Bestimmung relativer Ganzheitsbasen in relativquadratischen Zahlkörpern

Diplomarbeit
vorgelegt von
Mario Daberkow

Angefertigt an der Mathematisch-Naturwissenschaftlichen
Fakultät der Heinrich-Heine-Universität Düsseldorf

Inhaltsverzeichnis

Kapitel 1

Einleitung

Laut Zassenhaus liegen die Hauptziele der konstruktiven algebraischen Zahlentheorie in der Lösung der folgenden vier Probleme:

- die Bestimmung der Galoisgruppe
- die Bestimmung einer Ganzheitsbasis
- die Bestimmung der Einheitengruppe
- die Bestimmung der Klassengruppe

eines algebraischen Zahlkörpers $\mathcal{E}$.
Hierbei spielt die Ganzheitsbasis eine fundamentale Rolle, denn viele Methoden zur Bestimmung der Einheitengruppe oder zur Bestimmung der Klassengruppe setzen die Kenntnis einer solchen Basis bereits voraus. Gute Algorithmen für die Bestimmung einer Ganzheitsbasis sind deshalb oft unerläßlich, um Einheitengruppe und Klassengruppe bestimmen zu können.
Die bisher verwendeten Algorithmen, z.B der Round-2 [33] oder auch der Round-4 [9, 3], sind im wesentlichen darauf ausgelegt, $\mathbb{Z}$–Ganzheitsbasen von $o_{\mathcal{E}}$, dem Ring der ganzen Zahlen von $\mathcal{E}$, zu berechnen. Bei Zahlkörpern höheren Grades (> 50) werden die Rechenzeiten jedoch extrem lang, so daß es praktisch kaum möglich ist, die Ganzheitsbasis zu bestimmen.
Nun liegt es nahe, Kenntnisse über Teilkörper $\mathcal{F}$ von $\mathcal{E}$ in die Berechnungen

mit einzubeziehen, und das Problem erst in diesem Teilkörper $\mathcal{F}$ zu lösen, um dann *relativ* die Berechnungen weiterzuführen. Unser naives Ziel wäre also die Bestimmung einer $o_{\mathcal{F}}$–Basis von $o_{\mathcal{E}}$. Dieses Ziel ist im allgemeinen jedoch nicht zu erreichen, da $o_{\mathcal{E}}$ zwar ein endlich erzeugter $o_{\mathcal{F}}$–Modul ist, aber er nicht immer frei ist. Da, wie wir sehen werden, die Anzahl der nötigen Erzeuger im Verhältnis zum Grad der Körpererweiterung sehr klein gehalten werden kann, macht es Sinn auch dann Berechnungen anzustellen, wenn wir wissen, daß $o_{\mathcal{E}}$ kein freier $o_{\mathcal{F}}$–Modul ist. Dies werden wir in relativquadratischen Zahlköpern versuchen. Dabei werden wir zunächst ganz allgemein relative Zahlkörper betrachten und uns genauer mit der Struktur von $o_{\mathcal{E}}$ als $o_{\mathcal{F}}$–Modul beschäftigen. Wir stellen Kriterien, die auf E. Artin und A. Fröhlich zurückgehen, vor, die angegeben wann genau eine relative Ganzheitsbasis für Erweiterungen existiert.

Diese allgemeingültigen Aussagen werden dann auf relativquadratische Zahlkörper angewandt. Aufbauend auf den Ergebnissen von Hilbert in [13] werden wir die Ergebnisse von Sommer [32], der die Struktur von $o_{\mathcal{E}}$ als $o_{\mathcal{F}}$–Modul für relativquadratische Zahlkörper über quadratischen Grundkörpern beschrieben hat, verallgemeinern und den Ring der ganzen Zahlen eines relativquadratischen Zahlkörpers bzgl. der ganzen Elemente eines beliebigen Grundkörpers erstmalig vollständig beschreiben. Durch die vorgeführten Beweise können wir dann ein Konstruktionsverfahren für $o_{\mathcal{E}}$ als $o_{\mathcal{F}}$–Modul angeben. Eine große Menge nicht–trivialer Beispiele zeigt dann die praktische Anwendbarkeit der theoretischen Ergebnisse. Wie sich zeigt, ist das vorgestellte Verfahren speziell gegenüber dem Round–2 schon bei Körpern kleineren Grades (≥ 4) überlegen und benötigt in bestimmten Fällen nur eine kleinen Teil der Rechenzeit des Round–2. Wir werden dies am Ende der Arbeit genauer untersuchen.

Die bekannten Verfahren sind für Berechnung relativer Ganzheitsbasen nur bedingt verwendbar; so arbeitet der Round–2 z.B. dann korrekt, wenn $o_{\mathcal{F}}$ ein Hauptidealring ist. Dagegen ist der Round–4 für relative Berechnugen überhaupt nicht zu verwenden.

Um die Beweise durchführen zu können werden wir einige Ergebnisse der p–adischen Theorie in Zahlköpern verwenden. Ihrer Einführung und der damit verbundenen Bewertungstheorie wird ein größerer Raum im Rahmen dieser Arbeit eingeräumt.

Kapitel 2

Grundlagen

2.1 Algebraische Zahlkörper

Dieser Abschnitt ist eine kurze Einführung in die Theorie der algebraischen Zahlkörper. Man findet die hier vorgestellten Sätze und Definitionen in zahlreichen Standardwerken der Algebra und Zahlentheorie ([27, 23, 24, 7, 19, 21, 22]).

Wir betrachten im folgenden endliche algebraische Erweiterungen von $\mathbb{Q}$

$$\mathbb{Q} \subseteq \mathcal{F} \subseteq \mathcal{E} \subseteq \mathbb{C}.$$

Da $\mathbb{Q}$ ein vollkommener Körper ist [22], existiert ein $\rho \in \mathbb{C}$ mit:

$$\mathcal{E} = \mathcal{F}(\rho).$$

Hierbei ist ρ Nullstelle eines normierten und irreduziblen Polynoms $m_\rho(t) \in \mathcal{F}[t]$ und es gilt $[\mathcal{E} : \mathcal{F}] = deg(m_\rho) =: n$. Gilt nun $\mathcal{F} \neq \mathbb{Q}$, so bezeichnet man $\mathcal{E}$ als Relativerweiterung. Allgemein sind $\mathcal{F}$ und $\mathcal{E}$ algebraische Zahlkörper. Über $\mathbb{C}$ zerfällt $m_\rho(t)$ nun in Linearfaktoren:

$$m_\rho(t) = \prod_{i=1}^{n} (t - \rho^{(i)}) \qquad ; \ (\rho^{(1)} = \rho)$$

Dabei wird $\rho^{(i)}$ als **i-te Konjugierte** von ρ bezeichnet. Desweiteren definieren wir $\mathcal{E}^{(i)} := \mathcal{F}(\rho^{(i)})$ als den **i-ten Konjugiertenkörper** von $\mathcal{E}$. Betrachtet man nun die n paarweise verschiedenen Abbildungen

$$\tilde{\sigma}_i : \rho \to \rho^{(i)} \, (1 \leq i \leq n),$$

so werden durch sie $\mathcal{F}$ - Isomorphismen σ_i von $\mathcal{E}$ nach $\mathcal{E}^{(i)}$ induziert, d.h. diese Abbildungen lassen $\mathcal{F}$ elementweise invariant. Wie man nun sieht, sind die Konjugiertenkörper vermöge σ_i untereinander $\mathcal{F}$-isomorph.

Definition 2.1 *Sei $\alpha \in \mathcal{E}$ beliebig gegeben.*

(i) *Dasjenige normierte Polynom $m_\alpha(t) \in \mathcal{F}[t]$ minimalen Grades mit $m_\alpha(\alpha) = 0$ heißt das* **Minimalpolynom** *von α über $\mathcal{F}$.*

(ii) $\alpha^{(i)} := \sigma_i(\alpha)$ *heißt die* **i-te Konjugierte** *von α $(1 \leq i \leq n)$.*

(iii) *Die* **Spur** *und die* **Norm** *einer algebraischen Zahl $\alpha \in \mathcal{E}$ wird durch die Spur und Determinante der Transformation*

$$\psi_{\alpha,\mathcal{F}} \; : \; \mathcal{E} \longrightarrow \mathcal{E} \; : \; x \to \alpha x$$

des $\mathcal{F}$ – Vektorraumes $\mathcal{E}$ gegeben. Wir bezeichnen sie mit

$$\begin{aligned} \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha) &:= det(\psi_{\alpha,\mathcal{F}}) \\ \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha) &:= Trace(\psi_{\alpha,\mathcal{F}}). \end{aligned}$$

Ist klar, bezüglich welcher Körper wir die Norm und die Spur bestimmen wollen, so verzichten wir auf diese Hinweise und schreiben N *statt* $\mathrm{N}_{\mathcal{E}/\mathcal{F}}$ *sowie* Tr *statt* $\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}$.

(iv) *Ist $\alpha_1, \ldots, \alpha_n$ eine Basis von $\mathcal{E}/\mathcal{F}$, so setzen wir*

$$d(\alpha_1, \ldots, \alpha_n) := det(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha_i \alpha_j))$$

als die **Diskriminante** *von $\alpha_1, \ldots, \alpha_n$. Gilt bei passender Nummerierung $\alpha_i = a^{i-1}$ $(1 \leq i \leq n)$ für ein $a \in \mathcal{E}$, so schreiben wir abkürzend $d(a)$.*

Ist nun $\omega_1, \ldots, \omega_n$ eine $\mathcal{F}$-Basis von $\mathcal{E}$, sowie $\alpha \in \mathcal{E}$ beliebig, so heißt die der linearen Abbildung $\psi_{\alpha,\mathcal{F}}$ zugeordnete Matrix $M_{\alpha,\mathcal{F}}$ mit

$$\alpha \cdot (\omega_1, \ldots, \omega_n) = M_{\alpha,\mathcal{F}} \cdot (\omega_1, \ldots, \omega_n)$$

die **Darstellungsmatrix** von α. Als charakteristisches Polynom von α definieren wir

$$f_{\alpha,\mathcal{F}}(t) := det(t \cdot E_{n\times n} - M_{\alpha,\mathcal{F}}).$$

Gilt dann $f_{\alpha,\mathcal{F}}(t) = t^n + a_1 t^{n-1} + \ldots + a_n$, so werden die Norm und die Spur von α durch

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha) = (-1)^n a_n \quad bzw. \quad \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha) = -a_1$$

gegeben. Darüberhinaus gelten für die Spur und die Norm nun einige wichtige Gesetzmäßigkeiten:

Lemma 2.2 *Für $\alpha, \beta \in \mathcal{E}$ gelten*

(i) $\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$

(ii) $\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha\beta) = \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha)\, \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\beta)$

(iii) $\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$

(iv) Die Spur ist eine lineare Abbildung des $\mathcal{F}$–Vektorraums $\mathcal{E}$:

$$\mathrm{Tr}_{\mathcal{E}/\mathcal{F}} : (\mathcal{E}, +) \longrightarrow (\mathcal{F}, +)$$

Neben diesen Eigenschaften können wir die Norm und die Spur auch in Körpertürmen bestimmen, denn es gilt der folgende Zusammenhang:

Lemma 2.3 *Sind $\mathcal{F} \subseteq \hat{\mathcal{F}} \subseteq \mathcal{E}$ algebraische Zahlkörper, so gelten*

(i) $\mathrm{Tr}_{\mathcal{E}/\mathcal{F}} = \mathrm{Tr}_{\hat{\mathcal{F}}/\mathcal{F}} \circ \mathrm{Tr}_{\mathcal{E}/\hat{\mathcal{F}}}$

(ii) $\mathrm{N}_{\mathcal{E}/\mathcal{F}} = \mathrm{N}_{\hat{\mathcal{F}}/\mathcal{F}} \circ \mathrm{N}_{\mathcal{E}/\hat{\mathcal{F}}}$

Beenden wir hiermit zunächst die relativen Betrachtungen. Für den Rest dieses Paragraphen sei nun $\mathcal{F} = \mathbb{Q}$ und es sei $\mathcal{E} = \mathbb{Q}(\rho)$. Hierbei sei o.B.d.A. ρ Nullstelle eines normierten irreduziblen Polynoms in $\mathbb{Z}[t]$.
Kommen wir nun zu der für uns zentralen Struktur eines algebraischen Zahlkörpers. Unser Ziel ist es, diese Struktur möglichst gut beschreiben zu können.

Definition 2.4 *(i) Ein $\alpha \in \mathcal{E}$ heißt ganz (algebraisch), falls α einer normierten algebraischen Gleichung*

$$\alpha^l + a_1\alpha^{l-1} + \ldots + a_l = 0$$

mit Koeffizienten $a_i \in \mathbb{Z}$ $(1 \leq i \leq l)$ genügt. Man beachte, daß jedes $\alpha \in \mathcal{E}$ einer solchen normierten Gleichung mit Koeffizienten in $\mathbb{Q}$ genügt.

(ii) Wir definieren $o_{\mathcal{E}} := \{\alpha \in \mathcal{E} \mid \alpha \text{ ist ganz}\}$ als die Menge der ganz algebraischen Elemente in $\mathcal{E}$.

Die Menge der ganz algebraischen Zahlen ist ein Ring. Es gilt der folgende Satz:

Satz 2.5 *Der Ring $o_{\mathcal{E}}$ ist ein freier $\mathbb{Z}$–Modul vom Rang $n = [\mathcal{E} : \mathbb{Q}]$. Ist $\omega_1, \ldots, \omega_n$ eine $\mathbb{Z}$–Basis von $o_{\mathcal{E}}$, so nennen wir sie eine Ganzheitsbasis von $\mathcal{E}$.*

Allgemein bezeichnen wir einen unitären Teilring R von $o_{\mathcal{E}}$, der ein freier $\mathbb{Z}$–Modul vom Rang n, ist als eine Ordnung des Zahlkörpers $\mathcal{E}$. Wie wir sehen, ist $o_{\mathcal{E}}$ per Definition die größte Ordnung in $\mathcal{E}$. Wir nennen $o_{\mathcal{E}}$ deshalb auch die Maximalordnung von $\mathcal{E}$. Ferner nennen wir $\mathbb{Z}[\rho]$ Gleichungsordnung.
Eine wichtige Invariante von $\mathcal{E}$ ist seine Körperdiskriminante. Sie wird wie folgt definiert:

Definition 2.6 *Ist $\omega_1, \ldots, \omega_n$ eine Ganzheitsbasis von $\mathcal{E}$, so definieren wir die* **Körperdiskriminante** *von $\mathcal{E}$ als*

$$d_{\mathcal{E}} := d(\omega_1, \ldots, \omega_n)$$

Bemerkung 2.7 *(i) Die Körperdiskriminante eines algebraischen Zahlkörpers ist unabhänig von der Wahl der Ganzheitsbasis.*

(ii) *Ist R eine Ordnung in $o_{\mathcal{E}}$ mit $R = \sum_{i=1}^{n} \alpha_i \mathbb{Z}$, so gilt*

$$d(\alpha_1, \ldots, \alpha_n) = k^2\, d_{\mathcal{E}}$$

mit $k \in \mathbb{N}$. Gilt $R = \mathbb{Z}[\rho]$, so bezeichnen wir k als den Index von $\mathbb{Z}[\rho]$ zur Maximalordnung.

2.2 Die Maximalordnung als Dedekindring

Wir wollen nun näher auf die Struktur von $o_{\mathcal{E}}$ eingehen. Wie schon bemerkt ist $o_{\mathcal{E}}$ ein Ring, aber hat er besondere Eigenschaften?
Wohl grundlegend ist der auf die nächste Definition aufbauende Satz:

Definition 2.8 *Es sei $\Re$ ein Integritätsring mit 1 und $\mathcal{M}$ sei sein Quotientenkörper.*

(i) *Eine Teilmenge $\mathbf{b} \neq 0$ von $\mathcal{M}$, für die ein $\zeta \in \Re$ und ein Ideal $\mathbf{a}$ in $\Re$ existieren mit*

$$\mathbf{b} = \frac{1}{\zeta}\mathbf{a}$$

heißt **gebrochenes Ideal** *von $\Re$.*

(ii) *Bilden die gebrochenen Ideale von $\Re$ eine multiplikative Gruppe, so nennen wir $\Re$ einen* **Dedekindring**.

Satz 2.9 *Ist $\Re$ ein Dedekindring, so gelten*

(i) *Jedes Ideal $\mathbf{a}$ $(\mathbf{a} \neq 0, \Re)$ hat eine (bis auf Reihenfolge) eindeutige Zerlegung*

$$\mathbf{a} = \wp_1 \cdot \ldots \cdot \wp_r$$

in Primideale $\wp_i$ von $\Re$ $(1 \leq i \leq r)$.

(ii) *Jedes Primideal in $\Re$ ist maximal.*

Entscheidend ist nun die Tatsache, daß $o_{\mathcal{E}}$ ein Dedekindring ist([27]). Er hat damit eine Reihe von angenehmen Eigenschaften.
Durch die (eindeutige) Zerlegung von Idealen in Primideale haben wir die Möglichkeit die Summe und den Schnitt von zwei Idealen $\mathbf{a}, \mathbf{b}$ wie folgt zu beschreiben:

Lemma 2.10 *(i)* $\mathbf{a} + \mathbf{b} = ggt(\mathbf{a}, \mathbf{b})$

(ii) $\mathbf{a} \cap \mathbf{b} = kgv(\mathbf{a}, \mathbf{b})$

Hierbei sind ggt und kgv im Sinne der Primidealzerlegung zu sehen.

Betrachten wir nun wieder einfache Eigenschaften des Dedekindringes. Zunächst einmal ist offenbar jeder Hauptidealring ein Dedekindring, aber es gilt sogar:

Lemma 2.11 *Der Ring $o_{\mathcal{E}}$ ist genau dann ein Hauptidealring, wenn er ein ZPE–Ring ist.*

Über diese Eigenschaft hinaus können wir die (gebrochenen) Ideale in $o_{\mathcal{E}}$ besonders einfach darstellen.

Lemma 2.12 *Sei* $\mathbf{a}$ *ein gebrochenes Ideal von $o_{\mathcal{E}}$. Dann gelten*

(i) Es existieren $\alpha, \beta \in \mathcal{E}$ mit $\mathbf{a} = \alpha o_{\mathcal{E}} + \beta o_{\mathcal{E}}$.

(ii) Es existieren $\alpha_1, \ldots, \alpha_n \in \mathcal{E}$ mit $\mathbf{a} = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$.

Während die zweite Aussage des Lemmas entscheidend von der Tatsache getragen wird, daß $\mathbb{Z}$ ein Hauptidealring ist, geht die erste Aussage alleine auf die Dedekindeigenschaft von $o_{\mathcal{E}}$ zurück. Es sind, wie wir gesehen haben, die Ideale in $o_{\mathcal{E}}$, die von besonderem Interesse sind. Wir führen daher eine Funktion auf den Idealen von $o_{\mathcal{E}}$ ein, um diese besser betrachten zu können.

Definition 2.13 *Es sei* $\mathbf{a}$ *ein Ideal in $o_{\mathcal{E}}$. Dann definieren wir die Norm von* $\mathbf{a}$ *als*

$$\mathrm{N}(\mathbf{a}) := \sharp(o_{\mathcal{E}}/\mathbf{a}).$$

Man beachte, daß diese Definition in dieser Form nicht auf Relativerweiterungen zu verallgemeinern ist. Wir werden uns mit diesem Problem später noch auseinandersetzen.
Diese Definition ist die natürliche Verallgemeinerung der Norm einer ganz algebraischen Zahl. Dies zeigt das folgende Lemma:

Lemma 2.14 *Ist $\alpha \in o_{\mathcal{E}} \setminus \{0\}$ beliebig gegeben, so gilt*

$$\mathrm{N}(\alpha o_{\mathcal{E}}) = |\,\mathrm{N}(\alpha)|.$$

Neben dieser Eigenschaft hat die Idealnorm noch eine Eigenschaft mit der Norm von algebraischen Zahlen gemeinsam:

Lemma 2.15 *Die Idealnorm ist multiplikativ, d.h für Ideale $\mathbf{a}, \mathbf{b}$ in $o_{\mathcal{E}}$ gilt*

$$\mathrm{N}(\mathbf{ab}) = \mathrm{N}(\mathbf{a})\,\mathrm{N}(\mathbf{b}).$$

2.3 Klassenzahl und Klassengruppe

Definition 2.16 *Für einen algebraischen Zahlkörper $\mathcal{E}$ definieren wir*

(i) $I\!\!P_{\mathcal{E}} := \{\wp \mid \wp \textit{ ist ein Primideal} \neq \{0\} \textit{ von } o_{\mathcal{E}}\}$

(ii) $\mathcal{I}_{\mathcal{E}} := \{\mathbf{a} \mid \mathbf{a} \textit{ ist gebrochenes Ideal von } o_{\mathcal{E}}\}$

(iii) $\mathcal{H}_{\mathcal{E}} := \{\mathbf{a} \mid \mathbf{a} \textit{ ist gebrochenes Hauptideal von } o_{\mathcal{E}}\}$

(iv) $Cl_{\mathcal{E}} := \mathcal{I}_{\mathcal{E}}/\mathcal{H}_{\mathcal{E}}$ *als die Klassengruppe von $\mathcal{E}$.*

Da die Zerlegung eines Ideals in Primideale eindeutig ist, folgt aus der Gruppeneigenschaft der gebrochenen Ideale, daß auch die gebrochenen Ideale Potenzprodukte von Primidealen sind. Deshalb ist die folgende Definition sinnvoll:

Definition 2.17 *Für ein Primideal $\wp \in I\!P_{\mathcal{E}}$ definieren wir*

$$\nu_\wp(\cdot) \ : \ \mathcal{I}_{\mathcal{E}} \longrightarrow \mathbb{Z} \ : \ \mathbf{a} \rightarrow max\{k \in \mathbb{Z} \mid \ \wp^k|\mathbf{a}\}$$

Wir schreiben auch abkürzend $\nu_\wp(\alpha)$ für ein $\alpha \in \mathcal{E}$ und meinen damit natürlich $\nu_\wp(\alpha o_{\mathcal{E}})$.

Wir werden später noch genauer auf diese Funktion eingehen, bemerken jedoch schon hier, daß für ein gebrochenes Ideal $\mathbf{a}$ in $\mathcal{E}$

$$\mathbf{a} \subseteq o_{\mathcal{E}} \Leftrightarrow \forall \, \wp \in I\!P_{\mathcal{E}} \ : \ \nu_\wp(\mathbf{a}) \geq 0$$

gilt.
Wie wir wissen ist die Klassengruppe genau dann trivial, wenn $o_{\mathcal{E}}$ ein ZPE-Ring ist. Die Klassengruppe ist eine Invariante des Zahlkörpers und darüberhinaus ist die Klassenzahl ein Maß dafür, wie "weit" sich $o_{\mathcal{E}}$ von einem ZPE-Ring entfernt hat. Ein entscheidendes Ergebnis ist der folgende Satz:

Satz 2.18 *Die Klassengruppe $Cl_{\mathcal{E}}$ ist eine endliche abelsche Gruppe. Wir bezeichnen mit der Klassenzahl $h_{\mathcal{E}}$ die Anzahl der Elemente in $Cl_{\mathcal{E}}$.*

Mit dem folgenden Korollar schließen wir unsere Einführung in die Theorie der algebraischen Zahlkörper ab:

Korollar 2.19 *Ist $\mathbf{a}$ ein gebrochenes Ideal in $o_{\mathcal{E}}$ so, ist $\mathbf{a}^{h_{\mathcal{E}}}$ ein Hauptideal.*

Kapitel 3

Primideale

Bei der Betrachtung von algebraischen Zahlkörpern spielt das Verhalten von Primidealen eine wichtige Rolle. Insbesondere sind wir an dem Zerlegungsverhalten von Primidealen interessiert. Darunter verstehen wir die Primidealzerlegung von $\wp o_{\mathcal{E}} = \{\sum_{i=1}^{r} p_i x_i \mid r \in I\!N; p_i \in \wp; x_i \in o_{\mathcal{E}}\}$ in $o_{\mathcal{E}}$ für ein Primideal $\wp$ in $I\!P_{\mathcal{F}}$, wobei $\mathcal{E}$ und $\mathcal{F}$ algebraische Zahlkörper mit $\mathcal{F} \subset \mathcal{E}$ sind.
Bei diesen Untersuchungen erhält man eine Reihe von interessanten Ergebnissen. Die Beweise zu diesen findet man z.B. in [27].
Im weiteren seien $\mathcal{F} \subseteq \mathcal{E}$ algebraische Zahlkörper mit $[\mathcal{E} : \mathcal{F}] = n$. Falls wir nichts anderes sagen, sind $\wp$ und $\mathcal{P}$ Primideale ($\neq 0$) in $o_{\mathcal{F}}$ bzw. in $o_{\mathcal{E}}$.
Um die folgenden Definitionen zu motivieren, beginnen wir mit einem kleinen Lemma:

Lemma 3.1 *Es sind äquivalent:*

(i) $\mathcal{P} \mid \wp o_{\mathcal{E}}$

(ii) $\mathcal{P} \supseteq \wp o_{\mathcal{E}}$

(iii) $\mathcal{P} \supseteq \wp$

(iv) $\mathcal{P} \cap o_{\mathcal{F}} = \wp$

(v) $\mathcal{P} \cap \mathcal{F} = \wp$

Gilt in $o_\mathcal{E}$ die Primidealzerlegung $\wp o_\mathcal{E} = \mathcal{P}_1^{e_1} \cdot \ldots \cdot \mathcal{P}_g^{e_g}$ in paarweise verschiedene Primideale, so sind diese Primideale $\{\mathcal{P}_1, \ldots, \mathcal{P}_g\}$ genau die Ideale, die die Bed. (i)–(v) erfüllen. Wir definieren daher

Definition 3.2 *Erfüllen $\mathcal{P}$ und $\wp$ eine der Bedingungen (i)–(v) in 3.1, so sagt man, daß $\mathcal{P}$ über $\wp$ bzw. $\wp$ unter $\mathcal{P}$ liegt.*

Neben dieser Sprechweise spielt die folgende Definition eine wesentliche Rolle. Sie ist entscheidend für die weitere Theorie.

Definition 3.3 *Gilt für $\wp \in \mathbb{P}_\mathcal{F}$ in $o_\mathcal{E}$ die Primidealzerlegung*

$$\wp o_\mathcal{E} = \mathcal{P}_1^{e_1} \cdot \ldots \cdot \mathcal{P}_g^{e_g}$$

so bezeichnen wir $e(\mathcal{P}_i/\wp) := e_i$ als den **Verzweigungsindex** *von $\mathcal{P}_i$ über $\wp$. Gilt $e(\mathcal{P}_i/\wp) > 1$ für ein i, so heißt $\wp$* **verzweigt** *in $\mathcal{E}$. Sonst heißt $\wp$* **unverzweigt**.
Als den **Trägheitsgrad** *von $\mathcal{P}_i$ über $\wp$ bezeichnen wir mit $f(\mathcal{P}_i/\wp)$ den Körpergrad $[(o_\mathcal{E}/\mathcal{P}_i) : (o_\mathcal{F}/\wp)]$.*
Abkürzend schreiben wir oft f_i statt $f(\mathcal{P}_i/\wp)$ und e_i statt $e(\mathcal{P}_i/\wp)$.
Neben den Bezeichnungen verzweigt und unverzweigt nennen wir $\wp$ **total zerlegt**, *wenn $e_i = f_i = 1$ $(1 \le i \le g)$ und damit $g = [\mathcal{E} : \mathcal{F}]$ gilt.*

Bemerkung 3.4 *Liegt $\mathcal{P}$ über $\wp$, so gilt*

$$\mathrm{N}_{\mathcal{E}/\mathbb{Q}}(\mathcal{P}) = \mathrm{N}_{\mathcal{F}/\mathbb{Q}}(\wp)^{f(\mathcal{P}/\wp)}.$$

Zwischen dem Grad der Körpererweiterung $[\mathcal{E} : \mathcal{F}]$ und dem Verzweigungsindex bzw. dem Trägheitsgrad besteht nun der folgende Zusammenhang:

Satz 3.5 *Für $\wp \in \mathbb{P}_\mathcal{F}$ gelte die Zerlegung $\wp o_\mathcal{E} = \mathcal{P}_1^{e_1} \cdot \ldots \cdot \mathcal{P}_g^{e_g}$. Dann gilt*

$$[\mathcal{E} : \mathcal{F}] = \sum_{i=1}^{g} e_i f_i = \sum_{\mathcal{P} \mid \wp} e(\mathcal{P}/\wp) f(\mathcal{P}/\wp)$$

Mittels dieses Satzes können wir nun alle Möglichkeiten angeben, wie ein Primideal aus $o_{\mathcal{F}}$ in $o_{\mathcal{E}}$ zerlegt sein kann. Wir werden darauf später noch zurückkommen.
Als im weiteren nützlich wird sich die folgende Aussage erweisen:

Bemerkung 3.6 *Ist $\mathcal{P} \in \mathbb{P}_{\mathcal{E}}$ ein Primideal oberhalb von $\wp \in \mathbb{P}_{\mathcal{F}}$, so gilt:*

$$\nu_{\mathcal{P}}(\alpha) = e(\mathcal{P}/\wp) \cdot \nu_{\wp}(\alpha) \qquad ;\forall \alpha \in \mathcal{F}^*.$$

Hierbei ist $\mathcal{F}^*$ die multiplikative Gruppe von $\mathcal{F}$. Wir werden diese Bezeichnung auch allgemein für Ringe verwenden.

Es drängt sich nun natürlich die Frage auf, wie in einem konkreten Fall die Zerlegung eines Primideals aussieht und wie man sie bestimmen kann. In gewissen Fällen können wir eine Antwort geben. Dazu benötigen wir die folgende Definition:

Definition 3.7 *Es sei $\mathcal{R}$ eine Ordnung in $o_{\mathcal{E}}$. Dann bezeichnen wir das größte (bzgl. "$\subseteq$") Ideal in $o_{\mathcal{E}}$, das noch in $\mathcal{R}$ liegt, als den* **Führer** *f der Ordnung $\mathcal{R}$*

$$f = \{\alpha \in o_{\mathcal{E}} \mid \alpha o_{\mathcal{E}} \subseteq \mathcal{R}\}.$$

Wir können nun den Satz formulieren, der eine Beschreibung der Zerlegung der Primideale aus $o_{\mathcal{F}}$ in $o_{\mathcal{E}}$ liefert. Leider ist dieser Satz nicht auf alle Primideale aus $o_{\mathcal{F}}$ anwendbar. Gilt $\mathcal{E} = \mathcal{F}(\rho)$, so können wir den Satz nur auf die Primideale anwenden, die comaximal zu dem Führer von $o_{\mathcal{F}}[\rho]$ sind.

Satz 3.8 *Sei $\mathcal{E} = \mathcal{F}(\rho)$ mit $\rho \in o_{\mathcal{E}}$ und $\wp \in \mathbb{P}_{\mathcal{F}}$ ein Primideal, das teilerfremd zum Führer von $o_{\mathcal{F}}[\rho]$ ist.*
Ferner gelte für das Minimalpolynom $m_\rho(t) \in o_{\mathcal{F}}[t]$ von ρ die Zerlegung

$$\overline{m}_\rho(t) = \prod_{i=1}^{g} \bar{f}_i(t)^{e_i}$$

in Primpolynome in $(o_{\mathcal{F}}/\wp)[t]$. Sind dann $f_i(t)$ normierte Urbilder von $\bar{f}_i(t)$, so gilt die Primidealzerlegung

$$\wp o_{\mathcal{E}} = \mathcal{P}_1^{e_1} \cdot \ldots \cdot \mathcal{P}_g^{e_g}$$

mit

(i) $\mathcal{P}_i = \wp o_{\mathcal{E}} + f_i(\rho) o_{\mathcal{E}}$ $(1 \leq i \leq g)$

(ii) $f(\mathcal{P}_i/\wp) = deg(f_i)$ $(1 \leq i \leq g)$

Man beachte , daß die Primideale $\mathcal{P}_i$ $(1 \leq i \leq g)$ *paarweise verschieden sind.*

Eine Anwendung dieses Satzes ist das folgende Lemma, das für $\mathbb{Q}\,(i)$ auch schon Gauß bekannt war.

Lemma 3.9 *Sei* $\mathcal{F} = \mathbb{Q}(\sqrt{d})$ *eine quadratische Erweiterung von* $\mathbb{Q}$ *mit* $d \in \mathbb{Z}$ *quadratfrei. Ferner sei* $p \in \mathbb{P}$ *beliebig gegeben.*
Teilt p *die Körperdiskriminante, so gilt*

$$p o_{\mathcal{F}} = \wp^2 .$$

Ansonsten unterscheidet man die Fälle p *ungerade oder* p *gerade:*
Ist p *ungerade, so gilt*

$$p o_{\mathcal{F}} = \begin{cases} \wp_1 \cdot \wp_2 & ; \left(\frac{d}{p}\right) = 1 \\ \wp & ; \left(\frac{d}{p}\right) = -1 \end{cases} .$$

Ist aber $p = 2$*, so gilt*

$$p o_{\mathcal{F}} = \begin{cases} \wp_1 \cdot \wp_2 & ; d \equiv 1 \ mod\ 8 \\ \wp & ; d \equiv 5 \ mod\ 8 \end{cases} .$$

Hierbei ist $\left(\frac{d}{p}\right)$ *das Legendre–Symbol von* d *und* p*.*

Kapitel 4

Bewertungstheorie

Da im weiteren Verlauf der Arbeit die Betrachtung von sog. p-adischen Vervollständigungen algebraischer Zahlkörper eine entscheidende Rolle spielen wird, und wir dazu einige Ergebnisse aus der Bewertungstheorie benötigen, stellen wir nun hier die wichtigsten Ergebnisse dieser Theorie vor.
Man findet die folgenden Aussagen auch in [27] und [23].

