen aus $I^{k(2)}H^k$ und von $\mathfrak{p}$ erzeugt.

Also ist $[N(A^{\mathfrak{o}})H^k : I^{k(2)}H^k] = 1$ oder $= 2$ je nachdem ob $\mathfrak{p} \in I^{k(2)}H^k$ oder $\mathfrak{p} \notin I^{k(2)}H^k$.

Nach Lemma (20.33) ist $\mathfrak{p} \in I^{k(2)}H^k$ genau dann, wenn es $a \in k^\times$ gibt mit $2\mathbb{Z} = N_{k|\mathbb{Q}}(\mathfrak{p}) = N_{k|\mathbb{Q}}(a)\mathbb{Z}$, also genau dann, wenn es $a, b \in \mathbb{Q}$ gibt mit $2 = N_{k|\mathbb{Q}}(a+bi\sqrt{d}) = a^2 + b^2 d$, d.h. $2d = 4/b^2 - 2a^2/b^2$.

Dies ist gleichbedeutend mit $2d \in N_{\mathbb{Q}(\sqrt{2})|\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) =: M$.

Da $2 = 2^2 - 2\cdot 1^2 \in M$ und $-1 = 1^2 - 2\cdot 1^2 \in M$, ist dies äquivalent zu $\pm d \in M$.

Da $\mathbb{Q}(\sqrt{2})$ Klassenzahl 1 hat und 2 die einzige Verzweigungsstelle über $\mathbb{Q}$ ist, ist dies gleichbedeutend damit, daß alle Primteiler $p \in \mathbb{N}$ von d in $\mathbb{Q}(\sqrt{2})$ zerlegt sind, d.h. daß $p \equiv \pm 1 \bmod 8$ für alle Primteiler p von d (vgl. 21.11.i).

(21.28) Definition:

Sei $w := \begin{cases} 2, \text{ wenn für alle Primteiler } p \neq 2 \text{ von } d \text{ gilt: } p \equiv \pm 1 \bmod 8 \\ 1, \text{ wenn } d \text{ Primteiler } p \equiv \pm 3 \bmod 8 \text{ enthält} \end{cases}$

Wir haben also $[N(A^{\mathfrak{o}})H^k : I^{k(2)}H^k] = 2/w$ und daher

(21.29) Lemma: Sei $d \equiv 7 \bmod 8$. Dann ist $\#\widetilde{Q} = 2^{\delta-2}w$.

Ist $\mathfrak{M}$ eine Q-Maximalordnung mit $F_4^*(\mathfrak{M}) = \{\mathfrak{o}\}$, so ist

$l_4^*(\mathfrak{M}) = l_4^*(\mathfrak{M}, \mathfrak{o}) = 2^{\delta-1}w$.

Sei jetzt $d \equiv 1 \bmod 4$. Nach (14.8.i) ist Q unverzweigt über k.

K ist unverzweigt über k (siehe 21.3), also ist $e = 0$ und

$N(A^{\mathfrak{o}}) = I^{k(2)} = RI^{k(2)}$.

Ist $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal, so ist

$(\mathfrak{f} \to \mathfrak{o})(A^{\mathfrak{f}}) \supset (\mathfrak{f} \to \mathfrak{o}) \cdot (k \to \mathfrak{f})(I^k) = (k \to \mathfrak{o})(I^k) = A^{\mathfrak{o}}$, also

$[A^{\mathfrak{o}} : (\mathfrak{f} \to \mathfrak{o})(A^{\mathfrak{f}})] = 1$ und $N(A^{\mathfrak{f}}) = N(A^{\mathfrak{o}})$.

Ist $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{f} \in F_4^*(\mathfrak{M})$, so haben wir also

mit (19.10.ii): $l_4^*(\mathfrak{M}, \mathfrak{f}) = \kappa^{-1} \cdot 2^{\delta-1} \cdot \prod_{\mathfrak{p}|\mathfrak{f}} [U_{\mathfrak{p}}^{\mathfrak{o}\times} \cap \Delta^{-1}(U_{\mathfrak{p}}^{\mathfrak{f}\times}) : U_{\mathfrak{p}}^{\mathfrak{f}\times}]$

2 ist verzweigt in k. Sei $2\mathfrak{o} = \mathfrak{p}^2$. Nach Satz (18.9.ii) gibt es eine Q-Maximalordnung $\mathfrak{M}_0$ mit $2\mathfrak{o} \in F_4^*(\mathfrak{M}_0)$. Ist $\mathfrak{M}$ eine weitere Q-Maximalordnung und $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal, so ist nach Satz (18.18) $\mathfrak{f} \in F_4^*(\mathfrak{M})$ genau dann, wenn $\mathfrak{f} \in \{\mathfrak{o}, \mathfrak{p}, 2\mathfrak{o}\}$ und $N(\mathfrak{M}_0\mathfrak{M})2\mathfrak{f}^{-1} \in I^{k(2)}H^k$.

Im einzelnen erhalten wir :

$\sigma \in F_4^*(\mathfrak{M})$ und $2\sigma \in F_4^*(\mathfrak{M})$ genau dann, wenn $\mathfrak{M}_O$ und $\mathfrak{M}$ vom gleichen Typ sind.

$\mathfrak{p} \in F_4^*(\mathfrak{M})$ genau dann, wenn $N(\mathfrak{M}_O\mathfrak{M})_\mathfrak{p} \in I^{k(2)}H^k$.

Wenn $d \equiv 5 \bmod 8$, ist $\mathfrak{p}$ träge in K, nach (8.4.iii) also $\mathfrak{p} \notin N(I^K)H^k$ und erst recht $\mathfrak{p} \notin I^{k(2)}H^k$. Wir haben also:

(21.30) Lemma: Sei $d \equiv 5 \bmod 8$. Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $F_4^*(\mathfrak{M}) = \{\sigma, 2\sigma\}$, und es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}'}$, so daß $F_4^*(\mathfrak{M}') = \{\mathfrak{p}\}$. Es gilt $N(\mathfrak{M}\mathfrak{M}')_\mathfrak{p} \in I^{k(2)}H^k$.

Für alle anderen Maximalordnungstypen $\widetilde{\mathfrak{M}''}$ ist $F_4^*(\mathfrak{M}'') = \emptyset$.

(Es ist $\neq \widetilde{Q} = 2^{\delta-1}$).

Wenn $d \equiv 1 \bmod 8$, müssen wir untersuchen, ob $\mathfrak{p} \in I^{k(2)}H^k$.
Dies ist genau dann der Fall, wenn $w = 2$. (Der Beweis geht genauso wie in den vorbereitenden Bemerkungen zu Lemma 21.29). Also folgt:

(21.31) Lemma: Sei $d \equiv 1 \bmod 8$. Es ist $\neq \widetilde{Q} = 2^{\delta-1}$.
i) Wenn $w = 2$, gibt es genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $F_4^*(\mathfrak{M}) = \{\sigma, \mathfrak{p}, 2\sigma\}$. Für alle anderen Maximalordnungstypen $\widetilde{\mathfrak{M}'}$ ist $F_4^*(\mathfrak{M}') = \emptyset$.
ii) Sei $w = 1$. Dann gibt es genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $F_4^*(\mathfrak{M}) = \{\sigma, 2\sigma\}$. Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}'}$, so daß $F_4^*(\mathfrak{M}') = \{\mathfrak{p}\}$. Es gilt $N(\mathfrak{M}\mathfrak{M}')_\mathfrak{p} \in I^{k(2)}H^k$.
Für alle anderen Maximalordnungstypen $\widetilde{\mathfrak{M}''}$ ist $F_4^*(\mathfrak{M}'') = \emptyset$.

(21.32) Lemma: Sei $d \equiv 1 \bmod 4$. Dann gilt:

i) $O_\mathfrak{p}^{\sigma\times} \cap \Delta^{-1}(O_\mathfrak{p}^{\mathfrak{p}\times}) = O_\mathfrak{p}^{\mathfrak{p}\times}$

ii) $O_\mathfrak{p}^{\sigma\times} \cap \Delta^{-1}(O_\mathfrak{p}^{2\sigma\times}) = O_\mathfrak{p}^{\mathfrak{p}\times}$

iii) $[O_\mathfrak{p}^{\mathfrak{p}\times} : O_\mathfrak{p}^{2\sigma\times}] = 2$

Bew.: i) "$\supset$" ist klar.
"$\subset$": Sei $a \in O_\mathfrak{p}^{\sigma\times} \cap \Delta^{-1}(O_\mathfrak{p}^{\mathfrak{p}\times})$, also $\Delta(a) \in O_\mathfrak{p}^{\mathfrak{p}\times}$. Dann ist auch $a^2 = \Delta(a)\cdot N(a) \in O_\mathfrak{p}^{\mathfrak{p}\times}$. Also ist $\mathfrak{p}_\mathfrak{p}^2 = 2\sigma_\mathfrak{p} = D_{k_\mathfrak{p}}(O_\mathfrak{p}^\mathfrak{p})$ Teiler von $D_{k_\mathfrak{p}}(1,a^2)\sigma_\mathfrak{p} = (a^2 - a^{*2})^2\sigma_\mathfrak{p}$ und $\mathfrak{p}O_\mathfrak{p}^\sigma$ Teiler von $(a^2 - a^{*2})O_\mathfrak{p}^\sigma$.
Dann ist $\mathfrak{p}O_\mathfrak{p}^\sigma$ auch Teiler von $(a - a^*)^2O_\mathfrak{p}^\sigma = \left((a^2-a^{*2}) + 2(-aa^*+a^{*2})\right)O_\mathfrak{p}^\sigma$ und $\mathfrak{p}_\mathfrak{p}$ ist Teiler von $D_{k_\mathfrak{p}}(1,a)\sigma_\mathfrak{p} = (a-a^*)^2\sigma_\mathfrak{p}$. Wegen $D_{k_\mathfrak{p}}(O_\mathfrak{p}^\sigma) = \sigma_\mathfrak{p}$ ist also $\sigma_\mathfrak{p}[a] \neq O_\mathfrak{p}^\sigma$. Daher ist $\sigma_\mathfrak{p}[a] \subset O_\mathfrak{p}^\mathfrak{p}$ und insbesondere $a \in O_\mathfrak{p}^{\mathfrak{p}\times}$.

ii) "$\subset$" folgt aus i)

"$\supset$": Sei $a \in \mathcal{O}_{\mathfrak{P}}^{\mathfrak{P}\times}$, also $2\mathfrak{o}_{\mathfrak{P}} = D_{K_{\mathfrak{P}}}(\mathcal{O}_{\mathfrak{P}}^{\mathfrak{P}})$ Teiler von $(a-a^*)^2\mathfrak{o}_{\mathfrak{P}} = D_{K_{\mathfrak{P}}}(1,a)\mathfrak{o}_{\mathfrak{P}}$.

Zu zeigen ist: $\Delta(a) \in \mathcal{O}_{\mathfrak{P}}^{2\mathfrak{o}\times}$. Wegen $N(a) \in \mathfrak{o}_{\mathfrak{P}}^{\times}$ ist dies äquivalent zu $a^2 = \Delta(a)N(a) \in \mathcal{O}_{\mathfrak{P}}^{2\mathfrak{o}\times}$, d.h. zu der Beh., daß $4\mathfrak{o}_{\mathfrak{P}} = D_{K_{\mathfrak{P}}}(\mathcal{O}_{\mathfrak{P}}^{2\mathfrak{o}})$ Teiler von $(a^2 - a^{*2})^2\mathfrak{o}_{\mathfrak{P}}$ ist. Also ist zu zeigen, daß daß $2\mathcal{O}_{\mathfrak{P}}^{\mathfrak{o}}$ Teiler von $(a^2 - a^{*2})\mathcal{O}_{\mathfrak{P}}^{\mathfrak{o}}$ ist. Dies folgt wegen $a^2 - a^{*2} = (a - a^*)^2 + 2(aa^* - a^{*2})$.

iii) Nach (7.19.iv) und (7.23) ist

$$[\mathcal{O}_{\mathfrak{P}}^{\mathfrak{P}\times} : \mathcal{O}_{\mathfrak{P}}^{2\mathfrak{o}\times}] = [\mathcal{O}_{\mathfrak{P}}^{\mathfrak{o}\times} : \mathcal{O}_{\mathfrak{P}}^{2\mathfrak{o}\times}]/[\mathcal{O}_{\mathfrak{P}}^{\mathfrak{o}\times} : \mathcal{O}_{\mathfrak{P}}^{\mathfrak{P}\times}] = \mathcal{N}(\mathfrak{P}^2)/\mathcal{N}(\mathfrak{P}) = 2.$$

Jetzt folgt sofort:

(21.33) Lemma: Sei $d \equiv 1 \bmod 4$ und $d \neq 1$.
Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{o} \in F_4^*(\mathfrak{M})$ bzw. $\mathfrak{P} \in F_4^*(\mathfrak{M})$ bzw. $2\mathfrak{o} \in F_4^*(\mathfrak{M})$.
Dann ist $l_4^*(\mathfrak{M},\mathfrak{o}) = 2^{\delta-2}$ bzw. $l_4^*(\mathfrak{M},\mathfrak{P}) = 2^{\delta-2}$ bzw. $l_4^*(\mathfrak{M},2\mathfrak{o}) = 2^{\delta-1}$.

(21.34) Lemma: Sei $d = 1$. Ist $\mathfrak{M}$ eine Q-Maximalordnung, so ist $l_4^*(\mathfrak{M},\mathfrak{o}) = l_4^*(\mathfrak{M},\mathfrak{P}) = 1$ und $l_4^*(\mathfrak{M},2\mathfrak{o}) = 2$, also $l_4^*(\mathfrak{M}) = 4$.

Wir betrachten jetzt den Fall $d \equiv 2 \bmod 4$.
Nach (14.8.i) ist Q unverzweigt über k, also $RI^{k(2)}{}_H{}^k = I^{k(2)}{}_H{}^k$.
2 ist verzweigt in k, sei $2\mathfrak{o} = \mathfrak{P}^2$.
K ist Körper und über k genau an der Stelle $\mathfrak{P}$ verzweigt, also ist $e = 1$.
$N(A^{\mathfrak{o}})H^k$ wird von den Idealen aus $I^{k(2)}{}_H{}^k$ und von $\mathfrak{P}$ erzeugt.
Wie in der Vorbemerkung zu Lemma (21.29) schließt man, daß $[N(A^{\mathfrak{o}})H^k : I^{k(2)}{}_H{}^k] = 2/w$. Damit folgt:

(21.35) Lemma: Sei $d \equiv 2 \bmod 4$. Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{o} \in F_4^*(\mathfrak{M})$. Dann ist $l_4^*(\mathfrak{M},\mathfrak{o}) = 2^{\delta-2}w$.

(21.36) Lemma: Sei $d \equiv 2 \bmod 4$. Dann gilt:

i) $\mathcal{O}_{\mathfrak{P}}^{\mathfrak{o}\times} \cap \Delta^{-1}(\mathcal{O}_{\mathfrak{P}}^{\mathfrak{P}\times}) = \mathcal{O}_{\mathfrak{P}}^{\mathfrak{o}\times}$

ii) $[\mathcal{O}_{\mathfrak{P}}^{\mathfrak{o}\times} : \mathcal{O}_{\mathfrak{P}}^{\mathfrak{P}\times}] = 2$

iii) $[A^{\mathfrak{o}} : (\mathfrak{P} \to \mathfrak{o})(A^{\mathfrak{P}})] = 2$ und $N(A^{\mathfrak{P}}) = I^{k(2)}$

Bew.: i) "$\subset$" ist klar

"$\supset$" folgt genauso wie (21.32.ii), man muß im Beweis nur $\mathcal{O}_{\mathfrak{P}}^{\mathfrak{P}}$ durch $\mathcal{O}_{\mathfrak{P}}^{\mathfrak{o}}$ und $\mathcal{O}_{\mathfrak{P}}^{2\mathfrak{o}}$ durch $\mathcal{O}_{\mathfrak{P}}^{\mathfrak{P}}$ ersetzen.

ii) folgt mit (7.19.iv) und (7.23)

iii) Nach (19.10.iii) ist $\left[A^{\mathfrak{o}} : (\mathfrak{p} \to \mathfrak{o})(A^{\mathfrak{p}})\right] = \left[\Delta^{-1}(U_{\mathfrak{p}}^{\mathfrak{o}\times}) : \Delta^{-1}(U_{\mathfrak{p}}^{\mathfrak{p}\times})\, U_{\mathfrak{p}}^{\mathfrak{o}\times}\right]$.

Es ist $(\mathfrak{p} \to \mathfrak{o})(A^{\mathfrak{p}}) \supset (k \to \mathfrak{o})(I^k)$ und $\left[A^{\mathfrak{o}} : (k \to \mathfrak{o})(I^k)\right] = 2$ (siehe 19.8).

Es genügt also zu zeigen: $\left[\Delta^{-1}(U_{\mathfrak{p}}^{\mathfrak{o}\times}) : \Delta^{-1}(U_{\mathfrak{p}}^{\mathfrak{p}\times})\, U_{\mathfrak{p}}^{\mathfrak{o}\times}\right] > 1$.

(Dann folgt auch die zweite Behauptung.)

Da $K_{\mathfrak{p}}$ Körper ist, sieht man leicht ein, daß $\Delta^{-1}(U_{\mathfrak{p}}^{\mathfrak{o}\times}) = K_{\mathfrak{p}}^{\times}$.

Nach i) ist $U_{\mathfrak{p}}^{\mathfrak{p}\times} \subset \Delta^{-1}(U_{\mathfrak{p}}^{\mathfrak{p}\times})$, also ist zu zeigen: $\left[K_{\mathfrak{p}}^{\times} : \Delta^{-1}(U_{\mathfrak{p}}^{\mathfrak{p}\times})\right] > 1$.

Sei $\pi := i\sqrt{d}$. Da $\pi^2 \mathfrak{o}_{\mathfrak{p}} = -d\,\mathfrak{o}_{\mathfrak{p}} = 2 \cdot d/2\, \mathfrak{o}_{\mathfrak{p}} = 2\,\mathfrak{o}_{\mathfrak{p}}$, ist π ein Primelement von $\mathfrak{o}_{\mathfrak{p}}$ und $\{1, \pi^{-1}(1+i)\}$ ist Basis von $U_{\mathfrak{p}}^{\mathfrak{o}}$ über $\mathfrak{o}_{\mathfrak{p}}$.

Da $2 - d \equiv 0 \bmod 4$, ist $2 - d + 2i\sqrt{d} = 2\pi\varepsilon$ mit $\varepsilon \in \mathfrak{o}_{\mathfrak{p}}^{\times}$.

Sei $a := 1 + i\sqrt{d} + i$. Dann ist

$$\Delta(a) = \frac{a^2}{N(a)} = \frac{1 - d - 1 + 2i\sqrt{d} + 2i + 2i\sqrt{d}\cdot i}{(1 + i\sqrt{d})^2 + 1}$$

$$= \frac{-d - 2 + (2 + 2i\sqrt{d})(1 + i)}{2 - d + 2i\sqrt{d}}$$

$$= \frac{-d - 2}{2\pi\varepsilon} + \frac{(1 + \pi)}{\varepsilon} \cdot \frac{1 + i}{\pi}$$

Wegen $\varepsilon^{-1}(1 + \pi) \in \mathfrak{o}_{\mathfrak{p}}^{\times}$ ist $\Delta(a) \notin \mathfrak{o}_{\mathfrak{p}}[i] = U_{\mathfrak{p}}^{\mathfrak{p}}$.

(21.37) Lemma: Sei $d \equiv 2 \bmod 4$. Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{p} \in F_4^*(\mathfrak{M})$. Dann ist $l_4^*(\mathfrak{M}, \mathfrak{p}) = 2^{\delta - 1}$.

Bew.: folgt sofort aus (19.10) und (21.36)

Nach Satz (18.9.ii) gibt es eine Q-Maximalordnung $\mathfrak{M}_0$ mit $\mathfrak{p} \in F_4^*(\mathfrak{M}_0)$.

Ist $\mathfrak{M}$ eine weitere Q-Maximalordnung und $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal, so ist nach Satz (18.18) $\mathfrak{f} \in F_4^*(\mathfrak{M})$ genau dann, wenn $\mathfrak{f} \in \{\mathfrak{o}, \mathfrak{p}\}$ und $N(\mathfrak{M}_0 \mathfrak{M})_{\mathfrak{p}}\, \mathfrak{f}^{-1} \in N(A^{\mathfrak{p}}) H^k$.

Im einzelnen erhalten wir:

$\mathfrak{p} \in F_4^*(\mathfrak{M})$ genau dann, wenn $\mathfrak{M}_0$ und $\mathfrak{M}$ vom gleichen Typ sind.

$\mathfrak{o} \in F_4^*(\mathfrak{M})$ genau dann, wenn $N(\mathfrak{M}_0 \mathfrak{M})\, \mathfrak{p} \in N(A^{\mathfrak{o}}) H^k$, wegen $\mathfrak{p} \in N(A^{\mathfrak{o}})$

also genau dann, wenn $N(\mathfrak{M}_0 \mathfrak{M}) \in N(A^{\mathfrak{o}}) H^k$.

Wegen $\left[N(A^{\mathfrak{o}}) H^k : I^{k(2)} H^k\right] = 2/w$ ergibt sich:

(21.38) Lemma: Sei $d \equiv 2 \bmod 4$. Dann gilt: $\# \tilde{Q} = 2^{\delta-1}$ und
i) Wenn $w = 2$, gibt es genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $F_4^*(\mathfrak{M}) = \{\sigma, \gamma\}$. Für alle anderen Maximalordnungstypen ist $F_4^*(\mathfrak{M}) = \emptyset$.
ii) Sei $w = 1$. Dann gibt es genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$ mit $F_4^*(\mathfrak{M}) = \{\sigma, \gamma\}$ und es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}'}$ mit $F_4^*(\mathfrak{M}') = \{\sigma\}$. Es ist $N(\mathfrak{M}\mathfrak{M}')_{\mathfrak{p}} \in I^{k(2)}{}_{\mathrm{II}}{}^{k}$.
Für alle anderen Maximalordnungstypen $\widetilde{\mathfrak{M}''}$ ist $F_4^*(\mathfrak{M}'') = \emptyset$.

Wir haben jetzt das Material gesammelt, um λ_4 und λ_4^* zu berechnen (vgl. 18.26). Die Zusammenfassung und die Tabelle für $1 \leq d \leq 101$ und $Q \underset{k}{\sim} M_2(k)$ verschieben wir auf das Ende des vierten Teils, da wir dann mehr Ergebnisse beisammenhaben.

Teil IV
Die Konjugationsklassenzahlen der nichtzyklischen Gruppen

Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und sei Q eine k-Quaternionenalgebra.
In Teil IV will ich die Konjugationsklassenzahlen der nichtzyklischen, endlichen Gruppen in $\Gamma(\mathfrak{M})$ für die verschiedenen Q-Maximalordnungen $\mathfrak{M}$ berechnen. Ich setze daher voraus, daß $\Gamma(Q)$ nichtzyklische Gruppen enthält, d.h. daß $\zeta_{2n} + \zeta_{2n}^{-1} \in k$ und $Q \tilde{\in} ((\zeta_{2n}-\zeta_{2n}^{-1})^2, -1)_k$ für ein $n \in \mathbb{N}$, $n \geq 2$ (die genauen Bedingungen findet man in 13.3).
Selbstverständlich setze ich außerdem voraus, daß $\Gamma(\mathfrak{M})$ nicht endlich ist; dies ist für diese Quaternionenalgebren äquivalent zu der Voraussetzung, daß k nicht total reell ist.
Außer für Oktaeder- und Ikosaedergruppen berechne ich die Konjugationsklassenzahlen (wie bei den zyklischen Gruppen) indirekt, indem ich sie auf Konjugationsklassenzahlen von Erzeugendensystemen zurückführe.
Eine Sonderrolle spielt dabei n = 2 (§§ 23, 24).

Ich gebe eine Inhaltsübersicht über Teil IV:

1. In § 22 berechne ich die Konjugationsklassenzahlen von n-Diedergruppen für n > 2.
Dabei gehe ich davon aus, daß eine feste Q-Maximalordnung $\mathfrak{M}$ gegeben ist, für die $F_{2n}^*(\mathfrak{M})$ und $l_{2n}^*(\mathfrak{M}, f)$ für alle $f \in F_{2n}^*(\mathfrak{M})$ bekannt sind (diese Werte lassen sich ja mit § 18 bestimmen).
Jede n-Diedergruppe in $\Gamma = \Gamma(\mathfrak{M})$ wird von zwei Elementen $E, B \in \Gamma$ erzeugt mit $S(E) = \zeta_{2n} + \zeta_{2n}^{-1}$ und $BEB^{-1} = E^{-1}$.
Für n > 2 läßt sich die Konjugationsklassenzahl $\mu_n = \mu_n(\mathfrak{M})$ der n-Diedergruppen in Γ auf natürliche Weise in eine Summe von gewissen Zahlen $\mu_n(f)$ aufspalten, wobei $f = f(\mathfrak{M} \cap k[E])$ die Menge $F_{2n}^*(\mathfrak{M})$ durchläuft (22.5). Diese Aufspaltung ist nur möglich, wenn n > 2 ist, da nur dann jede n-Diedergruppe genau eine 2n-zyklische Gruppe enthält.
Im wesentlichen geschieht die Berechnung von μ_n in zwei Schritten (bei beiden Schritten wird die Unterteilung nach $f(\mathfrak{M} \cap k[E])$ berücksichtigt):
Im ersten Schritt führe ich $\mu_n(f)$ auf die Konjugationsklassenzahl von Erzeugendenpaaren (E,B) zurück (Lemma 22.8).
Im zweiten Schritt führe ich die Konjugationsklassenzahl von Erzeugendenpaaren (E,B) auf die Konjugationsklassenzahl $l_{2n}^*(f)$ von Elementen E zurück (Lemma 22.9.i).

Nach einer abschließenden Indexberechnung (22.10 und 22.12) kann ich das Endergebnis, Satz (22.13), formulieren.
Für imaginärquadratische Zahlkörper (und n = 3) ergibt sich daraus ein einfaches Resultat (Korollar 22.14 und anschließende Bemerkung).

2. In § 23 errechne ich die Konjugationsklassenzahl $\lambda_4^T(\mathfrak{M}) = 1_4^T(\mathfrak{M})$ der 4-zyklischen Gruppen in $\Gamma(\mathfrak{M})$, die in einer Tetraedergruppe in $\Gamma(\mathfrak{M})$ enthalten sind.
$1_4^T(\mathfrak{M})$ zerfällt kanonisch in eine Summe von $1_4^T(\mathfrak{M},\mathfrak{f})$ (23.5,6).
Die einzelnen Summanden und die Menge $F_4^T(\mathfrak{M})$ der Ideale $\mathfrak{f}$ mit $1_4^T(\mathfrak{M},\mathfrak{f}) > 0$ berechne ich fast genauso wie ich in § 18 $1_4^*(\mathfrak{M},\mathfrak{f})$ und $F_4^*(\mathfrak{M})$ berechnet habe. (Die Unterschiede liegen vor allem in der "lokalen" Technik zur Bestimmung von $F_4^T(\mathfrak{M})$.)
Einzelne Beweisteile kann ich direkt aus § 18 übernehmen.
Die Gruppe $Y^{\mathfrak{f}}$ (Def. 23.15) spielt in § 23 die gleiche Rolle wie die Gruppe $A^{\mathfrak{f}}$ der ambigen Ideale in § 18.
Hauptergebnis von § 23 sind die Sätze (23.22) und (23.26).
Im konkreten Fall kann man jetzt $\lambda_4^T(\mathfrak{M})$ für eine vorgegebene Q-Maximalordnung $\mathfrak{M}$ bestimmen, wenn man wenigstens eines der Ideale $\mathfrak{f} \in F_4^T(\mathfrak{M})$ (soweit vorhanden) ermitteln kann.

3. Die Kenntnis der $1_4^T(\mathfrak{M},\mathfrak{f})$ benötige ich zur Bestimmung der Konjugationsklassenzahlen μ_T von Tetraedergruppen und μ_2 von 2-Diedergruppen in § 24.
Ich setze hier (wie in § 22) eine feste Q-Maximalordnung $\mathfrak{M}$ mit bekannten $F_4^*(\mathfrak{M})$, $F_4^T(\mathfrak{M})$ und $1_4^*(\mathfrak{M},\mathfrak{f})$, $1_4^T(\mathfrak{M},\mathfrak{f})$ für $\mathfrak{f} \in F_4^*(\mathfrak{M})$ bzw. $\mathfrak{f} \in F_4^T(\mathfrak{M})$ voraus.
μ_2 zerfällt i.a. nicht in eine kanonische Summe von $\mu_2(\mathfrak{f})$, da jede 2-Diedergruppe genau 3 verschiedene 4-zyklische Gruppen enthält, denen auch verschiedene Ideale $\mathfrak{f}$ entsprechen können. Die Berechnung von μ_2 und μ_T wird dadurch komplizierter als die Berechnung von μ_n für $n > 2$; aber auch hier wird sie durch zwei wesentliche Schritte strukturiert:
Erster Schritt: Ich teile die 2-Diedergruppen aus $\Gamma(\mathfrak{M})$ in 4 grobe Klassen ein. Zu welcher der 4 Klassen eine 2-Diedergruppe gehört, hängt davon ab, ob sie in einer Tetraedergruppe in $\Gamma(\mathfrak{M})$ enthalten ist oder nicht, und davon, ob sie in einer 4-Diedergruppe in $\Gamma(\mathfrak{M})$ enthalten ist oder nicht (Def. 24.2 und 24.4).

(Bemerkung: Man kann es auch anders ausdrücken. Die (grobe) Klasse einer 2-Diedergruppe wird durch ihren Normalisator in $\Gamma(\mathfrak{M})$ bestimmt. Dieser ist entweder Oktaeder-, Tetraeder-, 4-Dieder- oder 2-Diedergruppe.)
Jede 2-Diedergruppe in $\Gamma(\mathfrak{M})$ wird von zwei Elementen $U, V \in \Gamma(\mathfrak{M})$ erzeugt mit $S(U) = S(V) = 0$ und $UV = -VU$.
In jeder der angegebenen groben Klassen kann man das Verhältnis der Konjugationsklassenzahl von 2-Diedergruppen zur Konjugationsklassenzahl von Paaren Erzeugender (U,V) berechnen (Lemma 24.14).
Zweiter Schritt: Die Konjugationsklassenzahlen von Paaren Erzeugender (U,V) kann man kanonisch aufspalten in eine Summe, in der über die $f = f(\mathfrak{M} \cap k[U]) \in F_4^*$ summiert wird. Diese Tatsache ermöglicht es, die Konjugationsklassenzahlen von Paaren (U,V) (in einem komplizierten Prozeß) zurückzuführen auf die $l_4^*(f)$ und $l_4^T(f)$.
Endergebnis ist Satz (24.27) bzw. Korollar (24.28).
(μ_2^- ist die Konjugationsklassenzahl von 2-Diedergruppen aus $\Gamma(\mathfrak{M})$, die in keiner Tetraedergruppe aus $\Gamma(\mathfrak{M})$ enthalten sind.)

4. Die Konjugationsklassenzahl der Oktaedergruppen in $\Gamma(\mathfrak{M})$ ist gleich der Konjugationsklassenzahl derjenigen 2-Diedergruppen in $\Gamma(\mathfrak{M})$, deren Normalisator in $\Gamma(\mathfrak{M})$ eine Oktaedergruppe ist (vgl. 25.12).
In § 25 entwickle ich eine andere Methode zur Berechnung der Konjugationsklassenzahlen μ_0 von Oktaedergruppen in $\Gamma(\mathfrak{M})$, die auch für die Ikosaedergruppen unverändert gültig ist.
Das Verfahren ist im wesentlichen das gleiche wie bei der Berechnung von $l_{2n}(\mathfrak{M}, f)$, $l_{2n}^*(\mathfrak{M}, f)$ und $l_4^T(\mathfrak{M}, f)$. Der Unterschied ist, daß ich hier die Konjugationsklassenzahl der Gruppen direkt und nicht indirekt über Erzeuger ermittle.
Das ist nur für Oktaeder- und Ikosaedergruppen möglich, vor allem deshalb, weil Oktaeder- und Ikosaedergruppen maximalendlich in $\Gamma(0)$ sind und als einzige Gruppen maximalendlich bleiben, wenn man den Koeffizientenkörper k beliebig erweitert (Oktaeder- und Ikosaedergruppen sind maximalendlich in $SL(2,\mathbb{C})$).
Das Hauptergebnis von § 25 ist Satz (25.9).

5. In § 26 berechne ich die Konjugationsklassenzahlen λ_4^T, μ_T und μ_2^- für den Fall, daß $k = \mathbb{Q}(i\sqrt{d})$ imaginärquadratischer Zahlkörper ist.
Die Methoden, die ich anwende, sind im wesentlichen die gleichen wie in den Paragrafen 20 und 21.

Die Ergebnisse für die 4-zyklischen Gruppen, 2-Dieder- und Tetraedergruppen, die ich in den §§ 21, 26 gewonnen habe, fasse ich zu Ende des Paragrafen in (26.12) bis (26.14) zusammen.
(Statt λ_4 habe ich jeweils $\lambda_4' = \lambda_4 - \lambda_4$ berechnet.)
Für $1 < d \leq 101$ und die Quaternionenalgebra $Q = M_2(k)$ habe ich die Werte mit Hilfe der Tabellen in /1/ explizit berechnet und tabelliert (26.15).
Schließlich habe ich noch (für $d < 119$ bzw. $d < 101$) die Konjugationsklassenzahlen der endlichen Gruppen tabelliert für den Fall, daß $Q = (-1, -1)_k$ bzw. $Q = (-3, -1)_k$ Divisionsalgebra ist (d.h. für $d \equiv 7 \bmod 8$ bzw. $d \equiv 2 \bmod 3$); siehe die Tabellen (26.16) und (26.17).