4.1 Einführung und Definition

Ziel ist es, auf einem beliebigen Körper K eine Topologie über die Definition einer Metrik einzuführen. Dazu betrachtet man eine Abbildung

$$\psi : K \longrightarrow \mathbb{R}$$

von K in den Körper der reellen Zahlen.

Definition 4.1 *Sei K ein Körper und $\psi : K \longrightarrow \mathbb{R}$ eine Abbildung mit den folgenden Eigenschaften:*

(i) $\psi(1) = 1$

(ii) $\psi(x) \geq 0$, $\psi(x) = 0 \Leftrightarrow x = 0 \qquad ; \forall x \in K$

(iii) $\psi(x \pm y) \leq \psi(x) + \psi(y) \qquad ; \forall x \in K$

(iv) $\psi(x \cdot y) = \psi(x) \cdot \psi(y) \qquad ; \forall x \in K$

ψ heißt dann eine **archimedische Bewertung** *des Körpers K. Gilt statt (iii)*

(iii)' $\psi(x \pm y) \leq max(\psi(x), \psi(y))$ *;* $\forall x, y \in K$

so bezeichnet man ψ als **nicht–archimedische Bewertung** *des Körpers K, oder kurz als* **Krullbewertung**.
Erfüllt die Abbildung ψ neben (i),(ii),(iv) die Voraussetzung (iii) oder (iii)', so nennem wir ψ ganz allgemein eine Bewertung.

Ist ψ nicht ausdrücklich als archimedische bzw. als nicht–archimedische Bewertung definiert, so ist ψ als eine Bewertung zu verstehen, die sowohl nicht-archimedisch als auch archimedisch sein kann.

Bemerkung 4.2 *Ist ψ eine Bewertung des Körpers K, so wird durch*

$$d(x, y) := \psi(x - y)$$

eine Metrik auf K definiert, welche eine Topologie auf K induziert.

Um den Begriff der Bewertung etwas klarer zu machen nun einige Beispiele für Bewertungen.

Beispiel 4.3 *(Bewertungen)*

(i) Die triviale Abbildung

$$\psi : K \longrightarrow I\!R : x \rightarrow \begin{cases} 0 & ; x = 0 \\ 1 & ; sonst \end{cases}$$

ist immer eine nicht-archimedische Bewertung.

(ii) *(Hensel) Es sei* $g \in \mathbb{Z}^{\geq 2}$ *beliebig gegeben. Wir setzen:*

$$|\cdot|_g : \mathbb{Q} \longrightarrow \mathbb{R} : x \to \begin{cases} 0 & ; x = 0 \\ g^{-n} & ; x = g^n \frac{r}{s} \; mit \; g \nmid r \; und \; ggt(g,s) = 1 \end{cases}$$

   (a) *Gilt* $g \in \mathbb{P}$, *so ist* $|\cdot|_g$ *eine nicht-archimedische Bewertung von* $\mathbb{Q}$.

   (b) *Gilt* $g \notin \mathbb{P}$ *so handelt es sich bei* $|\cdot|_g$ *um eine sogenannte Pseudo-Bewertung von* $\mathbb{Q}$.

(iii) *Eine Verallgemeinerung des letzten Beispiels wird durch folgende Definition erreicht:*
Sei $\mathcal{F}$ *ein algebraischer Zahlkörper und sei* $\wp$ *ein Primideal in* $o_{\mathcal{F}}$. *Definiert man dann*

$$|x|_{\wp,\alpha} := \alpha^{\nu_\wp(x)} \qquad ; |0|_{\wp,\alpha} := 0$$

mit einem $\alpha \in]0,1[$, *so wird durch* $|\cdot|_{\wp,\alpha}$ *eine nicht–arch. Bewertung auf* $\mathcal{F}$ *definiert. Wir nennen eine solche Bewertung eine* $\wp$*–adische Bewertung auf* $\mathcal{F}$.

(iv) *Der gewöhnliche Absolutbetrag ist eine archimedische Bewertung auf* $\mathbb{Q}$.

Bevor wir uns mit tieferliegenden Eigenschaften von Bewertungen beschäftigen, stellen wir einige im weiteren Verlauf immer wieder benötigten Eigenschaften zusammen. Im Anschluß daran werden wir auf die für algebraische Zahlkörper wichtigen Bewertungen eingehen.

Lemma 4.4 *Sei* $\psi : K \longrightarrow \mathbb{R}$ *eine Bewertung auf dem Körper* K. *Dann gelten*

(i) $\psi(-1) = 1$

(ii) $\psi(-\alpha) = \psi(\alpha) \quad \forall \alpha \in K$

(iii) *Ist* ψ *eine nicht–archimedische Bewertung und sind* $\alpha_1, \ldots, \alpha_n \in K$ *gegeben mit* $\psi(\alpha_i) \neq \psi(\alpha_j)$ $(1 \leq i < j \leq n)$, *so gilt*

$$\psi(\alpha_1 + \ldots + \alpha_n) = max\{\psi(\alpha_i) | 1 \leq i \leq n\}$$

(iv) *Sind $\alpha_1, \ldots, \alpha_n \in K$ gegeben mit $\alpha_1 + \ldots + \alpha_n = 0$, so gilt*

$$\exists 1 \leq i < j \leq n: \quad max\{\psi(\alpha_l)|1 \leq l \leq n\} = \psi(\alpha_i) = \psi(\alpha_j)$$

Beweis: Die Aussagen (i) und (ii) sind direkte Folgerungen der Definition 4.1. Man beachte, daß ψ multipikativ ist.
zu (iii): Wir beweisen (iii) mittels vollständiger Induktion und müssen sowohl für $n = 1$ als auch für $n = 2$ eine Induktionsverankerung durchführen.
Induktionsverankerung:
$n = 1$: klar.
$n = 2$: O.B.d.A gelte $\psi(\alpha_1) < \psi(\alpha_2)$. Dann folgt aus 4.1(iii)

$$\psi(\alpha_2) = \psi((\alpha_2 + \alpha_1) - \alpha_1) \leq max(\psi(\alpha_2 + \alpha_1), \psi(\alpha_1))$$

Da nach Vor. aber $\psi(\alpha_1) < \psi(\alpha_2)$ gilt, folgt also

$$\psi(\alpha_2) \leq max(\psi(\alpha_2 + \alpha_1))$$

und damit folgt mit Definition 4.1(iii) die Behauptung.
Induktionsschluß:
Ist nach dem Beweis für $n = 2$ klar.
zu (iv): Direkte Folgerung aus (iii). ■
Zur Motivation der nächsten Definition erinnern wir an das Beispiel 4.3 (iii). Dort haben wir eine Bewertung $|\cdot|_{\wp,\alpha}$ auf einem algebraischen Zahlkörper $\mathcal{F}$ zu einem Primideal $\wp$ und einem $\alpha \in]0,1[$ definiert. Betrachtet man nun zwei solche Bewertungen $|\cdot|_{\wp,\alpha_1}$ und $|\cdot|_{\wp,\alpha_2}$ zu zwei verschiedenen α_1 und α_2, so sind diese Bewertungen natürlich verschieden, obwohl sie auf $\mathcal{F}$ die gleichen Relationen erzeugen. Daher definieren wir:

Definition 4.5 (i) *Seien ψ_1, ψ_2 zwei Bewertungen auf einem Körper K. Dann heißen diese Bewertungen* **äquivalent**, *falls*

$$\forall \alpha, \beta \in K \; : \; \psi_1(\alpha) < \psi_1(\beta) \Leftrightarrow \psi_2(\alpha) < \psi_2(\beta)$$

(ii) *Ist ψ eine Krullbewertung, deren Bild des Definitionsbereiches zyklisch ist, so heißt ψ* **diskret**.

Bemerkung 4.6 *(i) Zwei Bewertungen ψ_1, ψ_2 sind genau dann äquivalent, wenn sie die gleiche Topologie auf K erzeugen.*

(ii) Sind ψ_1, ψ_2 zwei äquivalente Bewertungen des Körpers K, so existiert ein $\alpha \in I\!R^{>0}$ mit

$$\psi_1(x) = \psi_2(x)^\alpha \qquad\qquad \forall x \in K;$$

(iii) Eine Krullbewertung ist genau dann diskret, wenn

$$\{log(\psi(x)) \mid x \in K \setminus \{0\}\}$$

in $I\!R$ diskret ist.

(iv) Eine diskrete Bewertung ist nach Definition immer eine Krullbewertung, also immer nicht–archimedisch.

Lemma 4.7 *Ist ψ eine Krullbewertung auf K, so ist*

$$\Re_\psi := \{x \in K \mid \psi(x) \leq 1\}$$

ein lokaler Ring mit dem maximalen Ideal

$$\mathrm{m}_\psi := \{x \in K \mid \psi(x) < 1\}.$$

Beweis: Zunächst ist $\Re_\psi$, aufgrund der Bewertungseigenschaften von ψ, ein Ring.
Für den weiteren Beweis beachte man (vgl. [21])

$$\Re_\psi \textit{ ist lokaler Ring} \Leftrightarrow \Re_\psi \setminus \Re_\psi^* \textit{ ist ein Ideal in } \Re_\psi.$$

Für $x, x^{-1} \in \Re_\psi$ gilt

$$\begin{aligned} 1 = \psi(1) = \psi(x \cdot x^{-1}) &= \psi(x)\psi(x^{-1}) \\ \Rightarrow \qquad \psi(x) &= \psi(x^{-1}) = 1. \end{aligned}$$

Gilt andererseits $\psi(x) = 1$ für ein $x \in \Re_\psi$, so gilt für $x^{-1} (\in K)$ analog $\psi(x^{-1}) = 1$, also ist x eine Einheit in $\Re_\psi$. Womit gezeigt wäre:

$$x \in \Re_\psi \textit{ ist Einheit in } \Re_\psi \Leftrightarrow \psi(x) = 1.$$

Da m_ψ offenbar ein Ideal in $\Re_\psi$ ist, folgt daraus die Behauptung. ■
Der Ring $\Re_\psi$ ist der **Bewertungsring** und m_ψ ist das **Bewertungsideal** von ψ.
Kommen wir nun wieder auf die Betrachtung von diskreten Bewertungen zurück, da diese, wie wir später sehen werden, für algebraische Zahlkörper die entscheidende Rolle spielen.
Sei also ψ eine diskrete Bewertung von K. Dann gilt nach Definition 4.5 für ein $\alpha \in]0,1[$

$$\psi(x) = \alpha^{n(x)} \qquad ; \forall x \in K$$

Entscheidend für das Verhalten der diskreten Bewertung ψ ist also das Verhalten der Funktion n. Es macht daher Sinn sogenannte exponentielle Bewertungen zu definieren:

Definition 4.8 *Eine surjektive Abbildung*

$$\eta \; : \; K \longrightarrow \mathbb{Z} \cup \{\infty\}$$

heißt **exponentielle (Krull–) Bewertung**, *falls für alle $x, y \in K$ gilt*

(i) $\eta(x) = \infty \Leftrightarrow x = 0$,

(ii) $\eta(x \pm y) \geq min(\eta(x), \eta(y))$,

(iii) $\eta(xy) = \eta(x) + \eta(y)$,

(iv) $\eta(\pm 1) = 0$.

Wir haben vor dieser Definition schon kurz den Zusammenhang zwischen einer diskreten Bewertung und einer exponentiellen Bewertung angedeutet. Wir wollen dies nun vertiefen.

Bemerkung 4.9 *Ist η eine exponentielle Bewertung auf K, so ist η ein Homomorphismus von $(K^*, \cdot)$ nach $(\mathbb{Z}, +)$.*

Beispiel 4.10 *Sei $\mathcal{F}$ ein algebraischer Körper und $\wp \in \mathbb{P}_\mathcal{F}$ beliebig gegeben. Auf $\mathcal{F}$ wird dann durch $\nu_\wp$ eine exponentielle Bewertung definiert, wenn man*

$\nu_\wp$ auf die gebrochenen Hauptideale von $o_{\mathcal{F}}$ anwendet.
Man erkennt schon die Ähnlichkeit dieses Beispiels mit dem in 4.3 (iii) gegebenen Beispiel.

Den Zusammenhang zwischen diskreten Bewertungen und exponentiellen Bewertungen stellt das folgende Lemma dar:

Lemma 4.11 *Ist ψ mit $\psi(x) = \alpha^{n(x)}$ $(\alpha \in]0,1[)$ eine diskrete Bewertung, so ist n eine exponentielle Bewertung.*
Ist andererseits η eine exponentielle Bewertung, so wird mit $\alpha \in]0,1[$ durch $\nu(x) = \alpha^{\eta(x)}$ eine Krullbewertung definiert.

Zum Beweis: Siehe z.B. [23]

Bemerkung 4.12 *Der Bewertungsring einer exponentiellen Bewertung ist*

$$\Re_\eta = \{x \in K \mid \eta(x) \geq 0\}$$

mit dem maximalen Ideal

$$\mathrm{m}_\eta = \{x \in K \mid \eta(x) > 0\}.$$

Dieser Bewertungsring ist aufgrund der Analogie zwischen exponentiellen Bewertungen und diskreten Bewertungen ein lokaler Ring mit dem maximalen Ideal m_η.

Wir schließen diese Einführung mit folgendem Satz aus [23]:

Satz 4.13 *Sei η eine exponentielle Bewertung auf K. Dann ist $\Re_\eta$ ein Hauptidealring. Sein einziges Primideal (und somit maximales Ideal) wird durch eine beliebiges $\alpha \in K$ erzeugt mit $\eta(\alpha) = 1$.*

Beweis: Es bleibt nur noch die Hauptidealeigenschaft von $\Re_\eta$ zu zeigen.
Sei dazu α mit $\eta(\alpha) = 1$ beliebig gegeben. Dann gilt $\alpha\Re_\eta \subseteq m_\eta$ und für ein $\beta \in m_\eta$ mit $\eta(\beta) = m$ gilt $\beta\alpha^{-m} \in \Re_\eta$.

Daraus folgt $\beta = \alpha^m(\beta\alpha^{-m}) \in \alpha^m\Re_\eta \subset \alpha\Re_\eta$ und damit gilt schließlich $m_\eta \subseteq \alpha\Re_\eta$.
Ist nun $\mathbf{a} \neq m_\eta$ ein Ideal in $\Re_\eta$, so existiert $m \in I\!N$ mit $\mathbf{a} \subseteq m_\eta^m$ und $\mathbf{a} \not\subseteq m_\eta^{m+1}$ (man beachte : $\bigcap_{n\in I\!N} m_\eta^n = \{0\}$). Dann existiert in $\mathbf{a}$ ein β mit $\eta(\beta) = m$, denn es existiert ein $\beta \in \mathbf{a}$ mit $\beta \in m_\eta^m \setminus m_\eta^{m+1}$. Daher gilt $\beta = \alpha^m\gamma$, wobei γ eine Einheit in $\Re_\eta$ ist, und wir erhalten neben $\beta\Re_\eta = \alpha^m\Re_\eta$

$$m_\eta^m = \alpha^m\Re_\eta = \beta\Re_\eta \subseteq \mathbf{a}$$

und somit $\alpha^m\Re_\eta = \mathbf{a}$. ■

Bemerkung 4.14 *(i) Wie wir im Beweis des letzten Lemmas gesehen haben gilt für ein beliebiges Ideal* $\mathbf{a} \subseteq \mathrm{m}_\eta$*:*

$$\exists\, m \in I\!N \;:\; \mathrm{m}_\eta^m = \mathbf{a}$$

(ii) Aufgrund des Zusammenhanges zwischen exponentiellen Bewertungen und diskreten Bewertungen sind diese Aussagen natürlich auch für diskrete Bewertungen richtig.

4.2 Bewertungen auf algebraischen Zahlkörpern

Wir wollen uns nun näher mit Bewertungen auf algebraischen Zahlkörpern beschäftigen. Den Standardtyp einer solchen Bewertung haben wir schon kennengelernt (siehe 4.3 (iii)) und wir haben auch schon festgestellt, daß jede solche Bewertung eine exponentielle Bewertung erzeugt, bzw. von einer solchen erzeugt wird.
Die Frage lautet nun: Wie sehen (bis auf Äquivalenz) alle Bewertungen auf einem algebraischen Zahlkörper aus?
Der folgende Satz ist ein Ergebnis von A. Ostrowski [23] und beschreibt alle Bewertungen auf einem algebraischen Zahlkörper.

Satz 4.15 *Sei $\mathcal{F}$ ein algebraischer Zahlkörper über $\mathbb{Q}$. Dann ist jede nicht triviale Bewertung von $\mathcal{F}$ entweder diskret oder archimedisch.*
Ist ψ eine diskrete Bewertung, so existiert ein $\wp \in I\!P_{\mathcal{F}}$ und ein $\alpha \in]0,1[$ mit:

$$\psi(x) = \alpha^{\nu_\wp(x)} \qquad \forall x \in \mathcal{F}.$$

Ist ψ aber eine archimedische Bewertung auf $\mathcal{F}$, so gilt

$$\psi(x) = |\phi(x)| \qquad \forall x \in \mathcal{F},$$

wobei ϕ einer der $\mathbb{Q}$–Isomorphismen von $\mathcal{F}$ ist. Zwei archimedische Bewertungen sind genau dann äquivalent, wenn die zugehörigen Einbettungen zueinander komplex–konjugiert sind.

Bemerkung 4.16 *Nach dem letzten Satz sind auch alle Bewertungen auf $\mathbb{Q}$ bestimmt. Ist ψ eine Bewertung auf $\mathbb{Q}$, so ist sie entweder äquivalent zu einer von einer Primzahl $p \in I\!P$ erzeugten diskreten Bewertung, oder sie ist der gewöhnliche Absolutbetrag.*

Betrachten wir eine nicht–archimedische Bewertung auf einem algebraischen Zahlkörper, so sind wir nicht an den eigentlichen Funktionswerten dieser Bewertung interessiert; vielmehr interessiert uns der Bewertungsring und das Bewertungsideal und diese sind für alle äquivalenten nicht–archimedischen Bewertungen gleich. Für ein $\wp \in I\!P_{\mathcal{F}}$ sprechen wir daher von der Bewertung $|\cdot|_\wp$ und meinen eine beliebige von $\wp$ erzeugte Bewertung.
Wir definieren deshalb:

Definition 4.17 *Sei $\mathcal{F}$ ein algebraischer Zahlkörper und sei $\wp \in I\!P_{\mathcal{F}}$. Ferner sei $\mathcal{E}/F$ eine endliche Relativerweiterung.*

*(i) Ein $x \in \mathcal{F}$ heißt $\wp$–**ganz** falls $|x|_{\wp} \leq 1$ gilt.*

*(ii) Ein $x \in \mathcal{E}$ heißt $\wp$–**ganz** falls ein $f(t) = t^k + \sum_{i=1}^{k} a_i t^{k-i} \in \mathcal{F}[t]$ existiert mit $f(x) = 0$ und $|a_i|_{\wp} \leq 1$ $(1 \leq i \leq k)$.*

*(iii) $o_{\mathcal{F}}(\wp) := \{x \in \mathcal{F} \mid |x|_{\wp} \leq 1\}$ heißt die Menge der $\wp$–**ganzen Elemente in** $\mathcal{F}$.*

*(iv) $o_{\mathcal{E}}(\wp) := \{x \in \mathcal{E} \mid x$ ist $\wp$–ganz $\}$ heißt die Menge der $\wp$–**ganzen Elemente in** $\mathcal{E}$.*

Bemerkung 4.18 *Gilt $\mathcal{F} = \mathbb{Q}$, so schreiben wir $\mathbb{Z}(p)$ statt $o_{\mathcal{F}}(p)$ für $p \in I\!P$. Es gilt offenbar:*

$$\mathbb{Z}(p) = \{\frac{a}{b} \in \mathbb{Q} \mid ggt(a,b) = 1 \text{ und } p \not| b\}.$$

Mittels dieser Definition stellen wir nun abschließend fest:

Lemma 4.19 *Für einen algebraischen Zahlkörper $\mathcal{F}$ gilt:*

$$x \in o_{\mathcal{E}} \Leftrightarrow x \in o_{\mathcal{E}}(\wp) \quad \forall \wp \in I\!P_{\mathcal{F}}$$

Beweis: Der Beweis ist trivial, da $o_{\mathcal{E}}$ ein Dedekindring ist und somit jedes Ideal eine eindeutige Zerlegung in Primideale besitzt. ■

Kapitel 5

$\wp$–adische Körper

In diesem Kapitel gehen wir näher auf die Eigenschaften $\wp$–adischer Bewertungen auf algebraischen Zahlkörpern ein. Speziell interessiert uns das Verhalten von solchen Bewertungen in Relativerweiterungen. Bei solchen Untersuchungen spielt das Zerlegungsverhalten der Primideale des Grundkörpers in der Erweiterung eine sehr wichtige Rolle. Eine Möglichkeit, dieses Verhalten zu studieren, bilden die lokalen (auf ein Primideal beschränkten) Erweiterungen. Betrachtet man alle lokalen Erweiterungen $\mathcal{E}_{\mathcal{P}}/\mathcal{F}_{\wp}$, so kann man Rückschlüsse auf den globalen Fall $\mathcal{E}/\mathcal{F}$ ziehen.
Weisen wir nicht näher auf die Herkunft der Ergebnisse hin, so findet man sie in [5] oder in [23].
Im weiteren seien $\mathcal{E}, \mathcal{F}$ algebraische Zahlkörper mit $\mathcal{E} = \mathcal{F}(\rho)$ für ein ganz algebraisches ρ. Ferner seien $\wp \in I\!P_{\mathcal{F}}$ und $\mathcal{P} \in I\!P_{\mathcal{E}}$ mit $\mathcal{P} | \wp o_{\mathcal{E}}$ gegeben.

5.1 Vervollständigungen

Die Grundlage für unsere weiteren Betrachtungen bildet der nächste Satz, der u.a. auch in [27],[5],[6] zu finden ist.

Satz 5.1 *Es existiert ein Körper $\mathcal{F}_{\wp}$ mit* *(i)* $\mathcal{F}_\wp$ *ist vollständig bzgl. der Fortsetzung von* $|\cdot|_\wp$ *auf* $\mathcal{F}_\wp$ *(Wir bezeichnen diese Fortsetzung ebenfalls mit* $|\cdot|_\wp$*),*

(ii) $\mathcal{F}$ *liegt dicht in* $\mathcal{F}_\wp$*,*

(iii) Ist $\mathcal{R}$ *ein minimales Restsystem von* $o_\mathcal{F}/\wp$ *mit* $0 \in \mathcal{R}$ *und ist* $\pi \in \wp\backslash\wp^2$ ($\Rightarrow$ $|\pi|_\wp < 1$ *ist maximal), so gilt:*

$$\mathcal{F}_\wp = \{\sum_{i=m}^{\infty} \alpha_i \pi^i \mid \alpha_i \in \mathcal{R}\ ,\ m \in \mathbb{Z}\ ,\ \alpha_m \neq 0\}.$$

Die Fortsetzung von $|\cdot|_\wp$ auf $\mathcal{F}_\wp$ ist wieder eine diskrete Bewertung. Damit ist

$$\Re_\wp = \{\sum_{i=m}^{\infty} \alpha_i \pi^i \mid \alpha_i \in \mathcal{R}\ ,\ m \in \mathbb{Z}^{\geq 0}\ ,\ \alpha_m \neq 0\}$$

der Bewertungsring von $|\cdot|_\wp$ in $\mathcal{F}_\wp$ nach Satz 4.13 ein lokaler Hauptidealring mit dem maximalen Ideal

$$m_\wp = \{\sum_{i=m}^{\infty} \alpha_i \pi^i \mid \alpha_i \in \mathcal{R}\ ,\ m \in \mathbb{Z}^{\geq 1}\ ,\ \alpha_m \neq 0\}.$$

Die Elemente aus $\Re_\wp$ bezeichnen wir als die ganzen Elemente von $\mathcal{F}_\wp$. Nun gilt für diese Vervollständigung folgende Beziehung zum Grundkörper $\mathcal{F}$ (vgl. z.B. [5]):

$$o_\mathcal{F}(\wp) = \mathcal{F} \cap \Re_\wp, \qquad \wp = o_\mathcal{F} \cap m_\wp. \tag{5-1}$$

Darüber hinaus ist $\Re_\wp/m_\wp$ isomorph zu $o_\mathcal{F}/\wp$ ([23]).
Wir nennen $\mathcal{F}_\wp$ einen $\wp$–adischen oder auch lokalen Körper. Wir werden statt der Bezeichnung $\Re_\wp$ auch die Bezeichnung $\mathcal{S}_\wp$ gebrauchen, falls zwei Körper gleichzeitig verwendet werden.
Der folgende Satz ist eine Umkehrung des sogenannten Reduktionssatzes (vgl. [21]) und ist als “Hensel's Lemma” bekannt.

Satz 5.2 *Sei* Φ *der Restklassenkörper* $\Re_\wp/\mathrm{m}_\wp$ *und sei*

$$\psi\ :\ \Re_\wp \longrightarrow \Phi\quad :\quad x \to \bar{x}$$

die kanonische Restklassenabbildung. Ferner sei $f(t) \to \bar{f}(t)$ die Fortsetzung von ψ auf den Polynomring.
Gilt $deg(f) = deg(\bar{f})$ für ein Polynom $f(t) \in \Re_\wp[t]$ und ist das Polynom $\bar{f}(t)$ in $\Phi[t]$ Produkt zweier zueinander primer Polynome positiven Grades, so ist auch $f(t)$ in $\Re_\wp[t]$ als ein solches Produkt darstellbar.
Gilt $\bar{f}(t) = f_1(t)f_2(t)$ in $\Phi[t]$, so gilt in $\Re_\wp[t]$ die Zerlegung $f(t) = F_1(t)F_2(t)$ mit $deg(F_i) = deg(f_i)$ und $f_i(t) = \bar{F}_i(t)$ $(i = 1, 2)$.

Interessant ist dieser Satz für diese Arbeit aus folgendem Grund:

Korollar 5.3 *Hat für $f(t) \in \Re_\wp[t]$ das Polynom $\bar{f}(t) \in \Phi[t]$ eine einfache Nullstelle $\beta \in \Phi$, so existiert ein $\gamma \in \Re_\wp$ mit $\bar{\gamma} = \beta$ und $f(\gamma) = 0$.*

5.2 Erweiterungen

Kommen wir nun auf die algebraischen Zahlkörper und Relativerweiterungen zurück. Dabei betrachten wir auch beliebige (endliche) Erweiterungen $\wp$–adischer Körper.

Satz 5.4 *Sei $\mathcal{M}/\mathcal{F}_\wp$ eine endliche Erweiterung mit $[\mathcal{M} : \mathcal{F}_\wp] = n$. Dann existiert eine (bis auf Äquivalenz eindeutige) Fortsetzung $|\cdot|$ von $|\cdot|_\wp$ auf $\mathcal{M}$ mit:*

(i) $\mathcal{M}$ *ist vollständig bzgl.* $|\cdot|$

(ii) $|x| = |\,\mathrm{N}_{\mathcal{M}/\mathcal{F}_\wp}(x)|_\wp^{1/n} \quad \forall x \in \mathcal{M}$

Zum Beweis: Siehe z.B. [27] oder auch [5],[6].
Eine einfache, wenn auch wichtige Folgerung aus diesem Satz ist:

Korollar 5.5 *Ist $\mathcal{M}/\mathcal{F}_\wp$ eine endliche Erweiterung, so ist $x \in \mathcal{M}$ genau dann ganz, wenn $\mathrm{N}_{\mathcal{M}/\mathcal{F}_\wp}(x)$ in $\mathcal{F}_\wp$ ganz ist.*

Satz 5.6 *Sei $\mathcal{E}/\mathcal{F}$ eine Relativerweiterung vom Grad n und $|\cdot|_\wp$ eine Bewertung auf $\mathcal{F}$.*
Gilt dann $\wp o_\mathcal{E} = \mathcal{P}_1^{e_1} \cdot \ldots \cdot \mathcal{P}_g^{e_g}$, so sind die Bewertungen $|\cdot|_{\mathcal{P}_i}$ $(1 \leq i \leq g)$ alle Fortsetzungen von $|\cdot|_\wp$ nach $\mathcal{E}$.

Bemerkung 5.7 *Wir haben bei dem letzten Satz darauf verzichtet die genaue Gestalt von $|\cdot|_{\mathcal{P}_i}$ als Fortsetzung von $|\cdot|_\wp$ zu beschreiben, da wir dies nicht benötigen. Gilt aber $|x|_\wp = \alpha^{\nu_\wp(x)}$ so ist $|x|_{\mathcal{P}_i} := \alpha_i^{\nu_\mathcal{P}(x)}$ mit $\alpha_i := \alpha^{1/e_i}$ $(1 \leq i \leq g)$ die genaue Fortsetzung von $|\cdot|_\wp$.*

Diese Erkenntnis über die Fortsetzbarkeit von Bewertungen überträgt sich auch auf die $\wp$–adischen Erweiterungen von $\mathcal{E}$ und $\mathcal{F}$, wie der folgende Satz zeigt.

Satz 5.8 *Es sei $\mathcal{E}/\mathcal{F}$ eine Relativerweiterung und für $\wp \in I\!P_\mathcal{F}$ gelte die Zerlegung*

$$\wp o_\mathcal{E} = \mathcal{P}_1^{e(\mathcal{P}_1/\wp)} \cdot \ldots \cdot \mathcal{P}_g^{e(\mathcal{P}_g/\wp)}.$$

Für $1 \leq i \leq g$ gelten dann:

(i) $[\mathcal{E}_{\mathcal{P}_i} : \mathcal{F}_\wp] = e(\mathcal{P}_i/\wp) f(\mathcal{P}_i/\wp)$,

(ii) $\nu_\wp(\mathrm{N}_{\mathcal{E}_{\mathcal{P}_i}/\mathcal{F}_\wp}(\alpha)) = f(\mathcal{P}_i/\wp)\nu_{\mathcal{P}_i}(\alpha) \quad \forall \alpha \in \mathcal{E}$,

(iii) $\mathcal{E}_{\mathcal{P}_i} = \mathcal{E}\mathcal{F}_\wp$.

Wenn wir nun für zwei feste Primideale $\mathcal{P} \in I\!P_\mathcal{E}$ und $\wp \in I\!P_\mathcal{F}$, $\mathcal{P}|\wp o_\mathcal{E}$ mit $f := f(\mathcal{P}/\wp)$ und $e := e(\mathcal{P}/\wp)$ die $\wp$–adischen Vervollständigungen $\mathcal{E}_\mathcal{P}$ bzw. $\mathcal{F}_\wp$ betrachten, so betrachten wir natürlich auch das Verhältnis der Ringe der ganzen Elemente $\mathcal{S}_\mathcal{P}$ von $\mathcal{E}_\mathcal{P}$ bzw. $\Re_\wp$ von $\mathcal{F}_\wp$ zueinander. Wir stellen fest, daß $\mathcal{S}_\mathcal{P}$ eine $\Re_\wp$–Basis besitzt.

Lemma 5.9 *Sei $\pi \in \mathcal{P} \setminus \mathcal{P}^2$ und seien $\{\beta_1, \ldots, \beta_f\} \subset \mathcal{S}_\mathcal{P}$ die Vertreter einer Basis von $(\mathcal{S}_\mathcal{P}/\mathrm{m}_\mathcal{P})/(\Re_\wp/\mathrm{m}_\wp)$. Dann wird durch*

$$\{\beta_i \pi^j \mid 1 \leq i \leq f; 0 \leq j < e\}$$

eine $\Re_\wp$–Basis von $\mathcal{S}_\mathcal{P}$ gegeben.

Man kann sogar beweisen, daß es eine Potenzbasis gibt, die $\mathcal{S}_\mathcal{P}$ als $\Re_\wp$–Modul erzeugt, jedoch ist diese Aussage für die weitere Arbeit von keiner Relevanz. Daher bemerken wir dies nur am Rande.
Wichtiger ist die Tatsache, daß man die Basis aus Elementen aus $\mathcal{E}$ erzeugen kann.

5.3 Lokale Differenten

In diesem kurzen Paragraphen definieren wir eine Invariante einer $\wp$–adischen Erweiterung, die Differente.
Wie wir wissen ist $m_\mathcal{P}$ in $\mathcal{S}_\mathcal{P}$ sowohl ein Hauptideal, als auch das maximale Ideal in $\mathcal{S}_\mathcal{P}$. Es gelte daher im weiteren:

$$m_\mathcal{P} = (\sigma)$$

Lemma 5.10 *Definiert man*

$$\mathcal{D}^*_{\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp} := \{x \in \mathcal{E}_\mathcal{P} \mid \mathrm{Tr}_{\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp}(xy) \in \Re_\wp \ \forall y \in \mathcal{S}_\mathcal{P}\},$$

so ist $\mathcal{D}^*_{\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp}$ ein gebrochenes Ideal in $\mathcal{S}_\mathcal{P}$ mit $\mathcal{D}^*_{\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp} \supseteq \mathcal{S}_\mathcal{P}$.
Wir bezeichnen $\mathcal{D}^*_{\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp}$ als die **Codifferente** *von $\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp$.*

Da $\mathcal{S}_\mathcal{P}$ ein Hauptidealring ist und jedes Ideal in $\mathcal{S}_\mathcal{P}$ eine Potenz des Primideals ist, exsistiert ein $m \in \mathbb{Z}^{\geq 0}$ mit

$$\sigma^{-m}\mathcal{S}_\mathcal{P} = \mathcal{D}^*_{\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp}.$$

Mittels der Codifferente definieren wir nun die Differente der Erweiterung $\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp$:

Definition 5.11 *Gilt $\mathcal{D}^*_{\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp} = \sigma^{-m}\mathcal{S}_\mathcal{P}$, so heißt*

$$\mathcal{D}_{\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp} := (\mathcal{D}^*_{\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp})^{-1} = \sigma^m\mathcal{S}_\mathcal{P}$$

die **Differente** *der Erweiterung $\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp$.*

Für uns ist der Begriff der Differente deshalb wichtig, weil über die Differente auch eine Aussage über das Verzweigungsverhalten von $\mathcal{P}$ über $\wp$ gemacht werden kann. Dazu benutzen wir die Definition:

Definition 5.12 *Die Erweiterung $\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp$ heißt* **unverzweigt**, *wenn*

$$e = e(\mathcal{P}/\wp) = 1$$

gilt.

Nun der entscheidende Satz:

Satz 5.13 *Für die Erweiterung $\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp$ gilt:*

$$\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp \textit{ ist unverzeigt } \Leftrightarrow \mathcal{D}_{\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp} = \mathcal{S}_\mathcal{P}$$

5.4 Anwendungen

Die Anwendungen der $\wp$–adischen Theorie sind vielfältig. Viele Beispiele werden im nächsten Kapitel gegeben. Das Vorgehen bei der Anwendung ist immer so, daß man ein Problem lokal, d.h für alle $\wp$–adischen Erweiterungen löst und diese Lösungen auf den globalen Fall, d.h auf die Erweiterung $\mathcal{E}/\mathcal{F}$ überträgt. Dies ist das Hassesche "lokal – global Prinzip", das folgendes besagt:

> Ist eine Aussage lokal immer richtig, so ist sie auch global richtig.

In manchen Fällen greift diese Behauptung, sie ist im allgemeinen jedoch nicht richtig, wie z.B. Selmer in [31] zeigte. Wir werden jedoch eine für uns wichtige Anwendung dieses Prinzipes hier sehen.
Für den Rest dieses Paragraphen sei wieder $\wp \in I\!P_\mathcal{F}$ und es gelte

$$\wp o_\mathcal{E} = \mathcal{P}_1^{e_1} \cdot \ldots \cdot \mathcal{P}_g^{e_g}.$$

Zunächst kommen wir wieder auf die $\wp$–ganzen Elemente von $\mathcal{E}$ zurück.

Lemma 5.14 *Für $\alpha \in \mathcal{E}$ sind äquivalent:*

(i) α *ist* $\wp$*–ganz*

(ii) $|\alpha|_{\mathcal{P}_i} \leq 1$ *für* $1 \leq i \leq g$.

Bemerkung 5.15 *Da für jedes Primideal $\mathcal{P} \in I\!P_{\mathcal{E}}$ ein Primideal $\mathbf{q} \in I\!P_{\mathcal{F}}$ existiert mit $\mathcal{P}|\mathbf{q}o_{\mathcal{E}}$, gilt nach Lemma 4.19 für $x \in \mathcal{E}$:*

$$x \in o_{\mathcal{E}} \Leftrightarrow x \in o_{\mathcal{E}}(\mathbf{q}) \; \forall \mathbf{q} \in I\!P_{\mathcal{F}}.$$

Die $\wp$–ganzen Elemente bieten uns also die Möglichkeit mittels der Primideale aus $o_{\mathcal{F}}$ Aussagen über $o_{\mathcal{E}}$ zu machen. Nach 5-1 und dem letzten Lemma gilt

$$o_{\mathcal{E}}(\wp) = \bigcap_{i=1}^{g} (\mathcal{E} \cap \Re_{\mathcal{P}_i}) = \bigcap_{i=1}^{g} o_{\mathcal{E}}(\mathcal{P}_i). \tag{5-2}$$

Das interessante an $o_{\mathcal{E}}(\wp)$ ist nun die Tatsache, daß dieser Ring eine $o_{\mathcal{F}}(\wp)$–Basis hat. Diese setzt sich aus den lokalen Basen zusammen ([5]). Speziell gilt der Satz:

Satz 5.16 *Es gelte $\mathcal{E} = \mathcal{F}(\delta)$ für eine Nullstelle δ des normierten Polynoms $f(t) \in o_{\mathcal{F}}(\wp)$. Gilt dann für $1 \leq i \leq g$*

$$|f'(\delta)|_{\mathcal{P}_i} = 1,$$

so ist $1, \delta, \ldots, \delta^{[\mathcal{E}:\mathcal{F}]-1}$ eine $o_{\mathcal{F}}(\wp)$–Basis von $o_{\mathcal{E}}(\wp)$.

Zum Beweis: Siehe [5].
Wie angesprochen, ist es ja unsere Hoffnung mittels lokaler Informationen ein globales Problem zu lösen. Betrachten wir $Z\!\!Z$–Ganzheitsbasen, so gilt (vgl. [5]):

Lemma 5.17 *Es sei $[\mathcal{F} : \mathbb{Q}] = m$ und für jedes $p \in I\!P$ sei*

$$\{\omega_1, \ldots, \omega_m\}$$

eine $Z\!\!Z(p)$–Basis von $o_{\mathcal{F}}(p)$. Dann wird durch $\{\omega_1, \ldots, \omega_m\}$ eine Ganzheitsbasis von $o_{\mathcal{F}}$ gegeben.

Beweis: Die Behauptung folgt sofort aus Lemma 4.19, denn ist $\alpha \in o_{\mathcal{E}}$ beliebig gegeben, so hat α eine eindeutige Darstellung in der $\mathbb{Q}$–Basis $\omega_1, \ldots, \omega_m$ von $\mathcal{F}$:

$$\alpha = \sum_{i=1}^{m} \alpha_i \omega_i.$$

Da α ganz algebraisch ist, gilt nach 4.19 nun aber $\alpha_i \in \mathbb{Z}(p)\ \forall\, p \in \mathbb{P}$ für $1 \leq i \leq m$, also gilt $\alpha_i \in \mathbb{Z}$ und damit $o_{\mathcal{F}} \subseteq [\omega_1, \ldots, \omega_m]_{\mathbb{Z}}$.
Bleibt noch $[\omega_1, \ldots, \omega_m]_{\mathbb{Z}} \subseteq o_{\mathcal{F}}$ zu zeigen. Dies ist aber trivial , denn für $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}$ gilt

$$\alpha := \sum_{i=1}^{m} \alpha_i \omega_i \in \bigcap_{p \in \mathbb{P}} o_{\mathcal{F}}(p) = o_{\mathcal{F}}.$$

■

Andererseits wird durch eine Ganzheitsbasis von $o_{\mathcal{F}}$ auch immer eine lokale Basis gegeben ([5]):

Lemma 5.18 *Es sei $[\mathcal{F} : \mathbb{Q}\,] = m$ und $\omega_1, \ldots, \omega_m$ eine Ganzheitsbasis von $o_{\mathcal{F}}$. Dann wird für $p \in \mathbb{P}$ durch $\omega_1, \ldots, \omega_m$ auch eine $\mathbb{Z}(p)$–Basis von $o_{\mathcal{F}}(p)$ gegeben.*

Beweis: Sei $p \in \mathbb{P}$ beliebig gegeben. Für $\alpha \in o_{\mathcal{F}}(p)$ existiert dann ein $M \in \mathbb{Z} \setminus \{0\}$ mit $ggt(M, p) = 1$, so daß $M\alpha$ in $o_{\mathcal{F}}$ liegt. Es existieren also $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}$ mit

$$M\alpha = \sum_{i=1}^{m} \alpha_i \omega_i.$$

Da $\omega_1, \ldots, \omega_m$ eine $\mathbb{Q}$ –Basis von $\mathcal{F}$ ist, gilt also in eindeutiger Weise $\alpha = M^{-1} \sum_{i=1}^{m} \alpha_i \omega_i$. Da nach Voraussetzung $ggt(M, p) = 1$ gilt, ist M eine Einheit in $\mathbb{Z}(p)$ und es gilt $M^{-1} \in \mathbb{Z}(p)$. Daraus folgt $o_{\mathcal{F}}(p) \subseteq [\omega_1, \ldots, \omega_m]_{\mathbb{Z}(p)}$.
Sind andererseits $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}(p)$ gegeben, so existiert wieder ein $M \in \mathbb{Z} \setminus \{0\}$ mit $ggt(M, p) = 1$ und $M\alpha_i \in \mathbb{Z}$ $(1 \leq i \leq m)$. Durch

$$\alpha := M \sum_{i=1}^{m} \alpha_i \omega_i$$

wird also eine ganz algebraische Zahl in $\mathcal{F}$ definiert. Daher gilt für $\mathbf{q} \in \mathbb{P}_{\mathcal{F}}$ mit $\mathbf{q} | p o_{\mathcal{F}}$:

$$|\alpha|_{\mathbf{q}} \quad = \quad |MM^{-1}\alpha|_{\mathbf{q}}$$

$$
\begin{aligned}
&= |M^{-1}|_{\mathbf{q}} |M\alpha|_{\mathbf{q}} \\
&\overset{\mathrm{ggt}(M,p)=1}{=} |M\alpha|_{\mathbf{q}} \\
&\leq 1,
\end{aligned}
$$

womit $[\omega_1, \ldots, \omega_m]_{\mathbb{Z}(p)} \subseteq o_{\mathcal{F}}(p)$ gezeigt wäre. ■

Zum Abschluß dieses Paragraphen kommen wir noch auf die Komposition von Basen p–ganzer Elemente zu sprechen. Wir wollen folgende Situation untersuchen: Wir kennen eine $\mathbb{Z}(p)$–Basis von $o_{\mathcal{F}}(p)$ und wollen nun eine $\mathbb{Z}(p)$–Basis von $o_{\mathcal{E}}(p)$ bestimmen. Wie können wir eine solche Basis komponieren?

Lemma 5.19 *Sei $[\mathcal{F} : \mathbb{Q}] = m$ und $[\mathcal{E} : \mathcal{F}] = n$. Ferner sei $p \in \mathbb{P}$ und $\omega_1, \ldots, \omega_m$ eine $\mathbb{Z}(p)$–Basis von $o_{\mathcal{F}}(p)$. In $o_{\mathcal{F}}$ gelte $po_{\mathcal{F}} = \wp_1^{e_1} \cdot \ldots \cdot \wp_r^{e_r}$. Ist dann $\eta_1, \ldots, \eta_n$ eine $o_{\mathcal{F}}(\wp_i)$–Basis für $o_{\mathcal{E}}(\wp_i)$ $(1 \leq i \leq r)$, so wird durch*

$$\Phi := \{\omega_i \eta_j \mid 1 \leq i \leq m;\ 1 \leq j \leq n\}$$

eine $\mathbb{Z}(p)$–Basis von $o_{\mathcal{E}}(p)$ gegben.

Beweis: Ein $\alpha \in \mathcal{E}$ ist genau dann p–ganz, wenn α $\wp_i$–ganz ist für $1 \leq i \leq r$. Deshalb gilt für $\alpha \in o_{\mathcal{E}}(p)$

$$\alpha = \sum_{i=1}^{n} \alpha_i \eta_i$$

mit gewissen $\alpha_i \in \bigcap_{j=1}^{r} o_{\mathcal{F}}(\wp_j) = o_{\mathcal{F}}(p)$ $(1 \leq i \leq n)$. Jedes der α_i hat nun seinerseits eine (eindeutige) Darstellung $\alpha_i = \sum_{j=1}^{m} a_{i,j}\omega_j$ mit gewissen $a_{i,j} \in \mathbb{Z}(p)$ und damit hat α auch eine Darstellung $\alpha = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j}\omega_j\eta_i$. Somit gilt $o_{\mathcal{E}}(p) \subseteq [\Phi]_{\mathbb{Z}(p)}$.

Daraus folgt die Behauptung, denn es gilt offenbar nach der oben genannten Äquivalenz $[\Phi]_{\mathbb{Z}(p)} \subseteq o_{\mathcal{E}}(p)$. ■

Kapitel 6

Relativerweiterungen

Wir stellen in diesem Kapitel die für diese Arbeit wesentlichen Ergebnisse über Relativerweiterungen algebraischer Zahlkörper vor.
Der Inhalt dieses Kapitels ist im wesentlichen der Vorlesung "Konstruktive Zahlentheorie III" entnommen, die Prof. Pohst im Wintersemester 1991/92 an der Heinrich–Heine–Universität Düsseldorf gelesen hat.
Hauptsächlich interessiert uns im folgenden die Frage der Struktur der ganzen Zahlen im Oberkörper relativ zum Teilkörper. Um diese Frage umfassend beantworten zu können, führen wir zuerst einige wichtige Definitionen und Sätze auf.
Im folgenden sei $\mathcal{F}$ ($\neq \mathbb{Q}$) ein algebraischer Zahlkörper und $\mathcal{E}$ ein algebraischer Zahlkörper oberhalb von $\mathcal{F}$ mit $[\mathcal{E}:\mathcal{F}] = $ n. Ferner sei $o_{\mathcal{F}}$ bzw. $o_{\mathcal{E}}$ der Ring der ganz algebraischen Elemente von $\mathcal{F}$ bzw. von $\mathcal{E}$.

6.1 Die Idealnorm in Relativerweiterungen

Im Rahmen der Einführung (Kapitel 1) haben wir verschiedene Definitionen eingeführt. So haben wir die Spur und die Norm algebraischer Zahlen, die Norm von Idealen aber auch die Diskriminante einer Basis eines algebraischen Zahlkörpers $\mathcal{M}$ definiert. Die Definition der Spur und der Norm sowie der Diskriminante ist schon zu Beginn der Arbeit allgemein für Relativerweiterun-

gen erfolgt. Wir werden nun auch den Begriff der Idealnorm auf Relativerweiterungen verallgemeinern.
Bei dieser Definition handelt es sich um eine natürliche Verallgemeinerung des alten Begriffes. Hierbei muß z.B. der Tatsache, daß $o_{\mathcal{F}}$ i.a. kein Hauptidealring ist Rechnung getragen werden. Es macht daher Sinn folgendes zu definieren:

Definition 6.1 *Sei* $\mathbf{a} = \prod_{i=1}^{n} \mathcal{P}_i^{e_i} \in \mathcal{I}_{\mathcal{E}}$. *Dann definieren wir*

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathbf{a}) := \prod_{i=1}^{n} \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathcal{P}_i)^{e_i},$$

wobei für die Primideale $\mathcal{P} \in I\!P_{\mathcal{E}}$ *mit* $\wp = \mathcal{P} \cap \mathcal{F}$ *die Norm* $\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathcal{P})$ *wie folgt definiert wird:*

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathcal{P}) := \wp^{f(\mathcal{P}/\wp)}.$$

Daß wir mittels dieser Definition den alten Normbegriff verallgemeinert haben, zeigt das folgende Lemma:

Lemma 6.2 *(Eigenschaften der Relativnorm)*

(i) $\forall\, \alpha \in \mathcal{E}\backslash\{0\} \;:\; \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha o_{\mathcal{E}}) = \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha) o_{\mathcal{F}}$.

(ii) $\forall\, \wp \in I\!P_{\mathcal{F}} \;:\; \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\wp o_{\mathcal{E}}) = \wp^{[\mathcal{E}:\mathcal{F}]}$.

(iii) Gilt $\mathcal{F} = \mathbb{Q}$, *so folgt für ein Ideal* $\mathbf{a} \subseteq o_{\mathcal{E}}$

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathbf{a}) = (\mathrm{N}(\mathbf{a})\mathbb{Z}),$$

d.h die Relativnorm von $\mathbf{a} \in o_{\mathcal{E}}$ *ist das Hauptideal in* $\mathbb{Z}$, *das von* $\mathrm{N}_{\mathcal{E}/\mathbb{Q}}(\mathbf{a})$ *(wie in Definition 2.13) erzeugt wird.*

Interessant bei der Untersuchung der Relativnorm ist auch, wie sich der Wertebereich verhält und ob die Relativnorm Teilmengenbeziehungen erhält:

(iv) Ist $\mathbf{a} \in \mathcal{I}_{\mathcal{E}}$ *ein ganzes Ideal, d.h gilt* $\mathbf{a} \subseteq o_{\mathcal{E}}$, *so gilt*

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathbf{a}) \subseteq o_{\mathcal{F}}$$

(v) *Gilt* $\mathbf{a} \subseteq \mathbf{b}$ *für Ideale* $\mathbf{a}, \mathbf{b} \in \mathcal{I}_{\mathcal{E}}$, *so gilt auch*

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathbf{a}) \subseteq \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathbf{b}).$$

Beweis: Die Aussagen (ii),(iv) und (v) sind trivial. Sie sind eine direkte Folgerung aus der Definition und der Dedekind - Eigenschaft von $o_{\mathcal{E}}$ bzw. $o_{\mathcal{F}}$. Bleiben die Aussagen (i) und (iii) zu zeigen.

zu (i): Seien $\wp \in I\!P_{\mathcal{F}}, \mathcal{P} \in I\!P_{\mathcal{E}}$ *mit* $\mathcal{P} \supseteq \wp$ gegeben. Da $\mathcal{E} \subset \mathcal{E}_{\mathcal{P}}$ ist, gilt für $\alpha(\in \mathcal{E}_{\mathcal{P}})$ nach Satz 5.8 (ii)

$$\nu_{\mathcal{P}}(\alpha) n_{\mathcal{P}} = e(\mathcal{P}/\wp)\nu_{\wp}(\mathrm{N}_{\mathcal{E}_{\mathcal{P}}/\mathcal{F}_{\wp}}(\alpha))$$

mit $n_{\mathcal{P}} = e(\mathcal{P}/\wp) f(\mathcal{P}/\wp)(= [\mathcal{E}_{\mathcal{P}} : \mathcal{F}_{\wp}])$. Daher gilt:

$$\begin{aligned}
\sum_{\mathcal{P}\supseteq\wp} f(\mathcal{P}/\wp)\nu_{\mathcal{P}}(\alpha) &= \sum_{\mathcal{P}\supseteq\wp} \nu_{\mathcal{P}}(\mathrm{N}_{\mathcal{E}_{\mathcal{P}}/\mathcal{F}_{\wp}}(\alpha)) \\
&= \nu_{\wp}(\prod_{\mathcal{P}\supseteq\wp} \mathrm{N}_{\mathcal{E}_{\mathcal{P}}/\mathcal{F}_{\wp}}(\alpha)) \\
&= \nu_{\wp}(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha)). \qquad (6\text{-}1)
\end{aligned}$$

Es gilt aber auch

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha o_{\mathcal{E}}) = \prod_{\wp \in I\!P_{\mathcal{F}}} \wp^{\sum_{\mathcal{P}\supseteq\wp} f(\mathcal{P}/\wp)\nu_{\mathcal{P}}(\alpha)}. \qquad (6\text{-}2)$$

Aus 6-1 und 6-2 folgt nun sofort:

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha o_{\mathcal{E}}) = \prod_{\wp \in I\!P_{\mathcal{F}}} \wp^{\nu_{\wp}(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha))} = \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha) o_{\mathcal{F}}.$$

zu (iii): Da die in 6.1 definierte Norm offensichtlich multiplikativ ist, reicht es Aufgrund der Eindeutigkeit einer Primidealzerlegung die Behauptung für Primideale zu beweisen. Der allgemeine Fall ist dann eine direkte Folgerung. Sei also $\mathcal{P} \in I\!P_{\mathcal{E}}$ beliebig gegeben. Dann gilt nach Bemerkung 3.4

$$\mathrm{N}(\mathcal{P}) = p^{f(\mathcal{P}/p)}, \qquad (6\text{-}3)$$

falls $p\mathbb{Z} = \mathcal{P} \cap \mathbb{Z}$. Andererseits gilt nach 6.1:

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathcal{P}) = (p\mathbb{Z})^{f(\mathcal{P}/p)} = (p^{f(\mathcal{P}/p)})\mathbb{Z}. \qquad (6\text{-}4)$$

Damit folgt die Behauptung aus 6-3 und 6-4. ∎

Satz 6.3 *Sind $\mathcal{F} \subseteq \hat{\mathcal{F}} \subseteq \mathcal{E}$ algebraische Zahlkörper, so gilt für die Relativnormen:*

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}} = \mathrm{N}_{\hat{\mathcal{F}}/\mathcal{F}} \circ \mathrm{N}_{\mathcal{E}/\hat{\mathcal{F}}}.$$

Zum Beweis: Siehe z.B. [7].
Zum Abschluß dieser Einführung der Relativnorm stellen wir hier einen Satz vor, der nochmals (neben Lemma 6.2 (i)) verdeutlicht, wie eng die Relativnorm von Elementen algebraischer Zahlkörper mit der Relativnorm von Idealen zusammenhängt. Einen Beweis zu diesem Satz findet man z.B. in [23].

Satz 6.4 *Ist $\mathbf{a} \in \mathcal{I}_{\mathcal{E}}$ und ist $\mathbf{b} \in \mathcal{I}_{\mathcal{F}}$ das kleinste Ideal mit*

$$\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha) \in \mathbf{b} \quad \forall \alpha \in \mathbf{a},$$

so gilt $\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\mathbf{a}) = \mathbf{b}$.

6.2 Differente und Körperdiskriminante

Lemma 6.5 *Die* **Codifferente** *von $\mathcal{E}$ über $\mathcal{F}$ ist definiert als*

$$D^*_{\mathcal{E}/\mathcal{F}} := \{\alpha \in \mathcal{E} \,|\, \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha\beta) \in o_{\mathcal{F}} \;\forall \beta \in o_{\mathcal{E}}\}$$

und ist ein gebrochenes Ideal in $o_{\mathcal{E}}$ mit $D^*_{\mathcal{E}/\mathcal{F}} \supseteq o_{\mathcal{E}}$.

Zum Beweis: vgl. z.B [23] oder [16].
Mit Hilfe der Codifferente definieren wir nun zuerst die Differente $D_{\mathcal{E}/\mathcal{F}}$ des algebraischen Zahlkörpers $\mathcal{E}$ relativ zu $\mathcal{F}$ und dann die Diskriminante $d_{\mathcal{E}/\mathcal{F}}$ von $\mathcal{E}$ relativ zu $\mathcal{F}$.

Definition 6.6 *(i) Wir bezeichnen*

$$D_{\mathcal{E}/\mathcal{F}} := (D^*_{\mathcal{E}/\mathcal{F}})^{-1}$$

als **Differente** *von $\mathcal{E}$ über $\mathcal{F}$.*

(ii) Die **Diskriminante** *von $\mathcal{E}$ über $\mathcal{F}$ setzen wir als*

$$d_{\mathcal{E}/\mathcal{F}} := \mathrm{N}_{\mathcal{E}/\mathcal{F}}(D_{\mathcal{E}/\mathcal{F}})$$

Nun drängt sich die Frage auf, wie die Relativdiskriminante $d_{\mathcal{E}/\mathcal{F}}$ mit der globalen Körperdiskriminante $d_{\mathcal{E}}$ von $\mathcal{E}$ zusammenhängt. Um diese Frage beantworten zu können, müssen wir die Relativdifferenten genauer untersuchen, denn die Relativdiskriminante ist ja über die Relativdifferente definiert.
Einen ersten Anhaltspunkt liefert hierbei der nächste Satz:

Satz 6.7 *Für die Differente $D_{\mathcal{E}/\mathcal{F}}$ gilt die folgende Faktorisierung:*

$$D_{\mathcal{E}/\mathcal{F}} = \prod_{\mathcal{P}\in I\!P_{\mathcal{E}}} \mathcal{P}^{m(\mathcal{P})}$$

wobei $m(\mathcal{P})$ durch die lokale Differente definiert ist:

$$\mathcal{D}_{\mathcal{E}_{\mathcal{P}}/\mathcal{F}_{\wp}} = \sigma^{m(\mathcal{P})}\mathcal{S}_{\mathcal{P}}.$$

(Vergleiche hierzu auch Definition 5.11.)

Wir ziehen nun aus diesem Satz eine wichtige Folgerung, die uns einen Einblick in das Verzweigungsverhalten von Primidealen gibt. Bei dem Beweis werden, wie es die Satzaussage nahelegt, lokale Methoden verwendet.

Korollar 6.8 *Für ein Primideal $\mathcal{P} \in I\!P_{\mathcal{E}}$ mit $\wp = \mathcal{P} \cap o_{\mathcal{F}}$ gilt:*

$$e(\mathcal{P}/\wp) > 1 \Leftrightarrow \nu_{\mathcal{P}}(D_{\mathcal{E}/\mathcal{F}}) \geq 1.$$

Gilt $e(\mathcal{P}/\wp) > 1$ für das Ideal $\mathcal{P}$, so bezeichnet man das Ideal als verzweigt.

Beweis: Der Beweis ist eine einfache Anwendung von Satz 5.13. Mit den Bezeichnungen aus 6.7 gilt:

$$\begin{aligned} m(\mathcal{P}) = 0 \quad &\Leftrightarrow \quad \mathcal{D}_{\mathcal{E}_{\mathcal{P}}/\mathcal{F}_{\wp}} = \mathcal{S}_{\mathcal{P}} \\ &\Leftrightarrow \quad \mathcal{E}_{\mathcal{P}}/\mathcal{F}_{\wp} \text{ unverzweigt} \\ &\Leftrightarrow \quad e(\mathcal{P}/\wp) = 1. \end{aligned}$$

■

Bemerkung 6.9 *Wie man nun sieht gibt es nur endlich viele verzweigte Ideale in $I\!P_{\mathcal{E}}$, denn $D_{\mathcal{E}/\mathcal{F}}$ hat als Ideal in einem Dedekindring natürlich nur endlich viele Primteiler.*

Wir sind an Aussagen über das Zerlegungsverhalten der Primideale aus $o_{\mathcal{F}}$ in $o_{\mathcal{E}}$ interessiert. Korollar 6.8 und die Definition der Relativnorm legen nahe, daß wir einen Zusammenhang zwischen den Teilern von $d_{\mathcal{E}/\mathcal{F}}$ und dem Zerlegungsverhalten der Primideale herstellen können.

Satz 6.10 *Für ein Primideal $\wp \in I\!P_{\mathcal{F}}$ gilt:*

$$\wp \text{ ist verzweigt} \Leftrightarrow \nu_{\wp}(d_{\mathcal{E}/\mathcal{F}}) > 0. \tag{6-5}$$

Speziell gibt es also nur endlich viele verzweigt Primideale in $I\!P_{\mathcal{F}}$, und die Erweiterung $\mathcal{E}/\mathcal{F}$ ist genau dann unverzweigt, wenn $d_{\mathcal{E}/\mathcal{F}} = o_{\mathcal{F}}$ gilt.

Beweis: Der Beweis ist eine Anwendung von Satz 6.7 und Korollar 6.8. Offenbar reicht es die Aussage 6-5 zu zeigen, denn die weiteren Aussagen des Satzes sind eine Folgerung dieser, wenn man die Dedekindeigenschaft von $o_{\mathcal{E}}$ berücksichtigt.
Nach 6.7 und 6.6 gilt:

$$\begin{aligned} & D_{\mathcal{E}/\mathcal{F}} = \textstyle\prod_{\mathcal{P} \in I\!P_{\mathcal{E}}} \mathcal{P}^{m(\mathcal{P})} \\ \Rightarrow \quad & d_{\mathcal{E}/\mathcal{F}} = \textstyle\prod_{\wp \in I\!P_{\mathcal{F}}} \wp^{\sum_{\mathcal{P} \supseteq \wp} f(\mathcal{P}/\wp) m(\mathcal{P})}. \end{aligned}$$

Aus diesen Gleichungen folgt nun:

$$\begin{aligned} \nu_{\wp}(d_{\mathcal{E}/\mathcal{F}}) > 0 \quad & \Leftrightarrow \quad \sum_{\mathcal{P} \supseteq \wp} f(\mathcal{P}/\wp) m(\mathcal{P}) > 0 \\ & \Leftrightarrow \quad \exists \mathcal{P} \supseteq \wp : \ m(\mathcal{P}) > 0 \quad (d.h\ \mathcal{P} \text{ ist verzweigt}) \\ & \Leftrightarrow \quad \wp \text{ ist verzweigt}. \end{aligned}$$

■

Wir haben bisher nur Aussagen über die Struktur der Körperdifferente $D_{\mathcal{E}/\mathcal{F}}$ gesehen. Wir sind aber auch stark an der Struktur der Körperdiskriminante interessiert und man kann auch über sie einige Aussagen machen:

Satz 6.11 *Es gilt*

$$d_{\mathcal{E}/\mathcal{F}} = \langle \{ d(\alpha_1, \ldots, \alpha_n) \mid \alpha_1, \ldots, \alpha_n \in o_{\mathcal{E}} \text{ bilden eine Basis von } \mathcal{E}/\mathcal{F} \} \rangle .$$

Interessant in diesem Zusammenhang ist auch die Verknüpfungsformel für Körperdiskriminanten. Sie beschreibt, wie sich die Körperdiskriminante in einem Körperturm fortsetzt.

Satz 6.12 *Sind $\mathcal{F} \subseteq \hat{\mathcal{F}} \subseteq \mathcal{E}$ algebraische Zahlkörper, so gilt:*

$$d_{\mathcal{E}/\mathcal{F}} = \mathrm{N}_{\hat{\mathcal{F}}/\mathcal{F}}(d_{\mathcal{E}/\hat{\mathcal{F}}}) \cdot d_{\hat{\mathcal{F}}/\mathcal{F}}^{[\mathcal{E}:\hat{\mathcal{F}}]}.$$

Diese letzten beiden Aussagen findet man z.B. in [24].
Es ist uns nun also möglich die Körperdiskriminante von $\mathcal{E}$ mittels der Relativdiskriminante $d_{\mathcal{E}/\mathcal{F}}$ und der Körperdiskriminante $d_{\mathcal{F}}$ von $\mathcal{F}$ zu bestimmen. Es gilt:

$$|d_{\mathcal{E}}| = \mathrm{N}_{\mathcal{F}/\mathbb{Q}}(d_{\mathcal{E}/\mathcal{F}}) \cdot |d_{\mathcal{F}}|^{[\mathcal{E}:\mathcal{F}]} .$$

Man beachte, daß hier die in Kapitel 2 definierte Norm eines Ideals gemeint ist.

6.3 Relative Ganzheitsbasen

Wie in Kapitel 1 gesehen, existiert **immer** eine $\mathbb{Z}$- Ganzheitsbasis für einen gegebenen algebraischen Zahlkörper $\mathcal{F}$, d.h es gibt $\omega_1, \ldots, \omega_m \in o_{\mathcal{F}}$ mit

$$o_{\mathcal{F}} = \sum_{i=1}^{m} \mathbb{Z}\omega_i.$$

Da nun $\mathbb{Z}$ der Ring der ganzen Zahlen von $\mathbb{Q}$ ist, stellt sich die Frage, ob man das Problem der Existenz einer solchen Ganzheitsbasis auch relativ lösen kann. Die Frage lautet also:

> Gibt es algebraische Zahlen $\eta_1, \ldots, \eta_n \in o_{\mathcal{E}}$, so daß diese eine $o_{\mathcal{F}}$ Relativganzheitsbasis von $o_{\mathcal{E}}$ bilden:
>
> $$o_{\mathcal{E}} = \sum_{i=1}^{n} o_{\mathcal{F}}\eta_i$$

Im Allgemeinen muß man diese Frage leider mit nein beantworten, wie das Beispiel von Edgar [8] zeigt:

> Betrachtet man $\mathbb{Q}(\sqrt{5}, \sqrt{10})$ über $\mathbb{Q}(\sqrt{10})$, so existiert keine relative Ganzheitsbasis für diese Körpererweiterung.