§ 22 . Die Konjugationsklassenzahlen der n-Diedergruppen für n > 2

Jede n-Diedergruppe wird von Elementen E, B mit $S(E) = \zeta_{2n}+\zeta_{2n}^{-1}$ und $BEB^{-1} = E^{-1}$ erzeugt.
Grob gesprochen führen wir in § 22 die Konjugationsklassenzahl von n-Diedergruppen zurück auf die Konjugationsklassenzahl von Paaren (E,B) solcher Erzeugenden (Lemma 22.8) und diese wiederum auf die Konjugationsklassenzahl l_{2n}^* (Lemma 22.9).
Wir müssen, wie bei der Bestimmung von Konjugationsklassenzahlen zyklischer Gruppen zunächst eine Unterteilung nach $f(\mathfrak{M} \cap k[E])$ vornehmen. Hauptergebnis von § 22 ist Satz (22.13).
Das Beispiel imaginärquadratischer Zahlkörper ist dann ganz leicht zu behandeln (Korollar 22.14).
Wir können in diesem Paragrafen nur die n-Diedergruppen mit n > 2 untersuchen, da wir brauchen, daß eine n-Diedergruppe nur eine 2n-zyklische Untergruppe enthält (siehe 15.3). Nach Vorbereitung durch § 23 können wir dann in § 24 auch die 2-Diedergruppen (und Tetraedergruppen) untersuchen.

Wir machen für diesen Paragrafen folgende Generalvoraussetzung:

(22.1) Sei $n \in \mathbb{N}$, $n \geq 2$. Sei k algebraischer Zahlkörper mit Hauptordnung $\mathcal{O}$. Sei $\zeta_{2n}+\zeta_{2n}^{-1} \in k$. Sei k nicht total reell. Sei Q eine k-Quaternionenalgebra, $Q \tilde{\in} ((\zeta_{2n}-\zeta_{2n}^{-1})^2, -1)_k$. Sei $K := k[X]/(X^2 - (\zeta_{2n}+\zeta_{2n}^{-1})X + 1)k[X]$.
Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\lambda_{2n}^*(\mathfrak{M}) \neq 0$.
Wir kürzen ab: $\Gamma := \Gamma(\mathfrak{M})$, $F_{2n}^* := F_{2n}^*(\mathfrak{M})$, $L_{2n}^* := L_{2n}^*(\mathfrak{M})$ usw.

(22.2) Definition: i) Sei $M_n := M_n(\mathfrak{M}) := \{D \subset \Gamma \mid D \text{ ist n-Diedergruppe}\}$.
ii) Sei $\mu_n := \mu_n(\mathfrak{M}) := \#\# M_n/\sim$.

In diesem Paragrafen wollen wir μ_n für n > 2 bestimmen.
Dazu benutzen wir den Umweg über Erzeugende.

(22.3) Definition:
i) Sei $P_n := \{(E,B) \mid E, B \in \Gamma \text{ mit } S(E) = \zeta_{2n}+\zeta_{2n}^{-1} \text{ und } BEB^{-1} = E^{-1}\}$
ii) Wir definieren Abbildungen a und b folgendermaßen:

$a: P_n \to L_{2n}^*$, $(E,B) \mapsto E$

$b: P_n \to M_n$, $(E,B) \mapsto \{E^j, E^jB \mid 0 < j < 2n\}$

iii) Für $\mathfrak{f} \in F_{2n}^*$ sei $P_n(\mathfrak{f}) := a^{-1}(L_{2n}^*(\mathfrak{f}))$

und $M_n(\mathfrak{f}) := b(P_n(\mathfrak{f}))$.

iv) (E,B) und $(E',B') \in P_n$ heißen Γ-konjugiert, in Zeichen $(E,B) \sim (E',B')$, wenn es $M \in \Gamma$ gibt mit $MEM^{-1} = E'$ und $MBM^{-1} = B'$.

v) Die Restklasse von $G \in M_n$ (bzw. $(E,B) \in P_n$) in $M_n/\sim$ (bzw. $P_n/\sim$) bezeichnen wir mit $\overline{G}$ (bzw. $\overline{(E,B)}$).

(22.4) Lemma: i) Seien (E,B) und $(E',B') \in P_n$. Wenn $(E,B) \sim (E',B')$, dann ist $a(E,B) \sim a(E',B')$ und $b(E,B) \sim b(E',B')$.

ii) a und b sind surjektiv.

iii) Seien $\mathfrak{f}$ und $\mathfrak{f}' \in F_{2n}^*$ und sei $\mathfrak{f} \neq \mathfrak{f}'$.

Dann ist $P_n(\mathfrak{f}) \cap P_n(\mathfrak{f}') = \emptyset$.

Wenn $n > 2$, ist außerdem $M_n(\mathfrak{f}) \cap M_n(\mathfrak{f}') = \emptyset$.

iv) Seien $\mathfrak{f}$ und $\mathfrak{f}' \in F_{2n}^*$ und sei $\mathfrak{f} \neq \mathfrak{f}'$.

Ist $(E,B) \in P_n(\mathfrak{f})$ und $(E',B') \in P_n(\mathfrak{f}')$, so ist $(E,B) \not\sim (E',B')$.

Ist $D \in M_n(\mathfrak{f})$ und $D' \in M_n(\mathfrak{f}')$ sowie $n > 2$, so ist $D \not\sim D'$.

Bew.: i) klar, ii) klar

iii) Da $L_{2n}^*(\mathfrak{f}) \cap L_{2n}^*(\mathfrak{f}') = \emptyset$, folgt $P_n(\mathfrak{f}) \cap P_n(\mathfrak{f}') = \emptyset$ aus der Definition.

Sei $n > 2$ und sei $D \in M_n(\mathfrak{f}) \cap M_n(\mathfrak{f}')$.

Dann gibt es $(E,B) \in P_n(\mathfrak{f})$ und $(E',B') \in P_n(\mathfrak{f}')$ mit $b(E,B) = b(E',B') = D$.

Da nach (15.3) D nur eine 2n-zyklische Untergruppe enthält und diese genau zwei Erzeuger mit Spur $\zeta_{2n}+\zeta_{2n}^{-1}$ hat (siehe 15.4.ii), ist

entweder $E = E'$ oder $D = E'^{-1}$, also ist $E \in \{E',E'^{-1}\} \subset L_{2n}^*(\mathfrak{f}')$ $\lightning$.

iv) Wegen $E \in L_{2n}^*(\mathfrak{f})$ und $E' \in L_{2n}^*(\mathfrak{f}')$ folgt die erste Beh. mit (16.2).

zur zweiten Beh.: Wir nehmen an, daß $D \sim D'$, also $D' = MDM^{-1}$ mit $M \in \Gamma$.

Es gibt $(E,B) \in P_n(\mathfrak{f})$ mit $b(E,B) = D$.

Dann ist $(MEM^{-1},MBM^{-1}) \in P_n(\mathfrak{f})$ und $b(MEM^{-1},MBM^{-1}) = D'$, also $D' \in M_n(\mathfrak{f})$ $\lightning$.

(22.5) Definition: i) Sei $\overline{a}: P_n/\sim \to L_{2n}^*/\sim$ die durch a induzierte Quotientenabbildung.

ii) Sei $\overline{b}: P_n/\sim \to M_n/\sim$ die durch b induzierte Quotientenabbildung.

iii) Sei $p_n(\mathfrak{f}) := p_n(\mathfrak{M},\mathfrak{f}) := \#\#(P_n(\mathfrak{f})/\sim)$ und für $n > 2$ sei

$\mu_n(\mathfrak{f}) := \mu_n(\mathfrak{M},\mathfrak{f}) := \#\#(M_n(\mathfrak{f})/\sim)$. $(\mathfrak{f} \in F_{2n}^*)$

(22.6) Lemma: i) $\bar{a}$ und $\bar{b}$ sind surjektiv.

ii) Für $\mathfrak{f} \in F_{2n}^*$ ist $P_n(\mathfrak{f})/\sim \; = \bar{a}^{-1}(L_{2n}^*(\mathfrak{f})/\sim)$

Falls $n > 2$, ist außerdem $P_n(\mathfrak{f})/\sim \; = \bar{b}^{-1}(M_n(\mathfrak{f})/\sim)$

iii) Falls $n > 2$, ist $\mu_n = \dot{\bigcup}_{\mathfrak{f} \in F_{2n}^*} \mu_n(\mathfrak{f})$

Bew.: klar

(22.7) Definition: Für $\mathfrak{f} \in F_{2n}^*$ sei

$$q_n(\mathfrak{f}) := \begin{cases} 2, \text{ falls } \zeta_{4n}+\zeta_{4n}^{-1} \in k \text{ und } \mathfrak{f} \in F_{4n}^* \\ 1, \text{ sonst} \end{cases}$$

Bemerkung: Die Definition ist sinnvoll, denn falls $\zeta_{4n}+\zeta_{4n}^{-1} \in k$, ist $((\zeta_{2n}-\zeta_{2n}^{-1})^2, -1)_k \cong_k ((\zeta_{4n}-\zeta_{4n}^{-1})^2, -1)_k$ wegen $(\zeta_{2n}-\zeta_{2n}^{-1})^2 = (\zeta_{4n}-\zeta_{4n}^{-1})^2 \cdot (\zeta_{4n}+\zeta_{4n}^{-1})^2$. Wie man leicht sieht, ist dann außerdem $K \cong_k k[X]/\langle X^2 - (\zeta_{4n}+\zeta_{4n}^{-1})X + 1\rangle k[X]$.

(22.8) Lemma: Sei $n > 2$. Für $\mathfrak{f} \in F_{2n}^*$ ist $\mu_n(\mathfrak{f}) = 1/2 \cdot q_n(\mathfrak{f}) \cdot p_n(\mathfrak{f})$.

Bew.: Wegen $p_n(\mathfrak{f}) = \dot{\bigcup}_{\overline{D} \in M_n(\mathfrak{f})/\sim} \# (\bar{b}^{-1}(\overline{D}))$ genügt es zu zeigen, daß $\# \bar{b}^{-1}(\overline{D}) = 2 \cdot q_n(\mathfrak{f})^{-1}$ für $D \in M_n(\mathfrak{f})$.

Es gibt $(E,B) \in P_n(\mathfrak{f})$ mit $b(E,B) = D$.

Da D nur eine 2n-zyklische Untergruppe enthält, sieht man leicht, daß

$b^{-1}(D) = \{(E,E^iB) \mid 0 \leq i < 2n\} \cup \{(E^{-1},E^iB) \mid 0 \leq i < 2n\}$.

Wie im Beweis von (15.8.iv) oder (22.9.ii) folgt daraus:

$\bar{b}^{-1}(\overline{D}) = \overline{b^{-1}(D)} = \{\overline{(E,E^iB)} \mid 0 \leq i < 2n\} \cup \{\overline{(E^{-1},E^iB)} \mid 0 \leq i < 2n\}$.

Es ist $B \in \Gamma$ und für $0 \leq i < 2n$ ist $BE^{-1}B^{-1} = E$ und $BE^iBB^{-1} = E^{2n-i}B$.

Daher wird $\bar{b}^{-1}(\overline{D}) = \{\overline{(E,E^iB)} \mid 0 \leq i < 2n\}$.

Für $0 \leq j < n$ ist $E^j \in \Gamma$ und $E^jEE^{-j} = E$ und $E^jBE^{-j} = E^{2j}B$

sowie $E^jEE^{-j} = E$ und $E^j(EB)E^{-j} = E^{2j+1}B$.

Daher wird $\bar{b}^{-1}(\overline{D}) = \{\overline{(E,B)}, \overline{(E,EB)}\}$.

Wir müssen noch zeigen: $(E,B) \sim (E, EB)$ genau dann, wenn $q_n(\mathfrak{f}) = 2$.

Wenn $g_n(\wp) = 2$ ist, gibt es $E' \in \Gamma \cap k[E]$ mit $S(E') = \zeta_{4n}+\zeta_{4n}^{-1}$.
Daraus folgt leicht $S(E'^2) = \zeta_{2n}+\zeta_{2n}^{-1}$, also $E'^2 = E^{\pm 1}$.
Sei o.B.d.A. $E'^2 = E$ (sonst ersetzen wir E' durch E'^{-1}).
Dann wir $E'EE'^{-1} = E$ und $E'BE'^{-1} = E'BE'^{*} = E'^2B = EB$.

Wenn umgekehrt $(E,B) \sim (E,EB)$, gibt es $M \in \Gamma$ mit $MEM^{-1} = E$ und $MBM^{-1} = EB$. Wegen (3.2) ist $M \in k[E]$, also wird $EB = MBM^{-1} = M^2B$, d.h. $E = M^2$. Daher ist M Nullstelle des Polynoms
$X^4 - (\zeta_{2n}+\zeta_{2n}^{-1})X^2 + 1 = \left(X^2 - (\zeta_{4n}+\zeta_{4n}^{-1})X + 1\right)\cdot\left(X^2 + (\zeta_{4n}+\zeta_{4n}^{-1})X + 1\right)$.
Da $N(M) = 1$, muß $S(M) = \pm (\zeta_{4n}+\zeta_{4n}^{-1})$ sein.
Sei o.B.d.A. $S(M) = \zeta_{4n}+\zeta_{4n}^{-1}$ (sonst ersetzen wir M durch $-M$).
Dann erzeugen M und B eine $2n$-Diedergruppe in Γ und es ist
$\wp = f(\mathfrak{M} \cap k[E]) = f(\mathfrak{M} \cap k[M]) \in F_{4n}^{*}$.

(22.9) Lemma:
i) Für $\wp \in F_{2n}^{*}$ ist $p_n(\wp) = \overline{\overline{E \in L_{2n}^{*}(\wp)/\sim}} \neq \overline{a}^{-1}(\overline{E})$

ii) Für $E \in L_{2n}^{*}$ gilt: $\overline{a}^{-1}(\overline{E}) = \overline{a^{-1}(E)}$.

Bew.: i) klar
ii) " $\supset$ " klar
" $\subset$ ": Sei $\overline{(E',B')} \in \overline{a}^{-1}(\overline{E})$, also $\overline{E'} = \overline{a(E',B')} \in \overline{a}(\overline{a}^{-1}(\overline{E})) = \{\overline{E}\}$.
Dann gibt es $M \in \Gamma$ mit $E = ME'M^{-1}$. Wenn wir $B := MB'M^{-1}$ setzen,
so wird $B \in \Gamma$ und $\overline{(E',B')} = \overline{(E,B)} \in \overline{a^{-1}(E)}$.

(22.10) Lemma: Sei $\wp \in F_{2n}^{*}$. Sei $E \in L_{2n}^{*}(\wp)$ und sei $B \in \Gamma$ mit $BEB^{-1} = E^{-1}$.
Durch die Abbildung $\chi: \Gamma \cap k[E] \to a^{-1}(E)$
$M \mapsto (E,MB)$
wird eine bijektive Abbildung $\overline{\chi}: (\Gamma \cap k[E])/(\Gamma \cap k[E])^{(2)} \to \overline{a}^{-1}(\overline{E})$
induziert.

Bew.: Zunächst gilt für $M \in \Gamma \cap k[E]$:
$MB \in \Gamma$ und $(MB)E(MB)^{-1} = ME^{-1}M^{-1} = E^{-1}$, also tatsächlich Bild $\chi \subset a^{-1}(E)$.
Wohldefiniertheit:
Seien M, $M' \in \Gamma \cap k[E]$ und $M' = ML^2$ mit $L \in \Gamma \cap k[E]$.
Dann ist $LEL^{-1} = E$ und $L(MB)L^{-1} = L^2MB = M'B$, also $(E,MB) \sim (E,M'B)$.

Injektivität: Seien $M, M' \in \Gamma \cap k[E]$ und sei $(E,MB) \sim (E,M'B)$.
Dann gibt es $L \in \Gamma$ mit $LEL^{-1} = E$ und $LMBL^{-1} = M'B$.
Nach (3.2) ist $L \in \Gamma \cap k[E]$. Also wird $M'B = LMBL^{-1} = L^2MB$, d.h.
$M' = L^2M = ML^2$.
Surjektivität: Sei $(E,B') \in a^{-1}(E)$.
Dann ist $B'EB'^{-1} = BEB^{-1} = E^{-1}$, also $B^{-1}B'E = EB^{-1}B'$.
Nach (3.2) ist $B^{-1}B' \in \Gamma \cap k[E]$, also gibt es $M \in \Gamma \cap k[E]$
mit $B^{-1}B' = M^*$, d.h. $B' = BM^* = MB$.

(22.11) Definition: Sei r die Zahl der reellen, s die Zahl der komplexen Primstellen von k, insbesondere also $r + 2s = [k : \mathbb{Q}]$.

(22.12) Lemma: Sei $\mathfrak{f} \in F_{2n}^*$ und $E \in L_{2n}^*(\mathfrak{f})$. Dann ist
$\left[(\Gamma \cap k[E]) : (\Gamma \cap k[E])^{(2)}\right] = 2^s{}_K$.

Bew.: $\Gamma \cap k[E]$ ist abelsche Gruppe, also direktes Produkt seiner Torsionsuntergruppe, die hier Z heißen soll, mit einer freien abelschen Gruppe F.
Nun ist $\left[(\Gamma \cap k[E]) : (\Gamma \cap k[E])^{(2)}\right] = \left[Z : Z^{(2)}\right] \cdot \left[F : F^{(2)}\right]$
und $\left[F : F^{(2)}\right] = 2^{\text{rang } F} = 2^{\text{rang } (\Gamma \cap k[E])}$.
i) $k[E]$ sei Körper. $k[E]$ hat keine reellen Primstellen.
Da $[k[E] : \mathbb{Q}] = 2\,[k : \mathbb{Q}] = 2 \cdot (r + 2s)$, hat $k[E]$ genau $r + 2s$ komplexe Primstellen. Nach dem Dirichletschen Einheitensatz ist
rang $\mathfrak{O}^\times = r + 2s - 1$, wobei $\mathfrak{O} := \mathfrak{M} \cap k[E]$.
Ebenfalls nach dem Dirichletschen Einheitensatz ist rang $\mathfrak{o}^\times = r + s - 1$.
Wir betrachten die Normabbildung $N: \mathfrak{O}^\times \to \mathfrak{o}^\times$. Dann ist
$\Gamma \cap k[E] = N^{-1}(1)$. Wir haben also eine exakte Sequenz:
$\{1\} \to (\Gamma \cap k[E]) \hookrightarrow \mathfrak{O}^\times \xrightarrow{N} N(\mathfrak{O}^\times) \to \{1\}$.
Bekanntlich folgt daraus: rang $(\Gamma \cap k[E])$ - rang $\mathfrak{O}^\times$ + rang $N(\mathfrak{O}^\times) = 0$.
Wegen $\mathfrak{o}^\times \subset \mathfrak{O}^\times$ ist $\mathfrak{o}^{\times(2)} = N(\mathfrak{o}^\times) \subset N(\mathfrak{O}^\times) \subset \mathfrak{o}^\times$.
Da rang $\mathfrak{o}^{\times(2)}$ = rang $\mathfrak{o}^\times$, wird rang $N(\mathfrak{O}^\times)$ = rang $\mathfrak{o}^\times$ und deshalb:
rang $(\Gamma \cap k[E])$ = rang $\mathfrak{O}^\times$ - rang $\mathfrak{o}^\times = s$.
Nach dem Dirichletschen Einheitensatz ist Z Untergruppe der zyklischen Gruppe der Einheitswurzeln aus $\mathfrak{O}^\times$, also ist Z selber zyklisch.
Da $-1 \in Z$, ist $\neq Z$ gerade, also $\left[Z : Z^{(2)}\right] = 2$.

ii) Sei $k[E] = ke_1 \oplus ke_2$ mit $k[E]$-Idempotenten e_1, e_2 und sei wieder $\mathcal{O} = \mathfrak{M} \cap k[E]$.
Ist $e := \#(\sigma/\mathfrak{f})^\times$, so ist $A^e \in \mathcal{O}^\times$ für jedes $A \in (\sigma e_1 + \sigma e_2)^\times$ (leichter Beweis). Daher gilt:
$\operatorname{rang} \mathcal{O}^\times = \operatorname{rang} (\sigma e_1 + \sigma e_2)^\times = 2 \operatorname{rang} \sigma^\times = 2(r+s-1)$
Wie in i) haben wir eine exakte Sequenz
$\{1\} \to (\Gamma \cap k[E]) \hookrightarrow \mathcal{O}^\times \to N(\mathcal{O}^\times) \to \{1\}$ und deshalb
$\operatorname{rang}(\Gamma \cap k[E]) = \operatorname{rang} \mathcal{O}^\times - \operatorname{rang} \sigma^\times = r+s-1$.
Da $k[E]$ kein Körper ist ($\zeta_{2n} \in k$), hat k keine reellen Primstellen, d.h. $r = 0$.
Zu jedem Element $z \in Z$ gibt es ein eindeutig bestimmtes $\varepsilon \in \sigma^\times$ mit $z = \varepsilon e_1 + \varepsilon^{-1} e_2$. Z ist also isomorph zu einer (zyklischen) Untergruppe der zyklischen Torsionsuntergruppe von $\sigma^\times$.
Da $-1 \in Z$, folgt wieder $[Z : Z^{(2)}] = 2$.

Zusammenfassung der Lemmata (22.6.iii), (22.8), (22.9), (22.10) und (22.12) gibt:

(22.13) Satz: Voraussetzung (22.1). Sei $n > 2$. Dann ist

$$\mu_n(\mathfrak{M}) = 2^{s-1} \cdot \kappa \cdot \sum_{\mathfrak{f} \in F_{2n}^*(\mathfrak{M})} g_n(\mathfrak{f}) \cdot \lambda_{2n}^*(\mathfrak{f})$$

(22.14) Korollar: Sei $d \in \mathbb{N}$ quadratfrei, sei $k = \mathbb{Q}(i\sqrt{d})$ und $Q = (-3, -1)_k$. Sei $\mathfrak{M}$ eine Q-Maximalordnung.

i) Wenn $d = 3$, ist $\mu_3(\mathfrak{M}) = \lambda_6^*(\mathfrak{M}) = 1$.

ii) Wenn $d \neq 3$, ist $\mu_3(\mathfrak{M}) = 2 \cdot \lambda_6^*(\mathfrak{M})$.

Bew.: Es ist $s = 1$ und $F_6^*(\mathfrak{M}) \subset \{\sigma\}$. Da $\zeta_{12} + \zeta_{12}^{-1} = \sqrt{3} \notin k$, ist $g_3(\sigma) = 1$. (vgl. Satz 20.39)

Bemerkung: Wie eine genauere Betrachtung des bisherigen Beweisganges zeigt, ist für $d \neq 3$ jede 6-zyklische Untergruppe von $\Gamma(\mathfrak{M})$ entweder in keiner oder in genau zwei nicht Γ-konjugierten 3-Diedergruppen enthalten.

§ 23 . Berechnung der Konjugationsklassenzahl von zyklischen Gruppen der Ordnung 4, die in Tetraedergruppen enthalten sind.

Da eine 2-Diedergruppe nicht nur eine, sondern genau drei verschiedene 4-zyklische Untergruppen enthält, ist die Methode von § 22 hierfür nicht anwendbar. Stattdessen werden wir mit einem ähnlichen Verfahren im nächsten Paragrafen die Konjugationsklassenzahlen von 2-Dieder- und Tetraedergruppen gleichzeitig berechnen. Dafür müssen wir die Funktion l_4^T kennen, die wir in diesem Paragrafen untersuchen werden. § 23 hat einen ähnlichen Aufbau wie § 18 und vergleichbare Ergebnisse. Einige Beweise können direkt übernommen werden.
Hauptergebnis sind die Sätze (23.22) und (23.26).

Wir machen folgende Generalvoraussetzung, die wie in § 18 für den ganzen Paragrafen bis auf einige "lokale" Lemmata über optimale Einbettung gelten soll.

(23.1) Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$, sei k nicht total reell. Sei $Q = (-1, -1)_k$ und $K = k[X]/(X^2+1)k[X]$.

(23.2) Definition: Sei $\mathfrak{M}$ eine Q-Maximalordnung.

i) Sei $\Lambda_4^T(\mathfrak{M}) := \left\{ G \in \Lambda_4(\mathfrak{M}) \;\middle|\; \begin{array}{l} \text{Es gibt eine Tetraedergruppe } G' \\ \text{mit } G \subset G' \subset \Gamma(\mathfrak{M}) \end{array} \right\}$

ii) Sei $L_4^T(\mathfrak{M}) := c^{-1}(\Lambda_4^T(\mathfrak{M}))$
(Dabei sei c die in (15.2.v) definierte Abbildung)

Es gilt ein (15.6.ii) entsprechendes Lemma. Wir können also definieren:

(23.3) Definition: Ist $\mathfrak{M}$ eine Q-Maximalordnung, dann sei
$\lambda_4^T(\mathfrak{M}) := \#\,(\Lambda_4^T(\mathfrak{M})/\sim)$ und $l_4^T(\mathfrak{M}) := \#\,(L_4^T(\mathfrak{M})/\sim)$.

Folgendes Lemma ist leicht einzusehen (vgl. 15.10.i)

(23.4) Lemma: Sei $\mathfrak{M}$ eine Q-Maximalordnung.

i) $L_4^T(\mathfrak{M}) = \left\{ U \in \Gamma(\mathfrak{M}) \;\middle|\; \begin{array}{l} S(U) = 0 \text{ und es gibt } V \in \Gamma(\mathfrak{M}) \text{ mit } UV = -VU, \\ \text{so daß } 1/2\cdot(1+U+V+UV) \in \Gamma(\mathfrak{M}). \end{array} \right\}$

ii) $\overline{c}$ induziert eine Bijektion $\overline{c}: L_4^T(\mathfrak{M})/\sim \;\to\; \Lambda_4^T(\mathfrak{M})/\sim$.

Insbesondere ist $\lambda_4^T(\mathfrak{M}) = l_4^T(\mathfrak{M})$.

Lemma (16.2) gilt für L_4^T entsprechend. Wir können also definieren:

(23.5) Definition: Sei $\mathfrak{M}$ eine Q-Maximalordnung. Dann definieren wir:

i) Für $\mathfrak{f} \in I^k$ sei $L_4^T(\mathfrak{M}, \mathfrak{f}) := L_4^T(\mathfrak{M}) \cap L_4(\mathfrak{M}, \mathfrak{f})$

$= \{U \in L_4^T(\mathfrak{M}) \mid f(\mathfrak{M} \cap k[U]) = \mathfrak{f}\}$

und $1_4^T(\mathfrak{M}, \mathfrak{f}) := \#\,(L_4^T(\mathfrak{M}, \mathfrak{f})/\sim)$

ii) $F_4^T(\mathfrak{M}) := \{\mathfrak{f} \in I^k \mid L_4^T(\mathfrak{M}, \mathfrak{f}) \neq \emptyset\}$

(23.6) Lemma: Sei $\mathfrak{M}$ eine Q-Maximalordnung. Dann gilt:

i) $1_4^T(\mathfrak{M}) = \sum_{\mathfrak{f} \in F_4^T(\mathfrak{M})} 1_4^T(\mathfrak{M}, \mathfrak{f})$

ii) Ist $\mathfrak{M}'$ eine Q-Maximalordnung vom gleichen Typ wie $\mathfrak{M}$, dann ist $F_4^T(\mathfrak{M}') = F_4^T(\mathfrak{M})$ und für alle $\mathfrak{f} \in F_4^T(\mathfrak{M})$ ist $1_4^T(\mathfrak{M}, \mathfrak{f}) = 1_4^T(\mathfrak{M}', \mathfrak{f})$.

iii) $F_4^T(\mathfrak{M}) \subset F_4^*(\mathfrak{M})$

Bew.: klar

(23.7) Lemma: Sei k ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und Primelement π. Sei $Q \underset{k}{\cong} M_2(k)$ und seien D_{11}, D_{12}, D_{21}, $D_{22} \in Q$ Matrizeseinheiten. Genau dann ist $\mathfrak{M}$ eine Q-Maximalordnung mit $D_{11} \in \mathfrak{M}$, wenn es $r \in \mathbb{Z}$ gibt mit $\mathfrak{M} = \mathfrak{o}D_{11} + \mathfrak{o}D_{22} + \pi^r \mathfrak{o}D_{21} + \pi^{-r}\mathfrak{o}D_{12}$.

Bew.: $K := kD_{11} \oplus kD_{22}$ ist halbeinfache quadratische Erweiterung von k. Die Q-Maximalordnungen $\mathfrak{M}$ mit $D_{11} \in \mathfrak{M}$ sind genau die, die die Hauptordnung $\mathfrak{O} := \mathfrak{o}D_{11} + \mathfrak{o}D_{22}$ von K optimal enthalten.
$\mathfrak{M}_0 := \mathfrak{o}D_{11} + \mathfrak{o}D_{22} + \mathfrak{o}D_{12} + \mathfrak{o}D_{21}$ ist Q-Maximalordnung mit $D_{11} \in \mathfrak{M}$.
Sei $\mathfrak{M}$ eine Q-Maximalordnung. Nach (11.6) ist genau dann $D_{11} \in \mathfrak{M}$, wenn es $M \in K^\times$ gibt mit $\mathfrak{M} = M\mathfrak{M}_0M^{-1}$.
Wir können o.B.d.A. annehmen, daß $M = D_{11} + \pi^r D_{22}$ mit $r \in \mathbb{Z}$ (man ersetze M durch $M\pi^s\varepsilon$ mit geeignetem $s \in \mathbb{Z}$ und $\varepsilon \in \mathfrak{O}^\times$).
Die Beh. folgt jetzt mit direkter Rechnung.

(23.8) Lemma: Sei k ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und Primelement π. Sei π Teiler von 2 und $2 = \pi^r\varepsilon$ mit $\varepsilon \in \mathfrak{o}^\times$.
Das Polynom $X^2 - X + 1$ zerfalle in k.
Sei $Q \underset{K}{\cong} M_2(k) \underset{k}{\cong} (-1, -1)_k$ eine k-Quaternionenalgebra und seien $U, V \in \Gamma(Q)$ mit $S(U) = S(V) = 0$ und $W := UV = -VU$.
Sei $T := 1/2 \cdot (1 + U + V + W)$.
Dann gibt es Matrizeseinheiten $\begin{pmatrix}1&0\\0&0\end{pmatrix}$, $\begin{pmatrix}0&1\\0&0\end{pmatrix}$, $\begin{pmatrix}0&0\\1&0\end{pmatrix}$, $\begin{pmatrix}0&0\\0&1\end{pmatrix} \in Q$, so daß gilt:

Eine Q-Maximalordnung $\mathfrak{M}$ enthält genau dann die Elemente U und T (und daher die von U und T erzeugte Tetraedergruppe), wenn

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{o} & \pi^{-s}\mathfrak{o} \\ \pi^{s}\mathfrak{o} & \mathfrak{o} \end{pmatrix} \quad \text{mit } 0 < s < r.$$

Bew.: Sei $x \in k$ mit $x^2 - x + 1 = 0$. Dann ist $x \in \mathfrak{o}^\times$.
Seien $D_{11}, D_{12}, D_{21}, D_{22} \in Q$ Matrizeseinheiten. Wir definieren:

$U' := 1/3 \cdot (2x - 1) \cdot D_{11} - 1/3 \cdot D_{12} + 2 \cdot D_{21} + 1/3 \cdot (-2x + 1) \cdot D_{22}$ und

$V' := 1/3 \cdot (2x - 1) \cdot D_{11} + 1/3 \cdot (-x + 1) \cdot D_{12} - 2x \cdot D_{21} + 1/3 \cdot (-2x + 1) \cdot D_{22}$

Man kann leicht direkt nachrechnen, daß U' und V' eine 2-Diedergruppe erzeugen. Es gibt daher einen k-Algebrenautomorphismus $\sigma: Q \to Q$ mit $\sigma U' = U$ und $\sigma V' = V$. Dann sind
$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} := \sigma D_{11}$, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} := \sigma D_{12}$, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} := \sigma D_{21}$, $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} := \sigma D_{22}$
Matrizeseinheiten und wir erhalten:

$$U = \begin{pmatrix} 1/3 \cdot (2x - 1) & -1/3 \\ 2 & 1/3 \cdot (-2x + 1) \end{pmatrix}, \quad V = \begin{pmatrix} 1/3 \cdot (2x - 1) & 1/3 \cdot (-x + 1) \\ -2x & 1/3 \cdot (-2x + 1) \end{pmatrix}$$

$$W = \begin{pmatrix} 1/3 \cdot (2x - 1) & 1/3 \cdot x \\ 2 \cdot (x - 1) & 1/3 \cdot (-2x + 1) \end{pmatrix}, \quad T = \begin{pmatrix} x & 0 \\ 0 & -x + 1 \end{pmatrix}.$$

Ist $\mathfrak{M}$ eine Q-Maximalordnung, die U und T enthält, so enthält sie auch $(x^2 + x)^{-1} \cdot (x^2 + T) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, da $x^2 + x = 2x - 1 \in \mathfrak{o}^\times$.

Nach (23.7) ist also $\mathfrak{M} = \begin{pmatrix} \mathfrak{o} & \pi^{-s}\mathfrak{o} \\ \pi^{s}\mathfrak{o} & \mathfrak{o} \end{pmatrix}$ mit $s \in \mathbb{Z}$.

Wegen $U \in \mathfrak{M}$ und $-1/3 \in \mathfrak{o}^\times$ muß $s > 0$ sein.
Wegen $U \in \mathfrak{M}$ und $2\pi^{-r} \in \mathfrak{o}^\times$ muß $s < r$ sein.
Umgekehrt sieht man leicht, daß die angegebenen Maximalordnungen sowohl U als auch T enthalten.