Ein anders Beispiel dieser Art wurde z.B. von McKenzie und Scheunemann in [20] gegeben.
Allgemeiner gilt nach Mann ([17, 18]) sogar folgender Satz:

Satz 6.13 *Ist $\mathcal{F}$ ein algebraischer Zahlkörper mit Klassenzahl $h_{\mathcal{F}} \neq 1$, so existiert eine quadratische Erweiterung $\mathcal{E}$ von $\mathcal{F}$, so daß $o_{\mathcal{E}}$ keine relative $o_{\mathcal{F}}$ Ganzheitsbasis besitzt.*

Dieser Satz zeigt schon, in welche Richtung unsere Betrachtungen gehen: Die Klassenzahl ist entscheidend an dem Phänomen der nicht existierenden relativen Ganzheitsbasis beteiligt.
Bevor wir nun weiter auf die Struktur von $o_{\mathcal{E}}$ als $o_{\mathcal{F}}$ - Modul eingehen, wenden wir uns zunächst wieder der Körperdiskriminante zu und stellen einige Ergebnisse über freie $o_{\mathcal{F}}$ - Moduln in $o_{\mathcal{E}}$ vor.
Zuerst interessiert uns, wie sich die Körperdiskriminante zu Diskriminanten von $\mathcal{F}$–Basen von $\mathcal{E}$ verhält. Betrachtet man eine $\mathbb{Q}$ Basis $\omega_1, \ldots, \omega_m$ von $\mathcal{F}$, so gilt ja

$$d(\omega_1, \ldots, \omega_m) = k^2 d_{\mathcal{F}} \quad , mit\ k \in \mathbb{Q}\,.$$

Die Frage ist nun: Gilt ähnliches auch für die relative Körperdiskriminante $d_{\mathcal{E}/\mathcal{F}}$? Der folgende Satz liefert eine Antwort:

Satz 6.14 *Bilden $\alpha_1, \ldots, \alpha_n \in \mathcal{E}$ eine $\mathcal{F}$ - Basis von $\mathcal{E}/\mathcal{F}$, so gilt*

$$d(\alpha_1, \ldots, \alpha_n) o_{\mathcal{F}} = \mathbf{a}^2\, d_{\mathcal{E}/\mathcal{F}}.$$

mit einem gebrochenen Ideal $\mathbf{a} \in \mathcal{I}_{\mathcal{F}}$.

Da wir im weiteren Verlauf der Arbeit für relativquadratische Erweiterungen $\mathcal{E}/\mathcal{F}$ die Struktur von $o_{\mathcal{E}}$ als $o_{\mathcal{F}}$ Modul aufzeigen wollen, ist es von besonderem

Interesse ein notwendiges und hinreichendes Kriterium zu haben, um entscheiden zu können, ob eine $\mathcal{F}$ Basis $\eta_1, \ldots, \eta_n$ von $\mathcal{E}$ eine relative Ganzheitsbasis ist. Ein solches Kriterium liefert der nächste Satz:

Satz 6.15 *Eine $\mathcal{F}$-Basis $\eta_1, \ldots, \eta_n \in o_{\mathcal{E}}$ von $\mathcal{E}/\mathcal{F}$ ist genau dann eine Relativganzheitsbasis, wenn*

$$d(\eta_1, \ldots, \eta_n) o_{\mathcal{F}} = d_{\mathcal{E}/\mathcal{F}}.$$

gilt.

Wenden wir uns nun wieder dem Problem der Beschreibung von $o_{\mathcal{E}}$ als $o_{\mathcal{F}}$-Modul zu. Wie wir gesehen haben ist $o_{\mathcal{E}}$ nicht immer ein freier $o_{\mathcal{F}}$-Modul. Wenn aber $o_{\mathcal{E}}$ nicht frei ist, ist dann $o_{\mathcal{E}}$ wenigstens ein endlich erzeugter $o_{\mathcal{F}}$–Modul? Und wenn ja wieviele Erzeuger $\lambda_1, \ldots, \lambda_r$ benötigt man mimimal um die Gleichung

$$o_{\mathcal{E}} = \sum_{i=1}^{r} o_{\mathcal{F}} \lambda_i \tag{6-6}$$

zu erfüllen? Es gilt hierfür der folgende Satz (vgl. [23]):

Satz 6.16 *Für den Ring der ganzen Zahlen $o_{\mathcal{E}}$ als $o_{\mathcal{F}}$–Modul gilt:*

$$o_{\mathcal{E}} \cong_{o_{\mathcal{F}}} o_{\mathcal{F}}^{n-1} \oplus \mathbf{a},$$

wobei $\mathbf{a} \in \mathcal{I}_{\mathcal{F}}$ (vgl. Definition 2.16) ist. Die Klasse in $Cl_{\mathcal{F}}$ zu der das Ideal $\mathbf{a}$ *gehört bezeichnet man als die* **Steinitz–Klasse** *$\mathcal{C}_{\mathcal{F}}(\mathcal{E})$ von $\mathcal{E}/\mathcal{F}$.*

Aus diesem Satz ergeben sich sofort eine Reihe von Folgerungen:

Korollar 6.17 *Um eine Darstellung von $o_{\mathcal{E}}$ wie in 6-6 zu erhalten reichen immer $n+1 = [\mathcal{E}:\mathcal{F}]+1$ Erzeuger $\lambda_1, \ldots, \lambda_{n+1}$ aus.*

Beweis: Ein Ideal $\mathbf{a} \in \mathcal{I}_{\mathcal{F}}$ hat nach 2.12 eine Darstellung der Form:

$$\mathbf{a} = \alpha_1 o_{\mathcal{F}} + \alpha_2 o_{\mathcal{F}}.$$

Daraus folgt die Behauptung mit Satz 6.16. ■

Korollar 6.18 *Hat der algebraische Zahlkörper $\mathcal{F}$ die Klassenzahl 1, so existiert für jede Relativerweiterung eine Relativganzheitsbasis.*

Beweis: Gilt $h_{\mathcal{F}} = 1$, so ergibt sich für das Ideal $\mathbf{a}$ aus 6.16

$$\mathbf{a} = \alpha o_{\mathcal{F}}$$

für ein passendes $\alpha \in o_{\mathcal{F}}$. Daraus folgt dann ebenfalls aus 6.16 die folgende $o_{\mathcal{F}}$–Isomorphiekette:

$$o_{\mathcal{E}} \cong o_{\mathcal{F}}^{n-1} \oplus \mathbf{a} \cong o_{\mathcal{F}}^{n-1} \oplus \alpha o_{\mathcal{F}} \cong o_{\mathcal{F}}^{n}$$

■

Bevor wir uns nun der Untersuchung relativquadratischer Erweiterungen zuwenden, stellen wir zwei Ergebnisse vor, die uns über den Fall $h_{\mathcal{F}} = 1$ hinaus sagen, wann relative Ganzheitsbasen existieren.
Der folgende Satz geht auf eine Arbeit von A. Fröhlich [11] zurück und beschreibt den Fall $h_{\mathcal{F}}$ ungerade.

Satz 6.19 *Ist die Klassenzahl von $\mathcal{F}$ ungerade, so existiert für die Erweiterung $\mathcal{E}/\mathcal{F}$ genau dann eine Relativganzheitsbasis, wenn die Relativdiskriminante $d_{\mathcal{E}/\mathcal{F}}$ von $\mathcal{E}/\mathcal{F}$ ein Hauptideal ist.*

Bemerkung 6.20 *Der Satz 6.19 ist für den Fall $h_{\mathcal{F}} \in 2\mathbb{N}$ falsch, wie ein Beispiel von S.Pierce [25] zeigt.*

Der letzte Satz ist eine Aussage von E. Artin [2]. Auf ihn werden wir später noch genauer eingehen.

Satz 6.21 *Sei $\mathcal{E} = \mathcal{F}(\rho)$ für ein $\rho \in o_{\mathcal{E}}$. Dann gilt:*
Für $\mathcal{E}/\mathcal{F}$ existiert genau dann eine Relativganzheitsbasis, wenn das Ideal

$$\mathcal{I}_{\mathcal{F}} \ni \mathbf{a} := d(\rho)^{-1} d_{\mathcal{E}/\mathcal{F}}$$

das Quadrat (vgl. 6.14) eines Hauptideals ist.

Kapitel 7

Quadratische Erweiterungen

Die Betrachtung quadratischer Erweiterungen eines algebraischen Zahlkörpers $\mathcal{F}(\neq \mathbb{Q})$ gliedert sich in zwei große Bereiche, die wir jeweils einzeln betrachten wollen:

- Der Zahlkörper $\mathcal{F}$ hat Klassenzahl $h_{\mathcal{F}} = 1$
- Der Zahlkörper $\mathcal{F}$ hat Klassenzahl $h_{\mathcal{F}} \neq 1$

Da im ersten Fall die Existenz einer relativen Ganzheitsbasis sichergestellt ist, ist dieser Fall natürlich bei weitem einfacher. Wir werden ihn zuerst betrachten und dabei die grundlegenden Techniken für den allgemeinen Fall, d.h. für den Fall $h_{\mathcal{F}} \neq 1$ einführen.
Im folgenden sei $\mathcal{F}$ ein algebraischer Zahlkörper mit $[\mathcal{F} : \mathbb{Q}] = m$ und $\mathcal{E}$ sei ein weiterer algebraischer Zahlkörper mit

$$\begin{array}{ll} \text{(i)} & \mathcal{E} = \mathcal{F}(\sqrt{\mu}) \\ \text{(ii)} & [\mathcal{E} : \mathcal{F}] = 2 \end{array}$$

für eine $\mu \in o_{\mathcal{F}}$.

7.1 Die Diskriminante relativquadratischer Erweiterungen

Wir stellen in diesem Paragraphen die Ergebnisse von Hilbert [13] vor, wie man sie in Hasse [14] oder Pohst [26], aber auch in Sommer [32] (hier allerdings nur für den Fall $[\mathcal{F} : \mathbb{Q}] = 2$) vorfindet.

Lemma 7.1 *Für die Polynomdiskriminante $d(\mu)$ von $\mathcal{E}/\mathcal{F}$ gilt:*

$$d(\mu) = 4\mu.$$

Desweiteren gilt $d_{\mathcal{E}/\mathcal{F}} \mid (4\mu)$.

Beweis: Die erste Aussage des Lemmas folgt aus

$$d(\mu) = det \begin{pmatrix} 2 & 0 \\ 0 & 2\mu \end{pmatrix} = 4\mu,$$

da $Tr(1) = 2$, $Tr(\sqrt{\mu}) = 0$, sowie $Tr(\mu) = 2\mu$ gilt. Die zweite Aussage ist eine triviale Folgerung aus Satz 6.11. ■

Man erkennt nun sofort, daß für die Untersuchung der Relativdiskriminante nur die Primideale in $o_{\mathcal{F}}$, die $4\mu o_{\mathcal{F}}$ teilen, betrachtet werden müssen. Hierbei unterscheiden wir nun 2 Fälle für ein Primideal $\wp \in I\!P_{\mathcal{F}}$:

- $\wp$ teilt $\mu o_{\mathcal{F}}$ und nicht $2o_{\mathcal{F}}$
- $\wp$ teilt $2o_{\mathcal{F}}$

Im weiteren Verlauf der Arbeit werden wir folgende Rede– und Schreibweise verwenden: Statt "$\wp$ teilt $2o_{\mathcal{F}}$" schreiben wir nur $\wp$ teilt 2. Wollen wir genauer darauf hinweisen, daß es sich um ein Ideal handelt, so schreiben wir $(2)[= 2o_{\mathcal{F}}]$. Für den Fall $\wp$ teilt $\mu o_{\mathcal{F}}$ und $\wp$ teilt nicht $2o_{\mathcal{F}}$ gilt nun:

Satz 7.2 *Sei $\wp \in I\!P_{\mathcal{F}}$ gegeben mit $\wp^a \| \mu$ (d.h $\wp^a | \mu$ und $\wp^{a+1} \nmid \mu$) und $\wp \nmid 2$. Dann gilt mit $a \equiv b \bmod 2$ und $b \in \{0, 1\}$:*

$$\wp^b \| d_{\mathcal{E}/\mathcal{F}}.$$

Zum Beweis: Siehe [13].
Für den zweiten Fall $\wp|2$ kann nun die folgende Aussage formuliert werden, die ebenfalls in [13] nachzulesen ist:

Satz 7.3 *Sei $\wp \in I\!P_{\mathcal{F}}$ gegeben mit $\wp^a \| \mu$ und $\wp^e \| 2$. Dann gilt*

$$\wp | d_{\mathcal{E}/\mathcal{F}} \Leftrightarrow \forall \gamma \in o_{\mathcal{F}} \ : \ \gamma^2 \not\equiv \mu \ mod \ \wp^{2e+a}.$$

Da wir die Relativdiskriminante im weiteren in ihrer Primidealzerlegung benötigen, reicht uns die Aussage dieses Satzes nicht.
Hier hilft uns eine Aussage aus [14], die auch in [26] zu finden ist, weiter:

Satz 7.4 *Sei $\wp \in I\!P_{\mathcal{F}}$ gegeben mit $\wp^a \| \mu$ und $\wp^e \| 2$ und das Ideal $\wp$ teile die Diskriminante.*

(i) Gilt $a = 0$, so gilt mit

$$v := 2e - max\{0 \leq u \leq 2e-1 |\ \exists \gamma \in o_{\mathcal{F}} \ : \ \gamma^2 \equiv \mu \ mod \ \wp^u\} =: 2e - u :$$

$$\wp^{v+1} \| d_{\mathcal{E}/\mathcal{F}}.$$

Hierbei gilt insbesondere $u \equiv 1 \ mod \ 2$.

(ii) Gilt $a = 1$, so folgt

$$\wp^{2e+1} \| d_{\mathcal{E}/\mathcal{F}}.$$

Wir können nun also für Körper $\mathcal{E} = \mathcal{F}(\sqrt{\mu})$ die Köperdiskriminante berechnen, wenn

$$\wp \in I\!P_{\mathcal{F}} \ mit \ \wp|2 \Rightarrow \wp \| \mu \ \vee \ \wp \not| \mu \tag{7-1}$$

gilt. Dies ist auf den ersten Blick eine starke Einschränkung an die Wahl des Körpers $\mathcal{E}$. Wie das folgende Lemma jedoch zeigt, existiert für jeden Körper $\mathcal{E}$ ein $\mu \in o_{\mathcal{F}}$, das die Bedingung 7-1 erfüllt.

Lemma 7.5 *Sei $\Pi \subset I\!P_{\mathcal{F}}$ mit $|\Pi| < \infty$ beliebig gegeben. Dann existiert ein $\mu^* \in o_{\mathcal{F}}$ mit*

$$\mathcal{F}(\sqrt{\mu^*}) = \mathcal{F}(\sqrt{\mu}) \ (= \mathcal{E}) \tag{7-2}$$

und

$$\forall \wp \in \Pi \ : \quad \wp \| \mu^* \ \vee \ \wp \not| \mu^*. \tag{7-3}$$

Beweis: Der Beweis ist eine mehrfache Anwendung des chinesischen Restsatzes.
Wähle für jedes $\wp \in \Pi$ ein $\pi_\wp \in o_\mathcal{F}$ mit:

(i) $\pi_\wp \in \wp \backslash \wp^2$,

(ii) $\pi_\wp \notin \mathbf{q} \quad \forall \mathbf{q} \in \Pi \setminus \{\wp\}$.

Diese $\pi_\wp$ existieren gemäß dem chinesischen Restsatz. Sei nun

$$\tilde{\Pi} := \{\wp \in \Pi | \nu_\wp(\mu) > 0\}.$$

Für die ganz algebraischen Zahlen $\pi_\wp$ gelte die Primidealzerlegung

$$(\pi_\wp) = \wp \cdot \mathbf{a}_\wp.$$

Hierbei ist das Ideal $\mathbf{a}_\wp$ nach Definition von $\pi_\wp$ prim zu dem Ideal $\mathbf{b} := \prod_{\wp \in \Pi} \wp$.
Nach dem chinesischen Restsatz existiert für $\wp \in \tilde{\Pi}$ ein $\delta_\wp \in o_\mathcal{F}$ mit:

(i) $\delta_\wp \in \mathbf{a}_\wp$

(ii) $\delta_\wp \notin \mathbf{b}$

Setzt man nun für $\wp \in \tilde{\Pi}$

$$a_\wp := \begin{cases} \nu_\wp(\mu) & ; \nu_\wp(\mu) \textit{ gerade} \\ \nu_\wp(\mu) - 1 & ; \textit{sonst} \end{cases} , \tag{7-4}$$

so wird durch

$$\mu^* := \mu \cdot \prod_{\wp \in \tilde{\Pi}} \left(\frac{\delta_\wp}{\pi_\wp} \right)^{a_\wp}$$

aufgrund der Wahl von $\delta_\wp$ eine ganz algebraische Zahl in $\mathcal{F}$ definiert.
Für passende $\alpha_1, \alpha_2 \in o_\mathcal{F}$ gilt

$$\mu^* = \mu \left(\frac{\alpha_1}{\alpha_2} \right)^2, \tag{7-5}$$

da $a_\wp$ gerade ist für alle $\wp \in \tilde{\Pi}$. Desweiteren gilt nach 7-4 für alle $\wp \in \Pi$ die Ungleichung:

$$\begin{aligned} \nu_\wp(\mu^*) &= \nu_\wp(\mu \cdot \prod_{\wp \in \tilde{\Pi}} \left(\frac{\delta_\wp}{\pi_\wp}\right)^{a_\wp}) \\ &= \nu_\wp(\mu) + a_\wp \cdot \nu_\wp(\delta_\wp) - a_\wp \cdot \nu_\wp(\pi_\wp) \\ &= \nu_\wp(\mu) - a_\wp \\ &\leq \nu_\wp(\mu) - (\nu_\wp(\mu) - 1) \\ &= 1. \end{aligned} \tag{7-6}$$

Aus 7-5 folgt nun 7-2 und aus 7-6 folgt 7-3. ■

Bemerkung 7.6 *(i) Durch das, wie im Beweis des Lemmas beschriebene, Vorgehen begrenzt man zwar die Exponenten $\nu_\wp(\mu)$ auf einer endlichen Primidealmenge, doch die Exponenten der anderen Primideale werden i.a. größer.*

(ii) Setzt man $\Pi = \{\wp \in I\!P_{\mathcal{F}} | \quad \wp | 2\}$, so erhält man durch das Lemma eine algebraische Zahl μ^*, die die Bedingung 7-1 erfüllt und auch $\mathcal{E}$ erzeugt.

Im weiteren sei also der Erzeuger μ von $\mathcal{E}/\mathcal{F}$ o.B.d.A. so gewählt, daß er die Bedingung 7-1 erfüllt.
Wir können nun also für beliebige algebraische Zahlkörper $\mathcal{E}/\mathcal{F}$ mit $\mathcal{E} = \mathcal{F}(\sqrt{\mu})$ die Körperdiskriminante $d_{\mathcal{E}/\mathcal{F}}$ theoretisch berechnen.

7.2 Einige Lemmata

Als Vorbereitung auf die letzten beiden Paragraphen formulieren wir nun zwei wichtige Lemmata, die wir mehrfach anwenden werden.

Lemma 7.7 *Seien $\mathbf{a}_1, \ldots, \mathbf{a}_n$ comaximale Ideale in $o_{\mathcal{F}}$ und seien $\alpha, \alpha_1, \ldots, \alpha_n$ gegeben mit*

$$\alpha \equiv \alpha_i^2 \; mod \; \mathbf{a}_i \qquad ; 1 \leq i \leq n.$$

Dann existiert ein $\beta \in o_{\mathcal{F}}$ mit

$$\alpha \equiv \beta^2 \ mod \ \prod_{i=1}^{n} \mathbf{a}_i.$$

Beweis: Da die Ideale $\mathbf{a}_1, \ldots, \mathbf{a}_n$ comaximal sind, existieren

$$e_{i,j} \in \mathbf{a}_i \quad e_{j,i} \in \mathbf{a}_j \qquad ; 1 \leq i, j \leq n \ , \ i \neq j$$

mit

$$e_{i,j} + e_{j,i} = 1 \qquad ; 1 \leq i, j \leq n \ , \ i \neq j.$$

Definiert man nun

$$\tilde{e}_i := \prod_{\substack{j=1 \\ j \neq i}}^{n} e_{j,i} \quad (1 \leq i \leq n) \quad und \quad \beta := \sum_{i=1}^{n} \tilde{e}_i \alpha_i,$$

so gelten

(i) $\tilde{e}_i \equiv 1 \ mod \ \mathbf{a}_i \ \wedge \ \tilde{e}_i \equiv 0 \ mod \ \mathbf{a}_j \ (1 \leq i, j \leq n \ , \ i \neq j)$,

(ii) $\beta^2 \equiv \alpha_i^2 \ mod \ \mathbf{a}_i \quad (1 \leq i \leq n)$.

zu (i): Es gilt $\tilde{e}_i \equiv 1 \ mod \ \mathbf{a}_i$, denn

$$\begin{aligned} \tilde{e}_i - 1 &= \prod_{\substack{j=1 \\ j \neq i}}^{n} e_{j,i} - \prod_{\substack{j=1 \\ j \neq i}}^{n} (e_{i,j} + e_{j,i}) \\ &= \prod_{\substack{j=1 \\ j \neq i}}^{n} e_{j,i} - \prod_{\substack{j=1 \\ j \neq i}}^{n} e_{j,i} - \sum_{\substack{j=1 \\ j \neq i}}^{n} (e_{i,j} a_j) \quad ; a_j \in o_{\mathcal{F}} \ passend \\ &= \sum_{\substack{j=1 \\ j \neq i}}^{n} (e_{i,j} a_j) \in \mathbf{a}_i \qquad ; da \ e_{i,j} \in \mathbf{a}_i \ \ (j \neq i) \end{aligned}$$

Daraus folgt $\tilde{e}_i \equiv 1 \ mod \ \mathbf{a}_i$ und es gilt $\tilde{e}_i^2 \equiv 1 \ mod \ \mathbf{a}_i \ (1 \leq i, j \leq n \ , \ i \neq j)$.
Offenbar gilt nun nach Definition $\tilde{e}_i \in \mathbf{a}_j \ (1 \leq i, j \leq n \ , \ i \neq j)$.
zu (ii): Es gilt $\beta^2 = \sum_{i=1}^{n} \sum_{j=1}^{n} \tilde{e}_i \tilde{e}_j \alpha_i \alpha_j$ und da für $1 \leq i, j \leq n$ mit $j \neq i$

$$\begin{aligned} \tilde{e}_i \tilde{e}_j &\in \mathbf{a}_k \quad (1 \leq k \leq n) \\ \tilde{e}_i^2 &\in \mathbf{a}_k \quad (k \neq i) \end{aligned}$$

gilt, folgt aus (i)

$$\beta^2 \equiv \sum_{i=1}^{n}\sum_{j=1}^{n} \tilde{e}_i\tilde{e}_j\alpha_i\alpha_j \equiv \tilde{e}_i^2\alpha_i^2 \equiv \alpha_i^2 \; mod \; \mathbf{a}_i \quad (1 \le i \le n).$$

Daraus folgt $\alpha \equiv \beta^2 \; mod \; \mathbf{a}_i \quad (1 \le i \le n)$ und somit die Behauptung. ■

Lemma 7.8 *Für ein $\alpha \in \mathcal{E}$ gilt*

$$\alpha \in o_{\mathcal{E}} \Leftrightarrow \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha) \in o_{\mathcal{F}} \quad \wedge \quad \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha) \in o_{\mathcal{F}}.$$

Beweis: Sei $\alpha = \alpha_1 + \alpha_2\sqrt{\mu} \in \mathcal{E}$ beliebig gegeben.
"$\Rightarrow$" Klar nach Kapitel 1.
"$\Leftarrow$" Gilt $\alpha_2 = 0$, so folgt aus $\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha) = \alpha^2 \in o_{\mathcal{F}}$ sofort $\alpha \in o_{\mathcal{E}}$.
Ist aber $\alpha_2 \neq 0$, so gilt für das Minimalpolynom von α

$$m_\alpha(t) = t^2 - \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\alpha)t + \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\alpha) \in o_{\mathcal{F}}[t],$$

woraus die Behauptung folgt. ■

7.3 Klassenzahl 1

Gilt $h_{\mathcal{F}} = 1$, so ist die Überlegung aus Lemma 7.5 natürlich überflüssig, denn μ hat nicht nur eine eindeutige Zerlegung in Primideale, sondern auch eine (modulo Einheiten) eindeutige Zerlegung in Primelemente, da $o_{\mathcal{F}}$ ein Hauptidealring ist.
Für den Verlauf dieses Paragraphen treffen wir nun einige Vereinbarungen:
Es seien

$$(2) = \prod_{i=1}^{r} (\pi_i)^{e_i} \tag{7-7}$$

$$(\mu) = \prod_{i=1}^{r} (\pi_i)^{a_i} \cdot \mathbf{a} \tag{7-8}$$

Hierbei seien die π_i Primelemente in $o_{\mathcal{F}}$ $(1 \le i \le r)$ und o.B.d.A gelte für die a_i zum einen $a_i = 1$ für $i \in \{1, \ldots, k\}$ und $a_i = 0$ sonst. Ferner sei das Ideal $\mathbf{a}$

teilerfremd zu (π_i) $(1 \leq i \leq r)$ und enthalte nur Primteiler erster Ordnung. Gemäß Satz 7.2 gilt dann $\mathbf{a}|d_{\mathcal{E}/\mathcal{F}}$. Um die Primteiler der Diskriminante zu erhalten, die über $2o_{\mathcal{F}}$ liegen, wenden wir nun Satz 7.3 und Satz 7.4 an.
Als Ergebnis dieser Anwendung erhalte man:

$$d_{\mathcal{E}/\mathcal{F}} = \prod_{i=1}^{r} \pi_i^{\delta_i} \cdot \mathbf{a} \tag{7-9}$$

Hierbei sind die Exponenten δ_i gemäß den Sätzen 7.3 und 7.4 eindeutig bestimmt.
Wie gesehen existiert ein Ideal $(\Phi) \subseteq o_{\mathcal{F}}$ (man beachte, daß die Klassenzahl 1 ist) mit

$$(4\mu) = (\Phi)^2 \cdot d_{\mathcal{E}/\mathcal{F}}. \tag{7-10}$$

Wir bezeichnen im weiteren Φ als den Index von $o_{\mathcal{F}}[\sqrt{\mu}]$ in $o_{\mathcal{E}}$. Aufgrund vom 7-8 enthält (Φ) nur solche Primteiler, die über $2o_{\mathcal{F}}$ liegen.
Kommen wir nun zum Abschluß dieses Paragraphen, indem wir nun die relative Ganzheitsbasis (welche ja existiert) von $\mathcal{E}/\mathcal{F}$ beschreiben.

Lemma 7.9 *In $o_{\mathcal{F}}$ existiert ein ν mit:*

$$\nu^2 \equiv \mu \; mod \; (\Phi)^2.$$

Beweis: Wie bemerkt enthält (Φ) nur solche Primteiler, die über $2o_{\mathcal{F}}$ liegen. Wegen der Gleichung 7-10 und aufgrund der Bedinnung an die Exponenten a_i erhält man $\Phi|(2)$. Wir können sogar noch mehr sagen: Nach Satz 7.4 (ii) enthält (Φ) nur solche Primteiler, die nicht μ teilen.
Sei nun $\wp \in I\!P_{\mathcal{F}}$ ein Primteiler des Index mit $\wp^e \| (2)$ und $\wp^v \| (\Phi)^2$. Dann unterscheiden wir zwei Fälle:

(i) $\wp \not| d_{\mathcal{E}/\mathcal{F}}$
Da $\wp$ nicht die Diskriminante teilt, gilt zum einen $v = 2e$ und zum anderen gilt nach Satz 7.3:

$$\exists \gamma_\wp \in o_{\mathcal{F}} \; : \; \gamma_\wp^2 \equiv \mu \; mod \; \wp^{2e}$$

(ii) $\wp | d_{\mathcal{E}/\mathcal{F}}$
Nach Satz 7.4 (i) gilt:

$$v = max\{0 \leq u \leq 2e-1 | \exists \gamma \in o_{\mathcal{F}} \ : \ \gamma^2 \equiv \mu \ mod \ \wp^u\} - 1.$$

In beiden Fällen gilt also

$$\exists \gamma_\wp \in o_{\mathcal{F}} \ : \ \gamma_\wp^2 \equiv \mu \ mod \ \wp^v. \tag{7-11}$$

Nach 7-11 existiert also für jede Primteilerpotenz des Index ein quadratischer Rest für μ. Nach Lemma 7.7 gilt daher

$$\exists \nu \in o_{\mathcal{F}} \ : \ \nu^2 \equiv \mu \ mod \ (\Phi)^2,$$

was den Beweis beendet. ■

Satz 7.10 *Definiert man mit ν und Φ wie oben*

$$\begin{aligned} \omega_1 &:= 1, \\ \omega_2 &:= \tfrac{\nu+\sqrt{\mu}}{\Phi}, \end{aligned}$$

so wird durch ω_1, ω_2 eine $o_{\mathcal{F}}$-Basis von $o_{\mathcal{E}}$ gegeben.

Beweis: Wir führen den Beweis in zwei Schritten. Im ersten Schritt zeigen wir, daß ω_1 und ω_2 ganz algebraische Zahlen sind. Danach zeigen wir, daß diese Zahlen eine $o_{\mathcal{F}}$-Basis von $o_{\mathcal{E}}$ bilden.
(i) Wir wenden Lemma 7.8 an und zeigen $\omega_2 \in o_{\mathcal{E}}$.
Um $Tr(\omega_2)$ und $N(\omega_2)$ zu bestimmen, berechnen wir die Darstellungsmatrix von ω_2:

$$\omega_2 \cdot (1, \sqrt{\mu}) = (1, \sqrt{\mu}) \begin{pmatrix} \frac{\nu}{\Phi} & \frac{\mu}{\Phi} \\ \frac{1}{\Phi} & \frac{\nu}{\Phi} \end{pmatrix} =: (1, \sqrt{\mu}) \cdot M_{\omega_2}.$$

Daraus ergibt sich nun für $Tr(\omega_2)$ und $N(\omega_2)$:

$$\begin{aligned} Tr(\omega_2) &= Tr(M_{\omega_2}) = \tfrac{2\nu}{\Phi}, \\ N(\omega_2) &= Det(M_{\omega_2}) = \tfrac{\nu^2-\mu}{\Phi^2}. \end{aligned}$$

Wie im Beweis von Lemma 7.9 bemerkt, ist (Φ) ein Teiler von (2). Daher ist $Tr(\omega_2)$ ganz algebraisch in $\mathcal{F}$. Bleibt noch $N(\omega_2)$ zu untersuchen. Es gilt aber $\nu^2 \equiv \mu \; mod \; (\Phi)^2$, woraus $N(\omega_2) \in o_{\mathcal{F}}$ folgt.
(ii) ω_1, ω_2 bilden eine $o_{\mathcal{F}}$-Basis von $o_{\mathcal{E}}$.
Um dies zu beweisen, wenden wir Satz 6.15 an. Bestimmen wir also zuerst die Diskriminante von ω_1, ω_2. Dazu benötigen wir verschiedene Spuren, die wir hier nur angeben, da ihre Berechnung trivial ist:

$$\begin{aligned} &Tr(\omega_1) = 2, \\ &Tr(\omega_2) = \tfrac{2\nu}{\Phi}, \\ &Tr(\omega_2^2) = \tfrac{2(\nu^2+\mu)}{\Phi^2}. \end{aligned}$$

Daraus ergibt sich für $d(\omega_1, \omega_2)$:

$$d(\omega_1, \omega_2) = det \begin{pmatrix} Tr(\omega_1) & Tr(\omega_2) \\ Tr(\omega_2) & Tr(\omega_2^2) \end{pmatrix} = 4\frac{\nu^2+\mu}{\Phi^2} - 4\frac{\nu^2}{\Phi^2} = \frac{4\mu}{\Phi^2}.$$

Aus 7-10 folgt nun die Behauptung mit Satz 6.15. ■

Bemerkung 7.11 *Ist $\eta_1, \ldots, \eta_m$ eine $\mathbb{Z}$ -Ganzheitsbasis von $o_{\mathcal{F}}$, so wird durch*

$$\eta_1\omega_1, \ldots, \eta_m\omega_1, \eta_1\omega_2, \ldots, \eta_m\omega_2$$

eine $\mathbb{Z}$-Ganzheitsbasis von $o_{\mathcal{E}}$ gegeben.

Der Beweis ist offensichtlich, da $\eta_1, \ldots, \eta_m$ eine $\mathbb{Z}$-Basis von $o_{\mathcal{F}}$ ist und ω_1, ω_2 eine $o_{\mathcal{F}}$-Basis von $o_{\mathcal{E}}$ ist.
Als Anwendung dieses Satzes können wir nun ein kurzes Beispiel angeben.

Beispiel 7.12 *Sei $\mathcal{F} = \mathbb{Q}(\sqrt{6}) =: \mathbb{Q}(\rho)$. Dann hat $\mathcal{F}$ die Klassenzahl $h_{\mathcal{F}} = 1$ und $1, \sqrt{6}$ ist eine $\mathbb{Z}$-Ganzheitsbasis von $\mathcal{F}$.*
Betrachten wir nun die Erweiterung $\mathcal{E} = \mathcal{F}(\sqrt{5})$. Unser erster Schritt ist die Zerlegung von 2 und 5 in Primideale in $o_{\mathcal{F}}$. Es gilt:

$$\begin{aligned} (2) &= (2o_{\mathcal{F}} + \rho o_{\mathcal{F}})^2, \\ (5) &= (5o_{\mathcal{F}} + (4+\rho)o_{\mathcal{F}}) \cdot (5o_{\mathcal{F}} + (1+\rho)o_{\mathcal{F}}). \end{aligned}$$

Diese Zerlegung erhält man mittels 3.8 und 3.9. Beide Ideale über der 5 *teilen nach Satz 7.2 die Diskriminante genau. Zu untersuchen bleibt also noch das Ideal* $\mathbf{a} := (2o_{\mathcal{F}} + \rho o_{\mathcal{F}})$.
Aus $(1+2\rho)^2 = 25 + 4\rho$ *folgt:*

$$(1+2\rho)^2 \equiv 5 \; mod \; 4o_{\mathcal{F}}.$$

Daher teilt $\mathbf{a}$ *nach Satz 7.3 nicht die Diskriminante. Es gilt also:*

$$d_{\mathcal{E}/\mathcal{F}} = (5o_{\mathcal{F}} + (4+\rho)o_{\mathcal{F}}) \cdot (5o_{\mathcal{F}} + (1+\rho)o_{\mathcal{F}}) = (5) \tag{7-12}$$
$$\Phi = (2o_{\mathcal{F}} + \rho o_{\mathcal{F}})^2 = (2) \tag{7-13}$$

Es folgt mit Satz 7.10 aus 7-12 und 7-13

$$\begin{aligned} \omega_1 &:= 1 \\ \omega_2 &:= \frac{(1+2\rho)-\sqrt{5}}{2}, \end{aligned}$$

da wie oben gesehen $(1+2\rho)^2 \equiv 5 \; mod \; 4o_{\mathcal{F}}$ *gilt.*
Wir können nun sogar noch die Absolutdiskriminante von $\mathcal{E}$ *nach Satz 6.12 bestimmen und eine* $\mathbb{Z}$*–Ganzheitsbasis von* $o_{\mathcal{E}}$ *angeben:*

$$\begin{aligned} |d_{\mathcal{E}}| &= \mathrm{N}_{\mathcal{E}/\mathcal{F}}(d_{\mathcal{E}/\mathcal{F}}) \cdot d_{\mathcal{F}}^2 = 5^2 \cdot 24^2 = 14400 \\ o_{\mathcal{E}} &= [1, \sqrt{6}, \frac{1+2\sqrt{6}-\sqrt{5}}{2}, \frac{12+\sqrt{6}-\sqrt{6}\sqrt{5}}{2}]_{\mathbb{Z}}. \end{aligned}$$

7.4 Klassenzahl ungleich 1

Die Untersuchung des Falles “$\mathcal{F}$ hat Klassenzahl $\neq 1$” ist deshalb um so viel komplizierter, da wir nicht mehr jedem Primideal ein eindeutiges Primelement zuordnen können. Unser Erzeuger μ kann also in der Primidealzerlegung quadratische Teiler haben, ohne daß ein Primelement $\pi \in o_{\mathcal{F}}$ existiert mit $\pi^2|\mu$. Wir fordern deshalb für diesen Paragraphen für den Erzeuger μ von $\mathcal{E}$:

$$\forall \alpha \in o_{\mathcal{F}} \ : \ \ \alpha^2 \neq \mu.$$

Man beachte noch kurz, daß die Primideale über $2o_{\mathcal{F}}$ das Ideal $\mu o_{\mathcal{F}}$ maximal in erster Potenz teilen sollen, kurz μ erfüllt die Bedingung 7-1. Ähnlich wie im letzten Paragraphen sei $\Phi \in \mathcal{I}_{\mathcal{F}}$ das ganze Ideal mit

$$(4\mu) = \Phi^2 \cdot d_{\mathcal{E}/\mathcal{F}}.$$

Aufgrund der fehlenden Beschränkung an die Exponenten in der Primidealzerlegung von μ gilt i.a. $ggt((\mu), \Phi) \neq o_{\mathcal{F}}$, wir setzen deshalb:

$$\begin{aligned} &\Phi_2 := ggt((2), \Phi) \\ &\Phi_\mu := \Phi \cdot \Phi_2^{-1}. \end{aligned}$$

Es gilt dann:

$$\Phi = \Phi_2 \cdot \Phi_\mu. \tag{7-14}$$

Hierbei sind die Ideale Φ_2 und Φ_μ comaximal. Dies ergibt sich aus Teilbarkeitsgründen aus der Definition von Φ und aus der Bedingung 7-1.
Insbesondere wollen wir festhalten, daß

$$\Phi_2 \mid 2 \quad \wedge \quad \Phi_\mu^2 \mid \mu \tag{7-15}$$

gelten. Wir werden im folgenden zwei Fälle betrachten. Im einen Fall können wir eine relative Ganzheitsbasis, im anderen Fall nur ein Erzeugendensystem angeben. Dies hängt von der Hauptidealeigenschaft des Index Φ ab.
Bevor wir auf diese Unterscheidung eingehen, formulieren wir ein Lemma, das in beiden Fällen benötigt wird. Mittels der Zerlegung von Φ gilt:

Lemma 7.13 *(i) Es existiert ein $\tilde{\nu} \in o_{\mathcal{F}}$ mit*

$$\tilde{\nu}^2 \equiv \mu \; mod \; \Phi_2^2 \tag{7-16}$$

(ii) Es existiert eine Lösung $\nu \in o_{\mathcal{F}}$ der Kongruenz $x^2 \equiv \mu \; mod \; \Phi_2^2$ mit

$$(\nu) = \Phi_\mu \cdot \mathbf{a}_\nu. \tag{7-17}$$

Hierbei ist $\mathbf{a}_\nu \in \mathcal{I}_{\mathcal{F}}$ ganz.

Beweis: zu (i): Der Beweis von (i) ist schon in 7.9 gegeben worden. Man beachte nur, daß dort $\Phi = \Phi_2$ galt.
zu (ii): Sei $\tilde{\nu}$ eine Lösung der Kongruenz 7-16. Dann existiert nach dem chinesischen Restsatz ein $\nu \in o_{\mathcal{F}}$ mit:

$$\begin{aligned} &\nu \equiv \tilde{\nu} \; mod \; \Phi_2^2 \\ &\nu \equiv 0 \; mod \; \Phi_\mu. \end{aligned}$$

Für dieses ν gilt dann

$$\nu^2 - \tilde{\nu}^2 = (\nu - \tilde{\nu}) \cdot (\nu + \tilde{\nu}) \tag{7-18}$$

$$(\nu - \tilde{\nu}) \in \Phi_2^2 \tag{7-19}$$

Aus 7-18 folgt nun mit der Idealeigenschaft von Φ_2^2 und zusammen mit 7-19:

$$(\nu^2 - \tilde{\nu}^2) \in \Phi_2^2$$

Daraus folgt $\nu^2 \equiv \tilde{\nu}^2 \equiv \mu \; mod \; \Phi_2^2$ und somit die Behauptung. ■
Im weiteren sei $\nu \in o_{\mathcal{F}}$ mit $\nu^2 \equiv \mu \; mod \; \Phi_2^2$ und $(\nu) = \Phi_\mu \cdot \mathbf{a}_\nu$ fest gewählt.

7.4.1 Der Index ist ein Hauptideal

Betrachten wir nun den Fall, daß Φ ein Hauptideal ist. Es gelte

$$\Phi = (\gamma)$$

für ein $\gamma \in o_{\mathcal{F}}$. Wir können dann den folgenden Satz beweisen:

Satz 7.14 *Sind $\gamma, \nu \in o_{\mathcal{F}}$ wie oben gegeben, so bilden die algebraischen Zahlen*

$$\begin{aligned} \omega_1 &:= 1, \\ \omega_2 &:= \tfrac{\nu+\sqrt{\mu}}{\gamma} \end{aligned}$$

eine $o_{\mathcal{F}}$–Ganzheitsbasis von $o_{\mathcal{E}}$.

Beweis: Der Beweis wird ähnlich wie der Beweis von Satz 7.10 geführt. Zeigen wir also zuerst, daß ω_2 ganz ist.Es gilt (vgl. Beweis 7.10):

$$\begin{aligned} \mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_2) &= \tfrac{2\nu}{\gamma}, \\ \mathrm{N}_{\mathcal{E}/\mathcal{F}}(\omega_2) &= \tfrac{\nu^2-\mu}{\gamma^2}. \end{aligned}$$

Aus Lemma 7.13 und 7-14 folgt für das Ideal $(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_2))$:

$$(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_2)) = (2) \cdot \Phi_\mu \cdot \mathbf{a}_\nu \cdot \Phi_2^{-1} \cdot \Phi_\mu^{-1} \subseteq o_{\mathcal{F}}$$

Daher gilt $\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\omega_2) \in o_{\mathcal{F}}$. Es bleibt also noch $\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\omega_2) \in o_{\mathcal{F}}$ zu zeigen. Dazu beachten wir:

$$\begin{aligned} \nu^2 - \mu \in (\nu)^2 + (\mu) &= ggt((\nu^2), (\mu)) \\ &= ggt(\Phi_\mu^2 \cdot \mathbf{a}_\nu^2, \Phi_\mu^2 \cdot \mathbf{a}_\mu) \\ &= \Phi_\mu^2 \cdot \mathbf{a}_1, \end{aligned}$$

woraus nun sofort

$$\Phi_\mu^2 \cdot \mathbf{a}_1 \mid (\nu^2 - \mu) \tag{7-20}$$

mit einem ganzen Ideal $\mathbf{a}_1$ folgt. Ferner gilt nach der Wahl von ν

$$\nu^2 - \mu \in \Phi_2^2.$$

Deshalb gilt $\Phi_2^2 \cdot \mathbf{a}_2 = (\nu^2 - \mu)$ für ein ganzes Ideal $\mathbf{a}_2$. Wegen 7-20 und der Comaximalität von Φ_2 und Φ_μ existiert deshalb ein ganzes Ideal $\mathbf{a}$ mit:

$$(\nu^2 - \mu) = \Phi_2^2 \cdot \Phi_\mu^2 \cdot \mathbf{a} = \Phi^2 \cdot \mathbf{a}.$$

Damit ergibt sich schließlich für $\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\omega_2)$:

$$\begin{aligned}(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\omega_2)) &= (\frac{\nu^2-\mu}{\gamma^2}) \\ &= \Phi^2 \cdot \mathbf{a} \cdot \Phi^{-2} \\ &= \mathbf{a} \subseteq o_{\mathcal{F}}.\end{aligned}$$

Also ist auch $\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\omega_2)$ ganz in $\mathcal{F}$.
Der Beweis der Ganzheitsbasiseigenschaft ist völlig analog zu dem zu Satz 7.10 geführten Beweis. Wir verzichten deshalb hier darauf, diesen Beweis nochmals vorzuführen. ■

Bemerkung 7.15 *Ist ω_1, ω_2 die $o_{\mathcal{F}}$-Ganzheitsbasis von $o_{\mathcal{E}}$ wie in Satz 7.14 und ist $\eta_1, \ldots, \eta_m$ eine $\mathbb{Z}$-Ganzheitsbasis von $o_{\mathcal{F}}$, so gilt:*

$$o_{\mathcal{E}} = [\eta_1, \ldots, \eta_m, \eta_1\omega_2, \ldots, \eta_m\omega_2]_{\mathbb{Z}}$$

Beispiel 7.16 *Sei $\mathcal{F} = \mathbb{Q}(\sqrt{10})$. Dieser Zahlkörper hat die Klassenzahl 2, und eine Ganzheitsbasis wird durch*

$$\begin{aligned}\eta_1 &= 1 \\ \eta_2 &= \sqrt{10}\end{aligned}$$

gegeben.
Wir wollen nun die Erweiterung

$$\mathcal{E} := \mathcal{F}(\sqrt{17})$$

betrachten. Für die Ideale (2) und (17) ergeben sich die folgenden Zerlegungen:

$$\begin{aligned}(2) &= (2o_{\mathcal{F}} + \eta_2 o_{\mathcal{F}})^2 \\ (17) &= (17 o_{\mathcal{F}}).\end{aligned}$$

Aus $(1+2\eta_2)^2 \equiv 41 + 4\eta_2 \equiv 17 \mod (2o_{\mathcal{F}})^2$ folgt nun nach Satz 7.3 und Satz 7.2:

$$\begin{aligned}d_{\mathcal{E}/\mathcal{F}} &= 17 o_{\mathcal{F}} \\ \Phi &= 2 o_{\mathcal{F}}.\end{aligned}$$

Wie man sieht, ist Φ ein Hauptideal mit Erzeuger $\gamma = 2$. Aus Satz 7.14 ergibt sich folgende $o_{\mathcal{F}}$–Basis von $o_{\mathcal{E}}$:

$$\begin{aligned} \omega_1 &= 1 \\ \omega_2 &= \frac{1 + 2\eta_2 - \sqrt{17}}{2}. \end{aligned}$$

Ferner gilt nach Satz 6.12 und der vorangehenden Bemerkung:

$$\begin{aligned} |d_{\mathcal{E}}| &= 462400 \\ o_{\mathcal{E}} &= [1, \sqrt{10}, \frac{1 + 2\sqrt{10} - \sqrt{17}}{2}, \frac{20 + \sqrt{10} - \sqrt{17}\sqrt{10}}{2}]_{\mathbb{Z}}. \end{aligned}$$

7.4.2 Der Index ist kein Hauptideal

Betrachten wir nun abschließend den Fall, daß der Index Φ kein Hauptideal ist. Wie wir wissen (vgl. Satz 6.21), existiert dann keine relative Ganzheitsbasis. Jedoch gibt es, wie wir nach Korollar 6.17 wissen, ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$ mit 3 Erzeugern. Unsere Ziele sind nun die folgenden:

- Bestimmung eines $o_{\mathcal{F}}$ Erzeugendensystems von $o_{\mathcal{E}}$.
- Bestimmung einer $\mathbb{Z}$ - Basis von $o_{\mathcal{E}}$.

Unser Vorgehen wird im weiteren so sein, daß wir zuerst ein Erzeugendensystem bestimmen und dann dieses in eine $\mathbb{Z}$–Ganzheitsbasis von $o_{\mathcal{E}}$ überführen. Bestimmen wir also zuerst ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$.
Im weiteren sei:

$$\begin{aligned} \mathbf{b} &:= \Phi^{h_{\mathcal{F}}-1} \\ \mathbf{b} &= \beta_1 o_{\mathcal{F}} + \beta_2 o_{\mathcal{F}}, \end{aligned}$$

dann ist $\mathbf{b}$ ein ganzes Ideal in $o_{\mathcal{F}}$, da $h_{\mathcal{F}} > 1$ gilt. Durch diese Definition ist $\mathbf{b} \cdot \Phi$ ein Hauptideal. Wir setzen

$$(\gamma) := \mathbf{b} \cdot \Phi$$

und erinnern nochmals an die Wahl von $\nu \in o_{\mathcal{F}}$: Es gilt

$$\nu^2 \equiv \mu \; mod \; \Phi_2^2 \quad \wedge \quad (\nu) = \Phi_\mu \cdot \mathbf{a}_\nu.$$

Ein solches ν existiert nach Lemma 7.13.

Lemma 7.17 *Definiert man mit* $\mathbf{b} = \beta_1 o_{\mathcal{F}} + \beta_2 o_{\mathcal{F}}, \nu$ *und* γ *wie oben*

$$\xi_i := \beta_i \frac{\nu + \sqrt{\mu}}{\gamma} \qquad (i = 1, 2),$$

so gilt

$$\xi_i \in o_{\mathcal{E}} \qquad (i = 1, 2).$$

Beweis: Für den Beweis erinnern wir an die Ergebnisse aus dem Beweis von Satz 7.14. Dort haben wir

$$(\nu^2 - \mu) = \Phi^2 \cdot \mathbf{a}$$

mit einem ganzen Ideal $\mathbf{a} \subseteq o_{\mathcal{F}}$ gezeigt. Da die β_i $(i = 1, 2)$ in dem Ideal $\mathbf{b}$ liegen, gilt für die von β_i $(i = 1, 2)$ erzeugten Ideale:

$$(\beta_i) = \mathbf{b} \cdot \mathbf{b}_i \qquad ; (i = 1, 2)$$

mit ganzen Idealen $\mathbf{b}_i$ $(i = 1, 2)$.
Für $\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\xi_i) = \beta_i^2 \frac{\nu^2 - \mu}{\gamma^2}$ und $\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\xi_i) = \frac{2\beta_i \nu}{\gamma}$ $(i = 1, 2)$ ergeben sich daraus mit 7-15 für $i = 1, 2$:

$$\begin{aligned}
(\mathrm{Tr}_{\mathcal{E}/\mathcal{F}}(\xi_i)) &= (\frac{2\beta_i \nu}{\gamma}) \\
&= (2) \cdot \mathbf{b} \cdot \mathbf{b}_i \cdot \Phi_\mu \cdot \mathbf{a}_\nu \cdot (\Phi \cdot \mathbf{b})^{-1} \subset o_{\mathcal{F}} \\
(\mathrm{N}_{\mathcal{E}/\mathcal{F}}(\xi_i)) &= (\beta_i^2 \frac{\nu^2 - \mu}{\gamma^2}) \\
&= (\mathbf{b} \cdot \mathbf{b}_i)^2 \cdot \Phi^2 \cdot \mathbf{a} \cdot (\Phi \cdot \mathbf{b})^{-2} \subset o_{\mathcal{F}}.
\end{aligned}$$

Womit die Behauptung bewiesen ist. ∎
Formulieren wir nun die Hauptaussage:

Satz 7.18 *Sind* ξ_1, ξ_2 *wie in Lemma 7.17 definiert, so gilt*

$$o_{\mathcal{E}} = [1, \xi_1, \xi_2]_{o_{\mathcal{F}}}.$$

Für den Beweis dieses Satzes benötigen wir etwas mehr Raum.

7.4.3 Beweis der Hauptaussage

Zu Beginn dieses Abschnittes setzen wir zur Vereinfachung:

$$\Omega := \{1, \xi_1, \xi_2\}. \tag{7-21}$$

Ist $\tilde{\beta}_1, \ldots, \tilde{\beta}_m$ eine $\mathbb{Z}$–Basis von $\mathbf{b}$, so definieren wir

$$\eta_i \;:=\; \tilde{\beta}_i \frac{\nu + \sqrt{\mu}}{\gamma} \quad ; 1 \leq i \leq m. \tag{7-22}$$

Hierbei sind $\eta_1, \ldots, \eta_m$ nach 7.17 ganz algebraische Zahlen in $o_{\mathcal{E}}$.
Da Ω ein $o_{\mathcal{F}}$–Erzeugendensystem sein soll, muß mindestens $o_{\mathcal{F}}[\sqrt{\mu}] \subseteq [\Omega]_{o_{\mathcal{F}}}$ gelten. Wir beweisen dies in dem nächsten Lemma:

Lemma 7.19 *Es gilt*

$$o_{\mathcal{F}}[\sqrt{\mu}] \subseteq [\Omega]_{o_{\mathcal{F}}} =: \Gamma.$$

Beweis: Sei $\alpha = \alpha_1 + \alpha_2\sqrt{\mu} \in o_{\mathcal{F}}[\sqrt{\mu}]$ beliebig gegeben. Da $o_{\mathcal{F}} \subset \Gamma$ trivialerweise gilt, reicht es zu zeigen:

$$\exists\, \kappa \in o_{\mathcal{F}} \;:\; \alpha_2\sqrt{\mu} + \kappa \in \Gamma. \tag{7-23}$$

Aus $\gamma \in \mathbf{b}$ folgt $\alpha_2\gamma \in \mathbf{b}$. Daher existieren $\eta_1, \eta_2 \in o_{\mathcal{F}}$ mit $\eta_1\beta_1 + \eta_2\beta_2 = \alpha_2\gamma$ und es folgt nun:

$$\begin{aligned} \eta_1\xi_1 + \eta_2\xi_2 &= (\eta_1\beta_1 + \eta_2\beta_2)\frac{\nu + \sqrt{\mu}}{\gamma} \\ &= \alpha_2\nu + \alpha_2\sqrt{\mu}. \end{aligned}$$

Daraus ergibt sich 7-23 mit $\kappa = \alpha_2\nu$. ■
Unser Ziel ist es, zunächst einmal zu beweisen, daß die Menge

$$\{\zeta_1, \ldots, \zeta_m, \eta_1, \ldots, \eta_m\}$$

eine $\mathbb{Z}$–Ganzheitsbasis von $o_{\mathcal{E}}$ ist, wenn $\zeta_1, \ldots, \zeta_m$ eine $\mathbb{Z}$–Ganzheitsbasis von $o_{\mathcal{F}}$ ist. Dies werden wir mittels des Lemmas 5.17 tun. Der Beweis von Satz 7.18 ist dann nur noch ein kleiner Schritt.
Als erstes bestimmen wir für ein Primideal $\wp \in \mathbb{P}_{\mathcal{F}}$ eine $o_{\mathcal{F}}(\wp)$–Basis von $o_{\mathcal{E}}(\wp)$. Um dies zu tun, verwenden wir unter anderem auch lokale Methoden. Wichtig für unser Vorgehen ist das Zerlegungsverhalten der Primideale von $o_{\mathcal{F}}$ in $o_{\mathcal{E}}$. Nach Satz 3.5 zerlegt sich ein $\wp \in \mathbb{P}_{\mathcal{F}}$ in $o_{\mathcal{E}}$ auf eine der drei Arten:

(i) $\wp o_{\mathcal{E}} = \mathcal{P}_1 \cdot \mathcal{P}_2$

(ii) $\wp o_{\mathcal{E}} = \mathcal{P}_1^2$

(iii) $\wp o_{\mathcal{E}} = \mathcal{P}_1$

mit $\mathcal{P}_1 \neq \mathcal{P}_2 \in I\!P_{\mathcal{E}}$.
Um nun für ein $\wp \in I\!P_{\mathcal{F}}$ den Ring $o_{\mathcal{E}}(\wp)$ zu bestimmen, unterscheiden wir zwei Fälle, die wir in mehreren Sätzen behandeln werden.
Zuerst beschreiben wir die $\wp$–ganzen Elemente für den Fall, daß $\wp$ in $o_{\mathcal{E}}$ nach (i) zerfällt. Wir wenden dabei den Satz 5.16 an und verwenden im wesentlichen keine lokale Theorie. Für ein Primideal, das sich nach (ii) oder (iii) zerlegt gilt, wie wir gesehen haben, $o_{\mathcal{E}}(\wp) = \mathcal{E} \cap \Re_{\mathcal{P}_1}$. Wir bestimmen daher für die $\wp$–adische Erweiterung $\mathcal{E}_{\mathcal{P}_1}/\mathcal{F}_{\wp}$ eine lokale Ganzheitsbasis. Über diese erhalten wir dann eine $o_{\mathcal{F}}(\wp)$–Basis von $o_{\mathcal{E}}(\wp)$.

Sei nun $\wp$ ein Primideal in $o_{\mathcal{F}}$, das sich in $o_{\mathcal{E}}$ in zwei verschiedene Primideale zerlegt:

$$\wp o_{\mathcal{E}} = \mathcal{P}_1 \cdot \mathcal{P}_2.$$

Ferner sei $\pi \in \wp \setminus \wp^2$.
Wir bestimmen nun eine $o_{\mathcal{F}}(\wp)$–Basis von $o_{\mathcal{E}}(\wp)$. Da das Primideal unverzweigt ist, teilt es nicht die Diskriminate $d_{\mathcal{E}/\mathcal{F}}$ von $\mathcal{E}/\mathcal{F}$.

Lemma 7.20 *Es gelte $\wp^a \| \mu$ und $\wp \nmid 2$ mit $a > 0$. Dann wird durch*

$$1, \frac{1}{\pi^{a/2}}\sqrt{\mu} =: \delta$$

eine $o_{\mathcal{F}}(\wp)$–Basis von $o_{\mathcal{E}}(\wp)$ gegeben. Man beachte, daß a nach Satz 7.2 gerade ist, da $\wp$ nicht die Diskriminante teilt.

Beweis: Es gilt offenbar $\mathcal{E} = \mathcal{F}(\delta)$. Desweiteren ist δ eine Nullstelle von $f(t) = t^2 - \frac{\mu}{\pi^a} \in o_{\mathcal{F}}(\wp)[t]$ und es gilt

$$f'(\delta) = 2\delta.$$

Aufgrund der Definition von a gilt $\mathcal{P}_i \nmid \delta$ $(i = 1, 2)$. Da nach Voraussetzung $\wp$ nicht 2 teilt gilt, also $\mathcal{P}_i \nmid 2\delta$, womit

$$|f'(\delta)|_{\mathcal{P}_i} = 1 \qquad ; i = 1, 2$$

gezeigt ist. Mit Satz 5.16 folgt nun die Behauptung. ■

Bemerkung 7.21 *Nach der Definition von ν gilt $\nu = \Phi_\mu \cdot \mathbf{a}_\nu$. Daher gilt $\nu = \pi^{a/2}\alpha$ in $o_{\mathcal{F}}(\wp)$ mit einem $\alpha \in o_{\mathcal{F}}(\wp)$. Daraus folgt, daß auch $1, \frac{\nu+\sqrt{\mu}}{\pi^{a/2}}$ eine $o_{\mathcal{F}}(\wp)$–Basis von $o_{\mathcal{E}}(\wp)$ ist.*

Lemma 7.22 *Gilt $\wp^e \| 2$ und $\wp \not| \mu$ mit $e > 0$, so wird durch*

$$1, \frac{\nu + \sqrt{\mu}}{\pi^e} =: \delta$$

eine $o_{\mathcal{F}}(\wp)$–Basis von $o_{\mathcal{E}}(\wp)$ gegeben. Man beachte, daß nach Satz 7.3 und der Definition von ν die Kongruenz $\nu^2 \equiv \mu \bmod \wp^{2e}$ erfüllt ist.

Beweis: Es gilt $\mathcal{E} = \mathcal{F}(\delta)$ und δ ist Nullstelle des Polynoms $f(t) = t^2 - \frac{2\nu}{\pi^e}t + \frac{\nu^2-\mu}{\pi^{2e}}$. Aufgrund der Definition von ν und π gilt offenbar $f(t) \in o_{\mathcal{F}}(\wp)$. Um die Voraussetzungen des Satzes 5.16 vollständig zu erfüllen, betrachten wir $f'(\delta)$. Wir müssen zeigen, daß $|f'(\delta)|_{\mathcal{P}_i} = 1$ $(i = 1, 2)$ gilt.
Nach Vor. gilt $2 = \alpha\pi^e$ für eine Einheit $\alpha \in o_{\mathcal{F}}(\wp)$. Daraus folgt:

$$\begin{aligned} f'(\delta) \quad &= \alpha(\nu + \sqrt{\mu}) - \alpha\nu \\ &= \alpha\sqrt{\mu} \end{aligned}$$

und wir erhalten:

$$\begin{aligned} |f'(\delta)|_{\mathcal{P}_i} &= |\alpha\sqrt{\mu}|_{\mathcal{P}_i} \\ &= |\alpha|_{\mathcal{P}_i} \cdot |\sqrt{\mu}|_{\mathcal{P}_i} \\ &= 1 \cdot 1 = 1. \end{aligned}$$

Womit die Behauptung mittels Satz 5.16 bewiesen ist. ■

Lemma 7.23 *Gilt $\wp \not| 2\mu$, so wird durch*

$$1, \sqrt{\mu}$$

eine $o_{\mathcal{F}}(\wp)$–Basis von $o_{\mathcal{E}}(\wp)$ gegeben.

Beweis: Der Beweis ist eine direkte Folgerung aus Satz 5.16. ■

Bemerkung 7.24 *Durch die drei Lemmata werden alle Möglichkeiten abgedeckt, die für ein Primideal $\wp$ auftreten können, das in $o_{\mathcal{E}}$ in zwei verschiedene Primideale zerfällt.*
A priori gibt es für das Ideal $\wp$ noch den Fall, daß

$$\wp | 2 \quad \wedge \quad \wp | \mu$$

gilt. Dann folgt jedoch aus 7-4 und Satz 7.4, daß $\wp | d_{\mathcal{E}/\mathcal{F}}$ gilt und somit $\wp$ verzweigt ist. Also tritt dieser Fall nicht ein.

Lemma 7.25 *Ist $1, \delta$ die wie in 7.21, 7.22 oder 7.23 gegebene $o_{\mathcal{F}}(\wp)$–Basis von $o_{\mathcal{E}}(\wp)$, so existieren $a_0, a_1, a_2 \in o_{\mathcal{F}}(\wp)$ mit:*

$$\delta = a_0 + a_1 \xi_1 + a_2 \xi_2.$$

Beweis: Erfüllt $\wp$ die Vor. des Lemmas 7.23, so ist die Aussage trivial nach Lemma 7.19. Ansonsten gilt o.B.d.A. $\delta = \frac{\nu + \sqrt{\mu}}{\pi^r}$ mit $\wp^r \| 2$ bzw. $\wp^{2r} \| \mu$ nach 7.20, 7.21 und 7.22. Da aber $\wp$ nicht $d_{\mathcal{E}/\mathcal{F}}$ teilt, gilt auch $\wp^r | \Phi$ und somit gilt wegen $\gamma = \Phi \cdot \mathbf{b} = \wp^r \cdot \tilde{\Phi} \cdot \mathbf{b}$ in $o_{\mathcal{F}}$:

$$\gamma = \sum_{i=1}^{s} p_1^{(i)} \cdot \ldots \cdot p_r^{(i)} \cdot a^{(i)} \cdot \beta^{(i)}$$

mit $p_j^{(i)} \in \wp$, $a^{(i)} \in \tilde{\Phi}$ und $\beta^{(i)} \in \mathbf{b}$ $(1 \leq i \leq s, 1 \leq j \leq r)$. In $o_{\mathcal{F}}(\wp)$ hingegen gilt die Zerlegung:

$$\exists\, \lambda \in o_{\mathcal{F}}(\wp) : \gamma = \pi^r \cdot \lambda.$$

Wiederum in $o_{\mathcal{F}}(\wp)$ gelte $p_1^{(i)} \cdot \ldots \cdot p_r^{(i)} = \pi^r \cdot u^{(i)}$ für gewisse $u^{(i)} \in o_{\mathcal{F}}(\wp)$ $(1 \leq i \leq s)$. Dann gilt

$$\pi^r \lambda = \gamma = \sum_{i=1}^{s} p_1^{(i)} \cdot \ldots \cdot p_r^{(i)} \cdot a^{(i)} \cdot \beta^{(i)} = \pi^r \cdot \sum_{i=1}^{s} u^{(i)} \cdot a^{(i)} \cdot \beta^{(i)}. \tag{7-24}$$

Da $a^{(i)}\cdot\beta^{(i)}$ in dem Ideal $\mathbf{b}$ liegen, existieren $\kappa_1^{(i)}, \kappa_2^{(i)} \in o_{\mathcal{F}}$ mit $a^{(i)}\cdot\beta^{(i)} = \kappa_1^{(i)}\beta_1 + \kappa_2^{(i)}\beta_2$ $(1 \leq i \leq s)$. Definiert man $\lambda_j^{(i)} := u^{(i)}\kappa_j^{(i)} \in o_{\mathcal{F}}(\wp)$ $(j = 1, 2\ ;\ 1 \leq i \leq s)$, so folgt aus 7-24

$$\sum_{i=1}^{s} \lambda_1^{(i)}\beta_1 + \lambda_2^{(i)}\beta_2 = \lambda$$

Damit gilt nun

$$\sum_{i=1}^{s} \lambda_1^{(i)}\xi_1 + \sum_{i=1}^{s} \lambda_2^{(i)}\xi_2 = \sum_{i=1}^{s}(\lambda_1^{(i)}\beta_1 + \lambda_2^{(i)}\beta_2) \cdot \frac{\nu + \sqrt{\mu}}{\gamma} = \frac{\nu + \sqrt{\mu}}{\pi^r}$$

und es folgt mit $a_0 := 0$ und $a_j := \sum_{i=1}^{s} \lambda_j^{(i)}$ $(j = 1, 2)$ die Behauptung. ■
Damit wäre der Fall, daß sich das Primideal $\wp$ in $o_{\mathcal{E}}$ in zwei verschiedene Primideale zerlegt, abgehandelt.

Betrachten wir nun den Fall, daß sich das Primideal $\wp \in I\!P_{\mathcal{F}}$ in $o_{\mathcal{E}}$ nicht in zwei verschiedene Primideale zerlegt.
Im weiteren sei also $\wp \in I\!P_{\mathcal{F}}$ und $\mathcal{P} \in I\!P_{\mathcal{E}}$ sei das eindeutig bestimmte Primideal in $o_{\mathcal{E}}$ für das $\mathcal{P}|\wp o_{\mathcal{E}}$ gilt.
Nach Satz 5.8 gilt $[\mathcal{E}_{\mathcal{P}} : \mathcal{F}_{\wp}] = 2$ und nach Lemma 5.9 besitzt die Erweiterung $\mathcal{E}_{\mathcal{P}}/\mathcal{F}_{\wp}$ eine lokale Ganzheitsbasis. Ferner gilt

$$\mathcal{E}_{\mathcal{P}} = \mathcal{F}_{\wp}(\sqrt{\mu}).$$

Der nächste Satz, der auch in [23] zu finden ist, geht auf A. Fröhlich [10] zurück und beschreibt wie eine solche Ganzheitsbasis im quadratischen Fall aussieht.