(23.9) Lemma: gleiche Voraussetzung wie in (23.8).
i) Ist $\mathfrak{M}$ eine Q-Maximalordnung mit $U \in \mathfrak{M}$ und $T \in \mathfrak{M}$, so gilt:
$2\mathfrak{o} \mid D_k(k[U]) \cdot f(\mathfrak{M} \cap k[U])^2 \mid 4\mathfrak{o}$.
ii) Es gibt ein System $\{ \mathfrak{M}^f \mid f \in I^k \text{ und } 2\mathfrak{o} \mid D_k(k[U]) \cdot f^2 \mid 4\mathfrak{o} \}$ von Q-Maximalordnungen, so daß für alle $f, f' \in I^k$ mit $2\mathfrak{o} \mid D_k(k[U]) \cdot f^2 \mid 4\mathfrak{o}$ und $2\mathfrak{o} \mid D_k(k[U]) \cdot f'^2 \mid 4\mathfrak{o}$ gilt:
$U \in \mathfrak{M}^f$, $T \in \mathfrak{M}^f$ und $f(\mathfrak{M} \cap k[U]) = f$ sowie
$N(\mathfrak{M}^f \mathfrak{M}^{f'}) = f^{-1}f' + f f'^{-1}$, insbesondere also $N(\mathfrak{M}^f \mathfrak{M}^{f'}) f f'^{-1} \in I^{k(2)}$.

iii) Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $U \in \mathfrak{M}$ und $T \in \mathfrak{M}$.
Sei $\mathfrak{M}'$ eine weitere Q-Maximalordnung.
Genau dann ist $U \in \mathfrak{M}'$ und $T \in \mathfrak{M}'$ und $\mathfrak{M}' \cap k[U] = \mathfrak{M} \cap k[U]$,
wenn $\mathfrak{M}' = \mathfrak{M}$ oder $\mathfrak{M}' = (1 + U) \cdot \mathfrak{M} \cdot (1 + U)^{-1}$.

Bew.: Wir benutzen die gleichen Bezeichnungen wie im Beweis von (23.8).

i) Für $0 \leq s \leq r$ sei $\mathfrak{M}_s = \begin{pmatrix} o & \pi^{-s} o \\ \pi^s o & o \end{pmatrix}$. Wir müssen zeigen,
daß $2o \mid D_k(\mathfrak{M}_s \cap k[U]) \mid 4o$ für alle $0 \leq s \leq r$.
Sei $f(o[U]) =: \pi^t o$ und sei $\{1, \omega\}$ Basis von $\mathcal{O}^o(k[U])$ über o.
Dann gibt es $\alpha \in o^\times$ und $\beta \in o$ mit $\pi^t \omega = \alpha U + \beta$ (siehe Bew. 18.5.ii.a),
also $\pi^t \omega = \begin{pmatrix} \alpha/3 \cdot (2x - 1) + \beta & -\alpha/3 \\ 2\alpha & \alpha/3 \cdot (-2x + 1) + \beta \end{pmatrix}$.
Sei $s' = \min\{s, r-s\}$. Dann ist offensichtlich $\pi^{t-s'-1} \omega \notin \mathfrak{M}_s$.
Also ist $D_k(\mathfrak{M}_s \cap k[U])$ Vielfaches von $D_k(1, \pi^{t-s'} \omega) o = \pi^{-2s'} \cdot 4o$.
Da andererseits $\{1, U-1\}$ Basis von $o[U]$ über o ist und
$\pi^{-s'} \cdot (U-1) = \pi^{-s'} \cdot \begin{pmatrix} 2 \cdot (x-2)/3 & -1/3 \\ 2 & 2 \cdot (-x-1)/3 \end{pmatrix} \in \mathfrak{M}_s$, ist genau
$D_k(\mathfrak{M}_s \cap k[U]) = 4\pi^{-2s'} o$. Wegen $0 < 2s' \leq r$ folgt die Behauptung.

ii) Sei $\mathfrak{f} \in \Gamma^k$ und $2o \mid D_k(k[U]) \cdot \mathfrak{f}^2 \mid 4o$.
Sei $s \in \mathbb{Z}$ so bestimmt, daß $f(o[U]) \mathfrak{f}^{-1} = \pi^s o$.
Dann wird $s \geq 0$ und $D_k(k[U]) \cdot \mathfrak{f}^2 = 4 \cdot \pi^{-2s} o$, nach Vor. also $2s < r$
und insbesondere $s = \min\{s, r-s\}$.
Wir setzen $\mathfrak{M}^{\mathfrak{f}} := \mathfrak{M}_s$. Die Behauptungen folgen jetzt leicht.

iii) Falls $\mathfrak{M}' = (1+U) \cdot \mathfrak{M} \cdot (1+U)^{-1}$, folgt sofort $\mathfrak{M}' \cap k[U] = \mathfrak{M} \cap k[U]$.
Aus $(1+U)V(1+U)^{-1} = W$ folgt leicht, daß Konjugation mit $(1+U)$ einen
Automorphismus der durch U und T erzeugten Tetraedergruppe induziert.
Daher sind dann $U \in \mathfrak{M}'$ und $T \in \mathfrak{M}'$.
Sei umgekehrt $U \in \mathfrak{M}'$, $T \in \mathfrak{M}'$ und $\mathfrak{M}' \cap k[U] = \mathfrak{M} \cap k[U]$.
Wir können annehmen, daß $\mathfrak{M} \neq \mathfrak{M}'$ (andernfalls ist nichts mehr zu zeigen).
Es gibt $0 < s < r$ mit $\mathfrak{M} = \mathfrak{M}_s$. Dann muß $\mathfrak{M}' = \mathfrak{M}_{r-s}$ sein.
Wegen $\mathfrak{M} \neq \mathfrak{M}'$ ist außerdem $s \neq r-s$, d.h. $2s \neq r$.
Wenn wir zeigen können, daß $(1+U) \cdot \mathfrak{M}_s \cdot (1+U)^{-1} \neq \mathfrak{M}_s$, folgt daraus
$\mathfrak{M}' = (1+U) \cdot \mathfrak{M} \cdot (1+U)^{-1}$ (es bleibt keine andere Wahl).

Wir nehmen an, daß $(1+U)\,\mathfrak{M}_s = \mathfrak{M}_s(1+U)$ (und führen dies zum Widerspruch).
$\mathfrak{M}_s(1+U)$ ist zweiseitiges $\mathfrak{M}_s$-Ideal.
Nach (9.11.ii) gibt es $u \in \mathbb{Z}$ mit $\mathfrak{M}_s(1+U) = \mathfrak{M}_s\,\pi^u$,
also ist $1 + U = \pi^u\varepsilon'$ mit $\varepsilon' \in \mathfrak{M}_s^\times$.
Dann ist $\pi^r\varepsilon = 2 = N(1+U) = \pi^{2u}N(\varepsilon')$, also $2u = r$ und $N(\varepsilon') = \varepsilon$.

Es ist $\begin{pmatrix} 2\cdot\pi^{-u}\cdot(x+1)/3 & -\pi^{-u}\cdot 1/3 \\ 2\cdot\pi^{-u} & 2\cdot\pi^{-u}\cdot(-x+2)/3 \end{pmatrix} = \pi^{-u}(1+U) = \varepsilon' \in \mathfrak{M}_s$,

also $r-u \geq s$ und $-u \geq -s$. D.h. $u \geq s$ und $u \leq s$, also $s = u = r/2$ ↯.

(23.10) Lemma: Sei k ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und Primelement π. Sei π Teiler von 2 und $2 = \pi^{2r}\varepsilon$ mit $\varepsilon \in \mathfrak{o}^\times$.
Die Kongruenz $x^2 - x + 1 \equiv 0 \bmod \pi$ sei unlösbar in $\mathfrak{o}$.
Sei $Q \underset{k}{\cong} M_2(k) \underset{k}{\cong} (-1, -1)_k$ eine k-Quaternionenalgebra und seien
$U, V \in \Gamma(Q)$ mit $S(U) = S(V) = 0$ und $W := UV = -VU$.
Sei $T := 1/2\cdot(1 + U + V + W)$.
Dann gibt es genau eine Q-Maximalordnung $\mathfrak{M}$, die U und T enthält.
Es ist $D_k(k[U])\cdot f(\mathfrak{M} \cap k[U])^2 = D_k(\mathfrak{M} \cap k[U]) = 2\mathfrak{o}$.

Bew.: Man kann leicht nachrechnen, daß der $\mathfrak{o}$-Modul
$\mathfrak{M} = \mathfrak{o} + \pi^{-r}(1+U)\mathfrak{o} + \pi^{-r}(1+V)\mathfrak{o} + T\mathfrak{o}$ eine Q-Ordnung ist.
Es ist $D_k(\mathfrak{M}) = \pi^{-4r}\cdot D_k(1, 1+U, 1+V, T)\mathfrak{o} = \mathfrak{o}$ (siehe 12.6.iv),
also ist $\mathfrak{M}$ eine Q-Maximalordnung. Es sind $U \in \mathfrak{M}$ und $T \in \mathfrak{M}$.
Offensichtlich ist $\mathfrak{M} \cap k[U] = \mathfrak{o} + \pi^{-r}(1+U)\mathfrak{o}$, also
$D_k(\mathfrak{M} \cap k[U]) = \pi^{-2r}\,D_k(1, 1+U)\mathfrak{o} = 2\mathfrak{o}$.
Wir nehmen an, $\mathfrak{M}' \neq \mathfrak{M}$ sei eine Q-Maximalordnung mit $U \in \mathfrak{M}'$ und $T \in \mathfrak{M}'$.
Nach (11.1) gibt es Matrizeseinheiten $\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix} \in Q$

und $s \in \mathbb{N}_0$ mit $\mathfrak{M} = \begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{o} \end{pmatrix}$ und $\mathfrak{M}' = \begin{pmatrix} \mathfrak{o} & \pi^{-s}\mathfrak{o} \\ \pi^s\mathfrak{o} & \mathfrak{o} \end{pmatrix}$.

Da $\mathfrak{M} \neq \mathfrak{M}'$, ist $s > 0$.
Wegen $T \in \mathfrak{M} \cap \mathfrak{M}'$ gibt es $a, b, c, d \in \mathfrak{o}$ mit $T = \begin{pmatrix} a & b \\ \pi^s c & d \end{pmatrix}$

Dann ist $a + d = S(T) = 1$ und $a(1-a) - \pi^s bc = N(T) = 1$,
also $a^2 - a + 1 = -\pi^s bc \equiv 0 \bmod \pi$ ↯.

(23.11) Lemma: Sei k ein $\mathfrak{p}$-adischer Zahlkörper mit Hauptordnung $\mathfrak{o}$ und Primelement π. Ist $P \in \mathfrak{o}[X]$ ein Polynom und $a \in \mathfrak{o}$ mit $P(a) \equiv 0 \bmod \pi$ und $P'(a) \not\equiv 0 \bmod \pi$, dann gibt es $b \in \mathfrak{o}$ mit $P(b) = 0$.

Bew.: siehe /14/ S. 310 Corollary 2

(23.12) Lemma: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$.
Sei $\mathfrak{p}$ ein Primideal in $\mathfrak{o}$ mit $\mathfrak{p} \nmid 2\mathfrak{o}$. Dann sind äquivalent:
i) Das Polynom $X^2 - X + 1$ zerfällt in $\mathfrak{o}_\mathfrak{p}$.
ii) $X^2 - X + 1$ zerfällt in $\mathfrak{o}/\mathfrak{p}$.
iii) $t(\mathfrak{p}) \equiv 0 \bmod 2$

Bew.: i) $\Rightarrow$ ii) klar
ii) $\Rightarrow$ i): Es ist $(X^2 - X + 1)' = 2X - 1$.
Falls $a \in \mathfrak{o}$ mit $a^2 - a + 1 \equiv 0 \bmod \pi$, ist $2a - 1 \not\equiv 0 \bmod \pi$.
Die Behauptung folgt mit (23.11).
ii) $\Leftrightarrow$ iii): Wegen $\mathfrak{p} \mid 2$ ist $x^2 - x + 1 \equiv x^2 + x + 1 \bmod \pi$ für $x \in \mathfrak{o}$.
Es ist $X^3 - 1 = (X - 1)\cdot(X^2 + X + 1)$.
Daß $X^2 - X + 1$ in $\mathfrak{o}/\mathfrak{p}$ zerfällt, ist also äquivalent dazu, daß die zyklische Gruppe $(\mathfrak{o}/\mathfrak{p})^\times$ eine durch 3 teilbare Ordnung hat, d.h. daß

$$2^{t(\mathfrak{p})} - 1 = (\#\,\mathbb{Z}/2\mathbb{Z})^{[\,\mathfrak{o}/\mathfrak{p} \,:\, \mathbb{Z}/2\mathbb{Z}\,]} - 1 = \#\,(\mathfrak{o}/\mathfrak{p}) - 1 = \#\,(\mathfrak{o}/\mathfrak{p})^\times \equiv 0 \bmod 3.$$

Wegen $2 \equiv -1 \bmod 3$ ist dies äquivalent zu $t(\mathfrak{p}) \equiv 0 \bmod 2$.

(23.13) Satz: Voraussetzung (23.1).
i) Sei $\mathfrak{M}$ eine Q-Maximalordnung und $\mathfrak{f} \in F_4^T(\mathfrak{M})$. Dann gilt für die endlichen Primstellen $\mathfrak{p}$ von k:

a) $2\mathfrak{o}_\mathfrak{p} \mid D_k(K)_\mathfrak{p} \cdot \mathfrak{f}_\mathfrak{p}^2 \mid 4\mathfrak{o}_\mathfrak{p}$, falls $\mathfrak{p} \mid 2\mathfrak{o}$ und $t(\mathfrak{p}) \equiv 0 \bmod 2$
b) $D_k(K)_\mathfrak{p} \cdot \mathfrak{f}_\mathfrak{p}^2 = 2\mathfrak{o}_\mathfrak{p}$, falls $\mathfrak{p} \mid 2$ und $t(\mathfrak{p}) \not\equiv 0 \bmod 2$ und $2 \mid v(\mathfrak{p})$ } (23.14)
c) $\mathfrak{f}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}$ für alle anderen endlichen Primstellen $\mathfrak{p}$ von k

ii) Es gibt ein System $\{\mathfrak{M}^\mathfrak{f} \mid \mathfrak{f} \in I^k$ und $\mathfrak{f}$ erfüllt (23.14)$\}$ von Q-Maximalordnungen, so daß für alle $\mathfrak{f}, \mathfrak{f}' \in I^k$, die der Bedingung (23.14) genügen, gilt: $\mathfrak{f} \in F_4^T(\mathfrak{M}^\mathfrak{f})$ und $N(\mathfrak{M}^\mathfrak{f}\mathfrak{M}^{\mathfrak{f}'}) = \mathfrak{f}^{-1}\mathfrak{f}' + \mathfrak{f}\mathfrak{f}'^{-1}$; insbesondere also $N(\mathfrak{M}^\mathfrak{f}\mathfrak{M}^{\mathfrak{f}'})\,\mathfrak{f}\mathfrak{f}'^{-1} \in I^{k(2)}$.

Bew.: i) Es ist $F_4^T(\mathfrak{M}) \subset F_4^*(\mathfrak{M})$. Falls $\mathfrak{p} \nmid 2$ oder falls $\mathfrak{p} \mid 2$ und $t(\mathfrak{p}) \equiv v(\mathfrak{p}) \equiv 1 \bmod 2$, folgt daher die Beh. aus (18.9.i).
Falls $\mathfrak{p} \mid 2$ und $t(\mathfrak{p})\cdot v(\mathfrak{p}) \equiv 0 \bmod 2$, ist Q unverzweigt an der Stelle $\mathfrak{p}$ (siehe 13.4.iii). Die Beh. folgt leicht mit den Lemmata (23.9.i) und (23.10).
ii) Es gibt $U, V \in \Gamma(Q)$ mit $S(U) = S(V) = 0$ und $UV = -VU$.
Sei $T := 1/2\cdot(1 + U + V + UV)$. Man rechnet leicht nach, daß
$\mathcal{O} := \mathfrak{o} + \mathfrak{o}U + \mathfrak{o}V + \mathfrak{o}T$ eine Q-Ordnung mit $U \in \mathcal{O}$ und $T \in \mathcal{O}$ ist.
$\mathcal{O}$ ist in einer Q-Maximalordnung $\mathfrak{M}$ enthalten (4.4).

Mit Hilfe von Lemma (23.9.ii) können wir das System der $\mathfrak{M}^{\mathfrak{f}}$ konstruieren. Wir ändern die $\mathfrak{p}$-Komponenten von $\mathfrak{M}$ für die endlichen Primstellen $\mathfrak{p}$ von k mit $\mathfrak{p} \mid 2$ und $t'(\mathfrak{p}) \equiv 0 \bmod 2$ ab. (vgl. Bew. von 18.9.ii)

(23.15) Definition: Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei $k[U] \cong_k k[X]/(X^2+1)k[X]$ mit $U^2 + 1 = 0$. Sei $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal.

i) Für alle endlichen Primstellen $\mathfrak{p}$ von k definieren wir ein $\mathfrak{O}^{\mathfrak{f}}(k[U])$-Ideal $\mathfrak{a}^{\mathfrak{p}}$ durch die Vorschriften: $\mathfrak{a}^{\mathfrak{p}}_{\mathfrak{p}} = (1+U)\mathfrak{O}^{\mathfrak{f}}_{\mathfrak{p}}$ und $\mathfrak{a}^{\mathfrak{p}}_{\mathfrak{q}} = \mathfrak{O}^{\mathfrak{f}}_{\mathfrak{q}}$ für alle endlichen Primstellen $\mathfrak{q} \neq \mathfrak{p}$ von k.

ii) Sei $X^{\mathfrak{f}}$ die von den $\mathfrak{a}^{\mathfrak{p}}$ erzeugte Gruppe und sei $Y^{\mathfrak{f}} := \left((k \to \mathfrak{f})(I^k)\right) X^{\mathfrak{f}}$.
(Wir schreiben kurz $Y^{\mathfrak{f}}$ statt $Y^{\mathfrak{f}}(k[U])$, da immer entweder klar sein wird, welche Algebra $k[U]$ gemeint ist oder $k[U]$ nur bis auf Isomorphie interessiert, etwa bei Indexberechnungen)

(23.16) Lemma: Voraussetzung (23.1).
Seien $U, V \in \Gamma(Q)$ mit $S(U) = S(V) = 0$ und $UV = -VU$ und sei $T := 1/2 \cdot (1 + U + V + UV)$.
Sei $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal, das der Bedingung (23.14) genügt.
Sei $\mathfrak{O}^{\mathfrak{f}} := \mathfrak{O}^{\mathfrak{f}}(k[U])$ abgekürzt usw.
$\mathfrak{M}$ sei eine Q-Maximalordnung mit $T \in \mathfrak{M}$ und $\mathfrak{M} \cap k[U] = \mathfrak{O}^{\mathfrak{f}}$.
i) Sei $\mathfrak{M}'$ eine Q-Maximalordnung mit $T \in \mathfrak{M}'$ und $\mathfrak{M}' \cap k[U] = \mathfrak{O}^{\mathfrak{f}}$.
Dann gibt es $\mathfrak{a} \in Y^{\mathfrak{f}}$ mit $\mathfrak{M}' = \mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1}$.
ii) Sei $\mathfrak{a} \in Y^{\mathfrak{f}}$. Dann ist $T \in \mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1}$ und $\mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1} \cap k[U] = \mathfrak{O}^{\mathfrak{f}}$.

Bew.: i) Es ist $\mathfrak{U} := \mathfrak{o} + \mathfrak{o}U + \mathfrak{o}V + \mathfrak{o}T \subset \mathfrak{M} \cap \mathfrak{M}'$ und $D_k(\mathfrak{U}) = 4\mathfrak{o}$.
Also ist $\mathfrak{M}_{\mathfrak{p}} = \mathfrak{M}'_{\mathfrak{p}}$ für $\mathfrak{p} \nmid 2$.
Falls $\mathfrak{p} \mid 2$ und $t(\mathfrak{p}) \cdot v(\mathfrak{p}) \equiv 1 \bmod 2$, ist $Q_{\mathfrak{p}}$ Divisionsalgebra, also $\mathfrak{M}_{\mathfrak{p}} = \mathfrak{M}'_{\mathfrak{p}}$ nach (9.11.i).
Falls $\mathfrak{p} \mid 2$ und $t(\mathfrak{p}) \equiv 1 \bmod 2$ und $v(\mathfrak{p}) \equiv 0 \bmod 2$, ist $\mathfrak{M}_{\mathfrak{p}} = \mathfrak{M}'_{\mathfrak{p}}$ nach (23.10).
Mit Hilfe von Lemma (23.9.iii) läßt sich das gesuchte $\mathfrak{a} \in Y^{\mathfrak{f}}$ jetzt leicht konstruieren.
ii) Sei $\mathfrak{p}$ eine endliche Primstelle von k. Da $(1+U)^2 = 2U$ und $U \in \mathfrak{O}^{\mathfrak{f}\times}$, gibt es $a \in k_{\mathfrak{p}}^{\times}$ mit $\mathfrak{a}_{\mathfrak{p}} = a\mathfrak{O}^{\mathfrak{f}}_{\mathfrak{p}}$ oder $\mathfrak{a}_{\mathfrak{p}} = a(1+U)\mathfrak{O}^{\mathfrak{f}}_{\mathfrak{p}}$.
Dann ist $(\mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1})_{\mathfrak{p}} = \mathfrak{M}_{\mathfrak{p}}$ oder $(\mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1})_{\mathfrak{p}} = (1+U)\mathfrak{M}_{\mathfrak{p}}(1+U)^{-1}$,
also $(\mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1})_{\mathfrak{p}} \cap k_{\mathfrak{p}}[U] = \mathfrak{M}_{\mathfrak{p}} \cap k_{\mathfrak{p}}[U]$.
Da Konjugation mit (1+U) einen Automorphismus der durch U und T erzeugten Tetraedergruppe induziert, ist $T \in (\mathfrak{a}\mathfrak{M}\mathfrak{a}^{-1})_{\mathfrak{p}}$.
Die Behauptung folgt mit (4.13).

(23.17) Definition: Gleiche Voraussetzung wie in (23.16).
Dann sei $\mathfrak{M} Y^{\mathfrak{f}}$ die Menge der Ideale $\mathfrak{M}\mathfrak{a}$ mit $\mathfrak{a} \in Y^{\mathfrak{f}}$.

(23.18) Lemma: Gleiche Voraussetzung wie in (23.16).
Es ist $Y^{\mathfrak{f}} \subset A^{\mathfrak{f}}$ und es ist $\mathfrak{M} I^{\mathfrak{M}} \subset \mathfrak{M} Y^{\mathfrak{f}}$, insbesondere also $RI^{k(2)} \subset N(Y^{\mathfrak{f}})$.

Bew.: Da $\Delta(1+U) = (1+U)/(1-U) = U \in \mathcal{O}^{\mathfrak{f}\times}$, folgt $Y^{\mathfrak{f}} \subset A^{\mathfrak{f}}$ leicht aus der Definition von $Y^{\mathfrak{f}}$.
Sei $\mathfrak{p}$ eine endliche Primstelle von k, an der Q (und wegen 13.4.iv auch K) verzweigt ist und sei $\mathfrak{M}\mathfrak{p} = \mathfrak{P}^2$ mit einem Primideal $\mathfrak{P}$ von $\mathfrak{M}$.
Wie im Beweis von (17,8.c) gesehen, ist $\mathfrak{P} = \mathfrak{M}\mathfrak{a}$ mit $\mathfrak{a} \in A^{\mathfrak{f}}$ und $\mathfrak{a}^2 = \mathfrak{p}\mathcal{O}^{\mathfrak{f}}$. Wir müssen zeigen: $\mathfrak{a} \in Y^{\mathfrak{f}}$.
Nach (13.4.iii) ist $v := v(\mathfrak{p})$ ungerade. Es ist $\mathfrak{a}^{2v} = \mathfrak{p}^v \mathcal{O}^{\mathfrak{f}} = (1+U)^2 \mathcal{O}^{\mathfrak{f}}$.
Da $\mathfrak{f} + \mathfrak{p} = \mathfrak{o}$, folgt hieraus: $\mathfrak{a}^v = (1+U)\mathcal{O}^{\mathfrak{f}}$, also
$\mathfrak{a} = \mathfrak{p}^{-(v-1)/2} \cdot (1+U)\mathcal{O}^{\mathfrak{f}} \in Y^{\mathfrak{f}}$.

(23.19) Satz: Voraussetzung (23.1).
Sei $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal, das der Bedingung (23.14) genügt.
Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{f} \in F_4^T(\mathfrak{M})$.
Sei $\mathfrak{M}'$ eine weitere Q-Maximalordnung.
Genau dann ist $\mathfrak{f} \in F_4^T(\mathfrak{M}')$, wenn $N(\mathfrak{M}\mathfrak{M}') \in N(Y^{\mathfrak{f}})S_{\mathfrak{M}}$.

Bew.: ganz analog zum Beweis von (18.16).

Bemerkung: Die Sätze (23.13) und (23.19) gestatten es, eine Übersicht über $F_4^T(\mathfrak{M})$ für alle Maximalordnungstypen $\tilde{\mathfrak{M}}$ zu bekommen.
Die folgenden Sätze (23.22) und (23.23) machen die ganze Sache noch etwas durchsichtiger.

(23.20) Definition: Sei $C \subset I^k$ die Gruppe, die von den Primidealen $\mathfrak{p}$ mit $\mathfrak{p} \nmid 2$ und $v(\mathfrak{p}) \equiv 1 \bmod 2$ erzeugt wird.

(23.21) Lemma: Sei $\mathfrak{f}$ ein ganzes $\mathfrak{o}$-Ideal. Dann ist $N(Y^{\mathfrak{f}}) = CI^{k(2)}$.

Bew.: Sei $\mathfrak{p}$ eine endliche Primstelle von k. Wir müssen zeigen, daß $\mathfrak{p} \in N(Y^{\mathfrak{f}})$ genau dann, wenn $\mathfrak{p} \nmid 2$ und $v(\mathfrak{p}) \equiv 1 \bmod 2$.
Dies folgt leicht aus der Definition von $Y^{\mathfrak{f}}$, da $N(1+U) = 2$ und $2\mathfrak{o}_{\mathfrak{p}}$ genau dann kein Quadrat eines Ideals ist, wenn $v(\mathfrak{p}) \equiv 1 \bmod 2$.

(23.22) Satz: (Voraussetzung 23.1).
Sei $\mathfrak{f} \in I^k$ und $\mathfrak{f}$ erfülle die Bedingung (23.14).
Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{f} \in F_4^T(\mathfrak{M})$.
Sei $\mathfrak{M}'$ eine Q-Maximalordnung und $\mathfrak{f}'$ ein ganzes o-Ideal.
Genau dann ist $\mathfrak{f}' \in F_4^T(\mathfrak{M}')$, wenn $\mathfrak{f}'$ die Bedingung (23.14) erfüllt und $N(\mathfrak{M}\mathfrak{M}')\mathfrak{f}\mathfrak{f}'^{-1} \in CI^{k(2)}S_\mu$.

Bew.: analog zum Beweis von (18.18)

(23.23) Korollar: Voraussetzung (23.1). Seien $\mathfrak{M}$ und $\mathfrak{M}'$ zwei Q-Maximalordnungen.
i) $F_4^T(\mathfrak{M}) \cap F_4^T(\mathfrak{M}') \neq \emptyset \Rightarrow N(\mathfrak{M}\mathfrak{M}') \in CI^{k(2)}S_\mu$
ii) $N(\mathfrak{M}\mathfrak{M}') \in CI^{k(2)}S_\mu \Rightarrow F_4^T(\mathfrak{M}) = F_4^T(\mathfrak{M}')$

Bew.: folgt sofort aus (23.19)

(23.24) Bemerkung:
i) Folgendes Problem bleibt offen: Wie findet man für vorgegebenes $\mathfrak{f} \in I^k$, das die Bedingung (23.14) erfüllt, aus einem gegebenen Repräsentantensystem von $\tilde{Q}$ eine Maximalordnung $\mathfrak{M}$ mit $\mathfrak{f} \in F_4^T(\mathfrak{M})$?

ii) Wir haben F_4^* und F_4^T unabhängig voneinander untersucht in den Paragrafen 18 und 23. Wir kennen F_4^* und F_4^T (bis auf das Problem des Findens einer "Anfangsmaximalordnung"). Aber: Wir kennen i.a. nicht die Produktfunktion (F_4^*, F_4^T) !
Wir wissen, daß $F_4^T(\mathfrak{M}) \subset F_4^*(\mathfrak{M})$ für jede Q-Maximalordnung $\mathfrak{M}$. Aber dieser Satz und die übrigen Sätze aus den Paragrafen 18 und 23 erlauben es (meines Wissens) i.a. nicht, F_4^* und F_4^T eindeutig in Beziehung zueinander zu setzen. Dies ist ein echtes Problem, denn zur Berechnung der Konjugationsklassenzahlen von 2-Dieder- und Tetraedergruppen in einer Maximalordnung $\mathfrak{M}$ braucht man die Kenntnis von $F_4^*(\mathfrak{M})$ und $F_4^T(\mathfrak{M})$.
Für imaginärquadratische Zahlkörper kann man die Beziehung zwischen F_4^* und F_4^T allerdings eindeutig feststellen; siehe Satz (26.12).

iii) Sei $C' \subset I^k$ die Gruppe, die von den Primidealen $\mathfrak{p}$ mit $\mathfrak{p} \mid 2$ und $t(\mathfrak{p}) \equiv v(\mathfrak{p}) \equiv 0 \bmod 2$ erzeugt wird. Mit (23.22) und (23.23) erkennt man leicht, daß es $[C'CI^{k(2)}S_\mu : RI^{k(2)}S_\mu]$ verschiedene Maximalordnungstypen $\tilde{\mathfrak{M}}$ mit $F_4^T(\mathfrak{M}) \neq \emptyset$ gibt.

Diese Menge von Maximalordnungstypen zerfällt in $[C'CI^{k(2)}S_u : CI^{k(2)}S_u]$ Teilmengen mit jeweils $[CI^{k(2)}S_u : RI^{k(2)}S_u]$ Elementen, so daß gilt: Für alle $\tilde{\mathfrak{M}}$ aus einer sochen Teilmenge hat $F_4^T(\mathfrak{M})$ den gleichen Wert. Im Sinne von (10.11) sind die genannten Mengen affine Unterräume von $\tilde{Q}$.

Wir berechnen jetzt $l_4^T(\mathfrak{M}, \mathfrak{f})$ für vorgegebene Maximalordnung $\mathfrak{M}$ und $\mathfrak{f} \in F_4^T(\mathfrak{M})$:

(23.25) Lemma: Sei $\mathfrak{M}$ eine Q-Maximalordnung und sei $\mathfrak{f} \in F_4^T(\mathfrak{M})$. Seien U, V $\in \Gamma(\mathfrak{M})$ mit S(U) = S(V) = = und UV = - VU und T: = 1/2·(1 + U + V + UV) $\in \Gamma(\mathfrak{M})$ sowie $f(\mathfrak{M} \cap k[U]) = \mathfrak{f}$. Sei $\mathcal{O}^{\mathfrak{f}}$: = $\mathcal{O}^{\mathfrak{f}}(k[U])$ abgekürzt usw. Dann gilt:

i) Zu jedem $U' \in L_4^T(\mathfrak{M}, \mathfrak{f})$ gibt es $M \in Q^\times$, so daß $MUM^{-1} = U'$ und $MTM^{-1} \in \mathfrak{M}$.

ii) Sei $M \in Q^\times$. Genau dann ist $MUM^{-1} \in L_4^T(\mathfrak{M}, \mathfrak{f})$ und $MTM^{-1} \in \mathfrak{M}$, wenn es $\mathfrak{a} \in Y^{\mathfrak{f}}$ gibt mit $\mathfrak{M}M = \mathfrak{M}\mathfrak{a}$.

Bew.: analog zum Beweis von (18.20)

(23.26) Satz: (Voraussetzung 23.1).
Sei $\mathfrak{f}$ ein ganzes o-Ideal, das Bedingung (23.14) erfüllt und sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{f} \in F_4^T(\mathfrak{M})$. Dann ist

$$l_4^T(\mathfrak{M}, \mathfrak{f}) = \frac{[Y^{\mathfrak{f}} : Y^{\mathfrak{f}} \cap H^{\mathfrak{f}}]}{[N(Y^{\mathfrak{f}}) : N(Y^{\mathfrak{f}}) \cap S_u]} \cdot [u^\times : N(\mathcal{O}^{\mathfrak{f}\times})]$$

Bew.: Man ersetze im Beweisgang von (18.21) bis (18.25) immer A durch Y (und E durch U sowie l_{2n}^* durch l_4^T). Der Beweis bleibt wörtlich gültig.

§ 24 . Die Konjugationsklassenzahlen der 2-Dieder- und Tetraedergruppen

Die Berechnung der Konjugationsklassenzahlen für 2-Dieder- und Tetraedergruppen ist zum Teil vergleichbar mit der Berechnung der Konjugationsklassenzahlen für n-Diedergruppen, n > 2, in § 22. Wir übernehmen von dort die Definitionen und Lemmata, die auch für n = 2 gültig sind.

Die Konjugationsklassenzahlen für 2-Diedergruppen und Tetraedergruppen werden zurückgeführt auf Konjugationsklassenzahlen für Paare Erzeugender (U,V) von 2-Diedergruppen (Lemma 24.14).

Mit Hilfe der Unterscheidung nach $f(\mathfrak{M} \cap k[U])$ führen wir diese Konjugationsklassenzahlen dann zurück auf $l_4^*(\mathfrak{M}, \mathfrak{f})$ und $l_4^T(\mathfrak{M}, \mathfrak{f})$.

Hauptergebnis ist Satz (24.27), bzw. Korollar (24.28).

Wir machen für diesen Paragrafen folgende Generalvoraussetzung:

(24.1) Sei k algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$.
Sei k nicht total reell. Sei $Q = (-1, -1)_k$ und sei
$K = k[X]/(X^2 + 1)k[X]$.
Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $l_4^*(\mathfrak{M}) \neq 0$.
Wir kürzen ab: $\Gamma := \Gamma(\mathfrak{M})$, $F_4^* := F_4^*(\mathfrak{M})$ usw.
Wir benutzen die Definitionen aus § 22.

(24.2) Definition: i) $M_T := M_T(\mathfrak{M}) := \{G \subset \Gamma \mid G \text{ ist Tetraedergruppe}\}$

ii) $M_2^T := \{G \in M_2 \mid \text{Es gibt } G' \in M_T \text{ mit } G \subset G'\}$

iii) $M_2^- := M_2 - M_2^T$

iv) $\mu_T := \#\,(M_T/\sim)$; $\mu_2^T := \#\,(M_2^T/\sim)$; $\mu_2^- := \#\,(M_2^-/\sim)$

Zwei 2-Diedergruppen D, D' $\subset \Gamma$ sind höchstens dann Γ-konjugiert, wenn sie entweder beide oder beide nicht in Tetraedergruppen $\subset \Gamma$ enthalten sind (vgl. 15.6.ii).

Sind D, D' in Tetraedergruppen G, G' $\subset \Gamma$ enthalten, so gilt $D \sim D'$ genau dann, wenn $G \sim G'$. Denn jede 2-Diedergruppe ist in genau einer Tetraedergruppe enthalten und umgekehrt enthält jede Tetraedergruppe genau eine 2-Diedergruppe.

(24.3) Korollar: i) $\mu_2 = \mu_2^T + \mu_2^-$

ii) $\mu_T = \mu_2^T$

Wir wollen in diesem Paragrafen μ_2^T und μ_2^- berechnen.
Dazu müssen wir noch eine feinere Unterscheidung machen:

(24.4) Definition:

i) Sei $M^1 := \{D \in M_2^T \mid$ Es gibt eine 4-Diedergruppe $D' \subset \Gamma$ mit $D \subset D'\}$

$M^2 := M_2^T - M^1$

$M^3 := \{D \in M_2^- \mid$ Es gibt eine 4-Diedergruppe $D' \subset \Gamma$ mit $D \subset D'\}$

$M^4 := M_2^- - M^3$

ii) Für $1 \leq j \leq 4$ sei $\mu^j := \#\# M^j/\sim$.

Man überlegt sich wieder leicht:

(24.5) Lemma: $\mu_2^T = \mu^1 + \mu^2$ und $\mu_2^- = \mu^3 + \mu^4$

Zur Berechnung von μ^1 bis μ^4 benutzen wir den Umweg über Erzeugende.

(24.6) Definition: i) Sei $P_2^T := b^{-1}(M_2^T)$ und $P_2^- := b^{-1}(M_2^-)$.

ii) Für $1 \leq j \leq 4$ sei $P^j := b^{-1}(M^j)$.

iii) Sei $p_2 := \#\# P_2/\sim$; $p_2^T := \#\# P_2^T/\sim$ und $p_2^- := \#\# P_2^-/\sim$,

sowie $p^j := \#\# P^j/\sim$ für $1 \leq j \leq 4$.

(24.7) Lemma: i) Für $D \in M_2$ ist $\overline{b}^{-1}(\overline{D}) = \overline{b^{-1}(D)}$.

ii) $p_2 = p_2^T + p_2^-$ und $p_2^T = p^1 + p^2$ und $p_2^- = p^3 + p^4$

Bew.: i) vgl. den Beweis von (22.9.ii)
ii) klar

Bemerkung: Offensichtlich ist $P_2^T = \{(U,V) \in P_2 \mid 1/2 \cdot (1+U+V+UV) \in \Gamma\}$.

(24.8) Lemma: Sei $D = \{\pm 1, \pm U, \pm V, \pm W\} \in M_2$ mit $UV = W$.

i) $b^{-1}(D) = \{(\pm U, \pm V), (\pm V, \pm U), (\pm V, \pm W), (\pm W, \pm V), (\pm W, \pm U), (\pm U, \pm W)\}$

ii) $\overline{b}^{-1}(\overline{D}) = \{\overline{(U,V)}, \overline{(V,U)}, \overline{(V,W)}, \overline{(W,V)}, \overline{(W,U)}, \overline{(U,W)}\}$

Bew.: i) klar
ii) Es sind U, V, W $\in \Gamma$. Wegen
$UUU^{-1} = U$, $UVU^{-1} = -V$, $UWU^{-1} = -W$,
$VUV^{-1} = -U$, $VVV^{-1} = V$, $VWV^{-1} = -W$,
$WUW^{-1} = -U$, $WVW^{-1} = -V$, $WWW^{-1} = W$ folgt:

$(U,V) \sim (U,-V) \sim (-U,-V) \sim (-U,V)$

$(V,U) \sim (-V,U) \sim (-V,-U) \sim (V,-U)$

$(V,W) \sim (V,-W) \sim (-V,-W) \sim (-V,W)$

$(W,V) \sim (-W,V) \sim (-W,-V) \sim (W,-V)$

$(W,U) \sim (W,-U) \sim (-W,-U) \sim (-W,U)$

$(U,W) \sim (-U,W) \sim (-U,-W) \sim (U,-W)$

Jetzt folgt die Beh. mit (24.7.i).

(24.9) Lemma: gleiche Voraussetzung wie (24.8).

i) Wenn $D \in M_2^T = M^1 \cup M^2$, dann gilt:

$$\left.\begin{array}{l}(U,V) \sim (V,W),\ (V,W) \sim (W,U),\ (W,U) \sim (U,V) \text{ und} \\ (V,U) \sim (W,V),\ (W,V) \sim (U,W),\ (U,W) \sim (V,U)\end{array}\right\} \qquad (24.10)$$

ii) Wenn eine der sechs Relationen (24.10) gilt, dann ist $D \in M_2^T$.

Bew.: i) Sei $D \in M_2^T$. Dann ist $T := 1/2\cdot(1+U+V+W) \in \Gamma$.

Die Behauptung folgt wegen $TUT^{-1} = V$, $TVT^{-1} = W$ und $TWT^{-1} = U$.

ii) Sei o.B.d.A. $(U,V) \sim (V,W)$. Sei $T \in \Gamma$ mit $TUT^{-1} = V$ und $TVT^{-1} = W$.

Dann ist $TWT^{-1} = TUT^{-1}TVT^{-1} = VW = U$,

also $T^3UT^{-3} = T^2VT^{-2} = TWT^{-1} = U$.

Es ist $T \notin k[U]$; nach (3.2) ist aber $T^3 \in k[U]$,

also $T^3 \in \Gamma \cap k[T] \cap k[U] = \Gamma \cap k = \{\pm 1\}$.

Wenn wir evtl. T durch $-T$ ersetzen, wird $T^3 = -1$, also hat T die Ordnung 6

und es wird $T^{-1}V = UT^{-1}$ und $UT^{-1}U^{-1} = T^{-1}VU^{-1} = T^{-1}W = VT^{-1}$.

Also erzeugen U, V und T eine Tetraedergruppe (vgl. Def. 12.3.iii) G

mit $D \subset G \subset \Gamma$, d.h. $D \in M_2^T$.

(24.11) Lemma: Sei D eine 2-Diedergruppe, sei G eine 4-Diedergruppe

mit $D \subset G$.

Dann gibt es E, B $\in$ G mit $S(E) = \zeta_8 + \zeta_8^{-1} = \sqrt{2}$ und $BEB^{-1} = E^{-1}$,

so daß gilt: E und B erzeugen G und E^2 und B erzeugen D.

Bew.: Es gibt Erzeuger E und B von G mit $S(E) = \sqrt{2}$ und $BEB^{-1} = E^{-1}$.

Aus $[G : D] = 16/8 = 2$ folgt bekanntlich, daß D Normalteiler von G ist

und daß G/D abelsch ist. D enthält also die Kommutatorgruppe von G,

insbesondere ist $E^2 = EBE^{-1}B^{-1} \in D$.

Da $E^4 = -1$, ist $\{\pm 1, \pm E^2\} \subset D$.

i) Falls $B \in D$, ist $D_1 := \{\pm 1, \pm E^2, \pm B, \pm E^2B\} \subset D$.

D_1 ist eine 2-Diedergruppe, also $D_1 = D$.

ii) Falls $B \notin D$, ist $D \cap \{\pm B, \pm E^2B\} = \emptyset$. Außerdem ist $D \cap \{\pm E, \pm E^{-1}\} = \emptyset$, da E die Ordnung 8 hat. Also ist $D \subset \{\pm 1, \pm E^2, \pm EB, \pm E^3B\} =: D_2$. D_2 ist 2-Diedergruppe, also $D = D_2$.

Sei $B' = EB$. Dann gilt $B'EB'^{-1} = E^{-1}$ und: E, B' sind Erzeuger von G. Außerdem sind E^2 und B' Erzeuger von D.

(24.12) Lemma: gleiche Voraussetzung wie (24.8)

i) Wenn $D \in M^1 \cup M^3$, dann gilt mindestens eine der drei Aussagen a),b),c):

$$\left.\begin{array}{ll} \text{a)} & (U,V) \sim (V,U) \text{ und } (U,W) \sim (V,W) \text{ und } (W,U) \sim (W,V) \\ \text{b)} & (V,W) \sim (W,V) \text{ und } (V,U) \sim (W,U) \text{ und } (U,V) \sim (U,W) \\ \text{c)} & (W,U) \sim (U,W) \text{ und } (W,V) \sim (U,V) \text{ und } (V,W) \sim (V,U) \end{array}\right\} \quad (24.13)$$

ii) Wenn eine der neun Relationen (24.13) gilt, ist $D \in M^1 \cup M^3$.

Bew.: i) Sei $D \subset G \subset \Gamma$ mit einer 4-Diedergruppe G. Nach (24.11) gibt es E, $B \in G$ mit $S(E) = \sqrt{2}$ und $BEB^{-1} = E^{-1}$, so daß E und B die Gruppe G erzeugen und daß $D = \{\pm 1, \pm E^2, \pm B, \pm E^2B\}$.

Wir müssen nun eine Fallunterscheidung machen.

Wir untersuchen o.B.d.A. nur den Fall $E^2 = U$ und $B = V$.

Dann ist $E^2B = W$ und: $EUE^{-1} = U$, $EVE^{-1} = EBE^{-1} = W$ und $EWE^{-1} = -V$.

Wegen $E \in \Gamma$ ist also $(V,W) \sim (W,-V) \sim (W,V)$ und $(V,U) \sim (W,U)$ sowie $(U,V) \sim (U,W)$. Es gilt also b).

ii) Wir untersuchen o.B.d.A. nur die Voraussetzungen

α) $(V,W) \sim (W,V)$ bzw. β) $(V,U) \sim (W,U)$.

Falls α) gilt, ist auch $(V,W) \sim (W,-V)$. Es gibt also $E \in \Gamma$ mit $EVE^{-1} = W$ und $EWE^{-1} = -V$. Dann ist $EUE^{-1} = EVE^{-1}EWE^{-1} = -WV = U$, also gilt β). Umgekehrt kann man zeigen, daß aus β) auch α) folgt.

Nach (3.2) ist $E \in k[U]$. Da $E^2VE^{-2} = EWE^{-1} = -V$, wird $E^4VE^{-4} = V$, also $E^4 \in \Gamma \cap k[E] \cap k[V] = \{\pm 1\}$.

Da $N(E^2) = 1$ und $E^2 \notin k$, ist $E^4 + 1 = 0$.

$E^2 \in k[U]$ und U haben das gleiche Minimalpolynom, nach (2.12) ist $E^2 = \pm U$.

Da $VEV^{-1} = E^* = E^{-1}$, erzeugen E und V eine 4-Diedergruppe $\subset \Gamma$, die D enthält.

(24.14) Lemma: i) $p^1 = u^1$

ii) $p^2 = 2u^2$

iii) $p^3 = 3u^3$

iv) $p^4 = 6u^4$

Bew.: Für $1 \leq j \leq 4$ ist $p^j = \sum_{\overline{D} \in M^j/\sim} \# \overline{b}^{-1}(\overline{D})$

Sei $D = \{\pm 1, \pm U, \pm V, \pm W\} \in M_2$ mit $UV = W$.

Nach (24.8) ist $\overline{b}^{-1}(\overline{D}) = \{(\overline{U,V}), (\overline{V,U}), (\overline{V.W}), (\overline{W,V}), (\overline{W.U}), (\overline{U,W})\}$

i) Sei $D \in M^1$. Nach (24.9.i) ist
$\overline{b}^{-1}(\overline{D}) = \{(\overline{U,V}), (\overline{V,U})\} = \{(\overline{V,W}), (\overline{W,V})\} = \{(\overline{W,U}), (\overline{U,W})\}$.
Nach (24.12.i) ist also $\# \overline{b}^{-1}(\overline{D}) = 1$.
ii) Sei $D \in M^2$. Nach (24.9.i) ist $\overline{b}^{-1}(\overline{D}) = \{(\overline{U,V}), (\overline{V,U})\}$.
Nach (24.12.ii) ist $(\overline{U,V}) \neq (\overline{V,U})$, also $\# \overline{b}^{-1}(\overline{D}) = 2$.
iii) Sei $D \in M^3$. Wir wenden (24.12.i) an. Es gelte o.B.d.A. (24.13.a).
Dann ist $\overline{b}^{-1}(\overline{D}) = \{(\overline{U,V}), (\overline{V,W}), (\overline{W,U})\}$. Nach (24.9.ii) ist $\# \overline{b}^{-1}(\overline{D}) = 3$.
iv) Nach (24.9.ii) und (24.12.ii) sind $(\overline{U,V})$, $(\overline{V,U})$, $(\overline{V,W})$, $(\overline{W,V})$, $(\overline{W.U})$ und $(\overline{U,W})$ paarweise verschieden, wenn $D \in M^4$. Also ist $\# \overline{b}^{-1}(\overline{D}) = 6$.

Wir führen jetzt die p^i auf l_4^* und l_4^T zurück.

Offensichtlich gilt $a(P_2^T) = L_4^T$.

(24.15) Definition: Sei $\alpha: P_2^T \to L_4^T$ die durch a induzierte (surjektive) Abbildung.
Sei $\overline{\alpha}$ die durch α induzierte (surjektive) Abb. $\overline{\alpha}: P_2^T/\sim \to L_4^T/\sim$.

(24.16) Definition: Sei $\ell \in F_4^*$

i) Sei $P_2(\ell) := a^{-1}(L_4^*(\ell))$

ii) Sei $P_2^T(\ell) := P_2^T \cap P_2(\ell)$ und $P_2^-(\ell) := P_2^- \cap P_2(\ell)$

iii) Für $1 \leq i \leq 4$ sei $P^i(\ell) := P^i \cap P_2(\ell)$

iv) Sei $p_2(\ell) := \# P_2(\ell)/\sim$, $p_2^T(\ell) := \# P_2^T(\ell)/\sim$ und
$p_2^-(\ell) := \# P_2^-(\ell)/\sim$. Für $1 \leq i \leq 4$ sei $p^i(\ell) := \# P^i(\ell)/\sim$.

(24.17) Lemma: i) Für $\ell \in F_4^*$ ist $P_2^T(\ell) = \alpha^{-1}(L_4^T(\ell))$

ii) Für $\ell \in F_4^*$ ist $p_2(\ell) = p_2^T(\ell) + p_2^-(\ell)$ sowie
$p_2^T(\ell) = p^1(\ell) + p^2(\ell)$ und $p_2^-(\ell) = p^3(\ell) + p^4(\ell)$.

iii) Für $1 \leq i \leq 4$ ist $p^i = \sum_{\ell \in F_4^*} p^i(\ell)$

Bew.: klar

(24.18) Lemma: Sei $D = \{\pm 1, \pm U, \pm V, \pm UV\} \in M_2$.

Genau dann ist $D \in M^1 \cup M^3$, wenn gilt:
$f(\mathfrak{M} \cap k[U]) \in F_8^*$ oder $f(\mathfrak{M} \cap k[V]) \in F_8^*$ oder $f(\mathfrak{M} \cap k[UV]) \in F_8^*$.

Bew.: i) Sei $D \in M^1 \cup M^3$, sei G eine 4-Diedergruppe mit $D \subset G \subset \Gamma$.
Nach (24.11) gibt es $E, B \in G$ mit $S(E) = \sqrt{2}$ und $BEB^{-1} = E^{-1}$, so daß
$D = \{\pm 1, \pm E^2, \pm B, \pm E^2B\}$. Es ist $f(\mathfrak{M} \cap k[E]) \in F_8^*$.
Da $E^2 \in \{\pm U, \pm V, \pm UV\}$, ist $k[E] \in \{k[U], k[V], k[UV]\}$.
ii) Sei umgekehrt etwa $f(\mathfrak{M} \cap k[U]) \in F_8^*$, insbesondere also $\sqrt{2} \in k$.
Dann ist $D_k(\mathfrak{M} \cap k[U])$ Teiler von $(\zeta_8 - \zeta_8^{-1})^2 \mathfrak{o} = 2\mathfrak{o}$.
$U' := (1+U)/\sqrt{2}$ ist ganz über k und $D_k(1,U') = (1/\sqrt{2})^2 \cdot D_k(1,U) = -2$.
Also ist $U' \in \mathfrak{M}$, wegen $N(U') = 1$ ist $U' \in \Gamma$.
Es ist $U'^2 = U$, also erzeugen U' und V eine 4-Diedergruppe G mit $D \subset G \subset \Gamma$.

(24.19) Lemma: Sei $D = \{\pm 1, \pm U, \pm V, \pm UV\} \in M_2^T$. Dann ist
$f(\mathfrak{M} \cap k[U]) = f(\mathfrak{M} \cap k[V]) = f(\mathfrak{M} \cap k[UV])$.

Bew.: Es ist $T := 1/2 \cdot (1+U+V+UV) \in \Gamma$ und $TUT^{-1} = V$ sowie $TVT^{-1} = UV$.
Konjugation mit T induziert k-Algebrenisomorphismen $k[U] \to k[V]$
und $k[V] \to k[UV]$. Da $T \in \mathfrak{M}^\times$, folgt mit (6.11):
$f(\mathfrak{M} \cap k[U]) = f(T(\mathfrak{M} \cap k[U])T^{-1}) = f(\mathfrak{M} \cap k[V]) = f(\mathfrak{M} \cap k[UV])$.

(24.20) Lemma: i) $P^1 = \underbrace{\qquad}_{\mathfrak{f} \in F_8^* \cap F_4^T} P_2^T(\mathfrak{f})$ und

$P^2 = \underbrace{\qquad}_{\mathfrak{f} \in F_4^T - F_8^*} P_2^T(\mathfrak{f})$; daher

$p^1 = \sum_{\mathfrak{f} \in F_8^* \cap F_4^T} p_2^T(\mathfrak{f})$ und $p^2 = \sum_{\mathfrak{f} \in F_4^T - F_8^*} p_2^T(\mathfrak{f})$.

ii) $F_8^* \cap F_4^T$ enthält höchstens ein Element.
Ist $\mathfrak{f} \in F_8^* \cap F_4^T$, so gilt: $D_k(K) \cdot \mathfrak{f}^2 = 2\mathfrak{o}$.

Bew.: i) Es genügt zu zeigen, daß $P^1 = \underbrace{\qquad}_{\mathfrak{f} \in F_8^* \cap F_4^T} P_2^T(\mathfrak{f})$.

zu "$\subset$": Sei $(U,V) \in P^1$, also $\{\pm 1, \pm U, \pm V, \pm UV\} \in M^1$.
Da $1/2 \cdot (1+U+V+UV) \in \Gamma$, ist $f(\mathfrak{M} \cap k[U]) \in F_4^T$.
Nach (24.18) und (24.19) ist $f(\mathfrak{M} \cap k[U]) \in F_8^*$.

zu " $\supset$ ": Sei $(U,V) \in \bigcup_{f \in F_8^* \cap F_4^T} P_2^T(f)$. Wegen $f(\mathfrak{M} \cap k[U]) \in F_8^*$ ist nach Lemma (24.18) $\{\pm 1, \pm U, \pm V, \pm UV\} \in M^1 \cup M^3$, also $(U,V) \in P^1 \cup P^3$. Da nach Vor. $(U,V) \in P_2^T = P^1 \cup P^2$, folgt die Beh.

ii) Sei $f \in F_8^* \cap F_4^T$. Dann ist $\sqrt{2} \in k$ und $Q \tilde{k} ((\zeta_8 - \zeta_8^{-1})^2, -1)_k$ hat keine endlichen Verzweigungsstellen (siehe 13.4.ii).
Da $f \in F_4^T$, folgt jetzt mit (23.13.i), daß $2 \mathfrak{o} \mid D_k(K) f^2$.
Wegen $f \in F_8^*$ ist $D_k(K) f^2 \mid 2 \mathfrak{o}$ $\left(\text{denn } K \tilde{k} k[X]/(X^2 - \sqrt{2}X + 1)k[X]\right)$.

(24.21) Lemma: Sei $D = \{\pm 1, \pm U, \pm V, \pm UV\} \in M_2$.
Genau dann ist $D \in M^3$, wenn genau eins der Ideale $f(\mathfrak{M} \cap k[U])$, $f(\mathfrak{M} \cap k[V])$ und $f(\mathfrak{M} \cap k[UV])$ in F_8^* liegt.

Bew.: i) Sei $D \in M^3$. Nach (24.18) liegt mindestens eins der genannten Ideale in F_8^*. Wir nehmen an, daß mindestens zwei dieser Ideale in F_8^* liegen. Sei o.B.d.A. $f(\mathfrak{M} \cap k[U]) \in F_8^*$ und $f(\mathfrak{M} \cap k[V]) \in F_8$.
Wie im Beweis von (24.18.ii) gesehen, ist dann $(1+U)/\sqrt{2} \in \Gamma$ und $(1+V)/\sqrt{2} \in \Gamma$; also ist $1/2 \cdot (1+U+V+UV) = (1+U)/\sqrt{2} \cdot (1+V)/\sqrt{2} \in \Gamma$, d.h. $D \in M^1 \cup M^2$ $\lightning$.
ii) Sei umgekehrt o.B.d.A. $f(\mathfrak{M} \cap k[U]) \in F_8^*$, $f(\mathfrak{M} \cap k[V]) \notin F_8^*$ und $f(\mathfrak{M} \cap k[UV]) \notin F_8$. Nach (24.18) ist $D \in M^1 \cup M^3$.
Nach (24.19) ist $D \notin M^1 \cup M^2$, also $D \in M^3$.

(24.22) Lemma: $p^3 = 3 \cdot \sum_{f \in F_8^*} p^3(f)$

Bew.: Es genügt zu zeigen, daß für jedes $D \in M^3$ gilt:
$\# \overline{b}^{-1}(\overline{D}) = 3 \cdot \# \left(\overline{b}^{-1}(\overline{D}) \cap \left(\bigcup_{f \in F_8^*} P^3(f)/\sim\right)\right)$
Sei $D \in M^3$, sei $D = \{\pm 1, \pm U, \pm V, \pm UV\}$
Wie wir im Beweis von (24.14.iii) gesegen haben, ist $\# \overline{b}^{-1}(\overline{D}) = 3$.
Wir können o.B.d.A. annehmen, daß $\overline{b}^{-1}(\overline{D}) = \{\overline{(U,V)}, \overline{(V,W)}, \overline{(W,U)}\}$.
Nach (24.21) liegt genau eins der Paare (U,V), (V,W) und (W,U) in $\bigcup_{f \in F_8^*} P_2(f)$. Daraus folgt die Behauptung.

(24.23) Lemma: i) Für $\mathfrak{f} \in F_8^*$ ist $p^2(\mathfrak{f}) = p^4(\mathfrak{f}) = 0$.

ii) $p^3 = 3 \cdot \sum_{\mathfrak{f} \in F_8^*} p_2(\mathfrak{f}) - 3p^1$

iii) $p^4 = \sum_{\mathfrak{f} \in F_4^*} p_2(\mathfrak{f}) - (p^1 + p^2 + p^3)$

Bew.: i) Sei $\mathfrak{f} \in F_4^*$ und $(U,V) \in P^2(\mathfrak{f}) \cup P^4(\mathfrak{f})$, also $\{\pm 1, \pm U, \pm V, \pm UV\} \in M^2 \cup M^4$. Nach (24.18) ist $\mathfrak{f} = f(\mathfrak{M} \cap k[U]) \notin F_8^*$. Für $\mathfrak{f} \in F_8^*$ ist also $P^2(\mathfrak{f}) = P^4(\mathfrak{f}) = \emptyset$, d.h. $p^2(\mathfrak{f}) = p^4(\mathfrak{f}) = 0$.

ii) Nach (24.22) und i) ist $p^3 = 3 \cdot \sum_{\mathfrak{f} \in F_8^*} p^3(\mathfrak{f}) = 3 \cdot \sum_{\mathfrak{f} \in F_8^*} \left(p_2(\mathfrak{f}) - p^1(\mathfrak{f})\right)$.

Nach (24.20.i) ist $p^1(\mathfrak{f}) = 0$ für $\mathfrak{f} \notin F_8^* \cap F_4^T$, also $\sum_{\mathfrak{f} \in F_8^*} p^1(\mathfrak{f}) = p^1$.

iii) klar

Mit (24.20.i) und (24.23.ii,iii) haben wir die Berechnung von p^j, $1 \le j \le 4$ zurückgeführt auf die Berechnung von $p_2(\mathfrak{f})$ für $\mathfrak{f} \in F_4^*$ und $p_2^T(\mathfrak{f})$ für $\mathfrak{f} \in F_4^T$.

Nach (22.9.i), (22.10) und (22.12) ist $p_2(\mathfrak{f}) = 2^s \cdot \kappa \cdot l_4^*(\mathfrak{f})$.

(24.24) Lemma: i) Für $\mathfrak{f} \in F_4^T$ ist $p_2^T(\mathfrak{f}) = \sum_{\overline{U} \in L_4^T(\mathfrak{f})/\sim} \#\, \overline{\alpha}^{-1}(\overline{U})$

ii) Für $U \in L_4^T$ ist $\overline{\alpha}^{-1}(\overline{U}) = \overline{\alpha^{-1}(U)}$

Bew.: klar

(24.25) Lemma: Sei $\mathfrak{f} \in F_4^T$. Sei $U \in L_4^T(\mathfrak{f})$ und sei $V \in \Gamma$, so daß $(U,V) \in P_2^T(\mathfrak{f})$. Sei $\mathcal{O}^{\mathfrak{f}} := \mathcal{O}^{\mathfrak{f}}(k[U])$ usw.

Durch die Abbildung χ: $\Delta\left((n^{\mathfrak{f}})^{-1}(Y^{\mathfrak{f}})\right) \to \alpha^{-1}(U)$

$$M \mapsto (U, MV)$$

wird eine bijektive Abbildung $\overline{\chi}$: $\Delta\left((n^{\mathfrak{f}})^{-1}(Y^{\mathfrak{f}})\right) \Big/ \left(\Gamma \cap k[U]\right)^{(2)} \to \overline{\alpha}^{-1}(\overline{U})$ induziert.

Bemerkung: Es ist

$\Delta\left((n^{\mathfrak{f}})^{-1}(Y^{\mathfrak{f}})\right) \subset \Delta\left((n^{\mathfrak{f}})^{-1}(A^{\mathfrak{f}})\right) = \Delta\left(\Delta^{-1}(\mathcal{O}^{\mathfrak{f}\times})\right) = \mathcal{O}^{\mathfrak{f}\times} \cap N^{-1}(1) = \Gamma \cap k[U]$

(vgl. 18.12.iii und 19.6).

Für $M \in \Gamma \cap k[U]$ ist $\Delta(M) = MM^{*-1} = M^2$.

Bew. von (24.25): Falls $M \in \Delta\left((\eta^{\mathfrak{p}})^{-1}(Y^{\mathfrak{p}})\right)$, gibt es $L \in k[U]^{\times}$ mit $M = LL^{*-1}$ und $L\mathcal{O}^{\mathfrak{p}} \in Y^{\mathfrak{p}}$. Sei $T := 1/2\cdot(1+U+V+UV)$.
Mit (23.16.ii) folgt $LTL^{-1} \in \mathfrak{M}$ (man setze $\mathfrak{o} = L^{-1}\mathcal{O}^{\mathfrak{p}}$).
Also ist $(U,MV) = (LUL^{-1}, LVL^{-1}) \in \alpha^{-1}(U)$, d.h. χ hat den angegebenen Bildraum.
Wohldefiniertheit und Injektivität von $\overline{\chi}$ folgen wie in (22.10).
Surjektivität: Sei $(U,V') \in \alpha^{-1}(U)$. Es gibt $L \in Q^{\times}$ mit $LUL^{-1} = U$ und $LVL^{-1} = V'$. Nach (3.2) ist $L \in k[U]$, also $V' = LL^{*-1}V$.
Da $(U,V') \in P_2^T$, ist $LTL^{-1} \in \Gamma$, also $T \in L^{-1}\mathfrak{M}L$.
Außerdem ist $L^{-1}\mathfrak{M}L \cap k[U] = L^{-1}(\mathfrak{M} \cap k[U])L = \mathfrak{M} \cap k[U] = \mathcal{O}^{\mathfrak{p}}$.
Nach (23.16.i) gibt es $\mathfrak{o} \in Y^{\mathfrak{p}}$ mit $L^{-1}\mathfrak{M}L = \mathfrak{o}\mathfrak{M}\mathfrak{o}^{-1}$.
Dann ist $\mathfrak{M}L\mathfrak{o} = L\mathfrak{o}\mathfrak{M}$, nach (23.18) also $L\mathfrak{o} \in Y^{\mathfrak{p}}$.
Damit folgt $L \in (\eta^{\mathfrak{p}})^{-1}(Y^{\mathfrak{p}})$.

(24.26) Lemma: Sei $\mathfrak{p} \in F_4^T$ und $U \in L_4^T(\mathfrak{p})$ und $\mathcal{O}^{\mathfrak{p}} := \mathcal{O}^{\mathfrak{p}}(k[U])$.
Dann ist $\left[\Delta\left((\eta^{\mathfrak{p}})^{-1}(Y^{\mathfrak{p}})\right) : \left(\Gamma \cap k[U]\right)^{(2)}\right] = 2^{s}\cdot\kappa \Big/ \left[A^{\mathfrak{p}} \cap H^{\mathfrak{p}} : Y^{\mathfrak{p}} \cap H^{\mathfrak{p}}\right]$.

Bew.: Wegen (22.12) und der Bemerkung nach (24.25) müssen wir zeigen:
$\left[\Delta\left((\eta^{\mathfrak{p}})^{-1}(A^{\mathfrak{p}})\right) : \Delta\left((\eta^{\mathfrak{p}})^{-1}(Y^{\mathfrak{p}})\right)\right] = \left[A^{\mathfrak{p}} \cap H^{\mathfrak{p}} : Y^{\mathfrak{p}} : H^{\mathfrak{p}}\right]$
Es ist
$$\begin{aligned}\left[A^{\mathfrak{p}} \cap H^{\mathfrak{p}} : Y^{\mathfrak{p}} \cap H^{\mathfrak{p}}\right] &= \left[\eta^{\mathfrak{p}}\left((\eta^{\mathfrak{p}})^{-1}(A^{\mathfrak{p}})\right) : \eta^{\mathfrak{p}}\left((\eta^{\mathfrak{p}})^{-1}(Y^{\mathfrak{p}})\right)\right] \\ &= \left[(\eta^{\mathfrak{p}})^{-1}(A^{\mathfrak{p}}) : (\eta^{\mathfrak{p}})^{-1}(Y^{\mathfrak{p}})\right] \\ &= \left[\Delta\left((\eta^{\mathfrak{p}})^{-1}(A^{\mathfrak{p}})\right) : \Delta\left((\eta^{\mathfrak{p}})^{-1}(Y^{\mathfrak{p}})\right)\right]\end{aligned}$$
Die letzte Zeile folgt mit dem Homomorphiesatz (7.6), da $\Delta^{-1}(1) = k^{\times} \subset (\eta^{\mathfrak{p}})^{-1}(Y^{\mathfrak{p}})$.

Nach (24.24.i), (24.25) und (24.26) ist $p_2^T(\mathfrak{p}) = 2^{s}\cdot\kappa\cdot l_4^T(\mathfrak{p}) \Big/ \left[A^{\mathfrak{p}} \cap H^{\mathfrak{p}} : Y^{\mathfrak{p}} \cap H^{\mathfrak{p}}\right]$
und wir erhalten mit (24.14), (24.20) und (24.23):

(24.27) Satz: (Voraussetzung 24.1)

i) $$\mu^1 = \sum_{\mathfrak{p} \in F_8^* \cap F_4^T} 2^{s}\cdot\kappa\cdot l_4^T(\mathfrak{p}) \Big/ \left[A^{\mathfrak{p}} \cap H^{\mathfrak{p}} : Y^{\mathfrak{p}} \cap H^{\mathfrak{p}}\right]$$

ii) $$\mu^2 = \sum_{\mathfrak{p} \in F_4^T - F_8^*} 2^{s-1}\cdot\kappa\cdot l_4^T(\mathfrak{p}) \Big/ \left[A^{\mathfrak{p}} \cap H^{\mathfrak{p}} : Y^{\mathfrak{p}} \cap H^{\mathfrak{p}}\right]$$

iii) $$\mu^3 = \sum_{\mathfrak{p} \in F_8^*} 2^{s}\cdot\kappa\cdot l_4(\mathfrak{p}) - \mu^1$$

iv) $$\mu^4 = 1/3\cdot\left(\sum_{\mathfrak{p} \in F_4^* - F_8^*} 2^{s-1}\cdot\kappa\cdot l_4^*(\mathfrak{p}) - \mu^2 - \mu^3\right)$$

Bemerkung: Falls $\mu^1 \neq 0$, ist $\mu^1 = 2^s \cdot [I^k : I^{k(2)} S_\infty]$.
Dies läßt sich mit den Methoden aus § 19 zeigen.
Wir zeigen die Beh. allerdings auf eine andere Weise (siehe 25.12).