Satz 7.26 *Sei $\mathcal{F}_{\wp}$ die $\wp$–adische Vervollständigung von $\mathcal{F}$ bzgl. $\wp$ und sei $\tau \in \Re_{\wp} = \{x \in \mathcal{F}_{\wp} |\ |x|_{\wp} \leq 1\}$ mit $\tau \neq \alpha^2\ \ \forall \alpha \in \mathcal{F}_{\wp}$. Ferner gelte $\tau \notin \mathrm{m}_{\wp}^2$, wobei $\mathrm{m}_{\wp} := \{x \in \mathcal{F}_{\wp} |\ |x|_{\wp} < 1\}$ das maximale Primideal von $\Re_{\wp}$ ist. Definiert man dann*

$$L := F_{\wp}(\sqrt{\tau}),$$

so gilt für $S = \{x \in L |\ |x|_{\wp} \leq 1\}$ mit $\pi \in \mathrm{m}_{\wp} \setminus \mathrm{m}_{\wp}^2$:

(i) $\pi \not|\, 2\tau \Rightarrow S = [1, \sqrt{\tau}]_{\Re_{\wp}}$

(ii) $\pi|\tau \Rightarrow S = [1, \sqrt{\tau}]_{\Re_\wp}$

(iii) Gilt $\pi|2 \;\wedge\; \pi \not|\tau$ *und ist* l *die größte ganze Zahl mit*

$$\pi^l|2 \;\wedge\; \exists \beta \in \Re_\wp \;:\; \beta^2 \equiv \tau \; mod \; \mathrm{m}_\wp^{2l},$$

so folgt

$$S = [1, \frac{\beta + \sqrt{\tau}}{\pi^l}]_{\Re_\wp}.$$

(Wir bezeichnen die Bewertung auf L *auch mit* $|\cdot|_\wp$*, da sie ja eindeutig bestimmt ist.)*

Beweis: Der Beweis wird für alle drei Fälle einzeln geführt und beruht auf dem folgenden Zusammenhang.
Wie wir wissen existiert eine lokale Ganzheitsbasis (vgl. Satz 5.9) für S:

$$S = [1, \delta]_{\Re_\wp} \qquad ; mit \; \delta \in S.$$

Aufgrund der Darstellbarkeit von $\mathcal{F}_\wp$ (vgl. Satz 5.1) gilt

$$\delta = \frac{\delta_1 + \delta_2\sqrt{\tau}}{\pi^k}$$

mit gewissen $\delta_1, \delta_2 \in \Re_\wp$ und einem $k \geq 0$; o.B.d.A gelte $ggt(\delta_1, \delta_2, \pi) = 1$.
Da δ eine ganze Zahl in L ist, folgt aus 5.5:

$$\mathrm{N}_{\mathrm{L}/\mathcal{F}_\wp}(\delta) = \frac{\delta_1^2 - \delta_2^2\tau}{\pi^{2k}} \in \Re_\wp. \tag{7-25}$$

Wir benutzen diese Bezeichnungen im weitern, ohne dies zu betonen.

zu (i): Angenommen es gilt $k > 0$. Dann folgt aus 7-25, daß die Kongruenz $x^2 \equiv y^2\tau \; mod \; m_\wp$ eine Lösung $(x, y) \in (\Re_\wp \setminus m_\wp)^2$ (beachte $ggt(\delta_1, \delta_2, \pi) = 1$) hat. Da also y eine Einheit in $\Re_\wp$ ist (das Primideal $m_\wp$ ist maximal), hat sogar die Kongruenz

$$x^2 \equiv \tau \; mod \; m_\wp$$

eine Lösung in $\Re_\wp$. Nach der Folgerung 5.3 aus Hensels Lemma hat dann die Gleichnung $x^2 - a = 0$ auch eine Lösung in $\mathcal{F}_\wp$, denn aus $\pi \not| 2\tau$ folgt, daß $x^2 - \tau$

in $(\Re_\wp/m_\wp)$ keine doppelte Nullstelle hat. Dies liegt aber im Widerspruch zu unserer Wahl von τ, denn τ ist kein Quadrat in $\mathcal{F}_\wp$.
Also gilt $k = 0$ und somit $\delta = \delta_1 + \delta_2\sqrt{\tau}$. Daraus folgt

$$S = [1, \delta_1 + \delta_2\sqrt{\tau}]_{\Re_\wp} \overset{\delta_1,\delta_2 \in \Re_\wp}{\subseteq} [1, \sqrt{\tau}]_{\Re_\wp} \subseteq S,$$

womit die Behauptung (i) bewiesen ist.

zu (ii): Nach Voraussetzung gilt $\nu_{m_\wp}(\tau) = 1$, da sowohl $\tau \notin m_\wp^2$ als auch $\pi | \tau$ gilt. Daraus ergibt sich

$$\nu_{m_\wp}(\delta_1^2 - \delta_2^2\tau) \overset{4.4}{=} min(2\nu_{m_\wp}(\delta_1), 2\nu_{m_\wp}(\delta_2) + 1).$$

Für k muß daher nach 7-25 gelten:

$$2k \leq min(2\nu_{m_\wp}(\delta_1), 2\nu_{m_\wp}(\delta_2) + 1).$$

Aus $ggt(\delta_1, \delta_2, \pi) = 1$ folgt nun aber $\nu_{m_\wp}(\delta_1) = 0 \ \vee \ \nu_{m_\wp}(\delta_2) = 0$ und somit gilt $k = 0$.
Man schließt nun wie im Fall (i).

zu(iii): Wir beweisen diesen dritten Teil des Satzes in zwei Schritten.
Zunächst nehmen wir $k = 0$ an und zeigen, daß die Kongruenz $x^2 \equiv \tau \ mod \ m_\wp^2$ in $\Re_\wp$ nicht lösbar ist. Gilt aber $k \neq 0$, so zeigen wir, daß die Kongruenz $x^2 \equiv \tau \ mod \ m_\wp^{2l}$ maximal für $l = k$ lösbar ist.
Sei also $k = 0$. Angenommen die Kongruenz $x^2 \equiv \tau \ mod \ m_\wp^2$ hat eine Lösung $a \in \Re_\wp$. Dann gilt für

$$\alpha := \frac{a + \sqrt{\tau}}{\pi}$$

$\mathrm{N}_{\mathrm{L}/\mathcal{F}_\wp}(\alpha) \in \Re_\wp$, also nach 5.5 $\alpha \in S$, was ein Widerspruch zu

$$S = [1, \delta]_{\Re_\wp} \overset{k=0}{=} [1, \sqrt{\tau}]_{\Re_\wp}$$

ist. Also ist die Kongruenz nicht lösbar.
Sei nun $k \neq 0$. Wir zeigen mittels $\nu_{m_\wp}(\delta_1\delta_2) = 0$, daß sowohl δ_1 als auch δ_2 eine Einheit in $\Re_\wp$ ist. Wie in (ii) gesehen gilt $\nu_{m_\wp}(\delta_1) = 0 \ \vee \ \nu_{m_\wp}(\delta_2) = 0$. Gilt $\nu_{m_\wp}(\delta_1) = 0$ so folgt aus 7-25

$$\begin{aligned} & \delta_2^2\tau \equiv \delta_1^2 \not\equiv 0 \ mod \ m_\wp \\ \Rightarrow \quad & \delta_2^2\tau \notin m_\wp \\ \Rightarrow \quad & \nu_{m_\wp}(\delta_2) = 0. \end{aligned}$$

Analog zeigt man "$\nu_{m_\wp}(\delta_2) = 0 \Rightarrow \nu_{m_\wp}(\delta_1) = 0$". Hierbei beachte man, daß $\nu_{m_\wp}(\tau) = 0$ nach Voraussetzung gilt.
Zeigen wir nun, daß k die größte ganze Zahl in $\{0, 1, \ldots, \nu_{m_\wp}(2)\}$ ist, für die die Kongruenz

$$x^2 \equiv \tau \; mod \; m_\wp^{2l} \tag{7-26}$$

eine Lösung besitzt. Aus $d(1, \delta) = 4\tau \left(\frac{\delta_2}{\pi^k}\right)^2 \in \Re_\wp$ folgt sofort $\pi^{2k}|4$, da nach Voraussetzung $\pi \not| \tau$ gilt und gerade $\pi \not| \delta_2$ gezeigt wurde. Damit gilt natürlich $k \leq \nu_{m_\wp}(2)$ und somit

$$k \in \{0, 1, \ldots, \nu_{m_\wp}(2)\}.$$

Da δ_2 eine Einheit in $\Re_\wp$ ist, gilt $\frac{\delta_1}{\delta_2} \in \Re_\wp$, und nach 7-25 löst dieses Element die Kongruenz 7-26. Ist nun ein $m \in \{0, 1, \ldots, \nu_{m_\wp}(2)\}$ gegeben, für das ein $\beta \in \Re_\wp$ existiert mit $\beta^2 \equiv \tau \; mod \; m_\wp^{2m}$, so gilt

$$\frac{\beta + \sqrt{\tau}}{\pi^m} \in S$$

nach 7-25 und Satz 5.5. Aus $S = [1, \delta]_{\Re_\wp}$ folgt die Existenz von $a_1, a_2 \in \Re_\wp$ mit

$$\begin{array}{rc} & \frac{\beta+\sqrt{\tau}}{\pi^m} = a_1 + a_2 \frac{\delta_1 + \delta_2\sqrt{\tau}}{\pi^k} \\ \Rightarrow & \pi^{k-m} = a_2\delta_2 \\ \Rightarrow & k \geq m. \end{array}$$

Also war k maximal gewählt und somit ist der Satz bewiesen. ∎
Es gilt nun zu überprüfen inwieweit dieser Satz als Lösungshilfe für unser Problem (die Bestimmung einer $o_\mathcal{F}(\wp)$–Basis von $o_\mathcal{E}(\wp)$) dienen kann.
Wie schon für die total zerlegten Primideale werden wir nun für die restlichen Primideale in $\mathbb{P}_\mathcal{F}$ den Modul $o_\mathcal{E}(\wp)$ als freien $o_\mathcal{F}(\wp)$–Modul beschreiben.
Aufgrund des schon weiter oben angedeuteten Zusammenhanges zur lokalen Theorie betrachten wir die $\wp$–adischen Erweiterungen $\mathcal{E}_\mathcal{P}/\mathcal{F}_\wp$. Wie wir wissen, gilt $\mathcal{E}_\mathcal{P} = \mathcal{F}_\wp(\sqrt{\mu})$. Auf diese Erweiterung wollen wir den Satz 7.26 anwenden. Die Voraussetzungen des Satzes sind bis auf

$$\mu \notin m_\wp^2 \tag{7-27}$$

alle erfüllt, denn es gilt $\mu \in o_\mathcal{F}$ und somit nach 4.19 $\mu \in \Re_\wp$. Ferner ist μ kein Quadrat in $\mathcal{F}_\wp$, denn es gilt $[\mathcal{E}_\mathcal{P} : \mathcal{F}_\wp] = 2$.

Unter Berücksichtigung dieser Bemerkung beweisen wir nun die folgenden drei Lemmata.
Der besseren Unterscheidung wegen bezeichnen wir die Ringe der ganzen Elemente in $\mathcal{F}_\wp$ mit $\Re_\wp$ und in $\mathcal{E}_\mathcal{P}$ mit $\mathcal{S}_\mathcal{P}$. Ferner sei durch π ein Element aus $\wp \setminus \wp^2$ gegeben.

Lemma 7.27 *Gilt $\wp \not| 2\mu$, so folgt für $o_\mathcal{E}(\wp)$:*

$$o_\mathcal{E}(\wp) = [1, \sqrt{\mu}]_{o_\mathcal{F}(\wp)}.$$

Beweis: Aus $\wp \not| 2\mu$ folgt wegen $\wp = m_\wp \cap \mathcal{F}$

$$\mu \notin m_\wp$$

und daher gilt $\mu \notin m_\wp^2 \subset m_\wp$. Also ist auch die letzte Voraussetzung 7-27 erfüllt und es gilt

$$\mathcal{S}_\mathcal{P} = [1, \sqrt{\mu}]_{\Re_\wp}.$$

Wir erhalten nun also $o_\mathcal{E}(\wp) = [1, \sqrt{\mu}]_{o_\mathcal{F}(\wp)}$. ■

Lemma 7.28 *Gilt $\wp^a \| \mu$, so folgt für $o_\mathcal{E}(\wp)$:*

(i) $o_\mathcal{E}(\wp) = [1, \sqrt{\mu}]_{o_\mathcal{F}(\wp)}$, *falls $\wp | 2$ gilt.*

(ii) $o_\mathcal{E}(\wp) = [1, \frac{1}{\pi^{[a/2]}}\sqrt{\mu}]_{o_\mathcal{F}(\wp)}$, *falls $\wp \not| 2$ gilt.*

Beweis: Gilt für $\wp$ auch $\wp | 2$, so erfüllt μ nach 7-1 auch die Voraussetzung 7-27 und somit gilt in diesem Fall $\mathcal{S}_\mathcal{P} = [1, \sqrt{\mu}]_{\Re_\wp}$. Daraus folgt die Behauptung.
Gilt nun aber $\wp \not| 2$ so haben wir keine Kontrolle über $\nu_\wp(\mu)$, wie wir zu Beginn dieses Kapitels gesehen haben. In $\mathcal{F}_\wp$ (und auch in $o_\mathcal{F}(\wp)$) gilt

$$\mu = \pi^{2a_1 + a_2} \cdot \varepsilon$$

mit $a_2 \in \{0, 1\}$ und $|\varepsilon|_\wp = 1$. Daher gilt mit $\tilde{\mu} := \pi^{a_2} \cdot \varepsilon$

$$\mathcal{E}_\mathcal{P} = \mathcal{F}_\wp(\sqrt{\mu}) = \mathcal{F}_\wp(\sqrt{\tilde{\mu}})$$

und dieses $\tilde{\mu}$ erfüllt nun die Bedingung 7-27. Es gilt also

$$\mathcal{S}_{\mathcal{P}} = [1, \sqrt{\tilde{\mu}}]_{\Re_\wp} = [1, \frac{1}{\pi^{a_1}}\sqrt{\mu}]_{\Re_\wp}.$$

Daraus folgt die Behauptung, da $a_1 = \lfloor a/2 \rfloor$ gilt. ∎

Bemerkung 7.29 *Gilt $\wp^a \| \mu$ und $\wp \nmid 2$, so gilt nach Satz 7.2 $\wp^{\lfloor a/2 \rfloor} | \Phi_\mu$. Aus der Faktorisierung $(\nu) = \Phi_\mu \cdot \mathbf{a}_\nu$ folgt daher $\frac{\nu}{\pi^{\lfloor a/2 \rfloor}} \in o_{\mathcal{F}}(\wp)$.*
Daher gilt auch $o_{\mathcal{E}}(\wp) = [1, \frac{\nu+\sqrt{\mu}}{\pi^{\lfloor a/2 \rfloor}}]_{o_{\mathcal{F}}(\wp)}$.

Lemma 7.30 *Gilt $\wp^e \| 2$ und $\wp \nmid \mu$, so folgt*

$$o_{\mathcal{E}}(\wp) = [1, \frac{\nu + \sqrt{\mu}}{\pi^k}]_{o_{\mathcal{F}}(\wp)}.$$

Hierbei ist k durch $k = max\{0 \leq l \leq e | \exists \alpha \in o_{\mathcal{F}} : \alpha^2 \equiv \mu \bmod \wp^{2l}\}$ gegeben.

Beweis: Offenbar genügt μ den Vor. des Satzes 7.26.
Aufgrund der Sätze 7.3 und 7.4 gilt für u mit $\wp^u \| \Phi$:

$$u = max\{0 \leq l \leq e \mid \exists \alpha \in o_{\mathcal{F}} : \alpha^2 \equiv \mu \bmod \wp^{2l}\}.$$

Wegen der Reihendarstellung von $\mathcal{F}_\wp$ (vgl. 5.1) gilt, daß diese Kongruenz genau dann in $o_{\mathcal{F}}$ lösbar ist, wenn sie in $\Re_\wp$ lösbar ist. Daher gilt nach Satz 7.26 wegen

$$k = max\{0 \leq l \leq \nu_{m_\wp}(2) \mid \exists \alpha \in \Re_\wp : \alpha^2 \equiv \mu \bmod m_\wp^{2l}\}$$

also $k = u$.
Da ν eine Lösung der Kongruenz $x^2 \equiv \mu \bmod m_\wp^{2u}$ ist, gilt nach Satz 7.26

$$\mathcal{S}_{\mathcal{P}} = [1, \frac{\nu + \sqrt{\mu}}{\pi^k}]_{\Re_\wp}.$$

Womit die Behauptung bewiesen ist. ∎
Analog zu 7.25 gilt das Lemma:

Lemma 7.31 *Ist $1, \delta$ die wie in 7.27,7.28 (bzw. 7.29) oder 7.30 gegebene $o_{\mathcal{F}}(\wp)$–Basis von $o_{\mathcal{E}}(\wp)$, so existieren $a_0, a_1, a_2 \in o_{\mathcal{F}}(\wp)$ mit:*

$$\delta = a_0 + a_1\xi_1 + a_2\xi_2.$$

Da der Beweis dieses Lemmas völlig analog zu dem Beweis von 7.25 geführt wird, verzichten wir auf ihn.

Wir haben in den letzten Sätzen die $\wp$–ganzen Elemente von $\mathcal{E}$ für ein $\wp \in I\!P_{\mathcal{F}}$ vollständig beschrieben. Wir wollen die im weiteren wichtigen Punkte dieser Charakterisierung nun kurz festhalten.

Satz 7.32 *Ist $\wp$ ein beliebiges Primideal in $o_{\mathcal{F}}$ mit $\wp^u \| \Phi$, so gilt:*

$$o_{\mathcal{E}}(\wp) = [1, \delta := \frac{\nu + \sqrt{\mu}}{\pi^u}]_{o_{\mathcal{F}}(\wp)}$$

mit einem $\pi \in \wp \setminus \wp^2$. Ferner existieren $\alpha_0, \alpha_1, \alpha_2 \in o_{\mathcal{F}}(\wp)$ mit:

$$\delta = \alpha_0 + \alpha_1 \xi_1 + \alpha_2 \xi_2.$$

Zum Beweis: Der Beweis dieses Satzes wurde in den vorangegangenen Lemmata gegeben, denn man verifiziert sofort an den Aussageformulierungen von 7.20,7.22,7.23 sowie 7.27,7.28 und 7.30 die Richtigkeit des zu $\nu_{\wp}(\Phi)$ gegebenen Zusammenhangs.
Es ist uns nun möglich den Beweis des Satzes 7.18 anzugehen. Dazu konstruieren wir zunächst für ein $p \in I\!P$ eine $\mathbb{Z}(p)$–Basis von $o_{\mathcal{E}}(p)$. Dies werden wir mittels des Lemmas 5.19 tun. Das folgende Lemma ebnet den Weg:

Lemma 7.33 *Ist $\{\wp_1, \ldots, \wp_s\} \subset I\!P_{\mathcal{F}}$ eine endliche Menge paarweise verschiedener Primideale, so existiert ein $\delta \in \mathcal{E}$ mit:*

(i) $o_{\mathcal{E}}(\wp_i) = [1, \delta]_{o_{\mathcal{F}}(\wp_i)} \quad ; 1 \le i \le s$

(ii) Es existieren $\alpha_1, \alpha_2 \in \bigcap_{i=1}^{s} o_{\mathcal{F}}(\wp_i)$ mit:

$$\delta = \alpha_1 \xi_1 + \alpha_2 \xi_2$$

Beweis: Ist $1, \delta_i := \frac{\nu + \sqrt{\mu}}{\pi_i^{\phi_i}}$ eine Basis von $o_{\mathcal{E}}(\wp_i)$ ($\pi_i \in \wp_i \setminus \wp_i^2$ und $\pi_i \notin \wp_j$ für $1 \le i, j \le s$, $i \ne j$), so existiert gemäß dem chinesischen Restsatz ein τ in $o_{\mathcal{F}}$ mit:

$$\tau \equiv \pi_i^{\phi_i} \; mod \; \wp_i \quad ; 1 \le i \le s.$$

Definiert man damit nun $\delta := \frac{\nu+\sqrt{\mu}}{\tau}$, so gilt

$$\delta = u_i \delta_i \tag{7-28}$$

mit einer Einheit $u_i \in o_{\mathcal{F}}(\wp_i)$ $(1 \leq i \leq s)$.
Wir zeigen nun die Darstellung von δ in ξ_1, ξ_2 mittels einem zu dem Beweis von 7.25 ähnlichen Vorgehen.
Es gelte o.B.d.A $\phi_i > 0$ für $1 \leq i \leq s_1$ und $\phi_i = 0$ sonst. Aufgrund der Primidealzerlegung von γ und der Darstellung von Idealprodukten existiert in $o_{\mathcal{F}}$ die folgende Zerlegung:

$$\gamma = \sum_{i=1}^{n} p_{1,1}^{(i)} \cdot \ldots \cdot p_{1,\phi_1}^{(i)} \cdot \ldots \cdot p_{s_1,1}^{(i)} \cdot \ldots \cdot p_{s_1,\phi_{s_1}}^{(i)} \cdot a^{(i)} \cdot \beta^{(i)} \tag{7-29}$$

mit $p_{k,l}^{(i)} \in \wp_i$, $a^{(i)} \in \Phi \cdot (\prod_{j=1}^{s_1} \wp_j)^{-1}$, $\beta^{(i)} \in \mathbf{b}$ $(1 \leq k \leq s_1,\ 1 \leq l \leq \phi_k,\ 1 \leq i \leq n)$.
Ist dann $\beta \in ggt((\beta^{(1)}), \ldots, (\beta^{(n)}))$, so definieren wir $\xi := \beta \frac{\nu+\sqrt{\mu}}{\gamma}$ und beweisen

$$\forall\ 1 \leq i \leq s\ \ \exists\ \alpha^{(i)} \in o_{\mathcal{F}}(\wp_i)\ :\ \delta_i = \alpha^{(i)} \xi. \tag{7-30}$$

Daraus folgt dann die Behauptung, denn $1, \xi$ ist eine $\mathcal{F}$–Basis von $\mathcal{E}$, und deshalb existieren eindeutig bestimmte $a_1, a_2 \in \mathcal{F}$ mit

$$\delta = a_1 + a_2 \xi.$$

Nach 7-28 und 7-30 gilt dann $a_1 = 0$ und $a_2 = u_i \alpha^{(i)}$ $(1 \leq i \leq s)$. Daher gilt $a_2 \in o_{\mathcal{F}}(\wp_i)$ $(1 \leq i \leq s)$. Aus $\beta \in \mathbf{b}$ folgt dann $\beta = \kappa_1 \beta_1 + \kappa_2 \beta_2$ für gewisse $\kappa_1, \kappa_2 \in o_{\mathcal{F}}$. Daraus folgt schließlich $\xi = \kappa_1 \xi_1 + \kappa_2 \xi_2$ und somit die Behauptung.
Beweisen wir also noch 7-30:
Ist $i > s_1$ so ist die Aussage nach der Definition von β trivial. Sei also $i \leq s_1$.
Aufgrund der Definition von β gilt für γ nach 7-29 in $o_{\mathcal{F}}$

$$\gamma = \beta \cdot \sum_{i=1}^{n} p_{1,1}^{(i)} \cdot \ldots \cdot p_{1,\phi_1}^{(i)} \cdot \ldots \cdot p_{s_1,1}^{(i)} \cdot \ldots \cdot p_{s_1,\phi_{s_1}}^{(i)} \cdot a^{(i)} \cdot b^{(i)}$$

mit $b^{(i)} \in o_{\mathcal{F}}$. Daher gilt in $o_{\mathcal{F}}(\wp_i)$

$$\gamma = \pi_i^{\phi_i} \cdot \beta \cdot \sum_{i=1}^{n} u^{(i)} \cdot P^{(i)} \cdot a^{(i)} \cdot b^{(i)}$$

mit $P^{(i)} := \prod_{\substack{k=1\\k\neq i}}^{s_1} \prod_{l=1}^{\phi_k} p_{k,l}^{(i)}$ und passenden Zahlen $u^{(i)} \in o_{\mathcal{F}}(\wp_i)$. Es folgt

$$\begin{aligned} \delta_i &= \frac{\nu + \sqrt{\mu}}{\pi^{\phi_i}} \\ &= \beta \sum_{i=1}^{n} u^{(i)} \cdot P^{(i)} \cdot a^{(i)} \cdot b^{(i)} \frac{\nu + \sqrt{\mu}}{\gamma} \\ &= \left(\sum_{i=1}^{n} u^{(i)} \cdot P^{(i)} \cdot a^{(i)} \cdot b^{(i)} \right) \xi =: \alpha^{(i)} \xi \end{aligned}$$

und damit nach 7-30 die Behauptung. ■

Setzt man als Primidealmenge in diesem Lemma die Menge aller in $o_{\mathcal{F}}$ über einer Primzahl p gelegenen Primideale, so erhält man zusammen mit einer Ganzheitsbasis von $o_{\mathcal{F}}$ nach 5.18 und 5.19 eine $\mathbb{Z}(p)$–Basis der p–ganzen Elemente von $\mathcal{E}$. Diese Tatsache werden wir in dem abschließendem Satz benutzen.

Satz 7.34 *Ist $\zeta_1, \dots, \zeta_m$ eine $\mathbb{Z}$–Ganzheitsbasis von $o_{\mathcal{F}}$, so wird durch (die in 7-22 definierten)*

$$\{\zeta_1, \dots, \zeta_m, \eta_1, \dots, \eta_m\}$$

eine $\mathbb{Z}$–Ganzheitsbasis von $o_{\mathcal{E}}$ gegeben.

Beweis: Wir beweisen den Satz, indem wir zeigen:

$$\forall\, p \in \mathbb{P} \;:\; [\zeta_1, \dots, \zeta_m, \eta_1, \dots, \eta_m]_{\mathbb{Z}(p)} = o_{\mathcal{E}}(p). \tag{7-31}$$

Trivialerweise gilt $[\zeta_1, \dots, \zeta_m, \eta_1, \dots, \eta_m]_{\mathbb{Z}(p)} \subseteq o_{\mathcal{E}}(p)\ \forall\ p \in \mathbb{P}$, denn es gilt $\{\zeta_1, \dots, \zeta_m, \eta_1, \dots, \eta_m\} \subset o_{\mathcal{E}}$.

Bleibt also noch $o_{\mathcal{E}}(p) \subseteq [\zeta_1, \dots, \zeta_m, \eta_1, \dots, \eta_m]_{\mathbb{Z}(p)}\ \forall\ p \in \mathbb{P}$ zu zeigen. Dazu sei nun $p \in \mathbb{P}$ beliebig gegeben. Dann existiert nach Lemma 7.33 zu der Menge $\Pi := \{\wp \in \mathbb{P}_{\mathcal{F}} \mid \wp | p o_{\mathcal{F}}\}$ ein $\delta \in \mathcal{E}$ mit

$$[1, \delta]_{o_{\mathcal{F}}(\wp)} = o_{\mathcal{E}}(\wp) \qquad \forall\ \wp \in \Pi.$$

Daher wird nach 5.18 und 5.19 durch $\{\zeta_1, \dots, \zeta_m, \delta\zeta_1, \dots, \delta\zeta_m\}$ eine $\mathbb{Z}(p)$–Basis von $o_{\mathcal{E}}(p)$ gegben. Wir zeigen nun 7-31 indem wir beweisen:

$$\delta\zeta_i \in [\zeta_1, \dots, \zeta_m, \eta_1, \dots, \eta_m]_{\mathbb{Z}(p)} \qquad 1 \le i \le m. \tag{7-32}$$

Betrachten wir also $\delta\zeta_i$ für $1 \leq i \leq m$. Nach Lemma 7.33 existieren $a_1, a_2 \in o_{\mathcal{F}}(p)$ mit $\delta = a_1\xi_1 + a_2\xi_2$. Daher gilt

$$\begin{aligned} \delta\zeta_i &= (a_1\xi_1 + a_2\xi_2)\zeta_i \\ &= a_1\zeta_i\beta_1\frac{\nu+\sqrt{\mu}}{\gamma} + a_2\zeta_i\beta_2\frac{\nu+\sqrt{\mu}}{\gamma}. \end{aligned}$$

Da ζ_i in $o_{\mathcal{F}}$ liegt und β_1, β_2 in dem Ideal $\mathbf{b}$ liegen hat die algebraische Zahl $\zeta_i\beta_j$ $(j = 1, 2)$ eine $\mathbb{Z}$–Darstellung in $\tilde{\beta}_1, \ldots, \tilde{\beta}_m$. Sei etwa $\zeta_i\beta_j = \sum_{k=1}^m b_k^{(j)}\tilde{\beta}$ mit passenden $b_k^{(j)} \in \mathbb{Z}$ $(j = 1, 2)$. Da a_1, a_2 in $o_{\mathcal{F}}(p)$ liegen, gilt nach 5.18 $a_j = \sum_{k=1}^m a_k^{(j)}\zeta_k$ für gewisse $a_k^{(j)} \in \mathbb{Z}(p)$ $(j = 1, 2)$. Somit erhalten wir

$$\begin{aligned} \delta\zeta_i &= \left(\sum_{k=1}^m a_k^{(1)}\zeta_k\right)\left(\sum_{l=1}^m b_l^{(1)}\tilde{\beta}_l\right)\frac{\nu+\sqrt{\mu}}{\gamma} + \left(\sum_{k=1}^m a_k^{(2)}\zeta_k\right)\left(\sum_{l=1}^m b_l^{(2)}\tilde{\beta}_l\right)\frac{\nu+\sqrt{\mu}}{\gamma} \\ &= \left(\sum_{k=1}^m a_k^{(1)}\zeta_k\right)\left(\sum_{l=1}^m b_l^{(1)}\eta_l\right) + \left(\sum_{k=1}^m a_k^{(2)}\zeta_k\right)\left(\sum_{l=1}^m b_l^{(2)}\eta_l\right) \\ &= \sum_{k=1}^m\sum_{l=1}^m a_k^{(1)}b_l^{(1)}\zeta_k\eta_l + \sum_{k=1}^m\sum_{l=1}^m a_k^{(2)}b_l^{(2)}\zeta_k\eta_l. \end{aligned}$$

Schließlich existieren nun wegen $\tilde{\beta}_l \in \mathbf{b}$ und wegen $\zeta_k \in o_{\mathcal{E}}$ Elemente $c_j^{(k,l)} \in \mathbb{Z}$ mit $\sum_{j=1}^m c_j^{(k,l)}\tilde{\beta}_j = \zeta_k\tilde{\beta}_l$. Damit gilt dann $\zeta_k\eta_l = \sum_{j=1}^m c_j^{(k,l)}\eta_j$ und es folgt schließlich:

$$\begin{aligned} \delta\zeta_i &= \sum_{k=1}^m\sum_{l=1}^m a_k^{(1)}b_l^{(1)}\sum_{j=1}^m c_j^{(k,l)}\eta_j + \sum_{k=1}^m\sum_{l=1}^m a_k^{(2)}b_l^{(2)}\sum_{j=1}^m c_j^{(k,l)}\eta_j \\ &= \sum_{j=1}^m\sum_{k=1}^m\sum_{l=1}^m a_k^{(1)}b_l^{(1)}c_j^{(k,l)}\eta_j + \sum_{j=1}^m\sum_{k=1}^m\sum_{l=1}^m a_k^{(2)}b_l^{(2)}c_j^{(k,l)}\eta_j. \end{aligned}$$

Da die Koeffizienten $a_k^{(1)}, a_k^{(2)}, b_l^{(1)}, b_l^{(2)}, c_j^{(k,l)}$ für $1 \leq j, k, l \leq m$ alle in $\mathbb{Z}$ bzw. in $\mathbb{Z}(p)$ liegen, ist 7-32 und damit der Satz, bewiesen. ■

Mit diesem Satz ist natürlich auch Satz 7.18 bewiesen, denn ist $\alpha \in o_{\mathcal{E}}$, so gilt nun ja

$$\alpha = \sum_{i=1}^m \alpha_i\zeta_i + \sum_{i=1}^m \alpha_{i+m}\eta_i$$

mit $\alpha_i \in \mathbb{Z}$ $(1 \leq i \leq 2m)$ und einer $\mathbb{Z}$–Ganzheitsbasis $\zeta_1, \ldots, \zeta_m$ von $o_{\mathcal{F}}$. Daher gilt offensichtlich $\sum_{i=1}^{m} \alpha_i \zeta_i =: a_0 \in o_{\mathcal{F}}$. Ferner existieren $a_1, a_2 \in o_{\mathcal{F}}$ mit

$$a_1\beta_1 + a_2\beta_2 = \sum_{i=1}^{m} \alpha_{i+m}\tilde{\beta}_i.$$

Aufgrund der Definition von $\eta_1, \ldots, \eta_m$ und ω_1, ω_2 erhält man dann:

$$a_1\omega_1 + a_2\omega_2 = \sum_{i=1}^{m} \alpha_{i+m}\eta_i.$$

Damit haben wir nun für α die Darstellung

$$\alpha = a_0 + a_1\omega_1 + a_2\omega_2,$$

mit $a_0, a_1, a_2 \in o_{\mathcal{F}}$ erhalten.
Wie auch in den anderen Fällen geben wir auch hier ein kurzes Beispiel.