(24.28) Korollar: Voraussetzung (24.1)

i) $$\mu_T = \sum_{\mathfrak{f} \in F_4^T} \frac{2^{s-1} \cdot \kappa \cdot q(\mathfrak{f}) \cdot l_4^T(\mathfrak{f})}{[A^{\mathfrak{f}} \cap H^{\mathfrak{f}} : Y^{\mathfrak{f}} \cap H^{\mathfrak{f}}]}$$

ii) $$\bar{\mu}_2 = 1/3 \cdot \sum_{\mathfrak{f} \in F_4^*} \left[2^{s-1} \cdot \kappa \cdot q(\mathfrak{f})^2 \cdot \left(l_4^*(\mathfrak{f}) - \frac{l_4^T(\mathfrak{f})}{[A^{\mathfrak{f}} \cap H^{\mathfrak{f}} : Y^{\mathfrak{f}} \cap H^{\mathfrak{f}}]} \right) \right]$$

Dabei sei $q(\mathfrak{f}) := q_2(\mathfrak{f}) = \begin{cases} 2, \text{ falls } \sqrt{2} \in k \text{ und } \mathfrak{f} \in F_8^* \\ 1, \text{ sonst} \end{cases}$

§ 25 . Die Konjugationsklassenzahlen der Oktaeder- und Ikosaedergruppen

Die Berechnung der Konjugationsklassenzahlen von Oktaeder- und Ikosaedergruppen verläuft analog zur Berechnung von $l_{2n}(\mathfrak{M}, \mathfrak{f})$, $l_{2n}^*(\mathfrak{M}, \mathfrak{f})$ und $l_4^T(\mathfrak{M}, \mathfrak{f})$ in den §§ 17, 18 und 23.
Der Beweisgang ist hier im Gegensatz zu den anderen nichtzyklischen Gruppen so einfach, weil Oktaeder- und Ikosaedergruppen maximalendliche Gruppen in $SL(2,\mathbb{C})$ sind.
Hauptergebnis ist Satz (25.9).
Für die Oktaedergruppen beweisen wir noch, daß ihre Konjugationsklassenzahl gleich dem früher berechneten μ^1 ist.

(25.1) Satz: Sei k ein algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$.
Sei $\sqrt{2} \in k$ (bzw. $\sqrt{5} \in k$). Sei $Q = (-1, -1)_k$.
i) Sei $G \subset \Gamma(Q)$ eine Oktaedergruppe (bzw. Ikosaedergruppe).
Es gibt genau eine Q-Ordnung $\mathfrak{M}$, die G enthält. $\mathfrak{M}$ ist Q-Maximalordnung.
ii) Seien $\mathfrak{M}$, $\mathfrak{M}'$ zwei Q-Maximalordnungen, so daß $\Gamma(\mathfrak{M})$ und $\Gamma(\mathfrak{M}')$ Oktaedergruppen (bzw. Ikosaedergruppen) enthalten.
Dann sind $\mathfrak{M}$ und $\mathfrak{M}'$ vom gleichen Typ.

Bew.: i) $\mathfrak{M} := \sum_{g \in G} \mathfrak{o} \cdot g$ ist eine Q-Ordnung und offensichtlich die kleinste Q-Ordnung, die G enthält.
a) Sei $\sqrt{2} \in k$ und G eine Oktaedergruppe. Nach (12.6.v) gibt es $U', V' \in G$ mit $D_k(1,U',V',U'V') = -1$. Daher ist notwendig $D_k(\mathfrak{M}) = \mathfrak{o}$, also $\mathfrak{M}$ eine Q-Maximalordnung.

b) Sei $\sqrt{5} \in k$ und G eine Ikosaedergruppe . Dann enthält G eine 2-Diedergruppe und eine 5-Diedergruppe (siehe Def. 12.3.v). Daher ist $D_k(\mathfrak{M})$ Teiler von $5\mathfrak{o}$ und $16\mathfrak{o}$ (vgl. 12.6.ii), also ist $D_k(\mathfrak{M}) = \mathfrak{o}$ und $\mathfrak{M}$ eine Q-Maximalordnung.
Die Eindeutigkeit von $\mathfrak{M}$ ist in beiden Fällen klar.
ii) klar

Bemerkung: (25.1) ist eine Ergänzung zu (13.8).

(25.2) Definition: Sei k algebraischer Zahlkörper mit $\sqrt{2} \in k$ (bzw. $\sqrt{5} \in k$). Sei $Q = (-1, -1)_k$ und $\mathfrak{M}$ eine Q-Maximalordnung.
i) Sei $M_O(\mathfrak{M}) := \{G \subset \Gamma(\mathfrak{M}) \mid G \text{ ist Oktaedergruppe}\}$.
(bzw. $M_I(\mathfrak{M}) := \{G \subset \Gamma(\mathfrak{M}) \mid G \text{ ist Ikosaedergruppe}\}$)
ii) Sei $u_O(\mathfrak{M}) := \# M_O(\mathfrak{M})/\sim$ (bzw. $u_I(\mathfrak{M}) := \# M_I(\mathfrak{M})/\sim$).
iii) Für $G \in M_O(\mathfrak{M})$ (bzw. $G \in M_I(\mathfrak{M})$) bezeichne $\overline{G}$ die Restklasse in $M_O(\mathfrak{M})/\sim$ (bzw. $M_I(\mathfrak{M})/\sim$).

Für die weiteren Untersuchungen in diesem Paragrafen bis Satz (25.9) sei k ein algebraischer Zahlkörper mit Hauptordnung $\mathfrak{o}$. Sei k nicht total reell, sei $\sqrt{2} \in k$. Sei $Q = (-1, -1)_k$. Sei $G \subset \Gamma(Q)$ eine Oktaedergruppe. Sei $\mathfrak{M}$ die Q-Maximalordnung mit $G \subset \mathfrak{M}$.
Wir kürzen $\Gamma := \Gamma(\mathfrak{M})$ und $M_O := M_O(\mathfrak{M})$ ab.
Die folgenden Untersuchungen gelten genauso für Ikosaedergruppen.

(25.3) Lemma: i) Zu jedem $G' \in M_O$ gibt es $M \in Q^\times$ mit $G' = MGM^{-1}$.
ii) Sei $M \in Q^\times$. Genau dann ist $MGM^{-1} \in M_O$, wenn es $\mathfrak{a} \in I^k$ gibt mit $\mathfrak{M}M = \mathfrak{M}\mathfrak{a}$.

Bew.: i) klar (12.9.iii)
ii) Sei $MGM^{-1} \in M_O$, d.h. $MGM^{-1} \subset \mathfrak{M}$. Nach (25.1.i) ist dann $M\mathfrak{M}M^{-1} = \mathfrak{M}$. Das Ideal $M\mathfrak{M} = \mathfrak{M}M$ ist zweiseitiges $\mathfrak{M}$-Ideal. Da Q keine endlichen Verzweigungsstellen hat, ist $\mathfrak{M}M = \mathfrak{M}\mathfrak{a}$ mit $\mathfrak{a} \in I^k$ (siehe 9.13).
Sei umgekehrt $\mathfrak{M}M = \mathfrak{M}\mathfrak{a}$ mit $\mathfrak{a} \in I^k$. Die Rechtsordnung dieses Ideals ist $M^{-1}\mathfrak{M}M = \mathfrak{a}^{-1}\mathfrak{M}\mathfrak{a} = \mathfrak{M}$.
Aus dieser Gleichung folgt sofort: $MGM^{-1} \subset \mathfrak{M}$.

Sei η die in (17.3) definierte Abbildung. Lemma (25.3) besagt dann, daß durch die Vorschrift $M \mapsto MGM^{-1}$ eine surjektive Abbildung $\varepsilon: \eta^{-1}(\mathfrak{M} I^{\mathfrak{M}}) \to M_O$ definiert wird.

(25.4) Lemma: Sei $M \in \eta^{-1}(\mathfrak{m} I \mathfrak{m})$.
i) Sei $\gamma \in \Gamma$ und $a \in k^\times$. Dann ist $\gamma Ma \in \eta^{-1}(\mathfrak{m} I \mathfrak{m})$.
ii) Sei $M' \in \eta^{-1}(\mathfrak{m} I \mathfrak{m})$. Genau dann ist $MGM^{-1} \sim M'GM'^{-1}$, wenn es $\gamma \in \Gamma$ und $a \in k^\times$ gibt mit $M' = \gamma Ma$.

Bew.: i) Sei $\mathfrak{m} M = \mathfrak{m} \alpha$ mit $\alpha \in I^k$. Dann ist $\mathfrak{m} \gamma Ma = \mathfrak{m} Ma = \mathfrak{m} \alpha a$.
ii) Sei $MGM^{-1} \sim M'GM'^{-1}$. Dann gibt es $\gamma \in \Gamma$ mit $M'GM'^{-1} = \gamma MGM^{-1}\gamma^{-1}$, also $(M^{-1}\gamma^{-1}M')G(M^{-1}\gamma^{-1}M')^{-1} = G$.
Wegen dem folgenden Lemma (25.5) gibt es $a \in k^\times$ und $g \in G$ mit $M^{-1}\gamma^{-1}M' = ag$, d.h. $M' = \gamma Mag$. Da $G \subset \mathfrak{m}^\times$, ist
$\mathfrak{m} M' = \mathfrak{m} \gamma Mag = \mathfrak{m} Mag = \mathfrak{m} \alpha ag = \mathfrak{m} g \alpha a = \mathfrak{m} \alpha a = \mathfrak{m} Ma$.
Daher ist $\varepsilon := M'a^{-1}M^{-1} \in \mathfrak{m}^\times$. Es ist $N(\varepsilon) = N(\gamma Maga^{-1}M^{-1}) = 1$.
Also ist $\varepsilon \in \Gamma$ und $M' = \varepsilon Ma$.
Sei umgekehrt $a \in k^\times$ und $\gamma \in \Gamma$ mit $M' = \gamma Ma$. Dann ist
$M'GM'^{-1} = \gamma MaGa^{-1}M^{-1}\gamma^{-1} = \gamma MGM^{-1}\gamma^{-1}$, also $M'GM'^{-1} \sim MGM^{-1}$.

(25.5) Lemma: Der Normalisator von G in $Q^\times$ ist $k^\times G$.

Bew.: Offensichtlich ist $k^\times G$ im Normalisator enthalten.
Sei umgekehrt $a \in Q^\times$ mit $aGa^{-1} = G$. Die endliche Gruppe G hat nur endlich viele Automorphismen. Daraus folgt leicht, daß es ein kleinstes $m \in \mathbb{N}$ gibt, so daß Konjugation mit a^m die Gruppe G elementweise festläßt. Da G eine Basis von Q über k enthält, ist Konjugation mit a^m die Identität auf Q. Also liegt a^m im Zentrum von Q, d.h. $a^m \in k^\times$.
Sei K Zerfällungskörper des Polynoms $X^2 - N(a)$ über k und sei x eine Nullstelle dieses Polynoms in K. Wir betten jetzt k in K und Q in $Q' := Q \otimes_k K$ ein. Sei $b := x^{-1}a$. Dann ist $bGb^{-1} = G$ und $b^m \notin K^\times$.
Da $N_{Q'|K}(b) = x^{-2}N_{Q|k}(a) = 1$, folgt weiter $b^{2m} = N_{Q'|K}(b^m) = 1$.
Man sieht jetzt sofort ein, daß b und die Elemente von G eine endliche Untergruppe von $\Gamma(Q')$ erzeugen. Da es keine binäre Polyedergruppe gibt, die eine Oktaedergruppe als echte Teilmenge hat, ist $b \in G \subset Q^\times$.
Wegen $a \in Q^\times$ ist $x = ab^{-1} \in Q^\times \cap K = k^\times$, also $a \in k^\times G$ (und $K = k$).

Sei $p: \eta^{-1}(\mathfrak{m} I \mathfrak{m}) \to \Gamma \backslash \eta^{-1}(\mathfrak{m} I \mathfrak{m}) / k^\times$ die natürliche Projektion.
Nach Lemma (25.4) induziert die surjektive Abbildung e eine bijektive Abbildung $\overline{e}: \Gamma \backslash \eta^{-1}(\mathfrak{m} I \mathfrak{m}) / k^\times \to M_O/\sim$.

(25.6) Korollar: $\mu_O = \#\, \Gamma \backslash \eta^{-1}(\mathfrak{m} I \mathfrak{m}) / k^\times$.

Für $\alpha \in I^k$ bezeichnen wir die Restklasse in I^k/H^k mit $\overline{\alpha}$.

(25.7) Lemma: Wir können eine Abbildung $\psi: \Gamma \backslash \eta^{-1}(\mathfrak{m} I^{\mathfrak{m}})/k^\times \to I^k/H^k$ folgendermaßen definieren:
Ist $M \in \eta^{-1}(\mathfrak{m} I^{\mathfrak{m}})$, also $\mathfrak{M} M = \mathfrak{M} \alpha$ mit $\alpha \in I^k$,
so setzen wir $\psi(p(M)) = \overline{\alpha}$.
ψ hat die folgenden Eigenschaften:

i) $u_0 = \dfrac{\sum}{\overline{\alpha} \in \mathrm{Bild}\ \psi} \# \psi^{-1}(\overline{\alpha})$

ii) $\# \mathrm{Bild}\ \psi = \dfrac{[I^k : H^k]}{[I^{k(2)} : I^{k(2)} \cap S_u]} = \dfrac{[I^k : I^{k(2)} S_u]}{[H^k : S_u]}$

Bew.: wie der Beweis von (18.23). (Es ist $N(I^k) = I^{k(2)}$)

Wir wählen jetzt ein festes $\alpha \in I^k$ mit $\overline{\alpha} \in \mathrm{Bild}\ \psi$ und ein festes $M \in p^{-1}(\psi^{-1}(\overline{\alpha}))$. Zu jedem $M' \in p^{-1}(\psi^{-1}(\overline{\alpha}))$ gibt es dann ein $a \in k^\times$ mit $\mathfrak{M} M' = \mathfrak{M} M a$.

$\Gamma \mathfrak{o}^\times$ ist Normalteiler in $\mathfrak{M}^\times$ und zwar ist $\Gamma \mathfrak{o}^\times = N^{-1}(\mathfrak{o}^{\times(2)})$ für die Normabbildung $N: \mathfrak{M}^\times \to \mathfrak{u}^\times$.
Die Restklasse von $\varepsilon \in \mathfrak{M}^\times$ in $\mathfrak{M}^\times/\Gamma \mathfrak{o}^\times$ bezeichnen wir mit $\overline{\varepsilon}$.

(25.8) Lemma: Wir können eine Abbildung $\chi: \psi^{-1}(\overline{\alpha}) \to \mathfrak{M}^\times/\Gamma \mathfrak{o}^\times$ folgendermaßen definieren:
Ist $M' \in p^{-1}(\psi^{-1}(\overline{\alpha}))$, also $\mathfrak{M} M' = \mathfrak{M} M a$ mit $a \in k^\times$,
dann setzen wir $\chi(p(M')) = \overline{M' a^{-1} M^{-1}}$.
χ ist bijektiv; insbesondere gilt: $\# \psi^{-1}(\overline{\alpha}) = [\mathfrak{u}^\times : \mathfrak{o}^{\times(2)}]$.

Bew.: wie der Beweis von (17.13). Man muß dort nur $k[\mathfrak{M}]$ durch k und $\mathfrak{O}$ durch $\mathfrak{o}$ ersetzen. (Es ist $N(\mathfrak{o}^\times) = \mathfrak{o}^{\times(2)}$)

(25.9) Satz: Sei k algebraischer Zahlkörper, sei k nicht total reell. Sei $\sqrt{2} \in k$ (bzw. $\sqrt{5} \in k$). Sei $Q = (-1, -1)_k$ und sei $\mathfrak{M}$ eine Q-Maximalordnung, so daß $\Gamma(\mathfrak{M})$ eine Oktaedergruppe (bzw. Ikosaedergruppe) enthält. Dann ist
$u_0(\mathfrak{M}) = 2^s \cdot [I^k : I^{k(2)} S_u]$ $\left(\text{bzw. } u_1(\mathfrak{M}) = 2^s \cdot [I^k : I^{k(2)} S_u]\right)$

Bew.: Wir können uns auf den Fall beschränken, daß $\sqrt{2} \in k$ und $\Gamma(\mathfrak{M})$ eine Oktaedergruppe G enthält.

Mit (25.7) und (25.8) folgt: $u_0 = [I^k : I^{k(2)} S_u] \cdot \dfrac{[\mathfrak{u}^\times : \mathfrak{o}^{\times(2)}]}{[H^k : S_u]}$.

Da $\mathfrak{u}$ alle r reellen Primstellen von k enthält (13.8), folgt mit

Lemma (8.5): $\left[H^k : S_{\mathfrak{u}}\right] = \dfrac{\left[\Gamma^k : S_{\mathfrak{u}}\right]}{\left[\Gamma^k : \Pi^k\right]} = \dfrac{2^r}{\left[\mathfrak{o}^\times : \mathfrak{u}^\times\right]}$

Also $u_O = \left[\Gamma^k : \Gamma^{k(2)} S_{\mathfrak{u}}\right] \cdot 2^{-r} \cdot \left[\mathfrak{o}^\times : \mathfrak{u}^\times\right] \cdot \left[\mathfrak{u}^\times : \mathfrak{o}^{\times(2)}\right]$.

Aus dem Dirichletschen Einheitensatz folgt $\left[\mathfrak{o}^\times : \mathfrak{o}^{\times(2)}\right] = 2^{r+s}$

und damit die Beh.

Für die Oktaedergruppe machen wir noch einige Zusatzüberlegungen.

(25.10) Lemma: Sei k algebraischer Zahlkörper mit $\sqrt{2} \in k$.
Sei $Q = (-1, -1)_k$. Sei $G \subset \Gamma(Q)$ eine Oktaedergruppe.
Dann gibt es genau eine 2-Diedergruppe $D \subset G$, die Normalteiler in G ist.
Umgekehrt ist dann G der Normalisator von D in $\Gamma(Q)$.

Bew.: G wird von zwei Elementen U', V' erzeugt, so daß $U = U'^2$ und $V = V'^2$ eine 2-Diedergruppe $D \subset G$ erzeugen.
Wegen $U'UU'^{-1} = U$, $U'VU'^{-1} = U'^2V = UV$, $V'UV'^{-1} = V'^2U = VU$ und $V'VV'^{-1} = V$ ist D Normalteiler in G.
Gäbe es eine weitere 2-Diedergruppe $D' \subset G$, die normal in G liegt, so wäre $D \cap D'$ Normalteiler in G. Da die 4-zyklischen Untergruppen von D keine Normalteiler in G sind, müßte $D \cap D' = \{\pm 1\}$ sein, und daher $\# DD' = 8 \cdot \left[DD' : D'\right] = 8 \cdot \left[D : D \cap D'\right] = 32$.
DD' ist Untergruppe von G und $\# G = 48$. ↯
Natürlich ist G im Normalisator N von D in $\Gamma(Q)$ enthalten.
Wir müssen also noch zeigen, daß $\# N \leq 48$.
Wir erhalten einen Homomorphismus $\phi: N \to \mathrm{Aut}(D)$, wenn wir jedem $M \in N$ den Automorphismus zuordnen, der durch Konjugation mit M induziert wird. Da D eine Basis von Q über k enthält, liegt Kern ϕ im Zentrum von Q, also Kern $\phi \subset k^\times \cap \Gamma(Q) = \{\pm 1\}$.
Wir müssen noch zeigen, daß $\# \mathrm{Aut}(D) < 24$.
Für $\sigma \in \mathrm{Aut}(D)$ kann man $\sigma(U) \in \{\pm U, \pm V, \pm UV\}$ und $\sigma(V) \in \{\pm U, \pm V, \pm UV\} - \{\pm \sigma(U)\}$ vorschreiben.
Dadurch ist umgekehrt σ bestimmt. Also $\# \mathrm{Aut}(D) = 6 \cdot 4 = 24$.

(25.11) Lemma: Sei k algebraischer Zahlkörper, sei k nicht total reell.
Sei $\sqrt{2} \in k$. Sei $Q = (-1, -1)_k$ und sei $\mathfrak{M}$ eine Q-Maximalordnung
i) Seien G, $G' \subset \Gamma(\mathfrak{M})$ Oktaedergruppen und seien D, D' die 2-Diedergruppen, die normal in G, G' liegen. Es ist $G \sim G'$ genau dann, wenn $D \sim D'$.
ii) Sei $D \in \Gamma(\mathfrak{M})$ eine 2-Diedergruppe. Genau dann gibt es eine Oktaedergruppe $G \subset \Gamma(\mathfrak{M})$, die D als Normalteiler hat, wenn $D \in M^1(\mathfrak{M})$.

Bew.: i) folgt leicht mit (25.10)

ii) Sei $D = \{\pm 1, \pm U, \pm V, \pm UV\}$.

Ist G eine Oktaedergruppe, die D als Normalteiler hat, so wird G von $U' := (1+U)/\sqrt{2}$ und $V' := (1+V)/\sqrt{2}$ erzeugt.

Dann erzeugen U' und V eine 4-Diedergruppe; U und $T := U'V'$ erzeugen eine Tetraedergruppe in $\Gamma(\mathfrak{M})$. Beide Gruppen enthalten D.

Ist $D \in M^1$, so ist $T \in \Gamma(\mathfrak{M})$ und wir können o.B.d.A. annehmen (vgl. Bew. von 24.18), daß $U' \in \Gamma(\mathfrak{M})$. Dann erzeugen U' und $V' = TU'T^{-1}$ die Oktaedergruppe $G \subset \Gamma(\mathfrak{M})$, die D normal enthält.

(25.12) Korollar: gleiche Voraussetzung wie (25.11).

Dann ist $\mu_0(\mathfrak{M}) = \mu^1(\mathfrak{M})$.

§ 26 . Beispiel: 4-zyklische, 2-Dieder- und Tetraedergruppen in Quaternionenalgebren über imaginärquadratischen Zahlkörpern

Wir machen für diesen Paragrafen folgende Generalvoraussetzung:

(26.1) Sei $d \in \mathbb{N}$ quadratfrei, sei $k = \mathbb{Q}(i\sqrt{d})$, sei σ die Hauptordnung von k. Sei $Q = (-1, -1)_k$ und $K = k[X]/(X^2+1)k[X]$.

(Für $d \neq 1$ identifizieren wir $K = k(i)$)

Wir benutzen die gleichen Bezeichnungen wie in § 21.

Wir wollen $F_4^T(\mathfrak{M})$, $l_4^T(\mathfrak{M})$, $\mu_T(\mathfrak{M})$ und $\mu_2^-(\mathfrak{M})$ für die verschiedenen Maximalordnungen $\mathfrak{M}$ berechnen.

Im Anschluß daran werden wir die Ergebnisse aus den Paragrafen 21 und 26 zusammenfassen sowie spezielle Ergebnisse aus den Paragrafen 20, 21 und 26 tabellieren (für kleine d).

Es ist immer $s = 1$ und $F_8^*(\mathfrak{M}) = \emptyset$, da $\sqrt{2} \notin k$.

Also ist $g(\mathfrak{p}) = 1$ für alle $\mathfrak{p} \in F_4^*(\mathfrak{M})$.

Sei zuerst $d \equiv 7 \bmod 8$.

Für alle Q-Maximalordnungen $\mathfrak{M}$ ist $F_4^T(\mathfrak{M}) \subset F_4(\mathfrak{M}) = \{\sigma\}$.

Es ist $2\sigma = \mathfrak{p}\mathfrak{q}$ mit Primidealen $\mathfrak{p} \neq \mathfrak{q}$.

Es ist $(1+i)^2 O_\mathfrak{p}^\sigma = 2O_\mathfrak{p}^\sigma = \mathfrak{p} O_\mathfrak{p}^\sigma$ und $(1+i)^2 O_\mathfrak{q}^\sigma = \mathfrak{q} O_\mathfrak{q}^\sigma$.

Da K genau an den Stellen $\mathfrak{p}$ und $\mathfrak{q}$ über k verzweigt ist, folgt $Y^\sigma = A^\sigma$.

Daher folgt leicht durch Vergleich der entsprechenden Sätze:

(26.2) Lemma: Sei $d \equiv 7 \bmod 8$. Dann gibt es genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$ mit $F_4^T(\mathfrak{M}) = F_4^*(\mathfrak{M}) = \{\sigma\}$.
Für alle Q-Maximalordnungen $\mathfrak{M}$ gilt: $l_4^T(\mathfrak{M}) = l_4^*(\mathfrak{M})$ und
$\mu_T(\mathfrak{M}) = 2l_4^T(\mathfrak{M})$ sowie $\mu_2^-(\mathfrak{M}) = 0$.

Sei jetzt $d \equiv 3 \bmod 8$. Auch hier ist für alle Q-Maximalordnungen $\mathfrak{M}$:
$F_4^T(\mathfrak{M}) \subset F_4(\mathfrak{M}) = \{\sigma\}$.
2σ ist Primideal und $(1+i)^2\mathfrak{O}^\sigma = 2\mathfrak{O}^\sigma$.
Da K über k genau an der Stelle 2σ verzweigt ist, wird $Y^\sigma = A^\sigma$ und:

(26.3) Lemma: Sei $d \equiv 3 \bmod 8$. Dann gilt (26.2).

Sei jetzt $d \equiv 2 \bmod 4$. Es ist $2\sigma = \mathfrak{p}^2$ mit einem Primideal $\mathfrak{p}$.
Ist $\mathfrak{M}$ eine Q-Maximalordnung und $\mathfrak{f} \in F_4^T(\mathfrak{M})$, so folgt wegen $D_k(K) = 2\sigma$ aus (23.13.i), daß $2\mathfrak{f}_\sigma^2 = 2\mathfrak{o}_\sigma$ und $\mathfrak{f}_\mathfrak{q} = \mathfrak{o}_\mathfrak{q}$ für alle endlichen Primstellen $\mathfrak{q} \neq \mathfrak{p}$ von k. Also ist $\mathfrak{f} = \mathfrak{o}$.
Offensichtlich ist $C = \{\sigma\}$. Daher folgt mit (23.19):

(26.4) Lemma: Sei $d \equiv 2 \bmod 4$. Dann gibt es genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $F_4^T(\mathfrak{M}) = \{\sigma\}$. Für alle anderen Maximalordnungstypen $\widetilde{\mathfrak{M}}'$ ist $F_4^T(\mathfrak{M}') = \emptyset$.

Da $(1+i)^2\mathfrak{O}^\sigma = 2\mathfrak{O}^\sigma$, folgt $(1+i)\mathfrak{O}^\sigma = \mathfrak{p}\mathfrak{O}^\sigma$. Daher wird $Y^\sigma = (k \hookrightarrow \sigma)(I^k)$.
Ist $\mathfrak{M}$ eine Q-Maximalordnung mit $\sigma \in F_4^T(\mathfrak{M})$, so ist

$$l_4^T(\mathfrak{M}) = l_4^T(\mathfrak{M}, \sigma) = \frac{[Y^\sigma : Y^\sigma \cap H^\sigma]}{[N(Y^\sigma) : N(Y^\sigma) \cap H^k]} \cdot [\sigma^\times : N(\mathfrak{O}^{\sigma\times})] \text{ und}$$

$$\mu_T(\mathfrak{M}) = \frac{2 \cdot l_4^T(\mathfrak{M}, \sigma)}{[A^\sigma \cap H^\sigma : Y^\sigma \cap H^\sigma]}$$

Nach Lemma (19.7) ist $[A^\sigma : A^\sigma \cap H^\sigma] = \dfrac{[A^\sigma : (k \hookrightarrow \sigma)(I^k)] \cdot [I^k : H^k]}{2 \cdot [\sigma^\times : N(\mathfrak{O}^{\sigma\times})]}$

Also wird $\mu_T(\mathfrak{M}) =$

$$\frac{2 \cdot [Y^\sigma : Y^\sigma \cap H^\sigma] \cdot [\sigma^\times : N(\mathfrak{O}^{\sigma\times})]}{[A^\sigma \cap H^\sigma : Y^\sigma \cap H^\sigma] \cdot [I^{k(2)} : I^{k(2)} \cap H^k]} \cdot \frac{[A^\sigma : Y^\sigma] \cdot [I^k : H^k]}{2 \cdot [\sigma^\times : N(\mathfrak{O}^{\sigma\times})] \cdot [A^\sigma : A^\sigma \cap H^\sigma]}$$

d.h. $\mu_T(\mathfrak{M}) = \dfrac{[I^k : H^k]}{[I^{k(2)} H^k : H^k]} = [I^k : I^{k(2)} H^k] = 2^{\delta-1}$.

(26.5) Lemma: Sei $d \equiv 2 \bmod 4$. Dann ist $[A^\sigma \cap H^\sigma : Y^\sigma \cap H^\sigma] = 2$.

(langer) Bew.: Falls $d = 2$, ist $I^\sigma = H^\sigma$, also
$[\Lambda^\sigma \cap H^\sigma : Y^\sigma \cap H^\sigma] = [\Lambda^\sigma : (k \mapsto \sigma)(I^k)] = 2$ und $z = 2$, da $2 = 2^2 - 2 \cdot 1^2$.
Wir können also voraussetzen: $d \neq 2$
Λ^σ wird von den Idealen aus Y^σ und von $\mathfrak{P}$ mit $\mathfrak{P}^2 = \mathfrak{p}\mathcal{O}^\sigma$ erzeugt.
Da $\mathfrak{P}^2 \in Y^\sigma$, ist $[\Lambda^\sigma \cap H^\sigma : Y^\sigma \cap H^\sigma] < 2$.
Wenn $[\Lambda^\sigma \cap H^\sigma : Y^\sigma \cap H^\sigma] = 2$, gibt es $\mathfrak{a} \in I^k$, so daß $\mathfrak{a}\mathfrak{P} \in H^\sigma$.
Es ist dann $\mathfrak{a}\mathfrak{P} = a\mathcal{O}^\sigma$ mit $a \in K^\times$, also $N_{K'|k_+}(\mathfrak{P}) \cdot N_{K|k_+}(\mathfrak{a}\mathcal{O}^\sigma) = N_{K|k_+}(a)\,\sigma_+$.
Da $N_{K|k_+}(\mathfrak{a}\mathcal{O}^\sigma) = N_{k|\mathbb{Q}}(\mathfrak{a})\,\sigma_+ \in H^{k_+}$, ist also $N_{K'|k_+}(\mathfrak{P}) \in H^{k_+}$.
$\mathfrak{q} := N_{K|k_+}(\mathfrak{P})$ ist der Primteiler von 2 in k_+. Da $\mathfrak{q} \in H^{k_+}$, ist $\sigma = 2$ (siehe 21.7.ii).
Im Umkehrschluß folgt:
Wenn $q = 1$, ist $z = 1$ und (wie wir gerade gesehen haben) $[\Lambda^\sigma \cap H^\sigma : Y^\sigma \cap H^\sigma] = 1$.
Wir brauchen also nur noch den Fall $q = 2$ zu untersuchen.
Es ist $[\Lambda^\sigma \cap H^\sigma : Y^\sigma \cap H^\sigma] = \dfrac{[\Lambda^\sigma \cap H^\sigma : (k \mapsto \sigma)(H^k)]}{[Y^\sigma \cap H^\sigma : (k \mapsto \sigma)(H^k)]}$ und, wie im Beweis von (19.7) gezeigt wurde: $[\Lambda^\sigma \cap H^\sigma : (k \mapsto \sigma)(H^k)] = [\mathcal{O}^{\sigma\times} \cap N^{-1}(1) : \Delta(\mathcal{O}^{\sigma\times})]$.
Jetzt folgt mit (19.5) und (21.13):
$[\Lambda^\sigma \cap H^\sigma : (k \mapsto \sigma)(H^k)] = 2 \cdot [\sigma^\times : N(\mathcal{O}^{\sigma\times})] = 2xz/\sigma$.
Da $q = 2$, ist nach (21.10) auch $x = 2$.
Wir müssen also noch zeigen, daß $[Y^\sigma \cap H^\sigma : (k \mapsto \sigma)(H^k)] = 2$.
Wenn $\mathfrak{a} \in Y^\sigma \cap H^\sigma$, ist $\mathfrak{a} = \mathfrak{b}\mathcal{O}^\sigma = a\mathcal{O}^\sigma$ mit $\mathfrak{b} \in I^k$ und $a \in K^\times$.
Dann ist $N(\mathfrak{a}\mathcal{O}^\sigma) = \mathfrak{b}^2 = N(a)\sigma$, also $\mathfrak{b}^2 \in H^k$.
Bezeichne $'$ den nichttrivialen Automorphismus von K über k_+.
Dann ist auch $\mathfrak{b}\mathfrak{b}'^{-1} \in H^k$ und nach Lemma (20.21) ist $\mathfrak{b} \in \Lambda^k H^k$.
Also ist $[Y^\sigma \cap H^\sigma : (k \mapsto \sigma)(H^k)] = [(k \mapsto \sigma)(\Lambda^k H^k) \cap H^\sigma : (k \mapsto \sigma)(H^k)]$.
Da $(k \mapsto \sigma)(H^k) \subset H^\sigma$ und da $(k \mapsto \sigma)$ injektiv ist, wird:

$$[Y^\sigma \cap H^\sigma : (k \mapsto \sigma)(H^k)] = [\big((k \mapsto \sigma)(\Lambda^k) \cap H^\sigma\big)\big((k \mapsto \sigma)(H^k)\big) : (k \mapsto \sigma)(H^k)]$$
$$= [(k \mapsto \sigma)(\Lambda^k) \cap H^\sigma : (k \mapsto \sigma)(\Lambda^k) \cap (k \mapsto \sigma)(H^k)]$$
$$= [(k \mapsto \sigma)(\Lambda^k) \cap H^\sigma : (k \mapsto \sigma)(\Lambda^k \cap H^k)]$$

Sei $\overline{(k \mapsto \sigma)} : A^k/\Lambda^k \cap H^k \to (k \mapsto \sigma)(\Lambda^k)/(k \mapsto \sigma)(\Lambda^k) \cap H^\sigma$ die durch $(k \mapsto \sigma) : A^k \to (k \mapsto \sigma)(\Lambda^k)$ induzierte Abbildung.
Wir müssen zeigen, daß Kern $\overline{(k \mapsto \sigma)}$ die Ordnung 2 hat.

k und k_+ haben die gleichen endlichen Verzweigungsstellen über $\mathbb{Q}$.

Wir können daher einen surjektiven Homomorphismus $(k\to k_+): A^k \to A^{k_+}$ definieren durch $(k\to k_+)(\mathfrak{b}) = \mathfrak{b}\mathcal{O}^\sigma \cap k_+$ für $\mathfrak{b} \in A^k$.

Durch $(k\to k_+)$ wird ein surjektiver Homomorphismus

$\overline{(k\to k_+)}: A^k/A^k \cap H^k \to A^{k_+}/A^{k_+} \cap H^{k_+}$ induziert (vgl. Bew. von 20.18).

k_+ hat keine unendliche Verzweigungsstelle über $\mathbb{Q}$, also folgt mit (19.9):

$[A^{k_+} : A^{k_+} \cap H^{k_+}] = 2^{\delta-1}/[\mathbb{Z}^\times : N(\sigma_+^\times)] = 2^{\delta-2}$.

Da $[A^k : A^k \cap H^k] = 2^{\delta-1}$, hat Kern $\overline{(k\to k_+)}$ die Ordnung 2.

Wenn wir $(k_+\to\sigma): I^{k_+} \to I^\sigma$ definieren durch $(k_+\to\sigma)(\mathfrak{a}) = \mathfrak{a}\mathcal{O}^\sigma$ für $\mathfrak{a} \in I^{k_+}$, wird offensichtlich $(k\to\sigma) = (k_+\to\sigma)\circ(k\to k_+)$.

Wir müssen daher nur noch zeigen, daß $(k_+\to\sigma)$ eine injektive Abbildung

$\overline{(k_+\to\sigma)}: I^{k_+}/H^{k_+} \to I^\sigma/H^\sigma$ induziert.

Sei A' die Gruppe der über k_+ (bezüglich ') ambigen Ideale aus I^σ.

K hat über k_+ zwei reelle Verzweigungsstellen und die endliche Verzweigungsstelle σ. Daher ist nach (19.9):

$[A' : A' \cap H^\sigma] = 4\cdot[I^{k_+} : H^{k_+}]/[\sigma_+^\times : N_{K|k_+}(\mathcal{O}^{\sigma\times})]$

Mit (21.9.i) folgt, daß $\varepsilon \notin N_{K|k_+}(\mathcal{O}^{\sigma\times})$.

Da $-1 \notin N_{K|k_+}(\mathcal{O}^{\sigma\times})$, wird $[\sigma^\times : N_{K|k_+}(\mathcal{O}^{\sigma\times})] = 2$. Jetzt erhalten wir:

$$\left[(k_+\to\sigma)(I^{k_+}) : (k_+\to\sigma)(I^{k_+}) \cap H^\sigma\right] = \frac{[A' : A' \cap H^\sigma]\,[A' \cap H^\sigma : (k_+\to\sigma)(I^{k_+}) \cap H^\sigma]}{[A' : (k_+\to\sigma)(I^{k_+})]}$$

$$\geq [I^{k_+} : H^{k_+}]$$

Das genügt.

Wir haben also:

(26.6) Lemma: Sei $d \equiv 2 \bmod 4$ und $\mathfrak{M}$ eine Q-Maximalordnung mit $\sigma \in F_4^T(\mathfrak{M})$. Dann ist $l_4^T(\mathfrak{M}) = l_4^T(\mathfrak{M},\sigma) = 2^{\delta-2}z$ und $u_T(\mathfrak{M}) = 2^{\delta-1}$.

(26.7) Lemma: Sei $d \equiv 2 \bmod 4$ und $w = 2$. Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\sigma \in F_4^T(\mathfrak{M})$. Dann ist $u_2^-(\mathfrak{M}) = 2^{\delta-1}$.

Bew.: Wegen $F_4^T(\mathfrak{M}) \subset F_4^*(\mathfrak{M})$ und Lemma (21.38.i)' ist $F_4^*(\mathfrak{M}) = \{\sigma, \varphi\}$.

Nach (21.35) ist $l_4^*(\mathfrak{M},\sigma) = 2^{\delta-1}$. Nach (21.37) ist $l_4^*(\mathfrak{M},\varphi) = 2^{\delta-1}$.

Mit (24.28.ii) folgt: $u_2^-(\mathfrak{M}) = 1/3\cdot 2\cdot\left((2^{\delta-1}-2^{\delta-2}) + (2^{\delta-1}-0)\right) = 2^{\delta-1}$.

Falls w = 1, ist die Situation nicht auf den ersten Blick eindeutig. Es gibt die beiden Möglichkeiten (siehe 21.38.i):

i) $F_4^*(\mathfrak{M}) = \{\sigma\}$ und ii) $F_4^*(\mathfrak{M}) = \{\sigma, \mathfrak{p}\}$.

Im Fall i) ergibt sich $\mu_2^-(\mathfrak{M}) = 1/3 \cdot 2 \cdot (2^{\delta-2} - 2^{\delta-2}) = 0$

Im Fall ii) ergibt sich $\mu_2^-(\mathfrak{M}) = 1/3 \cdot 2 \cdot \left((2^{\delta-2}\ 2^{\delta-2}) + (2^{\delta-1} - 0)\right)$

$= 1/3 \cdot 2^{\delta}$, was nicht geht. Also gilt:

(26.8) Lemma: Sei $d \equiv 2 \bmod 4$ und $w = 1$. Sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\sigma \in F_4^T(\mathfrak{M})$. Dann ist $F_4^*(\mathfrak{M}) = \{\sigma\}$ und $\mu_2^-(\mathfrak{M}) = 0$.

Sei jetzt $d \equiv 1 \bmod 4$. Es ist $2\sigma = \mathfrak{p}^2$ mit einem Primideal $\mathfrak{p}$. Ist $\mathfrak{M}$ eine Q-Maximalordnung und $\mathfrak{f} \in F_4^T(\mathfrak{M})$, so folgt wegen $D_k(K) = \sigma$ aus (23.13.i), daß $\mathfrak{f}_\mathfrak{p}^2 = 2\sigma_\mathfrak{p}$ und $\mathfrak{f}_\mathfrak{q} = \sigma_\mathfrak{q}$ für alle endlichen Primstellen $\mathfrak{q} \neq \mathfrak{p}$ von k. Also ist $\mathfrak{f} = \mathfrak{p}$.
Offensichtlich ist $C = \{\sigma\}$. Daher folgt mit (23.19):

(26.9) Lemma: Sei $d \equiv 1 \bmod 4$. Dann gibt es genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $F_4^T(\mathfrak{M}) = \{\mathfrak{p}\}$. Für alle anderen Maximalordnungstypen $\widetilde{\mathfrak{M}'}$ ist $F_4^T(\mathfrak{M}') = \emptyset$.

Nach (21.32.i) ist $U_\mathfrak{p}^{\sigma\times} \cap \Lambda^{-1}(U_\mathfrak{p}^{\mathfrak{p}\times}) = U_\mathfrak{p}^{\mathfrak{p}\times}$. Daraus folgt leicht:

$A^\mathfrak{p} = (k \hookrightarrow \mathfrak{p})(I^k)$ (vgl. 19.10 und Bew. von 19.9).
Also ist $Y^\mathfrak{p} = A^\mathfrak{p} = (k \hookrightarrow \mathfrak{p})(I^k)$ und wir erhalten:

(26.10) Lemma: Sei $d \equiv 1 \bmod 4$ und sei $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{p} \in F_4^T(\mathfrak{M})$.

i) Falls $d \neq 1$, ist $l_4^T(\mathfrak{M}) = l_4^T(\mathfrak{M}, \mathfrak{p}) = 2^{\delta-2}$ und $\mu_T(\mathfrak{M}) = 2^{\delta-1}$.

ii) Falls $d = 1$, ist $l_4^T(\mathfrak{M}) = l_4^T(\mathfrak{M}, \mathfrak{p}) = \mu_T(\mathfrak{M}) = 1$.

Wenn wir $F_4^T(\mathfrak{M})$ für alle $\widetilde{\mathfrak{M}}$ kennen, kennen wir auch $F_4^*(\mathfrak{M})$ (siehe 21.30 und 21.31). Mit (24.28.ii) erhalten wir:

(26.11) Lemma: Sei $\mathfrak{M}$ eine Q-Maximalordnung.

i) Falls $d \equiv 1 \bmod 8$ und $w = 2$ und $F_4^*(\mathfrak{M}) = \{\sigma, \mathfrak{p}, 2\sigma\}$, ist $\mu_2^-(\mathfrak{M}) = 2^{\delta-1}$.

ii) Sei $d \equiv 1 \bmod 8$ und $w = 1$ oder sei $d \equiv 5 \bmod 8$.
Falls $F_4^T(\mathfrak{M}) = F_4^*(\mathfrak{M}) = \{\mathfrak{p}\}$, ist $\mu_2^-(\mathfrak{M}) = 0$.
Falls $F_4^*(\mathfrak{M}) = \{\sigma, 2\sigma\}$, ist $\mu_2^-(\mathfrak{M}) = 2^{\delta-1}$.

Wir fassen die wichtigsten Ergebnisse aus § 21 und § 26 zusammen:
(Zeichenerklärung folgt im Anschluß an 26.14)

(26.12) Satz: Sei $d \in \mathbb{N}$ quadratfrei, sei $k = \mathbb{Q}(i\sqrt{d})$ und sei $Q = (-1, -1)_k$.
i) Wenn $d \equiv 7 \bmod 8$, ist Q an den beiden Primteilern von 2 in k verzweigt. Es gibt genau einen Maximalordnungstyp $\mathfrak{M}$, so daß $\mu_T(\mathfrak{M}) = 2 \cdot \lambda_4^T(\mathfrak{M}) = 2 \cdot \lambda_4^*(\mathfrak{M}) = 2^\delta w$ und $\mu_2^-(\mathfrak{M}) = 0$ und $\lambda_4'(\mathfrak{M}) = 1/2 \cdot \left(z \cdot h(k_+) - 2^{\delta-1} w\right)$. Ist $\mathfrak{M}'$ einer der anderen $2^{\delta-2} w - 1$ Maximalordnungstypen, dann ist $\mu_T(\mathfrak{M}') = \mu_2^-(\mathfrak{M}') = \lambda_4^T(\mathfrak{M}') = \lambda_4^*(\mathfrak{M}') = 0$ und $\lambda_4'(\mathfrak{M}') = z/2 \cdot h(k_+)$.

ii) Wenn $d \equiv 3 \bmod 8$, ist $Q \tilde{\underset{k}{}} M_2(k)$. Es gibt genau einen Maximalordnungstyp $\mathfrak{M}$, so daß $\mu_T(\mathfrak{M}) = 2 \cdot \lambda_4^T(\mathfrak{M}) = 2 \cdot \lambda_4^*(\mathfrak{M}) = 2^\delta$ und $\mu_2^-(\mathfrak{M}) = 0$ und $\lambda_4'(\mathfrak{M}) = 1/2 \cdot \left(h(k_+) - 2^{\delta-1}\right)$. Ist $\mathfrak{M}'$ einer der anderen $2^{\delta-1} - 1$ Maximalordnungstypen, dann ist $\mu_T(\mathfrak{M}') = \mu_2^-(\mathfrak{M}') = \lambda_4^T(\mathfrak{M}') = \lambda_4^*(\mathfrak{M}') = 0$ und $\lambda_4'(\mathfrak{M}') = 1/2 \cdot h(k_+)$.

iii) Wenn $d \equiv 2 \bmod 4$ und $w = 2$, ist $Q \tilde{\underset{k}{}} M_2(k)$. Es gibt genau einen Maximalordnungstyp $\mathfrak{M}$, so daß $\mu_T(\mathfrak{M}) = \mu_2^-(\mathfrak{M}) = 1/2 \cdot \lambda_4^*(\mathfrak{M}) = 2^{\delta-1}$ und $\lambda_4^T(\mathfrak{M}) = 2^{\delta-2} z$ und $\lambda_4'(\mathfrak{M}) = 1/4 \cdot x(z+2) \cdot h(k_+) - 2^{\delta-1}$.
Ist $\mathfrak{M}'$ einer der anderen $2^{\delta-1} - 1$ Maximalordnungstypen, dann ist $\mu_T(\mathfrak{M}') = \mu_2^-(\mathfrak{M}') = \lambda_4^T(\mathfrak{M}') = \lambda_4^*(\mathfrak{M}') = 0$ und $\lambda_4'(\mathfrak{M}') = 1/4 \cdot x(z+2) \cdot h(k_+)$.

iv) Wenn $d \equiv 2 \bmod 4$ und $w = 1$, ist $Q \tilde{\underset{k}{}} M_2(k)$. Es gibt genau einen Maximalordnungstyp $\mathfrak{M}$, so daß $\mu_T(\mathfrak{M}) = 2 \cdot \lambda_4^T(\mathfrak{M}) = 2 \cdot \lambda_4^*(\mathfrak{M}) = 2^{\delta-1}$ und $\mu_2^-(\mathfrak{M}) = 0$ und $\lambda_4'(\mathfrak{M}) = 1/2 \cdot \left(3x \cdot h(k_+)/2 - 2^{\delta-2}\right)$.
Es gibt genau einen Maximalordnungstyp $\mathfrak{M}'$, so daß $\mu_T(\mathfrak{M}') = \lambda_4^T(\mathfrak{M}') = 0$ und $\mu_2^-(\mathfrak{M}') = 2^{\delta-1}$ und $\lambda_4^*(\mathfrak{M}') = 3 \cdot 2^{\delta-2}$ und $\lambda_4'(\mathfrak{M}') = 3/4 \cdot \left(x \cdot h(k_+) - 2^{\delta-1}\right)$.
Es ist $N(\mathfrak{M}\mathfrak{M}')_{\mathfrak{p}} \in I^{k(2)} {}_H{}^k$.
Ist $\mathfrak{M}''$ einer der anderen $2^{\delta-1} - 2$ Maximalordnungstypen, dann ist $\mu_T(\mathfrak{M}'') = \mu_2^-(\mathfrak{M}'') = \lambda_4^T(\mathfrak{M}'') = \lambda_4^*(\mathfrak{M}'') = 0$ und $\lambda_4'(\mathfrak{M}'') = 3x \cdot h(k_+)/4$.

v) Wenn $d \neq 1$ und $d \equiv 1 \bmod 8$ und $w = 2$, ist $Q \tilde{\underset{k}{}} M_2(k)$.
Es gibt genau einen Maximalordnungstyp $\mathfrak{M}$, so daß $\mu_T(\mathfrak{M}) = \mu_2^-(\mathfrak{M}) = 2 \cdot \lambda_4^T(\mathfrak{M}) = 1/2 \cdot \lambda_4^*(\mathfrak{M}) = 2^{\delta-1}$ und $\lambda_4'(\mathfrak{M}) = 2x \cdot h(k_+) - 2^{\delta-1}$.

Es gibt $2^{\delta-2} - 1$ Maximalordnungstypen $\widetilde{\mathfrak{M}}'$, so daß
$\mu_T(\mathfrak{M}') = \lambda_4^T(\mathfrak{M}') = \mu_2^-(\mathfrak{M}') = \lambda_4^*(\mathfrak{M}') = 0$ und $\lambda_4'(\mathfrak{M}') = 2x \cdot h(k_+)$;
und zwar sind das die Maximalordnungstypen $\widetilde{\mathfrak{M}}' \neq \widetilde{\mathfrak{M}}$ mit $N(\mathfrak{M}\mathfrak{M}') \in N(I^K)H^k$.
Für die restlichen $2^{\delta-2}$ Maximalordnungstypen $\widetilde{\mathfrak{M}}''$ ist
$\mu_T(\mathfrak{M}'') = \mu_2^-(\mathfrak{M}'') = \lambda_4^T(\mathfrak{M}'') = \lambda_4^*(\mathfrak{M}'') = \lambda_4'(\mathfrak{M}'') = 0$.

vi) Wenn $d \equiv 1 \bmod 8$ und $w = 1$, ist $Q \tilde{\underset{K}{}} M_2(k)$. Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $\mu_T(\mathfrak{M}) = 2 \cdot \lambda_4^T(\mathfrak{M}) = 2 \cdot \lambda_4^*(\mathfrak{M}) = 2^{\delta-1}$ und $\mu_2^-(\mathfrak{M}) = 0$ und $\lambda_4'(\mathfrak{M}) = 2x \cdot h(k_+) - 2^{\delta-3}$. Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}'$, so daß $\mu_T(\mathfrak{M}') = \lambda_4^T(\mathfrak{M}') = 0$ und $\mu_2^-(\mathfrak{M}') = 2^{\delta-1}$ und $\lambda_4^*(\mathfrak{M}') = 3 \cdot 2^{\delta-2}$ und $\lambda_4'(\mathfrak{M}') = 2x \cdot h(k_+) - 3 \cdot 2^{\delta-3}$. Es ist $N(\mathfrak{M}\mathfrak{M}')_{\mathfrak{p}} \in I^{k(2)}H^k$. Es gibt $2^{\delta-2} - 2$ Maximalordnungstypen $\widetilde{\mathfrak{M}}''$, so daß $\mu_T(\mathfrak{M}'') = \mu_2^-(\mathfrak{M}'') = \lambda_4^T(\mathfrak{M}'') = \lambda_4^*(\mathfrak{M}'') = 0$ und $\lambda_4'(\mathfrak{M}'') = 2x \cdot h(k_+)$;
und zwar sind das die Maximalordnungstypen $\widetilde{\mathfrak{M}}'' \notin \{\widetilde{\mathfrak{M}}, \widetilde{\mathfrak{M}}'\}$ mit
$N(\mathfrak{M}\mathfrak{M}'') \in N(I^K)H^k$. Für die restlichen $2^{\delta-2}$ Maximalordnungstypen $\widetilde{\mathfrak{M}}'''$
ist $\mu_T(\mathfrak{M}''') = \mu_2^-(\mathfrak{M}''') = \lambda_4^T(\mathfrak{M}''') = \lambda_4^*(\mathfrak{M}''') = \lambda_4'(\mathfrak{M}''') = 0$.

vii) Wenn $d \equiv 5 \bmod 8$, ist $Q \tilde{\underset{K}{}} M_2(k)$. Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$, so daß $\mu_T(\mathfrak{M}) = 2 \cdot \lambda_4^T(\mathfrak{M}) = 2 \cdot \lambda_4^*(\mathfrak{M}) = 2^{\delta-1}$ und $\mu_2^-(\mathfrak{M}) = 0$ und $\lambda_4'(\mathfrak{M}) = 1/2 \cdot \left(xy \cdot h(k_+) - 2^{\delta-2}\right)$. Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}'$, so daß $\mu_T(\mathfrak{M}') = \lambda_4^T(\mathfrak{M}') = 0$ und $\mu_2^-(\mathfrak{M}') = 2^{\delta-1}$ und $\lambda_4^*(\mathfrak{M}') = 3 \cdot 2^{\delta-2}$ und $\lambda_4'(\mathfrak{M}') = 1/2 \cdot \left(x(2y+1) \cdot h(k_+) - 3 \cdot 2^{\delta-2}\right)$.
Es ist $N(\mathfrak{M}\mathfrak{M}')_{\mathfrak{p}} \in I^{k(2)}H^k$. Es gibt $2^{\delta-2} - 1$ Maximalordnungstypen $\widetilde{\mathfrak{M}}_1$, so daß $\mu_T(\mathfrak{M}_1) = \mu_2^-(\mathfrak{M}_1) = \lambda_4^T(\mathfrak{M}_1) = \lambda_4^*(\mathfrak{M}_1) = 0$ und $\lambda_4'(\mathfrak{M}_1) = xy \cdot h(k_+)/2$; und zwar sind das die Maximalordnungstypen $\widetilde{\mathfrak{M}}_1 \neq \widetilde{\mathfrak{M}}$, so daß $N(\mathfrak{M}\mathfrak{M}_1) \in N(I^K)H^k$. Es gibt $2^{\delta-2} - 1$ Maximalordnungstypen $\widetilde{\mathfrak{M}}_1'$, so daß $\mu_T(\mathfrak{M}_1') = \mu_2^-(\mathfrak{M}_1') = \lambda_4^T(\mathfrak{M}_1') = \lambda_4^*(\mathfrak{M}_1') = 0$ und $\lambda_4'(\mathfrak{M}_1') = 1/2 \cdot x(2y+1) \cdot h(k_+)$; und zwar sind das die Maximalordnungstypen $\widetilde{\mathfrak{M}}_1' \neq \widetilde{\mathfrak{M}}'$ mit $N(\mathfrak{M}'\mathfrak{M}_1') \in N(I^K)H^k$.

viii) Wenn $d = 1$, ist $Q \tilde{\underset{K}{}} M_2(k)$. Es gibt genau einen Maximalordnungstyp. Für jede Q-Maximalordnung $\mathfrak{M}$ ist $\mu_T(\mathfrak{M}) = \mu_2^-(\mathfrak{M}) = \lambda_4^T(\mathfrak{M}) = 1$ und $\lambda_4^*(\mathfrak{M}) = 4$ und $\lambda_4'(\mathfrak{M}) = 0$

Zur besseren Übersicht tabellieren wir die Klassenzahlen sowie F_4, F_4^* und F_4^T.
In der Spalte ## steht die Zahl der Maximalordnungstypen, für die die nebenstehenden Werte zutreffen.
Die Maximalordnungstypen sind in der gleichen Reihenfolge aufgeführt wie in (26.12).

(26.13) Tabellarische Übersicht zu (26.12)

d	##	F_4	F_4^*	F_4^T	μ_T	$\bar{\mu}_2$	λ_4^T	λ_4^*	λ_4'
$d \equiv 7 \bmod 8$	1	$\mathfrak{o}$	$\mathfrak{o}$	$\mathfrak{o}$	$2^{\delta}w$	0	$2^{\delta-1}w$	$2^{\delta-1}w$	$1/2\cdot\left(z\cdot h(k_+) - 2^{\delta-1}w\right)$
	$2^{\delta-2}w - 1$	$\mathfrak{o}$	$\emptyset$	$\emptyset$	0	0	0	0	$1/2\cdot z\cdot h(k_+)$
$d \equiv 3 \bmod 8$	1	$\mathfrak{o}$	$\mathfrak{o}$	$\mathfrak{o}$	2^{δ}	0	$2^{\delta-1}$	$2^{\delta-1}$	$1/2\cdot\left(h(k_+) - 2^{\delta-1}\right)$
	$2^{\delta-1} - 1$	$\mathfrak{o}$	$\emptyset$	$\emptyset$	0	0	0	0	$1/2\cdot h(k_+)$
$d \equiv 2 \bmod 4$	1	$\mathfrak{o}, \mathfrak{p}$	$\mathfrak{o}, \mathfrak{p}$	$\mathfrak{o}$	$2^{\delta-1}$	$2^{\delta-1}$	$2^{\delta-2}z$	2^{δ}	$1/4\cdot x(z+2)\cdot h(k_+) - 2^{\delta-1}$
und $w = 2$	$2^{\delta-1} - 1$	$\mathfrak{o}, \mathfrak{p}$	$\emptyset$	$\emptyset$	0	0	0	0	$1/4\cdot x(z+2)\cdot h(k_+)$
$d \equiv 2 \bmod 4$	1	$\mathfrak{o}, \mathfrak{p}$	$\mathfrak{o}$	$\mathfrak{o}$	$2^{\delta-1}$	0	$2^{\delta-2}$	$2^{\delta-2}$	$1/2\cdot\left(3x\cdot h(k_+)/2 - 2^{\delta-2}\right)$
und $w = 1$	1	$\mathfrak{o}, \mathfrak{p}$	$\mathfrak{o}, \mathfrak{p}$	$\emptyset$	0	$2^{\delta-1}$	0	$3\cdot 2^{\delta-2}$	$3/4\cdot\left(x\cdot h(k_+) - 2^{\delta-1}\right)$
	$2^{\delta-1} - 2$	$\mathfrak{o}, \mathfrak{p}$	$\emptyset$	$\emptyset$	0	0	0	0	$3x\cdot h(k_+)/4$

(26.13) Tabellarische Übersicht zu (26.12), Fortsetzung

d	$\neq\neq$	F_4	F_4^*	F_4^T	μ_T	$\bar{\mu}_2$	λ_4^T	λ_4^*	λ_4'
$d \equiv 1 \bmod 8$	1	$\sigma, \varphi, 2\sigma$	$\sigma, \varphi, 2\sigma$	φ	$2^{\delta-1}$	$2^{\delta-1}$	$2^{\delta-2}$	2^{δ}	$2x \cdot h(k_+) - 2^{\delta-1}$
und $d \neq 1$	$2^{\delta-2} - 1$	$\sigma, \varphi, 2\sigma$	$\emptyset$	$\emptyset$	0	0	0	0	$2x \cdot h(k_+)$
und $w = 2$	$2^{\delta-2}$	$\emptyset$	$\emptyset$	$\emptyset$	0	0	0	0	0
$d \equiv 1 \bmod 8$	1	$\sigma, \varphi, 2\sigma$	φ	φ	$2^{\delta-1}$	0	$2^{\delta-2}$	$2^{\delta-2}$	$2x \cdot h(k_+) - 2^{\delta-3}$
und	1	$\sigma, \varphi, 2\sigma$	$\sigma, 2\sigma$	$\emptyset$	0	$2^{\delta-1}$	0	$3 \cdot 2^{\delta-2}$	$2x \cdot h(k_+) - 3 \cdot 2^{\delta-3}$
	$2^{\delta-2} - 2$	$\sigma, \varphi, 2\sigma$	$\emptyset$	$\emptyset$	0	0	0	0	$2x \cdot h(k_+)$
$w = 1$	$2^{\delta-2}$	$\emptyset$	$\emptyset$	$\emptyset$	0	0	0	0	0
	1	φ	φ	φ	$2^{\delta-1}$	0	$2^{\delta-2}$	$2^{\delta-2}$	$1/2 \cdot \left(xy \cdot h(k_+) - 2^{\delta-2}\right)$
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$	$\emptyset$	0	$2^{\delta-1}$	0	$3 \cdot 2^{\delta-2}$	$1/2 \cdot \left(x(2y+1) \cdot h(k_+) - 3 \cdot 2^{\delta-2}\right)$
$d \equiv 5 \bmod 8$	$2^{\delta-2} - 1$	φ	$\emptyset$	$\emptyset$	0	0	0	0	$1/2 \cdot xy \cdot h(k_+)$
	$2^{\delta-2} - 1$	$\sigma, 2\sigma$	$\emptyset$	$\emptyset$	0	0	0	0	$1/2 \cdot x(2y+1) \cdot h(k_+)$
$d = 1$	1	$\sigma, \varphi, 2\sigma$	$\sigma, \varphi, 2\sigma$	φ	1	1	1	4	0

(26.14) Satz: Sei $d \in \mathbb{N}$ quadratfrei, sei $k = \mathbb{Q}(i\sqrt{d})$. Sei Q eine k-Quaternionenalgebra. Sei $Q \not\cong_K (-1, -1)_k$, aber alle Verzweigungsstellen von Q über k seien in K verzweigt oder träge, d.h. die Bedingungen aus Satz (14.5) seien erfüllt, d.h. $\Gamma(Q)$ enthalte 4-zyklische Gruppen.
Dann ist $\lambda_4 = \lambda_4'$ konstant auf der Menge aller Q-Maximalordnungen.
Ist $\mathfrak{M}$ eine Q-Maximalordnung, dann gilt:

i) Wenn $d \equiv 7 \bmod 8$, ist $\lambda_4(\mathfrak{M}) = 2^{t-1}z \cdot h(k_+)$.

ii) Wenn $d \equiv 3 \bmod 8$, ist $\lambda_4(\mathfrak{M}) = 2^{t-1} \cdot h(k_+)$.

iii) Wenn $d \equiv 2 \bmod 4$ und Q an der Stelle $\mathfrak{p}$ verzweigt ist, ist $\lambda_4(\mathfrak{M}) = 2^{t-2}xz \cdot h(k_+)$.

iv) Wenn $d \equiv 2 \bmod 4$ und Q nicht an der Stelle $\mathfrak{p}$ verzweigt ist, ist $\lambda_4(\mathfrak{M}) = 2^{t-2}x(z+2) \cdot h(k_+)$.

v) Wenn $d \neq 1$ und $d \equiv 1 \bmod 8$, ist $\lambda_4(\mathfrak{M}) = 2^t x \cdot h(k_+)$.

vi) Wenn $d \equiv 5 \bmod 8$ und Q an der Stelle $\mathfrak{p}$ verzweigt ist, ist $\lambda_4(\mathfrak{M}) = 2^{t-2}x \cdot h(k_+)$.

vii) Wenn $d \equiv 5 \bmod 8$ und Q an der Stelle $\mathfrak{p}$ nicht verzweigt ist, ist $\lambda_4(\mathfrak{M}) = 2^{t-2}x(3y+1) \cdot h(k_+)$.

viii) Für $d = 1$ ist die Voraussetzung des Satzes nicht erfüllbar.

Zeichenerklärung zu (26.12) - (26.14):

δ ist die Zahl der endlichen Verzweigungsstellen von k über $\mathbb{Q}$.
$K = k[X]/(X^2+1)k[X]$.
Für $d \neq 1$ ist $k_+ = \mathbb{Q}(\sqrt{d})$. $h(k_+)$ ist die Klassenzahl von k_+.
$\mathfrak{o}$ ist die Hauptordnung von k.
Falls $d \not\equiv 3 \bmod 4$, ist $\mathfrak{p}$ das Primideal mit $2\mathfrak{o} = \mathfrak{p}^2$.
t ist die Zahl der Verzweigungsstellen von Q über k, die in K träge sind.
N bezeichnet immer die Norm von Idealen oder Zahlen aus Q oder K bzgl. k.

Es ist $w = \begin{cases} 2, & \text{wenn für alle Primteiler } p \neq 2 \text{ von } d \text{ gilt: } p \equiv \pm 1 \bmod 8 \\ 1, & \text{wenn } d \text{ Primteiler } p \equiv \pm 3 \bmod 8 \text{ hat} \end{cases}$

Für $d \neq 1$ ist

$$z = \begin{cases} 2, & \text{wenn } +2 \text{ Norm einer ganzen Zahl aus } k_+ \text{ ist} \\ 1, & \text{sonst} \end{cases}$$

und $\varepsilon = 1/2 \cdot (a + b\sqrt{d}) > 1$ die Grundeinheit in k_+ $(a, b \in \mathbb{N})$.

Dann ist

$$x = \begin{cases} 2, & \text{wenn } N_{k_+|\mathbb{Q}}(\varepsilon) = 1 \\ 1, & \text{wenn } N_{k_+|\mathbb{Q}}(\varepsilon) = -1 \end{cases} \qquad \text{und} \qquad y = \begin{cases} 3, & \text{wenn } b \equiv 0 \bmod 2 \\ 1, & \text{wenn } b \equiv 1 \bmod 2 \end{cases}$$

Erläuterungen zur Tabelle (26.15):

Wir wollen die Ergebnisse für $1 \leq d \leq 101$ und die Quaternionenalgebra $Q = M_2(k)$ tabellieren.
Dabei sei ## jeweils die Anhahl der verschiedenen Maximalordnungstypen, für die die nebenstehenden Werte gelten.
Für jedes d sind die Maximalordnungstypen (falls notwendig) in derselben Reihenfolge wie in Satz (26.12) aufgeführt.
Zur besseren Orientierung sind für $d \not\equiv 3 \bmod 4$ die Elemente aus $F_4^*(\mathfrak{M})$ aufgezählt. Für $d \equiv 5 \bmod 8$ sind auch die Elemente aus $F_4(\mathfrak{M})$ aufgezählt.

Es sind keine Nullen eingetragen. Die entsprechenden Felder sind stattdessen freigelassen.
Bei der Erstellung der Tabelle habe ich mit den Tabellen in /1/ gearbeitet.Alle notwendigen Werte außer z (für $d \not\equiv 1 \bmod 4$) lassen sich so ohne große Mühe bestimmen.
$z = 2$ kommt nur in Frage, wenn $w = 2$. Zur Bestimmung von z brauchen wir deshalb nur d = 2, 7, 14, 23, 31, 34, 46, 47, 62, 71, 79, 82, 94 zu untersuchen (hier ist $w = 2$). Für $\underline{d = 2}$ ist $2 = 2^2 - 2 \cdot 1^2$, also $z = 2$. Für $\underline{d = 82}$ ist $z = 1$ (siehe /10/ S.77). Für die anderen d ist $N_{k_+|\mathbb{Q}}(\varepsilon) = 1$, also höchstens eine der beiden Zahlen ± 2 Norm einer ganzen Zahl aus k_+. Für $\underline{d = 34}$ ist $2 = 6^2 - 34 \cdot 1^2$, also $z = 2$. Für die übrigen d ist $h(k_+) = 1$, also ist genau eine der Zahlen ± 2 Norm einer ganzen Zahl aus k_+. Für alle übriggebliebenen d ist $d \equiv 7 \bmod 8$ oder $d \equiv -2 \bmod 16$, nach (21.12.i) ist -2 nicht Norm einer ganzen Zahl aus k_+, also ist $z = 2$.