Beispiel 7.35 *Wie schon angemerkt, besitzt der Körper $\mathcal{E} := \mathbb{Q}(\sqrt{10}, \sqrt{5})$ keine relative Ganzheitsbasis über $\mathcal{F} := \mathbb{Q}(\sqrt{10})$, dem kleinsten reell-quadratischen Zahlkörper mit Klassenzahl ungleich 1. Für die Körperdiskriminante erhalten wir auf bekanntem Weg $d_{\mathcal{E}/\mathcal{F}} = (1)$ und*

$$\Phi = (2) \cdot (5o_{\mathcal{F}} + \sqrt{10}o_{\mathcal{F}}) = 10o_{\mathcal{F}} + (10 + 2\sqrt{10})o_{\mathcal{F}}.$$

Aus $35 + 10\sqrt{10} \equiv 5 \bmod 4o_{\mathcal{F}}$ ergibt sich $\nu = 35 + 10\sqrt{10}$ und wir erhalten wegen $h_{\mathcal{F}} = 2$ zum einen $\mathbf{b} = \Phi$, zum anderen $\gamma = 20$.
Damit wird durch

$$\{1, 10\frac{35 + 10\sqrt{10} + \sqrt{5}}{20}, (10 + 2\sqrt{10})\frac{35 + 10\sqrt{10} + \sqrt{5}}{20}\}$$

ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$ gegeben. Durch eine einfache Rechnung erhalten wir als $\mathbb{Z}$–Ganzheitsbasis:

$$\{1, \sqrt{10}, 10\frac{35 + 10\sqrt{10} + \sqrt{5}}{20}, 2\sqrt{10}\frac{35 + 10\sqrt{10} + \sqrt{5}}{20}\}.$$

Für die Körperdiskriminante ergibt sich schließlich

$$|d_{\mathcal{E}}| = \mathrm{N}_{\mathcal{E}/\mathcal{F}}(d_{\mathcal{E}/\mathcal{F}}) \cdot d_{\mathcal{F}}^2 = 1 \cdot 40^2 = 1600.$$

Bemerkung 7.36 *(i) Die hier getroffene Unterscheidung zwischen "der Index ist ein Hauptideal" und "der Index ist kein Hauptideal" ist scharf, denn nach dem Satz von Artin 6.21 existiert genau dann eine relative Ganzheitsbasis, wenn der Index ein Hauptideal ist. Wir haben die eine Richtung des Satzes hier sogar auf konstruktive Weise bewiesen.*

(ii) Die im zweiten Abschnitt für den Fall $h_{\mathcal{F}} \neq 1$ gezeigten Aussagen sind natürlich auch für den Fall $h_{\mathcal{F}} = 1$ richtig. Jedoch ist die Aussage aufgrund der einfacheren Struktur von $o_{\mathcal{E}}$ als $o_{\mathcal{F}}$–Modul im Fall $h_{\mathcal{F}} = 1$ klarer zu formulieren.

(iii) Alle hier vorgeführten Aussagen wurden im wesentlichen konstruktiv bewiesen, so daß die hier vorgeführten Sätze als Grundlage für eine rechnerische Durchführung dienen können. Wir werden dies im nächsten Kapitel sehen.

(iv) Die Wahl des Ideals $\mathbf{b}$ *als*

$$\mathbf{b} = \Phi^{h_{\mathcal{F}}-1}$$

ist in gewissem Sinne willkürlich. Man benötigt lediglich ein ganzes Ideal $\mathbf{b}$*, so daß*

$$\mathbf{b} \cdot \Phi \in \mathcal{H}_{\mathcal{F}}$$

gilt. Diese Tatsache wird bei der Anwendung Beachtung finden.

Kapitel 8

Anwendung

8.1 Konstruktive Grundlagen

Bevor wir die Implementierung des im letzten Kapitel beschriebenen Zusammenhanges darstellen, wollen wir einige wichtige Grundlagen der konstruktiven Zahlentheorie beschreiben und kurz die wichtigsten Begriffe erläutern.
Viele Operationen werden mit $\mathbb{Z}$–Matrizen durchgeführt. Deshalb benötigen wir eine spezielle Normalform für Matrizen, die wir durch eine unimodulare Transformation in $\mathbb{Z}^{(n,n)}$ aus einer beliebigen Matrix $\mathbf{M} \in \mathbb{Z}^{(m,n)}$ erhalten. Die von uns verwendete Normalform ist die Hermite–Normalform $Hnf(\mathbf{M})$. Bei ihr handelt es sich um eine untere Dreiecksmartix, die durch unimodulare Spaltentransformationen aus der ursprünglichen Matrix hervorgegangen ist. Ist $\mathbf{M}$ eine Matrix in $\mathbb{Z}^{(m,n)}$, so existiert eine Transformationsmatrix $\mathbf{U} \in \mathcal{GL}(n, \mathbb{Z})$ mit

$$Hnf(\mathbf{M}) = \mathbf{M} \cdot \mathbf{U}.$$

Eine genauere Beschreibung der Theorie und der Algorithmen zur Bestimmung der Hermite–Normalform findet man in [27] und [29]. Eine ausführliche Diskussion der bekannten Algorithmen findet man in [4]. Bei allen unseren Betrachtungen gehen wir davon aus, daß eine Ganzheitsbasis von $o_{\mathcal{F}}$ vorliegt; sie kann z.B. mit dem von Zassenhaus [33] entwickelten Round–2 bestimmt werden. Es ist dann möglich, algebraische Zahlen (die dann in dieser Basis dargestellt sind) zu addieren, multiplizieren und dividieren. Eine Beschreibung

dieser Algorithmen findet man in [27].
Auf die Ganzheitsbasis aufbauend (wir setzen eine Ganzheitsbasis $\omega_1, \ldots, \omega_n$ von $o_{\mathcal{F}}$ (o.B.d.A sei $\omega_1 = 1$),sowie die Klassenzahl von $o_{\mathcal{F}}$ als bekannt voraus), stellen wir die anderen algebraischen Strukturen (hier i.w. Ideale) dar. Wie schon bemerkt ist jedes Ideal $\mathbf{a}$ ein freier Modul vom Rang $[\mathcal{F} : \mathbb{Q}] = m$. Es existieren also $\alpha_1, \ldots, \alpha_m \in o_{\mathcal{F}}$ mit:

$$\mathbf{a} = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_m$$

Zu diesen $\alpha_1, \ldots, \alpha_m$ existiert nun eine Matrix $\mathbf{M_a} \in \mathbb{Z}^{(m,m)}$ mit

$$(\alpha_1, \ldots, \alpha_m) = \mathbf{M_a}(\omega_1, \ldots, \omega_m).$$

Diese Matrix $\mathbf{M_a}$ bezeichnen wir als eine (nicht eindeutige) $\mathbb{Z}$–Basisdarstellung des Ideals $\mathbf{a}$. Mittels der Hermite–Normalform ist es nun möglich eine eindeutige $\mathbb{Z}$–Basisdarstellung zu gewinnen, denn unimodulare Spaltentransformationen von $\mathbf{M_a}$ entsprechen einer Basistransformation der $\alpha_1, \ldots, \alpha_m$. Eine weitere interessante Anwendung der Hermite–Normalform ist die Addition zweier Ideale. Ist $\mathbf{M_a}$ eine $\mathbb{Z}$–Basisdarstellung des Ideals $\mathbf{a}$ und entsprechend $\mathbf{M_b}$ eine des Ideals $\mathbf{b}$, so ist $\tilde{\mathbf{M}} = Hnf(\mathbf{M_a}, \mathbf{M_b}) \in \mathbb{Z}^{m,2m}$ eine Matrix bei der die letzten m Spalten Nullspalten sind. Bezeichnen wir mit $\mathbf{M}$ die aus den ersten m Spalten bestehende Teilmatrix von $\tilde{\mathbf{M}}$, so ist $\mathbf{M}$ dann die $\mathbb{Z}$–Basisdarstellung von $\mathbf{a} + \mathbf{b}$. Wir werden diesen Zusammenhang später noch verwenden.
Neben der Addition von Idealen werden Algorithmen zur Multiplikation von Idealen, die Zerlegung eines Ideals in Primideale und auch ein Hauptidealtest verwendet. Wir werden diese hier nicht vorführen, da sie in [27] und auch in [29] ausreichend dargestellt wurden.

8.2 Implementierung

Im Rahmen dieser Arbeit wurde das oben Vorgestellte in dem Zahlentheoretischen Programmpacket KANT V2 [12] implementiert. Wir benutzen in diesem Kapitel die im letzten Kapitel benutzen Bezeichnungen für Variablen und Zahlkörper. Die Bestimmung von $o_{\mathcal{E}}$ als $o_{\mathcal{F}}$–Modul gliedert sich in mehrere Schritte:

- Die Bestimmung der Körperdiskriminante,
- Testen, ob eine relative Ganzheitsbasis existiert oder nicht.
- Bestimmung von γ, ν und evtl. $\mathbf{b}$.
- Simultane Bestimmung der $\mathbb{Z}$–Ganzheitsbasis und des $o_{\mathcal{F}}$–Erzeugendensystems (das evtl. auch eine Basis ist) von $o_{\mathcal{E}}$.

Wir werden diese Punkte nun im einzelnen abhandeln. .
Das Hauptproblem liegt sicher in der Bestimmung der relativen Körperdiskriminante $d_{\mathcal{E}/\mathcal{F}}$. Wir folgen bei ihrer Berechnung dem in den Sätzen 7.2, 7.3 und 7.4 aufgezeigten Weg. Wir werden also die Körerdiskriminante in zwei voneinander unabhänigen Schritten bestimmen. Im erste Schritt bestimmen wir den Teiler der Körperdiskriminante, der über $\mu o_{\mathcal{F}}$ und nicht über $2o_{\mathcal{F}}$ liegt und dann im zweiten Schritt den Teiler der Körperdiskriminante, der über $2o_{\mathcal{F}}$ liegt. Um diese beiden Teiler bestimmen zu können, benötigen wir sowohl die Primidealzerlegung von $2o_{\mathcal{F}}$ als auch von $\mu o_{\mathcal{F}}$. Wir bestimmen diese mit den in [29] vorgestellten Algorithmen. Bei all diesen Algorithmen setzten wir die Arithmetik in $o_{\mathcal{F}}$ als gegeben voraus.
Beginnen wir mit dem Algorithmus zur Bestimmung des Teilers der Körperdiskriminante, der über μ und nicht über der 2 liegt:

Algorithmus 8.1 (Bestimmung des Teilers $\mathbf{a}$ der Körperdiskriminante, der über $\mu o_{\mathcal{F}}$ und nicht über $2o_{\mathcal{F}}$ liegt.)
Input: *Zerlegung von* $2o_{\mathcal{F}} = \prod_{i=1}^{k} \wp_i^{k_i}$ *und* $\mu o_{\mathcal{F}} = \prod_{i=1}^{l} \mathbf{q}_i^{l_i}$ *in paarweise versch. Primideale.*
Output: $\mathbf{a} = \prod_{i=1}^{u} \mathbf{a}_i$ *sowie* $\Phi_\mu = \prod_{i=1}^{v} \mathbf{b}_i^{v_i}$. *Hierbei ist* $\mathbf{a}$ *der Teiler der Körperdiskriminante und* $\mathbf{a}_1, \ldots, \mathbf{a}_u, \mathbf{b}_1, \ldots, \mathbf{b}_v$ *sind Primideale.*

(1) $u \leftarrow 0$, $v \leftarrow 0$, $i \leftarrow 0$, $\mathbf{a} \leftarrow o_{\mathcal{F}}$, $\Phi_\mu \leftarrow o_{\mathcal{F}}$.
(2) $i \leftarrow i + 1$.
(3) Falls $i > l$: *Gehe zu (10).*
(4) Falls $\mathbf{q}_i = \wp_j$ *für ein* $j \in \{1, \ldots, k\}$: *Gehe zu (2).*
(5) Falls l_i *gerade: Gehe zu (9).*
(6) $u \leftarrow u + 1$, $\mathbf{a}_u \leftarrow \mathbf{q}_i$, $\mathbf{a} \leftarrow \mathbf{a} \cdot \mathbf{q}_i$.
(7) Falls $l_i - 1 = 0$: *Gehe zu (2).*

(8) $v \leftarrow v+1$, $\mathbf{b}_v \leftarrow \mathbf{q}_i$, $v_v \leftarrow l_i - 1$, $\Phi_\mu \leftarrow \Phi_\mu \cdot \mathbf{q}_i^{l_i-1}$, *Gehe zu (2).*
(9) $v \leftarrow v+1$, $\mathbf{b}_v \leftarrow \mathbf{q}_i$, $v_v \leftarrow l_i$, $\Phi_\mu \leftarrow \Phi_\mu \cdot \mathbf{q}_i^{l_i}$, *Gehe zu (2).*
(10) Ende.

Bei der Bestimmung des Diskriminantenanteils, der über der 2 liegt, müssen wir überprüfen, ob μ ein quadratischer Rest bezüglich gewisser Primidealpotenzen ist. Dazu beachte man:
Ist $\mathbf{a}$ ein Ideal in $o_{\mathcal{F}}$ mit einer $\mathbb{Z}$–Basisdarstellung $\mathbf{M_a} \in \mathbb{Z}^{(n,n)}$ in oberer Hermite-Normalform, so wird durch

$$R_{\mathbf{a}} := \left\{ \sum_{i=1}^{m} \alpha_i \omega_i \,\middle|\, \forall i \in [\![1,n]\!] \;:\; -\frac{m_{ii}}{2} \le \alpha_i < \frac{m_{ii}}{2} \right\} \tag{8-1}$$

ein vollständiges Restsystem gegeben, wenn $\mathbf{M_a} = (m_{ij})$ gilt.
Mittels dieser Feststellung ist es uns nun möglich zu überprüfen, ob μ ein quadratischer Rest ist oder nicht. Dazu betrachten wir ein von 8-1 abgeleitetes "halbes" Restsystem:

$$\tilde{R_{\mathbf{a}}} := \left\{ \sum_{i=1}^{m} \alpha_i \omega_i \,\middle|\, \forall i \in [\![1,n]\!] \;:\; -\frac{m_{ii}}{2} \le \alpha_i < \frac{m_{ii}}{2};\;\; \alpha_{min\{i \in [\![1,n]\!] \mid \alpha_i \neq 0\}} < 0 \right\}.$$

Genau dann, wenn μ ein quadratischer Rest modulo $\mathbf{a}$ ist, muß ein $\alpha \in \tilde{R_{\mathbf{a}}}$ existieren mit:

$$\mu - \alpha^2 \in \mathbf{a}.$$

Wir können deshalb den folgenden Algorithmus formulieren:

Algorithmus 8.2 (Überprüfung, ob μ ein quadratischer Rest modulo eines Ideals ist oder nicht.)
Input: μ, *Ideal* $\mathbf{a}$
Output: *Ausgabe von "μ ist kein quadratischer Rest" oder Ausgabe "μ ist quadratischer Rest". Falls μ ein solcher Rest ist, wird ein α zurückgegeben, so daß $\mu \equiv \alpha^2$ mod $\mathbf{a}$ gilt.*

(1) $\tilde{R_{\mathbf{a}}} := \left\{ \sum_{i=1}^{m} \alpha_i \omega_i \,\middle|\, \forall i \in [\![1,n]\!] \;:\; -\frac{m_{ii}}{2} \le \alpha_i < \frac{m_{ii}}{2},\; \alpha_{min\{i \in [\![1,n]\!] \mid \alpha_i \neq 0\}} < 0 \right\}.$
(2) Falls $\tilde{R_{\mathbf{a}}} = \emptyset$*: Ausgabe "$\mu$ ist kein quadratischer Rest"; Gehe zu (7).*

(3) *Wähle* $\alpha \in \tilde{R}_{\mathbf{a}}$; $\tilde{R}_{\mathbf{a}} \leftarrow \tilde{R}_{\mathbf{a}} \setminus \{\alpha\}$.
(4) $\beta \leftarrow \alpha^2$
(5) *Falls* $\mu - \beta \in \mathbf{a}$: *Ausgabe von "$\mu$ ist quadaratischer Rest" und* α; *Gehe zu (7).*
(6) *Gehe zu (2).*
(7) *Ende.*

Mit diesem Algorithmus sind wir nun in der Lage auch den Teiler der Diskriminante zu bestimmen, der über der 2 liegt. Der folgende Algorithmus beschreibt die Berechnung des Teilers:

Algorithmus 8.3 (Bestimmung des Teilers der Körperdiskriminante, der über $2o_{\mathcal{F}}$ liegt.)
Input: *Zerlegung von* $2o_{\mathcal{F}} = \prod_{i=1}^{k} \wp_i^{k_i}$ *und* $\mu o_{\mathcal{F}} = \prod_{i=1}^{l} \mathbf{q}_i^{l_i}$ *in paarweise versch. Primideale.*
Output: $\mathbf{a} = \prod_{i=1}^{u} \mathbf{a}_i^{u_i}$ *sowie* $\Phi_2 = \prod_{i=1}^{v} \mathbf{b}_i^{v_i}$. *Hierbei ist* $\mathbf{a}$ *der Teiler der Körperdiskriminante und* $\mathbf{a}_1, \ldots, \mathbf{a}_u, \mathbf{b}_1, \ldots, \mathbf{b}_v$ *sind Primideale.*

(1) $u \leftarrow 0,\ v \leftarrow 0,\ i \leftarrow 0,\ \mathbf{a} \leftarrow o_{\mathcal{F}},\ \Phi_2 \leftarrow o_{\mathcal{F}}$.
(2) $i \leftarrow i + 1$.
(3) *Falls* $i > k$: *Gehe zu (12).*
(4) *Falls* $\wp_i = \mathbf{q}_j$ *für ein* $j \in \{1, \ldots, l\}$: *Gehe zu (11).*
(5) $w \leftarrow max\{r \geq 0 \mid \exists \alpha \in o_{\mathcal{F}} \ :\ \alpha^2 \equiv \mu \bmod \wp_i^r\}$
(6) *Falls* $w \geq 2k_i$: *Gehe zu (10).*
(7) $u \leftarrow u + 1,\ \mathbf{a}_u \leftarrow \wp_i,\ u_u \leftarrow 2k_i - w + 1,\ \mathbf{a} \leftarrow \mathbf{a} \cdot \wp_i^{u_u}$.
(8) *Falls* $w - 1 = 0$: *Gehe zu (2).*
(9) $v \leftarrow v + 1,\ \mathbf{b}_v \leftarrow \wp_i,\ v_v \leftarrow (w-1)/2,\ \Phi_2 \leftarrow \Phi_2 \cdot \wp_i^{w-1}$, *Gehe zu (2).*
(10) $v \leftarrow v + 1,\ \mathbf{b}_v \leftarrow \wp_i,\ v_v \leftarrow k_i,\ \Phi_2 \leftarrow \Phi_2 \cdot \wp_i^{2k_i}$, *Gehe zu (2).*
(11) $u \leftarrow u + 1,\ \mathbf{a}_u \leftarrow \wp_i,\ u_u \leftarrow 2k_i + 1,\ \mathbf{a} \leftarrow \mathbf{a} \cdot \wp_i^{l_i}$, *Gehe zu (2).*
(12) *Ende.*

Die Rechenzeit dieses Algorithmus ist leider exponentiell im Grad von $\mathcal{F}$, da wir im ungünstigsten Fall bei der Überprüfung, ob μ ein quadratischer Rest ist oder nicht, für ein Primideal $\wp$ über $2o_{\mathcal{F}}$ $\mathrm{N}(\wp)/2$ viele algebraische Zahlen testen müssen. Falls $\wp$ träge ist, gilt dann z.B. $\mathrm{N}(\wp) \in O(2^{[\mathcal{F}:\mathbb{Q}]})$.
Wir können nun die Relativdiskriminante von $\mathcal{E}/\mathcal{F}$ vollständig bestimmen, indem wir $2o_{\mathcal{F}}$ und $\mu o_{\mathcal{F}}$ in Primideale faktorisieren und dann die Ergebnisse aus den Algorihmen 8.1 und 8.3 zusammensetzen.
Unser weiteres Vorgehen ist nun das folgende:

- Bestimme ν wie in Kapitel 7.
- Überprüfe, ob der Index Φ ein Hauptideal ist. Bestimme gegebenenfalls den Erzeuger $(\gamma) = \Phi$.
- Ist der Index kein Hauptideal, so bestimme $\gamma \in \Phi$ und setze $\mathbf{b} = \gamma o_{\mathcal{F}} \cdot \Phi^{-1}$. Es sei dann $\mathbf{b} = \beta_1 o_{\mathcal{F}} + \beta_2 o_{\mathcal{F}} = \tilde{\beta_1}\mathbb{Z} + \ldots + \tilde{\beta_m}\mathbb{Z}$.
- Ist der Index ein Hauptideal, so bestimme
$$\xi := \frac{\nu + \sqrt{\mu}}{\gamma}$$
$1, \xi$ bilden dann eine $o_{\mathcal{F}}$–Basis und $\omega_1, \ldots, \omega_m$, $\xi\omega_1, \ldots, \xi\omega_m$ bilden eine $\mathbb{Z}$–Basis von $o_{\mathcal{E}}$.
- Ist der Index kein Hauptideal, so bestimme
$$\xi_i := \beta_i \frac{\nu + \sqrt{\mu}}{\gamma} \quad ; (i = 1, 2)$$
und
$$\eta_i := \tilde{\beta_i} \frac{\nu + \sqrt{\mu}}{\gamma} \quad ; (1 \leq i \leq m)$$
$1, \xi_1, \xi_2$ bilden dann ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$ und $\omega_1, \ldots, \omega_m, \eta_1, \ldots, \eta_m$ bilden eine $\mathbb{Z}$–Basis von $o_{\mathcal{E}}$.

Gehen wir nun zuerst auf die Berechnung von ν ein. Nach Lemma 7.13 ist die Existenz von ν gesichert. Durch Anwendung des Algorithmus 8.2 erhalten wir ein $\alpha \in o_{\mathcal{F}}$ mit
$$\mu \equiv \alpha^2 \ mod \ \Phi_2^2.$$

Jedoch erfüllt dieses α nicht notwendig $\alpha \in \Phi_\mu$. Gilt $\alpha \in \Phi_\mu$, so setzen wir $\nu := \alpha$. Ansonsten verfahren wir wie im Beweis von 7.13 (ii) beschrieben. Dazu ist es notwendig simultan Kongruenzen lösen zu können, also den chinesischen Restsatz anwenden zu können. Der Beweis des chinesischen Restsatzes beruht auf der Tatsache, das in comaximalen Idealen $\mathbf{a}_1$ und $\mathbf{a}_2$ $a_1 \in \mathbf{a}_1$ und $a_2 \in \mathbf{a}_2$ existieren mit

$$1 = a_1 + a_2.$$

Solche Zahlen müssen wir bestimmen. Dies ist eine Anwendung der Hermite Normalform, denn ist $(\alpha_{1,1}, \ldots, \alpha_{1,m}) = (\omega_1, \ldots, \omega_m)\mathbf{M}_{\mathbf{a}_1}$ eine $\mathbb{Z}$–Basisdarstellung von $\mathbf{a}_1$ und $(\alpha_{2,1}, \ldots, \alpha_{2,m}) = (\omega_1, \ldots, \omega_m)\mathbf{M}_{\mathbf{a}_2}$ entsprechend eine $\mathbb{Z}$–Basisdarstellung von $\mathbf{a}_2$, so gilt wegen $\mathbf{a}_1 + \mathbf{a}_2 = o_{\mathcal{F}}$

$$(\mathbf{M}_{\mathbf{a}_1}, \mathbf{M}_{\mathbf{a}_2}) \cdot \mathbf{U} = Hnf(\mathbf{M}_{\mathbf{a}_1}, \mathbf{M}_{\mathbf{a}_2}) = E_{n,n}$$

für eine Martix $\mathbf{U} = (u_{i,j}) \in \mathbb{Z}^{(2n,n)}$. Nach 8-1 gilt daher:

$$\begin{aligned}(\omega_1, \ldots, \omega_m) &= (\omega_1, \ldots, \omega_m)(\mathbf{M}_{\mathbf{a}_1}, \mathbf{M}_{\mathbf{a}_2})\mathbf{U} \\ &= (\alpha_{1,1}, \ldots, \alpha_{1,m}, \alpha_{2,1}, \ldots, \alpha_{2,m})\mathbf{U}.\end{aligned}$$

Da wir $\omega_1 = 1$ gefordert haben ergibt sich daraus:

$$\sum_{i=1}^{m} u_{i,1}\alpha_{1,i} + \sum_{i=1}^{m} u_{i+m,1}\alpha_{2,i} = 1.$$

Deshalb leisten $a_j := \sum_{i=1}^{m} u_{i,1}\alpha_{j,i}$ $(j = 1, 2)$ das Gewünschte.
Wählen wir $\mathbf{a}_1 = \Phi_2^2$ und $\mathbf{a}_2 = \Phi_\mu$, so erhalten wir zwei algebraische Zahlen $a_1 \in \Phi_2^2$ und $a_2 \in \Phi_\mu$ mit $a_1 + a_2 = 1$. Ist nun $\kappa \in \Phi_\mu$ beliebig gegeben (z.B. ein Basiselement der $\mathbb{Z}$–Basis, die wir ja sowieso bestimmt haben), so setzen wir $\nu := a_2\alpha + a_1\kappa$. Dann gilt

$$\nu \equiv \alpha \; mod \; \Phi_2^2$$
$$\nu \equiv 0 \; mod \; \Phi_\mu.$$

Wie im Beweis zu 7.13 gesehen erfüllt diese ν dann alle unsere Voraussetzungen. Fassen wir das gerade vorgeführte in einem Algorithmus zusammen:

Algorithmus 8.4 (Bestimmung von ν wie im letzten Kapitel definiert)
Input: μ *sowie* Φ_2 *und* Φ_μ
Output: ν *mit* $\nu^2 \equiv \mu$ *mod* Φ_2^2 *und* $\nu \in \Phi_\mu$

(1) Führe Algorithmus 8.2 mit μ *und* Φ_2^2 *durch. Sei* α *die Ausgabe des Algorithmus.*
(2) Teste $\alpha \in \Phi_\mu$.
(3) Falls $\alpha \in \Phi_\mu$: $\nu \leftarrow \alpha$, *Gehe zu (8).*
(4) Bestimme $\mathbf{M}_{\Phi_2^2}$ *und* $\mathbf{M}_{\Phi_\mu}$ *als* $\mathbb{Z}$*–Basisdarstellung von* Φ_2^2 *und* Φ_μ.
(5) Bestimme a_1, a_2 *wie oben mit* $a_1 \in \Phi_2^2$, $a_2 \in \Phi_\mu$ *und* $1 = a_1 + a_2$.
(6) Wähle $\kappa \in \Phi_\mu$.
(7) $\nu \leftarrow a_2\alpha + a_1\kappa$.
(8) Ausgabe von ν.
(9) Ende.

Wir sind damit nun in der Lage den Kernalgorithmus zur Bestimmung von $o_\mathcal{E}$ anzugeben. Wir werden später noch auf seine Details eingehen.

Algorithmus 8.5 (Hauptalgorithmus: Bestimmung von $o_\mathcal{E}$)
Input: μ
Output: *Eine* $\mathbb{Z}$*–Ganzheitsbasis von* $o_\mathcal{E}$ *und falls eine* $o_\mathcal{F}$*–Basis von* $o_\mathcal{E}$ *existiert eine solche Basis, sonst ein* $o_\mathcal{F}$*–Erzeugendensystem von* $o_\mathcal{E}$ *mit drei Erzeugern.*

(1) Bestimme Index Φ *und Körperdiskriminante von* $\mathcal{E} = \mathcal{F}(\sqrt{\mu})$. *Sei* $\Phi = \Phi_2 \cdot \Phi_\mu$.
(2) Bestimme ν *mit Algorithmus 8.4.*
(3) Teste, ob Φ *ein Hauptideal ist.*
(3) Falls Φ *ein Hauptideal ist: Gehe zu (14).*
(5) Bestimme ein $\gamma \in \Phi$.
(6) $\mathbf{b} \leftarrow \gamma o_\mathcal{F} \cdot \Phi^{-1}$.
(7) Bestimme eine Zweielementdarstellung und eine $\mathbb{Z}$*–Basisdarstellung von* $\mathbf{b}$:
$\mathbf{b} = \beta_1 o_\mathcal{F} + \beta_2 o_\mathcal{F} = \mathbb{Z}\tilde{\beta}_1 + \ldots + \mathbb{Z}\tilde{\beta}_m$

(8) $\xi_i \leftarrow \beta_i \frac{\nu+\sqrt{\mu}}{\gamma}$ $(i = 1, 2)$.

(10) $\eta_i \leftarrow \tilde{\beta}_i \frac{\nu+\sqrt{\mu}}{\gamma}$ $(i = 1, \ldots, m)$.

(11) Ausgabe von $\omega_1, \ldots, \omega_m, \eta_1, \ldots, \eta_m$ *als* $\mathbb{Z}$*–Basis von* $o_{\mathcal{E}}$.

(12) Ausgabe von $1, \xi_1, \xi_2$ *als* $o_{\mathcal{F}}$*–Erzeugendensystem von* $o_{\mathcal{E}}$.

(13) Gehe zu (19).

(14) Bestimme $\gamma \in o_{\mathcal{F}}$ *mit* $\gamma o_{\mathcal{F}} = \Phi$.

(15) $\xi \leftarrow \frac{\nu+\sqrt{\mu}}{\gamma}$.

(16) $\eta_i \leftarrow \xi\omega_i$ $(i = 1, \ldots, m)$.

(17) Ausgabe von $\omega_1, \ldots, \omega_m, \eta_1, \ldots, \eta_m$ *als* $\mathbb{Z}$*–Basis von* $o_{\mathcal{E}}$.

(18) Ausgabe von $1, \xi$ *als* $o_{\mathcal{F}}$*–Basis von* $o_{\mathcal{E}}$.

(19) Ende.

Wie man bemerkt, wird die Körperdiskriminante als solche in diesem Algorithmus nicht benötigt, wir bestimmen sie jedoch trotzdem explizit, da wir so eine einfache Möglichkeit haben, die Diskriminante von $\mathcal{E}$ zu bestimmen. Wie wir gesehen haben, gilt

$$|d_{\mathcal{E}}| = \mathrm{N}(d_{\mathcal{E}/\mathcal{F}}) \cdot |d_{\mathcal{F}}|^2 .$$

Wir wollen nun feststellen, welche Daten von $\mathcal{F}$ bekannt sein müssen, um alle Berechnungen durchführen zu können.
Zuallererst muß eine Ganzheitsbasis von $o_{\mathcal{F}}$ bekannt sein, denn sonst ist es schon nicht möglich die Primidealzerlegung von $2o_{\mathcal{F}}$ und $\mu o_{\mathcal{F}}$ zu bestimmen. Ist die Ganzheitsbasis bekannt, so können wir alle arithmetischen Operationen in $o_{\mathcal{F}}$ durchführen (vgl. [27]). Betrachten wir nun die verwendeten Algorithmen, so stellen wir fest, daß diese bis auf den Hauptidealtest mit einer Ganzheitsbasis alle Berechnungen durchführen können. Nur der Hauptidealtest verlangt ein unabhäniges Einheitensystem von $o_{\mathcal{F}}$. Ein solches System läßt sich z.B. mit dem in [15] beschriebenen Verfahren bestimmen.
Im ungünstigsten Fall benötigen wir also folgende Daten über $\mathcal{F}$:

- Eine Ganzheitsbasis von $o_{\mathcal{F}}$.
- Ein unabhäniges Einheitensystem von $o_{\mathcal{F}}$.

Beschränken wir uns bei unseren Berechnungen darauf, eine $\mathbb{Z}$–Basis von $o_{\mathcal{E}}$ zu bestimmen, so verringert sich der Aufwand enorm, denn man nimmt nun immer an, daß der Index kein Hauptideal ist und führt alle Berechnungen unter dieser Prämisse durch.
Die Folge dieses Vorgehens ist, das man keinen Hauptidealtest mehr durchführen muß, und somit auch kein unabhäniges Einheitensystem von $o_{\mathcal{F}}$ kennen muß. Einzig und allein eine Ganzheitsbasis von $o_{\mathcal{F}}$ muß noch bekannt sein. Es ist nun klar, daß das Verfahren durch diese Vereinfachung enorm beschleunigt wird, denn ein Hauptidealtest ist im allgemeinen sehr Rechenzeitaufwendig.

8.3 Beispiele

Die im letzten Paragraphen vorgestellten Algorithmen wurden im Rahmen dieser Arbeit implementiert, und es wurden eine Reihe von Beispielen gerechnet.
Betrachtet wurden Grundkörper vom Grad zwei, vier und sechs und zu jedem dieser Körper wurde eine größere Anzahl von Erweiterungen untersucht.
Die gewonnen Daten werden (falls dies aus Platzgründen möglich ist) auszugsweise in den folgenden Tabellen präsentiert. In diesen Tabellen findet man neben der Charakterisierung des erzeugenden Elements der Relativerweiterung $\mathcal{E}$ die absolute und relative Körperdiskriminante der Relativerweiterung und die nicht–trivialen ($\neq 1$) $o_{\mathcal{F}}$–Erzeuger von $o_{\mathcal{E}}$. Eine Ganzheitsbasis und ein unabhäniges Einheitensystem der Grundkörper wurde mit den in KANT V2 implementierten Routinen bestimmt. Die Klassenzahl wurde mittels KANT V1 bestimmt. Die nachfolgend aufgeführten Tabellen umfassen folgende Angaben:

p	Es werden Körper betrachtet die mittels p aus dem Grundköper hervorgehen. Die genaue Vorschrift wird immer zusammen mit der Tabelle gegeben.
$\lvert d_{\mathcal{E}} \rvert$	Betrag der Absolutdiskriminante der Relativerweiterung $\mathcal{E}$.
$d_{\mathcal{E}/\mathcal{F}}$	Relativdiskriminante von $\mathcal{E}/\mathcal{F}$
$o_{\mathcal{E}}$	Es werden eine oder zwei algebraische Zahlen angegeben. Diese bilden zusammen mit der 1 ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}}$.