Das x in der letzten Spalte zeigt, welche Klassenzahlen zur Maximalordnung $\begin{pmatrix} \mathfrak{o} & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{o} \end{pmatrix}$ gehören (siehe Anhang zu dieser Arbeit).

(26.15) Tabelle der Konjugationsklassenzahlen μ_T, $\bar{\mu}_2$, λ_4^T, λ_4 und λ_4' für $\Omega = M_2(k)$, falls $k = \mathbb{Q}(i,\sqrt{d})$ und $1 \leq d \leq 101$

d	##	F_4	F_4^*	μ_T	$\bar{\mu}_2$	λ_4^T	λ_4^*	λ_4'	
1	1		$\sigma, \varphi, 2\sigma$	1	1	1	4		x
2	1		σ, φ	1	1	1	2		x
3	1			2		1	1		x
5	1	φ	φ	2		1	1		
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$		2		3		x
6	1		σ	2		1	1	1	x
	1		σ, φ		2		3		
7	1							1	x
10	1		σ	2		1	1	1	
	1		σ, φ		2		3		x
11	1			2		1	1		x
13	1	φ	φ	2		1	1		
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$		2		3		x
14	1		σ, φ	2	2	2	4		
	1							2	x
15	2							1	x
17	1		$\sigma, \varphi, 2\sigma$	2	2	1	4		x
	1								
19	1			2		1	1		x
21	1	φ	φ	4		2	2		
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$		4		6		
	1	φ						1	
	1	$\sigma, 2\sigma$						3	x
22	1		σ	2		1	1	1	x
	1		σ, φ		2		3		
23	1							1	x
26	1		σ	2		1	1	1	
	1		σ, φ		2		3		x
29	1	φ	φ	2		1	1		
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$		2		3		x

d	##	F_4	F_4^*	μ_T	$\bar{\mu}_2$	λ_4^T	λ_4^*	λ_4'	
30	1		σ	4		2	2	2	
	1		σ, φ		4		6		
	2							3	x
31	1							1	x
33	1		φ	4		2	2	3	x
	1		$\sigma, 2\sigma$		4		6	1	
	2								
34	1		σ, φ	2	2	2	4	2	x
	1							4	
35	1				4		2	2	
	1							1	x
37	1	φ	φ	2		1	1	1	
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$		2		3	2	x
38	1		σ	2		1	1	1	x
	1		σ, φ		2		3		
39	2							1	x
41	1		$\sigma, \varphi, 2\sigma$	2	2	1	4		x
	1								
42	1		σ	4		2	2	2	
	1		σ, φ		4		6		
	2							3	x
43	1				2		1	1	x
46	1		σ, φ	2	2	2	4		
	1							2	x
47	1							1	x
51	1				4		2	2	x
	1							1	
53	1	φ	φ	2		1	1		
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$		2		3		x
55	2							1	x

(26.15) Tabelle, Fortsetzung

d	##	F_4	F_4^*	μ_T	$\bar{\mu}_2$	λ_4^T	λ_4^*	λ_4'	
57	1		$\mathfrak{P}$	4		2	2	3	x
	1		$\sigma, 2\sigma$		4		6	1	
	2								
58	1		σ	2		1	1	1	
	1		$\sigma, \mathfrak{P}$		2		3		x
59	1			2		1	1		x
61	1	$\mathfrak{P}$	$\mathfrak{P}$	2		1	1		
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$		2		3		x
62	1		$\sigma, \mathfrak{P}$	2	2	2	4		
	1							2	x
65	1		$\mathfrak{P}$	4		2	2	3	
	1		$\sigma, 2\sigma$		4		6	1	x
	2								
66	1		σ	4		2	2	2	x
	1		$\sigma, \mathfrak{P}$		4		6		
	2							3	
67	1			2		1	1		x
69	1	$\mathfrak{P}$	$\mathfrak{P}$	4		2	2		
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$		4		6		
	1	$\mathfrak{P}$						1	
	1	$\sigma, 2\sigma$						3	x
70	1		σ	4		2	2	2	
	1		$\sigma, \mathfrak{P}$		4		6		
	2							3	x
71	1							1	x
73	1		$\sigma, \mathfrak{P}, 2\sigma$	2	2	1	4		x
	1								
74	1		σ	2		1	1	1	
	1		$\sigma, \mathfrak{P}$		2		3		x

d	##	F_4	F_4^*	μ_T	$\bar{\mu}_2$	λ_4^T	λ_4^*	λ_4'	
77	1	$\mathfrak{P}$	$\mathfrak{P}$	4		2	2		
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$		4		6		
	1	$\mathfrak{P}$						1	
	1	$\sigma, 2\sigma$						3	x
78	1		σ	4		2	2	2	
	1		$\sigma, \mathfrak{P}$		4		6		
	2							3	x
79	1							3	x
82	1		$\sigma, \mathfrak{P}$	2	2	1	4	1	x
	1							3	
83	1			2		1	1		x
85	1	$\mathfrak{P}$	$\mathfrak{P}$	4		2	2		
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$		4		6		x
	1	$\mathfrak{P}$						1	
	1	$\sigma, 2\sigma$						3	
86	1		σ	2		1	1	1	x
	1		$\sigma, \mathfrak{P}$		2		3		
87	2							1	x
89	1		$\sigma, \mathfrak{P}, 2\sigma$	2	2	1	4		x
	1								
91	1			4		2	2		
	1							1	x
93	1	$\mathfrak{P}$	$\mathfrak{P}$	4		2	2		
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$		4		6		
	1	$\mathfrak{P}$						1	
	1	$\sigma, 2\sigma$						3	x
94	1		$\sigma, \mathfrak{P}$	2	2	2	4		
	1							2	x
95	2							1	x
97	1		$\sigma, \mathfrak{P}, 2\sigma$	2	2	1	4		x
	1								
101	1	$\mathfrak{P}$	$\mathfrak{P}$	2		1	1	1	
	1	$\sigma, 2\sigma$	$\sigma, 2\sigma$		2		3	2	x

Erläuterungen zur Tabelle (26.16)

Wir wollen die Ergebnisse für $1 \leq d \leq 119$, $d \equiv 7 \bmod 8$ und die Quaternionenalgebra $Q = (-1, -1)_k$ tabellieren. Nach (26.12.i) ist $\mu_2^-(\mathfrak{M}) = 0$ für alle Q-Maximalordnungen $\mathfrak{M}$. Für $d = 103, 119$ ist $w = 2$.

Für $d = 103$ ist $N(\varepsilon) = +1$ und $h(k_+) = 1$, also ist genau eine der beiden Zahlen ± 2 Norm einer ganzen Zahl aus k_+. Es ist $103 \equiv 7 \bmod 8$, also ist -2 nicht Norm einer ganzen Zahl aus k_+ (21.12,i), d.h. $z = 2$.

Für $d = 119$ ist $2 = 11^2 - 119 \cdot 1^2$, also auch $z = 2$.

Eine Bemerkung zur Berechnung von λ_6^* und λ_6': Q ist an den beiden Primteilern von 2 in k verzweigt, insbesondere $Q \not\cong_k (-3, -1)_k$, d.h. $\lambda_6^*(\mathfrak{M}) = 0$ für alle Q-Maximalordnungen $\mathfrak{M}$. Wir können Satz (20.41) anwenden (es ist $t = 2$).

Im übrigen gelten die Bemerkungen zu Tabelle (26.15)

Erläuterungen zur Tabelle (26.17)

Wir wollen die Ergebnisse für $1 \leq d \leq 101$, $d \equiv 2 \bmod 3$ und $Q = (-3, -1)_k$ tabellieren. Mit (20.39.i) und (22.14.ii) berechnen wir μ_3, λ_6^* und λ_6'.

Es ist $Q \not\cong_k (-1, -1)_k$, also wird $\mu_T(\mathfrak{M}) = \mu_2^-(\mathfrak{M}) = \lambda_4^T(\mathfrak{M}) = \lambda_4^*(\mathfrak{M}) = 0$ für alle Q-Maximalordnungen $\mathfrak{M}$. Mit (26.14) berechnen wir $\lambda_4 = \lambda_4'$ (es ist $t = 2$). Im übrigen gelten die Bemerkungen zu Tabelle (26.15).

(26.16) Konjugationsklassenzahlen für $Q = (-1, -1)_k$, falls $k = \mathbb{Q}(i\sqrt{d})$, $d \equiv 7 \bmod 8$

d	#	μ_T	λ_4^T	λ_4'	λ_6
7	1	4	2		2
15	1	4	2		3
23	1	4	2		4
31	1	4	2		2
39	1	4	2		3
47	1	4	2		4
55	1	4	2		4
71	1	4	2		4
79	1	4	2	2	2
87	1	4	2		3
95	1	4	2		4
103	1	4	2		2
111	1	4	2		3
119	1	8	4		4
	1			2	4

(26.17) Konjugationsklassenzahlen für $Q = (-3, -1)_k$, falls $k = \mathbb{Q}(i\sqrt{d})$, $d \equiv 2 \bmod 3$

d	#	μ_3	λ_6^*	λ_6'	λ_4
2	1	4	2		4
5	1	4	2		4
11	1	4	2		2
14	1	4	2		8
17	1	4	2		4
23	1	4	2		4
26	1	8	4		6
	1			2	6
29	1	4	2		4
35	1	4	2		4
38	1	4	2		6
41	1	4	2		4
47	1	4	2		4
53	1	4	2		4
59	1	4	2		2
62	1	4	2		8
65	1	8	4		8
	1			2	8
71	1	4	2		4
74	1	8	4		6
	1			2	6
77	1	8	4		8
	1			2	8
83	1	4	2		2
86	1	4	2		6
89	1	4	2		4
95	1	4	2		4
101	1	4	2		10

Anhang

§ 27 . Die endlichen Untergruppen und ihre Konjugationsklassenzahlen in $SL(2,\mathfrak{o})$ über einem imaginärquadratischen Zahlkörper

Die Sätze (20.39), (20.41), (26.12) und (26.14) geben zwar eine Übersicht über die Konjugationsklassenzahlen der endlichen Gruppen in $\Gamma(\mathfrak{M})$ für die verschiedenen Maximalordnungen $\mathfrak{M} \subset M_2(k)$. Aber für eine vorgegebene Maximalordnung, etwa $M_2(\mathfrak{o})$, die richtigen Zahlen zu finden, ist nicht einfach.
In diesem Anhang wollen wir einige Lemmata entwickeln, die das Problem für $M_2(\mathfrak{o})$ bei einigen speziellen Körpern $k = \mathbb{Q}(i\sqrt{d})$ lösen (unter anderem für den Fall, daß d Primzahl oder das 3-fache einer Primzahl ist; und für alle $d \leq 101$).
Es ist hilfreich zu wissen, daß wir das Problem schon dann lösen können, wenn wir die endlichen Untergruppen von $SL(2,\mathfrak{o})$ bis auf Isomorphie kennen. (Das folgt ganz leicht aus den oben angegebenen Sätzen.)
Die Methoden in § 27 leben zum einen von den Ergebnissen des bisherigen Teils der Arbeit, zum anderen davon, daß wir Elemente endlicher Ordnung in $SL(2,k)$ explizit kennen.

Wir machen für diesen Paragrafen folgende Generalvoraussetzung:

(27.1) Sei $d \in \mathbb{N}$ quadratfrei. Sei $k = \mathbb{Q}(i\sqrt{d})$. Sei $\mathfrak{o}$ die Hauptordnung von k. Sei $Q = M_2(k)$. Sei δ die Zahl der endlichen Verzweigungsstellen von k über $\mathbb{Q}$. Wir behalten die in § 21 getroffenen Definitionen von q, K, k_+, $\mathfrak{o}_+$, w, z, $\varepsilon = 1/2\cdot(a + b\sqrt{d})$, x und y bei (siehe Zeichenerklärung zu 26.12 - 26.14). Die entsprechend in § 20 definierten Dinge benennen wir um in q', K', k'_+, $\mathfrak{o}'_+$, w', z', $\varepsilon' = 1/2\cdot(a'+b'\sqrt{d/3})$, x' und y'. Wir kürzen $\mathfrak{O}^{\mathfrak{p}} := \mathfrak{O}^{\mathfrak{p}}(K)$ und $\mathfrak{O}'^{\mathfrak{p}} := \mathfrak{O}^{\mathfrak{p}}(K')$ ab, falls $\mathfrak{p}$ ein ganzes $\mathfrak{o}$-Ideal ist. Falls 2 (bzw. 3) in k verzweigt ist, werde der Primteiler von 2 (bzw.3) in k mit $\mathfrak{p}$ (bzw. $\mathfrak{q}$) bezeichnet.

(27.2) Lemma: Sei $\mathfrak{M}$ eine Q-Maximalordnung.
i) Falls $d \equiv 7 \bmod 8$, ist $\mu_T(\mathfrak{M}) = \mu_2^-(\mathfrak{M}) = \lambda_4^T(\mathfrak{M}) = \lambda_4^*(\mathfrak{M}) = 0$.
ii) Falls $d \equiv 2 \bmod 3$, ist $\mu_3(\mathfrak{M}) = \lambda_6^*(\mathfrak{M}) = 0$.

Bew.: In diesem Fall ist $(-1, -1)_k$ bzw. $(-3, -1)_k$ Divisionsalgebra.

(27.3) Definition:

i) Für $\alpha \in I^k$ sei $\mathfrak{M}^\alpha := \begin{pmatrix} \sigma & \alpha^{-1} \\ \alpha & \sigma \end{pmatrix}$

ii) Sei $U := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ und $E := \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$

(27.4) Lemma: Es ist $\lambda_4(\mathfrak{M}^\sigma) > 0$ und $\lambda_6(\mathfrak{M}^\sigma) > 0$.

Bew.: Es ist $U \in \mathfrak{M}^\sigma$ und $S(U) = 0$ sowie $N(U) = 1$.
Es ist $E \in \mathfrak{M}^\sigma$ und $S(E) = 1$ sowie $N(E) = 1$ (siehe 12.6.i).

(27.5) Lemma: i) Falls $d \equiv 5 \bmod 8$, ist $F_4(\mathfrak{M}^\sigma) = \{\sigma, 2\sigma\}$ und $F_4(\mathfrak{M}^\mathfrak{p}) = \{\mathfrak{p}\}$.

ii) Falls $d \equiv 6 \bmod 9$, ist $F_6(\mathfrak{M}^\sigma) = \{\sigma\}$ und $F_6(\mathfrak{M}^\mathfrak{q}) = \{\sigma\}$.

Bew.: i) Sind $a, b \in k$ mit $a + bU = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathfrak{M}^\sigma$, so sind $a, b \in \sigma$.
Also ist $\mathfrak{M}^\sigma \cap k[U] = \sigma[U]$. Da $f(\sigma[U]) = 2\sigma$, ist $2\sigma \in F_4(\mathfrak{M}^\sigma)$.
Da $N(\mathfrak{M}^\sigma \mathfrak{M}^\mathfrak{p}) = \mathfrak{p}^{-1} \notin N(I^K)H^k$, folgt die Beh. mit (21.21.ii).
ii) entsprechend mit (20.25.ii)

(27.6) Korollar: i) Falls $d \equiv 5 \bmod 8$, ist $\mu_T(\mathfrak{M}^\sigma) = \lambda_4^T(\mathfrak{M}^\sigma) = 0$.

ii) Falls $d \equiv 6 \bmod 9$, ist $\mu_3(\mathfrak{M}^\sigma) = \lambda_6^*(\mathfrak{M}^\sigma) = 0$.

Bew.: i) Nach (26.9) ist $F_4^T(\mathfrak{M}^\sigma) \subset \{\mathfrak{p}\}$. Wegen (27.5.i) ist also $F_4^T(\mathfrak{M}^\sigma) = \emptyset$.

ii) folgt entsprechend wegen $F_6^*(\mathfrak{M}^\sigma) \subset \{\sigma\}$.

(27.7) Lemma: Sei $\mathfrak{M}$ eine Q-Maximalordnung.
i) Seien $U', V' \in \Gamma(\mathfrak{M})$ mit $S(U') = S(V') = 0$ und $U'V' = -V'U'$.
Sei $T' = 1/2 \cdot (1 + U' + V' + U'V') \in \Gamma(\mathfrak{M})$. Dann ist $\mathfrak{M} \cap k[T'] = \sigma[T']$.
ii) Seien $E', B' \in \Gamma(\mathfrak{M})$ mit $S(E') = 1$ und $B'E'B'^{-1} = E'^{-1}$.
Dann ist $\mathfrak{M} \cap k[B'] = \sigma[B']$.

Bew.: i) Es ist $D_k(\sigma[T']) = 3\sigma$, wegen $T' \in \mathfrak{M}$ also $D_k(\mathfrak{M} \cap k[T']) \mid 3\sigma$.
Sei $\mathfrak{O} := \sigma + \sigma U' + \sigma V' + \sigma T'$. Es ist $\mathfrak{O} \subset \mathfrak{M}$ und $\mathfrak{O} \cap k[T'] = \sigma[T']$.
Da $D_K(\mathfrak{O}) = D_k(1, U', V', T')\sigma = 4\sigma$, gilt für jeden Primteiler τ von 3σ:
$D_k(\mathfrak{O})_\tau = \sigma_\tau = D_k(\mathfrak{M})_\tau$, also $\mathfrak{O}_\tau = \mathfrak{M}_\tau$ und

$(\mathfrak{M} \cap k[T'])_\tau = (\mathfrak{O} \cap k[T'])_\tau = \mathfrak{o}_\tau[T']$.

$D_k(\mathfrak{M} \cap k[T'])$ und $D_k(\mathfrak{o}[T'])$ stimmen also in allen Komponenten überein; daher ist $\mathfrak{M} \cap k[T'] = \mathfrak{o}[T']$.

ii) folgt entsprechend aus $D_k(\mathfrak{o}[B']) = 4\mathfrak{o}$ und $D_k(1,E',B',E'B')\mathfrak{o} = 9\mathfrak{o}$.

(27.8) Lemma: Falls $d \equiv 21 \bmod 24$, ist $\lambda_4^*(\mathfrak{M}^\mathfrak{o}) = 0$.

Bew.: Es ist $d \equiv 5 \bmod 8$. Wäre $\lambda_4^*(\mathfrak{M}^\mathfrak{o}) > 0$, so wäre wegen $N(\mathfrak{M}^\mathfrak{o}\mathfrak{M}^\mathfrak{p}) = \mathfrak{p}^{-1}$ auch $\lambda_4^*(\mathfrak{M}^\mathfrak{p}) > 0$ (siehe 26.12.vii).

Wegen $\lambda_4^T(\mathfrak{M}^\mathfrak{o}) = 0$ wäre $\lambda_4^T(\mathfrak{M}^\mathfrak{p}) > 0$. Also enthielte $\Gamma(\mathfrak{M}^\mathfrak{p})$ eine Tetraedergruppe.

i) Sei $d \equiv 21 \bmod 72$. Dann ist $d \equiv 3 \bmod 9$. Da $\Gamma(\mathfrak{M}^\mathfrak{p})$ eine Tetraedergruppe enthält, ist $\lambda_6(\mathfrak{M}^\mathfrak{p}) > 0$. Man erkennt leicht mit (14.4), daß $\mathfrak{p}$ träge in K' ist, also ist $\mathfrak{p} \notin N(I^{K'})H^k$ (siehe 8.4.iii).

Nach (20.25.i) ist $\lambda_6(\mathfrak{M}^\mathfrak{o}) = 0$ ↯.

ii) $d \equiv 45 \bmod 72$ scheidet aus, da d quadratfrei ist.

iii) Sei $d \equiv 69 \bmod 72$. Dann ist $d \equiv 6 \bmod 9$.

Da $f(\mathfrak{o}[\zeta_6]) = \mathfrak{p}$, folgt mit (27.7.i), daß $\mathfrak{p} \in F_6(\mathfrak{M}^\mathfrak{p})$.

Da $\mathfrak{p} \notin N(I^{K'})H^k$, folgt mit (20.25.ii), daß $F_6(\mathfrak{M}^\mathfrak{o}) = \{\mathfrak{o}\}$ ↯.

(27.9) Lemma: Sei $d \equiv 0 \bmod 6$ oder $d \equiv 9 \bmod 24$.
Wenn $\lambda_4^*(\mathfrak{M}^\mathfrak{o}) > 0$ ist, dann ist sogar $\lambda_4^T(\mathfrak{M}^\mathfrak{o}) > 0$.

Bew.: Da $3|d$, ist $w = 1$. Da $\lambda_4^*(\mathfrak{M}^\mathfrak{o}) > 0$ und $N(\mathfrak{M}^\mathfrak{o}\mathfrak{M}^\mathfrak{p}) = \mathfrak{p}^{-1}$, ist auch $\lambda_4^*(\mathfrak{M}^\mathfrak{p}) > 0$ (siehe 26.12.iv und vi).

Wäre $\lambda_4^T(\mathfrak{M}^\mathfrak{o}) = 0$, so wäre $\lambda_4^T(\mathfrak{M}^\mathfrak{p}) > 0$.

i) Sei $d \equiv 3 \bmod 9$. Wie in (27.8.i) folgt $\lambda_6(\mathfrak{M}^\mathfrak{o}) = 0$ ↯.

ii) Sei $d \equiv 6 \bmod 9$. Wie in (27.8.iii) folgt $F_6(\mathfrak{M}^\mathfrak{o}) = \{\mathfrak{o}\}$ ↯.

(27.10) Lemma: Sei d Primzahl. Dann gilt:
i) Wenn $d \equiv 1 \bmod 8$ oder $d \equiv 3 \bmod 8$ oder $d = 2$, ist $\lambda_4^T(\mathfrak{M}^\mathfrak{o}) > 0$.
ii) Wenn $d \equiv 5 \bmod 8$, ist $\lambda_4^*(\mathfrak{M}^\mathfrak{o}) > 0$.

Bew.: i) Es gibt einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$ mit $\lambda_4^T(\widetilde{\mathfrak{M}}) > 0$.

Wenn $d \equiv 3 \bmod 8$ oder $d = 2$, ist $\neq\neq \widetilde{Q} = 2^{\delta-1} = 1$, also $\widetilde{\mathfrak{M}}^\mathfrak{o} = \widetilde{\mathfrak{M}}$.

Wenn $d \equiv 1 \bmod 8$, ist $\#\widetilde{Q} = 2^{\delta-1} = 2$. Es gibt einen Maximalordnungstyp $\widetilde{\mathfrak{M}}' \neq \widetilde{\mathfrak{M}}$ mit $\lambda_4(\mathfrak{M}') = 0$. Also ist notwendig $\widetilde{\mathfrak{M}}^{\upsilon} = \widetilde{\mathfrak{M}}$.

ii) Es ist $\#\widetilde{Q} = 2^{\delta-1} = 2$. Für beide Maximalordnungstypen $\widetilde{\mathfrak{M}}$ ist $\lambda_4^*(\mathfrak{M}) > 0$.

(27.11) Lemma: Seien p und p' Primzahlen mit $p \equiv p' \equiv 3 \bmod 8$ oder $p \equiv p' \equiv 5 \bmod 8$. Sei $d = pp'$ oder sei $d = 2p$. Dann ist $\lambda_4^*(\mathfrak{M}^{\upsilon}) > 0$.

Bew.: i) Sei $d = pp'$. Dann ist $d \equiv 1 \bmod 8$ und $w = 1$ und $\#\widetilde{Q} = 2^{\delta-1} = 4$.
Für zwei Maximalordnungstypen $\widetilde{\mathfrak{M}}$ ist $\lambda_4^*(\mathfrak{M}) > 0$.
Für die beiden anderen Maximalordnungstypen $\widetilde{\mathfrak{M}}'$ ist $\lambda_4(\mathfrak{M}') = 0$.

ii) Sei $d = 2p$. Dann ist $d \equiv 2 \bmod 4$ und $w = 1$ und $\#\widetilde{Q} = 2^{\delta-1} = 2$.
Für beide Maximalordnungstypen $\widetilde{\mathfrak{M}}$ ist $\lambda_4^*(\mathfrak{M}) > 0$.

(27.12) Lemma: Sei p Primzahl mit $p \equiv 1 \bmod 8$ oder $p \equiv 3 \bmod 8$ oder $p = 2$. Sei $d = 3p$. Dann ist $\lambda_4^T(\mathfrak{M}^{\upsilon}) > 0$.

Bew.: i) Sei $p \equiv 1 \bmod 8$. Dann ist $d \equiv 3 \bmod 8$ und $\#\widetilde{Q} = 2^{\delta-1} = 2$.
Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$ mit $\lambda_4^T(\mathfrak{M}) > 0$
und genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}'$ mit $\lambda_4^T(\mathfrak{M}') = 0$.
Es ist $d \equiv 0 \bmod 3$, also $f(\upsilon[\zeta_6]) = \upsilon\eta$. Nach (27.7.i) ist $\upsilon\eta \notin F_6(\mathfrak{M})$.
Falls $d \equiv 3 \bmod 9$, ist $F_6(\mathfrak{M}') = \emptyset$ nach (20.25.i).
Falls $d \equiv 6 \bmod 9$, ist $F_6(\mathfrak{M}') = \{\upsilon\}$ nach (20.25.ii).
Da $\upsilon\eta \in F_6(\mathfrak{M}^{\upsilon})$, ist notwendig $\widetilde{\mathfrak{M}}^{\upsilon} = \widetilde{\mathfrak{M}}$.

ii) Sei $p \equiv 3 \bmod 8$ oder $p = 2$. Nach (27.11) ist $\lambda_4^*(\mathfrak{M}^{\upsilon}) > 0$.
Es ist $d \equiv 9 \bmod 24$ oder $d = 6$. Nach (27.9) ist $\lambda_4^T(\mathfrak{M}^{\upsilon}) > 0$.

(27.13) Lemma: Sei d Primzahl und $d \equiv 1 \bmod 3$. Dann ist $\lambda_6^*(\mathfrak{M}^{\upsilon}) > 0$.

Bew.: i) Sei $d \equiv 7 \bmod 12$. Dann ist $\#\widetilde{Q} = 2^{\delta-1} = 1$.
Nach (20.39.ii) also notwendig $\lambda_6^*(\mathfrak{M}^{\upsilon}) > 0$.

ii) Sei $d \equiv 1 \bmod 12$. Dann ist $\#\widetilde{Q} = 2^{\delta-1} = 2$.
Es gibt genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$ mit $\lambda_6^*(\mathfrak{M}) > 0$
und genau einen Maximalordnungstyp $\widetilde{\mathfrak{M}}'$ mit $\lambda_6^*(\mathfrak{M}') = 0$.
Es ist $d \equiv 1 \bmod 4$, also $f(\upsilon[i]) = 2\upsilon$. Nach (27.7.ii) ist $2\upsilon \in F_4(\mathfrak{M})$.

Falls $d \equiv 1 \bmod 8$, ist $F_4(\mathfrak{M}') = \emptyset$ nach (21.21.i).
Falls $d \equiv 5 \bmod 8$, ist $F_4(\mathfrak{M}') = \{\mathfrak{p}\}$ nach (21.21.ii).
Da $2\sigma \in F_4(\mathfrak{M}^\sigma)$, ist notwendig $\widetilde{\mathfrak{M}^\sigma} = \widetilde{\mathfrak{M}}$.

(27.14) Lemma: Sei p Primzahl mit $p \equiv 1 \bmod 3$. Sei $d = 3p$.
Dann ist $\lambda_6^*(\mathfrak{M}^\sigma) > 0$.

Bew.: i) Sei $p \equiv 1 \bmod 12$. Dann ist $d \equiv 3 \bmod 9$ und $\neq \widetilde{Q} = 2^{\delta-1} = 2$.
Für einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$ ist $\lambda_6^*(\mathfrak{M}) > 0$. Für den anderen Maximalordnungstyp $\widetilde{\mathfrak{M}'}$ ist $\lambda_6(\mathfrak{M}') = 0$. Also ist notwendig $\widetilde{\mathfrak{M}^\sigma} = \widetilde{\mathfrak{M}}$.

ii) Sei $p \equiv 7 \bmod 24$. Dann ist $d \equiv 3 \bmod 9$ und $d \equiv 5 \bmod 8$ und $\neq \widetilde{Q} = 2^{\delta-1} = 4$. Es gibt zwei Maximalordnungstypen $\widetilde{\mathfrak{M}}_1 \neq \widetilde{\mathfrak{M}}_2$ mit $\lambda_6(\mathfrak{M}_1) = \lambda_6(\mathfrak{M}_2) = 0$. Es gibt einen Maximalordnungstyp $\widetilde{\mathfrak{M}}_3$ mit $\lambda_4^T(\mathfrak{M}_3) > 0$ (und insbesondere $\lambda_6(\mathfrak{M}_3) > 0$).
Dann ist $F_4(\mathfrak{M}_3) = \{\mathfrak{p}\}$ (siehe 26.9 und 21.21.ii).
Nach (27.4) und (27.5.i) ist $\widetilde{\mathfrak{M}^\sigma} \notin \{\widetilde{\mathfrak{M}}_1, \widetilde{\mathfrak{M}}_2, \widetilde{\mathfrak{M}}_3\}$.
Es gibt einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$ mit $\lambda_6^*(\mathfrak{M}) > 0$. Insbesondere ist $\lambda_6(\mathfrak{M}) > 0$. Da $d \equiv 5 \bmod 8$, ist $f(\sigma[i]) = 2\sigma$. Nach (27.7.ii) ist daher $2\sigma \in F_4(\mathfrak{M})$. Also ist $\widetilde{\mathfrak{M}} \notin \{\widetilde{\mathfrak{M}}_1, \widetilde{\mathfrak{M}}_2, \widetilde{\mathfrak{M}}_3\}$, d.h. $\widetilde{\mathfrak{M}} = \widetilde{\mathfrak{M}^\sigma}$.

iii) Sei $p \equiv 19 \bmod 24$. Dann ist $d \equiv 3 \bmod 9$ und $d \equiv 1 \bmod 8$ und $\neq \widetilde{Q} = 2^{\delta-1} = 4$. Es ist $\mathfrak{p}$ zerlegt in K und träge in K'.
Entsprechend ist $\mathfrak{q}$ zerlegt in K' und träge in K.
Also ist $\mathfrak{p} \in N(I^K)H^k$, aber $\mathfrak{p} \notin N(I^{K'})H^k$; es ist $\mathfrak{q} \in N(I^{K'})H^k$, aber $\mathfrak{q} \notin N(I^K)H^k$.
Daher sind $\widetilde{\mathfrak{M}^\sigma}$, $\widetilde{\mathfrak{M}^\mathfrak{p}}$, $\widetilde{\mathfrak{M}^\mathfrak{q}}$ und $\widetilde{\mathfrak{M}^{\mathfrak{p}\mathfrak{q}}}$ paarweise verschieden.
Da $\lambda_4(\mathfrak{M}^\sigma) > 0$ und $\lambda_6(\mathfrak{M}^\sigma) > 0$, folgt mit (20.25.i) und (21.21.i), daß $\lambda_6(\mathfrak{M}^\mathfrak{p}) = \lambda_6(\mathfrak{M}^{\mathfrak{p}\mathfrak{q}}) = 0$ und $\lambda_4(\mathfrak{M}^\mathfrak{q}) = \lambda_4(\mathfrak{M}^{\mathfrak{p}\mathfrak{q}}) = 0$.
Es gibt einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$ mit $\lambda_6^*(\mathfrak{M}) > 0$. Insbesondere ist $\lambda_6(\mathfrak{M}) > 0$ und $\lambda_4(\mathfrak{M}) > 0$. Da $\neq \widetilde{Q} = 4$, ist notwendig $\widetilde{\mathfrak{M}} = \widetilde{\mathfrak{M}^\sigma}$.

In iii) haben wir folgendes interessante Korollar bewiesen, das offenbar auch gilt, wenn d/3 keine Primzahl ist:

(27.15) Korollar: Sei $d \equiv 57 \bmod 72$. Dann sind $\{1\}$ und $\{\pm 1\}$ die einzigen endlichen Untergruppen von $\Gamma(\mathfrak{M}^{\beta\gamma})$.

Bemerkung: Offensichtlich ist $d \equiv 57 \bmod 72$ (d.h. $d \equiv 3 \bmod 9$ und $d \equiv 1 \bmod 8$) notwendige Bedingung dafür, daß es eine Q-Maximalordnung $\mathfrak{M}$ gibt mit $\lambda_4(\mathfrak{M}) = \lambda_6(\mathfrak{M}) = 0$.
Ist $d \equiv 52 \bmod 72$ und $\mathfrak{M}$ eine Q-Maximalordnung, so ist $\lambda_4(\mathfrak{M}) = \lambda_6(\mathfrak{M}) = 0$ genau dann, wenn $N(\mathfrak{M}\mathfrak{M}^{\beta\gamma}) \in N(I^K)H^k \cap N(I^{K'})H^k$.

(27.16) Lemma: Sei $d \equiv 1 \bmod 4$ oder $d \equiv 2 \bmod 4$. Sei $d \neq 1$.
i) Wenn $x = 1$, ist $\lambda_4^*(\mathfrak{M}^{\sigma}) > 0$ und $\mu_2^-(\mathfrak{M}^{\sigma}) > 0$.
ii) Wenn $x = 2$, ist $\lambda_4'(\mathfrak{M}^{\sigma}) > 0$.