Als einführendes Beispiel betrachten wir den schon mehrfach benutzten Zahlkörper $\mathcal{F} = \mathbb{Q}(\sqrt{10})$. Dieser hat die Klassenzahl 2 und durch

$$\omega_1 = 1, \quad \omega_2 = \sqrt{10}$$

wird eine Ganzheitsbasis von $o_{\mathcal{F}}$ gegeben. Die Erweiterungskörper in dieser Tabelle entstehen durch Adjunktion von $\sqrt{p}$ zu $\mathcal{F}$.

p	$\lvert d_{\mathcal{E}}\rvert$ und $d_{\mathcal{E}/\mathcal{F}}$	$o_{\mathcal{F}}$–Erzeuger von $o_{\mathcal{E}}$
3	57600	$1+\omega_2-\sqrt{3}$
	$6o_{\mathcal{F}}$	$(-12-3\omega_2+(2+\omega_2)\sqrt{3})/2$
5	1600	$(25+10\omega_2-\sqrt{5})/2$
	$o_{\mathcal{F}}$	$(-225-75\omega_2+(5+\omega_2)\sqrt{5})/10$
7	313600	$1+\omega_2-\sqrt{7}$
	$14o_{\mathcal{F}}$	$(-12-3\omega_2+(2+\omega_2)\sqrt{7})/2$
11	774400	$1+\omega_2-\sqrt{11}$
	$22o_{\mathcal{F}}$	$(-12-3\omega_2+(2+\omega_2)\sqrt{11})/2$
13	270400	$(1+2\omega_2-\sqrt{13})/2$
	$13o_{\mathcal{F}}$	
17	462400	$(1+2\omega_2-\sqrt{17})/2$
	$17o_{\mathcal{F}}$	
19	2310400	$1+\omega_2-\sqrt{19}$
	$38o_{\mathcal{F}}$	$(-12-3\omega_2+(2+\omega_2)\sqrt{19})/2$
23	3385600	$1+\omega_2-\sqrt{23}$
	$46o_{\mathcal{F}}$	$(-12-3\omega_2+(2+\omega_2)\sqrt{23})/2$
29	1345600	$(1+2\omega_2-\sqrt{29})/2$
	$29o_{\mathcal{F}}$	
31	6150400	$1+\omega_2-\sqrt{31}$
	$62o_{\mathcal{F}}$	$(-12-3\omega_2+(2+\omega_2)\sqrt{31})/2$
37	2190400	$(1+2\omega_2-\sqrt{37})/2$
	$37o_{\mathcal{F}}$	
41	2689600	$(1+2\omega_2-\sqrt{41})/2$
	$41o_{\mathcal{F}}$	
43	11833600	$1+\omega_2-\sqrt{43}$
	$86o_{\mathcal{F}}$	$(-12-3\omega_2+(2+\omega_2)\sqrt{43})/2$
47	14137600	$1+\omega_2-\sqrt{47}$
	$94o_{\mathcal{F}}$	$(-12-3\omega_2+(2+\omega_2)\sqrt{47})/2$
53	4494400	$(1+2\omega_2-\sqrt{53})/2$
	$53o_{\mathcal{F}}$	

p	$\lvert d_{\mathcal{E}}\rvert$ und $d_{\mathcal{E}/\mathcal{F}}$	$o_{\mathcal{F}}$–Erzeuger von $o_{\mathcal{E}}$
59	22278400 $118o_{\mathcal{F}}$	$1+\omega_2-\sqrt{59}$ $(-12-3\omega_2+(2+\omega_2)\sqrt{59})/2$
61	5953600 $61o_{\mathcal{F}}$	$(1+2\omega_2-\sqrt{61})/2$
67	28729600 $134o_{\mathcal{F}}$	$1+\omega_2-\sqrt{67}$ $(-12-3\omega_2+(2+\omega_2)\sqrt{67})/2$
71	32262400 $142o_{\mathcal{F}}$	$1+\omega_2-\sqrt{71}$ $(-12-3\omega_2+(2+\omega_2)\sqrt{71})/2$
73	8526400 $73o_{\mathcal{F}}$	$(1+2\omega_2-\sqrt{73})/2$
79	39942400 $158o_{\mathcal{F}}$	$1+\omega_2-\sqrt{79}$ $(-12-3\omega_2+(2+\omega_2)\sqrt{79})/2$
83	44089600 $166o_{\mathcal{F}}$	$1+\omega_2-\sqrt{83}$ $(-12-3\omega_2+(2+\omega_2)\sqrt{83})/2$
89	12673600 $89o_{\mathcal{F}}$	$(1+2\omega_2-\sqrt{89})/2$
97	15054400 $97o_{\mathcal{F}}$	$(1+2\omega_2-\sqrt{97})/2$

Wie man sieht, haben von diesen 24 Körpern 10 eine relative Ganzheitsbasis und 14 haben keine. Betrachtet man die 153 Körper, die durch Adjungtion der Quadratwurzel einer ungeraden Primzahl kleiner 900 entstehen, so haben 73 von diesen Körpern eine relative Ganzheitsbasis und 80 haben keine solche Basis. Ohne näher auf dieses Thema einzugehen, möchten wir hier nur kurz anmerken, daß $\mathbb{Q}(\sqrt{10},\sqrt{5})$ der Hilbertsche Klassenkörper zu $\mathbb{Q}(\sqrt{10})$ ist.

Nach diesem, doch eher einfachem Beispiel betrachten wir nun einige Körper vierten Grades.
$\mathcal{F}=\mathbb{Q}(\rho)$ sei von einer Nullstelle ρ des Polynoms $f(t)=t^4-72t^2+256$ erzeugt. Dieser Körper hat die Klassenzahl 4 und eine Ganzheitsbasis wird durch

$$\omega_1=1,\quad \omega_2=1/2\rho,\quad \omega_3=-2\rho+1/32\rho^3,\quad \omega_4=-4+1/8\rho^2$$

gegeben. In der folgenden Tabelle wird die Relativerweiterung durch $\mathcal{F}(\sqrt{p})$ definiert.

p	$\lvert d_{\mathcal{E}}\rvert$ und $d_{\mathcal{E}/\mathcal{F}}$	$o_{\mathcal{F}}$–Erzeuger von $o_{\mathcal{E}}$
3	94758543360000	$1+\omega_2+\omega_3-\sqrt{3}$
	$6o_{\mathcal{F}}$	$(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{3})/2$
5	73116160000	$(-215-70\omega_2-70\omega_3-70\omega_4-\sqrt{5})/2$
	$o_{\mathcal{F}}$	$(3175+3600\omega_2+1125\omega_3+1050\omega_4+(5+6\omega_2+\omega_3)\sqrt{5})/10$
7	2808830402560000	$1+\omega_2+\omega_3-\sqrt{7}$
	$14o_{\mathcal{F}}$	$(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{7})/2$
11	17127899176960000	$1+\omega_2+\omega_3-\sqrt{11}$
	$22o_{\mathcal{F}}$	$(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{11})/2$
13	73116160000	$(169+26\omega_2+26\omega_3+26\omega_4-\sqrt{13})/2$
	$o_{\mathcal{F}}$	$(-6383-7995\omega_2-1807\omega_3-1937\omega_4+(19+25\omega_2+\omega_3+\omega_4)\sqrt{13})/26$
17	6106734799360000	$(1+2\omega_2+2\omega_3+2\omega_4-\sqrt{17})/2$
	$17o_{\mathcal{F}}$	
19	152457137397760000	$1+\omega_2+\omega_3-\sqrt{19}$
	$38o_{\mathcal{F}}$	$(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{19})/2$
23	327374389288960000	$1+\omega_2+\omega_3-\sqrt{23}$
	$4o_{\mathcal{F}}$	$(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{23})/2$
29	51713670760960000	$(1+2\omega_2+2\omega_3+2\omega_4-\sqrt{29})/2$
	$29o_{\mathcal{F}}$	
31	1080388947189760000	$1+\omega_2+\omega_3-\sqrt{31}$
	$62o_{\mathcal{F}}$	$(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{31})/2$
37	137031455541760000	$(1+2\omega_2+2\omega_3+2\omega_4-\sqrt{37})/2$
	$37o_{\mathcal{F}}$	
41	206608793397760000	$(1+2\omega_2+2\omega_3+2\omega_4-\sqrt{41})/2$
	$41o_{\mathcal{F}}$	
43	3999513614786560000	$1+\omega_2+\omega_3-\sqrt{43}$
	$86o_{\mathcal{F}}$	$(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{43})/2$
47	5708536587919360000	$1+\omega_2+\omega_3-\sqrt{47}$
	$94o_{\mathcal{F}}$	$(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{47})/2$
53	576921671272960000	$(1+2\omega_2+2\omega_3+2\omega_4-\sqrt{53})/2$
	$53o_{\mathcal{F}}$	
59	14175598490460160000	$1+\omega_2+\omega_3-\sqrt{59}$
	$118o_{\mathcal{F}}$	$(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{59})/2$
61	1012354725890560000	$(1+2\omega_2+2\omega_3+2\omega_4-\sqrt{61})/2$
	$61o_{\mathcal{F}}$	
67	23573961395445760000	$1+\omega_2+\omega_3-\sqrt{67}$
	$134o_{\mathcal{F}}$	$(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{67})/2$
71	29728072541839360000	$1+\omega_2+\omega_3-\sqrt{71}$
	$142o_{\mathcal{F}}$	$(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{71})/2$

p	$\lvert d_{\mathcal{E}} \rvert$ und $d_{\mathcal{E}/\mathcal{F}}$	$o_{\mathcal{F}}$–Erzeuger von $o_{\mathcal{E}}$
73	2076370332674560000 $73o_{\mathcal{F}}$	$(1+2\omega_2+2\omega_3+2\omega_4-\sqrt{73})/2$
79	4556608567054336000 $158o_{\mathcal{F}}$	$1+\omega_2+\omega_3-\sqrt{79}$ $(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{79})/2$
83	5551952306507776000 $166o_{\mathcal{F}}$	$1+\omega_2+\omega_3-\sqrt{83}$ $(-12-9\omega_2+\omega_3-2\omega_4+(2+\omega_2+\omega_3+2\omega_4)\sqrt{83})/2$
89	4587471731714560000 $89o_{\mathcal{F}}$	$(1+2\omega_2+2\omega_3+2\omega_4-\sqrt{89})/2$
97	6472921074280960000 $97o_{\mathcal{F}}$	$(1+2\omega_2+2\omega_3+2\omega_4-\sqrt{97})/2$

Unter den Körpern in dieser Tabelle befinden sich 9 mit einer relative Ganzheitsbasis und 15 haben keine solche Basis.
Betrachtet man in Ergänzung zu dieser Tabelle wieder alle Erweiterungen, die durch Adjunktion der Quadratwurzel einer ungeraden Primzahl kleiner 900 entstehen, so befinden sich unter diesen Körpern 72 verschiedene Erweiterungen, die eine relative Ganzheitsbasis besitzen und 81 die keine solche Basis haben.
Bevor wir nun zu Grundkörpern höheren Grades übergehen, betrachten wir als Grundkörper den von einer Wurzel ρ von

$$f(t) := t^4 - 176t^2 + 4624$$

erzeugten Körper $\mathcal{F} = \mathbb{Q}(\rho)$. Eine Ganzheitsbasis dieses Körpers ist durch

$$\begin{aligned} \omega_1 &= 1 \\ \omega_2 &= -27/34\rho + 1/136\rho^3 \\ \omega_3 &= 22/17\rho - 1/136\rho^3 \\ \omega_4 &= -22 + 1/4\rho^2 \end{aligned}$$

gegeben. Die Klassenzahl des Körpers ist 8. Für eine ungerade Primzahl betrachten wir nun die Erweiterungen der Form

$$\mathcal{E} := \mathcal{F}(\sqrt{1 + p\omega_2})$$

In der nachfolgenden Tabelle sind wieder die Daten für $3 \leq p \leq 50$ zusammengefaßt.

p	$\lvert d_{\mathcal{E}}\rvert$ und $d_{\mathcal{E}/\mathcal{F}}$	$o_{\mathcal{F}}$–Erzeuger von $o_{\mathcal{E}}$
3	48037275005091840000 $356o_{\mathcal{F}} - (416 + 2\omega_2 + 356\omega_3)o_{\mathcal{F}}$	$\omega_3 + -\sqrt{1+3\omega_2}$ $(-29 - 17\omega_2 + 2\omega_3 - \omega_4 + (3 + 3\omega_2 + 2\omega_3 + \omega_4)\sqrt{1+3\omega_2})/2$
5	41778662733250560000 $(36 + 14\omega_2)o_{\mathcal{F}}$	$-423 - 223\omega_2 - 5\omega_3 - 23\omega_4$ $-(11 + 2\omega_2)\sqrt{1+5\omega_2}$ $(4323 + 4281\omega_2 + 888\omega_3 + 855\omega_4$ $+(141 + 31\omega_2 + 26\omega_3 + 5\omega_4)\sqrt{1+5\omega_2})/6$
7	161128943266037760000 $(-44 + 18\omega_2)o_{\mathcal{F}}$	$-105 + 33\omega_2 - 9\omega_3 + 9\omega_4$ $+(-11 + 2\omega_2)\sqrt{1+7\omega_2}$ $(2595 - 987\omega_2 + 648\omega_3 - 267\omega_4$ $+(177 - 25\omega_2 + 40\omega_3 - 7\omega_4)\sqrt{1+7\omega_2})/6$
11	5828029450813440000 $124o_{\mathcal{F}} + (220 + 2\omega_2 + 124\omega_3)o_{\mathcal{F}}$	$102258 + 116839\omega_2 + 188165\omega_3 + 5258\omega_4$ $+(197 + 485\omega_2)\sqrt{1+11\omega_2}$ $(2978313 - 2847273\omega_2 - 4692480\omega_3 - 246675\omega_4$ $+(-8853 - 12403\omega_2 + 310\omega_3 + 763\omega_4)\sqrt{1+11\omega_2})/78$
13	192227332673765376000 $(-84 + 34\omega_2)o_{\mathcal{F}}$	$-105 + 33\omega_2 - 9\omega_3 + 9\omega_4$ $+(-11 + 2\omega_2)\sqrt{1+13\omega_2}$ $(2595 - 987\omega_2 + 648\omega_3 - 267\omega_4$ $+(177 - 25\omega_2 + 40\omega_3 - 7\omega_4)\sqrt{1+13\omega_2})/6$
17	69432996027432960000 $(12 - 10\omega_2)o_{\mathcal{F}}$	$(855 - 20970\omega_2 - 963\omega_3 - 2097\omega_4$ $-(107 + 233\omega_2)\sqrt{1+17\omega_2})/3$ $(-284013 + 484587\omega_2 - 19458\omega_3 + 101313\omega_4$ $+(-1857 + 4111\omega_2 + 344\omega_3 + 749\omega_4)\sqrt{1+17\omega_2})/18$
19	97518518597320704000 $1604o_{\mathcal{F}} + (-1984 - 2\omega_2 - 1604\omega_3)o_{\mathcal{F}}$	$(-510 - 129\omega_2 - 333\omega_3 - 72\omega_4$ $+(43 + 29\omega_2)\sqrt{1+19\omega_2})/3$ $(7757 + 1465\omega_2 + 562\omega_3 - 131\omega_4$ $+(103 - 35\omega_2 - 46\omega_3 - 31\omega_4)\sqrt{1+19\omega_2})/2$
23	188496362852293017600000 $(156 + 62\omega_2)o_{\mathcal{F}}$	$-423 - 223\omega_2 - 5\omega_3 - 23\omega_4$ $-(+11 + 2\omega_2)\sqrt{1+23\omega_2}$ $(4323 + 4281\omega_2 + 888\omega_3 + 855\omega_4$ $+(141 + 31\omega_2 + 26\omega_3 + 5\omega_4)\sqrt{1+23\omega_2})/6$
29	476479856830552473600000 $(196 + 78\omega_2)o_{\mathcal{F}}$	$-423 - 223\omega_2 - 5\omega_3 - 23\omega_4$ $-(+11 + 2\omega_2)\sqrt{1+29\omega_2}$ $(4323 + 4281\omega_2 + 888\omega_3 + 855\omega_4$ $+(141 + 31\omega_2 + 26\omega_3 + 5\omega_4)\sqrt{1+29\omega_2})/6$
31	622174528554113433600000 $(-204 + 82\omega_2)o_{\mathcal{F}}$	$-105 + 33\omega_2 - 9\omega_3 + 9\omega_4$ $+(-11 + 2\omega_2)\sqrt{1+31\omega_2}$ $(2595 - 987\omega_2 + 648\omega_3 - 267\omega_4$ $+(177 - 25\omega_2 + 40\omega_3 - 7\omega_4)\sqrt{1+31\omega_2})/6$
37	6064546775040000 $4o_{\mathcal{F}} + (4 + 2\omega_2 + 4\omega_3)o_{\mathcal{F}}$	$(536884760 + 536884768\omega_2 + 536884789\omega_3 - 237073356\omega_4$ $+(187498241 - 2026268\omega_2)\sqrt{1+37\omega_2})/117$ $(536884677 + 536884790\omega_2 + 536884672\omega_3 + 536884788\omega_4$ $+(536884732 + 6862643\omega_2 + 536884727\omega_3 + 6862643\omega_4)\sqrt{1+37\omega_2})/234$
41	112655627347820544000 $1724o_{\mathcal{F}}$ $+(-2544 - 2\omega_2 - 1724\omega_3)o_{\mathcal{F}}$	$-7839 + 45455\omega_2 + 137125\omega_3 - 73439\omega_4$ $+(-1841 + 328\omega_2)\sqrt{1+41\omega_2}$ $(62283 - 5048355\omega_2 - 16524768\omega_3 + 8818407\omega_4$ $+(220857 - 39257\omega_2 + 578\omega_3 - 103\omega_4)\sqrt{1+41\omega_2})/78$

p	$\lvert d_{\mathcal{E}}\rvert$ und $d_{\mathcal{E}/\mathcal{F}}$	$o_{\mathcal{F}}$–Erzeuger von $o_{\mathcal{E}}$
43	23034706633668427776000	$-105 + 33\omega_2 - 9\omega_3 + 9\omega_4$
		$+(-11 + 2\omega_2)\sqrt{1 + 43\omega_2}$
	$(-284 + 114\omega_2)o_{\mathcal{F}}$	$(2595 - 987\omega_2 + 648\omega_3 - 267\omega_4$
		$+(177 - 25\omega_2 + 40\omega_3 - 7\omega_4)\sqrt{1 + 43\omega_2})/6$
47	32878193795171352576000	$-423 - 223\omega_2 - 5\omega_3 - 23\omega_4$
		$-(11 + 2\omega_2)\sqrt{1 + 47\omega_2}$
	$(316 + 126\omega_2)o_{\mathcal{F}}$	$(4323 + 4281\omega_2 + 888\omega_3 + 855\omega_4$
		$+(141 + 31\omega_2 + 26\omega_3 + 5\omega_4)\sqrt{1 + 47\omega_2})/6$

Betrachten wir nun einen Körper sechsten Grades. Wir führen die Ergebnisse der Rechnungen als Platzgründen nur exemplarisch auf. Der betrachtete Körper $\mathcal{F}$ ist ein Zahlköper sechsten Grades, der von einer Nullstelle ρ des Polynoms

$$f(t) = t^6 - 2t^5 - 33t^4 + 46t^3 + 282t^2 - 184t - 559$$

erzeugt wird. Dieser Körper hat die Klassenzahl 2 und eine Ganzheitsbasis von $o_{\mathcal{F}}$ wird durch

$$\begin{aligned}
\omega_1 &= 1 \\
\omega_2 &= (106262 + 40764\rho - 24704\rho^2 - 4428\rho^3 + 1021\rho^4 + 80\rho^5)/43511 \\
\omega_3 &= (32669 - 58594\rho - 8531\rho^2 + 8158\rho^3 + 379\rho^4 - 226\rho^5)/43511 \\
\omega_4 &= (-32669 + 102105\rho + 8531\rho^2 - 8158\rho^3 - 379\rho^4 + 226\rho^5)/43511 \\
\omega_5 &= (308776 - 8915\rho - 38373\rho^2 + 1865\rho^3 + 700\rho^4 - 73\rho^5)/43511 \\
\omega_6 &= (220545 - 86386\rho - 56577\rho^2 + 30249\rho^3 + 2488\rho^4 - 1254\rho^5)/43511
\end{aligned}$$

gegeben. Aufgrund der großen Datenmengen dieses Beispieles geben wir nur zwei Erweiterungen explizit an.
Die beiden betrachteten Körper werden von der Quadratwurzel der Primzahlen 41 und 47 erzeugt.
Der nun folgende Körper $\mathcal{E}_1 := \mathcal{F}(\sqrt{41})$ hat eine relative Ganzheitsbasis. Sie wird durch

$$\begin{aligned}
\xi_1 &= 1 \\
\xi_2 &= (1 + 2\omega_2 + 2\omega_3 + 2\omega_4 + 2\omega_5 + 2\omega_6 - \sqrt{41})/2
\end{aligned}$$

gegeben. Die relative Körperdiskriminante wird durch das Hauptideal $41o_{\mathcal{F}}$ gegeben und die Absolutdiskriminante beträgt 1121624296596317839360000000.
Unser zweites Beispiel zu diesem Körper ist die Erweiterung $\mathcal{E}_2 := \mathcal{F}(\sqrt{47})$. Im Gegensatz zu dem Körper $\mathcal{E}_1$ besitzt dieser keine relative Ganzheitsbasis.

Ein $o_{\mathcal{F}}$–Erzeugendensystem von $o_{\mathcal{E}_2}$ bilden die folgenden drei Elemente:

$$
\begin{aligned}
\xi_1 &= 1\\
\xi_2 &= 1+\omega_4+\omega_5+\omega_6-1\sqrt{47}\\
\xi_3 &= (-62-2\omega_2+8\omega_3-\omega_4-7\omega_5-3\omega_6+(2+2\omega_2+2\omega_3+\omega_4+\omega_5+\omega_6)\sqrt{47})/2
\end{aligned}
$$

Wieder ist die relative Körperdiskriminante ein Hauptideal. Sie wird durch $d_{\mathcal{E}_2/\mathcal{F}} = 94o_{\mathcal{F}}$ gegben. Die Absolutdiskriminante lautet

$$|d_{\mathcal{E}_2}| = 16289636367160974770176000000.$$

Betrachtet man alle 14 Erweiterungen von $\mathcal{F}$ für Primzahlen p mit $3 \le p \le 50$, so besitzen von diesen Körpern 9 keine relative Ganzheitsbasis und 5 besitzen eine solche.

Bevor wir dieses Kapitel beenden wollen wir das in dieser Arbeit entwickelte Verfahren mit dem Round–2 vergleichen. Uns interessiert in diesem Zusammenhang, ob das hier vorgestellte Verfahren bei der Klasse der relativquadratischen Zahlkörpern dem Round–2 überlegen ist, d.h. das Ergebniss schneller als der Round–2 liefert. Einen Anhaltspunkt hierzu gibt die nachstehende Tabelle. Alle Rechenzeiten wurden auf einem handelsüblichen Computer mit einem 33 MHz getaktetem Intel 80486 Prozessor ermittelt. Als Betriebssystem diente ein BSD 4.3 Unix. Beide Programme, sowohl der Round–2 als auch die relative – Methode, verwenden die gleiche Arithmetik und Speicherverwaltung von KANT V2.

Beide Methoden bestimmen ausschließlich eine $\mathbb{Z}$–Ganzheitsbasis und die Rechenzeiten, die zur relativen Methode angegeben sind, beinhalten auch alle nötigen Berechnungen im Grundkörper. Da wir nur die $\mathbb{Z}$–Ganzheitsbasis bestimmen wird, wie wir wissen, als Information des Grundkörpers nur dessen $\mathbb{Z}$–Ganzheitsbasis benötigt. Da die angegebenen Rechenzeiten der Beispiele für die im Rahmen der Arbeit durchgeführten Berechnungen repräsentativ sind werden nur einige Zeiten exemplarisch aufgeführt.

Es seien

$$
\begin{aligned}
f_1(t) &:= t^2-10\\
f_2(t) &:= t^4-72t^2+256\\
f_3(t) &:= t^6-2t^5-33t^4+46t^3+282t^2-184t-559
\end{aligned}
$$

und $\mathcal{F}_i = \mathbb{Q}(\rho_i)$ sei der durch eine Nullstelle ρ_i von f_i $(i=1,2,3)$ definierte Zahlkörper. Wir betrachten im weiteren nun Körper $\mathcal{E} = F_i(\sqrt{p})$ (mit $p \in$

$\mathbb{P}$) und führen die Rechenzeiten, die zur Bestimmung einer Ganzheitsbasis $\mathcal{E}$ benötigt wurden, auf.

Körper	Round–2 [sec]	Relative Methode [sec]
$\mathcal{F}_1(\sqrt{5})$	0.3	< 0.1
$\mathcal{F}_1(\sqrt{11})$	0.3	< 0.1
$\mathcal{F}_1(\sqrt{881})$	0.4	< 0.1
$\mathcal{F}_2(\sqrt{5})$	14.3	0.7
$\mathcal{F}_2(\sqrt{13})$	19.3	0.7
$\mathcal{F}_2(\sqrt{31})$	23.6	0.6
$\mathcal{F}_2(\sqrt{53})$	21.5	0.6
$\mathcal{F}_3(\sqrt{3})$	159	9.4
$\mathcal{F}_3(\sqrt{5})$	464	2.8
$\mathcal{F}_3(\sqrt{13})$	313	2.9
$\mathcal{F}_3(\sqrt{17})$	680	3.0

Die im Vergleich zu den anderen Erweiterungen von $\mathcal{F}_3$ hohe Rechenzeit für das Beispiel $\mathcal{F}_3(\sqrt{3})$ ergibt sich durch die Berechnung der Relativdiskriminante. Bei den anderen Beispielen ist sie ein echter Teiler von $po_{\mathcal{F}}$, aber bei diesem Körper beträgt sie $3o_{\mathcal{F}}$, so daß zu ihrer Berechnung (vgl. den letzten Paragraphen) ein höherer Aufwand betrieben werden muss.
Man erkennt aber anhand dieser Tabelle die Überlegenheit der relativen Methode gegenüber der absoluten Methode des Round–2. Deshalb ist es sicher vorteilhaft sich in Zukunft näher mit Algorithmen zu beschäftigen, die aufbauend auf Zwischenkörpern Berechnungen weiterführen.

Kapitel 9

Bezeichnungen

Wir vereinbaren folgende Bezeichnungen (sofern sie nicht im Zusammenhang erklärt werden):

$\mathbb{N}$	:=	Menge der natürlichen Zahlen
$\mathbb{P}$	:=	Menge der Primzahlen
$\mathbb{Z}$	:=	Menge der ganzen Zahlen
$\mathbb{Q}$	:=	Menge der rationalen Zahlen
$\mathbb{R}$	:=	Menge der reellen Zahlen
$\mathbb{C}$	:=	Menge der komplexen Zahlen
R^*	:=	Die Einheiten des Ringes R.
$\|M\| bzw. \sharp M$	:=	Anzahl der Elemente in der Menge M.
$[\![a, b]\!]$	:=	$\{a, \ldots, b\}$ (mit $a, b \in \mathbb{Z};\ a \leq b$)
$[a_1, \ldots, a_k]_{\mathbb{Z}}$	:=	$a_1\mathbb{Z} + \ldots + a_k\mathbb{Z}$
p, q	:=	Primzahlen
$\nu_p(a)$	:=	Exponent von p in der Primfaktorzerlegung von $a \in \mathbb{Z} \setminus \{0\}$
a_{ij} bzw. $A(i, j)$	:=	Element der Matrix A an Stelle (i, j)
$\mathbf{a}, \mathbf{b}, \mathbf{c}$	:=	Ideale
$\wp, \mathcal{P}, \mathbf{q}$	:=	Primideale
$\nu_\wp(\mathbf{a})$	:=	Exponent von $\wp$ in der Primidealzerlegung von $\mathbf{a}$
$\mathbf{M_a}$	:=	$\mathbb{Z}$–Basisdarstellung des ganzen Ideals $\mathbf{a}$
α, β	:=	ganz algebraische Zahlen
$\nu_\wp(\alpha)$	:=	Exponent von $\wp$ in der Primidealzerlegung von αo_F

Literaturverzeichnis

[1] E. Artin und G. Whalpes, *Axiomatic characterization of fields by the product formula for valuations*, Bulletin of the American Math. Society **51** (1945), 469 – 492.

[2] E. Artin, *Questiones de base minimale dans la théorie des nombres algébrique*, Collected Works.

[3] R. Böffgen, *Der Algorithmus von Ford/Zassenhaus zur Berechnung von Ganzheitsbasen in Polynomalgebren*, Annales Universitatis Saraviensis **1 (3)** (1987).

[4] R. J. Bradford, *On the computation of integral bases and defects of integrity*, Dissertation, Bath 1988.

[5] J.W.S. Cassels, *Local Fields*, Cambridge University Press 1986.

[6] J.W.S. Cassels und A. Fröhlich, *Algebraic number theory*, Academic Press 1967.

[7] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer Verlag 1978.

[8] H.M. Edgar, *A number field without an integral basis*, Math. Mag. **52** (1979), 248 – 251.

[9] D.J. Ford, *The construction of maximal orders over a Dedekind domain*, Journal of Symbolic Computation **4** (1987), 69 – 75.

[10] A. Fröhlich, *Discriminants of algebraic number fields*, Math. Zeitschrift **74** (1960), 18 – 28.

[11] A. Fröhlich, *The discriminant of relative extensions and the existence of integral bases*, Mathematika **7** (1960), 15 – 22.

[12] Fachgruppe Computeralgebra der GI, *Computeralgebra in Deutschland*, Fachgruppe Computeralgebra der GI (1993), 212 – 218.

[13] D. Hilbert, *Über die Theorie des relativquadratischen Zahlkörpers*, Math. Ann. **51** (1898).

[14] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jahresbericht, Deut. Math. Ver. **35** (1926).

[15] Max Jüntgen, *Berechnung von Einheiten in algebraischen Zahlkörpern mittels des verallgemeinerten Lagrangeschen Kettenbruchalgrithmus*, Diplomarbeit, Düsseldorf 1990.

[16] S. Lang, *Algebraic Number Theory*, Addison - Wesley 1970.

[17] H. B. Mann, *On integral bases*, Proceedings of the American Mathmatical Society **9** (1958), 167 – 172.

[18] H. B. Mann und V. Hanley, *A note to the paper "On integral bases" by H. B. Mann*, Proceedings of the American Mathmatical Society **9** (1958), 173 – 174.

[19] D. A. Marcus, *Number Fields*, Springer 1977.

[20] R. McKenzie und J. Scheunemann, *A number field without a relative integral basis*, American Mathematical Monthly **78** (1971), 882 – 883.

[21] K. Meyberg, *Algebra 1*, 2. Aufl., Hanser.

[22] K. Meyberg, *Algebra 2*, 2. Aufl., Hanser.

[23] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2. Aufl., Springer Verlag 1990.

[24] J. Neukirch, *Algebraische Zahlentheorie*, 1. Aufl., Springer Verlag 1992.

[25] S. Pierce, *Steinitz classes in quartic fields*, Proceedings of the American Mathematical Society, **43** (1974), 39 –41.

[26] M. Pohst, *Berechnung kleiner Diskriminanten total reeller algebraischer Zahlkörper*, Journal für reine und angewandte Mathematik **278/279** (1975), 278 – 300.

[27] M. Pohst und H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press 1989.

[28] Friedrich Schiller, *Schiller, Ein Lesebuch*, Aufbau–Verlag 1976.

[29] J.Graf v. Schmettow, *Über die Berechnug von Klassengruppen algebraischer Zahlkörper*, Diplomarbeit, Düsseldorf 1987.

[30] J.Graf v. Schmettow, *Beiträge zur Klassengruppenberechnung*, Dissertation, Düsseldorf 1991.

[31] E. S. Selmer, *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Mathematica **51** 1951, 203 – 362.

[32] J. Sommer, *Vorlesung über Zahlentheorie*, B. G. Teubner 1907.

[33] H. Zassenhaus, *Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung*, Funktionalanalysis, Approx. Th., Numer. Math., Oberwolfach 1965, 90 – 103.

Der Metaphysiker

"Wie tief liegt unter mir die Welt,
Kaum seh ich noch die Menschlein unten wallen!
Wie trägt mich meine Kunst, die höchste *unter allen,*
So nahe an des Himmels Zelt!"
So ruft von seines Turmes Dache
Der Schieferdecker, so der kleine Mann
Hans Metaphysikus in seinem Schreibgemache.
Sag an, du kleiner Mann,
Der Turm, von dem dein Blick so vornehm niederschaut,
Wovon *ist er* – worauf *ist er erbaut?*
Wie kamst du selbst hinauf – und seine kahlen Höhn,
Wozu sind sie dir nütz, als in das Tal zu sehen?

(Friedrich Schiller, [28])

Hiermit erkläre ich, daß ich die vorliegende Arbeit selbständig verfaßt und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

Düsseldorf, den 14. Januar 1993

Ich danke Herrn Professor M. Pohst für die Überlassung des Themas dieser Arbeit sowie für seine Diskussionsbereitschaft und seine Ratschläge.
Mein besonderer Dank gilt aber meinen Eltern, die mich nicht nur während meines Studiums immer unterstützt haben. Ihnen ist diese Arbeit gewidmet.