Bew.: Falls $d \equiv 1 \bmod 4$, ist $\sigma[i] = \mathcal{O}^{2\sigma}$. Wie in den Rechnungen vor (21.24) und (21.25) nachgewiesen, ist dann $[\sigma^\times : N(\sigma[i]^\times)] = x$.
Falls $d \equiv 2 \bmod 4$, ist $\sigma[i] = \mathcal{O}^{\beta}$. Wie vor (21.20) nachgewiesen, ist auch hier $[\sigma^\times : N(\sigma[i]^\times)] = x$.
i) Sei $x = 1$. Dann gibt es $a, b \in \sigma$ mit $a^2 + b^2 = N(a + bi) = -1$.
Man überzeugt sich leicht, daß U und $V = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$ eine 2-Diedergruppe in $\Gamma(\mathfrak{M}^{\sigma})$ erzeugen. Also ist $\lambda_4^*(\mathfrak{M}^{\sigma}) > 0$.

Wäre $\mu_2^-(\mathfrak{M}^{\sigma}) = 0$, so müßte gelten:
$1/2 \cdot \begin{pmatrix} 1+a-b & -1+a+b \\ 1+a+b & 1-a-b \end{pmatrix} = 1/2 \cdot (1 + U + V + UV) \in \mathfrak{M}^{\sigma}$, also $1+a+b \in 2\sigma \subset \mathfrak{P}$.
Wegen $\mathfrak{N}(\mathfrak{P}) = 2$ müßte also entweder $a \in \mathfrak{P}$ oder $b \in \mathfrak{P}$ sein.
Wir nehmen o.B.d.A. an, daß $a \in \mathfrak{P}$ und $b \notin \mathfrak{P}$.
Es müßte $2 \cdot (a+b+ab) = 1+a^2+b^2+2 \cdot (a+b+ab) = (1+a+b)^2 \in 4\sigma$ sein, also $a+b+ab \in 2\sigma$. Daraus folgt $b \in \mathfrak{P}$ ↯.
ii) Sei $x = 2$. Wäre $\lambda_4'(\mathfrak{M}^{\sigma}) = 0$, so gäbe es $a, b, c, d' \in \sigma$, so daß U und $V = \begin{pmatrix} a & b \\ c & d' \end{pmatrix}$ eine 2-Diedergruppe in $\Gamma(\mathfrak{M}^{\sigma})$ erzeugen.
Dann wäre $\begin{pmatrix} -c & -d' \\ a & b \end{pmatrix} = UV = -VU = \begin{pmatrix} -b & a \\ -d' & c \end{pmatrix}$ und $ad' - bc = 1$.
Also $d' = -a$, $b = c$ und $-a^2-b^2 = 1$, d.h. $N(a+ib) = -1$ ↯.

(27.17) Lemma: Sei $d \equiv 3 \bmod 8$.
i) Falls $-2 \in N_{k_+|\mathbb{Q}}(\sigma_+)$, ist $\lambda_4^*(\mathfrak{M}^{\sigma}) > 0$ (nach 26.12.ii also auch $\lambda_4^T(\mathfrak{M}^{\sigma}) > 0$).
ii) Falls $-2 \notin N_{k_+|\mathbb{Q}}(\sigma_+)$, ist $\lambda_4'(\mathfrak{M}^{\sigma}) > 0$.

Bew.: Es ist $o[i] = \mathcal{O}^o$. Nach (21.13) ist $[o^\times : N(o[i]^\times)] = xz/q$. Da $d \equiv 3 \bmod 4$, ist $x = 2$. Insbesondere kann nicht sowohl $-2 \in N_{k_+|\mathbb{Q}}(o_+)$ als auch $+2 \in N_{k_+|\mathbb{Q}}(o_+)$ sein. Also ist $[o^\times : N(o[i]^\times)] = 1$ genau dann, wenn $-2 \in N_{k_+|\mathbb{Q}}(o_+)$ (dann ist $z = 1$ und $q = 2$). Sonst ist $[o^\times : N(o[i]^\times)] = 2$. Der Beweis geht jetzt genauso wie der Beweis von (27.16). (Allerdings ist 2 in k träge, daher können wir nicht schließen: $\mu_2^-(\mathfrak{M}^o) > 0$)

(27.18) Korollar: Sei $d \equiv 3 \bmod 8$. Falls d einen Primteiler p mit $p \equiv 5 \bmod 8$ oder $p \equiv 7 \bmod 8$ hat, ist $\lambda_4'(\mathfrak{M}^o) > 0$.

Bew.: vgl. (21.12.i)

(27.19) Lemma: Sei $d \equiv 1 \bmod 8$, sei $x = 2$, sei $w = 1$ und sei $h(k_+) = 2^{\delta-3}$. Dann ist $\mu_2^-(\mathfrak{M}^o) = 0$.

Bew.: Wäre $\mu_2^-(\mathfrak{M}^o) > 0$, dann müßte $F_4(\mathfrak{M}^o) = \{o, \mathfrak{p}, 2o\}$ und $F_4^*(\mathfrak{M}^o) = \{o, 2o\}$ sein (vgl.26.11.ii). Dann wäre $l_4(\mathfrak{M}^o, 2o) = 2x \cdot h(k_+) = 2^{\delta-1} = l_4^*(\mathfrak{M}^o, 2o)$ (siehe 21.24 und 21.33). Dies ist ein Widerspruch, da $U \in L_4(\mathfrak{M}^o, 2o)$ aber $U \notin L_4^*(\mathfrak{M}^o, 2o)$. (siehe 27.16.ii).

(27.20) Lemma: Sei $d \equiv 2 \bmod 4$.
i) Falls $-2 \in N_{k_+|\mathbb{Q}}(o_+)$, dann ist $\lambda_4^T(\mathfrak{M}^o) > 0$.

ii) Falls $-2 \notin N_{k_+|\mathbb{Q}}(o_+)$ und $x = 2$ und $h(k_+) = 2^{\delta-2}$, dann ist $\lambda_4^*(\mathfrak{M}^o) = 0$.

iii) Falls $q = 1$ und $x = 2$ und $h(k_+) = 2^{\delta-1}$ und $w = 2$, dann ist $\lambda_4^*(\mathfrak{M}^o) = 0$.

Bew:i) Für $d = 2$ ist die Beh. klar. Sei also $d \neq 2$.
Da $q = 2$, ist nach (21.10) auch $x = 2$. Nach Vor. folgt daraus $z = 1$.
Nach (21.13) ist also $[o^\times : N(\mathcal{O}^{o\times})] = xz/q = 1$.
Man überprüft leicht, daß $\mathcal{O}^o = o + \mathfrak{p}^{-1}(1+i)$.
Es gibt also $a \in o$ und $b \in \mathfrak{p}^{-1}$ mit $-1 = N(a+b(1+i)) = a^2+2ab+2b^2$.
Man kann leicht nachprüfen, daß $U' := \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}$ und $V' := \begin{pmatrix} a & b \\ 2a+2b & -a \end{pmatrix}$ eine 2-Diedergruppe in $\Gamma(\mathfrak{M}^\mathfrak{p})$ erzeugen. Also ist $\lambda_4^*(\mathfrak{M}^\mathfrak{p}) > 0$.

Falls w = 2, ist $\mathfrak{p} \in I^{k(2)}H^k$ (vgl. Vorbemerkung zu 21.29).
Da $N(\mathfrak{M}^{\mathfrak{o}}\mathfrak{M}^{\mathfrak{p}}) = \mathfrak{p}^{-1}$, ist dann $\widetilde{\mathfrak{M}^{\mathfrak{o}}} = \widetilde{\mathfrak{M}^{\mathfrak{p}}}$, also $\lambda_4^*(\mathfrak{M}^{\mathfrak{o}}) > 0$.

Nach (26.12.iii) ist dann auch $\lambda_4^T(\mathfrak{M}^{\mathfrak{o}}) > 0$.

Wir nehmen jetzt an, daß w = 1. Dann ist $\mathfrak{p} \notin I^{k(2)}H^k$, also $\widetilde{\mathfrak{M}^{\mathfrak{o}}} \neq \widetilde{\mathfrak{M}^{\mathfrak{p}}}$.
Nach (26.12.iv) ist $\lambda_4^*(\mathfrak{M}^{\mathfrak{o}}) > 0$ und es gilt:

Entweder ist $\lambda_4^T(\mathfrak{M}^{\mathfrak{o}}) > 0$ und $\mu_2^-(\mathfrak{M}^{\mathfrak{o}}) = 0$ oder $\lambda_4^T(\mathfrak{M}^{\mathfrak{p}}) > 0$
und $\mu_2^-(\mathfrak{M}^{\mathfrak{p}}) = 0$. Wäre $\lambda_4^T(\mathfrak{M}^{\mathfrak{p}}) > 0$ und $\mu_2^-(\mathfrak{M}^{\mathfrak{p}}) = 0$, so müßte
$1/2\cdot\begin{pmatrix}2-2b & -1+a\\ 2+2a & 2b\end{pmatrix} = 1/2\cdot(1 + U' + V' + U'V') \in \mathfrak{M}^{\mathfrak{p}}$ sein. Dann wäre
$b \in \mathfrak{o}$, also $a+b(1+i) \in \mathfrak{O}^{\mathfrak{p}}$. Daraus folgt $x = \left[\mathfrak{o}^\times : N(\mathfrak{O}^{\mathfrak{p}\times})\right] = 1$ ↯.

ii), iii) Ist $\mathfrak{M}$ eine Q-Maximalordnung mit $\mathfrak{o} \in F_4^*(\mathfrak{M})$, dann ist
$l_4(\mathfrak{M},\mathfrak{o}) = 1/2\cdot xz\cdot h(k_+)$ und $l_4^*(\mathfrak{M},\mathfrak{o}) = 2^{\delta-2}w$ (siehe 21.18 und 21.35).
Natürlich ist $l_4(\mathfrak{M},\mathfrak{o}) \geq l_4^*(\mathfrak{M},\mathfrak{o})$.
Wenn Voraussetzung ii) erfüllt ist, folgt also $z \geq w$. Da natürlich
$z \leq w$, haben wir dann: $l_4(\mathfrak{M},\mathfrak{o}) = l_4^*(\mathfrak{M},\mathfrak{o})$.
Wenn Voraussetzung iii) erfüllt ist, ist z = 1 und w = 2. Wir haben
also auch dann $l_4(\mathfrak{M},\mathfrak{o}) = l_4^*(\mathfrak{M},\mathfrak{o})$.

Wäre $\lambda_4^*(\mathfrak{M}^{\mathfrak{o}}) > 0$, so wäre auch $\lambda_4^*(\mathfrak{M}^{\mathfrak{p}}) > 0$ (Bew. wie in i)).

Dann wäre $\mathfrak{o} \in F_4^*(\mathfrak{M}^{\mathfrak{p}})$, also $L_4(\mathfrak{M}^{\mathfrak{p}},\mathfrak{o}) = L_4^*(\mathfrak{M}^{\mathfrak{p}},\mathfrak{o})$.
Sei $U' = \begin{pmatrix}1 & -1\\ 2 & -1\end{pmatrix}$. Wegen $\mathfrak{p}^{-1}(1+U') \in \mathfrak{M}^{\mathfrak{p}}$ ist
$\mathfrak{M}^{\mathfrak{p}} \cap k[U'] = \mathfrak{o} + \mathfrak{p}^{-1}(1+U') = \mathfrak{O}^{\mathfrak{o}}(k[U'])$.
Also ist $U' \in L_4(\mathfrak{M}^{\mathfrak{p}},\mathfrak{o}) = L_4^*(\mathfrak{M}^{\mathfrak{p}},\mathfrak{o})$. Daher gibt es a, d' $\in \mathfrak{o}$,
$b \in \mathfrak{p}^{-1}$ und $c \in \mathfrak{p}$, so daß U' und $V' := \begin{pmatrix}a & b\\ c & d'\end{pmatrix}$ eine 2-Diedergruppe
in $\Gamma(\mathfrak{M}^{\mathfrak{p}})$ erzeugen. Dann muß gelten: ad' - bc = 1 und

$\begin{pmatrix}a-c & b-d'\\ 2a-c & 2b-d'\end{pmatrix} = U'V' = -V'U' = \begin{pmatrix}-a-2b & a+b\\ -c-2d' & c+d'\end{pmatrix}$; d.h. $c = 2a+2b$,
$d' = -a$ und $1 = -a^2 - b(2a+2b) = -N(a+b(1+i))$.
Da $q = z$ (wegen $-2 \notin N_{k_+|\mathbb{Q}}(\mathfrak{o}_+)$), haben wir:
$1 = \left[\mathfrak{o}^\times : N(\mathfrak{O}^{\mathfrak{o}\times})\right] = xz/q = 2$ ↯.

(27.21) Korollar: Sei $d \equiv 2 \bmod 4$ und x = 2 und $h(k_+) = 2^{\delta-2}$. Wenn d einen Primteiler p mit $p \equiv 5 \bmod 8$ oder $p \equiv 7 \bmod 8$ hat, ist $\lambda_4^*(\mathfrak{M}^{\mathfrak{o}}) = 0$.

Bew.: folgt aus 27.20.ii. Vgl. 21.12.i.

Bemerkung: In (27.19), in (27.20.ii,iii) und (27.21) kann man die Voraussetzung $x = 2$ weglassen, da sie aus den anderen Voraussetzungen jeweils folgt.

(27.22) Lemma: Sei $d \equiv 1 \bmod 3$.

i) Falls $-3 \in N_{k_+'|\mathbb{Q}}(o_+')$, dann ist $\lambda_6^*(\mathfrak{M}^o) > 0$.

ii) Falls $-3 \in N_{k_+'|\mathbb{Q}}(o_+')$, dann ist $\lambda_6'(\mathfrak{M}^o) > 0$.

iii) Falls d einen Primteiler p mit $p \equiv 2 \bmod 3$ hat, ist $\lambda_6'(\mathfrak{M}^o) > 0$.

Bew.: Es ist $o[\zeta_6] = O'^o$. Daher ist $[o^\times : N(o[\zeta_6]^\times)] = 2/q'$ (vgl. Bew. von 20.17). Nach (20.13.ii) ist $z' = 1$.
Daher ist $[o^\times : N(o[\zeta_6]^\times)] = 1$ genau dann, wenn $-3 \in N_{k_+'|\mathbb{Q}}(o_+')$.

i) Sei $-3 \in N_{k_+'|\mathbb{Q}}(o_+')$. Dann gibt es $a, b \in o$ mit $a^2 + b^2 + ab = N(a + b\zeta_6) = -1$. Man überlegt sich leicht, daß E und $B = \begin{pmatrix} a & b \\ a+b & -a \end{pmatrix}$ eine 3-Diedergruppe in $\Gamma(\mathfrak{M}^o)$ erzeugen.

ii) Sei $-3 \notin N_{k_+'|\mathbb{Q}}(o_+')$. Wäre $\lambda_6'(\mathfrak{M}^o) = 0$, so gäbe es $a, b, c, d' \in o$, so daß E und $B = \begin{pmatrix} a & b \\ c & d' \end{pmatrix}$ eine 3-Diedergruppe in $\Gamma(\mathfrak{M}^o)$ erzeugen.
Dann wäre $ad' - bc = 1$ und
$\begin{pmatrix} a-c & b-d' \\ a & b \end{pmatrix} = EB = BE^{-1} = \begin{pmatrix} -b & a+b \\ -d' & c+d' \end{pmatrix}$. Also $c = a+b$, $d' = -a$ und $1 = -a^2 - b(a+b) = -N(a + b\zeta_6)$.
Da $d \neq 1$, folgt hieraus: $[o^\times : N(o[\zeta_6]^\times)] = 1$ ↯.
iii) folgt aus ii). Vgl. (20.13.i).

(27.23) Lemma: Sei $d \equiv 3 \bmod 9$ und $d \neq 3$.

i) Falls $x' = 1$, so ist $\lambda_6^*(\mathfrak{M}^q) > 0$.

ii) Falls $x' = 2$ und $h(k_+') = 2^{\delta-3}$, so ist $\lambda_6^*(\mathfrak{M}^q) = 0$.

Bew.: Da $(1+\zeta_6)^2 = 3\zeta_6$, überprüft man leicht, daß $O'^o = o + q^{-1}(1+\zeta_6)$.
Nach (20.9.i) ist $q' = 1$. Nach (20.11) ist daher $[o^\times : N(O'^{o\times})] = x'$.
i) Sei $x' = 1$. Dann gibt es $a \in o$ und $b \in q^{-1}$ mit $-1 = N(a + b(1+\zeta_6)) = a^2 + 3ab + 3b^2$. Sei $E' = \begin{pmatrix} 2 & -1 \\ 3 & -1 \end{pmatrix}$ und und $B' = \begin{pmatrix} a & b \\ 3a+3b & -a \end{pmatrix}$. Man prüft leicht nach, daß $E', B' \in \Gamma(\mathfrak{M}^q)$, daß $S(E') = 1$ und daß $B'E'B'^{-1} = E'^{-1}$.

ii) Sei $x' = 2$. Ist $\mathfrak{M}$ eine $\mathbb{Q}$-Maximalordnung mit $\mathfrak{o} \in F_6^*(\mathfrak{M})$, dann ist $l_6(\mathfrak{M},\mathfrak{o}) = x' \cdot h(k_+') = 2^{\delta-2} = l_6^*(\mathfrak{M},\mathfrak{o})$. (siehe 20.26.i und 20.38)
Wäre $\lambda_6^*(\mathfrak{M}^\eta) > 0$, dann wäre $\mathfrak{o} \in F_6^*(\mathfrak{M}^\eta)$, also $L_6(\mathfrak{M}^\eta,\mathfrak{o}) = L_6^*(\mathfrak{M}^\eta,\mathfrak{o})$.
Sei $E' = \begin{pmatrix} 2 & -1 \\ 3 & -1 \end{pmatrix}$. Wegen $\eta^{-1}(1+E') \in \mathfrak{M}^\eta$ ist
$\mathfrak{M}^\eta \cap k[E'] = \mathfrak{o} + \eta^{-1}(1+E') = \mathfrak{O}^{\mathfrak{o}}(k[E'])$. Also ist $E' \in L_6^*(\mathfrak{M}^\eta,\mathfrak{o})$.
Daher gibt es $a, d' \in \mathfrak{o}$, $b \in \eta^{-1}$ und $c \in \eta$, so daß E' und $B' = \begin{pmatrix} a & b \\ c & d' \end{pmatrix}$ eine 3-Diedergruppe in $\Gamma(\mathfrak{M}^\eta)$ erzeugen.
Dann muß gelten: $ad' - bc = 1$ und

$$\begin{pmatrix} 2a-c & 2b-d' \\ 3a-c & 3b-d' \end{pmatrix} = E'B' = B'E'^{-1} = \begin{pmatrix} -a-3b & a+2b \\ -c-3d' & c+2d' \end{pmatrix};$$

d.h. $c = 3a+3b$, $d' = -a$ und $1 = -a^2 - b(3a+3b) = -N(a + b(1+\zeta_6))$.
Daher haben wir $1 = [\mathfrak{o}^\times : N(\mathfrak{O}^{\mathfrak{o}\times})] = x' = 2$ ↯.

(27.24) Korollar: Sei $d \equiv 3 \bmod 9$.

i) Sei $x' = 1$ und für alle Primteiler p von $d/3$ gelte: $p \equiv 1 \bmod 12$.
Dann ist $\lambda_6^*(\mathfrak{M}^\mathfrak{o}) > 0$.

ii) Sei $x' = 1$ und $d/3$ habe einen Primteiler p mit $p \equiv 5 \bmod 12$.
Dann ist $\lambda_6^*(\mathfrak{M}^\mathfrak{o}) = 0$.

iii) Sei $x' = 2$ und $h(k_+') = 2^{\delta-3}$. Für alle Primteiler $p \neq 2$ von $d/3$ gelte: $p \equiv \pm 1 \bmod 12$. Dann ist $\lambda_6^*(\mathfrak{M}^\mathfrak{o}) = 0$.

iv) Sei $h(k_+') = 1$. Sei $d/3 = pp'$ mit Primzahlen p, p', so daß $p \equiv p' \equiv 7 \bmod 12$. Dann ist $\lambda_6^*(\mathfrak{M}^\mathfrak{o}) > 0$.

Bew.: Es ist $\widetilde{\mathfrak{M}^\mathfrak{o}} = \widetilde{\mathfrak{M}^\eta}$ genau dann, wenn $\eta \in I^{k(2)}H^k$. Dies ist genau dann der Fall, wenn für alle Primteiler $p \neq 2$ von $d/3$ gilt: $p \equiv \pm 1 \bmod 12$.
(Zum Beweis vergleiche man den Beweisgang von 20.33 und 20.34 und ändere ihn zweckmäßig ab.)
Wendet man diese Tatsache auf (27.23.i) an, so erhält man genau i) und ii).
(Man beachte, daß wegen $x' = 1$ nur die 2 oder Primzahlen $p \equiv 1 \bmod 4$ als Primteiler von $d/3$ möglich sind.)
iii) folgt entsprechend aus (27.23.ii)

iv) Wegen $p \equiv 7 \bmod 12$ ist $x' = 2$. Wegen $d \equiv 3 \bmod 4$ ist $\delta = 3$.
Die Voraussetzungen von (27.23.ii) sind also erfüllt, es ist
$\lambda_6^*(\mathfrak{M}^\eta) = 0$. Wegen $\begin{pmatrix} 2 & -1 \\ 3 & -1 \end{pmatrix} \in \mathfrak{M}^\eta$ ist $\lambda_6(\mathfrak{M}^\eta) > 0$.
Es ist $\widetilde{\mathfrak{M}}^\eta \neq \widetilde{\mathfrak{M}}^\circ$. Insgesamt gibt es $2^{\delta-1} = 4$ Maximalordnungstypen.
Wegen $d \equiv 3 \bmod 9$ gibt es zwei Maximalordnungstypen $\widetilde{\mathfrak{M}}_1 \neq \widetilde{\mathfrak{M}}_2$
mit $\lambda_6(\mathfrak{M}_1) = \lambda_6(\mathfrak{M}_2) = 0$.
Es gibt einen Maximalordnungstyp $\widetilde{\mathfrak{M}}$ mit $\lambda_6^*(\mathfrak{M}) > 0$.
Da $\widetilde{\mathfrak{M}} \notin \{\widetilde{\mathfrak{M}}^\eta, \widetilde{\mathfrak{M}}_1, \widetilde{\mathfrak{M}}_2\}$, ist notwendig $\widetilde{\mathfrak{M}} = \widetilde{\mathfrak{M}}^\circ$.

Bemerkung: i) In (27.23.ii) und (27.24.iii) kann man die Voraussetzung $x' = 2$ weglassen, da sie aus den anderen Voraussetzungen jeweils folgt.
ii) (27.24.iv) würde gültig bleiben, wenn man die Voraussetzung $p \equiv p' \equiv 7 \bmod 12$ ersetzt durch $p \equiv p' \equiv 5 \bmod 12$ oder durch $p = 2$ und $p' \equiv 5 \bmod 12$. Dann sind aber die Voraussetzungen insgesamt nicht erfüllbar (siehe /1/ S.271 Aufgabe 28).

Die bisherigen Lemmata reichen für $d = 34$ nicht aus. Wir brauchen:

(27.25) Lemma: Sei $d = 34$. Dann erzeugen

$$\begin{pmatrix} i\sqrt{34} & 3 \\ 11 & -i\sqrt{34} \end{pmatrix} \text{ und } \begin{pmatrix} 13 & -i\sqrt{34} \\ -5i\sqrt{34} & -13 \end{pmatrix}$$ eine 2-Diedergruppe in $\Gamma(\mathfrak{M}^\circ)$.

Bew.: leichte Rechnung

Wir bemerken noch, daß $-2 = 8^2 - 66 \cdot 1^1$ und $-3 = 33^2 - 3 \cdot 91 \cdot 2^2$.
Jetzt haben wir genug Material gesammelt, um die Konjugationsklassenzahlen der endlichen Untergruppen in $\Gamma(\mathfrak{M}^\circ)$ zu berechnen, falls $1 \leq d \leq 101$.
Wir sammeln die Ergebnisse in der Tabelle (27.26).
In der Tabelle sind keine Nullen eingetragen. Die entsprechenden Felder sind freigelassen.

(27.26) Die Konjugationsklassenzahlen der endlichen Untergruppen von $SL(2,\sigma)$ für $k = \mathbb{Q}(i\sqrt{d})$ mit $1 \le d \le 101$

d	λ_4'	λ_4^*	λ_4^T	μ_T	μ_2^-	λ_6'	λ_6^*	μ_3
1		4	1	1	1		1	2
2		2	1	1	1	1		
3		1	1	2		1	1	1
5		3			2	1		
6	1	1	1	2		1		
7	1						1	2
10		3			2	1		
11		1	1	2		1		
13		3			2		2	4
14	2					1		
15	1					1		
17		4	1	2	2	1		
19		1	1	2			1	2
21	3					2	2	4
22	1	1	1	2		1		
23	1					1		
26		3			2	2		
29		3			2	1		
30	3					3		
31	1						1	2
33	3	2	2	4		4		
34	2	4	2	2	2	1		
35	1					1		
37	2	3			2		2	4
38	1	1	1	2		1		
39	1					1	1	2
41		4	1	2	2	1		
42	3					2		
43		1	1	2			1	2
46	2					1		
47	1					1		

d	λ_4'	λ_4^*	λ_4^T	μ_T	μ_2^-	λ_6'	λ_6^*	μ_3
51		2	2	4		1		
53		3			2	1		
55	1					1		
57	3	2	2	4		2	2	4
58		3			2	1		
59		1	1	2		1		
61		3			2		2	4
62	2					1		
65	1	6			4	2		
66	2	2	2	4		3		
67		1	1	2			1	2
69	3					2		
70	3					2		
71	1					1		
73		4	1	2	2	1	2	4
74		3			2	2		
77	3					2		
78	3					2		
79	3						1	2
82	1	4	1	2	2	1		
83		1	1	2		1		
85		6			4	2		
86	1	1	1	2		1		
87	1					1		
89		4	1	2	2	1		
91	1						2	4
93	3					2	2	4
94	2					1		
95	1					1		
97		4	1	2	2	1	2	4
101	2	3			2	1		

Beispiel für die Benutzung der Tabelle (27.26):

Sei $d = 73$, d.h. $k = \mathbb{Q}(i\sqrt{73})$ und $\mathfrak{o}$ die Hauptordnung von k.
Dann gilt:

$\lambda_4' = 0$: Alle zyklischen Untergruppen der Ordnung 4 in $SL(2,\mathfrak{o})$ sind in einer 2-Diedergruppe in $SL(2,\mathfrak{o})$ enthalten.

$\lambda_4 = 4$: Die Konjugationsklassenzahl dieser Gruppen in $SL(2,\mathfrak{o})$ ist 4.

$\lambda_4^T = 1$: Die zyklischen Untergruppen der Ordnung 4 in $SL(2,\mathfrak{o})$, die in einer Tetraedergruppe in $SL(2,\mathfrak{o})$ enthalten sind, sind alle $SL(2,\mathfrak{o})$-konjugiert zueinander.

$\mu_T = 2$: Die Konjugationsklassenzahl der Tetraedergruppen in $SL(2,\mathfrak{o})$ ist 2.

$\bar{\mu}_2 = 2$: Es gibt zwei Konjugationsklassen von 2-Diedergruppen in $SL(2,\mathfrak{o})$, die in keiner Tetraedergruppe in $SL(2,\mathfrak{o})$ enthalten sind.

Ist $\{D_1,\ldots,D_4\}$ ein Repräsentantensystem der $\mu_T + \bar{\mu}_2$ Konjugationsklassen von 2-Diedergruppen in $SL(2,\mathfrak{o})$, so ist also für genau zwei der D_i auch die zugehörige Tetraedergruppe in $SL(2,\mathfrak{o})$ enthalten.

$\lambda_6' = 1$: Es gibt eine Konjugationsklasse von zyklischen Gruppen der Ordnung 6 in $SL(2,\mathfrak{o})$, die in keiner 3-Diedergruppe in $SL(2,\mathfrak{o})$ enthalten sind.

$\lambda_6 = 2$: Die Konjugationsklassenzahl der zyklischen Untergruppen G der Ordnung 6 in $SL(2,\mathfrak{o})$, für die es eine 3-Diedergruppe $G' \subset SL(2,\mathfrak{o})$ gibt mit $G \subset G'$, ist 2.

$\mu_3 = 4$: Die Konjugationsklassenzahl der 3-Diedergruppen in $SL(2,\mathfrak{o})$ ist 4. (Jede 6-zyklische Gruppe ist entweder in keiner oder in genau zwei nicht konjugierten 3-Diedergruppen in $SL(2,\mathfrak{o})$ enthalten.)

Schlußbemerkungen:

i) Auf Grund von (27.7) lassen sich in Spezialfällen F_4 und F_6 miteinander vergleichen. Dieses "Reziprozitätsgesetz" ist sehr wertvoll. Z.B. konnte ja (27.8) damit bewiesen werden.
Ich vermute, daß man die Voraussetzungen in (27.8) abschwächen kann zu: $d \equiv 5 \bmod 8$ und d hat einen Primteiler $p \equiv 3 \bmod 4$.
Der Beweis müßte dann m. E. mit Hilfe eines ähnlichen Lemmas wie (27.7) geführt werden. Zum Beweis einer Modifikation (Verallgemeinerung) von (27.7) wäre es nötig, auch andere quadratische Körpererweiterungen von k in die Untersuchungen einzubeziehen als $k(i)$ und $k(i\sqrt{3})$.

ii) Vielleicht kann man weiteren Aufschluß über die endlichen Untergruppen von $\Gamma(\mathfrak{M})$ für die verschiedenen Maximalordnungen gewinnen, wenn man auch Durchschnitte $k[E] \cap \mathfrak{M}$ untersucht, für die $E \notin \mathfrak{M}$. (Die Bedingungen in (18.9) und (23.13) werden dann aber vermutlich komplizierter werden)

iii) Wir haben in dieser Arbeit Methoden entwickelt, um die Konjugationsklassenzahlen von 2n-zyklischen Gruppen zu bestimmen , die in n-Diedergruppen in $\Gamma(\mathfrak{M})$ enthalten sind. Zumindest in Spezialfällen dürfte es möglich sein, auch die Konjugationsklassenzahlen von 4-zyklischen Gruppen zu bestimmen, die in n-Diedergruppen enthalten sind.

Für imaginärquadratische Zahlkörper $k = \mathbb{Q}(i\sqrt{d})$, $d \neq 3$ wissen wir daß jede 6-zyklische Gruppe in $\Gamma(\mathfrak{M})$ entweder in keiner oder in genau 2 nicht konjugierten 3-Diedergruppen in $\Gamma(\mathfrak{M})$ enthalten ist. In Spezialfällen wird man sicher auch etwas darüber aussagen können, in wieviel nicht konjugierten Tetraedergruppen in $\Gamma(\mathfrak{M})$ eine 6-zyklische Untergruppe von $\Gamma(\mathfrak{M})$ enthalten ist.

Untersuchungen in den genannten Richtungen würden dazu beitragen, das "Geflecht" näher kennenzulernen, das die Konjugationsklassen der endlichen Untergruppen von $\Gamma(\mathfrak{M})$ bilden.

Literaturverzeichnis

/1/ S.I. Borewicz, I.R. Safarevic
Zahlentheorie
Birkhäuser Verlag, Basel 1966

/2/ R. Dedekind
Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers
Gesammelte mathematische Werke, Band I, S. 105 - 158
Verlag Friedr. Vieweg & Sohn, Braunschweig 1930

/3/ M. Deuring
Algebren
Chelsea Publishing Company, New York 1948

/4/ M. Eichler
Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren
Journal für die reine und angewandte Mathematik 176 (1937), S.192-202

/5/ M. Eichler
Über die Idealklassenzahl hyperkomplexer Systeme
Mathematische Zeitschrift 43 (1938), S. 481 - 494

/6/ M. Eichler
Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und ihre L-Reihen
Journal für die reine und angewandte Mathematik 179 (1938), S.227-251

/7/ M. Eichler
Zur Zahlentheorie der Quaternionenalgebren
Journal für die reine und angewandte Mathematik 195 (1955), S.127-151

/8/ H. Hasse
Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil Ia: Beweise zu Teil I
Jahresbericht der deutschen Mathematiker-Vereinigung 36 (1927), S. 233 - 311

/9/ H. Hasse
Über gewisse Ideale in einer einfachen Algebra
Hermann et Cie., Paris 1934

/10/ H. Hasse
Über die Klassenzahl abelscher Zahlkörper
Akademie-Verlag, Berlin 1952

/11/ H. Hasse
Vorlesungen über Klassenkörpertheorie
Physica-Verlag, Würzburg 1967

/12/ D. Hilbert
Die Theorie der algebraischen Zahlkörper
Jahresbericht der Deutschen Mathematikervereinigung 4 (1897), S.175-546
in: Gesammelte Abhandlungen, Erster Band: Zahlentheorie, S. 63 - 363
Verlag von Julius Springer, Berlin 1932

/13/ T.Y. Lam
The algebraic theory of quadratic forms
Benjamin, New York 1973

/14/ S. Lang
Algebra
Addison-Wesley, 1971

/15/ E. Noether
Zerfallende verschränkte Produkte und ihre Maximalordnungen
Hermann et Cie., Paris 1934

/16/ A. Prestel
Die elliptischen Fixpunkte der Hilbertschen Modulgruppen
Mathematische Annalen 177 (1968), S 181-209

/17/ V. Schneider
Die elliptischen Fixpunkte zu Modulgruppen in Quaternionenschiefkörpern
Mathematische Annalen 217 (1975), S. 29 - 45

/18/ V. Schneider
Elliptische Fixpunkte und Drehfaktoren zu Modulgruppe in Quaternionenschiefkörpern über reellquadratischen Zahlkörpern
Mathematische Zeitschrift 152 (1977), S. 145 - 163

/19/ H. Shimizu
On discontinuous groups operating on the product of the upper half planes
Annals of Mathematics 77 (1963), S. 33 - 71

/20/ T.A. Springer
Invariant Theory
Springer Verlag, Berlin/Heidelberg 1977